# Troubleshooting Avaya Experience Portal

Release 8.0
Issue 1
September 2020

### Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

### Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

### Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

### Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

### Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

### License types

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

### Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

### Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

### Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third

Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

### Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

### Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

### Trademarks

Avaya, the Avaya logo, Avaya Experience Portal, Avaya Aura® Communication Manager, and Avaya Orchestration Designer are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

### Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

### Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

# Contents

# Chapter 1: Introduction

## Purpose

This document provides general information about troubleshooting and resolving system problems, and detailed information about finding and resolving specific problems.

This document is intended for anyone who is involved with troubleshooting and maintaining Avaya Experience Portal at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

# Chapter 2: Diagnostic procedures

## Troubleshooting categories

When the Avaya Experience Portal system experiences problems, the problems are detected in one of the following categories:

**Customer-reported problems:** The administrator must collect specific information from customer and the system, regarding what actually happened, and how the system behaved

**System generated alarms:** Experience Portal events and alarms provide a way to troubleshoot problems which occur on the Experience Portal system. Major and Critical alarms combined with Error and Fatal events identify the large issues. Minor alarms and Warning events can identify small issues.

**Call report analysis:** The analysis of standard reports reveals the problems so that you can avoid the system failure. For this reason, you should use the system report capabilities to generate and analyze the standard reports.

## Experience Portal system status

Experience Portal generates events and alarms when you make changes in the Experience Portal system. Some of these notifications are purely informational, however, others indicate errors. There are two ways to monitor Experience Portal events and alarms:

- View internally generated Experience Portal events and alarms through the EPM web interface.
- Use third party network management software to receive SNMP notifications when certain error conditions occur.

You can also generate an Audit Log report to view recent system configuration changes and login activities.

### Checking the status of MPPs

The following table provides the tasks you need to perform to check the status of the MPPs in a Experience Portal system.

| # | Task | ✔ |
|---|---|---|
| 1 | Log into EPM. | |
| 2 | Check the operational states of all MPPs .<br>If the operational state of an MPP is:<br>• Running but the MPP is not taking calls, check for a synchronization problem between EPM and the MPP as described in Identifying synchronization problems between the EPM and an MPP on page 16.<br>• Not running and you did not intentionally place it in this state, continue with this procedure. | |
| 3 | Check the alarm status for all MPPs.<br>If the <System name> Details tab on the System Monitor page indicates any alarm conditions, click a red or yellow alarm symbol. The Alarm Monitor page helps identify which system component is having problems.<br>**Note:**<br>The Alarms column displays one of the following alarm status indicators for all MPP:<br>• Green: There are no active major or critical alarms<br>• Yellow: There are one or more active minor alarms<br>• Red: There are one or more active major or critical alarms | |
| 4 | Generate an alarm report.<br>Examine the alarm report for the alarms generated by the system component in question. All alarms have associated events, which are identified in the alarm report. To obtain more details about a particular event, click the event in the **Event Code** column of the report. | |
| 5 | Generate an event log report using the Log Viewer.<br>Examine the Log Report to see if you can identify other related events that occurred during the same time. | |

# Checking the status of port connections

If all MPP servers are correctly functioning and do not indicate any error or alarm conditions, the next step is to check the Port Distribution page. This page provides information about the status of port connections to the Communication Manager.

## Solution

### Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.

2. From the EPM main menu, select **Real-time Monitoring** > **Port Distribution**.
3. If the **Current Allocation** column shows that:

| MPP port allocation | Next step |
|---|---|
| **None of the MPPs have allocated ports** | No MPP servers have allocated ports on page 11 |
| **One or more MPPs do not have allocated ports.** | One or more MPPs have no allocated ports on page 11 |
| **One or more licensed ports have not been allocated to an MPP.** | One or more licensed ports have not been allocated to an MPP server on page 13 |

# No MPP servers have allocated ports

The Port Distribution page shows that none of the MPP servers in the system have allocated ports. This problem can occur because:

- Experience Portal cannot connect to the Avaya license server.
- The Experience Portal license has expired.
- The Experience Portal license server is down.
- The specified gatekeeper address or alternative gatekeeper address is incorrect.

## Proposed Solution

### Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. From the EPM main menu, select **Security** > **Licensing**.
3. On the Licensing page, verify the following:
   - Connection to the Avaya license server.
   - Expiry date on the Experience Portal license.
   - Status of the Experience Portal license server.
4. From the EPM main menu, select **System Configuration** > **VoIP Connections**.
5. On the VoIP Connections page, check the gatekeeper and alternate gatekeeper addresses.

# One or more MPPs have no allocated ports

The Port Distribution page shows that one or more of the MPPs in the system do not have allocated ports. This problem can occur because:

- The MPP has stopped, is not responding, or is offline.

- Experience Portal does not have sufficient licensed port connections to support the MPP servers in the system.

## Proposed Solution 1

### About this task

Check the operational status of each MPP that does not have allocated ports.

### Procedure

1. Log on to the EPM web interface by using an account with the Administration or Operations user role.
2. From the EPM main menu, select **Real-time Monitoring** > **System Monitor**.
3. On the <System name> Details tab, check the **Mode** and **State** column for the MPP servers in the system.

   If the mode of one or more MPP servers is listed as Offline, or if the state is listed as Halted, Not Responding, Restart Needed, or Stopped, continue with Step 4. If all MPP servers are up and running, continue with Proposed Solution 2 on page 13.
4. From the EPM main menu, select **System Management** > **MPP Manager**.
5. On the MPP Manager page, use the Selection check box in the MPP server table to select which MPP you want to change.
6. If you want to:
   - Bring an MPP online:
     a. Click **Online** in the **Mode Commands** group.
     b. Use the Selection check box in the MPP server table to select the MPP.
     c. Click **Start** in the **State Commands** group.
   - Start a stopped or halted MPP, click **Start** in the **State Commands** group.
   - Restart an MPP, click **Restart** in the **State Commands** group.
   - Reboot an MPP, click **Reboot** in the **State Commands** group.
7. When you have finished setting the operational mode, click **Refresh** to ensure the mode is correctly set up.
8. If the MPP does not respond to command through the EPM, reboot the physical MPP server manually.
9. From the EPM main menu, select **Real-time Monitoring** > **System Monitor**.
10. If all MPP servers are listed as Online and Running, from the EPM main menu, select **Real-time Monitoring** > **Port Distribution**.
11. Verify that all MPP servers now have allocated ports. If there is still a problem, continue with Proposed Solution 2.

## Proposed Solution 2

### About this task

Verify that you have created enough VoIP connections.

### Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. From the EPM main menu, select **System Configuration** > **VoIP Connections**.
3. If you are using:

| VoIP connection type | Next steps |
|---|---|
| **H.323 only** | a. Go to the H.323 tab and count the number of stations defined in the **Stations** column.<br>b. If there are fewer stations than ports, either add more H.323 connections or add more stations to one or more existing connections. |
| **SIP only** | a. Go to the SIP tab and look at the **Maximum Simultaneous Calls** defined for the active SIP connection.<br>b. If the maximum number of calls is less than the total number of licensed ports, click the connection name to open the Change SIP Connection page and increase the maximum number of calls for the connection. |
| **H.323 and SIP** | a. Go to the H.323 tab and count the number of stations defined in the **Stations** column.<br>b. Go to the SIP tab and look at the **Maximum Simultaneous Calls** defined for the active SIP connection.<br>c. If the number of defined stations plus the maximum number of SIP calls does not equal the number of licensed ports available, either increase the number of H.323 stations or the maximum number of SIP calls. |

# One or more licensed ports have not been allocated to an MPP server

The Port Distribution page shows that one or more licensed ports are not allocated to an MPP server. This problem can occur because:

- The MPP is in Offline or Test mode.
- The maximum call capacity for the MPP is too low.

## Proposed Solution 1

### About this task

Check the operational status of each MPP that does not have allocated ports. Change the operational status to Online.

### Procedure

1. Log on to the EPM web interface by using an account with the Administration or Operations user role.
2. Select **Real-time Monitoring** > **System Monitor**.
3. On the <System name> Details tab, check the status of the MPP servers in the system.

   If one or more MPP servers is down, continue with Step 4. If all MPP servers are up and running, continue with Proposed Solution 2.
4. From the EPM main menu, select **System Management** > **MPP Manager**.
5. On the MPP Manager page, use the Selection check box in the MPP server table to select which MPP you want to change.
6. Click the desired operational state button in the **Mode Commands** group. You can select:
   - **Test** if the MPP server is currently in Offline mode.
   - **Online** if the MPP server is currently in Offline mode.
7. When you have finished setting the operational mode, click **Refresh** to ensure the mode is correctly set up.

## Proposed Solution 2

### About this task

Check the maximum call capacity of the MPP. Change the value.

### Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. From the EPM main menu, select **Real-time Monitoring** > **System Monitor** and go to the appropriate <System name> Details tab.
3. In the **Server Name** column, click the name of the MPP whose details you want to view.
4. On the <MPP name> Details page, review the value of the **Maximum Call Capacity** field.

   If this value is too low, Experience Portal will not allocate enough ports to the MPP. To increase the number of allocated ports, you must increase the value of the **Maximum Simultaneous Calls** field on the Change MPP Server page.
5. From the EPM main menu, select **System Configuration** > **MPP Servers**.
6. On the MPP Servers page, click the name of the MPP you want to reconfigure in the **Name** column.
7. On the Change MPP Server page, update the value in the **Maximum Simultaneous Calls** field.

   For assistance in sizing your MPP server capacity and setting the correct value for the **Maximum Simultaneous Calls** parameter for each MPP server, contact your Avaya Services representative or Avaya Business Partner. For more information, see the *MPP server capacity* topic in the *Administering Avaya Experience Portal*.

8. Click **Save** to save your changes.

# Event and alarm logs

Other places to look for indications of problems are the event and alarm logs. You can use the Log Viewer and the Alarm Manager to generate reports that can help to diagnose and resolve problems with the system.

When you generate these reports, use the information you collected regarding the time the problems occurred and what components might be involved. As you examine the events and alarms that the system generated on those components during the time the problems occur, you can get a good sense of what the problem is and how to resolve it. Use the event and alarm codes in these reports to diagnose any further problems.

For more information about generating:

- Event reports, see the *Creating an event report* topic in the *Administering Avaya Experience Portal*.
- Alarm reports, see the *Creating an alarm report* topic in the *Administering Avaya Experience Portal*.

You can also use the information from these reports to help identify the call sessions that experienced the problems. Once you identify call sessions, you can check the transcriptions for those call sessions to further diagnose the problem.

# Cannot generate a log or alarm report

If you cannot generate a Log Report or an Alarm Report within the EPM web interface, you can still view and examine the event and alarm logs for EPM. The EPM log file contains the same information as displayed in the Log Report and Alarm Report.

**Note:**

Examine the EPM log file directly *only* if you cannot use the EPM web interface to generate a Log Report or Alarm Report.

## Proposed Solution

### Procedure

1. Log on to the EPM Linux server.
2. In a text editor, open the EPM log file from the following location: `$AVAYA_VPMS_HOME/logs/avaya.vpms.log`

# Checking the application for proper function and behavior

### Procedure

1. Check the resources being used by all current applications in the system by selecting **Real-time Monitoring** > **Active Calls** from the EPM main menu.
2. In Experience Portal, create an Application Detail report or Application Summary report. These reports let you view application messages and any `log` tag messages downloaded with the report data.
3. Check the transcriptions of the call sessions using the Session Detail report.
4. Review the log files for the application server and any Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) servers used by the application.

# Enabling Avaya Voice Browser Logging

### About this task

Enable Avaya Voice Browser (AVB) logging if you need more information about the application problems that you encountered.

**! Important:**

Enabling AVB logging can cause performance degradation.

### Procedure

If you want to:

- Enable AVB logging for all MPPs in your Experience Portal system, see the *Setting the global grace period and trace level parameters* topic in *ImplementingAvaya Experience Portal on a single server* .
- Enable AVB logging on a specific MPP, see the *Changing an MPP* topic in *Administering Avaya Experience Portal*.

# Identifying synchronization problems between the EPM and an MPP

### Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. From the EPM main menu, select **Real-time Monitoring** > **System Monitor** and go to the appropriate <System name> Details tab.
3. In the **Server Name** column, click the name of the MPP.
4. On the <MPP name> Details page, click **Service Menu** in the **Miscellaneous** group.

The Media Server Service Menu opens in a new browser window.

5. Arrange the browser windows so that you can see both the <MPP name> Details page and the Media Server Service Menu home page.
6. Compare the following fields on the two pages:

| EPM Field and Group | Media Server Service Menu Field/Table |
|---|---|
| Current State in the Operational State group | Run State in the MPP Status table |
| Current State in the Configuration group | Configuration State in the MPP Status table |
| Last Successful Poll in the General Information group | Time of last heartbeat in the MPP Status table |

### Next steps

If these fields do not match, follow the procedure described in Synchronizing the EPM and an MPP on page 17.

## Synchronizing the EPM and an MPP

### Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. From the EPM main menu, select **System Maintenance** > **Log Viewer**.
3. In the Log Viewer page, create an event report for the **EPM** and the MPP you want to synchronize.

   **Tip:**

   When you specify the report criteria, in the **Date and Time** group, make sure the report starts before the last successful poll of the MPP. You can find this date on the <MPP name> Details page.
4. Examine the resulting report for any messages that contain the word "heartbeat" or "poll" and see if these messages have exact information to solve the problem.

   For more information, see the *Events and alarms* topic in the *Administering Avaya Experience Portal* guide.
5. For more information related to the report, log on to the Media Server Service Menu for the MPP:
   a. From the EPM main menu, select **Real-time Monitoring** > **System Monitor** .
   b. In the **Server Name** column, click the name of the MPP.
   c. On the <MPP name> Details page, click **Service Menu** in the **Miscellaneous** group.
6. Click **Logs** in the Media Server Service Menu menu bar.
7. On the Log Directories page, click **MMS**.
8. On the Log Files page, click **MmsServer.log**.

9. Examine the log file to see if the MMS web server has been receiving heartbeat requests from the EPM.
10. If the log file shows that heartbeat requests are received, log onto Linux on the MPP server.
11. Verify that the `mpp` service is running by entering the `/sbin/service mpp status` command.
12. If the `mpp` service is not running, enter the `/sbin/service mpp start` command.
13. Navigate to the httpd logs directory by entering the `cd /var/log/httpd` command.
14. Examine the following log files to see if Apache has been receiving heartbeat requests from the EPM server:
    - `error_log`
    - `ws_access_log`
    - `ws_error_log`
15. If the log files show that heartbeat requests are received, reboot the MPP server.
16. Log in to Linux on the EPM server.
17. Examine the `$CATALINA_HOME/logs/catalina.out` log file to see if any errors were generated during the reboot.
18. If the problem still exists after the MPP server restarts, reboot the EPM server.

**Related links**

System does not answer or produces only busy signals on page 64

# Checking the call session

### About this task

You can use information gathered from callers and from event and alarm reports to identify particular call sessions that had problems. Once you identify the problem sessions, use the Contact Detail report to view session information.

### Procedure

1. Create a Contact Detail report.
2. Click the **View Session Details** icon at the end of the appropriate row.
3. On the Session Details page for the session, review the call session details for information about the problem that occurred during the session.

### Next steps

If you still cannot determine the problem from an examination of the call session, more information is available in the session log file.

## Viewing the session log file

### About this task

The log file for the session is called `$AVAYA_MPP_HOME/logs/process/SessMgr/SessionSlot-XXX.log`, where *XXX* is the value of the **Slot** field on the Session Details page.

### Procedure

1. On the Session Details page for the call, go to the **Server Information** group.
2. Get the value of the session slot from the **Slot** field.
3. To view the log file through Experience Portal:
    a. Log into the Media Server Service Menu.
    b. From the Media Server Service Menu, select **Logs**.
    c. On the Log Directories page, click **SessMgr**.
    d. On the Log Files page, click **View** or **Download** for the `SessionSlot-XXX.log` entry that matches the one you want to view.

       As the session log files are large in size, these files might take time to display or save to the location you select for **Download**.

## Finding the version numbers for the Experience Portal software

### About this task

If you need to contact technical support, you should have the version numbers for the Experience Portal software available.

### Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. Click **Help** at the top of any EPM page and select **About**.

   The EPM displays the About Avaya Experience Portal page, which shows the version numbers of the EPM and MPP software.
3. To get the version number for the WebLM server:
    a. From the EPM main menu, select **Security** > **Licensing**.

       Depending on the user role associated with your account, the EPM web interface displays the Licensing page or the View Licensing page.

b. Click **Verify**.

The EPM opens a new browser window displaying the License Administration page for the WebLM license server, which displays the version number for that server.

# Timer Release

In Experience Portal 7.1 and later, the default values of MPP timers that control speech server events and protect speech server failures have been re-calibrated. Depending upon the application deployed, you can modify these values.

| Timer Name | Previous Release | Experience Portal 7.1 |
|---|---|---|
| mpp.mrcpsessionrefresh.timer | 40 | 40 |
| mpp.mrcppoststartofspeechevent.timer | 20 | 80 |
| mpp.mrcppostrecogstartedevent.timer | 20 | 20 + Dynamic value |

### mpp.mrcpsessionrefresh.timer

Use this timer as a guard against a speech server failure while playing prompts or using ASR. You can also use this timer to generate some traffic when speech is not being used to prevent a speech server session timeout.

`mpp.mrcpsessionrefresh.timer` value should always be set to 20 seconds lesser than the speech server session timeout value. This value must be larger than the largest prompt to be played and must be longer than the longest expected ASR response.

The session timeout value is 60 seconds by default for Nuance. On each Nuance speech server, modify the value in the `server.mrcp2.sip.sessionTimeout` for MRCP V2 and in `server.mrcp1.rtsp.sessionTimeout` for MRCP V1 in the configuration file. Other vendors may have a different way to update this value.

For example, if you need to play a prompt that is 180 seconds long, then set the value of `mpp.mrcpsessionrefresh.timer` to 190 seconds on each MPP server and set the speech server session timeout to 210.

### mpp.mrcppoststartofspeechevent.timer

Use this timer as a guard for cases where the MPP has received a Start of Speech Event, but has not received Recognition done or an error response because the speech server has gone out of service.

The value should always be 20 seconds more than the maximum speech value set for the speech server.

The value on the speech server can be updated in the following ways in the order of precedence:

1. As a VXML property: This method is the preferred method as it is specific to Individual Grammar. property `<name="maxspeechtimeout" value="10s"/>`

2. By logging into the EPM and changing the value of Recognition Timeout:
   - Log on to **EPM** > **Applications** > **Change Application** page.
   - In **Speech Parameters** > **ASR** change the value of Recognition Timeout.

     This is a parameter that applies to all the recognition requests for the particular application.
3. By changing the `maxspeechtimeout` property: On the Nuance Speech Server, change the `maxspeechtimeout` property in the `Recognizer's Baseline.xml` file.

   (Default is 22s for V1 and 10s for V2)
4. Repeat Step 3 on all Speech Servers.

   Other vendors may have a different way to specify this value.

   If the maximum value set for speech for all applications is less than 60 seconds, then there is no need to modify the MPP configuration. For values greater than 60 seconds, modify the MPP configuration value for mpp.mrcppoststartofspeechevent.timer to the maximum speech value + 20 seconds on each MPP server.

### mpp.mrcppostrecogstartedevent.time

Use this timer as a guard against a speech server failure while waiting for recognition-complete. The guard timeout value is dynamically calculated by adding the configured value (mpp.mrcppostrecogstartedevent.timer) to the no-input timeout value passed to the speech server.

**Note:**

As the guard value is dynamically calculated, the MPP configured value should not be modified.

A no-input timeout value is passed to the speech server as RECOGNITON-START-TIMERS in case of MRCP V1 or START-INPUT-TIMERS in case of MRCPv2.

This MPP guard value starts with `mpp.mrcppostrecogstartedevent.timer` that is set to 20 seconds, and then adds the no-input timeout value set through one of the following method in order of precedence:

1. Change the value of VXI: The default value of VXI for timeout is 7 seconds. You can change this value per recognition request as follows:

   <property name="timeout" value="10s"/>

   For example, the guard's value will be 20 + 10 = 30 seconds.
2. Globally updating the no-input timeout value: This method updates the no-input timeout value globally in the Application, unless each recognition request has a property tag used for setting the timeout value as mentioned in method 1.
   - Log on to **EPM** and navigate to **Applications** page > **Speech Parameters** > **ASR**.
   - Update the value of No Input Timeout.

For example: No Input Timeout = 45000 milliseconds

This will set the value of the guard to 20 + 45 = 65 seconds.

**Note:**

The no-input timeout value passed to the speech server should not be greater than the value set for the speech server session timeout.

# Chapter 3: Troubleshooting worksheets

## Collecting information related to a problem

If problems are reported by customers trying to call in to the system or problems related to outcalls, collect as much information as you can. The following steps include the questions that you need to answer about the problem and the information to collect.

| # | Task | ✔ |
|---|---|---|
| 1 | Obtain the following information from the caller:<br>What number did the caller dial (the DNIS)?<br>What number was the caller calling from (the ANI)?<br>What time (and day) did the caller try to call the system, and what time zone was the caller calling from?<br>How did the system respond when the caller tried to call in? For example, did the system:<br>• Give a busy signal?<br>• Ring but not answer?<br>• End the call unexpectedly in the middle of the session?<br>• Produce garbled or unrecognizable output?<br>• Fail to recognize the responses of the caller?<br>• Suddenly stop responding to the caller? | |
| 2 | Using the information from the caller:<br>• Try to reproduce the system response.<br>• Collect whatever additional information that you can from your own observations of the system responses.<br>If you can reproduce the system response and the problem, you can easily troubleshoot the problem. | |
| 3 | Check the Avaya Experience Portal system to see if any component see if any component fails or is not functioning correctly. For example, check the MPP status. | |
| 4 | Check the event and alarm logs. | |

*Table continues…*

| # | Task | ✔ |
|---|---|---|
| 5 | Check the transcription of the call session to learn exactly what happened with the call. | |
| 6 | If you are unable to troubleshoot the problem and need to contact customer support:<br>• Collect and pack the diagnostic logs on the MPP as described in Packing MPP logs and transcriptions in a TAR file on page 137.<br>• Get the version numbers of the Experience Portal software as described in Finding the version numbers for the Experience Portal software on page 19. | |

**Related links**

Packing MPP logs and transcriptions in a TAR file on page 137

# Information needed for Services to initiate troubleshooting

When you need to contact customer support, collect as much information as you can. The following steps include the questions that you need to answer about the problem and the information to collect.

**Note:**

Steps 3 to 11 are mandatory.

| # | Task | ✔ |
|---|---|---|
| 1 | You must update Experience Portal with the most recent Service Pack installed on the system. You can get the latest Service Pack from the Avaya Support site at http://support.avaya.com. | |
| 2 | Check if the issue is a known issue that is listed as Product Support Notice (PSN). PSN's are posted on the Avaya support site at http://support.avaya.com under the appropriate release in Experience Portal product category. | |
| 3 | Detailed description of the issue. | |
| 4 | Release information of the Experience Portal on which you are facing the issue. | |
| 5 | Is the system a fresh install or an upgrade. In case of an upgrade, from which version is the system upgraded. | |
| 6 | Version of the RHEL or Avaya Linux installed. | |
| 7 | Total Number of EPM and MPPs deployed; along with the port and license information. | |
| 8 | Versions and license information of CM (PBX/switch), ASR and TTS. | |

*Table continues…*

| # | Task | ✔ |
|---|---|---|
| 9 | Remote access details for accessing the machine remotely to debug the problem. | |
| 10 | Warning and Errors seen in the logs. Export the alarm logs/Log Report from EPM web page. | |
| 11 | Collect the EPM and MPP logs. For details see, Collecting logs from EPM on page 25 and Collecting logs from MPP on page 26. | |
| 12 | Special instructions, if any. | |

## Collecting logs from EPM

### Procedure

1. Log in to the EPM web interface using an account with the Administration user role.
2. Collect the logs from the Alarm Manager menu:
    a. From the EPM main menu, select **System Maintenance** > **Alarm Manager**.
    b. Enter the appropriate time when the failure occurred in the **Date and Time** field.
    c. Click **OK** to generate the alarm report.
    d. Export the report.
3. Collect the logs from the Log Viewer menu:
    a. From the EPM main menu, select **System Maintenance**n > Log Viewer.
    b. Enter the appropriate time when the failure occurred in the **Date and Time** field.
    c. Click **OK** to generate the report.
    d. Export the report.
4. Collect the logs from the Reports menu:
    a. From the EPM main menu, select Reports > Standard Reports.
    b. Click on the Contact Detail report.
    c. Enter the appropriate time around when the failure occurred in the **Date and Time** field.
    d. Click **OK** to generate the report.
    e. Click **Export** and then select **Export as XLS format** or **Export as PDF format** to export the report in the desired format.
    f. Repeat this procedure for the Session Detail report.
5. Collect all log files from `/opt/Avaya/ExperiencePortal/VPMS/logs`.
6. Collect the `catalina.*` files from the `$CATALINA_HOME/logs` folder.

# Collecting logs from MPP

## Procedure

1. Log on to the Linux server of the MPP.
2. On each MPP, enter the `getmpplogs.sh --logs --transcriptions --debugfiles` command to get the MPP logs.

   The filename of the stored logs and the path appears.

# Chapter 4: Troubleshooting EPM issues

## Taking the Auxiliary EPM offline using the EPM Web interface

### About this task

Before you work with an EPM server, you need to take the EPM offline. This procedure explains how take the EPM offline using the EPM Web interface.

### Procedure

1. Log on to the EPM web interface by using an account with the Administration or Operations user role.
2. From the EPM main menu, select **System Management > EPM Manager**.
3. 3. On the EPM Manager page, use the Selection check box in EPM server table to select which EPM server you want to take offline.
4. Click the **Stop** button in the **State Commands** group and confirm your selection when prompted.

   Avaya Experience Portal stops the selected EPM server when the last active call completes or the grace period expires, whichever comes first.
5. After a few minutes, click **Refresh** and verify that the **State** is **Stopped** for the EPM server that you want to upgrade.
6. If the EPM operational state:
   - Changed to **Stopped**, continue with this procedure.
   - Did *not* change, you need to stop the `vpms` service as described in Stopping the EPM service on page 28.
7. Use the Selection check box in the EPM server table to reselect the EPM server you want to take offline.
8. Click **Offline** in the **Mode Commands** group.
9. Click **Refresh** and verify that the **Mode** is **Offline** for the EPM server you want to upgrade.

# Stopping the EPM service

You should always try to take the EPM offline using the EPM web interface. If the EPM is not communicating with the EPM , however, you can take the EPM offline by stopping the `vpms` service.

### Procedure

1. Log in to Linux on the EPM Server.

   If you are an Avaya Services representative, and are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

   Otherwise, log in to Linux locally as root user, or log in remotely as a non-root user then change the user to root by entering the su - command.
2. Enter the `/sbin/service vpms stop` command.

# Authorized user cannot log in to EPM

An authorized individual cannot log in to the EPM. This problem typically occurs because:

- The user does not have the correct login ID or password.
- The user entered the login ID or password incorrectly more than the allowable number of times, and the account is locked.

## Proposed Solution

### Procedure

1. Verify that the user has entered the correct login ID and password.
2. Check to see if the account is locked.
3. If the account is locked, have a system administrator unlock it or wait for the lockout period to end.

   You can set the Lockout period on the **Login Options** web page.

# User cannot log in to the EPM web interface remotely

If you cannot log into the EPM web interface remotely, the primary EPM server may have lost its network connection or Tomcat may not be running.

To investigate this, you need to check the physical network connection and test the communication between the primary EPM server and the MPP servers. This procedure assumes that:

- Your Avaya Experience Portal deployment consists of the EPM and MPP software running on two or more dedicated servers.
- ICMP is not disabled on your system and you can **`ping`** one server from another.

## Proposed Solution

### Procedure

1. Log into Linux on another server in the Experience Portal network and enter the `ping` *`epm_identifier`* command, where *`epm_identifier`* is the hostname or IP address for the primary EPM server.
2. If the **`ping`** is unsuccessful:
   a. Go to the physical primary EPM server and make sure that the network cable is properly connected.
   b. Enter the **`ping`** command again.
3. If the primary EPM server responds to the **`ping`** command, log into Linux on the primary EPM server as any user.
4. Enter the `ping` *`mpp_identifier`* command, where *`mpp_identifier`* is the hostname or IP address for one of the MPP servers.
5. If the **`ping`** command is unsuccessful, repeat the **`ping`** command specifying another MPP in the Experience Portal system until you receive a successful `ping` message or you have tried contacting all available MPP servers..

   If any MPP servers on the system respond to the **`ping`** command, then the network is functioning and the issue could be caused by problems with Tomcat on the primary EPM server. Follow the procedures in Troubleshooting vpms service issues on page 30.
6. If you cannot ping any MPP servers from the primary EPM server, restart the network connection for the primary EPM server. If there is:
   - More than one network connection, enter the `/sbin/service network restart` command.
   - A single network connection, enter the commands:
     a. `ifconfig eth`*`xx`*` down`
     b. `ifconfig eth`*`xx`*` up`

Where `xx` is the name of the ethernet connection that you are restarting. The default for an Avaya-provided server is `eth0`.

# EPM pages do not display or have garbled content

If the EPM pages do not display at all or display garbled content, Tomcat may not be running or may have one or more processes that are hung or not functioning correctly.

✱ **Note:**

If none of the following recommended actions resolves the problem, contact your Avaya technical support representative for assistance.

## Proposed Solution

### Procedure

1. Ensure that the *vpms* service and all its required components are running.

   Check the Tomcat folders in the classpath. It should not contain duplicate files or any unnecessary files as this may cause a conflict.
2. Ensure that the Axis Web services container is running.
3. Check for PostgreSQL issues.

## Troubleshooting *vpms* service issues

If the EPM pages do not display properly, this issue can be caused by problems with the *vpms* service or one of its components.

### Proposed Solution 1: Verifying the *vpms* service status

### Procedure

1. Check the status of the *vpms* service by entering the `service vpms status` command.

   If the *vpms* service is running properly, the command displays messages indicating that the `tomcatd`, `SL`, and `ActiveMQ` services are all running. The command ends with the message: `Overall Status: VPMS is running`.
2. If the *vpms* service is:
   - Not running, start it as described in Proposed Solution 2: Start the vpms service on page 31 given below.

- Running, there may be a problem with one of the required components. Restart the *vpms* service as described in Proposed Solution 3: Restart the vpms service on page 31 given below.

## Proposed Solution 2: Start the *vpms* service

### Procedure

1. Start the *vpms* service by entering the `/sbin/service vpms start` command.

   You will see a series of messages as the command starts several EPM components. When the command has successfully started all relevant components, the system displays the message: `VPMS Start Status: [ OK ]`.
2. Try to log into the EPM web interface again.
3. If the problem persists, there may be an issue with Tomcat. Check the status of the individual Tomcat processes as described in Proposed Solution 4: Checking the Tomcat processes on page 31 given below.

## Proposed Solution 3: Restart the *vpms* service

### Procedure

1. Restart the *vpms* service by entering the `/sbin/service vpms restart` command.

   You will see a series of messages as the command starts to shut down EPM components. When the command has successfully stopped all relevant components, the system displays the message: `VPMS Shutdown Status: [ OK ]`.

   The command immediately starts the relevant components. When the command is run successfully, the system displays the message: `VPMS Start Status: [ OK ]`.
2. Wait for several minutes to let the service initialize, then verify that there is only one *vpms* service by entering the *`service vpms status`* command.
3. Try to log into the EPM web interface again.
4. If the problem persists, there may be an issue with Tomcat. Check the status of the individual Tomcat processes as described in Proposed Solution 4: Checking the Tomcat processes on page 31 given below.

## Proposed Solution 4: Checking the Tomcat processes

### About this task

If Tomcat is running but one or more of its processes are not functioning correctly, you can have problems with loading the EPM pages. To check Tomcat processes and verify that the processes are running:

### Procedure

1. At the Linux command line prompt, enter the `ps -ax | grep java` command.

The system should respond with output similar to the following:

```
/usr/java/default/bin/java -Djava.util.logging.config.file=/opt/Tomcat/tomcat/
conf/logging.properties -
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -server -
XX:+HeapDumpOnOutOfMemoryError -Dcom.sun.management.jmxremote -
XX:+UseCompressedOops -Ddss.idle_time=2000 -XX:MaxNewSize=256m -Xmx1536M -
XX:+UseConcMarkSweepGC -XX:ThreadStackSize=1024 -Ddss.port=31050 -
XX:PermSize=256m -XX:MaxPermSize=320m -XX:GCTimeRatio=19 -
XX:CMSInitiatingOccupancyFraction=60 -XX:SurvivorRatio=8 -
XX:TargetSurvivorRatio=90 -XX:MaxTenuringThreshold=0 -
XX:+UseCMSCompactAtFullCollection -XX:CMSFullGCsBeforeCompaction=1 -
Dsun.lang.ClassLoader.allowArraySyntax=true -XX:-DoEscapeAnalysis -
Djsse.enableSNIExtension=false -XX:CompileCommand=exclude,net/sf/jasperreports/
engine/export/JRGridLayout,horizontallyMergeEmptyCells -Djava.awt.headless=true -
Dorg.apache.el.parser.COERCE_TO_ZERO=false -Djava.endorsed.dirs=/opt/Tomcat/
tomcat/endorsed -classpath /opt/Tomcat/tomcat/bin/bootstrap.jar -
Dcatalina.base=/opt/Tomcat/tomcat -Dcatalina.home=/opt/Tomcat/tomcat -
Djava.io.tmpdir=/opt/Tomcat/tomcat/temp org.apache.catalina.startup.Bootstrap
start
```

2. Examine the Tomcat log file for indications that Tomcat is experiencing errors or other problems that might be affecting its performance. This log file is located at `$CATALINA_HOME/logs/catalina.out`.

   **Note:**

   Tomcat folders in the classpath should not contain duplicate files or any unnecessary files as this may cause a conflict.

3. If the system does not respond with the expected output, verify that the Axis Web services container is configured properly as described in Verifying Axis configuration on page 32.

## Verifying Axis configuration

Axis is a Web services container that 'is dependent of Tomcat. If Tomcat is running but Axis is not configured properly, you can experience problems with the EPM web interface.

**Note:**

Because Axis runs on top of Tomcat, if Tomcat is not running, neither is Axis.

**Related links**

#unique_47

#unique_48

### Proposed Solution

#### Procedure

1. In your Web browser, enter the URL https://*epm_host_address*/axis/servlet/AxisServlet

   Where *epm_host_address* is the fully qualified domain name or IP address of the EPM server.

2. On the And now...Some Services page, verify that all the following services are listed:
    - LogServer-1.0 (wsdl)
    - AdminService (wsdl)
    - AppIntfWS (wsdl)
    - Version (wsdl)
    - VPReport4 (wsdl)
    - AlarmServer-1.0 (wsdl)
    - AlarmRetrieverServer-1.0 (wsdl)
    - AlarmConfigServer-1.0 (wsdl)
    - LogRetrieverServer-1.0 (wsdl)
    - UpgradeWS (wsdl)
    - VPAppRuntimeVars (wsdl)
3. If any required components or services are not listed, reinstall the EPM.
4. In your Web browser, enter the URL `https://`*`epm_host_address`*`/axis2/services/listServices`

    Where *`epm_host_address`* is the fully qualified domain name or IP address of the EPM server.
5. Accept the certificate (if prompted).
6. On the Available Services page, verify that all the following Axis2 services are listed:
    - VPManagementService (wsdl)
    - VPAppIntfService (wsdl)
    - VPAppVarsService (wsdl)
    - VPAppLogService (wsdl)
7. If any required components or services are not listed, reinstall the EPM.
8. Are Axis 1 and Axis 2 configured properly?
    - If yes, then verify that PostgreSQL is running properly, as described in Troubleshooting PostgreSQL issues on page 33.
    - If no, reinstall the EPM.

## Troubleshooting PostgreSQL issues

PostgreSQL is the database server that provides access to the databases required by the EPM web interface. If PostgreSQL is not running or is experiencing difficulties, the EPM pages can exhibit unexpected behavior or cease to respond at all.

**Note:**

The Experience Portal internal database should not be modified. If you want to modify the database, contact your Avaya technical support representative for assistance.

The following solutions help to identify and troubleshoot issues with PostgreSQL.

## Proposed Solution 1: Verifying the PostgreSQL status

### Procedure

1. At the Linux command line prompt, enter the `/sbin/service postgresql status` command.
2. Does the system display a message that the PostgreSQL service is running?
    - If yes, verify that the `postmaster` process is running as described in Proposed Solution 2: Verifying that the postmaster process is running on page 34.
    - If no, start the PostgreSQL service as described in Proposed Solution 3: Starting PostgreSQL on page 34.

## Proposed Solution 2: Verifying that the postmaster process is running

### Procedure

1. At the Linux command line prompt, enter the `ps -edf | grep postgres` command.
2. Is the `postmaster` process listed?
    - If yes, and the problem with the EPM pages continues, reboot the EPM server. If the problem continues, contact your Avaya technical support representative for assistance.
    - If no, try stopping and restarting PostgreSQL as described in Proposed Solution 4: Stopping and restarting PostgreSQL on page 34.

## Proposed Solution 3: Starting PostgreSQL

### Procedure

1. At the Linux command line prompt, start PostgreSQL by entering the `/sbin/service postgresql start` command.

    The system responds with a series of messages indicating that the PostgreSQL service is started.
2. Did this resolve the problem, and does the system now display EPM pages properly?
    - If yes, no further action is required.
    - If no, reboot the EPM server. If the problem continues, contact your Avaya technical support representative for assistance.

## Proposed Solution 4: Stopping and restarting PostgreSQL

### About this task

If PostgreSQL is running but does not appear to be functioning correctly, you can try stopping and restarting PostgreSQL.

### Procedure

1. At the Linux command line prompt, stop PostgreSQL by entering the `/sbin/service postgresql stop` command.

   The system responds with a series of messages indicating that the PostgreSQL service is stopped.

2. At the Linux command line prompt, restart PostgreSQL by entering the `/sbin/service postgresql start` command.

   The system responds with a series of messages indicating that the PostgreSQL service is started.

3. Did this resolve the problem, and does the system now display EPM pages properly?

   - If yes, no further action is required.
   - If no, reboot the EPM server. If that does not resolve the problem, contact your Avaya technical support representative for assistance.

# Cannot view or use an EPM page

You cannot view or use the desired EPM pages. This problem typically occurs because you are assigned with a user role that does not permit access to certain pages. This is not an error, but a system design feature.

## Proposed Solution

### Procedure

To gain access to those pages, you must obtain a user account with a different user role.

# Cannot access or view certain features in EPM

You cannot access or view the desired EPM features and options. This is not an error, but a system design feature.

This problem typically occurs because of the following reasons:

- The role assigned to you does not permit access to certain features or options on the EPM pages. For example, the role assigned to you has permissions to add a user account but does not permit to delete any user accounts.
- You are not assigned with the correct role.
- The role assigned to you is not configured for appropriate access. For example, where a reporting role should permit you to generate all the reports, it was not configured correctly to

do so. It allows you to generate standard reports but does not permit to generate a custom report or schedule a report.

With the role based access, you can perform only those actions for which you have access permissions. The options for performing other actions are either not displayed or disabled on the EPM pages for that particular feature.

# EPM screen not displayed after restoring Experience Portal on a new server

EPM screen is not displayed after restoring Experience Portal on a new server. This problem typically occurs when the postgres password on the new EPM server is different from the password configured on the primary EPM server.

## Proposed Solution

### Before you begin

- Ensure you have a backup of Experience Portal data on the backup server
- Make sure you have restored the Experience Portal backup data on a new server.
- Verify if EPM and Tomcat application server are running.

### Procedure

1. Log on to Linux on the Primary or Auxiliary EPM server.

   If you are an Avaya Services representative and are using Avaya Enterprise Linux, the Avaya Service accounts will not be available after the Avaya Enterprise Linux upgrade. The Avaya Service accounts will be available through EASG configuration during the Experience Portal upgrade. So,

   - Log on to the local Linux console as root.
   - Or log on remotely as a non-root user and enter the `su - root` command to change the user to root.

2. Enter the `cd $AVAYA_HOME/Support/Security-Tools` command, where `$AVAYA_HOME` is an environmental variable pointing to the name of the installation directory specified during the Experience Portal software installation.
3. Enter the `bash SetDbPassword.sh update -u` *`username`* command, where *username* is the name of the user account whose password you want to change. The username in this case is vpcommon.
4. Type the password you want to use for this account and press `Enter`.

   After the password is accepted and updated, the script will display a message prompt indicating the services will be restarted and ask if the user wants to proceed.

```
The following services will be restarted automatically:
-  postgresql
- vpms
- mmsserver
- avpSNMPAgentSvc
Do you wish to proceed? [Y/n]
```

5. Type one of the following:
   - `Y` to restart the services that are listed.
   - `n` to cancel the restarting services.

     **Note:**

     If you cancel restarting the services, you should manually restart the services for the changes to take effect.

# EPM pages display ??? in the fields

If one or more EPM pages display ??? in the fields, the language settings in the Web browser are incorrect.

## Proposed Solution

### Procedure

1. In Internet Explorer, select **Tools** > **Internet Options**.
2. In the Internet Options dialog box, select the **General** tab.
3. Click **Languages** and make sure that the list includes US English.

# EPM running out of disk space

If the EPM server runs out of disk space, you can check the disk space usage and determine which proposed solution to follow to free up the disk space.

**Note:**

If none of the following recommended actions resolve the problem, contact your Avaya technical support representative for assistance.

# Prerequisites

### About this task

Prior to following any of the proposed solutions, you need to check the disk space usage. This will help you determine which proposed solution to follow.

**Note:**

Do not delete files from the server without analyzing the possible outcome.

### Procedure

1. Log in to Linux on the primary or auxiliary EPM server.

   If you are an Avaya Services representative, and are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and then change the user to sroot by entering the su - sroot command.

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and change the user to root by entering the su - command.

2. Isolate the directory that uses the maximum disk space.

   a. Enter the **`du -b --max-depth=1 -h /`** command to display a list of top level directories on the server along with the currently-occupied disk space.

      The table below is an example of the output:

      ```
      [sroot@vp-a11 /]# du -b --max-depth=1 -h /
      20K /mnt
      12M /tmp
      1.8G /home
      5.9M /bin
      24K /root
      9.3G /opt
      995M /var
      16G /
      [sroot@vp-a11 /]#
      ```

   b. Check the output to determine which directory uses the maximum disk space. In the example given above, the `/opt` directory uses the maximum space.

   c. To further isolate the directory that uses the maximum space, enter the **`du -b --max-depth=1 -h /`**<*directory name*> command where <*directory name*> is the directory uses the maximum space.

      For example, enter the **`du -b --max-depth=1 -h /opt`** command to check the directories under the`/opt` directory.

> **Note:**
>
> Repeat the command to locate the specific directory or file that uses the maximum disk space.

3. Analyze the information, and based on the observations follow up with the possible solutions, as mentioned in the steps below.

4. If the `/var` directory uses maximum disk space, it is possible that the retention period for the report data (Call/Session, Application, and/or Performance), Alarm Logs, Event Log, or Audit Logs are set too high. When Experience Portal is initially installed, the retention period for these tables are set to default values. Depending on the system load and applications being run, these values may need change to retain less data and thereby use less disk space.

   > **Note:**
   >
   > The database that Experience Portal uses is located in the `/var` directory.

   a. From the EPM menu, select **Real Time Monitoring > System Monitor**.

   b. In the **Server Name** column, select the link for EPM.

   c. Use the **<EPM> Details** page to view the detailed database status of the primary EPM server. The **Database Status** section shows the database tables that use the most disk space and the corresponding size, in bytes. The database tables are listed in descending order as per the size.

   d. Choose the **Proposed Solution** based on which table or tables is using more disk space than expected:

   - Use **Proposed Solution 1** for the following tables:
     - CDR
     - SDR
     - vpapplog
     - vpperformance
   - Use **Proposed Solution 2** for the following tables:
     - alarmrecord
     - cslog
     - csadminauditlog
   - Use **Proposed Solution 3** for the vpreportresults table

5. If the `/opt/Avaya/InstallAgent/download` directory uses the maximum disk space on Linux, use **Proposed Solution 4** to free up disk space by removing the old ISO image files. Experience Portal stores a copy of the Experience Portal ISO image file in this directory.

   The ISO image file is used during a managed upgrade (only on Linux systems). As newer versions of Experience Portal are installed, the older ISO image files are not removed.

6. If the `/opt` directory uses maximum disk space, then it is possible that there is a file that is abnormally using a lot of disk space. Experience Portal is installed in this directory (`/opt/Avaya/ExperiencePortal` by default. There are no Experience Portal related files in the `/opt` directory on Linux that use a large amount of disk space. But depending on other applications running on the EPM server, there may be components using the disk space.
7. If another directory uses the maximum disk space, contact your Avaya technical support representative for assistance.

   ❗ **Important:**

   Do not delete files unless the directory or file that uses the maximum disk space is identified.

## Proposed Solution 1: Adjust report data retention and free disk space

### Procedure

1. Log in to the EPM web interface using an account with the Administration user role.

   ❗ **Important:**

   As an alternative to steps 2 and 3, you can run the **`PurgeReportDataLocalDB`** and **`PurgeReportDataExtDB`** scripts. These scripts recover the disk space used by the database tables. The time taken to recover the disk space depends on the amount of data in the database tables. However, this activity purges all data in the CDR, SDR, vpapplog, and vpperformance tables. All existing data in these tables is permanently lost. For more information on purging report data, see *Administering Avaya Experience Portal*.
2. From the EPM menu, select **System Configuration** > **EPM Servers** > **Report Data**.
   a. On the **Report Data Configuration** page, verify that the **Purge Records** option in the **Report Database Record Data** section is set to **Yes**.
   b. Depending on which table or tables has high disk use, adjust the Call/Session (CDR and SDR), Application (vpapplog), or Performance (vpperformance) retention period to a smaller number of days.
   c. Click **Apply** to save your changes.

      The scheduled purge tasks for the Call/Session, Application, and Performance logs are run at 02:00 hours by default, to purge records from the tables that are older than the configured retention period.
3. After the scheduled purge task is completed (which is typically the day after you make changes to the **Report Data Configuration** page in EPM), stop the *vpms* service.
4. To run the script, enter the `$AVAYA_HOME/Support/VP-Tools/CleanLogsLocalDB` *`<table name>`* command:

The above command enables you to recover the unused disk space allocated to that table, where <table name> is the name of the table from which you want to recover disk space.

For example: **`$AVAYA_HOME/Support/VP-Tools/CleanLogsLocalDB vpperformance`**

## Proposed Solution 2: Adjust Alarm/Log/Audit retention and free disk space

### Procedure

1. Log in to the EPM web interface using an account with the Administration user role.
2. From the EPM menu, select **System Configuration** > **EPM Servers** > **Alarm/Log Options**.
3. On the **Alarm/Log Options** page, depending on which table or tables has the maximum disk use:

    a. Verify that the **Purge Enabled** option in the Alarms, Logs, or Audit Logs section is set to **Yes**.

    b. Adjust the **Retention Period** in the Alarms, Logs, or Audit Logs section to a smaller number of days.

    c. Click **Apply** to save your changes.

    The scheduled purge tasks for Alarms, Logs, or Audit Logs are run to purge records from the tables that are older than the configured retention period at midnight by default.
4. After the scheduled purge task is completed, (which is typically the day after you make changes to the **Alarm/Log Options** page in EPM) stop the vpms service.
5. Enter the `$AVAYA_HOME/Support/VP-Tools/CleanLogsLocalDB` *`<table name>`* command.

    The above command enables you to recover the unused disk space allocated to that table, where *<table name>* is the name of the table (alarmrecord, cslog, or csadminauditlog) from which you want to recover disk space.

    For example: **`$AVAYA_HOME/Support/VP-Tools/CleanLogsLocalDB alarmrecord`**.

    **Note:**

    The script may also take several minutes to run, depending on how much disk space is being recovered.

## Proposed Solution 3: Adjust scheduled report output retention and free disk space

### Procedure

1. Log in to Linux on the primary or auxiliary EPM server. If you are an Avaya Services representative, and are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and enter the `su - sroot` command to change the user to sroot.

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and enter the `su -` command to change the user to root.

2. From the EPM menu, select **System Configuration** > **EPM Servers** > **Report Data**.
3. On the **Report Data Configuration** page, edit the **Scheduled Reports** section as follows:

   a. Set the **Output Folder Size** to a lower number in order to reduce the amount of disk space that the scheduled reports can use.

   b. Set all the **Output Retention (days)** settings to lower numbers to reduce the number of days the reports are retained and the amount of disk space the scheduled reports use.

   c. Click **Apply** to save your changes.

      The scheduled purge tasks for the reports are run at 02:00 hours by default, to purge records from the tables that are older than the configured retention period.

## Proposed Solution 4: Remove older copies of the Avaya Experience Portal ISO image file

### Procedure

1. Log in to Linux on the primary EPM server.

   If you are an Avaya Services representative, and are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and enter the `su - sroot` command to change the user to sroot.

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and enter the `su -` command to change the user to root.

2. Change directories to the location of the ISO image files:

```
cd $AVAYA_IA_HOME/download
```

3. Remove all ISO image files except the file with the newest version.

# EPM server fails due to hardware problems

The EPM server fails due to hardware problems, and you need to move the software to a different server.

## Proposed Solution

### Procedure

Move the EPM software to a new server. For more information, see the backup and restore procedures in Administering Avaya Experience Portal.

# SIP: The root CA certificate will expire in {0} days

When the root certificate on the EPM expires, you need to generate a new certificate by using the **UpdateRootCertificate.sh** script.

## Proposed Solution

### Procedure

1. Log onto Linux on the primary EPM server.

   If you are an Avaya Services representative, and use Avaya Enterprise Linux, the Avaya Service accounts will not be available after the Avaya Enterprise Linux upgrade. The Avaya Service accounts will be available through EASG configuration during the Experience Portal upgrade.

   - Log on to the local Linux console as root.
   - Or log on remotely as a non-root user and then change the user to root by entering the `su - root` command.

2. Navigate to the Support/Security-Tools directory by entering the **`cd $AVAYA_HOME/Support/Security-Tools`** command.

   $AVAYA_HOME is the environment variable pointing to the name of the installation directory specified during the Experience Portal software installation. The default value is`/opt/Avaya/ExperiencePortal`.

> **Tip:**
>
> This script is also available in the Support/Security-Tools directory of the Experience Portal installation DVD.

3. To run the script, enter the `UpdateRootCertificate` command to generate a new security certificate.
4. Type `Y` and press `Enter` when prompted, to restart the vpms service.

> **Note:**
>
> - Restart all MPPs and auxiliary EPM for the new security certificate to take effect.
> - If the Experience Portal system uses SIP Connection over TLS, then ensure that the SIP Connection server is updated with the newly generated certificate.

# Email and SMS data not collected from Auxiliary EPM

The Primary EPM periodically collects report data related to email and SMS processing from each Auxiliary EPM. If an Auxiliary EPM server is re-imaged, then the Primary EPM will stop collecting report data from it.

To work around this issue, reset the report data position on the Primary EPM server whenever you reimage an Auxiliary EPM server. Follow whichever procedure below is appropriate for your system.

## Proposed Solution 1: Resetting report data position for systems using local Experience Portal database

### Procedure

1. Log into Linux on the Primary EPM server as a user with root privileges.
2. To navigate to the appropriate directory, run the `cd $AVAYA_HOME/Support/Security-Tools` command.
3. To reset the report data position, run the `./ResetEmailSMSLocalDB <Auxiliary_EPM_Name>` command.

   Where:

   - `<Auxiliary_EPM_name>` is the name of the Auxiliary EPM as it appears on the **EPM Servers** page of the EPM web interface.
4. Reboot the Primary EPM server.

## Proposed Solution 2: Resetting report data positions on systems using external database

### Procedure

1. Log into Linux on the Primary EPM server as a user with root privileges.
2. To navigate to the appropriate directory, run the `cd $AVAYA_HOME/Support/Security-Tools` command.
3. To reset the report data position, run the `./ResetEmailSMSExtDB "<Database_URL>" <JDBC_Driver> <Database_User_Name> <Experience_Portal_Name> <Auxiliary_EPM_Name>` command.

   Where:

   - `"<Database_URL>"` is the URL of the external database as it appears on the **Report Database Settings** page of the EPM Web interface.

     **Important:**

     Put quotation marks around the URL.
   - `<JDBC_Driver>` is the JDBC driver for the external database as it appears on the **Report Database Settings** page of the EPM web interface.
   - `<Database_User_Name>` is the user name for the external database as it appears on the **Report Database Settings** page of the EPM web interface.
   - `<Experience_Portal_Name>` is the name of the Experience Portal system as it appears on the **EPM Settings** page of the EPM web interface.
   - `<Auxiliary_EPM_name>` is the name of the Auxiliary EPM as it appears on the **EPM Servers** page of the EPM web interface.
4. Reboot the Primary EPM server.

# Email and SMS report data not collected from Primary EPM

A component of the Primary EPM periodically collects report data that is generated by the email and SMS processing components that also run on the Primary EPM. If the Primary EPM server is re-imaged and the system is configured to use an external database, then the Primary EPM will stop sending email and SMS report data from the Primary EPM server to the external database.

To work around this issue, reset the report data position on the Primary To work around this issue, reset the report data position on the Primary EPM server whenever you re-image a Primary EPM server that is configured to use an external database. server whenever you re-image a Primary EPM server that is configured to use an external database.

## Proposed Solution: Resetting the report data position

### Procedure

1. Log into Linux on the Primary EPM server as a user with root privileges.
2. To navigate to the appropriate directory, run the `cd $AVAYA_HOME/Support/VP-Tools` command.
3. To reset the report data position, run the `./ResetEmailSMSExtDB "<Database_URL>" <JDBC_Driver> <Database_User_Name> <Experience_Portal_Name> <Primary_EPM_Name>` command.

   Where:

   - `"<Database_URL>"` is the URL of the external database as it appears on the **Report Database Settings** page of the EPM Web interface.

     **Important:**

     Put quotation marks around the URL.
   - `<JDBC_Driver>` is the JDBC driver for the external database as it appears on the **Report Database Settings** page of the EPM web interface.
   - `<Database_User_Name>` is the user name for the external database as it appears on the **Report Database Settings** page of the EPM web interface.
   - `<Experience_Portal_Name>` is the name of the Experience Portal system as it appears on the **EPM Settings** page of the EPM web interface.
   - `<Primary_EPM_name>` is the name of the Primary EPM as it appears on the **EPM Servers** page of the EPM web interface.
4. Reboot the Primary EPM server.

# EPM fails sending a configuration to MPP due to the Read timed out error

If Avaya Experience Portal has a large configuration, for example, more than 100 applications, MPP cannot update the configuration before the default timeout. When the EPM does not receive the confirmation from MPP in time, it starts sending repetitive configuration requests, which form an infinite loop.

In this case, the EPM logs can contain the following message: `Failed sending Configuration to <MPP name> with error Read timed out.`

To troubleshoot this issue, increase the default timeout of the MPP and EPM.

- For 100 - 500 applications, increase the timeout to one minute.
- For 500 - 1000 applications, increase the timeout to two minutes.
- For every 1000 applications thereafter, increase the timeout by a minute. For example, for 2000 applications, increase the default timeout to three minutes. For 3000 applications, increase the timeout to four minutes, and so on.

## Proposed Solution

### About this task

Use this procedure to set a two minute timeout.

### Procedure

1. Log in to EPM.
   a. In the `/opt/Tomcat/tomcat/lib/config/voiceportal.properties` file, set the following properties:

      ```
      mmsClientTimeout=120000
      ```

      ```
      mppResponseCompletionTimeoutMS=120000
      ```

   b. Restart EPM by running the following command:

      ```
      service vpms restart
      ```

2. Log in to MPP.
   a. In the `/opt/Avaya/ExperiencePortal/MPP/config/mppconfig.xml` file, set the following property:

      ```
      <parameter name="mms_cmd_response_timeout">120</parameter>
      ```

   b. Restart MPP by running the following command:

      ```
      service mpp restart
      ```

   c. In the `/etc/httpd/conf/httpd.conf` file, set the following property:

      ```
      Timeout 120
      ```

   d. Restart the HTTPD server by running the following command:

      ```
      service httpd restart
      ```

# Setting trace logging options

## About this task

If you are facing problems with your Avaya Experience Portal system, there are several trace logging options that you can set in the EPM. Before you do this, however, see Troubleshooting categories on page 9 for detailed troubleshooting procedures.

## Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM navigation pane, click **System Configuration** > **Applications**.
3. Click the name of the application for which you want to set up performance tracing.
4. On the Change Application page, do the following:
    a. Click **Reporting Parameters** and go to the **Transcription** section.
    b. In the **Transcription Enabled** field, select **Yes**.
    c. In the **Performance Trace** field, select **Yes** .
    d. Click **Save**.
5. On the EPM navigation pane, click **System Configuration** > **MPP Servers**.
    a. On the MPP Servers page, click **MPP Settings** .
    b. On the MPP Settings page, go to the **Transcription** section.
    c. In the **Transcriptions Retention Period** field, set the length of time that the transcription log files will remain on the MPP server.
    d. In the **Maximum Transcriptions per Day** field, set the maximum number of log files that the MPP server will record on any given day.
    e. Click **Save**.
6. On the EPM navigation pane, click **System Configuration** > **EPM Servers** > **Report Data**.
    a. On the Report Data Configuration page, go to the **Report Database Record Data** group and make sure that the **Call/Session Retention Period** field is set to a value equal to or greater than the length of time you entered in the **Transcriptions Retention Period** field.

       You cannot access the transcription data for a call unless the call data also exists in the Avaya Experience Portal database.
    b. Click **Save**.

# Chapter 5: Troubleshooting MPP issues

## Taking the MPP offline using the EPM web interface

### About this task

Before you work with an MPP server, you need to take the MPP offline. This procedure explains how take the MPP offline using the EPM Web interface.

### Procedure

1. Log on to the EPM web interface by using an account with the Administration or Operations user role.
2. From the EPM main menu, select **System Management** > **MPP Manager**.
3. On the MPP Manager page, use the Selection check box in the MPP server table to select which MPP server you want to take offline.
4. Click the **Stop** button in the **State Commands** group and confirm your selection when prompted.

   Avaya Experience Portal stops the selected MPP server when the last active call completes or the grace period expires, whichever comes first.
5. After a few minutes, click **Refresh** and verify that the **State** is **Stopped** for the MPP server that you want to upgrade.
6. If the MPP operational state:
   - Changed to **Stopped**, continue with this procedure.
   - Did *not* change, you need to stop the `mpp` service as described in Stopping the MPP service on page 50.
7. Use the Selection check box in the MPP server table to reselect the MPP server you want to take offline.
8. Click **Offline** in the **Mode Commands** group.
9. Click **Refresh** and verify that the **Mode** is **Offline** for the MPP server you want to upgrade.

# Stopping the MPP service

You should always try to take the MPP offline using the EPM web interface. If the EPM is not communicating with the MPP, however, you can take the MPP offline by stopping the `mpp` service.

### Procedure

1. Log in to Linux on the MPP server as a user with root privileges.

   If you are an Avaya Services representative, and are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

   Otherwise, log in to Linux locally as root user, or log in remotely as a non-root user then change the user to root by entering the su - command.

2. Enter the `/sbin/service mpp stop` command.

# Isolating an MPP for troubleshooting

### Before you begin

If desired, on the Communication Manager PBX for the system, create a special hunt group for maintenance numbers.

Make sure that at least one H.323 station has been defined as a maintenance number guide.

### About this task

If your system has multiple MPPs, and a single MPP appears to be having problems, you can isolate the suspect MPP to facilitate the troubleshooting process. If you isolate an MPP in Test mode, you can direct test calls to that MPP only.

### Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. From the EPM main menu, select **System Configuration** > **Applications**.
3. On the Applications page, in the **Launch** column, ensure that at least one speech application is specifically associated with the maintenance stations defined for the H.323 connection.
4. If no application is assigned to handle the maintenance stations:
   - Add a new application. Ensure you specify the maintenance stations in the **Application Launch** group on the Add Application page.

- Change an existing application so that it is specifically associated with the maintenance station . Ensure you specify the maintenance stations in the **Application Launch** group on the Change Application page.

# Checking the basic status of an MPP

If the MPP is not functioning correctly, check the basic status of the MPP and its key processes.

**Note:**

These strategies assume that you have logged in to the EPM and have checked the <System name> Details tab on the System Monitor page.

## Proposed Solution

### Procedure

1. Check the operational state of the MPP.
2. Check the configuration state of the MPP.
3. Check the states of the critical MPP processes.

# Checking the operational state of an MPP

If the EPM <System name> Details tab on the System Monitor page indicates that the operational state of the MPP is any state other than **Running**, you can verify the operational state.

## Proposed Solution 1: if you can log in to the Media Server Service Menu

### Procedure

1. Log in to the Media Server Service Menu .
2. In the **MPP Status** table on the MPP Service Menu home page, look at the value of the **Run state** field. If this field is:
    - **Running**, the problem lies in the communication between the primary EPM server and the MPP. Verify that the servers can communicate.
    - Any other state, start the MPP. If you cannot start the MPP, check the status of the httpd daemon process. For more information, see Checking the state of an MPP process on page 54.

## Proposed Solution 2: if you cannot log in to the Media Server Service Menu

### Procedure

1. If you cannot log in to the Media Server Service Menu, enter the `stat.php` command on the MPP to determine the operational state of the MPP.
2. Check the status of the httpd daemon process. For more information, see For more information, see Checking the state of an MPP process on page 54.

## Check the configuration state of the MPP

### Procedure

1. Verify on the MPP Service Menu home that the **Configuration state** field in the **MPP Status** table says **Configuration OK**.
2. If the value of the **Configuration state** field is *not* **Configuration OK**, locate the indicated state in the following table and perform the corrective action.

| Configuration state | Corrective action |
|---|---|
| **No Configuration** | This state is most commonly seen just after the mpp daemon has started.<br>If the **Telephony configuration needed** state does not automatically replace this state, see MPP is in an unexpected operational state on page 62. |
| **Telephony configuration needed** | The MPP has received configuration parameters from the EPM, but has not yet been assigned any ports.<br>If the MPP is in the Running operational state, but the **Configuration state** remains in this state, check the Port Distribution page to see if any ports have been assigned to the MPP.<br>If the MPP has assigned ports, check the Log Viewer for errors that might prevent the EPM from sending port information to the MPP. |
| **Restart Needed** | An administrator has made a change to the system that requires that the MPP be restarted.<br>Restart the MPP, as described in the *Restarting one or more MPP servers* topic in the *Administering Avaya Experience Portal*. |
| **Reboot Needed** | An administrator has made a change to the system that requires that the MPP be rebooted.<br>Reboot the MPP. . |

3. In the menu on the left, click **Diagnostics**.

4. On the Diagnostics page, click **Check connections to servers**.
5. On the Check Server Connections page, verify the status of the connections to the ASR, TTS, telephony, and application servers.
6. If the connection status is okay, click **Resources** in the main menu.
7. On the Resources page, click **Telephony**.

   ⊕ **Tip:**

   If you cannot log in to the Media Server Service Menu, you can use the administrative scripts described in Administrative scripts available on the MPP on page 55 to view the MPP status and configured telephony and speech server resources.
8. If the appropriate telephony resources table displays data and if one or more of the switch settings for the Communication Manager are not correct, troubleshoot the indicated problem between the Communication Managerand the MPP:
   a. Create a log report and check for telephony errors logged on the EPM.
   b. Check the Session Manager log files for telephony-related errors.
9. If the appropriate telephony resources table does not display data:
   a. From the EPM main menu, select **Real-time Monitoring** > **Port Distribution**.
   b. Verify that there are ports allocated to the MPP.

**Related links**

Checking the status of port connections on page 10

# Checking the states of the critical MPP processes

When you troubleshoot MPP issues, if the operational state of the MPP is **Running**, check the states of the critical MPP processes.

## Proposed Solution

### Procedure

1. Log into Linux on the MPP server as any user.
2. Enter the `ps -e | grep` *`process_name`* command, where *`process_name`* is the name of the process whose state you want to check.

   The critical processes are:

   - `ccxml`
   - `EventMgr`

- `vxmlmgr`

3. To check if the processes are running, enter the **`stat.php`** command.
4. If a state of any process is other than **Running**, check the `$AVAYA_MPP_HOME/logs/core` directory for any files related to the problem.

   For `ccxml` and `vxmlmgr`. some processes will be in the Stopped state and some will be in the Running state. Therefore, the Stopped state doesn't mean that the `ccxml` and `vxmlmgr` processes are in a critical state.

   If you find any related files, contact your Avaya technical support representative for assistance.
5. If all three processes indicate that they are running, check the configuration state of the MPP.

# Checking the state of an MPP process

## Procedure

1. Log into Linux on the MPP server as any user.
2. Enter the `ps -e | grep` *`process_name`* command, where *`process_name`* is the name of the process whose state you want to check.

   The MPP processes are:

| Process Name | Descriptive Name | Notes |
|---|---|---|
| `ccxml` | CCXML Interpreter | This process controls all call handling behavior for each VoiceXML application that runs on the MPP. It also controls each request to obtain or release a telephony resource for a given VoiceXML application.<br>Experience Portal uses the Oktopous™ ccXML Interpreter. |
| `CdhService` | Call Data Handler (CDH) | This process is a web service that runs when the EPM is downloading Contact Detail Records (CDRs) and Session Detail Records (SDRs). |
| `EventMgr` | Event Manager | This process collects events from other MPP processes and sends them to the network log web service on the EPM. |
| `httpd` | Apache Web Server | This process enables the other web services running on the MPP.<br>The first Apache Web Server process started by the daemon runs as root. The root process starts the processes that run as the `avayavp` user in the avayavpgroup group. |

*Table continues…*

| Process Name | Descriptive Name | Notes |
|---|---|---|
| `MmsServer` | MPP Management Service (MMS) | This process is a web service interface that allows the EPM server to send commands to the MPP server. It runs only when the EPM is polling or sending commands to the MPP. |
| `mppmaint` | MPP Maintenance Utility | This is a `cron` process runs the MPP Maintenance Utility daily at 04:00 a.m. to purge CDRs, SDRs, and transcriptions data based on the retention period specified in the EPM. |
| `mppmon` | MPP Monitor | This process runs as root and monitors the `httpd` service and restarts them. |
| `mppsysmgr` | System Manager | This process handles the majority the tasks required to manage the MPP.<br>For example, this process monitors system resources such as CPU usage, memory usage, and disk usage. If any of these values exceed the baseline set in the EPM, the System Manager issues an alarm message.<br>When instructed by the EPM, the System Manager starts or stops all MPP processes and distributes EPM configuration updates to all MPP processes as they occur. |
| `SessionManager` | Session Manager | This process runs as root and integrates and controls the interaction between the MPP and media resources, as well as between the speech application and the ASR, TTS, and telephony components. |
| `TransService` | | This process uploads any transcription data to the Experience Portal database. |
| `vxmlmgr` | VoiceXML Manager | This process works with the Session Manager to run multiple VoiceXML dialog sessions. It also interfaces with the CCXML, telephony, ASR, and TTS subsystems.<br>The VoiceXML Manager and the Session Manager communicate by sending messages. The Session Manager is responsible for interpreting these messages and routing the calls to the appropriate platform subsystems on behalf of the VoiceXML Manager. |

For an active process, the system returns the process id and CPU time.

## Administrative scripts available on the MPP

The following administrative scripts are available on the MPP. You can run any of these scripts from a command line on the MPP machine:

| Script/Executable | Type | Description |
|---|---|---|
| `app.php` | php | Summary of the application information downloaded from the EPM. |
| `appstat.php` | php | The statistics of all applications running on the MPP since the MPP was last started or the application changed.<br>**Note:**<br>This information also appears on the Application Statistics page in the Media Server Service Menu. |
| `asr.php` | php | Summary of the ASR server information downloaded from the EPM.<br>**Note:**<br>This script provides a summary, not a complete list of all properties for the ASR servers. |
| `setup_vpms.php` | php | Downloads the EPM certificate that is used for the mutual authentication with the Web Service and the EPM.<br>**Note:**<br>This script has been replaced by `$AVAYA_HOME/`Support/Security-Tools/`/setup_vpms.php` script. |
| `dirclean.sh` | bash | Removes all application error handlers that were downloaded from the EPM.<br>**Note:**<br>This script is automatically called when the MPP service is stopped. When the MPP service is restarted, the event handlers are downloaded again to ensure that the latest copy is always available on the MPP. |
| `dropcall.php` *`station_id,switch name`* | php | Causes a specific station to drop any current call.<br>Specify the following parameters:<br>• *station_id*: the station number<br>• *switch name*: the name of the H.323 or SIP connection under which the station is defined.<br>**Tip:**<br>You can generate a list of stations with the `listst.php` script.<br>From EP 7.0 onwards, this script works with both H.323 and SIP. |
| `dropsession.php` *`session_id`* | php | Causes the MPP to drop the session whose Session ID is specified in *session_id*. |

*Table continues…*

| Script/Executable | Type | Description |
|---|---|---|
| `dumpRecords` | exe | Dumps the contents of an MPP's Contact Detail Record (CDR) or Session Detail Record (SDR) bin file. |
| `getmpplogs.sh` | bash | Automatically combines the MPP logs in a TAR.GZ file so that you can archive them or send them to your Avaya support representative.<br>**Tip:**<br>You can restore these logs with the `restorempplogs.sh` script. |
| `installstatus.php [--history]` | php | Lists the MPP version and release number. If you use the optional `--history` parameter, it lists the installation history starting with Avaya Experience Portal release 7.0. |
| `listcalls.php` | php | Lists the active calls on the MPP. |
| `listsessions.php` | php | Lists all sessions on the MPP. |
| `listss.php` | php | Summarizes the speech server resources currently available to the MPP, including the number of resources that the MPP server can use without shorting other MPP servers in the system (known as the H value) and the total number of ports that the MPP needs if the system is operating under a full call load (the M value).<br>**Note:**<br>This information also appears on the Speech Servers page in the Media Server Service Menu. |
| `listst.php` | php | Lists the configured stations and their statuses. |
| `mppMoveLogs.sh` | bash | Moves the current MPP logs directory to a different drive or partition and creates a symbolic link so that all future MPP logs will be written to the new location. |
| `mpprollback.sh` | bash | Rolls the MPP installation back to the previously installed version.<br>**Tip:**<br>The Version page in the Media Server Service Menu displays the current installed release and the available rollback version. |
| `restorempplogs.sh` | bash | Restores the MPP logs archived by the `getmpplogs.sh` script. |
| `SMDump` | exe | Dumps Telephony, ASR, and TTS status detail.<br>**Note:**<br>The `SessionManager` process must be running and you must be logged in as `root` or `sroot` to run this executable. |

*Table continues…*

| Script/Executable | Type | Description |
|---|---|---|
| `stat.php` | php | Lists the MPP state and the running state of its monitored processes. |
| `tts.php` | php | Summary of the TTS server information downloaded from the EPM.<br>**Note:**<br>This script provides a summary, not a complete list of all properties for the TTS servers. |
| `usr.php` | php | Displays a list of the users downloaded from the EPM.<br>**Note:**<br>User roles and passwords are encrypted in this list. |
| `xml.php` | php | Dumps out two XML configurations:<br>• Configuration loaded from the `$AVAYA_MPP_HOME/config/mppconfig.xml`<br>• Configuration downloaded from the EPM |

# Advanced troubleshooting scripts available on the MPP

⚠ **Caution:**

Only run these scripts under explicit instructions from your Avaya technical support representative. Under other circumstances, use the EPM to start, stop, or configure any MPP in the Experience Portal system to ensure that the EPM and the MPP stay synchronized.

The available advanced troubleshooting scripts are:

| Script | Type | Description |
|---|---|---|
| `installstatus.pl` | perl | This script has been replaced by `installstatus.php [--history]` and is installed for backwards compatibility only. |
| `launchccxml.php` | php | Launches an outbound call for a CCXML application.<br>**Important:**<br>You can use the Application Interface web service to launch such calls. For details, see *The Application Interface web service* in *Administering Avaya Experience Portal*. |

*Table continues…*

| Script | Type | Description |
|---|---|---|
| `launchvxml.php` | php | Launches an outbound call for a VoiceXML application.<br>**Important:**<br>You must use the Application Interface web service to launch such calls. |
| `msgs.php` | php | Lists statistics about the data sent between MPP processes.<br>**Note:**<br>This information also appears on the Process Messages page in the Media Server Service Menu. |
| `mppuninstall.sh` | bash | Uninstalls the MPP. |
| `start.php` | php | Instructs the MPP System Manager to start all MPP processes, such as `ccxml`, `vxmlmgr`. |
| `stationin.php` *`station_id,switch name`* | php | Instructs the MPP System Manager to bring a station into service.<br>Specify:<br>• *station_id*: the station number<br>• *switch name*: the name of the H.323 Connection under which the station is defined.<br>**Tip:**<br>You can generate a list of stations with the `listst.php` script. |
| `stationout.php` *`station_id,switch name`* | php | Instructs the MPP System Manager to bring a station out of service.<br>Specify:<br>• *station_id*: the station number<br>• *switch name*: the name of the H.323 Connection under which the station is defined.<br>**Tip:**<br>You can generate a list of stations with the `listst.php` script. |
| `stop.php` | php | Instructs the MPP System Manager to stop all MPP processes, such as `ccxml`, `vxmlmgr`. |

# Symptoms of common MPP problems

The key to diagnosing and resolving MPP problems is to quickly identify the component causing the problem. The following table provides examples of the most common system response errors.

Use these examples as a starting point to identify and isolate the problem component in cases where the problem component is not obvious.

| Symptoms | Possible causes | Where to go for more help |
|---|---|---|
| The system does not respond as expected. | Hyperthreading may not be enabled on the Experience Portal servers. | If hyper threading is not enabled, see Verifying if hyperthreading is enabled on the HP ProLiant DL360 G9 on page 64. |
| The system is not taking calls. All MPPs are unresponsive. | The WebLM license has expired, or the system is not able to contact the license server. | Verify that your license is valid and that the EPM can contact the Avaya license server. |
| | One or more system resources, such as the CPU usage, disk space, or available memory, might be overtaxed. | On the EPM, check the status of the system resources for the MPP.<br>For more information, see the **Resource Status** group on the <MPP name> Details page. |
| | Network or PBX problems might be causing the ports to go to the Out-of-Service state. | On the EPM, check the status of the telephony ports. For more information, see the Port Distribution page. |
| | Network problems might be preventing MPPs from running the speech applications. | On the EPM, verify that you can reach the root document of the speech application. For more information, see the Change Application page. |
| The system either does not answer or produces only busy signals. | One or more MPPs might be out-of-service or experiencing other problems. | Troubleshoot the MPP as described in System does not answer or produces only busy signals on page 64. |
| The system answers, but then immediately hangs up on the caller. | The number the caller dialed (DNIS) might not have a valid URI for a speech application assigned. | Verify the DNIS and URI settings for the application. For more information, see System answers and then hangs up on page 66. |
| | The MPP might be having trouble routing the caller to the proper application, fetching pages or resources, or interpreting the application pages. | Troubleshoot the MPP according to the guidelines provided in System answers and then hangs up on page 66. |
| The system answers the call, but does not recognize or respond to caller inputs. | The MPP receiving the call might be experiencing difficulties. | Troubleshoot the MPP according to the guidelines provided in the *Viewing Avaya Experience Portal system status* topic in the *Administering Avaya Experience Portal*. |
| | System encryption settings might be out of sync. | Troubleshoot the EPM according to the guidelines provided in Encryption settings are not synchronized on page 67. |

*Table continues…*

| Symptoms | Possible causes | Where to go for more help |
|---|---|---|
| | The ASR might be malfunctioning. | Use the EPM Alarm Monitor page to determine whether any ASR resources are having difficulty. For more information, see the *Viewing Avaya Experience Portal system status* topic in the *Administering Avaya Experience Portal*. |
| The system answers, but either becomes silent or responds with gibberish or other unusable output. | The MPP receiving the call might be experiencing difficulties. | Check the MPP basic status, as described in Checking the basic status of an MPP on page 51. If the state is not **Running**, see MPP is in an unexpected operational state on page 62. |
| | The network traffic might be too heavy for the bandwidth allowed. This can cause audio "stuttering." | Use one or more network traffic monitoring tools to assess the amount of bandwidth being consumed at the time that problems are experienced. Take steps to increase network bandwidth. |
| | System encryption settings might be out of sync. | Troubleshoot the EPM according to the guidelines provided in Encryption settings are not synchronized on page 67. |
| | The speech application might not be functioning as designed. | Debug the speech application. For more information, see the documentation for your application development tool.<br>You can also check for system resource availability, such as CPU usage, disk space, and memory usage, on the application server.<br>If the application was created with Avaya Orchestration Designer, you can run an Application report in the EPM. |
| | One or more system resources might be unavailable or not functioning properly. | Use the EPM <System name> Details tab on the System Monitor page to identify and isolate the system resource that is causing the problem. |
| | The audio codec on the switch may not match the Voice over IP (VoIP) audio settings. | Use the EPM VoIP Settings page to check the MPP Native Format drop-down setting. If it is set to audio/basic, then the codec set on the switch must include G711MU. If it is set to audio/x-alaw-basic, then the codec set on the switch must include G711A. |
| Converse-on data is not being received at the beginning of a call where it is expected. | The application might not be configured for Converse-on data. | • Verify that the application itself is designed to handle Converse-on data.<br>• Verify that the application is configured on the Experience Portal system to handle Converse-on data. |

*Table continues…*

| Symptoms | Possible causes | Where to go for more help |
|---|---|---|
| | The Converse-on data might not be making it to the application. | Troubleshoot the Converse-on data processing according to the guidelines provided in Converse-on data is not received on an H.323 connection on page 68. |

## MPP is in an unexpected operational state

The <System name> Details tab on the System Monitor page in the EPM shows the MPP operational state as Not Responding, Degraded, or Error.

### Proposed Solution 1

#### About this task

Use this solution if the httpd daemon is not running or is experiencing problems.

#### Procedure

1. At the Linux command line prompt, check the status of the `httpd daemon` process by entering the `/sbin/service httpd status` command.
2. If the `httpd daemon` process is not running, start it by entering the `/sbin/service httpd start` command.
3. If the `httpd daemon` process is running, stop it and then restart it:
    a. Stop the `httpd daemon` process by entering the `/sbin/service httpd stop` command.

    The system should respond with a message that ends with `[OK]` to indicate that the service has stopped.

    b. Restart the `httpd daemon` process by entering the `/sbin/service httpd start` command.

    The system should respond with a message that ends with `[OK]` to indicate that the service has started.
4. If these steps do not resolve the issues with the httpd daemon, continue with the solutions in Troubleshooting the httpd daemon process on page 70.

### Proposed Solution 2

#### About this task

Use this solution if the mpp daemon is not running or is experiencing problems

#### Procedure

1. At the Linux command line prompt, check the status of the `mpp daemon` process by entering the `/sbin/service mpp status` command.

2. If the systems responds with a message that the service is not running, start it by entering the `/sbin/service mpp start` command.
3. If the service is running, stop and then restart it:
    a. Stop the `mpp daemon` process by entering the `/sbin/service mpp stop` command.

    The system should respond with a message that ends with `[OK]` to indicate that the service has stopped.

    b. Restart the `mpp daemon` process by entering the `/sbin/service mpp start` command.

    The system should respond with a message that ends with `[OK]` to indicate that the mppsysmgr daemon has started.
4. If these steps do not resolve the issues with the mpp daemon, continue with the solutions in Troubleshooting the mpp daemon process on page 73.

## Proposed Solution 3

### About this task

Use this solution if one or more system resources is overtaxed, such as the CPU usage, disk space, or available memory.

### Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. From the EPM main menu, select **Real-time Monitoring** > **System Monitor**.
3. Go to the <System name> Details tab on the System Monitor page, where <System Name> matches the name of the Experience Portal system that contains the MPP whose Media Server Service Menu you want to access.
4. From the Media Server Service Menu, select **Resources**.
5. Check the status of the system resources for the MPP.

## Proposed Solution 4

### About this task

Use this solution for problems with the SSL certificate.

### Procedure

1. Check to see if an SSL certificate has been installed on the MPP.
2. If the installed SSL certificate has problems, download a new copy of the SSL certificate from the EPM.
3. Verify that the SSL certificate has been accepted on the EPM.

# Verifying if hyperthreading is enabled on the HP ProLiant DL360 G9

If the Experience Portal system does not respond as expected, hyperthreading may not be enabled on the Experience Portal servers.

Whether your system is equipped with a single processor or multiple processors, you must enable hyperthreading on the HP ProLiant DL360 G9. Hyperthreading makes each processor operate like two separate devices and increases system performance without having to add an additional processor to the system.

In the Avaya-provided or bundled server offer, hyperthreading is enabled by default. If you have opted for the Customer-provided server offer, verify if hyperthreading is enabled on the server. To enable hyperthreading, refer to the specific server documentation.

## Proposed Solution

### About this task

To verify if hyperthreading is enabled on the HP ProLiant DL360 G7:

### Procedure

1. Ensure that the server has an attached monitor and keyboard as this procedure cannot be preformed remotely.
2. Reboot the **HP ProLiant DL360 G7** server.
3. During the bootup, press **F9** to access **Configuration/Setup Utility**.
4. Using the **Down Arrow** key, highlight **System Options** and press the **Enter** key.
5. From the **System Options** menu, use the **Down Arrow** key to highlight **Processor Options** and press the **Enter** key.
6. Verify if **Intel® Hyperthreading® Options** is selected.

   **Note:**

   If the **Intel® Hyperthreading® Options** is disabled, contact the system administrator to enable it.
7. Press the **Esc** key to exit the **Processor Options** menu.
8. Press the **Esc** key to exit the **System Options** menu.
9. On the **Configuration/Setup Utility** menu, use the **Down Arrow** key to highlight **Exit Setup** and press the **Enter** key.

# System does not answer or produces only busy signals

A variety of system problems can cause the MPP to not answer a call or respond with a busy signal. For example, one or more MPPs might be out-of-service or experiencing other problems.

The following solutions can help you to resolve the majority of these cases. If none of these solutions help to identify and resolve the problem, contact your Avaya technical support representative for assistance.

**Related links**

Synchronizing the EPM and an MPP on page 17

## Proposed Solution 1

### Procedure

1. Log into the EPM using any valid EPM user account.
2. Verify that the operational state of the MPP is **Running**.
3. Verify that ports are being assigned to the MPP.
4. Create an alarm report for that MPP and resolve any issues noted in the alarms.
5. On the Applications pages, check the **Launch** column to make sure that there is an application with the DNIS (the number that the caller dialed) assigned.

## Proposed Solution 2

### Procedure

1. Log in to the Media Server Service Menu, as described in the *Logging in to the MPP Service Menu* topic in the *Administering Avaya Experience Portal* guide.

   **Note:**

   If you cannot log in to the Media Server Service Menu, check the status of the httpd daemon process.

2. On the MPP Service Menu home page, verify that the value of the **Run state** field in the **MPP Status** table is **Running**.

   - If the operational state displayed in this field differs from the operational state displayed on the <System name> Details tab on the System Monitor page, synchronize the EPM and the MPP to resolve connection problems.
   - If the **Run state** field does *not* say **Running**, start the MPP or troubleshoot the problem that is keeping the MPP from starting.

3. On the MPP Service Menu home page, verify that the value of the **Configuration state** field in the **MPP Status** table is **Configuration OK**.

   If the **Configuration state** field does *not* say **Configuration OK**, check the configuration state of the MPP.

4. Check the state of all critical processes.

## Proposed Solution 3

### Procedure

1. On the Media Server Service Menu, click **Resources**.

2. On the Resources page, click **Telephony**.

   **Tip:**

   You can also use the `listst.php` administrative script to obtain this information about the MPP.

3. On the Telephony Resources page, verify that all channels display a state of **In-Service** in the **Channel State** column.

4. If a channel does *not* display **In-Service**, troubleshoot the problem between the Communication Manager and the MPP:

   - On the EPM, check the H.323 connection settings, especially the password as described in the *H.323 connections in Avaya Experience Portal* topic in the *Administering Avaya Experience Portal* guide.
   - On the EPM, check the information for the channel (port) or channels that seem to be experiencing problems.
   - Check theCommunication Manager to see if it displays the same status for the affected channels (ports) as the MPP does, as described in your Communication Manager documentation.
   - If you cannot resolve the problem using any of these strategies, contact your Avaya technical support representative for assistance.

5. Check the `SessionManager` logs for errors that indicate the system has had problems gaining access to Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) resources:

   a. On the Media Server Service Menu, click **Logs**.

   b. On the Log Directories page, click **SessMgr**.

   c. Click on the log you want to view.

      The available log types are:

      - `SessionManager.log`: Contains data related to events that are not specifically associated with a single session.
      - `SessionSlot-###.log`: Contains data related to Session Manager operations for individual sessions. The `###` represents the unique cookie, or identifier, that you can use to find related Session Manager, CCXML interpreter, and Avaya Voice Browser logs.

## System answers and then hangs up

**Related links**

Experience Portal system status on page 9

## Proposed Solution

### Procedure

1. If you cannot verify any URI settings, troubleshoot the problem with the URI settings.
2. If you created your applications in Orchestration Designer, use the EPM to create an Application report containing the application messages, as described in the *Application activity reports* topic in the *Administering Avaya Experience Portal* guide.
3. Use the Session Detail report to examine session details for the affected calls, as described in the *Creating a Session Detail report* topic in the *Administering Avaya Experience Portal* guide.

# Encryption settings are not synchronized

If the encryption settings on the Experience Portal system and on the Communication Manager do not agree, the system can fail to either prompt callers or recognize responses, even though the MPPs seem otherwise to be healthy. This condition is evident when the system answers calls but then fails to respond further.

For more information about the encryption settings on:

- Experience Portal, see *H.323 connections in Experience Portal* in the *Administering Avaya Experience Portal* .
- Communication Manager, see your Communication Manager documentation set.

## Proposed Solution

### About this task

Both Experience Portal and Communication Manager must have encryption enabled or both must have encryption disabled.

### Procedure

1. Ensure that the encryption settings on the Experience Portal system and on the Communication Manager match.
2. If you are using:
    - H.323 connections, make sure that you have configured Communication Manager as described in *Avaya Configuration Note 3910*.
    - SIP connections, make sure that you have configured Communication Manager as described in *Avaya Configuration Note 3911*.

# Converse-on data is not received on an H.323 connection

If converse-on data is not received at the beginning of a call using an H.323 connection, the system may have encountered the following problems:

- The application is not configured for Converse-on data.
- The Converse-on data was not sent to the application.

If both the application and the EPM are configured correctly for Converse-on, but at run-time, the Converse-on data is not processed, you must troubleshoot to find out where the data is getting lost.

**Related links**

Experience Portal system status on page 9

## Proposed Solution

### Procedure

1. On the MPP, navigate to the `$AVAYA_MPP_HOME/logs/process/SessMgr` directory and open the `SessionSlot###.log` files.

   Where `###` is a three-digit ID number.

2. To see if Converse-on data is received by the MPP, check the Session Manager logs for entries that contain the following text:

   ```
   waiting for ConverseOnData
   received converse on digits
   ```

3. If the Session Manager logs indicate that Converse-on data is:

   - Not received, go to Step 4.
   - Received, go to Step 5.

4. Verify with the Communication Manager programmer or administrator that the vector is properly configured and is sending the expected data.

5. Navigate to the `$AVAYA_MPP_HOME/logs/process/VB` directory and open the `SessionSlot###.log` files.

   Where `###` is a three-digit ID number.

6. To verify that the Converse-on data is added to the query string that is sent to the application, search the VB logs for the term "converse":

   In these logs, the Converse-on digits collected by the Session Manager should be part of a query string sent to the application server as:

   ```
   &session vpconverseondata=###...
   ```

   Where ###... is the sequence of digits sent.

7. On the application server, verify that the Converse-on data is being received.

   Contact your application developer if you need assistance.

# PHP script fails to run with Aborted error message

When a PHP script fails to run and the system generates an error message that says `Aborted (core dumped)`, there are several possible causes. For example, the user may not be logged into Linux with the proper permissions.

## Proposed Solution

### Procedure

1. Log on to Linux on the Experience Portal MPP server as a user with root privileges.
2. Verify that the user is a member of avayavpgroup by entering the `cat /etc/group | grep avayavpgroup` command.

   The system displays the list of users that are members of avayavpgroup.
3. If the user does not appear in the list of group members, add the user to the avayavpgroup by entering the `gpasswd -a` *`username`* `avayavpgroup` command, where *`username`* is the user ID you want to add to the group.
4. Verify that the following files and their parent directories have the group set to avayavpgroup and read-write permissions set:
   - `$AVAYA_MPP_HOME/tmp/mgtlib.php.out`
   - `$AVAYA_MPP_HOME/logs/process/SysMgr/logfile.log`
5. If one or both the files or directories do not have the correct group or permissions, set them to read-write for the avayavpgroup.
6. If these actions do not resolve the problem, contact your Avaya technical support representative for assistance.

# Monitoring call progress in real time

If your Experience Portal system encounters problems during the progress of a call, you can set up your system to monitor call progress in real time.

**Related links**

MPP server logs on page 133

## Proposed Solution

### Procedure

1. If your system uses H.323 connections, you must configure the MPP server you want to monitor to use the Test operational mode so that you are certain your test calls will go to the correct MPP.

2. Verify that you have the trace logging for the MPP enabled and set to the appropriate levels.
    a. Log on to the EPM web interface by using an account with the Administration user role.
    b. From the EPM main menu, select **System Configuration** > **MPP Servers**.
    c. On the MPP Servers page, click the name of the MPP you want to monitor in the **Name** column.
    d. On the Change MPP Server page, go to the **Categories and Trace Levels** section and set the appropriate options.
    e. When you are finished, click **Save**.
3. If you want to clear all log files so that you can easily see what data is being added:
    a. Log in to the Media Server Service Menu as described in the *Logging in to the MPP Service Menu* topic in the *Administering Avaya Experience Portal* guide.
    b. From the Media Server Service Menu, select **Logs**.
    c. Click **Clear log files in all the directories**.
4. Log in to Linux on the MPP server that you want to monitor using an account that is a member of the avayagroup.
5. If you want to monitor:
    - Live output to the Session Manager log file, enter the commands `cd $AVAYA_MPP_HOME/logs/process/SessMgr` and `tail -f SessionManager.log`
    - Live output to the session slot log file, enter the commands `cd $AVAYA_MPP_HOME/logs/process/SessMgr` and `tail -f SessionSlot-####.log`
6. Make a test call and observe the data output.

    **Tip:**

    Depending on the trace logging level you have selected for the MPP, the information might scroll by faster than you can read it. If that happens, use the **`vi`** command.
7. If the `SessionManager.log` file does not contain the information you need to solve your problem, review the other MPP server log files.

# Troubleshooting the httpd daemon process

The MPP uses the Apache Web server for performing operations. The Apache Web server is identified on the system and controlled by the `httpd daemon` process process. Therefore, if you suspect problems with the Apache Web server, check the status of the `httpd daemon` process.

**Note:**

These strategies assume that you have checked the Avaya Experience Portal system status on the <System name> Details tab of the System Monitor page.

Problems with the `httpd daemon` process can manifest in the following ways:

- The EPM indicates that the operational state of the MPP is **Not Responding** or **Unknown**.
- When you log in to the Media Server Service Menu, the browser window displays an error message that the page cannot be displayed, the server cannot be found, or there is a DNS error.
- An improper system shutdown left a locked process file.
- The MPP key and/or certificate is corrupted.

If none of these solutions help to identify and resolve the problem, contact your Avaya technical support representative for assistance.

## Proposed Solution 1: Restarting the httpd daemon process

### Procedure

1. Log on to the MPP server as a root user.
2. At the Linux command line prompt, check the status of the `httpd daemon` process by entering the `/sbin/service httpd status` command.
3. If the `httpd daemon` process is not running, start it by entering the `/sbin/service httpd start` command.
4. If the `httpd daemon` process is running, stop it and then restart it:
    a. Stop the `httpd daemon` process by entering the `/sbin/service httpd stop` command.

    The system should respond with a message that ends with `[OK]` to indicate that the service has stopped.

    b. Restart the `httpd daemon` process by entering the `/sbin/service httpd start` command.

    The system should respond with a message that ends with `[OK]` to indicate that the service has started.
5. If the system responds with a message stating that the service cannot be started because there are locked files:
    a. Delete the lock file by entering the `rm /var/lock/subsys/httpd` command.

    b. Start the service again by entering the `/sbin/service httpd start` command.

    If the service still does not start, see Proposed Solution 2: Examining the httpd daemon process MPP log files on page 72.

6. Let the service run for several minutes, and then check the status by entering the `/sbin/service httpd status` command.

   If the service is:

   - Running, wait and see if the problems reoccur. If they do, see Proposed Solution 2: Examining the httpd daemon process MPP log files on page 72.
   - Stopped , see Proposed Solution 2: Examining the httpd daemon process MPP log files on page 72.

## Proposed Solution 2: Examining the httpd daemon process MPP log files

### Procedure

1. In an ASCII editor, open the following log files:
   - `/var/log/error_log`
   - `/var/log/httpd/ws_error_log`
2. Search both log files for the following error messages:
   - `>Unable to configure RSA server private key`
   - `>SSL Library Error: 185073780 error:0B080074:x509`
   - `certificate routines:X509_check_private_key:key values`
   - `mismatch`
3. If you find these errors in either log file, reinstall the MPP software to create a new certificate on the MPP.

   When you reconnect the MPP and the EPM, these errors should be resolved.
4. If you do not find these errors in either log file, see Proposed Solution 3: Examining the httpd daemon process log files on page 72.

## Proposed Solution 3: Examining the httpd daemon process log files

### Procedure

1. Log into Linux on the EPM server.
2. In an ASCII editor, open the EPM log file `/opt/Avaya/ExperiencePortal/VPMS/logs/avaya.vpms.log`.
3. Search for error messages relating to the `httpd daemon` process.
4. If you do not find any messages relating to the problem, In an ASCII edit, open the log file `$CATALINA_HOME/logs/catalina.out`.

5. Search for error messages relating to the `httpd daemon` process.
6. If you do not find any messages relating to the problem, contact Avaya technical support.

# Troubleshooting the mpp daemon process

The MPP uses the `mpp daemon` process to start and control the various processes that enable the MPP to function as it should. If this process does not start, stops working, or experiences other problems, the MPP does not respond as it should. Therefore, if you are having problems with the MPP and you have confirmed that the `httpd daemon` process is running correctly as described in Troubleshooting the httpd daemon process on page 70, the next step is to check the status of the `mpp daemon` process.

Problems with the `mpp daemon` process can manifest in the following ways:

- An improper system shutdown left a locked process file.
- A conflict exists with permissions for the `mppsysmgr` directory or log file.

## Proposed Solution 1: Restarting the mpp daemon process

### Procedure

1. At the Linux command line prompt, check the status of the `mpp daemon` process by entering the `/sbin/service mpp status` command.
2. If the systems responds with a message that the service is not running, start it by entering the `/sbin/service mpp start` command.
3. If the service is running, stop and then restart it:
    a. Stop the `mpp daemon` process by entering the `/sbin/service mpp stop` command.

       The system should respond with a message that ends with `[OK]` to indicate that the service has stopped.

    b. Restart the `mpp daemon` process by entering the `/sbin/service mpp start` command.

       The system should respond with a message that ends with `[OK]` to indicate that the mppsysmgr daemon has started.
4. If the system responds with a message stating that the service cannot be started because there are locked files:
    a. Delete the lock file by entering the `rm /var/lock/subsys/mppsysmgr` command.

    b. Try to start the service again by entering the `/sbin/service mpp start` command.

If the service still does not start, see Proposed Solution 2: Examining the mpp daemon process log files on page 74.

5. Let the service run for several minutes, and then check the status again by entering the `/sbin/service mpp status` command.

   If the service status is not running, or if the problems reoccur, see Proposed Solution 2: Examining the mpp daemon process log files on page 74.

## Proposed Solution 2: Examining the mpp daemon process log files

### Procedure

1. In an ASCII editor, examine the `$AVAYA_MPP_HOME/logs/process/SysMgr/logfile.log` log file.
2. If you find relevant error messages in the file, perform the troubleshooting procedures described for that error message.
3. If you cannot find any relevant error messages or if the troubleshooting procedures do not resolve the problems, see Proposed Solution 3: Checking for core files on page 74.

## Proposed Solution 3: Checking for core files

### Procedure

1. Log into Linux on the MPP server.
2. Navigate to the `$AVAYA_MPP_HOME/logs/core` directory and check to see if there are any `mppsysmgr*` core files in that directory.
3. If the directory contains core files, delete the `$AVAYA_MPP_HOME/logs/process/SysMgr/` directory.

   This solution resolves problems with permissions on the log file or directory.
4. Reboot the MPP server.
5. If you do not find any core files, or if deleting the files does not solve the problem, contact Avaya technical support.

# Troubleshooting SSL Issues

## SSL certificate requirements

The MPP and EPM use SSL mutual authentication to protect the data exchanged between the Web Services on both servers. Mutual authentication requires that certificates be exchanged between the servers. If the certificates do not exist or are corrupted, the EPM is not able to establish contact with the MPP.

MPP configuration for mutual authentication requires that:

- The MPP has its own key and certificate. This certificate is used when the MPP Web services or the Media Server Service Menu is accessed. During the installation of MPP software, you are prompted to either provide the certificate or have the installation create one for you.
- The MPP has a valid copy of the EPM SSL certificate downloaded to register the EPM as a recognized certificate authority. The EPM SSL certificate is downloaded during MPP software installation. However, if the MPP SSL certificate and key appear valid and you are still having trouble with exchange of data between the MPP and the EPM, you can validate, and redownload the EPM SSL certificate.
- The MPP configuration file, `mpp.conf`, must have the correct paths to the SSL certificate and key files. The httpd daemon uses this file at startup to establish communications between the MPP and the EPM. If the paths in this file are not valid, the two servers cannot establish secure communications.

For more information about Apache and SSL, see SSL/TLS Strong Encryption.

## MPP SSL certificate and key location

The MPP key and certificate files are located at:

- `/opt/Avaya/ExperiencePortal/pki/ep_identity_cert.crt`
- `/opt/Avaya/ExperiencePortal/pki/ep_private_key.key`
- `/var/www/html/cert.pem`

### Sample MPP SSL certificate

```
-----BEGIN CERTIFICATE-----
MIICfDCCAeWgAwIBAgIBADANBgkqhkiG9w0BAQQFADA5MQwwCgYDVQQLEwNNUFAx
DjAMBgNVBAoTBUF2YXlhMRkwFwYDVQQDExBtbHZvaWNlcG9ydGFsLWE5MB4XDTA1
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQCU36+QLX56yDK0l4wkb8Ai
VQQKEwVBdmF5YTEZMBcGA1UEAxMQbWx2b2ljZXBvcnRhbC1hOTCBnzANBgkqhkiG
zPEZEzz12iYGBB7EzvN8WsbUVU+7hN1ojNsidt25gTu8ol2Pnz4pnonGAc3xowAo
9w0BAQEFAAOBjQAwgYkCgYEAt9166cK3sMldlsq83aFwwykCeItEA/XDZbyYewKP
z2T6RDS2TD+EwDKQjuxo8h1upDVFgherJdK4Ks+PvbnN6yIxW39wOU8Gl3JbWJgR
1WrRVjelUg5hpVcHxkdkRynkmM8bJBvaohqS5NMiygBfUXaz+Qx7wWVevkM7qdeM
MDkyOTE2MTExM1oXDTE1MDkyNzE2MTExM1owOTEMMAoGA1UECxMDTVBQMQ4wDAYD
GMMCAwEAAaOBkzCBkDAdBgNVHQ4EFgQUUH67bdY3lHOTZVx6u34wj1roPvwwYQYD
WSz+QXogX265wzyYXZDQuGZ9hRm0nhQjXv20C6EfNK8T+g03/NfqqxqjJdKrelya
VR0jBFowWIAUUH67bdY3lHOTZVx6u34wj1roPvyhPaQ7MDkxDDAKBgNVBAsTA01Q
UDEOMAwGA1UEChMFQXZheWExGTAXBgNVBAMTEG1sdm9pY2Vwb3J0YWwtYTmCAQAw
```

```
WZg0Cm00qzzk9qWf9SKpbg==
-----END CERTIFICATE-----
```

### Sample MPP SSL key

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDRDLYER7QG4eqj
st3RVzOoHdRqxnbbVDCiGEfX6IvgvSTVc9own+diMA89RkLluZXeVwT5qiJIUWKM
CtQI5MLYSlgfEW/TO4rXPHTKh9nOShZEcvqmj4J4YZL7A6hqbGpPIyaCwiwLIi6U
ajz5mQiH4teaThxFs+A+tuHo9+gPfg7Uj2z2eYXrp0HBRwQ9VstIoX1TVoynf651
1RRWekrixHeWB/ZyffGINf2h2Qgd3a1J7U8Ofm3+7b6+bBBc6sdkx/SCiiFf8Rw7
wM86SFpHB+TtRKt/DVd0tbfBWyxPcIOpWHdgtHxMT5NQug6mile/LkVf62EzCsN3
RvP5sL+PAgMBAAECggEAZLfCDifZtaMs4DeyJUTlL29HwzXhV+SlFcOrAXwZwGqA
j5Kkod64pRbQkM4ENxgF+7xjOkJdCAil+SDSbYKB2aFf+X/2J4g9aVvITTfMmVYa
iln3Jz5nNsaUAPoPL08SnRQrXr5cZ/TNClZxEDRJ5uZEyCQv/Okf9jc4enzOQn+z
U/1AvZNnGsOHI7XDpkuUArILLTjezgD7PKLHiQC2YKZzwMjM3Na1qfyBhFPqbatn
nkkShUMNV2ED+2q9qdJfEH8iSIqFYGx/c4Paiejfp49XdFpwvGKeHamljmh/2ytk
3i31QYBR99y40qyr0CnMJlBzp4Ym/n93LnDoKddRsQKBgQDx8nuG62yFcPxgPPfJ
WW4r5Xtgq1fpMeYHWrW5+Y5kLXmgb8flE8tAY8lLgGESAbEMzc6sSQFf7TrQ3NCL
lGxV7r98G/FOFD9Q66Ef0yK86vEXkvvljKhf7u2olpw+nl0Lwownmc+ig0i8iXlU
bNqmojtdbHRrj+4/MwfgTltHxwKBgQDdMRMCSq2/UP876E1i/YkDrVVt7Orts9H9
tx02Dv0LvbnIW+0+Hn8r86fQHUHYNljmjc4WbL7LlSl+NfAOi1hzmC5X06WYe6cH
OHR5j825DVKvdDrNj7aEmiAlvQIGhzjgfGkYK7VR16GTnHC2fTGp3Skt2wvBbTEM
Q/x5tu6Z+QKBgQDxFziiPAvaeLjzySz8lcHjufuUW4jxVYirQWeelx+dkXcGOPzO
t0estQKL2rRfthHP+XD9Wo4lIYafQ7oHrHG7u3lR2aI9tI1XPEVFKiYObGqrnAqo
Nd4+Ih7uBI5TE4kSQ91XRLyTaxDa1n5xczr6GuTe9kiYOkck8NvjVxE8VwKBgQDA
GGJ91wVV5a4EBRdQJQfdHafXs63DiiuQwHqp/BJfJAI4sz0yeaHQNedDomUQtQI4
GGcmqoJ4o65JYeZ9ex7yJPP6amCiMKE6cBkXiYAMejmZDsQSygCk4IWSwLcFnGIU
83cB+tOZpD86xt5MXiXHc77TiCyJa57xHAokWm6VYQKBgHhwqqrZ6no6Yf0ms444
o+i9rQX4DzscNwyCpQ8qVhClZajZ9Cv4CBWebufLxYRxRDVGWcyh1DISc+z1TdpS
QUcJ8tmUpVwrl0dSPI6h3aj1iASwAv0yUkq2A7n2DNqQ4oVu3zGUydiajGO7xq2E
t6oS/fVsqS/sCl866FUycshZ
-----END PRIVATE KEY-----
```

If these files appear valid, check the Apache logs for possible errors. If these files are missing or appear to be corrupted, either reinstall the certificates, or reinstall the MPP software to generate new self-signed certificates. For more information on the Apache logs, see MPP server logs on page 133.

## Validating the EPM SSL certificate copy on the MPP

### About this task

During MPP installation, the installation script creates a symbolic link to this file, which Apache uses to access the certificate. If that symbolic file does not exist, a connection cannot be established between the MPP and the EPM. Therefore, you must also verify that the symbolic link exists on the MPP.

### Procedure

1. Compare the MPP certificate to the one on the EPM by entering the `curl http://`*`EPM-server`*`/cert.pem` command, where *`EPM-server`* is the domain name or IP address of the system where the primary EPM software is installed.
2. At the Linux command line prompt, enter the `cat $AVAYA_MPP_HOME/web/ssl.crt/vpms.crt` command.

The system should respond with a message similar to the following:

```
-----BEGIN CERTIFICATE-----
MIICfDCCAeWgAwIBAgIBADANBgkqhkiG9w0BAQQFADA5MQwwCgYDVQQLEwNNUFAx
DjAMBgNVBAoTBUF2YXlhMRkwFwYDVQQDExBtbHZvaWNlcG9ydGFsLWE5MB4XDTA1
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQCU36+QLX56yDK0l4wkb8Ai
VQQKEwVBdmF5YTEZMBcGA1UEAxMQbWx2b2ljZXBvcnRhbC1hOTCBnzANBgkqhkiG
zPEZEzz12iYGBB7EzvN8WsbUVU+7hN1ojNsidt25gTu8ol2Pnz4pnonGAc3xowAo
9w0BAQEFAAOBjQAwgYkCgYEAt9166cK3sMldlsq83aFwwykCeItEA/XDZbyYewKP
z2T6RDS2TD+EwDKQjuxo8h1upDVFgherJdK4Ks+PvbnN6yIxW39wOU8Gl3JbWJgR
1WrRVjelUg5hpVcHxkdkRynkmM8bJBvaohqS5NMiygBfUXaz+Qx7wWVevkM7qdeM
MDkyOTE2MTExM1oXDTE1MDkyNzE2MTExM1owOTEMMAoGA1UECxMDTVBQMQ4wDAYD
GMMCAwEAAaOBkzCBkDAdBgNVHQ4EFgQUUH67bdY3lHOTZVx6u34wj1roPvwwYQYD
WSz+QXogX265wzyYXZDQuGZ9hRm0nhQjXv20C6EfNK8T+g03/NfqqxqjJdKrelya
VR0jBFowWIAUUH67bdY3lHOTZVx6u34wj1roPvyhPaQ7MDkxDDAKBgNVBAsTA01Q
UDEOMAwGA1UEChMFQXZheWExGTAXBgNVBAMTEG1sdm9pY2Vwb3J0YWwtYTmCAQAw
WZg0Cm00qzzk9qWf9SKpbg==
-----END CERTIFICATE-----
```

3. Change to the directory in which the SSL certificate from the EPM resides by entering the `cd $AVAYA_MPP_HOME/web/ssl.crt/` command.
4. List all files in this directory by entering the `ls -al` command.

   You should see a symbolic link to the `vpms.crt` file, similar to the following entry:

   ```
   lrwxrwxrwx  1 ^sroot^root^   8 Oct  7 18:21 36c998fa.0 -> vpms.crt
   ```

   The "`l`" at the beginning and the"`-> vpms.crt`" text at the end indicate that the symbolic file has been created. In this example, the file is named`36c998fa.0`.

   **Note:**

   This file is created and named automatically by the installation script, using a hash security encryption scheme.
5. Did the system respond correctly to both these commands?
   - If yes, an SSL certificate is correctly installed on the MPP. No further action is required, unless you want to ensure that the certificate is valid. In that case, you can reinstall the certificate.
   - If no, the SSL certificate either is not installed or is invalid. Try reinstalling the certificate.

## Validating the MPP configuration file for the SSL certificates

### About this task

The MPP configuration file, `mpp.conf`, contains, among other things, the paths for the SSL certificates, both for the MPP and for the EPM.

**Important:**

The EPM expects to find the MPP certificate at `/var/www/html/cert.pem`. If you change this location, the EPM may not be able to find the certificate.

## Procedure

1. Log in to the MPP server whose configuration file you want to validate.
2. At the Linux command line prompt, enter the `cat $AVAYA_MPP_HOME/config/mpp.conf` command.

   The system displays the contents of the entire MPP configuration file.
3. Locate the entry for the MPP SSL certificate and key in the Global section.

   The entry should be identical to the following:

   ```
   SSLCertificateKeyFile
   /opt/Avaya/ExperiencePortal/pki/ep_private_key.key
   SSLCertificateFile
   /opt/Avaya/ExperiencePortal/pki/ep_identity_cert.crt
   ```
4. Locate the entry for the MPP SSL certificate and key in the Virtual Host port 9443 section.

   The entry should be identical to the following:

   ```
   SSLCertificateKeyFile
   /opt/Avaya/ExperiencePortal/pki/ep_private_key.key
   SSLCertificateFile
   /opt/Avaya/ExperiencePortal/pki/ep_identity_cert.crt
   ```
5. Locate the entry for the MPP SSL certificate and key in the Virtual Host port 10443 section.

   The entry should be identical to the following:

   ```
   SSLCertificateKeyFile
   /opt/Avaya/ExperiencePortal/pki/ep_private_key.key
   SSLCertificateFile
   /opt/Avaya/ExperiencePortal/pki/ep_identity_cert.crt
   SSLCertificateChainFile
   /opt/Avaya/ExperiencePortal/pki/ep_cert_chain.crt
   ```
6. Locate the entry for the EPM SSL certificate download.

   This entry should look similar or identical to:

   ```
   SSLCACertificatePath "/opt/Avaya/ExperiencePortal/MPP/web/ssl.crt"
   ```
7. If any of these entries are different from what you have actually configured on your system, use a text editor to edit the `mpp.conf` file to reflect the actual configuration.
8. If you manually edit the `mpp.conf` file, you must restart the `httpd daemon` process to activate the changes:

   a. Stop the `httpd daemon` process by entering the `/sbin/service httpd stop` command.

      The system should respond with a message that ends with `[OK]` to indicate that the service has stopped.

   b. Restart the `httpd daemon` process by entering the `/sbin/service httpd start` command.

      The system should respond with a message that ends with `[OK]` to indicate that the service has started.

# Reinstalling the SSL certificate from the EPM

## Procedure

1. Log on to Linux on the Experience Portal MPP server.

   If you are an Avaya Services representative, and use Avaya Enterprise Linux, the Avaya Service accounts will not be available after the Avaya Enterprise Linux upgrade. The Avaya Service accounts will be available through EASG configuration during the Experience Portal upgrade.

   - Log on to the local Linux console as root.
   - Or log on remotely as a non-root user and then change the user to root by entering the `su - root` command.

2. At the Linux command line prompt, enter the `$AVAYA_HOME/Support/Security-Tools/setup_vpms.php` *`myhost`* command, where *`myhost`* is the server name or IP address where the EPM software is installed.

   The MPP queries the EPM for the SSL certificate, and if the certificate is located, asks for confirmation that you want to install it:

   ```
   Please enter ’y’ to accept this certificate as an authorized
   controller of the MPP server, or enter ’n’ to abort. [y]?
   ```

3. Enter `y`.

   The system responds with the following message and prompt:

   ```
   The httpd daemon (Apache) must be restarted to complete the certificate's
   installation.
   Enter 'y' if you would like httpd restarted now. [y]
   ```

4. Enter `y`.

   The system responds with the following message and prompt:

   ```
   The NTP daemon should be configured to use the EPM as the NTP server.
   Enter 'y' if you would like the NTP daemon configured with this EPM. [y]
   ```

5. If you want the EPM server to be configured as the NTP server for this MPP, enter `y`. Otherwise, enter `n`.

   The Network Time Protocol (NTP) allows the clock on the EPM server to be used as the reference point for synchronizing the clocks of all servers in the Experience Portal network. Because this can make troubleshooting and other maintenance activities more efficient, you can select this option.

6. Does the MPP indicate that the certificate was installed successfully?

   - If yes, and if the problems the system was experiencing do not recur, no further action is required.
   - If yes, but the problems persist, pursue other possible solutions or contact your Avaya technical support representative for assistance.

- If no, try rebooting the MPP. If that does not resolve the problem, contact your Avaya technical support representative for assistance.

# Chapter 6: Troubleshooting general issues

## Cannot mount DVD on an Avaya Linux server

When you run the **`mount /mnt/cdrom`** command on an Avaya Linux server, the server might display the error `mount:No medium found`.

The server displays the error if the wrong physical device is mapped to the mount point `/mnt/cdrom in the file /etc/fstab`.

## Proposed Solution

### Procedure

1. Log in to Linux on the Experience Portal server as a user with root privileges.
2. Run the **`cat /proc/sys/dev/cdrom/info`** command.

   The system displays the information about the DVD devices. An example of the information that the system displays:

   ```
   drive name:        sr0   had
   drive speed:       0    24
   drive # of slots:  1    1
   drive # of slots:  1    1
   ```
3. In the output displayed, find the row for drive speed.
4. Within the row for drive speed, find the column that contains a non-zero value.

   For example, in the system output mentioned in Step 2, the column that contains the a non-zero value is in the second row with a value of `24`.
5. In the column that contains a non-zero value, move up one row to find the drive name.

   For example, in the system output mentioned in Step 2, the drive name is hda.
6. Run the **`ls -l /dev | grep cdrom`** command to display a list of device special files associated with the DVD devices.

   The system displays a list of device special files. For example:

   ```
   lrwxrwxrwx..1..sroot..root..4..Aug 31 08:11...cdrom ->     scd0
   lrwxrwxrwx..1..sroot..root..3..Aug 16 11:16...cdrom-hda -> hda
   lrwxrwxrwx .1..sroot..root..4..Aug 31 08:11...cdrom-sr0 -> scd0
   ```
7. In the output displayed, find the line for the drive name that you have identified in step 5.

For example, if you identify the drive name hda in step 5, the line that you need to find ends with `cdrom-hda -> hda`.

8. In the line, find the device special file name that is listed before the drive name.

   For example, in the system output mentioned in Step 6, the device special file name is `cdrom-hda`.

9. Open the file `/etc/fstab` in a text editor.

10. Find the line `/dev/cdrom /mnt/cdrom iso9660 noauto,owner,ro 0 2`

11. Change `/dev/cdrom` to the path of the device special file that you locate in step 8.

    For example, if the file name is `cdrom-hda`, the corrected line is `/dev/cdrom-hda /mnt/cdrom iso9660 noauto,owner,ro 0 2`.

12. Save and close the file.

# Troubleshooting issue with SDR not created for sendSMS and sendEmail

An SDR record is not created unless an application session is started. Without an application session, the SDR is 99% empty.

Typically the `sendEmail` and `sendSMS` are handled by the Pluggable Device Connector (PDC) that passes the Session ID of the running application. The running application has an SDR. For example, the SMS registration application is a VoiceXML application that handles `sendSMS`. An SDR and two CDRs (one for voice call and one of the outbound SMS) are generated for the voice application , all sharing the same Session ID.

Only a launched SMS application generates an SDR. An SMS application is launched either by an incoming message or launched by the `LaunchSMS` Webservice method.

**Note:**

The `sendSMS` Webservice method does not launch an SMS application. This method merely sends an SMS message. The application is not involved. The application name referenced in the `sendSMS` method determines how much of the message to log in the CDR record based on the privacy settings in the EPM configuration of that application.

# Application is not receiving an inbound SMS

## Proposed solution

### Procedure

1. From the **EPM** menu, select **Real-Time Monitoring** > **System Monitor**.
2. Check if the SMS processor is in the **Running** state.

   The **System Monitor** might show any of the following statuses for the SMS processor:

   - **Need Configuration**: SMS processor is not configured and enabled
   - **Need Connection**: SMS connection is not configured and enabled
   - **Running**: The SMS processor is connected to all SMS connections
   - **Degraded**: Some of the SMS connections are experiencing a connection issue. For example: Invalid credential, Firewall issue, bad IP address, and so on
   - **Error**: All the SMS connections are experiencing a connection issue

   **Note:**

   - If the System Monitor does not show an SMS processor, then check if an SMS processor is configured and enabled.
   - When multiple SMS processors are defined, ensure that the connection under test is assigned to the expected processor. You can view a list of the SMS processors and associated SMPP connections in the primary EPM web page at Home >Multi-Media Configuration > SMS. Ensure to check the log file, which is mentioned in the following step, on the correct processor.
3. If the SMS processor is in **Running** state, proceed to the next step. Else, check the error log in **EPM Log Viewer**, from: **EPM Home** > **System Maintenance** > **Log Viewer**.
4. Check if the SMS processor is receiving any message from the provider.

   a. From the EPM menu, select **Home** > **Multi-Media Configuration** > **SMS** > **SMS Settings** to view the SMS settings.

   b. Ensure that the SMS trace levels are set to **finer** or **finest**.

   c. Search `/opt/Avaya/ExperiencePortal/VPMS/logs/avaya.sms.log` for the word **onInbound** for SMPP connections or **processInboundHTTP** for HTTP inbound connections such as Avaya Zang. For example:

   @2013-09-24 20:16:40,793||FINER|sms.core.SmppLink|VoicePortal|Receiver-10|SmppLink[ODSVSimulator].**onInbound**: requestId: EPM-1380079000793-42; sessionId: EPM-2013267201640-18; ucid: 10002000391380079000; seqNum: 1; from: 4085551212; to: 4085551313 |####

   @2016-07-28 10:31:00,956||FINEST|avaya.smsbrowser.PollInboundSMS|VoicePortal|SMS-Poller|**processInboundHTTP**: Requesting URL <https://

```
api.zang.io/v2/Accounts/ACbf88908423893ae92688445588a843d1/SMS/
Messages.json?To=17795551212&Page=0&PageSize=10&DateSent>=2017-01-27>|
####

@2016-07-28 10:31:01,823||FINEST|avaya.smsbrowser.PollInboundSMS|
VoicePortal|SMS-Poller|processInboundHTTP: Received 5551 bytes|####

@2016-07-28 10:31:01,824||FINEST|avaya.smsbrowser.PollInboundSMS|
VoicePortal|SMS-Poller|processInboundHTTP: Saving SID
SM22889084ef3ddc8be4c14603b9ccccaa for longcode 17795551212|####

@2016-07-28 10:31:01,824||FINER|avaya.smsbrowser.PollInboundSMS|VoicePortal|
SMS-Poller|processInboundHTTP: Read 1 new message from link Avaya Zang for
code 17795551212|####
```

5. If the SMS processor is receiving a message from the provider, proceed to the next step. Else, run the reports from your SMSC. If the messages are arriving intermittently, you might have another connection from another EP system that is taking the message.
6. Check, which application the message was routed to. Search for the word **Seleted** in `avaya.sms.log`. For example:

   ```
   @2013-09-24 20:16:45,510||FINER|avaya.smsbrowser.InboundMessageProcessor|
   VoicePortal|pool-2-thread-42|Selected app: 0:appname for TextMessage[Id=SMS-58;
   4085551212->4085551313;type=normal;providerId=1;status=0]|####
   ```

7. If the application name is correct and the application is enabled in EPM, proceed to the next step. Else, check your application configuration on the EPM, from **Home** > **System Configuration** > **Applications** > **Change Application**.

   Check the selected application, as it might have similar launch parameters.
8. Check if the `trace.log` file on the application server indicates that the Orchestration Designer application was started.
   a. Set the value of **Application Traces** to **Yes**. You can view the **Application Traces** field under the **Reporting Parameters** section for application configuration on the EPM, at **Home** > **System Configuration** > **Applications** > **Change Application**
   b. Depending on the value of the `trace.log` file, do the following:

| OD application started? | Resolution |
|---|---|
| **Yes** | You might have an application related problem. Add additional trace statements to the application to debug further. |
| **No** | Check the application URL in the application configuration section of the EPM. Click the **Verify** button next to the URL to ensure that the application URL is accessible from the EPM. Verify that the correct proxy server and port, if required, is configured at **Home** > **Multi-Media Configuration** > **SMS** > **Browser Settings**. |

# Outbound SMS are not received on the cell phone

## Proposed Solution

### Procedure

1. From the **EPM** menu, select **Real-Time Monitoring** > **System Monitor**.
2. Check if the SMS processor is in the **Running** state.

   The **System Monitor** might show any of the following statuses for the SMS processor:

   - **Need Configuration**: SMS processor is not configured and enabled
   - **Need Connection**: SMS connection is not configured and enabled
   - **Running**: The SMS processor is connected to all SMS connections
   - **Degraded**: Some of the SMS connections are experiencing a connection issue. For example: Invalid credential, Firewall issue, bad IP address, and so on
   - **Error**: All the SMS connections are experiencing a connection issue

   ✱ **Note:**

   - If the System Monitor does not show an SMS processor, then check if an SMS processor is configured and enabled.
   - When multiple SMS processors are defined, ensure that the connection under test is assigned to the expected processor. You can view a list of the SMS processors and associated SMPP connections in the primary EPM web page at Home >Multi-Media Configuration > SMS. Ensure to check the log file, which is mentioned in the following step, on the correct processor.

3. If the SMS processor is in **Running** state, proceed to the next step. Else, check the error log in **EPM Log Viewer**, from: **EPM Home** > **System Maintenance** > **Log Viewer**.
4. Check if the SMS processor received a request to submit a message to the provider.

   a. From the EPM menu, select **Home** > **Multi-Media Configuration** > **SMS** > **SMS Settings** to view the SMS settings.

   b. Ensure that the SMS trace levels are set to **finer** or **finest**.

   c. Search for the word **sendSMS** in `/opt/Avaya/ExperiencePortal/VPMS/logs/avaya.sms.log`. For example:

   @2013-10-03 09:45:39,034||FINE|avaya.smsbrowser.SMSBrowser|VoicePortal|TP-Processor35| SMSBrowser:sendSms [from,to]=14085551212,14085551313|####

   d. If the message was sent using the Application Interface web service, search for the word **SmsService.sendSms** in `avaya.sms.log`. For example:

   @2013-10-03 09:45:39,034||FINER|sms.service.SmsService|VoicePortal|TP-Processor35|SmsService.sendSms [requestId: AuxiliaryEPM-1380818739033-60;

app: 4:PlayGame559; from: 14085551212; to: 14085551313; sessionId: 123; ucid: 10003000581380818739; params: RequestId=AuxiliaryEPM-1380818739033-60;SessionId=123;UCID=10003000581380818739]|####

5. If a sendSMS request was not logged, proceed to the next step. If a sendSMS request was logged, the provider must respond within 2 minutes with a status.

   Search for **outboundResponse** in `avaya.sms.log`. For example:

   @2013-10-03 11:02:59,468||FINEST|sms.core.MessageProcessor|VoicePortal|pool-15-thread-1|MessageProcessor.outboundResponse: Response [1244]: requestId = PrimaryEPM-1380823379438-2; messageId = 4; status = 0; success = true|####

   **Note:**

   Any non-zero status value indicates a problem. Contact your SMSC provider for the meaning of their status code. You can also view this status value by running a **Contact Detail** report on the EPM and selecting the **Message Status** column. A status of -1 indicates that no response was received from the provider within 2 minutes. Contact your SMSC provider for such issues.

6. Check if the Application Interface Web service received a request to submit an SMS.

   a. View the activity and error log from `/opt/Avaya/ExperiencePortal/VPMS/logs/avaya.appintfservice.log`.

   b. Ensure that the sending application is correctly configured to call the Web service.

      For more information about Application Interface Web service, see *Administering Avaya Experience Portal*.

# The application is not receiving inbound emails

## Proposed Solution

### Procedure

1. From the **EPM** menu, select **Real-Time Monitoring** > **System Monitor**.
2. Check if the email processor is in **Running** state.

   The **System Monitor** might show any of the following statuses for the email processor:

   - **Need Configuration**: Email processor is not configured and enabled
   - **Need Connection**: Email connection is not configured and enabled
   - **Running**: The email processor is connected to all email connections
   - **Degraded**: Some of the email connections are experiencing a connection issue. For example: Invalid credential, Firewall issue, bad IP address, and so on

- **Error**: All the email connections are experiencing a connection issue

**Note:**

- If the System Monitor does not show an email processor, then check if an email processor is configured and enabled
- When multiple email processors are defined, ensure that the connection under test is assigned to the expected processor. You can view a list of the email processors and associated SMPP connections in the primary EPM web page at Home >Multi-Media Configuration > Email. Ensure to check the log file, which is mentioned in the following step, on the correct processor.

3. If the email processor is in **Running** state, proceed to the next step. Else, check the error log in **EPM Log Viewer**, from: **EPM Home** > **System Maintenance** > **Log Viewer**.
4. Check if the email processor is receiving any message from the provider.

    a. View the email settings at **Home** > **Multi-Media Configuration** > **Email** > **Email Settings**.

    b. Ensure that the email trace levels are set to **finer** or **finest**. Search for the word **InboundData** at `/opt/Avaya/ExperiencePortal/VPMS/logs/avaya.email.log`. For example:

    ```
    @2013-10-02 10:14:12,096||FINER|email.core.Reporter|VoicePortal|pool-6-thread-1|
    Reporter: RecordId [206]: InboundData [206]: requestId =
    PrimaryEPM-1380734051778-1; ucid [10000000011380734051]; messageId =
    <082E8CFEC2081640832D69FC17C493F542C45D7F@AZ-
    US1EXMB05.global.avaya.com>|####
    ```

5. If the email processor is receiving message from the provider, proceed to the next step. Else, run the reports from your SMSC.

    If the messages are arriving intermittently, you might have another connection from another EP system that is taking the message.

6. Check, which application the message was routed to.

    Search for the word **Selected** in `avaya.email.log`. For example:

    ```
    2013-10-02 10:14:16,742||FINER|avaya.emailbrowser.InboundMessageProcessor|
    VoicePortal|pool-2-thread-20|Selected app: 0:ColorEmail for
    TextMessage[Id=EML-206;user1@domain.com-
    >epm@domain.com;type=normal;providerId=206;status=0]|####
    ```

7. If the application name is correct and the application is enabled in EPM, proceed to the next step. Else, check your application configuration on the EPM, at **Home** > **System Configuration** > **Applications** > **Change Application**.

    Check the selected application, as it might have similar launch parameters.

8. Check if the `trace.log` file on the application server indicates that the Orchestration Designer application was started.

    a. Set the value of **Application Traces** to **Yes**.

    You can view the **Application Traces** field under the **Reporting Parameters** section for application configuration on the EPM, from **Home** > **System Configuration** > **Applications** > **Change Application**.

    b. Depending on the value of the `trace.log` file, do the following:

| OD application started? | Resolution |
|---|---|
| **Yes** | You might have an application related problem. Add additional trace statements to the application to debug further. |
| **No** | Check the application URL in the application configuration section of the EPM. Click the **Verify** button next to the URL to ensure that the application URL is accessible from the EPM. Verify that the correct proxy server and port, if required, is configured at **Home** > **Multi-Media Configuration** > **Email** > **Browser Settings**. |

# Outbound email not received on the cell phone

## Proposed Solution

### Procedure

1. From the **EPM** menu, select **Real-Time Monitoring** > **System Monitor**.
2. Check if the email processor is in **Running** state.

    The **System Monitor** might show any of the following statuses for the email processor:

    - **Need Configuration**: Email processor is not configured and enabled
    - **Need Connection**: Email connection is not configured and enabled
    - **Running**: The email processor is connected to all email connections
    - **Degraded**: Some of the email connections are experiencing a connection issue. For example: Invalid credential, Firewall issue, bad IP address, and so on
    - **Error**: All the email connections are experiencing a connection issue

    **Note:**

    - If the System Monitor does not show an email processor, then check if an email processor is configured and enabled

- When multiple email processors are defined, ensure that the connection under test is assigned to the expected processor. You can view a list of the email processors and associated SMPP connections in the primary EPM web page at Home >Multi-Media Configuration > Email. Ensure to check the log file, which is mentioned in the following step, on the correct processor.

3. If the email processor is in **Running** state, proceed to the next step. Else, check the error log in **EPM Log Viewer**, from: **EPM Home** > **System Maintenance** > **Log Viewer**.
4. Check if the email processor received a request to submit a message to the provider.
    a. To view the email settings, select **Home** > **Multi-Media Configuration** > **Email** > **Email Settings**

    b. Ensure that all email trace levels are set to **finer** or **finest**.

    c. Search for the word **sendEmail** in `/opt/Avaya/ExperiencePortal/VPMS/logs/avaya.email.log`. For example:

    ```
    @2013-10-02 10:14:17,838||FINER|avaya.emailbrowser.EmailBrowser|VoicePortal|
    pool-2-thread-20| EmailBrowser:sendEmail
    ret=sessionid=123;ucid=10000000021380734057;requestid=PrimaryEPM-138073405
    7787-2|####
    ```

    d. If the message was sent using the Application Interface web service, search for the word **EmailService.sendEmail** in `avaya.email.log`. For example:

    ```
    @2013-10-02 10:14:17,787||FINER|email.service.EmailService|VoicePortal|pool-2-
    thread-20|EmailService.sendEmail [requestId: PrimaryEPM-1380734057787-2; app:
    0:ColorEmail; from: epm@domain.com; to: user1@domain.com; ; ucid:
    10000000021380734057]|####
    ```
5. If a sendEmail request was not logged, proceed to the next step. If a sendEmail request was logged, your email server might generate an undeliverable notification, DSN, within a minute or two.
    a. Use an email client to examine the inbox of the sending mailbox and read the contents of the DSN email. Alternatively, run the **Contact Detail** report on the EPM.

    b. Select the **Message Status** column and select a **Media Type** filter of **Email DSN**.

    The **Message Status** column might contain any one of the following codes:

    - **0**: The message was successfully delivered to the specified recipient address. It does not indicate if the message was read. This is a terminal state and does not provide further DSN for this recipient.
    - **1**: The message could not be delivered to the recipient. The reporting MTA has abandoned any attempts to deliver the message to this recipient. No further notifications.
    - **2**: The message has been relayed or sent through a gateway into an environment that does not accept responsibility for generating DSNs for successful delivery.
    - **3**: The reporting MTA is unable to deliver or relay the message. However, the MTA will continue to attempt to deliver the message. Additional notification messages

may be issued as the message is further delayed or successfully delivered, or if delivery attempts are later abandoned.

- **4**: Unknown error. The details may be in the DSN message.

6. Check if the Application Interface Web service received a request to submit an email. You can view the activity and error log from `/opt/Avaya/ExperiencePortal/VPMS/logs/avaya.appintfservice.log`.
7. Ensure that the sending application is correctly configured to call the Web service.

   For more information about Application Interface Web service, see *Administering Avaya Experience Portal*.

# Cannot view the report output from the email link

If you click the link in an email, which is sent by EPM as the result of a scheduled report, you might see either a blank page or **`The requested file is no longer available`** message.

The issue occurs when the scheduled report name contains multi-byte characters and the browser that you use is Internet Explorer 6.0.

To work around this issue, do any one of the following:

- Change the name of the scheduled report in Experience Portal so that the name does not contain multi-byte characters.
- Upgrade the browser to Internet Explorer 8.0 or later.

# Purging conversations from the conversation repository database

## About this task

Use the PurgeConversationsLocalDB script to:

- Delete all the conversations stored in the conversation repository.
- Delete the conversations stored in the conversation repository for a specific application.
- Optimize disk space usage on the database tables used by the conversation repository.

## Procedure

1. Log in to Linux on the EPM server which is hosting the conversation repository that requires purging or optimization.

   If you are an Avaya Services representative, and use Avaya Enterprise Linux, the Avaya Service accounts will not be available after the Avaya Enterprise Linux upgrade. The

Avaya Service accounts will be available through EASG configuration during the Experience Portal upgrade.

- Log on to the local Linux console as root.
- Or log on remotely as a non-root user and then change the user to root by entering the `su - root` command.

2. Navigate to the `Support/VP-Tools` directory in the Experience Portal installation directory.
3. Enter the `cd $AVAYA_HOME/Support/Security-Tools` command. $AVAYA_HOME is an environmental variable pointing to the name of the installation directory specified during the Experience Portal software installation.

   The default value is `/opt/Avaya/ExperiencePortal`.
4. Enter the `bash PurgeConversationsLocalDB` command followed by one of the following parameters:
   - -p to purge all conversations in the repository.
   - -a application-name to purge all conversations for the specified application name.
   - –v to perform a **`vacuum full`** command to recover or reuse disk space occupied by the updated or deleted rows. This option is not required if you have used the -p option.

   The system might take some time to execute the script depending on the number of conversations in the repository tables. If the script runs successfully, it returns a message stating that the operation completed without any errors. Otherwise, the script returns a message stating the errors.

# High number of failures or unknown status for outbound emails

When sending out emails, EPM expects the email to be processed in 15 minutes. If the email processing takes longer than 15 minutes, then the emails are marked as completed with status set to failures/unknown status.

One scenario that results in this situation is when an application sends out a number of email messages with notifications and delivery receipts turned on, attachments of size 1 MB or greater, without pacing the requests. The email server and/or the application server can become a bottle neck in this scenario resulting in longer times for processing each mail.

## Proposed Solution 1

### Procedure

Pace out the requests instead of sending the requests as soon as possible.

## Proposed Solution 2

### Procedure

Increase the value specified for the browser.db.purge.interval property in the `$MMSSERVER_HOME/lib/config/emailserver.properties` file on each of the EPMs.

The default value for this property is 15 (minutes). The valid range is from 15 through 60 (minutes). The value to be specified depends upon the size of the attachment and the performance of the email server and the application server. Once the value is updated, the EPM server needs to be restarted from the EPM manager.

**Note:**

Increasing the value for browser.db.purge.interval property will provide better results for failures/unknown status but might result in lower performance.

# Runtime error in the online help search functionality

If you encounter a run-time error while using the search functionality in the online help, the debug option might be enabled.

## Proposed Solution

### Procedure

1. In Internet Explorer, select **Tools** > **Internet Options**.
2. In the **Internet Options** dialog box, select the **Advanced** tab.
3. In the **Browsing** group:
   a. Select the **Disable script debugging (Internet Explorer)** check box.
   b. Clear the selection of the **Display a notification about every script error** check box.
4. Click **OK**.
5. Restart Internet Explorer.

# Web site security certificate error when accessing Experience Portal URL

If you encounter an error while accessing the URL to the Experience Portal server, the security certificates might not be added as Trusted Sites.

## Proposed Solution

### Procedure

1. In Internet Explorer, enter the URL for the Experience Portal server.

   An error message regarding the Web site's security certificate appears on the web page.
2. Click **Continue to this website (not recommended)** link on the error page.
3. Click the **Certificate Error** in the toolbar.

   **Note:**

   The **Certificate Error** appears on the tool bar next to the URL that you have entered.
4. Click **View certificates** on the **Untrusted Certificate** page.
5. Click **Install Certificate** in the **Certificate** dialog box.
6. In the **Certificate Import Wizard**:
   1. Click **Next**.
   2. Select **Automatically select the certificate store based on the type of certificate** option.
   3. Click **Next**.
   4. Click **Finish**.
   5. Click **Yes** on the **Security Warning** message.
7. Click **OK** to close the **Certificate Import Wizard**.
8. Click **OK** to close the **Certificate** dialog box.
9. Restart Internet Explorer and enter the URL for the Experience Portal server.

# Incorrect search results in the Help

While searching for a topic in the **Search** tab of the help file, sometimes the search result displays fewer topics. This problem might occur because of the existing browsing history of your Internet Explorer Web browser.

## Proposed Solution

### Procedure

1. Open Internet Explorer.
2. Select **Tools** > **Internet Options**.

The system displays the Internet Options window.

3. In the **Browsing history** area, click **Delete**.
4. Click Delete Browsing History.
5. Select the fields that you want to delete.
6. Click **Delete**.
7. Restart Internet Explorer.

# File cannot be found error when exporting a Report

This error occurs only if you are using Internet Explorer.

When exporting a report, if you select the **Open** option in the **File Download** dialog box and `This file cannot be found` error is displayed, it could be due to a setting in Internet Explorer.

## Proposed Solution

### Procedure

1. In Internet Explorer, select **Tools** > **Internet Options**.
2. In the **Internet Options** dialog box, select the **Advanced** tab.
3. In the **Security** group, clear the selection of the **Do not save encrypted pages to disk** check box.
4. Click **OK**.
5. Restart Internet Explorer.

# Long TTS prompt does not play when Nuance is configured to MRCP V2 (TLS)

There is a known issue with initializing the TTS resource for a long TTS prompt when you configure Nuance server with MRCP V2 (TLS).

## Proposed Solution

To resolve this, perform one of the following actions:

- Set the TTS parameter that is, **Prosody Volume** or **Prosody Rate** on the Change Application page, to an audible volume range that is greater than zero and less than 100.

  **Note:**

  You must set the **Prosody Volume** and **Prosody Rate** values to 50.
- Initialize short prompt first.

Setting the **Prosody Volume** and **Prosody Rate** values to 50 ensures that:

- The TTS resource is properly initialized for the request.
- All prompts from different speech server with different default volume settings, that include prerecord prompts, are played at the same volume.

# TTS servers have different volume for the same pre-recorded prompts

Since the default volume settings in different speech servers are different, the volume of a pre-recorded prompt may vary for each TTS server.

To make this volume consistent, you can configure the TTS prosody volume from the Add Application or Change application page in EPM.

## Proposed Solution

To resolve this, perform one of the following actions:

- Set the TTS parameter that is, **Prosody Volume** or **Prosody Rate** on the Change Application page, to an audible volume range that is greater than zero and less than 100.

  **Note:**

  You must set the **Prosody Volume** and **Prosody Rate** values to 50.
- Initialize short prompt first.

Setting the **Prosody Volume** and **Prosody Rate** values to 50 ensures that:

- The TTS resource is properly initialized for the request.
- All prompts from different speech server with different default volume settings, that include prerecord prompts, are played at the same volume.

# Network interfaces move

When you install Red Hat Enterprise Linux Server 6 on a server that previously had Red Hat Enterprise Linux 5 installed on it, you might find that logical network interfaces eth0, eth1, and so on. have moved to different physical network ports on the server. For example, the port that was interface eth0 on Red Hat Enterprise Linux 5 might become interface eth2 on Red Hat Enterprise Linux Server 6, while the port that was interface eth2 on Red Hat Enterprise Linux 5 might become logical network interface eth0 on Red Hat Enterprise Linux Server 6. Similarly, the ports associated with network interfaces eth1 and eth3 might be reversed after you upgrade Linux. In such a scenario, you either need to move network cables that are plugged into the server to match the Linux network configuration, or change the Linux network configuration.

# Privacy Manager role

Users require the Privacy Manager role to change the values in the **Privacy Settings** page of EPM and the values related to session transcription data in the **Change Application** page.

Before the Experience Portal 6.0 release, users with the Administration role could perform the tasks that now require the Privacy Manager role. You must assign the Privacy Manager role to users with the Administration role so that users can perform the tasks that require the Privacy Manager role.

# Package mod_dnssd

Depending on the options you select during the Red Hat Enterprise Linux Server installation, the package mod_dnssd might get installed. There is a compatibility issue between Experience Portal and mod_dnssd. Therefore, do not install mod_dnssd.

If the package mod_dnssd is installed when Experience Portal is installed, the Experience Portal installer automatically disables the incompatible entry in the mod_dnssd configuration file and displays the following warning message:

```
Possible Error during operation: Install/Configure Apache for VPMS
- Start error description -
Notice: Incompatible DNSSDEnable entry found in
/etc/httpd/conf.d/mod_dnssd.conf. Automatically disabling this entry. Please
see Experience Portal documentation for more details. This notice is not an error.
```

You can ignore the warning message.

# External system issues

## Avaya Aura® Session Manager

### Install Experience Portal certificate

In order for Experience Portal to establish a TLS connection to a Session Manager server, you must install the security certificate from Experience Portal on Session Manager.

If your Session Manager is version 6.x, refer to your Session Manager product documentation for instructions on how to install a security certificate on Session Manager. The relevant information can be found in the document *Administering Avaya Aura® Session Manager* in *Chapter 3: Managing Security*.

### Session Manager Certificate URL

In order for Experience Portal to establish a TLS connection to a Session Manager server, you must install the security certificate from Session Manager on Experience Portal. The correct URL to obtain the security certificate from Session Manager is `https://<Session_Manager_SM-100>:5061`.

## Loquendo speech servers

### MRCPv2 not supported

Experience Portal communicates with speech servers using either Media Resource Control Protocol version one (MRCPv1) or Media Resource Control Protocol version two (MRCPv2). You must configure Experience Portal to use MRCPv1 when communicating with Loquendo speech servers.

### System port limit

Experience Portal systems that use Loquendo speech servers are limited to a maximum of 100 ASR ports and 100 TTS ports.

**Note:**

Refer to the appropriate interoperability guide that came with your Loquendo software for instructions on configuring your Loquendo speech servers and configuring Experience Portal to work with them.

# Application logging

If you run Orchestration Designer applications on Experience Portal, ensure that the applications use Dialog Designer version 5.1 SP3 or later. Application logging fails when you use Dialog Designer runtime versions earlier than 5.1 SP3 with Experience Portal.

If you run a Dialog Designer or Orchestration Designer application that does application logging, and the Experience Portal system is configured to handle more than 75 simultaneous calls, you must make the following configuration change on the Primary EPM:

1. Log in to Linux on the Primary EPM server as a user with root privileges.
2. Open the file `$CATALINA_HOME/conf/server.xml` in a text editor.
3. Find the entry **maxThreads="500"** in `<Connector port="3009"`.
4. Change the value from 500 to 1000.
5. Save and close the file.
6. Run the **`/sbin/service vpms restart`** command to restart the vpms service.

# Prompt (with barge-in enabled) times out before playing completely

If the default value of session timeout (60 sec) is shorter than the prompt, and barge-in is enabled in the application, the recognition event reaches timeout before the prompt is played completely.

## Proposed Solution

### About this task

**Note:**

This modification is required only if the customized application has a long play prompt with barge-in enabled, that exceeds the recognition session timeout.

To prevent timeout before the long prompt play is complete:

### Procedure

1. Log in to the NSS speech server.
2. Navigate to the `$NSSSVRSDK` directory.

   The environment variable`$NSSSVRSDK` points to

   `/usr/local/Nuance/SpeechServer_5/server/config` (for NSS )

   Or

   `/usr/local/Nuance/Speech_Server/server/config` (for NSS). For more information on speech server versions, see *Avaya Experience Portal Overview and Specification*.
3. In an ASCII editor, open the `NSSserver.cfg` file.
4. Modify the following parameters:

   server.mrcp2.sip.sessionTimeout VXIInteger 120000 server.mrcp1.rtsp.sessionTimeout VXIInteger 120000

**Note:**

The timeout value should be greater than the prompt play length.

5. Save and close the file.
6. Restart the NSS speech server.

# Application logging on the Linux application server

If the Orchestration Designer application performs application logging and the Primary EPM is out of service, Orchestration Designer temporarily stores the application log data on the application server. Orchestration Designer stores the application log data until the Primary EPM is back in service.

If the application server is a Tomcat server installed on Linux and the Primary EPM is out of service for a long time, Tomcat might crash because the system runs out of file handles.

## Proposed Solution

### Procedure

1. Log in to Linux on the Tomcat server as a user with root privileges.
2. Open the file `/etc/init.d/tomcat` in a text editor.
3. Find the **start()** procedure.
4. Add the line `ulimit -n 8192` to the start procedure.
5. Save and close the file.
6. Run the **`/sbin/service tomcat restart`** command to restart the Tomcat service.
7. Change the Tomcat startup options to improve garbage collection on the application server:
    a. Log in to Linux on the Tomcat server as a user with root privileges.
    b. Open the file `/etc/init.d/tomcat` in a text editor.
    c. Find the line that begins with **export JAVA_OPTS=**.
    d. Change the line to read as follows:`export JAVA_OPTS="-server -Xmx1024m -XX:MaxNewSize=30m -X:+UseParNewGC -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=60-XX:ThreadStackSize=512"`.

    **Important:**

    Enter the text in a single line.

e. Save and close the file.
f. Run the `/sbin/service tomcat restart` command to restart the Tomcat service.

# Supporting non-English applications

### Application language

When an application runs on the MPP, the VoiceXML Interpreter defaults to the language configured in the **Language** field on the **EPM** > **Browser Settings** page. The default value for the field is English (USA) en-US. If the application uses a language other than English, the application must specify the correct language using the xml:lang attribute. Applications can specify the language either globally on each page or as part of each individual <grammar> tag and <prompt> tag.

### Default event handlers

When the VoiceXML interpreter or CCXML interpreter generates an event to a page that does not have a handler defined for the event, the interpreter invokes the default event handler configured on the Event Handlers page of the EPM. The default event handlers, which Experience Portal provides, play an error prompt spoken in English. If an application uses a language other than English, you must configure the appropriate default event handler for the application.

**Note:**

If you write a code that is used as a default event handler and the code refers to prerecorded prompt files, refer to the prompt files by file name. Experience Portal searches for prompt files in the appropriate directory.

# Application error PSESM00070

When you change the configuration for an Experience Portal application to use an ASR or TTS language, and if that language is recently added to the server, the application might display the `PSESM00070` event.

## Proposed Solution

### About this task

You might need to restart the MPP server to resolve this issue. Use the following procedure to restart the MPP server that you are using.

### Procedure

1. Log in to the EPM Web interface with an account that has *Administrator* or *Operations* privilege.
2. From the EPM main menu, select **System Management** > **MPP Manager**.
3. On the **MPP Manager** page, select the server that you want to restart.
4. In the **State Commands** area, click **Restart**.

   Avaya Experience Portal restarts the selected MPP server when the last active call completes or the grace period expires, whichever is earlier.
5. Click **Refresh** to verify that the **State** of the MPP server that you restart is displayed as **Running**.

# Making outcall using SIP

On an Experience Portal system that has both H.323 and SIP configured, when a CCXML application makes a <createcall> request, the MPP looks for an available H.323 port to place the call on before looking for an available SIP port. Experience Portal provides the ability for CCXML applications to request the MPP to look for an available SIP port first. The application can send the suggest_sip hint on the <createcall> request.

An example of the CCXML code that demonstrates how to make an outcall using SIP:

```
<var name="suggest_sip" expr="true"/>
<script>var hints= new Object(); hints.suggest_sip = suggest_sip; </script>
<createcall dest="'14085551234'" hints="hints"/>
```

# Cannot access remote database

Recent versions of Java include code to handle cipher block chaining (CBC) attacks. This security enhancement might prevent Avaya Experience Portal from connecting to a Microsoft SQL Server 2008 external database. To work around this issue you must disable CBC protection in Java.

## Proposed Solution

### About this task

Perform the following procedure on the Primary EPM server and each Auxiliary EPM server.

### Procedure

1. Log in to Linux on the EPM server as a user with root privileges.

2. Open the file /etc/profile.d/epm.sh in a text editor.
3. Locate the line that begins with export JAVA_OPTS_EPM.
4. Change this line to include the text `-Djsse.enableCBCProtection=false`.

   ❗ **Important:**

   Ensure that you enter the text in a single line.

   For example:

   ```
   JAVA_OPTS_EPM="-server -XX:MaxNewSize=256m -Xmx1024M -
   XX:+UseConcMarkSweepGC -XX:+UseParNewGC -XX:ThreadStackSize=1024 -
   Ddss.port=31050
   -XX:PermSize=256m -XX:MaxPermSize=256m -
   XX:+HeapDumpOnOutOfMemoryError -XX:GCTimeRatio=19 -
   XX:CMSInitiatingOccupancyFraction=60
   -Dcom.sun.management.jmxremote -XX:SurvivorRatio=8 -
   XX:TargetSurvivorRatio=90 -XX:MaxTenuringThreshold=0 -
   XX:+UseCMSCompactAtFullCollection
   -XX:CMSFullGCsBeforeCompaction=1 -
   Dsun.lang.ClassLoader.allowArraySyntax=true -XX:-DoEscapeAnalysis -
   Djsse.enableCBCProtection=false"
   ```
5. Save and close the file.
6. Restart the server.

## Remote DTMF detection

If you use Nuance speech servers and you have applications with the Advanced Parameter **Support Remote DTMF Processing** set to **Yes**, then the Nuance speech servers must all run NSS 5.0.4 or later.

For more information on speech server versions, see *Avaya Experience Portal Overview and Specification*.

This is to prevent <noinput> VoiceXML exceptions from occurring for remote DTMF detection.

## Recognition timeout while playing a long prompt

If an application plays a long prompt with barge-in enabled, the Nuance speech server might return a recognition timeout event before the prompt has completed playing.

To resolve the problem, increase the session timeout parameter on the Nuance speech server to be longer than your longest application prompt.

## Proposed Solution

### Procedure

1. For a Nuance Speech Server running on Linux:
    a. On the Nuance server, open the file `$NSSSVRSDK/config/NSSserver.cfg` in a text editor.
    b. Locate the line that reads as follows:

       server.mrcp2.sip.sessionTimeout VXIInteger XXXXXX

       ✱ **Note:**

       The XXXXXX value is the session timeout in milliseconds. For example, for a two minute timeout, XXXXXX value is 120000.
    c. Increase the timeout value in the line.
    d. Locate the line that reads as follows:

       server.mrcp1.rtsp.sessionTimeout VXIInteger XXXXXX

       ✱ **Note:**

       The XXXXXX value is the session timeout in milliseconds. For example, for a two minute timeout, XXXXXX value is 120000.
    e. Increase the timeout value in the line.
    f. Save and close the file.
    g. Restart the Nuance server.
2. For a Nuance Speech Server running on Windows:
    a. On the Nuance server, open the file `%NSSSVRSDK%\config\NSSserver.cfg` in a text editor.
    b. Locate the line that reads as follows:

       server.mrcp2.sip.sessionTimeout VXIInteger XXXXXX

       ✱ **Note:**

       The XXXXXX value is the session timeout in milliseconds. For example, for a two minute timeout, XXXXXX value is 120000.
    c. Increase the timeout value in the line.
    d. Locate the line that reads as follows:

       server.mrcp1.rtsp.sessionTimeout VXIInteger XXXXXX

**Note:**

The XXXXXX value is the session timeout in milliseconds. For example, for a two minute timeout, XXXXXX value is 120000.

e. Increase the timeout value in the line.

f. Save and close the file.

g. Restart the Nuance server.

# Getting recognition results on nomatch event

If you use Nuance speech servers with the default configuration, and when the application receives a <nomatch> event in response to a recognition request, the application variable *application.lastresult$* is not updated with recognition results.

For the application to receive recognition results when a nomatch event is generated, the Nuance speech servers must use NSS or NRec . Additionally, you must perform the following procedure on each Nuance speech server.

For more information on speech server versions, see *Avaya Experience Portal Overview and Specification*.

## Proposed Solution

### Procedure

1. For a Nuance Speech Server running on Linux:

   a. On the Nuance server, open the file `$NSSSVRSDK/config/NSSserver.cfg` in a text editor.

   b. Locate the line that reads as follows:

   ```
   server.mrcp2.osrspeechrecog.mrcpdefaults.VSP.server.osrspeechrecog.result.sendnomatch
   ```

   c. Change the line to read as follows:

   ```
   server.mrcp2.osrspeechrecog.mrcpdefaults.VSP.server.osrspeechrecog.result.sendnomatch VXIString true
   ```

   **Note:**

   Ensure that you enter the text in a single line.

   Remove the # character at the beginning of the line, if it is present, to uncomment it.

   d. Locate the line that reads as follows:

   server.mrcp1.osrspeechrecog.result.sendnomatch

e. Change the line to read as follows:

```
server.mrcp1.osrspeechrecog.result.sendnomatch VXIString true
```

**Note:**

Ensure that you enter the text in a single line.

Remove the # character at the beginning of the line, if it is present, to uncomment it.

f. Save and close the file.

g. Open the file `$SWISRSDK/config/Baseline.xml` in a text editor.

h. If you use NRec 9.0.11 or 9.0.12, find the series of lines beginning with the following:

```
<param name="swisr_result_enable_speech_mode">
```

i. Change the series of lines to read as follows:

```
<param name="swisr_result_enable_speech_mode">
    <value>1</value>
</param>
```

j. Save and close the file.

k. If you use NRec 9.0.13 or later, find the series of lines beginning with the following:

```
<param name="swirec_result_enable_speech_mode">
```

l. Change the series of lines to read as follows:

```
<param name="swirec_result_enable_speech_mode">
    <value>1</value>
</param>
```

m. Save and close the file.

n. Restart the Nuance server.

For more information on speech server versions, see *Avaya Experience Portal Overview and Specification*.

2. For a Nuance Speech Server running on Windows:

a. On the Nuance server, open the file `%NSSSVRSDK%\config\NSSserver.cfg` in a text editor.

b. Locate the line that reads as follows:

```
server.mrcp2.osrspeechrecog.mrcpdefaults.VSP.server.osrspeechrecog.result.sen
dnomatch
```

c. Change the line to read as follows:

```
server.mrcp2.osrspeechrecog.mrcpdefaults.VSP.server.osrspeechrecog.result.sen
dnomatch VXIString true
```

**Note:**

Ensure that you enter the text in a single line.

Remove the # character at the beginning of the line, if it is present, to uncomment it.

d. Locate the line that reads as follows:

server.mrcp1.osrspeechrecog.result.sendnomatch

e. Change the line to read as follows:

```
server.mrcp1.osrspeechrecog.result.sendnomatch VXIString true
```

**Note:**

Ensure that you enter the text in a single line.

Remove the # character at the beginning of the line, if it is present, to uncomment it.

f. Save and close the file.

g. Open the file `%SWISRSDK%\config\Baseline.xml` in a text editor.

h. If you use NRec 9.0.11 or 9.0.12, find the series of lines beginning with the following:

```
<param name="swisr_result_enable_speech_mode">
```

i. Change the series of lines to read as follows:

```
<param name="swisr_result_enable_speech_mode">
    <value>1</value>
</param>
```

j. Save and close the file.

k. If you use NRec 9.0.13 or later, find the series of lines beginning with the following:

```
<param name="swirec_result_enable_speech_mode">
```

l. Change the series of lines to read as follows:

```
<param name="swirec_result_enable_speech_mode">
    <value>1</value>
</param>
```

m. Save and close the file.

n. Restart the Nuance server.

For more information on speech server versions, see *Avaya Experience Portal Overview and Specification*.

# Property inputmodes

A VoiceXML application can use the property inputmodes to control whether the speech server recognizes speech input, DTMF input, or both. However, Nuance speech servers do not support the property inputmodes with MRCP V1 connection.

To use inputmodes with a Nuance speech server you must configure Experience Portal to communicate with the speech server using MRCP V2.

# Stability issues with MRCPv2

Experience Portal uses either MRCPv1 or MRCPv2 to communicate with speech servers. When Experience Portal uses MRCPv2 to communicate with Loquendo Speech servers, you might face issues such as failure to acquire speech resources, and long latencies. To avoid the issues, configure Experience Portal to use MRCPv1 when Experience Portal communicates with Loquendo speech servers.

# Speech Server using MRCPv2: First call fails but second call succeeds when Nuance is configured to use hostname

If the configuration for an Experience Portal speech server is set to use MRCPv2 (TLS or TCP) and the Engine Type is Nuance, then the MPP might not be able to resolve the hostname sent in the contact tag from the **SIP 200 OK** that speech server sends back.

## Proposed Solution 1: Set “useHostIPAddress” to 1

### Procedure

1. On each Nuance server machine, log in to the operating system and navigate to the directory in which Nuance NSSserver.cfg is stored.
2. Open the NSSserver.cfg file in an ASCII editor.
3. Modify the value for the parameter useHostIPAddress to set the value to `1`.
4. Save and close the file.
5. Restart the Nuance server.
6. Repeat this procedure for any other Nuance ASR servers in the Experience Portal system.

## Proposed Solution 2: Add speech server hostname to local hosts file on all MPPs

### Procedure

1. Log on to Linux on the Experience Portal server with root privileges.
2. Take a back up of the original file prior to editing the file by entering the **`cp /etc/hosts /etc/hosts.bak`** command.
3. Open the /etc/hosts file in an ASCII text editor of your choice.

4. Create a new line for each speech server in the Experience Portal system using the format `IP_address hostname1 hostname2...` where:
    - IP_address is the IP address of a server in the Experience Portal system.
    - hostname1 hostname2... is one or more hostnames, separated by tabs or spaces, to associate with the IP address.
5. Save and close the file.
6. Repeat this procedure for each MPP in your Experience Portal system.

# Chinese TTS using Nuance Speech Server

In order to generate either Traditional Chinese or Simplified Chinese TTS using Nuance RealSpeak voice Mei-Ling with Nuance Speech Server (NSS) , you must configure NSS correctly.

For more information on speech server versions, see *Avaya Experience Portal Overview and Specification*.

## Proposed Solution

### Procedure

1. For a Nuance Speech Server running on Linux:
    a. On the Nuance server, open the file `$NSSSVRSDK/config/NSSserver.cfg` in a text editor.

    b. Locate the following series of lines:

    ```
    server.rsspeechsynth.languageid.zh VXIString Mandarin Chinese
    server.rsspeechsynth.languageid.zh-CN VXIString Mandarin Chinese
    server.rsspeechsynth.languageid.zh-guoyu VXIString Mandarin Chinese
    ```

    c. Change the series of lines to read as follows:

    ```
    server.rsspeechsynth.languageid.zh VXIString Mandarin Chinese
    server.rsspeechsynth.languageid.zh-CN VXIString Mandarin Chinese GB
    server.rsspeechsynth.languageid.zh-guoyu VXIString Mandarin Chinese B5
    ```

    d. Save and close the file.

    e. Restart the Nuance server.
2. For a Nuance Speech Server running on Windows:
    a. On the Nuance server, open the registry editor.

    b. Create or edit registry keys to match the following values:

    ```
    [HKEY_LOCAL_MACHINE\SOFTWARE\ScanSoft\RealSpeak 4.0\Language Resources
    \Mandarin Chinese B5 (Mei-Ling)]
    "Gender"="female"
    "LanguageName"="Mandarin Chinese B5"
    "LanguageTag"="zh-guoyu-b5"
    ```

```
"VoiceName"="Mei-Ling"
[HKEY_LOCAL_MACHINE\SOFTWARE\ScanSoft\RealSpeak 4.0\Language Resources
\Mandarin Chinese GB (Mei-Ling)]
"Gender"="female"
"LanguageName"="Mandarin Chinese GB"
"LanguageTag"="zh-guoyu-gb"
"VoiceName"="Mei-Ling"
```

c. Close the registry editor.

d. Open the file `%NSSSVRSDK%\config\NSSserver.cfg` in a text editor.

e. Locate the following series of lines:

```
server.rsspeechsynth.languageid.zh VXIString Mandarin Chinese
server.rsspeechsynth.languageid.zh-CN VXIString Mandarin Chinese
server.rsspeechsynth.languageid.zh-guoyu VXIString Mandarin Chinese
```

f. Change the series of lines to read as follows:

```
server.rsspeechsynth.languageid.zh VXIString Mandarin Chinese
server.rsspeechsynth.languageid.zh-CN VXIString Mandarin Chinese GB
server.rsspeechsynth.languageid.zh-guoyu VXIString Mandarin Chinese B5
```

g. Save and close the file.

h. Restart the Nuance server.

# Security problem while trying to play utterances

You might see the error "A security problem occurred" in the Windows Media Player while playing an utterance from a Session Detail report. To listen to the utterance, right-click the utterance link and select **Save Target As**. For more information, see http://support.microsoft.com/default.aspx?scid=kb;en-us;885136.

# Cannot view exported file

When you click the Export button on an EPM page, the system displays the File Download dialog box with options to **Open**, **Save**, and **Cancel** the file.

If the Internet Explorer security option **Do not save encrypted pages to disk** is enabled, the **Open** button does not function.

## Solution

### About this task

Use any one of the following steps to resolve the issue.

### Procedure

1. Use the **Save** button and view the file after it is downloaded on the system.
2. Or make the following changes in the Internet Explorer settings:
   a. In Internet Explorer, select **Tools** > **Internet Options**.
   b. On the Internet Options page, select the **Advanced** tab.
   c. On the **Advanced** tab, disable the **Do not save encrypted pages to disk** option, which is located in the **Security** section.

# External database URL

If you use an external Oracle database, and enter a leading space in the **EPM Servers** > **Report Database Settings** > **URL** field, the system did not report an error.

If the URL value in the **Report Database Settings** page contains a leading space,Experience Portal cannot gain access to the external database. Verify that the **URL** field in the **Report Database Settings** page does not contain a leading space.

# System displays incorrect time zone for the default zone

While switching from daylight saving-time to the standard time, or from standard time to daylight-saving time, the system might display the time zone as **US/Pacific-New** for the default zone, irrespective of the time zone that you configure in the system.

## Proposed Solution 1: Changing the localtime information

### Procedure

1. Select your country, from `/usr/share/zoneinfo`.

   ✱ **Note:**

   Depending on the distribution of the system, the location of `zoneinfo` might vary.
2. Use the command `$ ln -sf /usr/share/zoneinfo/your time zone /etc/localtime` to link *localtime* to your city or to any city in your time zone, where *your time zone* is the time zone you want to configure. For example, US/Pacific.

## Proposed Solution 2: Setting the TZ environment variable

### Procedure

1. In the `/etc/profile.d` directory, create a shell script with the command export `TZ= “your time zone”`, where *your time zone* is the time zone you want to configure. For example, US/Pacific.

   **Note:**

   If your system does not support the `/etc/profile.d` directory, add the `export TZ` command to the */etc/profile* initialization script.

2. Restart the *vpms* service by entering the */sbin/service vpms restart* command.

# Chapter 7: Troubleshooting installation and upgrade issues

## Installation log files

The installation log files contain detailed information about the installation process.

Avaya Experience Portal creates several log files during the installation process. The installation process creates the `/opt/Avaya/InstallLogs/aepinstall.log` log file. The PVI checker creates the `/opt/Avaya/InstallLogs/pvichecker.log` log file.

### General installation log files

| Log filename | Description |
|---|---|
| `aepinstall.log` | This is the first log file you should consult if you need to troubleshoot an installation issue.<br>**Note:**<br>This file contains detailed log messages which might appear to be warnings or errors, but can safely be ignored, particularly if those warnings do not appear in the installation summary (ISSummary.log). |
| `SetIAVersion<component>.log` | Version history of the Experience Portal components installed. The <component> can be VPMS, MPP, or Docs. |
| `GetIAVersionVPMS.err.log` | Log file containing any warning messages generated while trying to retrieve version information as part of an upgrade. The presence of a warning in this log file does not necessarily indicate an error. |

### MPP-specific installation log files

| Log filename | Description |
|---|---|
| `av-mpp-<buildnumber>-Install-<date>.log` | `mppinstall.sh` script output. |
| `av-mpp-<buildnumber>-Install-rpm-<date>.log` | Output from the Red Hat Package Manager (RPM) during the MPP software installation. |

### EPM-specific installation log files

| Log filename | Description |
|---|---|
| `vpms.cert.gen.out.log` | Results from the security certificate generation process. |
| `vpms.cert.gen.err.log` | Any internal errors generated from the certificate generation process. |

# Troubleshooting disk partition related issues

On a Primary EPM server, the Experience Portal database might increase to a large size. The report data that is generated by Experience Portal causes the database to increase by approximately 4GB for every one million calls processed. If the applications use the Experience Portal application logging feature, the database grows at a faster rate.

By default, the Experience Portal database is saved in the directory `/var/lib/pgsql/data`. In the software-only offer for Experience Portal, when you install RHEL on the EPM server, ensure that the disk partitions provide adequate space for the Experience Portal database. The default partitioning provided by RHEL is adequate for most Experience Portal installations as the Experience Portal database is in a partition that spans most of the hard disk.

On an MPP server, the MPP logs directory might increase to a large size, especially if the applications use the VoiceXML <log> tag or CCXML <log> tag to generate application log data.

By default, the MPP logs are saved in the directory `/opt/Avaya/ExperiencePortal/MPP/logs`. In the software-only offer for Experience Portal, when you install RHEL on the MPP server, ensure that the disk partitions provide adequate space for the MPP logs. The default partitioning provided by RHEL is adequate for most Experience Portal installations as the MPP logs are in a partition that spans most of the hard disk.

In the partitioning provided by Avaya Enterprise Linux, the MPP logs are saved in a relatively smaller disk partition. If you encounter space related issues, move the MPP logs to a different location. For more information on moving the MPP logs to a different location, see *Administering Avaya Experience Portal*.

# Unable to connect to RHN during Experience Portal installation

If you update your operating system through Red Hat Network (RHN) or similar mechanism prior to installing Experience Portal, you must ensure the following to minimize the prerequisite dependency issues:

- Perform the Experience Portal installation after the operating system update is done so that new updates and potential conflicts will not cause an issue.

- Keep RHN (or equivalent) enabled during the Experience Portalinstallation. Disconnecting RHN prevents the Experience Portal prerequisite installer from automatically downloading package updates and dependencies, and might require manual resolution of RPM conflicts.

# Mounting a DVD on Avaya Linux

When you run the **`mount/mnt/cdrom`** command on Avaya Linux, you may see the `mount: No medium found` error.

This error occurs because the wrong physical device is mapped to the `/mnt/cdrom` mount point in the `/etc/fstab` file.

## Proposed Solution

### Procedure

1. Log in to Linux on the Experience Portal server as a user with root privileges.
2. Run the **`cat/proc/sys/dev/cdrom/info`** command. The system displays the following information table about your DVD device:

```
drive name:         sr0  hda
drive speed:        0    24
drive # of slots:   1    1
Can close tray:     1    1
...
```

3. Find the **drive name** row in the information table above.
4. In the **drive name** row, go to the last column. For example, the column you should be looking for contains the `hda` value .
5. Run the **`ls -l /dev | grep cdrom`** command. It displays the following list of device special files associated with your DVD devices.

```
lrwxrwxrwx 1 sroot root 4 Aug 31 08:11 cdrom -> scd0
lrwxrwxrwx 1 sroot root 3 Aug 16 11:16 cdrom-hda -> hda
lrwxrwxrwx 1 sroot root 4 Aug 31 08:11 cdrom-sr0 -> scd0
```

6. Find the line for the drive name that you found earlier.

   **Note:**

   In the example shown above, you should find the line that ends with `cdrom-hda -> hda`.

7. In the line that ends with `cdrom-hda -> hda`, find the device special file name.

   **Note:**

   In the example shown above, the device special file name is `cdrom-hda`.

8. Open the **`/etc/fstab`** file in a text editor.
9. Find the `/dev/cdrom /mnt/cdrom iso9660 noauto,owner,ro 0 2` line in the text editor.
10. Change **`/dev/cdrom`** with the path of the device special file that you just found.

    **Note:**

    In the example given above, the corrected line reads as follows:

    ```
    /dev/cdrom-hda   /mnt/cdrom   iso9660 noauto,owner,ro 0   2
    ```
11. Save and close the file.

# MPP install files have Windows style newline characters

### Condition

During MPP installation, when copying files to the MPP-RPM folder, Windows style newline characters (CR) characters are present in the script files.

### Cause

Copying files between Windows and Linux servers.

### Solution

Remove all Windows style newline characters in the install files such as `installstatus.php` and `mppinstall.sh`.

a. Open the files using Notepad++.
b. Click **Edit** > **EOL conversion** > **Unix/OSX format** to remove the characters.

# File system check (fsck) reports number of days error

If a file system check (fsck) is performed during the boot up process and indicates an error of extremely large number of days since the file system was checked, it is likely that:

- The system's clock was set backwards manually.
- NTP was reconfigured and then restarted at the time of OS or software installation.

## Solution

### Procedure

You can ignore the number of days reported since the last check. Regardless of the exact number of days since the file system was last checked, fsck performs this check and reports the file system errors.

# Changing PostgreSQL user account passwords

### Before you begin

If you have just installed the EPM software and are still logged into the EPM server, make sure that the environment variables are properly loaded.

### About this task

Experience Portal uses the following PostgreSQL user accounts:

| Default account name | Description |
|---|---|
| postgres | The database administrator can use this account to log in to the local Avaya Experience Portal database and perform database administration tasks.<br>The password for this account is automatically generated. You cannot add other accounts of this type, delete this account, or change the account name.<br>**Important:**<br>Contact the Avaya Services representative to modify the local VoicePortal database as the database contains critical configuration information used to run the system. |
| report | You can have any number of accounts of this type with any account names. |
| reportwriter | This user account can only change the data in the tables that store report data in the Experience Portal database on the Auxiliary EPM server.<br>You can have any number of accounts of this type with any account names.<br>**Important:**<br>Contact the Avaya Services representative to modify the tables that store report data in the local VoicePortal database. |
| vpcommon | This account allows each Auxiliary EPM server limited access to the main Experience Portal database, and it is required if you plan to configure an Auxiliary EPM server.<br>You can delete this account and set the password for this account, but you cannot add other accounts of this type or change the account name. |

Use the `SetDbPassword.sh` script to change all account passwords and add and delete all accounts except for postgres, which you cannot delete.

### Procedure

1. Log on to Linux on the Experience Portal server with root privileges.
2. Enter the `cd $AVAYA_HOME/Support/Security-Tools/SetDbPassword` command, where `$AVAYA_HOME` is an environmental variable pointing to the name of the installation directory specified during the Experience Portal software installation.
3. Enter the `bash SetDbPassword.sh update -u` *`username`* command, where *username* is the name of the user account whose password you want to change.
4. Type the password you want to use for this account and press `Enter`.

   When you change the password for the postgres account, Experience Portal stops and then restarts the **vpms** service.
5. Enter the `/sbin/`*`service vpms status`* command to verify if the **vpms** service has started.

### Next steps

If you change the password for the vpcommon account on the primary EPM server, you must also change the password on the auxiliary EPM server.

# Time synchronization problems

Experience Portal uses *chronyd daemon* to control and synchronize the clocks when the EPM and MPP software is running on different servers. The dedicated MPP servers and the optional auxiliary EPM server point to the primary EPM server as the reference clock.

**Note:**

If the time difference is too large, chronyd cannot synchronize the client and server clocks immediately. A workaround is to manually synchronize the clocks before starting chronyd. After chronyd starts, it adjusts the clients clock with the server timings slowly. The slow process is by design so that confusion with other processes that are running and depends on the clock can be avoided.

To troubleshoot synchronization errors, perform the following procedures in the order given, advancing to the next procedure only if the problem continues to persist.

## Determining whether the servers are synchronized

### Procedure

1. Simultaneously log in to Linux on the EPM server, each MPP server, and, if configured, the optional auxiliary EPM server.

2. On each server, during the same time enter the `date` command.
3. Verify that each MPP server and the optional auxiliary EPM server are synchronized with the primary EPM server.
4. If you find one or more unsynchronized servers, follow the procedure Verify that the chronyd service is operating properly on page 118 .

## Verify that the chronyd service is operating properly

### Procedure

1. Log on to Linux on the Experience Portal server with root privileges.
2. Enter the `systemctl status chronyd` command.

   If the server returns a message stating that the chronyd service is running, continue with this procedure. Otherwise, go to Synchronizing the MPP or auxiliary clock with the primary on page 118.
3. To verify that chronyd is operating properly, enter the `chronyc tracking` command.

   The system displays a status message similar to the following:

   ```
   Reference ID    : 0A868E42 (10.134.142.66)
   Stratum         : 4
   Ref time (UTC)  : Thu Sep 17 12:47:44 2020
   System time     : 0.000000488 seconds fast of NTP time
   Last offset     : +0.000008485 seconds
   RMS offset      : 0.000039525 seconds
   Frequency       : 24.108 ppm slow
   Residual freq   : +0.001 ppm
   Skew            : 0.030 ppm
   Root delay      : 0.147401720 seconds
   Root dispersion : 0.003942181 seconds
   Update interval : 1037.7 seconds
   Leap status     : Normal
   ```

   Verify that the Reference ID points to the Primary EPM server.

## Synchronizing the MPP or auxiliary EPM clock with the primary EPM

### Procedure

1. If you are working with an MPP server and the MPP software is running, stop it using the EPM web interface:
   a. Log on to the EPM web interface by using an account with the Administration or Operations user role.
   b. From the EPM main menu, select **System Management** > **MPP Manager**.
   c. On the MPP Manager page, click the selection box associated with the MPP that you want to stop, then click **Stop** in the **State Commands** group.

   d. Confirm the action when requested.
   e. Wait until the operational state changes to Stopped.

      To check this, click **Refresh** and look at the **State** field.

      **Note:**

      The operational state changes when the last active call completes or the operational grace period expires, whichever comes first.

2. If necessary, log in to Linux on the server.
   - If you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, log on to the local Linux console as root.
   - Otherwise, log on remotely as a non-root user, and then change the user to root by entering the `su - root` command.
3. If you are working with:
   - An MPP server, stop the `mpp` process by entering the `/sbin/service mpp stop` command.
   - The auxiliary EPM server, stop the vpms service by entering the /sbin/*service vpms stop* command.
4. Restart the chronyd process by entering the `systemctl restart chronyd` command.
5. To verify that chronyd is operating properly, enter the `chronyc tracking` command.

   The system displays a status message similar to the following:

   ```
   Reference ID    : 0A868E42 (10.134.142.66)
   Stratum         : 4
   Ref time (UTC)  : Thu Sep 17 12:47:44 2020
   System time     : 0.000000488 seconds fast of NTP time
   Last offset     : +0.000008485 seconds
   RMS offset      : 0.000039525 seconds
   Frequency       : 24.108 ppm slow
   Residual freq   : +0.001 ppm
   Skew            : 0.030 ppm
   Root delay      : 0.147401720 seconds
   Root dispersion : 0.003942181 seconds
   Update interval : 1037.7 seconds
   Leap status     : Normal
   ```

   Verify that the Reference ID points to the Primary EPM server.
6. If you are working with:
   - An MPP server, start the `mpp` process by entering the `/sbin/service mpp start` command.
   - The auxiliary EPM server, start the vpms service by entering the /sbin/*service vpms start* command.
7. Verify the service has started by entering the `/sbin/service mpp status` or `/sbin/service vpms status` command.

## Time Synchronization between external database and EPM servers

If you connect a Experience Portal system to an external database, you may want to make sure that you synchronize the time so that it is same across all servers. While Experience Portal only requires that the EPM and MPP server time be synchronized, you can also synchronize all the servers that Experience Portal connects to. For more information, see the *External time sources* topic in the *Implementing Avaya Experience Portal on multiple servers* guide.

# BIOS corrupted error on HPDLG7 and G8 common servers after installing Avaya Linux

### Condition

BIOS corrupted error on HPDLG7 and G8 common servers after installing Avaya Linux. This issue occurred when the system restarted.

### Cause

The problem is that the BIOS must normally release the performance counters. Instead, the BIOS holds them and updates them for itself. This will not affect the system performance, rather when attempting to measure the performance, things might not appear reliable.

### Solution

Informational messages added in Red Hat Enterprise Linux 6.1 do not affect the normal usage of the system. Kernel version 2.6.32-131.0.15.el6 or later includes a fix which allows the performance events subsystem to load when using these servers, but only using the same counter that the BIOS uses. Performance counter (profiling) data may be unreliable due to the HP ProLiant BIOS design. You can ignore these messages per HP Advisory c03265132.

# Compatibility issues

## Application Interface web service

Experience Portal 6.0.x includes two instances of the Application Interface web service, which allows web service clients to launch applications on Experience Portal and generate outcalls. One instance of the Application Interface web service uses Apache Axis and the other instance uses Apache Axis2.

Beginning with Experience Portal 7.0, only the instance of the Application Interface web service that uses Apache Axis2 is supported. This instance is accessed via the URL `https://<EPM_Server>/axis2/services/VPAppIntfService`.

Where, *<EPM-server>* is the host name or IP address of a Primary EPM or Auxiliary EPM server.

**Note:**

When using a SOAP web service client, ensure that the URL used for invoking the web service is similar to `https://`*`<EPM-server>`*`/axis2/services/VPAppIntfService`.

Applications that use the Axis based instance of the Application Interface web service should be modified to use the Axis2 based instance before the system is upgraded to this release.

## Application Logging web service

Experience Portal 6.0.x includes two instances of the Application Logging web service, which allows web service clients to log information that will be displayed on Experience Portal Application Detail reports. One instance of the Application Logging web service uses Apache Axis and the other instance uses Apache Axis2.

Beginning with Experience Portal 7.0, only the instance of the Application Logging web service that uses Apache Axis2 is supported. This instance is accessed via the URL `https://<EPM_Server>/axis2/services/VPAppLogService`.

**Note:**

The *<EPM_Server>* above is the host name or IP address of a Primary EPM or Auxiliary EPM server.

Applications that use the Axis based instance of the Application Logging web service should be modified to use the Axis2 based instance before the system is upgraded to this release.

## Speech server requirements

Experience Portal 8.0 requires newer versions of speech software than previous versions of Experience Portal. As a result, you may need to upgrade your speech servers before upgrading to this release.

For details about which versions of Loquendo and Nuance speech software are supported by this release of Experience Portal, see .*Avaya Experience Portal Overview and Specification* available at https://support.avaya.com/.

# Chapter 8: Validating Application Interface web service with Application Interface test client

## Verifying communication with the Application Interface web service

### About this task

Use this procedure to verify the communication with the Application Interface web service and Avaya Experience Portal.

**Note:**

If FIPS is enabled on the system where `VPAppIntfClient.sh` is being launched, you need to specify the following additional command line arguments:

- `-K <Java Truststore>`: The Java truststore file name including the path which contains all the trusted certificates. If the command is running on Primary EPM, the Primary EPM truststore can be specified using the value EPM_TRUSTSTORE.
- `-O <Java Truststore password>`: The password for the Java truststore file. If the command is running on Primary EPM, the Primary EPM truststore password can be specified using the value EPM_TRUSTSTORE_PASS

### Before you begin

Ensure that you configure Avaya Experience Portal for the Application Interface test client as described in the *Configuring Avaya Experience Portal for the Application Interface test client* topic in the *Implementing Avaya Experience Portal on multiple servers*.

### Procedure

1. Log on to Linux on the Experience Portal server.

   If you are an Avaya Services representative using Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server, do one of the following:

   - Log on to the local Linux console as sroot.
   - Log on remotely as a non-root user, and then change the user to sroot by entering the `su - sroot` command.

Otherwise, log on to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Navigate to the Application Interface test client directory by entering the `cd $AVAYA_HOME/Support/OutCallTest/VPAppIntfClient` command.
3. Use the following examples to know the calling Application Interface test client using different authentication schemes:
    a. Password Authentication

    Enter the `./VPAppIntfClient.sh —n <outcall-username> —p <outcall password>` command to request the number of available outbound ports.

    - <outcall-username> is an Experience Portal user name configured with the Web services role on the Users page of the EPM web interface.
    - <outcall password> is the password assigned to the <outcall-username> above that is configured from on the Users page of the EPM web interface.

    **Note:**

    The user must have the Web Services user role.

    b. Certificate Authentication

    Enter the `./VPAppIntfClient.sh -y certificate -k <Java Keystore> —o <Java Keystore password>` command to request the number of available outbound ports, where:.

    - -y: <certificate> the authentication type is certificate.
    - -k: <Java Keystore> the Java keystore file name including the path. The Java keystore should contain the User identity certificate including the private key.
    - -o: <Java Keystore password> the password for the Java keystore file.

    **Note:**

    Import the User identity certificate to the EPM and ensure that the certificate is assigned to a user of Certificate type.

    The user must have the Web Services user role.

    c. Password and Certificate Authentication

    Enter the `./VPAppIntfClient.sh -n <outcall-username> -p <outcall password> -y password+certificate -k <Java Keystore> —o <Java Keystore password>` command to request the number of available outbound ports.

    - <outcall-username> is an Experience Portaluser configured on the Users page of the EPM web interface..
    - <outcall password> is the password for <outcall-username> that is configured on the Users page of the EPM web interface..
    - -y: <password+certificate> the authentication type is password + certificate.

- -k: <Java Keystore> the Java keystore file name including the path. The Java keystore should contain the User identity certificate including the private key.
- -o: <Java Keystore password> the password for the Java keystore file.

**Note:**

Import the User identity certificate to the EPM and ensure that the certificate is assigned to the <outcall-username> and the user authentication type is Password and Certificate.

The user must have the Web Services user role.

4. Verify that the Application Interface test client displays a response that shows the total ports and unused ports available for outcalls.

   Fri Oct 17 15:21:02 PDT 2008: VPAppIntfServiceClient: : queryResources succeeded, TotalResources = 25, UnusedH323 = 15, UnusedSIP = 10

   Fri Oct 17 15:21:02 PDT 2008: VPAppIntfServiceClient: : exiting.

# Verifying outcalls and application launching with the Application Interface web service

## About this task

Use this procedure to verify outcalls and the launching of Avaya Experience Portal with the Application Interface web service.

**Note:**

If FIPS is enabled on the system where `VPAppIntfClient.sh` is being launched, you need to specify the following additional command line arguments:

- `-K <Java Truststore>`: The Java truststore file name including the path which contains all the trusted certificates. If the command is running on Primary EPM, the Primary EPM truststore can be specified using the value EPM_TRUSTSTORE.
- `-O <Java Truststore password>`: The password for the Java truststore file. If the command is running on Primary EPM, the Primary EPM truststore password can be specified using the value EPM_TRUSTSTORE_PASS

## Before you begin

Ensure that you configure Avaya Experience Portal for the Application Interface test client as described in the *Configuring Avaya Experience Portal for the Application Interface test client* topic in the *Implementing Avaya Experience Portal on multiple servers*.

## Procedure

1. Log on to Linux on the Experience Portal server.

If you are an Avaya Services representative, and use the Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as sroot.
- Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Navigate to the Application Interface test client directory by entering the `cd $AVAYA_HOME/Support/OutCallTest/VPAppIntfClient` command.
3. Use the following examples to show calling Application Interface test client using different authentication schemes

   a. Password Authentication

      Enter the `./VPAppIntfClient.sh —R 1 —A <application name> —T <number-to-dial> —n <outcall-username> —p <outcall password>` command to initiate an outcall and launch the Experience Portal test application, where:

      - <application–name> is the same test application name as it was entered on the application page.
      - <number-to-dial> is the phone number to place the outcall to.
      - <outcall-username> is an Experience Portal user configured from EPM Web interface.
      - <outcall password> is the password for <outcall-username> that is configured from the EPM Web interface .

      **Note:**

      The user must have the Web Services user role.

   b. Certificate Authentication

      Enter the `./VPAppIntfClient.sh —R 1 —A <application name> —T <number-to-dial> -y certificate -k <Java Keystore> —o <Java Keystore password>` command to initiate an outcall and launch the Experience Portal test application, where:.

      - <application–name> is the same test application name as it was entered on the application page.
      - <number-to-dial> is the phone number to place the outcall to.
      - -y: <certificate> the authentication type is certificate.
      - -k: <Java Keystore> the Java keystore file name including the path. The Java keystore should contain the User identity certificate including the private key.
      - -o: <Java Keystore password> the password for the Java keystore file.

> **Note:**
>
> Import the User identity certificate to the EPM and ensure that the certificate is assigned to a user of Certificate type.
>
> The user must have the Web Services user role.

c. Password and Certificate Authentication

Enter the `./VPAppIntfClient.sh —R 1 —A <application name> —T <number-to-dial> -n <outcall-username> -p <outcall password> -y password+certificate -k <Java Keystore> —o <Java Keystore password>` command to initiate an outcall and launch the Experience Portal test application, where:.

- <application–name> is the same test application name as it was entered on the application page.
- <number-to-dial> is the phone number to place the outcall to.
- <outcall-username> is an Experience Portaluser configured on the Users page of the EPM web interface..
- <outcall password> is the password for <outcall-username> that is configured on the Users page of the EPM web interface..
- -y: <password+certificate> the authentication type is password + certificate.
- -k: <Java Keystore> the Java keystore file name including the path. The Java keystore should contain the User identity certificate including the private key.
- -o: <Java Keystore password> the password for the Java keystore file.

> **Note:**
>
> Import the User identity certificate to the EPM and ensure that the certificate is assigned to the <outcall-username> and the user authentication type is Password and Certificate.
>
> The user must have the Web Services user role.

4. Verify that the dialed phone number rings.
5. Answer the phone and verify that the Experience Portal test application is handling the call.

> **Note:**
>
> The application handles the call in the same way as when an actual user calls into the system.

6. Verify that the Application Interface test client displays:

- A response that shows the result of the LaunchVXML operation.
- The total ports and the unused ports available for outcalls.

```
Fri Oct 17 15:24:58 PDT 2008: VPAppIntfServiceClient: launchVXML succeeded,
SessionID = sys-mpp-2008291222458-2, TotalRes = 24, UnusedH323 = 12, UnusedSIP =
12
```

Fri Oct 17 15:24:58 PDT 2008: VPAppIntfServiceClient: exiting.

# Additional Application Interface web service validations with Application Interface test client

## About this task

Experience Portal supports Axis 2.0 web services that provides outcall functionality and the ability to launch CCXML and VXML applications.. It also provides functionality to send SMS and Email messages and the ability to launch SMS and Email applications.

**Note:**

Axis 2.0 uses Basic authentication. This applies to the Application Interface web service as well as the Application Logging web service.

The Application Interface test client supports the following parameters which you can use to validate or query the Application Interface web service:

**Note:**

Use the `VPAppIntfClient <parameter> command`. For example:

- To query the resources: `VPAppIntfClient -S sys-vpms-a1 -R 4`
- To launch a CCXML application: `VPAppIntfClient -S 123.234.12.34 -R 2 -x tel: -C ccxmltest -t 15`
- To initiate an outcall and launch a VXML application: `VPAppIntfClient -S sys-vpms-a1 -R 1 -T 1234 -F 1122 -A test -t 10`
- To send an event to a CCXML application: `VPAppIntfClient -S sys-vpms-a1 -R 3 -s sys-mpp-a12-2006286000025-26 -e`
- To send an SMS message: `VPAppIntfClient -S sys-vpms-a1 -n user1 -p password1 -R 8 -T 4085551212 -F 114171631 -A MySMSAppName -M this-is-a-test-message -t 30 -s 1234567890`

  **Note:**

  To use an application in the specific zone while sending or launching an SMS or Email message/application, prefix the zoneID to the application name (zoneID:ApplicationName) in the command. If you do not specify the zone in the command, the default zone (0) is used automatically. For example:

  ```
  VPAppIntfClient -S sys-vpms-a1 -n user1 -p password1 -R 8 -T 4085551212 -F 114171631 -A 0:MySMSAppName -M this-is-a-test-message -t 30 -s 12345678900
  ```

- To launch an SMS application: `VPAppIntfClient -S sys-vpms-a1 -n user1 -p password1 -R 7 -T 114171631 -A MySMSAppName -M another-test-message -t 30 -s 1234567891`
- To send an Email message: `VPAppIntfClient -S sys-vpms-a1 -n user1 -p password1 -R 10 -T destination@email.com -F senders-`

```
email@mycorp.com -A MySMSAppName -B this-is-a-test-email -t 30 -J
Subject:-Test-Message -s 1234567897
```

- To launch an Email application: `VPAppIntfClient -S sys-vpms-a1 -n user1 -p password1 -R 9 -T connection-senders-email@mycorp.com -F myemail@email.com -A MySMSAppName -B this-is-a-test-email -t 30 -J Subject:-Test-Message -s 1234567899`

| Parameter | Description | Function |
|---|---|---|
| -S | server-name | Sets the server-name or IP address where the EPM Application Interface Web Service is running. The default is “localhost”. |
| -R | request | Sets the request type that will be issued. Using the following definitions:<br>1 = LaunchVXML<br>2 = LaunchCCXML<br>3 = SendCCXMLEvent<br>4 = QueryResources<br>5 = GetStatus<br>5 = GetStatusEx<br>7 = LaunchSMS,<br>8 = SendSMS,<br>9 = LaunchEmail,<br>10 = SendEmail<br>11 = CreateConversation<br>12 = DeleteConversation<br>13 = GetConversation<br>14 = UpdateConversation<br>15 = GetConversationByAlias<br>16 = AddConversationAlias<br>17 = LaunchHtml<br>The default is “4”. |
| -X | count | Issues the request in asynchronous mode. Count is the number of requests to send. The default value is synchronous with a count of 1. Valid only for LaunchVXML and LaunchCCXML.", |
| -Q | size | Specifies the queue size when sending asynchronous requests. The default value is 10. Valid only for LaunchVXML and LaunchCCXML.", |

*Table continues…*

| Parameter | Description | Function |
|---|---|---|
| -T | toURI / to | Sets the toURI / to value that is used when sending requests. The default value is "tel:2100". For LaunchVXML the number can be prefixed with "tel:", "sip:", or "sips" as a suggestion of the type of resource to use. |
| -F | fromURI/ from | Sets the from URI/from value that is used when sending requests. The default value is "1234567". |
| -A | applicationName | Sets the application name value that is used when LaunchVXML,SMS and Email requests are sent. The default value is "test". |
| -C | applicationName | Sets the application name value that is used when", LaunchCCXML requests are sent. The default value is "ccxmltest". |
| -U | appURLParams | Sets the application URL parameters that will be used when LaunchVXML or LaunchCCXML requests are sent.<br>The default value is null. |
| -P | parameters / appParameters | Sets the parameters values that will be used when LaunchVXML, LaunchCCXML, and SendCCXMLEvent requests are sent. The default value is null. Sets appParameters field for LaunchSMS and LaunchEmail. For LaunchEmail use this field to pass Attachments, ReplyTo, and other parameters. |
| -u | uuiInfo / ucid | Sets the user to user information parameters that will be passed when LaunchVXML or LaunchCCXML requests are sent. The default value is null. Sets ucid for LaunchSMS, SendSMS, LaunchEmail and SendEmail requests. |
| -t | timeout | Sets the timeout value that is used when LaunchVXML or LaunchCCXML requests are sent. The default value is "30" seconds.Sets requestTimeout for LaunchSMS, SendSMS, LaunchEmail and SendEmail requests. |
| -z | zone | Sets the string that is used as the zone. |
| -x | hint | Sets the string that is used as a hint for what type of resources are going to be needed by the CCXML application. Values should be "tel:", "sip:", or "sips". The default value is "tel". |
| -s | sessionId/ parentID | Sets the session ID string that is used when sending events to a CCXML application using the request SendCCXMLEvent. Sets the session ID for SendSMS and SendEmail. Sets parentID field for LaunchSMS and LaunchEmail. |

*Table continues…*

| Parameter | Description | Function |
|---|---|---|
| -e | eventName | Sets the event name string that is used when sending events to a CCXML application using the request SendCCXMLEvent. |
| -n. | name | Sets the user name for the authenticated request. The user name must be configured as an Experience Portal user with the Web Services role in the EPM -> Users page.<br>The default value is "outcall". |
| -p | password | Sets the password for the authenticated request. The default value is "ocpassword1". |
| -y | authenticateType | Sets the authentication type for the user. The authenticateType can be password, certificate, or password+certificate.<br>By default, the authenticateType is password.<br>If the authenticateType is certificate, there is no need to set user name and password. |
| -k | clientKeyStoreFile | Sets the client keystore file in JKS format for certificate authenticated request. The keystore should have the client certificate private key and public certificate. It should also have the signing CA if the client certificate is signed by third-party CA. The whole chain of public certificates needs to be imported to the EPM trusted certificates page under the User category. |
| -o | clientKeyStorePasswd | Sets the password for the client keystore file. |
| -K | truststoreFile | Sets the truststore file (full path) in JKS format with all the trusted certificates.<br>On the Primary EPM, the value EPM_TRUSTSTORE can be specified to use the Primary EPM's truststore. |
| -O | truststorePasswd | Sets the password for the truststore file.<br>On the Primary EPM, the value EPM_TRUSTSTORE_PASS can be specified to use the password for the Primary EPM's truststore. |
| -M | message | Sets the message to send in the LaunchSMS or SendSMS request. This tool does not work with spaces in this field. Use a character like '.' or '-' instead. |
| -m | smsParameters | Sets the SMS parameters sent in the LaunchSMS or SendSMS request. |
| -c | cc | Sets the email CC field for the LaunchEmail or SendEmail request. |
| -b | bcc | Sets the email BCC field for the LaunchEmail or SendEmail request. |

*Table continues…*

| Parameter | Description | Function |
|---|---|---|
| -a | attachments | Sets the email attachments field for the LaunchEmail or SendEmail request. |
| -H | headers | Sets the email headers field for the LaunchEmail or SendEmail request. |
| -J | subject | Sets the email subject field for the LaunchEmail or SendEmail request. This tool doesn't work with spaces in this field. Use a character like '.' or '-' instead. |
| -B | body | Sets the email body field for the LaunchEmail or SendEmail request. |
| -E | emailParameters | Sets the email emailParameters field for the LaunchEmail or SendEmail request. For SendEmail use this field to pass Attachments, ReplyTo, and other parameters." |
| -Z | automated | Sets the test into automated mode. The value for this parameter is the number of iterations to perform. The default is 0. |
| -D | conversationData | Sets the conversationData field for CreateConversation and UpdateConversation. |
| -I | conversationId | Sets the conversationId field for CreateConversation and DeleteConversation. |
| -i | alias | Sets the alias field for GetConversationByAlias and AddConversationAlias. |
| -d | debugLevel | Sets the global debug level for logging output. Valid values are OFF, ERROR, WARN, INFO, and DEBUG. |
| -h | | Displays help and then exits the application. |
| -v | | Displays version information and then exits. |

# Chapter 9: Avaya Experience Portal log files

## EPM server logs

The following logs detail EPM server activities:

- Database log tables on page 132
- EPM PostgreSQL logs on page 132
- EPM logs on page 132
- Tomcat logs on page 133
- Apache/httpd logs on page 133

### Database log tables

These logs are stored in the Avaya Experience Portal database.

| Log | Location | Comments |
|---|---|---|
| Alarm table | Database | Contains alarm data from EPM and MPPs. |
| Application log table | Database | Contains Orchestration Designer errors and application specific log data. |
| Report tables | Database | Contains call and performance report data. |
| System log table | Database | Contains log data from EPM and MPPs. |

### EPM PostgreSQL logs

These logs are stored in the `/var/lib/pgsql/data/pg_log/postgresql-*ddd*.log` directory, where *ddd* is a three letter abbreviation for the day the log was created.

This log contains log data specific to the PostgreSQL database. It is in ASCII format and can be viewed with any text editor.

### EPM logs

These logs are stored in the `$AVAYA_VPMS_HOME/logs/` directory.

| Log name | Comments |
|---|---|
| `avaya.vpms.log` | Contains log data including debug information. Non-debug log entries are copied to the EPM database.<br>All logs are in ASCII format and can be viewed with any text editor. |
| `avaya.networklogserver.log` | |

### Tomcat logs

These logs are stored in the `$CATALINA_HOME/logs/` directory. All logs are in ASCII format and can be viewed with any text editor.

| Log name | Comments |
|---|---|
| `catalina.out` | Contains Tomcat-generated log data and console data. |
| `localhost_log.`*`yyyy-mm-dd`*`.txt` | Contains data from EPM web pages. |

### Apache/httpd logs

These logs are stored in the `/var/log/httpd` directory.

| Log name | Comments |
|---|---|
| `access_log` | Records all requests processed by the MPP. |
| `error_log` | Records diagnostic information and any errors the MPP encounters while processing requests. If the MPP does not start or operate properly, you can usually find details about what went wrong in this file and the `ssl_error_log` file. |
| `ssl_access_log` | Records all requests processed by the MPP. |
| `ssl_error_log` | Records diagnostic information and any errors the MPP encounters while processing requests. If the MPP does not start or operate properly, you can usually find details about what went wrong in this file and the `error_log` file. |
| `ssl_request_log` | Records all requests processed by the MPP. |

# MPP server logs

The following logs are on each Media Processing Platform (MPP) running in the Experience Portal system. All logs are in ASCII format and can be viewed with any text editor.

- Apache/httpd logs on page 133
- MPP process logs on page 134
- MPP records logs on page 135
- MPP transcription logs on page 135

### Apache/httpd logs

These logs are stored in the `/var/log/httpd` directory.

| Log name | Comments |
|---|---|
| `access_log` | Records all requests processed by the MPP. |

*Table continues…*

| Log name | Comments |
|---|---|
| error_log | Records diagnostic information and any errors the MPP encounters while processing requests. If the MPP does not start or operate properly, you can usually find details about what went wrong in this file and the ssl_error_log file. |
| ssl_access_log | Records all requests processed by the MPP. |
| ssl_error_log | Records diagnostic information and any errors the MPP encounters while processing requests. If the MPP does not start or operate properly, you can usually find details about what went wrong in this file and the error_log file. |
| ssl_request_log | Records all requests processed by the MPP. |
| ws_access_log | Records all requests for Avaya Experience Portal Web services. |
| ws_error_log | Records information concerning the MPP Web Services MMS, CdhService, and TransService, including errors when these services process requests. If the EPM cannot contact the MPP, look in this file first. |

## MPP process logs

The process logs contain event and trace messages from the MPP subsystems. By default, they are stored in subdirectories under the $AVAYA_MPP_HOME/logs/process/ directory, and they are accessible from the Log Directories page of the Media Server Service Menu.

**Note:**

The maximum size for each log and the number of logs to retain is set in the **Trace Logger** group of the MPP Settings page.

| Directory name | Log name | Comments |
|---|---|---|
| Administration | mppmaint.log | This file records the actions of themppmaint process, which runs daily to purge the MPP of outdated Contact Detail Record (CDR), Session Detail Record (SDR), and session transcription records. |
| CXI | CCXML-global-*x*.log | This file contains data related to events that are not specifically associated with a CCXML single session. If there is more than one CXI process, the *x* represents the number of processes. |
| | CCXML-SessionSlot-###.log, where ### represents the unique log identifier. | This file contains data related to CCXML operations for individual sessions. The unique identifier can be used to find related Session Manager and Avaya Voice Browser logs. |
| CdhService | CDHService.log | These files record the actions of the CDHService Web Service, which enables the EPM to download CDR and SDR records from the MPP. |
| ServiceMenu | ServiceMenu.log | This file records the actions of the Service Menu process. |

*Table continues…*

| Directory name | Log name | Comments |
|---|---|---|
| EventMgr | EventMgr.log | This file records the actions of the Event Manager, which collects events from other MPP processes and sends them to the network log web service on the EPM. |
| MMS | MmsServer.log | This file contains messages from the MMS Web Service, which is accessed by the EPM to send commands, configuration changes, and heartbeat requests the MPP. |
| OCWSServer | OCWSServer.log | This file contains messages produced by Application Logging web service, which is used to make outbound calls on the MPP. |
| SessMgr | SessionManager.log | This file contains data related to events that are not specifically associated with a single session. |
| | SessionSlot-###.log, where *###* represents a unique log identifier | This file contains data related to Session Manager operations for individual sessions. |
| SysMgr | logfile.log | This file records messages produced by the System Manager process. |
| TraceService | TraceService.log | A set of files that contain trace entries from the trace web service on the MPP that uploads trace data to the EPM Trace Viewer. |
| TransService | transervice.log | This file contains messages from the TransService Web Service, which is accessed by the EPM to download transcription and utterance files from the MPP for inclusion in the Session Detail report. |
| VB | globalx.log | This file contains data related to events that are not specifically associated with a single session. If there is more than one AVB process, the *x* represents the number of processes. |
| | SessionSlot-###.log, where *###* represents a unique log identifier | This file contains data related to AVB operations for individual sessions. |

## MPP records logs

The record logs contain Contact Detail Records (CDRs) and Session Detail Records (SDRs). All data is sent to the EPM. These logs are stored in the `$AVAYA_MPP_HOME/logs/records/<yyyy>/<mm>/<dd>/` directory, and the log names are:

- `<name>_cdr_<#>_<date>.bin`
- `<name>_sdr_<#>_<date>.bin`

## MPP transcription logs

These logs contain session transcription data.

You can access these log files by creating a Session Detail report through the EPM.

The transcriptions are stored in the `$AVAYA_MPP_HOME/logs/<yyyy>/<mm>/<dd>/transcriptions/` directory.

If utterances are saved for an application, they are stored in the `$AVAYA_MPP_HOME/logs/transcriptions/<yyyy>/<mm>/<dd>/utterances/<session-id>` directory.

## Moving the MPP logs to a different location

### About this task

If you need to free up space on an MPP server, you can use the `mppMoveLogs.sh` script to create a new directory and move the MPP logs to that directory.

### Procedure

1. If necessary, install the target drive or create the target partition as described in your operating system documentation.

   **Important:**

   Do *not* create the new directory on this drive or partition, as the script will fail if a directory already exists.

   The drive or partition must be local to the MPP server and it must contain either 2 GB of free space or as large in size as the current `$AVAYA_MPP_HOME/logs` directory, whichever value is greater.

   **Tip:**

   For a good tutorial about creating a partition, see http://tldp.org/HOWTO/html_single/Partition/.

2. If you created a new partition, add an entry for the partition in the `/etc/fstab` file so that it is automatically mounted when the system is booted.

   If the partition for the directory will only host the Experience Portal log directory, you can improve security by setting its properties in the `/etc/fstab` file to `rw,nosuid,noexec,auto,nouser,async,noatime,nodev`. For more information about these options, see http://www.faqs.org/docs/securing/chap5sec45.html.

3. Log on to the EPM web interface by using an account with the Administration or Operations user role.

4. Stop the MPP whose logs you want to move:

   a. From the EPM main menu, select **System Management** > **MPP Manager**.

   b. On the MPP Servers page, click the Selection check box next to the name of the MPP you want to stop.

   c. Click **Stop** in the **State Commands** group

   d. Confirm the action when requested.

   e. Wait until the operational state becomes Stopped. To check this, click **Refresh** and look at the **State** field.

      **Note:**

      The operational state changes when the last active call completes or the grace period expires, whichever comes first.

5. Log on to Linux on the Experience Portal MPP server.

   If you are an Avaya Services representative, and use Avaya Enterprise Linux, the Avaya Service accounts will not be available after the Avaya Enterprise Linux upgrade. The Avaya Service accounts will be available through EASG configuration during the Experience Portal upgrade.

   - Log on to the local Linux console as root.
   - Or log on remotely as a non-root user and then change the user to root by entering the `su - root` command.

6. Enter the `bash mppMoveLogs.sh [-logdir` *`directory_name`*`]` command, where `–logdir` *`directory_name`* is an optional parameter specifying the directory name that you want to use.

   If you do not specify this parameter on the command line, the script prompts you for the directory name during execution. If the directory you specify already exists, the script returns an error message and fails. This ensures that no existing files will be overwritten by the script.

   When the script completes successfully, all of the current logs will reside in the new location, and all future logs will be stored in the new location.

7. Restart the MPP:

   a. From the EPM main menu, select **System Management** > **MPP Manager**.

   b. On the MPP Servers page, click the Selection check box next to the name of the MPP you want to start.

   c. Click **Retart** in the **State Commands** group

   d. Wait until the operational state becomes Running. To check this, click **Refresh** and look at the **State** field.

# Packing MPP logs and transcriptions in a TAR file

## About this task

You can use the Diagnostics in the Media Server Service Menu to pack the logs, transcriptions, and debug files into a single TAR file for further diagnostics and troubleshooting.

**Note:**

You can use the `getmpplogs.sh` script to customize which files are packed.

### Procedure

1. Log into the Media Server Service Menu.
2. From the Media Server Service Menu, select **Diagnostics**.
3. On the Diagnostics page, click **Pack Files**.
4. On the Pack Files Options page, select the files you want to pack. You can select any or all of the following:
   - Select all check box: Pack all available files.
   - **Logs**: Pack all the MPP log files.
   - **Transcriptions and utterances**: Pack all the transcriptions and utterances saved by the applications running on the MPP.
   - **Debug files**: Pack all the debug (trace) data recorded on the MPP.
5. Click **Pack**.

   Avaya Experience Portal creates a TAR file with the format `<hostname>_<date and time stamp>_MPP.tar` that contains all of the selected information. In addition, Avaya Experience Portal creates a TAR file for each MPP component with the format `<MPP component>_<hostname>_<date and time stamp>_MPP.tar`.

   Avaya Experience Portal displays the TAR file names at the bottom of the page.
6. To save any TAR file, right-click the file name and select **Save As** from the pop-up menu.

### Next steps

If you need to restore the packed log files, use the `restorempplogs.sh` script.

## Packing MPP logs and transcriptions using getmpplogs.sh

The `getmpplogs.sh` script packs system information files, logs, and transcriptions into one TAR file.

### About this task

**Note:**

You can also pack the log files from the Diagnostics page in the Media Server Service Menu.

### Procedure

1. Log on to Linux on the Experience Portal MPP server.

   If you are an Avaya Services representative, and use Avaya Enterprise Linux, the Avaya Service accounts will not be available after the Avaya Enterprise Linux upgrade. The Avaya Service accounts will be available through EASG configuration during the Experience Portal upgrade.

   - Log on to the local Linux console as root.

- Or log on remotely as a non-root user and then change the user to root by entering the `su - root` command.

**Note:**

You can run this script as an avayagroup member, but if you run this script while logged in as `root` or sroot, it collects additional log files.

2. Navigate to the MPP `bin` directory by entering the `cd $AVAYA_MPP_HOME/bin` command.
3. Enter the `getmpplogs.sh` command with the following options.

| Option | Purpose |
|---|---|
| **--logs** | To export system information and MPP logs, Apache logs, and system event logs.<br>The system information exported is:<br>• hostname<br>• system uptime<br>• system CPU and memory information<br>• network configuration<br>• storage usage<br>• `/etc/hosts` file<br>• currently running processes<br>• CPU activity information<br>• RPM database information<br>• MPP specific configuration |
| **--transcriptions** | To export system information and all the transcriptions and utterances. |
| **--debugfiles** | To export only the system information and all the latest core files from each MPP component with libraries and debug symbols. |
| **--help** | To display the above `getmpplogs.sh` commands.<br>**Note:**<br>This parameter cannot be combined with any other parameters. |

Except for the --help option, you can specify any combination of parameters when you run the `getmpplogs.sh` script. The types of files that are packed in the TAR file depends on the combination of the command options that you use.

For example, to pack all transcriptions, system information, and debug files in a TAR file stored in the `$AVAYA_MPP_HOME/web/admin/AVPSupport` directory, enter the `getmpplogs.sh --logs --transcriptions --debugfiles` command.

### Next steps

If you need to restore the packed log files, use the `restorempplogs.sh` script.

## Restoring packed MPP log files

### About this task

You can use the `restorempplogs.sh` script to restore the MPP log files that were packed using either the `getmpplogs.sh` script or the Pack Files Options page available from the Media Server Service Menu.

The `restorempplogs.sh` script:

- Restores the call data records
- Restores the installation logs
- Restores the process logs, if available
- Restores the transcriptions and utterances, if available

### Procedure

1. If the MPP was started through the EPM:
    a. Log on to the EPM web interface by using an account with the Administration or Operations user role.
    b. From the EPM main menu, select **System Management** > **MPP Manager**.
    c. On the MPP Manager page, use the Selection check box in the MPP server table to select which MPPs you want to change.
    d. Click **Stop** in the **State Commands** group.
    e. After the grace period expires, click **Refresh** to ensure that the state is now **Stopped**.
    f. Click **offline** in the **`Mode Commands`**.
2. Log on to Linux on the Experience Portal MPP server.

    If you are an Avaya Services representative, and use Avaya Enterprise Linux, the Avaya Service accounts will not be available after the Avaya Enterprise Linux upgrade. The Avaya Service accounts will be available through EASG configuration during the Experience Portal upgrade.

    - Log on to the local Linux console as root.
    - Or log on remotely as a non-root user and then change the user to root by entering the `su - root` command.
3. Restore the log files by entering the `bash restorempplogs.sh` *`<path/file.tar.gz>`* command, where *`<path/file.tar.gz>`* is the fully qualified path and file name of the file created by the **`Pack`** command or the `getmpplogs.sh` script.

    If the script finds the file, it displays the following:

```
This utility will restore records of type:
 Records
 Installation logs
 Process logs
 Transcriptions & Utterances
from a tar file generated by the getmpplogs script.
If the directories for these records already exist, then
the directory will be renamed to <directory-YYYYMMDD-HHMM> before
the restore.
Press Enter to continue, or press Control-c to cancel
```

4. Press `Enter` to run the script and restore the log files. The script produces output similar to the following:

```
Extracting files from
'/opt/Avaya/ExperiencePortal/MPP/tmp/AEPSupport/cl-
mpplab-02_Apr_24_2007_14_12_17_MPP.tar.gz'...
 Depending on the amount of data, this may take several minutes.
  Stopping services...
    Checking service 'mpp'
    - stopping: 'mpp'
 - Restoring 'Records'
    Moving existing '/opt/Avaya/ExperiencePortal/MPP/logs/records'
to
    '/opt/Avaya/ExperiencePortal/MPP/logs/records-20070424-1419'...
Restoring '/tmp/untar/logs/records' to '/opt/Avaya/
ExperiencePortal/MPP/logs/records'...
    Restoring directory and file permissions...
 - Restoring 'Installation logs'
    Moving existing '/opt/Avaya/ExperiencePortal/MPP/logs/install'
to
    '/opt/Avaya/ExperiencePortal/MPP/logs/install-20070424-1419'...
    Restoring '/tmp/untar/logs/install' to '/opt/Avaya/
ExperiencePortal/MPP/logs/install'...
    Restoring directory and file permissions...
 - Restoring 'Process logs'
    Moving existing '/opt/Avaya/ExperiencePortal/MPP/logs/process'
to
    '/opt/Avaya/ExperiencePortal/MPP/logs/process-20070424-1419'...
    Restoring '/tmp/untar/logs/process' to '/opt/Avaya/
ExperiencePortal/MPP/logs/process'...
    Restoring directory and file permissions...
 - Restoring 'Transcriptions & Utterances'
    Moving existing '/opt/Avaya/ExperiencePortal/MPP/logs/
transcriptions' to
    '/opt/Avaya/ExperiencePortal/MPP/logs/
transcriptions-20070424-1419'...
    Restoring '/tmp/untar/transcriptions' to '/opt/Avaya/
ExperiencePortal/MPP/logs/transcriptions'...
Restoring directory and file permissions...
Log Restoration Complete!
INFO: The service 'mpp' will not be automatically restarted by
this script.  If you wish to restart
this service, use the command:
          /sbin/service mpp start
```

5. If the hostname of the current machine is different than the hostname stored in the log files, the `restorempplogs.sh` script displays a warning message alerting you that the names of the log files in the `$AVAYA_MPP_HOME/logs/records` and `$AVAYA_MPP_HOME/logs/transcriptions` directories need to be changed so that the hostname included in the filename matches the server's new hostname.

   When you rename these files:

   - Use the short name for the server instead of the fully qualified domain name.
   - Make sure that the hostname you specify matches the exact server hostname, including case.

   **Note:**

   If you do not change the log file names, then these records will not be accessible to the EPM server and therefore will not be accessible to any reports created through the EPM.

# Application server logs

Application server logs are available only when you use Orchestration Designer to create the speech application and are running it in a Tomcat environment.

All application server logs are in ASCII format. You can view them in any text editor.

## Application server servlet container logs

The logs contain log data from the servlet container. You can find these log files in the following locations:

- `$CATALINA_HOME/logs/catalina.out`
- `$CATALINA_HOMElocalhost.date.log.txt`

For more information on setting the number of application server failover logs in the EPM settings, see the*EPM Settings and View EPM Settings Page field descriptions* topic in the *Administering Avaya Experience Portal*.

**Note:**

If you install or upgrade Experience Portal and this log already exists, Experience Portal automatically renames the existing file as `catalina.nnn`, where *nnn* is a unique sequential identifier starting with 000. It then creates a new version of `catalina.out` and writes all log entries from the current installation forward into that file.

## Orchestration Designer errors and application reports log

This log file only exists if Orchestration Designer cannot write data to the EPM when its session ends. The next time Orchestration Designer ends, it again tries to write its log data to the EPM, so the information in this log is eventually transferred to the EPM.

You can find this log file in the following location: `$CATALINA_HOME/webapps/app_name/data/logs/savereport.log`

**Note:**

If application reporting is disabled, no data is logged. Otherwise, all report data is sent to the EPM.

### Orchestration Designer trace log

If the query string includes`ddtrace=true`, this log contains application specific trace data.

You can find this log file in the following location: `$CATALINA_HOME/logs.log`

You can change the location, format, and contents of this log, in the `webapps/app_name/data/ddlog4j.properties` file.

## Third party logs for ASR and TTS servers

The following third party logs contain vendor-specific data for the Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) servers.

### ASR, TTS, and NSS Server Logs for Nuance

The following information on logs covers two platforms:

- Nuance Speech Server with Nuance Recognizer and Nuance Vocalizer
- Nuance Speech Server with Nuance Recognizer
- **Linux**: All logs located in `$NSSSVRSDK/logs`

For more information about interpreting the log files, see your Nuance documentation.

### ASR, TTS, and LSS Server Logs for Loquendo

The following information on logs covers two platforms:

- Loquendo MRCP Server
- Loquendo Speech Server
- **Linux**:
    - LMS/LSS: `/var/opt/Loquendo/Platform/logs`
    - ASR: `/var/opt/Loquendo/Platform/logs/LASR`[1]
    - TTS: `/var/opt/Loquendo/Platform/logs/LTTS`[2]

For more information about the location and details about the log files, see your Loquendo documentation.

[1] Only if option **lasrEnableLogging** is enabled in the Loquendo management console.

[2] Only if option **lttsEnableLogging** is enabled in the Loquendo management console.

# Chapter 10: Resources

## Documentation

The following table lists the documents related to Experience Portal. Download the documents from the Avaya Support website at http://www.avaya.com/support:

| Title | Description | Audience |
|---|---|---|
| *Avaya Experience Portal Documentation Roadmap* | Lists all the documents related to Experience Portal and describes the organization of content across the documents. | Avaya Professional Services<br>Implementation engineers |
| *Avaya Experience Portal Overview and Specification* | Describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements. | Implementation engineers |
| *Implementing Avaya Experience Portal on a single server* | Provides procedures to install and configure the Avaya Experience Portal software on a single server. | Implementation engineers |
| *Implementing Avaya Experience Portal on multiple servers* | Provides procedures to install and configure Avaya Experience Portal software on two or more dedicated servers. | Implementation engineers |
| *Upgrading to Avaya Experience Portal 8.0* | Describes how to upgrade your Avaya Experience Portal 7.2.3 to Experience Portal 8.0. | Implementation engineers |
| *Administering Avaya Experience Portal* | Provides general information about and procedures for administering and configuring specific Experience Portal functions and features using a web-based interface. | Implementation engineers |

*Table continues…*

| Title | Description | Audience |
|---|---|---|
| *Avaya Experience Portal Security White Paper* | Provides information about the security strategy for Experience Portal, and provides suggestions that companies can use to improve the security of the Experience Portal systems and applications. | Avaya Professional Services<br>Implementation engineers |
| Avaya Experience Portal 8.0 Mobile Web Best Practices White Paper | Provides recommended strategies for deploying Avaya Orchestration Designer Mobile Web applications with Avaya Experience Portal 8.0, detailing configuration for security, scalability and high availability. | Avaya Professional Services<br>Implementation engineers |

# Finding documents on the Avaya Support website

### Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

# Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

**Important:**

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
  - Click **Filters** to select a product and then type key words in **Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( 🌐 ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon (👁).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

**Note:**

Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

# Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

### About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
    - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
    - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

      The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
    - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
    - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

  **Note:**

  Videos are not available for all products.

# Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

# Appendix A: New common server R3

## New common server R3

### HP DL 360 G7, G8, and G9 hardware specification for Experience Portal

For more information, see Maintaining and Troubleshooting the HP ProLiant DL360 G9 Server.

### Experience Portal specific list of FRUs

**Table 1: : External Maintenance Field Replaceable Units**

| Description | Hot-swappable? |
|---|---|
| DL360G9 300GB 10K SAS 2.5" HDD | Y |
| DL360G9 800 WAC PWR SUP | Y |

For more information, see the section External Maintenance Field Replaceable Units in the *Maintaining and Troubleshooting the Dell PowerEdge R630 Server* guide.

**Table 2: : Server Field Replaceable Unit (SFRU)**

| Description | Hot-swappable? |
|---|---|
| DL360G9 SRVR 2CPU MID 800WAC FRU | N |
| A Server FRU is based on the Server core components. A server FRU will have the correct number and type of CPUs, it will have 4 DIMMs and the 4 embedded NIC ports. The following components will need to be sourced from the existing server: HDDs, Power Supply Unit (PSU), PCIe Cards, and any additional DIMMs over 4. | |

For more information, see the section Server Field Replaceable Unit in the *Maintaining and Troubleshooting the Dell PowerEdge R630 Server* guide.

**Table 3: : Internal Field Replaceable Units**

| Description | Hot-swappable? |
|---|---|
| DL360G9 DVD-RW DRIVE W/BRKT | N |
| DL360G9 1Gb PCIE DUAL PT NIC | N |
| DL360G9 CHASSIS FAN | N |
| DL360G9 4GB RDIMM | N |

For more information, see the section Internal Field Replaceable Units in the *Maintaining and Troubleshooting the Dell PowerEdge R630 Server* guide.

**Table 4: : Customer replaceable unit (CRU)**

| Description | Hot-swappable? |
|---|---|
| DL360G9 RAID battery | N |

For more information, see the section RAID Battery in the *Maintaining and Troubleshooting the Dell PowerEdge R630 Server* guide.

### Dell R630 hardware specification for Experience Portal

For more information, see Maintaining and Troubleshooting the Dell PowerEdge R630 Server at https://downloads.avaya.com/css/P8/documents/101016383

# Appendix B: MPP MRCP Timers

## Timer Release

In Experience Portal 7.1 and later, the default values of MPP timers that control speech server events and protect speech server failures have been re-calibrated. Depending upon the application deployed, you can modify these values.

| Timer Name | Previous Release | Experience Portal 7.1 |
|---|---|---|
| mpp.mrcpsessionrefresh.timer | 40 | 40 |
| mpp.mrcppoststartofspeechevent.timer | 20 | 80 |
| mpp.mrcppostrecogstartedevent.timer | 20 | 20 + Dynamic value |

### mpp.mrcpsessionrefresh.timer

Use this timer as a guard against a speech server failure while playing prompts or using ASR. You can also use this timer to generate some traffic when speech is not being used to prevent a speech server session timeout.

`mpp.mrcpsessionrefresh.timer` value should always be set to 20 seconds lesser than the speech server session timeout value. This value must be larger than the largest prompt to be played and must be longer than the longest expected ASR response.

The session timeout value is 60 seconds by default for Nuance. On each Nuance speech server, modify the value in the `server.mrcp2.sip.sessionTimeout` for MRCP V2 and in `server.mrcp1.rtsp.sessionTimeout` for MRCP V1 in the configuration file. Other vendors may have a different way to update this value.

For example, if you need to play a prompt that is 180 seconds long, then set the value of `mpp.mrcpsessionrefresh.timer` to 190 seconds on each MPP server and set the speech server session timeout to 210.

### mpp.mrcppoststartofspeechevent.timer

Use this timer as a guard for cases where the MPP has received a Start of Speech Event, but has not received Recognition done or an error response because the speech server has gone out of service.

The value should always be 20 seconds more than the maximum speech value set for the speech server.

The value on the speech server can be updated in the following ways in the order of precedence:

1. As a VXML property: This method is the preferred method as it is specific to Individual Grammar. property `<name="maxspeechtimeout" value="10s"/>`
2. By logging into the EPM and changing the value of Recognition Timeout:
   - Log on to **EPM** > **Applications** > **Change Application** page.
   - In **Speech Parameters** > **ASR** change the value of Recognition Timeout.

     This is a parameter that applies to all the recognition requests for the particular application.
3. By changing the `maxspeechtimeout` property: On the Nuance Speech Server, change the `maxspeechtimeout` property in the `Recognizer's Baseline.xml` file.

   (Default is 22s for V1 and 10s for V2)
4. Repeat Step 3 on all Speech Servers.

   Other vendors may have a different way to specify this value.

   If the maximum value set for speech for all applications is less than 60 seconds, then there is no need to modify the MPP configuration. For values greater than 60 seconds, modify the MPP configuration value for mpp.mrcppoststartofspeechevent.timer to the maximum speech value + 20 seconds on each MPP server.

### mpp.mrcppostrecogstartedevent.time

Use this timer as a guard against a speech server failure while waiting for recognition-complete. The guard timeout value is dynamically calculated by adding the configured value (mpp.mrcppostrecogstartedevent.timer) to the no-input timeout value passed to the speech server.

**Note:**

As the guard value is dynamically calculated, the MPP configured value should not be modified.

A no-input timeout value is passed to the speech server as RECOGNITON-START-TIMERS in case of MRCP V1 or START-INPUT-TIMERS in case of MRCPv2.

This MPP guard value starts with `mpp.mrcppostrecogstartedevent.timer` that is set to 20 seconds, and then adds the no-input timeout value set through one of the following method in order of precedence:

1. Change the value of VXI: The default value of VXI for timeout is 7 seconds. You can change this value per recognition request as follows:

   <property name="timeout" value="10s"/>

   For example, the guard's value will be 20 + 10 = 30 seconds.
2. Globally updating the no-input timeout value: This method updates the no-input timeout value globally in the Application, unless each recognition request has a property tag used for setting the timeout value as mentioned in method 1.
   - Log on to **EPM** and navigate to **Applications** page > **Speech Parameters** > **ASR**.
   - Update the value of No Input Timeout.

For example: No Input Timeout = 45000 milliseconds

This will set the value of the guard to 20 + 45 = 65 seconds.

✱ **Note:**

The no-input timeout value passed to the speech server should not be greater than the value set for the speech server session timeout.

# Index