Administering Avaya Experience Portal

Release 8.1
Issue 1
July 2021

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.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

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 as indicated in the order, Documentation, or as authorized by Avaya in writing. 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). End User 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”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage

Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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.

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.

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 administering and configuring specific Avaya Experience Portal functions and features using a web-based interface.

This document is intended for anyone who is involved with configuring and administering the functions and features of Avaya Experience Portal at a customer site. The audience includes and is not limited to system administrators, implementation engineers, business partners, and customers.

Chapter 2: User management

Users in Avaya Experience Portal

In Avaya Experience Portal, users are people authorized to access the:

- Experience Portal Manager (EPM) web interface, which enables users to perform administrative, configuration, and maintenance tasks.
- Media Server Service Menu web interface, which helps administrators troubleshoot problems on a Media Processing Platform (MPP).

Both web interfaces require either a unique user name and password, a unique user name and certificate, or a unique user name, password and certificate created by an Experience Portal administrator. You can also create an unlimited number of accounts and ensure that the passwords and/or certificates they use are secure

Roles-based access in Experience Portal

Experience Portal provides role-based access to the EPM pages. 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. For example, if you have the View Only permission on the Users EPM page, you cannot add, change, or delete a user. To gain access to these pages, you must obtain a user account with a different user role.

These roles are default EP roles, but you can create a custom role for any particular purpose.

User roles

Experience Portal provides role based access to the EPM pages. The user roles determine which pages the user can see and what actions the user can perform on those pages. The roles are:

Role	Description
Administration	User accounts with Administration access can perform all system-related functions through the EPM, such as managing MPPs, VoIP connections, and speech applications. The only things Administrators *cannot* do are managing user accounts and viewing the audit logs. Administrators also have some other limitations. For example, administrators do not have Privacy Manager permissions. Because users with the Administration role have such a wide range of access and privilege, you must strictly limit the use of these accounts.
Auditor	User accounts with Auditor access can generate the Audit Log report and set the retention period for records in the audit log.
Maintenance	User accounts with Maintenance access can view system information, but they cannot make any changes to the Experience Portal system.
Operations	User accounts with Operations access can control the operation of MPPs, including stopping, starting, and rebooting those systems. Operators can also change the status of alarms to denote that they have been acknowledged or can be retired. Operators *cannot* configure an MPP. They can only control the ones that an Administrator has already added to the Experience Portal system.
Privacy Manager	User accounts with Privacy Manager role can update: • All the Transcription related configuration under Reporting Parameters group for an application. • Privacy Settings for traces. User accounts with Privacy Manager role can access the Privacy Settings menu in EPM > System Configuration > EPM Server.
Reporting	User accounts with Reporting access can generate the standard reports, add, edit, or delete the custom and scheduled reports. They can also change the schedules for the scheduled reports. User accounts with Reporting access cannot make any changes to the other features in the Experience Portal system.
User Manager	User accounts with User Manager access can add and change Experience Portal user accounts. User Managers can create new roles with specific access permissions. They can change or delete the defined roles, and assign these roles to the user accounts. They can also configure an LDAP connection between a corporate directory and the EPM so that EPM users no longer need to be defined locally on the EPM. Only Users with the User Manager role can see the User Management section of the main EPM menu.
Web Services	User accounts with Web Services access can use Application Interface Web Service to launch any application configured on the Experience Portal system. They can also use Application Logging Web Service to save application and call flow data information for any application.
POM Administration	User accounts with POM Administration access can administer the functioning of Proactive Outreach Manager through Experience Portal.

Table continues…

Role	Description
POM Campaign Manager	User accounts with POM Campaign Manager access can administer the different campaigns created. With this user role, you can create, edit, and delete campaigns in POM.
POM Contact Attributes Unmask	A new role is created in the POM system to display the contact list data as un-masked. If this role is assigned to the user, then all the contact list fields are displayed as un-masked.
Org POM Campaign Manager	User accounts with Org POM Campaign Manager access can administer the different campaigns created for the specific organization. With this user role, you can create, edit, and delete campaigns in POM.
Org POM Contact Attributes Unmask	A new role is created in the POM system to display the contact list data as un-masked for an organization. If this role is assigned to the user, then all the contact list fields are displayed as un-masked. **Note:** If the Org POM Contact Attributes Unmask role is assigned to Org user, then the value displayed is unmasked to that user. Also, if this role is assigned to default organization user, then the value displayed is unmasked to that default user only.

Note:

Additional roles may be available if you have installed a managed application on Experience Portal. For more information on managed application based roles, see the documentation delivered with the managed application.

Password administration

Passwords are keys to the Experience Portal system. They must be protected and *strong*. A strong password is one that is not easily guessed and is not listed in any dictionary. Protected and strong passwords are especially important for root and administrative-level passwords since they have no access restrictions. Passwords created during Experience Portal installation are checked for minimal characteristics as follows:

- Passwords must contain at least one alphabetic character and one digit.
- Passwords are case-sensitive and should contain a combination of upper and lower case letters.
- A password cannot contain the associated user name.
- Although you can determine the minimum password length, you must not use fewer than eight characters.

After installation, when you use the EPM to create additional user accounts, the minimal characteristics for passwords are enforced. However, administrators can customize the minimum password length. Password length can be between 4 to 256 characters. You should set this value to at least eight characters.

For security reasons, you should change your default password when you log on to Experience Portal for the first time. Password reset is not required on first logon in the following scenarios:

- If the password longevity is not checked at the time of adding a user.
- If the login options password longevity is set to 0.

To ensure that strong passwords are created, you should use a nonsensical combination of letters and digits when creating passwords.

Logging in to the Experience Portal web interface

About this task

The Experience Portal Manager (EPM) web interface is the main interface of the Experience Portal system.

For any Experience Portal administrative tasks, you must log in to the EPM web interface on the primary EPM server.

Note:

The users configured for certificate-based authentication are authenticated and redirected to the EPM home page.

Procedure

1. On an IE browser, enter the URL of your Experience Portal system.

   The default URL is: `https://<EPM-server>/VoicePortal`

   where, *<EPM-server>* is the host name or IP address of the system where the primary EPM software is installed.

   Note:

   Enable Transport Layer Security (TLS) on your IE browser. For more information on configuring web browsers to use TLS security, see *Implementing Avaya Experience Portal on multiple servers*.

2. On the EPM login page, in the **User Name** field, enter your EPM user name.

   The user name is case-sensitive. It must exactly match the existing Experience Portal EPM account name.

   If organization level access is enabled in the Experience Portal system and you are assigned to an organization, prefix your user name with the organization name and a forward slash character.

3. Click **Submit**.
4. In the **Password** field, enter your EPM login password.

The password is case-sensitive. It must exactly match the password assigned to the specified user name.

5. Click **Logon**.
6. **(Optional)** If you are forced to change the password on the first login, do the following:
   a. Click the **Change Password** link.
   b. Enter the information in the **User Name**, **Old Password**, and **New Password** fields.
   c. Re-enter the new password in the **Verify Password** field.
7. Click **Submit**.

Changing your account password

About this task

Use this procedure to change your account password or set a new password if your password expires.

Procedure

1. On your Internet Explorer browser, enter the URL of your Experience Portal system.

   The default URL is `https://<EPM-server>/VoicePortal`, where *<EPM-server>* is the name of the system where the EPM software is installed.
2. On the Login page, click the **Change Password** link at the bottom of the page.
3. On the Change Password page, do the following:
   a. In the **User Name** field, enter your user name.
   b. In the **Old Password** field, enter your old password.
   c. In the **New Password** field, enter your new password.

      The password is case-sensitive. It must comply with the number of characters defined in the **Minimum Password Length** field.
   d. In the **Verify Password** field, re-enter your new password.
   e. Click **Submit**.

Setting global login parameters

Procedure

1. Log on to the EPM web interface by using an account with the User Manager user role.
2. On the EPM main menu, click **User Management** > **Login Options**.

3. On the Login Options page, set the global login parameters in the **User Login Options** group.
4. Click **Save**.

Unlocking a user account

About this task

After multiple unsuccessful login attempts, a user might be locked for some time. The locking period depends on the settings that are configured in the following global login parameters:

- **Failed Login Lockout Threshold**
- **Failed Login Lockout Duration**

User Managers can unlock an account manually before the **Failed Login Lockout Duration** expires.

Procedure

1. Log on to the EPM web interface by using an account with the User Manager user role.
2. On the EPM main menu, click **User Management** > **Users**.
3. On the Users page, click the **Unlock** link in the **Locked** column for each user account that you want to unlock.

Viewing a user account

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, Maintenance, or User Manager user role.
2. On the EPM main menu, click **User Management** > **Users**.

   If you are not logged in to the EPM with the User Manager user role, the EPM displays the Users page in the view-only mode.

Adding a user account

Procedure

1. Log on to the EPM web interface by using an account with the User Manager user role.
2. On the EPM main menu, click **User Management** > **Users**.

3. On the Users page, click **Add** in the **User accounts** section.
4. On the Add User page, enter the appropriate information and click **Save**.

Note:

If you select the Administration user role, this EPM account can also access the Media Server Service Menu on each MPP server.

Changing a user account

About this task

Use this procedure to modify an existing EPM user account.

Note:

You cannot change the existing user name.

Procedure

1. Log on to the EPM web interface by using an account with the User Manager role.
2. On the EPM main menu, click **User Management** > **Users**.
3. On the Users page, in the **Name** column, click the name of the account that you want to change.
4. On the Change User page, enter the appropriate information and click **Save**.

   Users must specify the current password of the account when updating their account information.

Deleting an EPM user account

About this task

You can delete all the EPM user accounts except for the user account that you use to log in to the EPM. Also, if Avaya Services is maintaining this system, you cannot delete the init account created while configuring the Avaya Service accounts.

Note:

Ensure that the user account that you want to delete is not the only user account with the User Manager role. Without a User Manager account, you cannot add or change user accounts in the EPM. You must reinstall Experience Portal to create a User Manager account. However, if you have two user accounts, you can delete the admin user if you are logged in as the non-admin user.

Procedure

1. Log on to the EPM web interface by using an account with the User Manager role.
2. On the EPM main menu, click **User Management** > **Users**.
3. On the Users page, do one of the following:
   - To delete individual accounts: Select the check box for the user account name that you want to delete.
   - To delete all accounts: Select the selection check box in the header row of the table, which automatically selects all user accounts.

   If you select the accounts of any users who are currently logged in to the EPM, those users will continue to have access until their current session ends. After the end of the session, the users cannot log back in to the EPM.

   Note:

   An account that displays **Remote User** in the **Assigned Roles** column belongs to a user who has logged in using an authorized account in the corporate directory. If you delete this account, the EPM removes it from the table in this section, but it does *not* keep the user from logging back into the EPM. In order to do that, you need to change the corporate directory account access rules defined in the **LDAP Settings** group on the Login Options page.
4. Click **Delete**.

   The EPM deletes all the selected EPM user accounts without requesting confirmation.

Using a corporate directory to specify Experience Portal users

About this task

In addition to creating user accounts through the EPM, you can also establish a link between Experience Portal and a corporate directory using Lightweight Directory Access Protocol (LDAP).

The first time users in the directory log in to the EPM, Experience Portal verifies the permissions users must have based on their directory settings. Experience Portal then creates a temporary account for those users with the appropriate user roles.

Important:

If an account with the same user name exists on both the EPM and the corporate directory, Experience Portal uses the permissions specified on the EPM account regardless of the directory settings.

Before you begin

Consult your corporate directory administrator to determine the following:

- The LDAP settings you need to use to establish a connection to the corporate directory.
- The directory structure to enter the appropriate search filters and paths.

Procedure

1. In your corporate directory, add an attribute to each record that specifies the Experience Portal permissions that the user must have.

   This attribute can specify the exact roles or be a custom group map name whose permissions you set within Experience Portal.
2. Log on to the EPM web interface by using an account with the User Manager role.
3. On the EPM main menu, click **User Management** > **Users**.
4. On the Login Options page, in the **LDAP Settings** group, enter appropriate information in the fields.
5. Click **Save**.
6. Verify that the connection is properly established by logging on to the EPM using one of the user names associated with an authorized Experience Portal group in the corporate directory.

Users page field descriptions

Use this page to add, view, or change the existing Experience Portal Manager (EPM) user accounts and global account settings. You can also delete the existing user accounts.

Column or Button	Description
Selection check box	Use this Selection check box to select which accounts you want to delete.
Name	The unique identifier for this account. This name is case-sensitive and must be unique across all EPM user accounts. **Note:** You cannot change a user name once it is created.

Table continues…

Column or Button	Description
Enable	The options are: • **Yes**: The user account is active and can be used to log into the EPM. • **No**: The user account is inactive and cannot be used to log into the EPM. **Note:** The Enable option is available to the EPM Administrator user account that is added during the EP installation and is by default set to “Yes”.
Type	The type of the user. The options are: • EP (Password): An EP Web user authenticated by a password. • EP (Certificate): An EP Web user authenticated by a certificate. • EP (Password and Certificate): An EP Web user authenticated by a password and a certificate. • LDAP: An LDAP user authenticated by an external LDAP server. • OS: A Linux OS user authenticated by the local operating system. • SMGR: A System Manager user authenticated by System Manager SSO. • EASG: An Avaya service account authenticated by EASG when EASG is enabled.
Assigned Roles/ Features	The options are: • One or more of the Experience Portal user roles. This indicates a locally-defined EPM user account or LDAP or Linux OS user. **Note:** For LDAP and Linux OS users, this field shows the roles that were assigned when the LDAP and Linux OS users login to the Experience Portal system successfully last time. • One or more of the Experience Portal features. This indicates a System Manager user Single Sign-On to EPM.
Last Login	The options are: • **Never**: No one has ever logged in with this user name. • The most recent day, date, and time that a user logged in using that account. For the current user, this column displays the day, date, and time that the user logged in to the current session. If this field displays in red, then the inactivity timeout set in the **Inactivity Lockout Threshold** field has been exceeded. Hover the mouse over any red field to see the date on which the account was last locked or unlocked.

Table continues…

Column or Button	Description
Failed Attempts	The number of failed login attempts for this user, if any. This number is reset to 0 after a successful login. If this number is greater than or equal to the value set in the **Failed Login Lockout Threshold** field, this number displays in red. Hover the mouse over any red value in this field to view the date and time of the last failed login attempt.
Locked	This field displays **(Unlock)** if the user has: • Tried to log in unsuccessfully more times than allowed in the **Failed Login Lockout Threshold** field, and the lockout duration specified in the **Failed Login Lockout Duration** field is still in effect. • Not logged in within the time period allotted in the **Inactivity Lockout Threshold** field. Click this link to unlock the account.
Password Longevity (days)	The options are: • **<The Number of Days Password Longevity is Enforced>**: The Password Longevity option is enabled for this account. Password Longevity, configured in **EPM** > **User Management** > **Login Options**, specifies the number of days for which a given password is valid. After this amount of time has passed, the user is required to change the password. **Note:** If a user has multiple roles assigned, and each role has different password longevity in terms of days, the user is warned about the expiry of the password that expires the earliest. The default is 60 days. • **Not Enforced**: The password for this account is not enforced. • **N/A**: The **Enforce Password Longevity** option is not applicable for the user of the following types. - OS - LDAP - SMGR - EP certificate user
Add	Opens the Add User page.

Table continues…

Column or Button	Description
Delete	Deletes the user accounts whose Selection check box has been checked. **Note:** If you delete a remote user account, the EPM removes it from the table in this section, but it does *not* keep the user from logging back into the EPM. To do that, you need to change the corporate directory account access rules defined in the **LDAP Settings** group. **Note:** Ensure that the user account you want to delete is not the only user account with user manager role. Without a user manager account you cannot add or change Experience Portal user accounts and will need to reinstall Experience Portal in order to create a user manager account.

Add User page field descriptions

Use this page to create a user account that can access the Experience Portal Manager (EPM) web interface.

Field	Description
Organization	The organization associated with the user you want to add. **Note:** This field is displayed only if organization level access is enabled in the Experience Portal system and you have logged in as a user not assigned to any organization. For more information on organization level access see Organization level access in.
User Name	The unique identifier for this account. This name is case-sensitive and must be unique across all EPM user accounts. Enter from 1 to 95 characters. The user name must not contain : / ! ( ) characters. **Note:** • If you select an organization in the field above, the selected organization and forward slash character are automatically prefixed to the user name. If you do not select the organization name, this indicates that the user does not belong to any organization. For more information on organization level access see Organization level access in. • Once you save the user, this name cannot be changed.

Table continues…

Field	Description
Enable	The options are: • **Yes**: The user account is active and can be used to log into the EPM. • **No**: The user account is inactive and cannot be used to log into the EPM. **Note:** The Enable option is available to the EPM Administrator user account that is added during the EP installation and is by default set to “Yes”.
Roles	Each user account can have one or more roles.
Authentication	The system displays this field only if a certificate of a type `User` is imported to the Experience Portal system and this certificate is not assigned to any Experience Portal web user. The options are: • Password • Certificate • Password and Certificate **Note:** If you select the option **Certificate**, the system does not display the **Password**, **Verify Password** and **Enforce Password Longevity** fields. The **Authentication** field is not displayed if there is no unassigned User type of trusted certificate.
Certificate Details	A list of unassigned User type of trusted certificates. This field is displayed only if unassigned User type of trusted certificate is available.
Password	The initial password for this account. The password is case-sensitive and must have at least the number of characters defined in the **Minimum Password Length** field. If you are changing the roles for an existing account but do not want to change the password, leave this field and **Verify Password** field blank. **Important:** The Experience Portal system forces the user to change the default password on first login only if you have configured the **Password Longevity** field in **EPM** > **User Management** > **Login Options**. **Note:** This field does not appear if you select the **Certificate** option in the **Authentication** field.

Table continues…

Field	Description
Verify Password	The initial password again for verification purposes. **Note:** This field does not appear if you select the **Certificate** option in the **Authentication** field.
Enforce Password Longevity	Enables the Password Longevity option for this account. Password Longevity, configured in *EPM* > *User Management* > *Login Options*, specifies the number of days for which a given password is valid. After this amount of time has passed, the user is required to change the password. If you do not select this option, the password for this account will not expire. **Note:** This field does not have any effect if the Password Longevity is not set. If this field is not checked, password change option on first login will not be enforced. This field does not appear if you select the **Certificate** option in the **Authentication** field.

Note:

For more information, see Configuring Certificate-based User Authentication.

Change User page field descriptions

Use this page to change an existing user account for the Experience Portal Manager (EPM) web interface.

Field	Description
User Name	The unique identifier for this account. This name is case-sensitive and must be unique across all EPM user accounts. **Note:** This field cannot be changed.
Enable	The options are: • **Yes**: The user account is active and can be used to log into the EPM. • **No**: The user account is inactive and cannot be used to log into the EPM. **Note:** The Enable option is available to the EPM Administrator user account that is added during the EP installation and is by default set to “Yes”.
Roles	Each user account can have one or more roles.

Table continues…

Field	Description
Authentication	The system displays this field only if a certificate of a type `User` is imported to the Experience Portal system and this certificate is not assigned to any Experience Portal web user. The options are: • Password • Certificate • Password and Certificate **Note:** If you select the option **Certificate**, the system does not display the **Password**, **Verify Password** and **Enforce Password Longevity** fields. The **Authentication** field is not displayed if there is no unassigned User type of trusted certificate.
Certificate Details	A list of unassigned User type of trusted certificates. This field is displayed only if unassigned User type of trusted certificate is available.
Created	The options are: • The date and time at which this user account was created. • **N/A** if the account creation time is not available.
Password	The password for this account. The password is case-sensitive and must satisfy the conditions defined in the **Password Settings** section in the topic Login Options page field descriptions on page 35. If you are changing the roles for an existing account but do not want to change the password, leave this field and the **Verify Password** field blank. **Important:** If you change the password, the Experience Portal system forces the user to change the password on login. **Note:** This field does not appear if you select the **Certificate** option in the **Authentication** field.
Verify Password	The password again for verification purposes. **Note:** This field does not appear if you select the **Certificate** option in the **Authentication** field.

Table continues…

Field	Description
Enforce Password Longevity	Enables the Password Longevity option for this account. Password Longevity, configured in **EPM > User Management > Login Options**, specifies the number of days for which a given password is valid. After this amount of time has passed, the user is required to change the password. If you do not select this option, the password for this account will not expire. **Note:** This field does not have any effect if the Password Longevity is not set. If this field is not checked, password change option on first login will not be enforced. This field does not appear if you select the **Certificate** option in the **Authentication** field.
Current Password	The current password field is required when administrators update their own account information. **Note:** This field does not appear if the administrator is updating other users account. This field does not appear if the administrator is the type of Certificate user.

Note:

For more details on configuring certificate-based authentication, see Configuring certificate-based user authentication on page 46.

Login Options page field descriptions

Use this page to configure security options for all user accounts.

To avoid defining the EPM users locally on the EPM, you can configure:

- An LDAP connection between a corporate directory and the EPM.
- OS user settings for authentication of local operating system users.
- System Manager Settings for Single Sign-On with System Manager.

You can choose to use any one or both of the above mentioned configurations.

User Login Options group

Field	Description
Session Timeout (minutes)	The number of minutes a user's logged in session remains active. A logged-in user's session is timed-out if the inactivity time is greater than the timeout value. The timeout value can be changed. The default is 10 minutes. Enter an integer between 5 and 60. **Note:** Once the session timeout is updated, you must restart Experience Portal Manager for the new session timeout value to take effect. You can restart the Experience Portal Manager Service using the **`command service vpms restart`** from the Linux command prompt
Failed Login Alarm Threshold (attempts)	The number of attempts users get to successfully log in to the system before the system raises an alarm. This value is usually the same as the **Failed Login Lockout Threshold (attempts)**. The default is 3. Enter an integer between 0 and 100. **Note:** To disable these alarms, set this field to `0` (zero).
Maximum Concurrent Sessions	The maximum number of concurrent logged-in active sessions allowed for the system. The default is 0. This implies there is no limitation on the number of concurrent logged in active sessions. Enter an integer between 0 and 6000. **Note:** Active sessions are orphaned when the browser closes abruptly without the user logging off. Such sessions will time-out as per the time set in the **Session Timeout** field.
Maximum Concurrent Sessions Per User	The maximum number of concurrent logged-in active sessions allowed for a user. The default is 0. This implies there is no limitation on the number of concurrent logged in active sessions for any user. Enter an integer between 0 and 600 **Note:** Active sessions are orphaned when the browser closes abruptly without the user logging off. Such sessions will time-out as per the time set in the **Session Timeout** field.
Account Lockout Settings	

Table continues…

Field	Description
Failed Login Lockout Threshold (attempts)	The number of attempts users get to successfully log in to the system. If they exceed this number of attempts, they are locked out of the system and cannot log in until the amount of time designated in the **Failed Login Lockout Duration** field has passed. The default is 3. Enter an integer between 0 and 100. **Note:** To disable the account lockout feature, set this field to `0` (zero).
Failed Login Lockout Duration (minutes)	The amount of time, in minutes, to lock out users who do not successfully log in within the number of attempts defined in the **Failed Login Lockout Threshold** field. If a user is locked out because of repeated unsuccessful login attempts, then that user cannot attempt to log in again until this amount of time has passed. The default is 10. The valid range is between 0 and 1440. • 0 - Do not lock. • -1 - Indefinite user lock out. The user remains locked until the administrator manually unlocks the user.
Inactivity Lockout Threshold (days)	The number of days to wait until Experience Portal should consider the account inactive and lock it out of the system. The inactivity counter: • Is reset to 0 each time a user logs in. • Starts counting as soon as a new account is created. Therefore, you could have an account locked out for inactivity before the first login attempt is made. • Is reset to 0 if a user manager unlocks the account, either for inactivity or for exceeding the number of failed login attempts. The default is 0, which means that accounts are never locked out regardless of how much time passes between logins. Enter an integer between 0 and 365. **Note:** This field is only used for local user accounts. Any user accounts created through a corporate directory do not expire.

Table continues…

Field	Description
Failed Login Lockout Message	The system displays the message on the login page instead of the regular login error message. This field is optional and the maximum length is of 120 characters. The following special characters are not allowed in this field: • & • < • >
Password Settings	
Minimum Password Length (characters)	The minimum number of characters users must use in setting their passwords. The default is 8 characters. The length of the password must be between 4 characters and 256 characters. **Note:** For security purposes, set this field to 8 or more characters.
Mix of Letters and Numbers	Select this option if the new password must consist of a mix of letters and numbers. This is the default selection.
Minimum Number of Each Character Type	Select this option if the new password must include a minimum number of each of the following character types: • **Uppercase Letters**: The minimum number of uppercase letters that the user must use in the new password. Enter an integer from 0 - 256, where 0 means uppercase letters are not required. • **Lowercase Letters**: The minimum number of lowercase letters that the user must use in the new password. Enter an integer from 0 - 256, where 0 means lowercase letters are not required. • **Numbers**: The minimum number of numbers that the user must use in the new password. Enter an integer from 0 - 256, where 0 means numbers are not required. • **Special Characters**: The minimum number of special characters that the user must use in the new password Enter an integer from 0 - 256, where 0 means special characters are not required. The new password can contain these special characters: `! @ # $ % ^ & * ( ) – + [ ].` **Note:** The total number of Uppercase Letters, Lowercase Letters, Numbers, and Special Characters cannot exceed the Minimum Password Length.
Enforce No Repeated and Sequential Characters	The option to enforce the new password to contain not more than three repeated or sequential letters or numbers. For example, `abcdefgh`, `12345678`, and `bbbbb`. By default, this option is selected.

Table continues…

Field	Description
Password Longevity (days)	The number of days for which a given password is valid. After this amount of time has passed, the user is required to change the password. The default is 60. Enter an integer between 0 and 365, where 0 means that passwords never expire.
Password Expiration Warning (days)	The maximum number of days before a user password expires when Experience Portal displays a message to warn the user that they need to change their password. Once this time limit has been reached, Experience Portal will display the warning message every time the user logs in until they have changed their password. The default is 10. Enter an integer between 1 and 30. **Note:** This field is ignored if **Password Longevity** is set to 0.
Maximum Password Changes in 24 Hours	The maximum password changes allowed within a 24 hour time period. The default is 3. Enter an integer between 0 and 24. The value 0 implies unlimited. **Note:** The 24–hour period is the last 24 hours from the current time. If the number of times a user has updated his password exceeds the value specified in this field, then the user is restricted from changing the password.
Maximum Password History	Determines the number of unique new passwords that are associated with a user account before an old password can be reused. The default is 12. Enter an integer between 0 and 12.
LDAP Settings	Opens the **LDAP Settings** page.
OS User Settings	Opens the **OS User Settings** page.
System Manager Settings	Opens the **System Manager Settings** page.

OS User Settings page field descriptions

Use this page to configure the parameters for OS User Settings, which enable EPM to access local Operating System user accounts.

Field	Description
Enable OS Authentication field	The options are: • **Yes:** OS authentication is enabled. • **No:** OS authentication is disabled.

Role Assignment Settings section

Field	Description

OS Group/User	The OS group name or the OS user name to associate with a given set of Avaya Experience Portal user roles.
	Note:
	• If the OS Group/User that you enter is a valid Linux user with user ID 0, the following warning message displays:
	`Warning: The specified local user ({0}) has user ID of "0" and will not be allowed to login to the EPM.`
	Where, {0} is the user ID that you have entered. For example, (root) or (root, john).
	• If the OS Group/User that you enter is not a valid Linux group or user, the following warning message displays:
	`Warning: The specified local group or user ({0}) does not exist.`
	Where, {0} is the Linux group or user that you have entered. For example, (abc) or (abc, xxx).
	This column displays the names of any previously-defined group maps as well as a text field that lets you specify a new group map name.
	If you specify a new group name, use the **Assigned Roles** field to select the roles to associate with this map name.

Assigned Roles	Displays the roles associated with the existing group maps. You can also use the check boxes to select one or more user roles to associate with a new group map name.
add link	Associates a new group map name with the selected user roles.
del link	Deletes the group map name along with the associated user roles.

View OS User Settings page field descriptions

Use this page to view the parameters for OS User Settings, which enable EPM to access local Operating System user accounts.

Field	Description
Enable OS Authentication field	The options are: • **Yes:** OS authentication is enabled. • **No:** OS authentication is disabled.

Role Assignment Settings section

Field	Description
OS Group/User	The OS group name or the OS user name to associate with a given set of Avaya Experience Portal user roles. This column displays the names of any previously-defined group maps.
Assigned Roles	The roles associated with the existing group maps.

Roles page field descriptions

Use this page to view the existing Experience Portal Manager (EPM) user roles.

You can also use this page to add a new custom role and modify an existing custom role.

Field or Button	Description
Selection check box	Use this Selection check box to select which roles you want to delete. **Note:** You cannot delete the System or Organization roles. You cannot delete Custom roles to which users are assigned.
Name	The unique identifier for the user role. **Note:** You cannot change a role name once it is created.

Table continues…

Field or Button	Description
Type	This field displays one of the following role types: • **System**: The system roles are the predefined roles. You cannot add, modify, or delete a system role. However, you can view the details of any system role. • **System (Organizations)** : The organization roles are system defined roles for the organization level access. For more information on organization level access, see Organization level access in Avaya Experience Portal on page 115and Organization level roles on page 116 • **Custom**: The custom roles are the user defined roles. You can add a new custom role and modify an existing role. **Note:** You cannot delete a custom-defined role that has a user assigned to it. Remove the role assignment from all users in order to proceed. • **Custom (Organizations)** : For custom roles for organizations, the list of roles is restricted to only organization-level roles. The feature selection web page only allows selection of features which are limited to organization users. For example, since an organization user cannot start or stop a media server, this feature is not available when defining a custom role for an organization.
Assigned To	List of users who are assigned to the corresponding role in the **Name** field.
Password Longevity (days)	The number of days for which the given password is valid for the users assigned to the role. A user can have multiple roles that have values specified either to use custom password longevity or System password longevity. The smallest value of the two values is used to determine the user password longevity. By default, the System password longevity takes precedence if a role has not been configured custom password longevity.
 **Pencil icon**	Click this icon to change the password longevity.
show	Shows all users who are assigned to the corresponding roles. **Note:** This field is displayed only if the total length of all the user names assigned to a particular role exceeds 115 characters.
hide	Shows only the first few users who are assigned to the corresponding roles. **Note:** This field is displayed only if you click **Show** to view all the users assigned to the corresponding roles.
Add	Opens the Add New Role page for the creation of a new role.

Table continues…

Field or Button	Description
Delete	Deletes the selected user roles. You can select roles using the check box next to the custom user roles. **Note:** You can only delete custom roles to which users are not assigned. If you select multiple roles to delete, only the roles that are not assigned are deleted. A warning message is shown on the page to show which roles are not deleted. For more information about deleting a user role completely, see Deleting a custom user role on page 45.

Add New Role page field descriptions

Use this page to create a new Experience Portal Manager (EPM) user roles.

Field or Button	Description
Name	The unique identifier for the user role you want to create. **Note:** You cannot create a new role with the same name as a system role.
Organization	The organization to which roles are assigned. Select **Yes** to enable the drop-down box with the list of organizations configured in the system. You can select the relevant organization from the list. **Note:** This field does not display for the Organization level roles. For more information, see Organization level roles on page 116.
Password Longevity	The number of days for which the given password is valid for a role. The options are: • **System**: The password longevity is assigned to the system role. If you select **System**, then the default range appears in the text box. The default range is 0, which means that the password never expires. • **Custom**: The password longevity is assigned to the custom role. If you select **Custom**, you can configure the number of days for password longevity. • **System (or Organization)**: The password longevity is assigned to the Organization role. This field appears only for Organization level roles. For more information, see Organization level roles on page 116.

Table continues…

Field or Button	Description
Start with Role	Existing system or custom user role names. On selecting a predefined system or custom role, the new role is created using the permissions defined for the selected role. You can modify the permissions for the new role using the Edit Role page.
Continue	Opens the Edit Role page. Use this page to modify the user role permissions.

Adding a new user role

About this task

Note:

You cannot create and add a new system user role.

Procedure

1. Log on to the EPM web interface by using an account with the User Manager role.
2. On the EPM main menu, click **User Management** > **Roles**.
3. On the Roles page, click **Add**.
4. On the Add New Role page, do the following:
   a. In the **Name** field, enter a name for the custom role that you want to add.

      The role name must have between 1 to 256 alphanumeric characters.

   b. In the **Start with Role** field, select a role.

      The privileges assigned to the role that you select in this list are used as a base for creating a new user role.

   c. Click **Continue**.

      The web interface displays the Edit Role page.
5. **(Optional)** Click the required role to give or remove permissions.

   The following indicates the status of user permissions:

   - **Red**: The user does not have permissions for the role.
   - **Green**: The user has permissions for the role.
   - **Yellow**: The user does not have permissions for a particular node under a parent node.
6. Click **Save**.

   After you save the role, you cannot change the role name.

Changing a user role

About this task

Note:

You cannot change the existing user role name.

Procedure

1. Log on to the EPM web interface by using an account with the User Manager role.
2. On the EPM main menu, click **User Management** > **Roles**.
3. On the Roles page, in the **Name** column, click the name of the role that you want to change.

   Note:

   You cannot change any of the System roles.

   The web interface displays the Edit Role page with a hierarchical list of features that are available in the Experience Portal system.
4. On the Edit Role page, select or clear the check boxes associated with the required feature node to assign privileges to access the various pages and functions of each feature.

   Note:

   Nodes that are children of a particular feature are considered its dependents. Granting access to a child node automatically grants access to the parent features.
5. Click **Save**.

Deleting a custom user role

About this task

Important:

You cannot delete a custom-defined role that has a user assigned to it. Remove the role assignment from all users before you proceed.

Procedure

1. Log on to the EPM web interface by using an account with the User Manager role.
2. On the EPM main menu, click **User Management** > **Roles**.
3. On the Roles page, do one of the following:
   - To delete individual user roles: Select the check box for the custom user role that you want to delete.

- To delete all user roles: Select the selection check box in the header row of the table, which automatically selects all user roles.

4. Click **Delete**.

   If you select multiple roles to delete, EPM deletes only the roles that are not assigned. The interface displays a warning message showing the roles that are not deleted.

Certificate-based user authentication

In earlier releases of Avaya Experience Portal, the EPM user authentication was based only on password validation. From Release 7.2, certificate-based authentication is combined with password-based authentication resulting in a two-factor authentication. This two-factor authentication is an extra layer of security that requires not only a user name and password but validates the user certificate as well.

Certificate-based authentication is available to both the EPM web user login and EPM Web Service calls. However, the authentication between VPAppLogClient component and VPAppLog Web Services in Avaya Experience Portal continues to use basic authentication.

Configuring certificate-based user authentication

The following steps describe how to configure certificate-based user authentication:

No.	Task	Description	Notes	✔
1	Create user identity certificate.	The certificate must represent a user identity. The certificate can be a self-signed certificate or signed by a third-party CA. The following certificate characteristics are preferred: • 2048-bits long public key and private key • SHA256 Signature Algorithm • X509 V3 extension— Extended Key Usage: clientAuth		

Table continues…

No.	Task	Description	Notes	✔
2	Import user identity certificate to the web browser or web service client.	**Web browser:** When accessing the EPM administration webpages through a browser, you must install and configure the client certificates on the browser. When the user tries to access the EPM webpages, the browser sends the certificates to the EPM for authentication. You must import a whole chain of certificates and the private key to the web browser. Different web browsers have different ways to import the user identity certificate. For example, Internet Explorer 11 or Chrome have a tab named Personal on the Certificates page. Firefox has a tab named Your Certificates on the Certificate Manager page. **Web service client:** When calling the EPM web services, the web service clients must send the appropriate certificates to the EPM server to use client-based authentication. To configure SSL for Axis2 web service client, see the Axis2 open sources documentation. The Application Interface test client VPAppIntfClient.sh has been enhanced to include certificate-based authentication. For more information, see the *Running the Application Interface test client VPAppIntfClient.sh* topic in the *Upgrading to Avaya Experience Portal 8.1* guide.		
3	Import user certificate to EPM.	You must select the Certificate type of User when you upload or import the user identity certificate. For more information about how to upload or import the user identity certificate, see Trusted Certificates tab on the Certificates page field descriptions on page 589.		

Table continues…

No.	Task	Description	Notes	✔
4	Configure a user for certificate-based authentication.	The administrator can select an authentication method on the enhanced Add User page and Change User page. The options are: • **Password**: To authenticate the user by password. Password Longevity applies. • **Certificate**: To authenticate the user by certificate. The administrator can select a certificate that has been imported to EPM and assign the certificate to the user. The type of user certificate cannot be shared among users. Password Longevity does not apply. • **Password and Certificate**: To authenticate the user by a two-factor authentication, password and certificate. If one factor fails, the user cannot log in to the EPM. For information about how to configure the authentication type for the user, see the online document section of Add User page field descriptions on page 31 and Change User page field descriptions on page 33.		
5	Send user identity certificate to EPM from web browser.	The EPM URL is received from the web browser. The web browser usually prompts the user to select a user identity certificate to send to EPM for authentication. If the user is configured as a Certificate type of User with a valid user identity certificate, the user will arrive at the EPM main page without needing a password. However, it is mandatory that the user is enabled and not locked. If the user is configured as a Password and Certificate type of User, and if the user identity certificate is valid, EPM presents the login page. The user must then enter valid user credentials to pass the authentication. .		

End user experience in client certificate authentication

Note the following regarding end user experience with client certificate authentication:

- The user certificate is not portable in different browsers.
- If the user wants to select a different certificate, sometimes the browser might not prompt for the selection of certificate. In such cases, the user must clear the browser cache, close the browser, and then restart the browser.
- A user might not close the browser after logging off, and clicks Refresh or enters the EPM URL. In this case, the browser sends the same certificate to Avaya Experience Portal without asking the user for certificate selection.
- If the user certificate is expired in the browser, the browser might not send the expired certificate to the EPM. In this case, the user is directed to the EPM login page. The user should contact the administrator to correct the expired certificate.
- When a Certificate type of user logs out, the user is redirected to a logout page that prompts the user to close all instances of the browser to clear any cached information.

Chapter 3: System configuration

Licenses and ports

Avaya Experience Portal licenses

The Experience Portal Manager (EPM) contacts an Avaya WebLM server on a regular basis to determine the number of licenses that are authorized for your system. For security reasons, the license server must run WebLM 7.0 or later, and a valid Avaya Experience Portal Release 8 license must be installed on the license server. You must reinstall the license file while upgrading from a previous Experience Portal version that uses older WebLM versions.

Avaya recommends the Enterprise License model when sharing a license between multiple Experience Portal systems. This configuration allows control of the licenses values and eliminates any timing related issues when multiple systems are trying to access the license server. Direct access of the license is supported only when a single Experience Portal system is accessing the license server.

After the EPM receives current information about authorized licenses, it allocates the available licenses among the servers in the system.

Experience Portal requires a license for:

Component	Description
Telephony ports	Each license authorizes you to use one port for telephony activities. **Note:** To configure an authorized telephony port on the Experience Portal system, you must establish an H.323 or SIP connection.
Automatic Speech Recognition (ASR) connections	Each license authorizes you to use one connection, or port, for speech recognition activities. If you do not purchase any ASR licenses, you cannot configure ASR servers on your system. You need one ASR proxy license for each call that requires ASR resources. The license will not become available again until the call completes.

Table continues…

Component	Description
Google Automatic Speech Recognition (ASR) connections	Each license authorizes you to use one connection for Google Speech Recognition engine. If you do not purchase any Google ASR licenses, you will not be able to use any configured Google ASR servers on your system. **Note:** Google Speech Recognition engine is also referred to as Google Cloud Speech-to-Text which is a cloud-based speech transcription service that transcribes speech into text. For more details, see Google Speech recognition on page 350.
Text-to-Speech (TTS) connections	Each license authorizes you to use one connection, or port, for speech synthesis activities. If you do not purchase any TTS licenses, you cannot configure TTS servers on your system. You need one TTS proxy license while a call is using TTS resources. As soon as the call stops using TTS resources, the license becomes available to other calls.
Google Dialogflow Connections	Each license authorizes you to use one connection for Google Dialogflow service. If you do not purchase any Google Dialogflow licenses, you will not be able to use any configured Google Dialogflow servers on your system. For more information, see Google Dialogflow on page 353.
Call Anchoring Ports	The number of Call Anchoring Ports on your system. This setting is the maximum number of calls which can be simultaneously anchored at any given time.
Zones	You need these licenses for configuring zones in the system. If the value is non-zero (positive), the zone feature is enabled. If the value is zero, the zone feature is disabled.
Email units	You need these licenses for configuring email resources (email processors and email connections) The licenses features for email units provides the ability to charge customers according to the capacity required.
SMS units	You need these licenses for configuring SMS resources (SMS processors and SMPP/HTTP connections). The licenses features for SMS units provides the ability to charge customers according to the capacity required.
HTML Units	The number represents the daily HTML processing capacity on your system. An HTML unit is required to handle an incoming HTML request.

Viewing your licenses

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM main menu, click **Security** > **Licensing**.

EPM displays one of the following pages:

- The Licensing page, if you are authorized to change the license information.
- The View Licensing page.

Configuring the connection to the Avaya license server

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **Security** > **Licensing**.
3. In the **License Server URL** field, click the editing tool ( ) .

   The web interface displays the License Server URL page.
4. In the **License Server URL** field, enter the new URL.

   The URL must be in the format `https://<WebLM-machine>:port/WebLM/LicenseServer`, where *<Weblm-machine>* is the hostname or IP address of the WebLM server and *:port* consists of a colon followed by the port number for the WebLM server. If WebLM uses the default configuration, specify `:52233`.
5. Click **Verify** to ensure that the URL is correct.
6. If your system can connect to the Avaya license server, click **Apply** > **OK** to confirm.

   Experience Portal immediately polls the Avaya WebLM server to retrieve the current license information and, if successful, updates the fields on the Licensing page.

Updating license information manually

About this task

If the license information changes on the WebLM server, it can take up to 10 minutes before Experience Portal polls that server and is informed of the changes. If you do not want to wait, you can make Experience Portal poll the license server immediately.

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **Security** > **Licensing**.
3. In the **License Server URL** field, click the editing tool ( ).

   The web interface displays the License Server URL page.
4. Click **Save**.

   Experience Portal polls the license server immediately even if no changes are made on the page.

Licensing page field descriptions

Use this page to:

- View the number of licenses currently available on the Experience Portal system.
- View the URL that links Experience Portal to the Avaya WebLM license server.
- Verify that the connection to the WebLM license server is valid.
- View the number of licenses currently available on the managed application installed on Experience Portal.

Note:

You can view the managed application license details only if you have installed a managed application on Experience Portal. For more information on the fields related to the managed application, see the documentation delivered with the respective managed application.

Important:

Experience Portal requires a valid license from Avaya. If this system is currently operating with an invalid license, a message is displayed in red stating the problem and when the grace period expires. If you do not replace the license within that time, Experience Portal sets all the acquired licenses to 0 (zero) and cannot handle any inbound or outbound calls.

This page contains the:

- License Server Information section on page 53
- Licensed Products section on page 54

License Server Information section

Field	Description
License Server URL	The complete URL to the Avaya WebLM license server that is currently in use.
Last Updated	The last successful time that the License Server URL was changed.
Last Contacted	The last time that the communication with the license server was attempted. **Note:** This field is displayed only if the server was never able to successfully poll the license server.
Last Successful Poll	The last successful time that the licenses were acquired from the license server.
License Server Information icon 	Opens the License Server URL page for updating the license server URL.

Licensed Products section

Field or Button	Description
Announcement Ports	The number of Announcement Ports licenses on your system. The system requires an announcement port license to handle calls that do not require DTMF processing and/or ASR and TTS capability.
ASR Connections	The number of Automated Speech Response (ASR) licenses on your system. ASR technology enables an interactive voice response (IVR) system to collect verbal responses from callers. This setting is the maximum number of MRCP connections to ASR servers that can be active at any one time.
Call Anchoring Ports	The number of Call Anchoring Ports on your system. This setting is the maximum number of calls which can be simultaneously anchored at any given time.
Email Units	The number represents the email processing capacity that is on your system. If the value is non-zero (positive), the email feature is enabled. If the value is zero, the email feature is disabled. **Note:** This feature is not required for using generation of email for reports and alarms.
Enable Media Encryption	Indicates if Media Encryption is enabled on your system. Media Encryption provides data security. If the value is a non-zero (positive) number, the media encryption is enabled. If it is zero, media encryption is disabled.
Enhanced Call Classification	The number of enhanced call classification licenses on your system. Enhanced Call Classification licenses on the Experience Portal system provide the functionality to differentiate between human and answering machine responses to outbound calls. If the value is a non-zero (positive) number, the enhanced call classification is enabled. If the value is zero, the enhanced call classification feature is disabled.
Google ASR Connections	The number of Google Automated Speech Response (ASR) licenses on your system. This setting is the maximum number of simultaneous connections to Google ASR servers that can be active at any one time.

Table continues…

Field or Button	Description
Google Dialogflow Connections	The number of Google Dialogflow licenses on your system. This setting is the maximum number of simultaneous connections to Google Dialogflow servers that can be active at any given time.
HTML Units	The number represents the daily HTML processing capacity on your system. An HTML unit is required to handle an incoming HTML request.
SIP Signaling Connections	The number of SIP Signaling connections licenses on your system. The system requires a SIP Signaling Connection to handle calls that do not require media (that is no RTP stream is created). **Note:** The maximum number of SIP Signaling Connections used by the system can not be greater than the sum of the Telephony Ports and Announcement Ports.
SMS Units	The number represents the SMS processing capacity that is on your system. If the value is non-zero (positive), the SMS feature is enabled. If the value is zero, the SMS feature is disabled.
Telephony Ports	The number of Telephony Ports licenses on your system. The system requires a telephony port license to handle calls that require DTMF processing and/or ASR capability and TTS capability.
TTS Connections	The number of Text-to-Speech (TTS) licenses on your system. TTS technology enables an IVR system to render text content into synthesized speech output according to algorithms within the TTS software This setting is the maximum number of MRCP connections to TTS servers that can be active at any one time.
Video Server Connections	Specifies the maximum number of video connections to the video servers on the MPP. Enter `0` (zero) to disable the video feature.
Zones	The number represents whether the Zone feature is enabled for the system or not. If the value is non-zero (positive), the zone feature is enabled. If the value is zero, the zone feature is disabled.
Version	The version number of the license.
Expiration Date	The date when the license expires.

Table continues…

Field or Button	Description
Last Contacted	The last time that the license server was contacted for acquiring licenses. **Note:** This field is displayed only if the server was never able to successfully acquire licenses.
Last Successful Poll	The last successful time that the licenses were acquired from the license server.
Last Changed	The last successful time that the licenses were different on the license server.
Avaya Experience Portal icon	Opens the Avaya Experience Portal License Settings page for updating the license settings.
Allocations button	Opens the Allocations page for displaying the H.323 and SIP ports configured and licensed for the system.

Allocations page field descriptions

This page displays the H.323 and SIP resources that are configured, licensed, and allocated for the system. To accept or initiate a call, a resource must be configured, licensed, and allocated.

Field	Description
Zones	The zones to which telephony resources are allocated. **Note:** This field is displayed only if zones are configured in the system.
Type	The VoIP connection types that are configured and licensed for the system. The options are: • H.323 • SIP
Configured	The number of resources that are configured on the **H.323 Connection** or **SIP Connection** pages.
Licensed	The number of telephony resources that are licensed by WebLM. If the total number of telephony ports, including announcement ports, specified by the license is sufficient, then all configured VoIP resources are licensed. In this case the value shown in the **Licensed** column matches the value shown in the **Configured** column. If the licensed resources are not sufficient, then the licenses are distributed proportionally based on the number of VoIP resources configured. Configured VoIP resources above what is licensed will not be used.

Table continues…

Field	Description
Allocated	The number of telephony resources that are allocated to media servers. If the total capacity of the media servers is sufficient, then all licensed VoIP resources are allocated to media servers. In this case, the value shown in the **Allocated** column matches the value shown in the **Licensed** column. If the capacity of the media servers is not sufficient, the allocated value is reduced. The Allocated resource cannot exceed the capacity of the media servers. If both H.323 and SIP are configured, then they are reduced in proportion to the licensed value. Licensed VoIP resources for which no media server is available will not be used.
Details link icon 	The details link (zoom lens icon) displays additional information for SIP allocations.
 **Zones** filter icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The system displays the **Zones** filter icon only when you create new zones. If you do not create any new zones, you do not see the icon.

License Server URL page field descriptions

Use this page to:

- Update the license server URL
- Access the License Administration page for the WebLM server

Column or Button	Description
License Server URL	The complete URL to the Avaya WebLM license server. The URL must be in the format `https://<WebLM-machine>:port/WebLM/LicenseServer`, where `<Weblm-machine>` is the hostname or IP address of the WebLM server and `:port` consists of a colon followed by the port number for the WebLM server. If WebLM uses the default configuration, specify `:52233`. **Note:** Unless your site uses a dedicated WebLM server machine, the WebLM server is installed on the Experience Portal EPM server.

Table continues…

Column or Button	Description
Verify	Opens a new browser window and loads the License Administration page for the WebLM license server. If this page loads properly, then Experience Portal can connect to the license server.

Avaya Experience Portal License Settings page field descriptions

Use this page to update the license settings.

Column or Button	Description
Announcement Ports	Specify the minimum and maximum number of licenses. • Minimum: Indicates the minimum number of licenses below which the Experience Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 50,000. • Maximum: Indicates the maximum number of licenses to be retrieved by EPM for that feature. Enter a value in the range 0 to 50,000.
ASR Connections	Specify the minimum and maximum number of licenses. • Minimum: Indicates the minimum number of licenses below which the Experience Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 50,000. • Maximum: Indicates the maximum number of licenses to be retrieved by EPM for that feature. Enter a value in the range 0 to 50,000.

Table continues…

Column or Button	Description
Call Anchoring Ports	Specify the minimum and maximum number of licenses. • Minimum: Indicates the minimum number of licenses below which the Experience Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 50,000. • Maximum: Indicates the maximum number of licenses to be retrieved by EPM for that feature. Enter a value in the range 0 to 50,000.
Email Units	Specify the minimum and maximum number of licenses. • Minimum: Indicates the minimum number of licenses below which the Experience Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 5,000. • Maximum: Indicates the maximum number of licenses to be retrieved by EPM for that feature. Enter a value in the range 0 to 5,000.
Google ASR Connections	Specify the minimum and maximum number of licenses. • Minimum: Indicates the minimum number of licenses below which the Experience Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 50,000. • Maximum: Indicates the maximum number of licenses to be retrieved by EPM for that feature. Enter a value in the range 0 to 50,000.

Table continues…

Column or Button	Description
Google Dialogflow Connections	Specify the minimum and maximum number of licenses. • Minimum: Indicates the minimum number of licenses below which the Experience Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 50,000. • Maximum: Indicates the maximum number of licenses to be retrieved by EPM for that feature. Enter a value in the range 0 to 50,000.
HTML Units	Specify the minimum and maximum number of licenses. • Minimum: Indicates the minimum number of licenses below which the Experience Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 1,000,000. • Maximum: Indicates the maximum number of licenses to be retrieved by EPM for that feature. Enter a value in the range 0 to 1,000,000.
SIP Signaling Connections	Specify the minimum and maximum number of licenses. • Minimum: Indicates the minimum number of licenses below which the Experience Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 50,000. • Maximum: Indicates the maximum number of licenses to be retrieved by EPM for that feature. Enter a value in the range 0 to 50,000. **Note:** The maximum number of SIP Signaling Connections used by the system can not be greater than the sum of the Telephony Ports and Announcement Ports.

Table continues…

Column or Button	Description
SMS Units	Specify the minimum and maximum number of licenses. • Minimum: Indicates the minimum number of licenses below which the Experience Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 5,000. • Maximum: Indicates the maximum number of licenses to be retrieved by EPM for that feature. Enter a value in the range 0 to 5,000.
Telephony Ports	Specify the minimum and maximum number of licenses. • Minimum: Indicates the minimum number of licenses below which the Experience Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 50,000. • Maximum: Indicates the maximum number of licenses to be retrieved by EPM for that feature. Enter a value in the range 0 to 50,000.
TTS Connections	Specify the minimum and maximum number of licenses. • Minimum: Indicates the minimum number of licenses below which the Experience Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 50,000. • Maximum: Indicates the maximum number of licenses to be retrieved by EPM for that feature. Enter a value in the range 0 to 50,000.

Viewing telephony port distribution

About this task

Experience Portal automatically distributes telephony ports across all Media Processing Platform (MPP) servers.

Procedure

1. Log on to the EPM web interface by using an account with one of the following roles:
   - Administration
   - Operations
   - Maintenance
2. On the EPM main menu, click **Real-time Monitoring** > **Port Distribution**.
3. On the Port Distribution page, in the **Servers** field, select the relevant MPP server.
4. On the Port Distribution Report page, in the **Port** column, click a port number to view more information about a particular port.

   EPM displays the Port Information window.

Telephony port states

State	Description
Active	The port has been assigned to an MPP but the MPP does not know the status of the port because the EPM and the MPP are out of sync.
Adding	The port has been assigned to an MPP but the MPP has not taken the port yet.
Alerting	The port is ringing and checking resources.
Available	The port is ready to be assigned to an MPP.
Connected	The port is in service and calls are in progress.
Delete	The port is in the process of being deleted from the system, but there is a call in progress. The port will stay in use until the call ends or the grace period expires, whichever comes first. For more information, see Setting the global grace period and trace level parameters on page 271.
Idle	The port is assigned to an MPP but the MPP is not registered with the switch. The port cannot take calls.
In Service	The port is assigned to an MPP and the MPP is registered with the switch. The port is ready to take a call.
None	The assigned port is missing.
Out of Service - Fault	The MPP is trying to register with the port.
Out of Service - Manual	The port is being manually taken offline from the MPP.
Proceeding	The port was taken offline but is currently coming back into service.
Removing	The port is being deleted from the MPP. It will soon be available for assignment to another MPP.
Trying	The MPP is trying to register with the port.

Port Distribution page field descriptions

Use this page to specify the filter criteria for the Port Distribution report.

Name	Description
Zones	The <Default> zone exists by default. The Zones drop-down box appears only when you create new zones, apart from the already existing <Default> zone. Select the name of the zone from the drop-down box. You can filter the records based on the zone that you select. **Note:** The **Zones** drop-down box appears only when you create new zones. If you do not create any new zones, you do not see the drop-down box. You can see only the <Default> zone.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones and for setting the time zone display. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
Servers	The MPP servers that are configured on the system for the selected zone. **Note:** If no servers are configured for the selected zone, then the drop-down box only shows the **All Servers** option.

Port Distribution Report page field descriptions

Use this page for a real-time view of telephony port distribution across all Media Processing Platform (MPP) servers. You can configure the telephony resources on the VoIP Connections page.

Note:

If there is a port conflict, the text for a particular port appears in red. For more information, see the **Current Allocation** column.

Column	Description
Zone	The name of the zone within which the MPP server is configured.

Table continues…

Column	Description
Servers	The MPP servers for which you want to see the Port Distribution Report. **Note:** This field appears only if you have selected one or more servers from the **Port Distribution** page. If you select **All Servers** from the **Servers** list on the **Port Distribution** page, the system does not display this field.
Port	The Experience Portal port number associated with the port. **Note:** The port distribution report for SIP protocol displays only the highest port distribution record. For detailed port information, click the number of the port to access the Port Information window. Click the **Up** arrow in the column header to sort the ports in ascending order and the **Down** arrow to sort the ports in descending order.
Mode	The operational mode of the port. The options are: • **Online**: The port is available for normal inbound and outbound calls and is allocated to an MPP. • **Inbound**: The port is available for normal inbound calls and is allocated to an MPP. • **Test**: The port is available for calls made to one of the defined H.323 maintenance stations and is allocated to an MPP in Test mode. • **Offline**: The port is not available and is not allocated to any MPP. Click the **Up** arrow in the column header to sort the modes in ascending order and the **Down** arrow to sort the modes in descending order

Table continues…

Column	Description
State	The state of the port. The options are: • **Active:** The port has been assigned to an MPP but the MPP does not know the status of the port because the EPM and the MPP are out of sync. • **Adding:** The port has been assigned to an MPP but the MPP has not taken the port yet. • **Alerting:** The port is ringing and checking resources. • **Available:** The port is ready to be assigned to an MPP. • **Connected:** The port is in service and calls are in progress. • **Delete:** The port is in the process of being deleted from the system. It is in use until the grace period expires. • **Idle:** The port is assigned to an MPP but the MPP is not registered with the switch. The port cannot take calls. • **In Service:** The port is assigned to an MPP and the MPP is registered with the switch. The port is ready to take a call. • **None:** The assigned port is missing. • **Out of Service - Fault:** The MPP is trying to register with the port. • **Out of Service - Manual:** The port is manually taken offline from the MPP. • **Proceeding:** The port was taken offline but is currently coming back into service. • **Removing:** The port is being deleted from the MPP. It will soon be available for assignment to another MPP. • **Trying:** The MPP is trying to register with the port. **Tip:** You can hover the mouse over this column to view more information about the state, including any fault information if the port could not be registered.
Port Group	The name of the port group that the port belongs to. Port groups are administered on the System Configuration pages. Click the **Up** arrow in the column header to sort the groups in ascending order and the **Down** arrow to sort the groups in descending order
Protocol	The port protocol. **Note:** The port distribution data for SIP is consolidated to a single line in each MPP. The port distribution report for SIP protocol displays only the highest port distribution record. Click the **Up** arrow in the column header to sort the protocols in ascending order and the **Down** arrow to sort the protocols in descending order.

Table continues…

Column	Description
Current Allocation	The name of the MPP to which the port is currently allocated. If there is a port conflict, you can hover the mouse over this field to view a tooltip containing one of the following error messages: • Unconfigured port currently owned by *<MPP Name>*. • Port allocated to *<MPP1 Name>* but currently owned by *<MPP2 Name>*. • Port not yet allocated but owned by *<MPP Name>*. • Port allocated to *<MPP Name>* but not owned by it. • Port allocation not yet sent. • Waiting for confirmation of the port allocation.
Base Allocation	The options are: • " " (blank): The port is currently allocated to the optimal MPP. • An MPP name: The optimal allocation for the port. If the base allocation field is not blank, it probably means that the optimal MPP went out of service and the port was reallocated.

Port Information window field descriptions

Use this window to view detailed information about an Experience Portal telephony port.

This window contains the:

- Details group on page 66
- Status group on page 67
- Allocation group on page 68

Details group

Field	Description
Port	The Experience Portal port number associated with the port. **Note:** The port information for SIP displays a range from 1 to the port number of the selected port.
Port Group	The name of the port group that the port belongs to.
Gatekeeper	The IP address of the H.323 Gatekeeper.
Gatekeeper Port	The port number of the H.323 Gatekeeper port.

Status group

Field	Description
State	The state of the port. The options are: • **Active:** The port has been assigned to an MPP but the MPP does not know the status of the port because the EPM and the MPP are out of sync. • **Adding:** The port has been assigned to an MPP but the MPP has not taken the port yet. • **Alerting:** The port is ringing and checking resources. • **Available:** The port is ready to be assigned to an MPP. • **Connected:** The port is in service and calls are in progress. • **Delete:** The port is in the process of being deleted from the system. It is in use until the grace period expires. • **Idle:** The port is assigned to an MPP but the MPP is not registered with the switch. The port cannot take calls. • **In Service:** The port is assigned to an MPP and the MPP is registered with the switch. The port is ready to take a call. • **None:** The assigned port is missing. • **Out of Service - Fault:** The MPP is trying to register with the port. • **Out of Service - Manual:** The port is manually taken offline from the MPP. • **Proceeding:** The port was taken offline but is currently coming back into service. • **Removing:** The port is being deleted from the MPP. It will soon be available for assignment to another MPP. • **Trying:** The MPP is trying to register with the port.
Fault Code and Reason	If this port encountered a fault condition, this will be **PTELE00031 - Channel Out of Service**. Hover the mouse over this field to display the reason provided to Experience Portal by the switch.
Call Type	If the port is currently being used, displays the type of call that is currently using the port.
Mode	The operational mode of the port. The options are: • **Online**: The port is available for normal inbound and outbound calls and is allocated to an MPP. • **Inbound**: The port is available for normal inbound calls and is allocated to an MPP. • **Test**: The port is available for calls made to one of the defined H.323 maintenance stations and is allocated to an MPP in Test mode. • **Offline**: The port is not available and is not allocated to any MPP.

Allocation group

Field	Description
Current Allocation	The options are: • **<None>**: The port is not currently allocated to an MPP. • The name of the MPP to which the port is currently allocated along with any error messages that may have been generated by port conflicts.
Base Allocation	The options are: • " " (blank): The port is currently allocated to the optimal MPP. • An MPP name: The optimal allocation for the port. If the base allocation field is not blank, it probably means that the optimal MPP went out of service and the port was reallocated.

VoIP connections

H.323 connections in Experience Portal

H.323 is an Internet standard set of protocols for the transmission of real-time audio, video, and data using packet-switching technology. Experience Portal uses H.323 connections with an Communication Manager to handle Voice over IP (VoIP) telephony.

To provide VoIP capabilities, H.323 uses:

- Terminals, which can be PCs or dedicated IP softphone devices.
- Gateways, which “translate” communications between dissimilar networks, such as IP networks and Public Switched Telephone Network (PSTN). In the Experience Portal system, the Communication Manager handles this function.
- A gatekeeper, which acts as the control center for all H.323 VoIP interactions in the system. In the Experience Portal system, the Communication Manager handles this function.

Important:

You must use Communication Manager 3.1 build 369 or later with the Avaya Special Application SA8874 feature. This combination provides:

- VoiceXML supervised transfers. Without the SA8874 feature, supervised transfers have no access to call progress information and behave like a blind transfer.
- The Application Interface web service for outbound calling. Without the SA8874 feature, the web service has no access to call progress information and may start a VoiceXML application even when the connection attempt receives a busy signal.

Note:

The SA8874 feature comes with Communication Manager version 3.1 or later, but it requires a separate license before it can be enabled.

Viewing existing H.323 connections

Procedure

1. Log on to the EPM web interface by using an account with one of the following roles:
   - Administration
   - Operations
   - Maintenance
2. On the EPM main menu, click **System Configuration** > **VoIP Connections**.
3. On the VoIP Connections page, click the H.323 tab.

   EPM displays the list of existing H.323 connections. On this page, authorized users can also add, delete, or change H.323 connections.

Adding an H.323 connection

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **System Configuration** > **VoIP Connections**.
3. On the VoIP Connections page, click the H.323 tab.
4. Click **Add**
5. On the Add H.323 Connection page, enter appropriate information, and click **Save**.

Changing an H.323 connection

Procedure

1. Log on to the EPM web interface by using an account with the Administration role.
2. On the EPM main menu, click **System Configuration** > **VoIP Connections**.
3. On the VoIP Connections page, click the H.323 tab.
4. In the **Name** column, click the name of the connection that you want to change.
5. On the Change H.323 Connection page, enter appropriate information and click **Save**.

Defining maintenance stations for an H.323 connection

About this task

With maintenance stations, you can isolate call activity to an MPP running in the Test operational mode.

Experience Portal creates a port running in Test mode for each defined maintenance station. It then assigns one of those ports to an MPP when it enters Test mode.

If you have:

- More Test mode ports than MPPs in Test mode: Each Test mode MPP is assigned one port and the extra ports are ignored.
- More MPPs in Test mode than Test mode ports: Experience Portal randomly distributes the available ports to a subset of the MPPs in Test mode.

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **System Configuration** > **VoIP Connections**.
3. On the VoIP Connections page, click the H.323 tab.
4. To create a new connection, do the following:
   a. Click **Add**.
   b. On the Add H.323 Connection page, enter the required information in the General section, and click **Save**.
5. To add one or more maintenance stations to an existing connection, click the name of the connection in the **Name** column.

   The EPM displays the Change H.323 Connection page.
6. In the **New Stations** section, do the following:
   a. In the **Station** field, do the following:
      - In the **From** field, type the first maintenance station number.
      - To specify a range of numbers, in the **To** field, type the last number in the range.
   b. In the **Password** field, type a password.
   c. In the **Station Type** field, select **Maintenance**.
   d. Click **Add**.
7. **(Optional)** If you want to define another maintenance station or a range of numbers, repeat Step 6.
8. Click **Save**.

Deleting H.323 connections

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **System Configuration** > **VoIP Connections**.
3. On the VoIP Connections page, click the H.323 tab, and do the following:
   - To delete connections individually: Select the check box for the connection name that you want to delete.
   - To delete all connections: Select the selection check box in the header row of the table, which automatically selects all connections.

4. Click **Delete**.

Add H.323 Connection page field descriptions

Use this page to add a new H.323 connection to the Experience Portal system.

This page contains the:

General section

Field	Description
Zone	The name of the zone where the H.323 connection is configured. Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only if you have created zones on your Experience Portal system. If you do not create any new zones, you do not see the drop-down box.
Name	The unique identifier for this H.323 connection on the Experience Portal system. The name can be up to 32 alphanumeric characters. Do not use any special characters. **Note:** Once you save the H.323 connection, this name cannot be changed.
Enable	Whether this H.323 connection is available for use by the Experience Portal system. The default is **Yes**, which means the connection is available.
Gatekeeper Address	The network address of the H.323 gatekeeper. The gatekeeper resides on the Communication Manager and acts as the control center for all H.323 VoIP interactions in the Experience Portal system. This must be a valid network address in the form of a fully qualified hostname or an IP address.
Alternative Gatekeeper Address	The network address of the alternate H.323 gatekeeper that resides on Communication Manager. The Gatekeeper address and the Alternate Gatekeeper Address are used for initial contact with Communication Manager, and Communication Manager can instruct the media manager to use other addresses for further communications. For more information on the alternate H.323 gatekeeper, refer to *Avaya Aura® Communication Manager Feature Description and Implementation* on http://support.avaya.com. This must be a valid network address in the form of a fully qualified hostname or an IP address.
Gatekeeper Port	The port on the gatekeeper that Experience Portal uses for this connection. This value must be in the range from 1024 to 65535. The default port is 1719.

Table continues…

Field	Description
Media Encryption	The options are: • **Yes**: Experience Portal encrypts all calls that use this connection. This is the default. • **No**: Calls are not encrypted. **Note:** The use of encryption can affect system performance, especially if you are using the connection for a large number of simultaneous calls.

New Stations group

Field or Button	Description
Station	The stations to use for this H.323 connection. These stations represent the telephone numbers or extensions that can use this H.323 connection for VoIP calls. The options are: • A single station. Enter the station number in the **From** field. • A range of stations. Enter the lowest number of the range in the **From** field, and the highest number of the range in the **To** field. When you specify the stations, keep in mind that: • Each station can be a maximum of 15 digits in length. • This station or range of stations must be unique. That is, you cannot assign the same stations or an overlapping range of stations to different H.323 connections. • The total number of stations you enter cannot exceed the number of Experience Portal ports you have licensed. For more information on the number of available licenses, see Viewing your licenses on page 51.
Password	The numeric password to be associated with either the first station or all stations. The H.323 gatekeeper uses passwords as an extra measure of security when using the stations on this connection. The password can be a maximum of 8 digits in length.
Password type radio buttons	The options are: • **Same Password**: Experience Portal uses the password specified in the **Password** field for all stations in the specified range. • **Use sequential passwords**: Experience Portal uses the password specified in the **Password** field for the first station in the specified range. The system automatically increments this base password by one for each of the other stations in the specified range.

Table continues…

Field or Button	Description
Station Type	The options are: • **Inbound and Outbound**: The specified stations can be used for inbound or outbound calls. • **Inbound Only**: The specified stations can be used for inbound calls only. • **Maintenance**: The specified stations are special numbers that you can configure on the switch and on the MPP for use in troubleshooting problems with the MPP. Maintenance stations make it possible to isolate a single MPP for troubleshooting purposes in multiple-MPP systems. For more information, see Using the Test operational mode on page 291. **Note:** If you select **Maintenance**: • Experience Portal only allocates one maintenance port to each MPP that is currently in Test mode. Therefore, specifying a range of stations is only useful if you put several MPPs into Test mode at the same time.
Add	Associates the station or range of stations with the connection.

Configured Stations group

Field or Button	Description
Display text box	The stations that can use this H.323 connection. If an entry is followed by: • **(I)**: the stations are inbound only. • **(M)**: the stations are maintenance stations. • " " (blank), the stations are both inbound and outbound. Select an individual entry in this list by clicking on it, or use `Ctrl+Click` and `Shift +Click` to select multiple entries.
Remove	Removes the selected entries from the list of Configured Stations.

Change H.323 Connection page field descriptions

Use this page to change an existing H.323 connection.

This page contains the:

General section

Field	Description
Zone	The name of the zone where the H.323 connection is configured. Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only if you have created zones on your Experience Portal system. If you do not create any new zones, you do not see the drop-down box.
Name	The unique identifier for this H.323 connection on the Experience Portal system. **Note:** This field cannot be changed.
Enable	Whether this H.323 connection is available for use by the Experience Portal system. The default is **Yes**, which means the connection is available.
Gatekeeper Address	The network address of the H.323 gatekeeper. The gatekeeper resides on the Communication Manager and acts as the control center for all H.323 VoIP interactions in the Experience Portal system. This must be a valid network address in the form of a fully qualified hostname or an IP address.
Alternative Gatekeeper Address	The network address of the alternate H.323 gatekeeper that resides on Communication Manager. The Gatekeeper address and the Alternate Gatekeeper Address are used for initial contact with Communication Manager, and Communication Manager can instruct the media manager to use other addresses for further communications. For more information on the alternate H.323 gatekeeper, refer to *Avaya Aura® Communication Manager Feature Description and Implementation* on http://support.avaya.com. This must be a valid network address in the form of a fully qualified hostname or an IP address.
Gatekeeper Port	The port on the gatekeeper that Experience Portal uses for this connection. This value must be in the range from 1024 to 65535. The default port is 1719.
Media Encryption	The options are: • **Yes**: Experience Portal encrypts all calls that use this connection. This is the default. • **No**: Calls are not encrypted. **Note:** The use of encryption can affect system performance, especially if you are using the connection for a large number of simultaneous calls.

New Stations group

Field or Button	Description
Station	The stations to use for this H.323 connection. These stations represent the telephone numbers or extensions that can use this H.323 connection for VoIP calls. The options are: • A single station. Enter the station number in the **From** field. • A range of stations. Enter the lowest number of the range in the **From** field, and the highest number of the range in the **To** field. When you specify the stations, keep in mind that: • Each station can be a maximum of 15 digits in length. • This station or range of stations must be unique. That is, you cannot assign the same stations or an overlapping range of stations to different H.323 connections. • The total number of stations you enter cannot exceed the number of Experience Portal ports you have licensed. For more information on the number of available licenses, see Viewing your licenses on page 51.
Password	The numeric password to be associated with either the first station or all stations. The H.323 gatekeeper uses passwords as an extra measure of security when using the stations on this connection. The password can be a maximum of 8 digits in length.
Password type radio buttons	The options are: • **Same Password**: Experience Portal uses the password specified in the **Password** field for all stations in the specified range. • **Use sequential passwords**: Experience Portal uses the password specified in the **Password** field for the first station in the specified range. The system automatically increments this base password by one for each of the other stations in the specified range.

Table continues…

Field or Button	Description
Station Type	The options are: • **Inbound and Outbound**: The specified stations can be used for inbound or outbound calls. • **Inbound Only**: The specified stations can be used for inbound calls only. • **Maintenance**: The specified stations are special numbers that you can configure on the switch and on the MPP for use in troubleshooting problems with the MPP. Maintenance stations make it possible to isolate a single MPP for troubleshooting purposes in multiple-MPP systems. For more information, see Using the Test operational mode on page 291. **Note:** If you select **Maintenance**: • Experience Portal only allocates one maintenance port to each MPP that is currently in Test mode. Therefore, specifying a range of stations is only useful if you put several MPPs into Test mode at the same time.
Add	Associates the station or range of stations with the connection.

Configured Stations group

Field or Button	Description
Display text box	The stations that can use this H.323 connection. If an entry is followed by: • **(I)**: the stations are inbound only. • **(M)**: the stations are maintenance stations. • " " (blank), the stations are both inbound and outbound. Select an individual entry in this list by clicking on it, or use `Ctrl+Click` and `Shift +Click` to select multiple entries.
Remove	Removes the selected entries from the list of Configured Stations.

H.323 tab on the VoIP Connections page field descriptions

Use this tab to view, add, or change H.323 connections on the Experience Portal system.

Tip:

To sort the connections by any column, click the up arrow (sort ascending) or down arrow (sort descending) in the column header.

Column or Button	Description
Selection check box	Use this Selection check box to select which connections you want to delete.

Table continues…

Column or Button	Description
Zone	The name of the zone where the H.323 connection is configured.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
Name	The unique identifier for this H.323 connection on the Experience Portal system. Click the name to open the Change H.323 Connection page.
Enable	The options are: • **Yes**: This connection is available for use by the Experience Portal system. • **No**: This connection is disabled.
Gatekeeper Address	The network address of the H.323 gatekeeper. The gatekeeper resides on the Communication Manager and acts as the control center for all H.323 VoIP interactions in the Experience Portal system.
Alternative Gatekeeper Address	The network address of the alternate H.323 gatekeeper that resides on Communication Manager. The Gatekeeper address and the Alternate Gatekeeper Address are used for initial contact with Communication Manager, and Communication Manager can instruct the media manager to use other addresses for further communications. For more information on the alternate H.323 gatekeeper, refer to *Avaya Aura® Communication Manager Feature Description and Implementation* on http://support.avaya.com.
Gatekeeper Port	The port on the gatekeeper that Experience Portal uses for this connection.
Stations	The stations that can use this H.323 connection. If an entry is followed by: • **(I)**: the stations are inbound only. • **(M)**: the stations are maintenance stations. • " " (blank), the stations are both inbound and outbound.
Media Encryption	If this field displays **Yes**, Experience Portal encrypts all calls that use this connection.
Add	Opens the Add H.323 Connection page.
Delete	Deletes the H.323 connections whose associated Selection check box is checked.

SIP connections in Experience Portal

Session Initiation Protocol (SIP) is an IP telephony signaling protocol developed by the IETF. Primarily used for Voice over Internet Protocol (VoIP) calls, SIP can also be used for video or any media type.

SIP is a text-based protocol that is based on HTTP and MIME, which makes it suitable and very flexible for integrated voice-data applications. SIP is designed for real time transmission, uses

fewer resources and is considerably less complex than H.323. Its addressing scheme uses URLs and is human readable; for example: `sip:john.doe@company.com`.

SIP relies on the Session Description Protocol (SDP) for session description and the Real-time Transport Protocol (RTP) for actual transport.

You can configure the Experience Portal SIP connection as either a TCP connection or a TLS connection. The Avaya Aura®Session Manager (ASM) is used as the SIP proxy when configuring Experience Portal to use SIP. For more information on SIP integration with Experience Portal and ASM, see *Application Notes for Avaya Experience Portal, Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Acme Packet Net-Net 6.2.0 with AT&T IP Toll Free Service using MIS/PNT or AVPN Transport – Issue 1.0* on the Avaya online support Web site, http://support.avaya.com.

Note:

While configuring the SIP proxy for a system with Experience Portal zones, you must take the following into consideration:

- In a system with zones, the applications, media servers, and other resources are grouped into zones.
- A SIP proxy is configured for each zone.
- When the target application resides in only one zone, configure the SIP proxy for the application with only those media servers that are assigned to the target zone.
- If the same SIP proxy is used across multiple zones and the application is configured in multiple zones, the media servers from the multiple zones can be targeted.

Viewing existing SIP connections

About this task

Use this procedure to view the list of existing SIP connections. Users logged in with the Administration user role can add, delete, and change connections.

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **System Configuration** > **VoIP Connections**.
3. On the VoIP connections page, click the SIP tab.

   EPM displays the list of existing SIP connections.

Adding a SIP connection

About this task

To configure TLS as the Proxy Transport for SIP signaling, you must configure the appropriate trusted certificates on Experience Portal and Avaya Session Manager:

- Install the CA certificate(s) that signed the Avaya Session Manager identity certificate as a trusted certificate of type SIP Connection on the EPM server.

- Install the CA certificate(s) that signed the MPP server identity certificate as a trusted certificate on Avaya Aura® Session Manager

The identity certificates and trusted certificate are used to establish a mutually authenticated connection between Experience Portal and the SIP Proxy. Avaya Session Manager is typically used as the SIP Proxy server.

Note:

If the MPP server identity certificate is signed by the EP Certificate Authority, then export the EP Signing Certificate (Root) and install on the Avaya Session Manager.

If the MPP server identity certificate is signed by an external Certificate Authority, then install the external Certificate Authority trusted certificate chain on the Avaya Session Manager.

For more information, see Certificate Authorities on page 567 and Installing trusted certificate for TLS authentication with Avaya Aura Session Manager on page 592.

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **System Configuration** > **VoIP Connections**.
3. On the VoIP Connections page, click the SIP tab.
4. Click **Add**.
5. On the Add SIP Connection page, enter the appropriate information and click **Save**.

Changing SIP connections

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **System Configuration** > **VoIP Connections**.
3. On the VoIP Connections page, click the SIP tab.
4. In the **Name** column, click the name of the connection that you want to change.
5. On the Change SIP Connection page, enter appropriate information and click **Save**.

Deleting SIP connections

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **System Configuration** > **VoIP Connections**.
3. On the VoIP Connections page, click the SIP tab, and do the following:
   - To delete connections individually: Select the check box for the connection name that you want to delete.
   - To delete all connections: Select the selection check box in the header row of the table, which automatically selects all connections.
4. Click **Delete**.

Add SIP Connection page field descriptions

Use this page to add a new Session Initiation Protocol (SIP) connection to the Experience Portal system. Using this page you can also specify more than one proxy server address for the SIP connection.

Add SIP Connection page

If MPP is installed with the Experience Portal system, this page contains the:

- General section on page 80
- Proxy Servers and DNS SRV Domain section on page 81
- SIP Timers section on page 84
- Call Capacity section on page 84
- SRTP group on page 85
- Configured SRTP List group on page 86

General section

Column	Description
Zone	The name of the zone where the SIP connection is configured. Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only if you have created zones on your Experience Portal system. If you do not create any new zones, you do not see the drop-down box.
Name	The unique identifier for this SIP connection on the Experience Portal system. The name can be up to 32 alphanumeric characters. Do not use any special characters. **Note:** This field cannot be changed.
Enable	Whether this SIP connection is available for use by the Experience Portal system. The default is **Yes**, which means the connection is available. **Note:** While you can configure multiple SIP connections, only one can be active at any one time.

Table continues…

Column	Description
Proxy Transport	The IP Protocol used by the SIP connection. The options are: • **TCP** • **TLS**

Proxy Servers and DNS SRV Domain section

Field	Description
Address	The address of the proxy server. This must be a valid network address in the form of a fully qualified hostname or an IP address. This field is enabled only when you select the **Proxy Server** option.
Port	The port used by the proxy server. The default for TCP is 5060, and the default for TLS is 5061. This field is enabled only when you select the **Proxy Server** option.
Priority	When you configure more than one proxy server, this field determines the order in which outbound calls are sent to the list of proxy servers. Calls are sent to the proxy server with the lowest priority value first. If this proxy server fails, calls are sent to the proxy server with the second lowest priority value. This continues up the proxy server list in priority order until either the call succeeds or the list is exhausted. Enter a number in the range 0 to 65535. The default is 0. This field is enabled only when you select the **Proxy Server** option.
Weight	When you add more than one proxy server with the same priority value, this field determines the relative chances of which proxy server is used for an outbound call. The proxy server with the highest weight has the greatest odds of receiving a call. For example, if proxy servers 1 and 2 are assigned a priority of 1, and weight of 4 and 6 respectively, then proxy server 1 has a 40% (4/(4+6)) chance of receiving a call while proxy server 2 has a 60% (6/(4+6)) chance. Enter a number in the range 0 to 65535. The default is 0. This field is enabled only when you select the **Proxy Server** option.

Table continues…

Field	Description
Remove	Removes the proxy server. This field is enabled only when you select the **Proxy Server** option.
Additional Proxy Server	Adds additional proxy addresses and ports. You cannot use the same proxy server address and port for adding another proxy server. This field is enabled only when you select the **Proxy Server** option.
DNS Server Domain	This is the domain name under which the SIP proxy list is configured in the DNS server. **Note:** The DNS server must support the DNS SRV protocol. The entry must be a valid hostname. Ensure that the DNS server domain is configured to retrieve the ordered list of available server records which can be used to handle calls. This field is enabled only when you select the **DNS Server Domain** option.
Listener Port	The port used by the Listener. The default for TCP is 5060, and the default for TLS is 5061.
SIP Domain	The domain in which the SIP connection is configured. The SIP domain must match the domain name of the connected proxy (that is the domain name in SIP URIs for incoming calls). * (asterisk) means that all calls are routed to this trunk.
P-Asserted-Identity	The assumed identity used to determine the service class and the restriction permissions class for the SIP connection. For Communications Manager, this should map to an extension configured on the switch.
Maximum Redirection Attempts	The number of redirection attempts allowed before the call is considered to have failed. The MPP redirects a call when it receives a 302 response code from an INVITE request. This response code indicates that the endpoint which received the call has moved to another location, and the call should be redirected to the new location. The call continues to be redirected until either no further 302 response is received or the retry count is exhausted. Enter a number in the range 0 to 100. The default is 0. Redirect attempt is disabled when the number in this field is set to 0.

Table continues…

Field	Description
Consultative Transfer	If a connection cannot be established, Consultative Transfer allows Experience Portal to regain control of the call. The following options determine the SIP messages used for a VXML Consultative Transfer: • **INVITE with REPLACES**: When Experience Portal receives INVITE with REPLACES in the SIP message, it establishes a secondary call to the transfer destination to: - Determine availability - Ensure that the destination answers within the established timeout The secondary call is then merged with the primary call that is being transferred. Experience Portal sends a request to the transferee for an INVITE message with a Replaces header that contains the information necessary to take control over the primary call. Experience Portal controls the progress of the call in case the response of the second call is not positive. **Note:** This option requires the transfer destination to support the INVITE with Replaces SIP message. • **REFER**: With this option, the transferee determines the entire process of establishing the new call to the transfer destination. If the transfer destination is unavailable or does not respond to the call, the transferee sends the call to Experience Portal. The default option is **INVITE with REPLACES**.
SIP Reject Response Code	The response code that is sent to a SIP proxy when all SIP resources for an MPP are in use. The options are: • **ASM (503)**: Sends a request to ASM to call another MPP that might be available. • **SES (480)**: Sends a request to SES to call another MPP that might be available. • **Custom**: Allows custom response codes to be set for interoperability with other proxies and media gateways that might require a different response code to initiate a similar operation as stated above.

SIP Timers section

Field	Description
T1	Timer T1 is a general estimate of the maximum round trip time for SIP packets between the MPP and the proxy. It is used to determine the minimum retransmit interval for SIP messages. The default value is 250 millisecond(s). Enter a number in the range of 10 to 8000 millisecond(s).
T2	Timer T2 is the maximum retransmit interval for SIP messages. The T1 and T2 values are used together in an algorithm that backs off message retransmits in case of congestion. The default value is 2000 millisecond(s). Enter a number in the range of 10 to 8000 millisecond(s).
B and F	Timers B and F are the transaction timeouts for INVITE and non-INVITE requests, respectively. They determine the amount of wait time before a SIP request is aborted, when no response is received. The default value is 4000 millisecond(s). Enter a number in the range of 500 to 180000 millisecond(s).

Call Capacity section

Field	Description
Maximum Simultaneous Calls	The maximum number of calls that this trunk can handle at one time. Enter a number from 1 to 99999.

Table continues…

Field	Description
Call type radio buttons	The options are: • **All Calls can be either inbound or outbound**: This connection accepts any number of inbound or outbound calls up to the maximum number of calls defined in **Maximum Simultaneous Calls**. • **Configure number of inbound and outbound calls allowed**: If this option is selected, Experience Portal displays the fields: - **Inbound Calls Allowed**: Enter the maximum number of simultaneous inbound calls allowed. This value must be less than or equal to the number of **Maximum Simultaneous Calls**. - **Outbound Calls Allowed**: Enter the maximum number of simultaneous outbound calls allowed. This value must be less than or equal to the number of **Maximum Simultaneous Calls**. The combined number of inbound and outbound calls must be equal to or greater than the number of **Maximum Simultaneous Calls**. **Note:** If all the SIP capacity configured (Maximum Simultaneous Calls) cannot be used because either the license or the total MPP capacity is not sufficient, then the number of inbound calls and outbound calls allowed will be reduced in proportion to the usable capacity.

SRTP group

Field	Description
Enable	The options are: • **Yes**: This connection uses SRTP. • **No**: This connection does not use SRTP.
Encryption Algorithm	The options are: • **AES_CM_128**: This connection uses 128 key encryption. • **None**: Messages sent through this connection are not encrypted.
Authentication Algorithm	The options are: • **HMAC_SHA1_80**: Authentication is done with HMAC SHA-1. • **HMAC_SHA1_32**: Authentication is done with HMAC SHA-1.
RTCP Encryption Enabled	The options are: • **Yes**: This connection uses RTCP encryption. • **No**: This connection does not use RTCP encryption.
RTP Authentication Enabled	The options are: • **Yes**: This connection uses RTP authentication. • **No**: This connection does not use RTP authentication.
Add	Adds the SRTP configuration to the connection.

Configured SRTP List group

This group displays any SRTP configurations defined for the connection.

Note:

This group only appears if the **Proxy Transport** field is set to **TLS**.

Field	Description
Display	Displays the SRTP configurations for this connection.
Remove	Removes the association between the SRTP configuration selected in the display text box and the SIP connection.

Change SIP Connection page field descriptions

Use this page to change an existing Session Initiation Protocol (SIP) connection. Using this page you can also add or remove more than one proxy server address on the same SIP connection, and change the proxy transport option.

If MPP is installed with the Experience Portal system, this page contains the:

General section

Column	Description
Zone	The name of the zone where the SIP connection is configured. Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only when you create new zones. If you do not create any new zones, you do not see the drop-down box.
Name	The unique identifier for this SIP connection on the Experience Portal system. **Note:** This field cannot be changed.
Enable	Whether this SIP connection is available for use by the Experience Portal system. The default is **Yes**, which means the connection is available. **Note:** While you can configure multiple SIP connections, only one can be active at any one time.

Table continues…

Column	Description
Proxy Transport	The IP Protocol used by the SIP connection. The options are: • **TLS** • **TCP**

Proxy Servers and DNS SRV Domain section

Field	Description
Address	The address of the proxy server. This must be a valid network address in the form of a fully qualified hostname or an IP address. This field is enabled only when you select the **Proxy Server** option.
Port	The port used by the proxy server. The default for TCP is 5060, and the default for TLS is 5061. This field is enabled only when you select the **Proxy Server** option.
Priority	When you configure more than one proxy server, this field determines the order in which outbound calls are sent to the list of proxy servers. Calls are sent to the proxy server with the lowest priority value first. If this proxy server fails, calls are sent to the proxy server with the second lowest priority value. This continues up the proxy server list in priority order until either the call succeeds or the list is exhausted. Enter a number in the range 0 to 65535. The default is 0. This field is enabled only when you select the **Proxy Server** option.
Weight	When you add more than one proxy server with the same priority value, this field determines the relative chances of which proxy server is used for an outbound call. The proxy server with the highest weight has the greatest odds of receiving a call. For example, if proxy servers 1 and 2 are assigned a priority of 1, and weight of 4 and 6 respectively, then proxy server 1 has a 40% (4/(4+6)) chance of receiving a call while proxy server 2 has a 60% (6/(4+6)) chance. Enter a number in the range 0 to 65535. The default is 0. This field is enabled only when you select the **Proxy Server** option.

Table continues…

Field	Description
Remove	Removes the proxy server. This field is enabled only when you select the **Proxy Server** option.
Additional Proxy Server	Adds additional proxy addresses and ports. You cannot use the same proxy server address and port for adding another proxy server. This field is enabled only when you select the **Proxy Server** option.
DNS Server Domain	This is the domain name under which the SIP proxy list is configured in the DNS server. **Note:** The DNS server must support the DNS SRV protocol. The entry must be a valid hostname. Ensure that the DNS server domain is configured to retrieve the ordered list of available server records which can be used to handle calls. This field is enabled only when you select the **DNS Server Domain** option.
Listener Port	The port used by the Listener. The default for TCP is 5060, and the default for TLS is 5061.
SIP Domain	The domain in which the SIP connection is configured. The SIP domain must match the domain name of the connected proxy (that is the domain name in SIP URIs for incoming calls). * (asterisk) means that all calls are routed to this trunk.
P-Asserted-Identity	The assumed identity used to determine the service class and the restriction permissions class for the SIP connection. For Communications Manager, this should map to an extension configured on the switch.
Maximum Redirection Attempts	The number of redirection attempts allowed before the call is considered to have failed. The MPP redirects a call when it receives a 302 response code from an INVITE request. This response code indicates that the endpoint which received the call has moved to another location, and the call should be redirected to the new location. The call continues to be redirected until either no further 302 response is received or the retry count is exhausted. Enter a number in the range 0 to 100. The default is 0. Redirect attempt is disabled when the number in this field is set to 0.

Table continues…

Field	Description
Consultative Transfer	If a connection cannot be established, Consultative Transfer allows Experience Portal to regain control of the call. The following options determine the SIP messages used for a VXML Consultative Transfer: • **INVITE with REPLACES**: When Experience Portal receives INVITE with REPLACES in the SIP message, it establishes a secondary call to the transfer destination to: - Determine availability - Ensure that the destination answers within the established timeout The secondary call is then merged with the primary call that is being transferred. Experience Portal sends a request to the transferee for an INVITE message with a Replaces header that contains the information necessary to take control over the primary call. Experience Portal controls the progress of the call in case the response of the second call is not positive. **Note:** This option requires the transfer destination to support the INVITE with Replaces SIP message. • **REFER**: With this option, the transferee determines the entire process of establishing the new call to the transfer destination. If the transfer destination is unavailable or does not respond to the call, the transferee sends the call to Experience Portal. The default option is **INVITE with REPLACES**.
SIP Reject Response Code	The response code that is sent to a SIP proxy when all SIP resources for an MPP are in use. The options are: • **ASM (503)**: Sends a request to ASM to call another MPP that might be available. • **SES (480)**: Sends a request to SES to call another MPP that might be available. • **Custom**: Allows custom response codes to be set for interoperability with other proxies and media gateways that might require a different response code to initiate a similar operation as stated above.

SIP Timers section

Field	Description
T1	Timer T1 is a general estimate of the maximum round trip time for SIP packets between the MPP and the proxy. It is used to determine the minimum retransmit interval for SIP messages. The default value is 250 millisecond(s). Enter a number in the range of 10 to 8000 millisecond(s).
T2	Timer T2 is the maximum retransmit interval for SIP messages. The T1 and T2 values are used together in an algorithm that backs off message retransmits in case of congestion. The default value is 2000 millisecond(s). Enter a number in the range of 10 to 8000 millisecond(s).
B and F	Timers B and F are the transaction timeouts for INVITE and non-INVITE requests, respectively. They determine the amount of wait time before a SIP request is aborted, when no response is received. The default value is 4000 millisecond(s). Enter a number in the range of 500 to 180000 millisecond(s).

Call Capacity section

Field	Description
Maximum Simultaneous Calls	The maximum number of calls that this trunk can handle at one time. Enter a number from 1 to 99999.

Table continues…

Field	Description
Call type radio buttons	The options are: • **All Calls can be either inbound or outbound**: This connection accepts any number of inbound or outbound calls up to the maximum number of calls defined in **Maximum Simultaneous Calls**. • **Configure number of inbound and outbound calls allowed**: If this option is selected, Experience Portal displays the fields: - **Inbound Calls Allowed**: Enter the maximum number of simultaneous inbound calls allowed. This value must be less than or equal to the number of **Maximum Simultaneous Calls**. - **Outbound Calls Allowed**: Enter the maximum number of simultaneous outbound calls allowed. This value must be less than or equal to the number of **Maximum Simultaneous Calls**. The combined number of inbound and outbound calls must be equal to or greater than the number of **Maximum Simultaneous Calls**. **Note:** If all the SIP capacity configured (Maximum Simultaneous Calls) cannot be used because either the license or the total MPP capacity is not sufficient, then the number of inbound calls and outbound calls allowed will be reduced in proportion to the usable capacity.

SRTP group

Field	Description
Enable	The options are: • **Yes**: This connection uses SRTP. • **No**: This connection does not use SRTP.
Encryption Algorithm	The options are: • **AES_CM_128**: This connection uses 128 key encryption. • **None**: Messages sent through this connection are not encrypted.
Authentication Algorithm	The options are: • **HMAC_SHA1_80**: Authentication is done with HMAC SHA-1. • **HMAC_SHA1_32**: Authentication is done with HMAC SHA-1.
RTCP Encryption Enabled	The options are: • **Yes**: This connection uses RTCP encryption. • **No**: This connection does not use RTCP encryption.
RTP Authentication Enabled	The options are: • **Yes**: This connection uses RTP authentication. • **No**: This connection does not use RTP authentication.
Add	Adds the SRTP configuration to the connection.

Configured SRTP List group

This group displays any SRTP configurations defined for the connection.

Note:

This group only appears if the **Proxy Transport** field is set to **TLS**.

Field	Description
Display	Displays the SRTP configurations for this connection.
Remove	Removes the association between the SRTP configuration selected in the display text box and the SIP connection.

SIP tab on the VoIP Connections page field descriptions

Use this tab to view, add, or change Session Initiation Protocol (SIP) connections on the Experience Portal system.

Tip:

To sort the connections by any column, click the up arrow (sort ascending) or down arrow (sort descending) in the column header.

Column	Description
Selection check box	Use this Selection check box to select which SIP connections you want to delete.
Zone	The name of the zone where the SIP connection is configured.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
Name	The unique identifier for this SIP connection on the Experience Portal system. Click the name to open the Change SIP Connection page.
Enable	The options are: • **Yes**: This connection is available for use by the Experience Portal system. • **No**: This connection is disabled.
Proxy Transport	The IP Protocol used by the SIP connection. The options are: • **TCP** • **TLS**
Proxy/DNS Server Address	The address of the proxy server or the DNS server. This must be a valid network address in the form of a fully qualified hostname or an IP address.
Proxy Server Port	The port used by the proxy server.

Table continues…

Column	Description
Listener Port	The port used by the Listener.
SIP Domain	The domain in which the SIP connection is configured. The SIP domain must match the domain name of the connected proxy (that is the domain name in SIP URIs for incoming calls).
Add	Opens the Add SIP Connection page.
Delete	Deletes the SIP connections whose associated Selection check box is checked.
Maximum Simultaneous Calls	The maximum number of calls that this trunk can handle at one time. Enter a number from 1 to 99999.

Comparison of features supported on H.323 and SIP

This table compares:

- Standard H.323.
- H.323 with the Avaya Special Application SA8874 feature enabled in Communication Manager.
- SIP.

Feature	H.323	H.323 with SA8874 feature	SIP
Outbound calling using the Application Interface web service	Partially supported No call progress information is available, so an application may start before a call is answered	Supported	Supported
Call conferencing	Supported	Supported	Supported
Call classification	Supported	Supported	Supported
Blind transfer	Supported	Supported	Supported

Table continues…

Feature	H.323	H.323 with SA8874 feature	SIP
Supervised transfer (also called consultative transfer) **Note:** If a connection cannot be established, the Consultative Transfer feature in Experience Portal allows the application to regain control of the call.	Operates like a blind transfer **Note:** The only supported VoiceXML event for this transfer is `error.connection.noroute`.	Supported	Supported
Bridge transfer)	Partially supported No call status information, such as "line is busy", is available	Supported	Supported except for the VoiceXML `<transfer>` tag's `connecttimeout` parameter, which is not supported
DTMF detection **Note:** Experience Portal supports only out-band DTMF detection for H.323 and H.323 with SA8874 feature.	Supported	Supported	Supported **Note:** In case of SIP VoIP connection, the signaling group doesn't support the out- band option. It supports the in-band and RTP-payload DTMF options.
Playing prompt files	Supported	Supported	Supported
Recording	Supported	Supported	Supported

Table continues…

Feature	H.323	H.323 with SA8874 feature	SIP
Converse-on vectoring	Supported	Supported	Not supported
Encryption options	• Disabled • AES • AEA	• Disabled • AES • AEA	• Disabled • TLS • SRTP
Quality of Service	Supported	Supported	Supported
User to User Information (UUI)	Not supported	Not supported	For an incoming call, UUI values are populated in the VoiceXML session variables for both UUI and Application to Application Information (AAI). For more information, see Universal Call Identifier (UCID) values included in UUI data on page 403.
Universal Call Identifier (UCID)	Supports the capability to receive UCID over H323 from Communication Manager. **Note:** This capability is available in Communication Manager 5.2. To enable this feature, you need to administer ucid-info on button 10 on the 7434ND stations used by Experience Portal.	Supports the capability to receive UCID over H323 from Communication Manager. **Note:** This capability is available in Communication Manager 5.2. To enable this feature, you need to administer ucid-info on button 10 on the 7434ND stations used by Experience Portal.	Supports the capability to both send and receive UCID. For more information, see Universal Call Identifier (UCID) values included in UUI data on page 403.

Table continues…

Feature	H.323	H.323 with SA8874 feature	SIP
Switch failover	An alternate gatekeeper address can be specified in the EPM, and an alternate gatekeeper address list can come from Communication Manager	An alternate gatekeeper address can be specified in the EPM, and an alternate gatekeeper address list can come from Communication Manager	No additional support is supplied by Experience Portal, but the Avaya Aura®Session Manager (AASM) has support for high availability including switch failover support.
Merge (Refer with replaces)	Not supported	Not supported	Supported

Bridge transfers in a mixed SIP/H.323 environment

If you have both SIP and H.323 connections defined in your Experience Portal system, Experience Portal handles bridge transfers in the following manner. For an outbound call with:

- `SIP` or `SIPS` in the `ToURI` field, there must be a SIP outbound channel available.
- `TEL` in the `ToURI` field, Experience Portal tries to get an outbound port from the same H.323 port group. If none are available, Experience Portal tries any H.323 port.

  If no H.323 ports are available, Experience Portal converts the `TEL` into `SIP` in the `ToURI` field and tries and get a SIP outbound channel.

VoIP in Experience Portal

Experience Portal uses H.323 or SIP connections to switches to transmit and receive Voice over IP (VoIP) data. The system makes use of a variety of Internet protocols to allow the real-time transmission and reception of voice data. In particular, the Media Processing Platform (MPP) servers use protocols such as the User Datagram Protocol (UDP), the Transmission Control Protocol (TCP), and the Media Resource Control Protocol (MRCP) to establish Real-time Transport Protocol (RTP) sessions and to transmit and receive voice data packets.

Note:

To function effectively, the TCP and MRCP ports should not overlap.

In addition, the Experience Portal system can use a Real-time Transport Control Protocol (RTCP) monitor to collect data about the real-time transport of data as delivered by the MPP, the switches, and any other IP components that are configured to send status information about RTP sessions. The RTCP monitor then aggregates all the RTP session data into reports that contain information about packet loss, “jitter,” and other variables concerned with the health of RTP connections in the

network. This RTCP monitor provides the system administrator one central location from which to gauge the status and performance of the network with respect to the bandwidth and latency requirements of VoIP.

Viewing the Avaya Experience Portal VoIP settings

Procedure

1. Log on to the EPM web interface by using an account with one of the following roles:
   - Administration
   - Operations
   - Maintenance
2. On the EPM main menu, click **System Configuration** > **MPP Servers**.
3. On the MPP Servers page, click the **VoIP Settings** button.

   The EPM displays the VoIP Settings page. If you are not logged in with the Administration user role, the EPM displays the VoIP Settings page in view-only mode.

Configuring the Avaya Experience Portal VoIP settings

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **System Configuration** > **MPP Servers**.
3. On the MPP Servers page, click the **VoIP Settings** button.
4. On the VoIP Settings page, enter appropriate information and click **Save**.

   Note:

   If you made any changes to the VoIP Settings page, restart all MPPs as described in the topic Restarting one or more MPP servers on page 289.

VoIP Settings page field descriptions for MPP

Use this page to configure Voice over IP (VoIP) on your Experience Portal system.

This page contains the:

Port Ranges group

Field	Description
UDP	The range of port numbers used by User Datagram Protocol (UDP) transactions. Enter the lower value of the range of port numbers in the **Low** field, and the higher value in the **High** field. The range must be within 1024 to 65535. The default range is 11000 to 30999. **Note:** Each call that uses ASR and TTS resources requires a total of six UDP ports.
TCP	The TCP range which you specify in this field must be large enough for the network connections, which vary based on the configuration as well as the load. Enter the lower value of the range of port numbers in the **Low** field, and the higher value in the **High** field. The range must be within 1024 to 65535. The default range is 31000 to 33499. **Important:** Do not limit the TCP range to the absolute minimum as it will possibly impact functionality such as failover. Do not overlap ranges for the TCP and MRCP protocols.
MRCP	The port numbers used by Transmission Control Protocol (TCP) transactions. Enter the lower value of the range of port numbers in the **Low** field, and the higher value in the **High** field. The range must be within 1024 to 65535. The default range is 34000 to 36499. The number of MRCP ports you need depends on the setting of the **New Connection per Session** option for the Experience Portal speech servers. If this option is enabled, you need one MRCP port for each speech server license. If this option is not enabled, you need one MRCP port per speech server. For example, if you have one ASR server with five ASR licenses and one TTS server with two TTS licenses and: • The **New Connection per Session** option is enabled for both the ASR and TTS server, you would need seven MRCP ports because you have seven total licenses. • The **New Connection per Session** option is enabled for the ASR server but not the TTS server, you would need six MRCP ports because you have five ASR licenses plus one TTS server. • The **New Connection per Session** option is not enabled for either the ASR or TTS server, you would need two MRCP ports because you have two speech servers.

Table continues…

Field	Description
H.323 Station	The H.323 Station port range configures a range of UDP ports that are used exclusively for gatekeeper discovery and registration. However, the bulk of H.323 communication occurs over a TCP socket that is allocated from the TCP range. For each H.323 station, you need to configure one UDP and one TCP port. If either port fails to be allocated, the H.323 station will be marked out of service. Enter the lower value of the range of port number in the **Low** field, and the last number of the range in the **High** field. The range must be within 1024 to 65535. The default range is 37000 to 39499. **Important:** The H.323 Station range must not overlap with UDP range.

RTCP Monitor Settings group

Field	Description
Host Address	The network address of the RTCP monitor, which collects status data about RTP sessions from the MPP and other components in the system. This must be a valid network address in the form of a fully qualified hostname or an IP address.
Port	The number of the port on the RTCP monitor that the EPM uses to communicate with the RTCP monitor.

VoIP Audio Formats group

Field	Description
MPP Native Format	The audio encoding codec the MPP uses as the default for audio recording within the Avaya Voice Browser (AVB) when the speech application does not specify the format for recording caller inputs. The options are: • **audio/basic**: The AVB uses the mu-Law encoding format, which is used mostly in the United States and Japan. If you select this option then the codec set on the switch must include G711MU. • **audio/x-alaw-basic**: The AVB uses the A-Law encoding format, which is used in most countries other than the United States and Japan. If you select this option then the codec set on the switch must include G711A. With either option, the AVB records input using a G.711-compliant format that is a raw (headerless) 8kHz 8-bit mono [PCM] single channel format. **Note:** The AVB ignores this setting if a recording format is specified in a given speech application. If you make any change to the setting of this field, you must restart the MPP for the changes to take effect.

Audio Codecs group

Field	Description
Offer	When sending a SIP INVITE, Experience Portal offers the supported codecs in a priority order that the administrator can configure. The default order is: • **G729** • **G711uLaw** • **G711aLaw**
Answer	When receiving a SIP INVITE,Experience Portal accepts the supported codecs based on a priority order that the administrator configures. By default, Experience Portalaccepts the first codec offered by the other side that Experience Portal supports.
Packet Time	The interval in milliseconds, for transmitting each audio packet. The time intervals you can select are: 10, 20, 30, 40, 50, 60, 70, and 80. The default is 20.
G729	G.729 codec is used for audio data compression for both H.323 and SIP connections. It supports G.729 Annexes A and B. The options are: • **Yes**: Select **Yes** to enable this option. • **No**: Select **No** to disable this option. The default is **Yes**.
Reduced Complexity Encoder	The G.729A reduced complexity encoding algorithm lowers the performance cost of G.729 transcoding. This setting affects only the encoding of G.729 audio sent by Experience Portal. The audio quality is reduced slightly when you enable this option. Experience Portal continues to receive and decode G.729 and G.729A audio data, regardless of the option selected in this field. **Note:** This field is enabled only if you have selected **Yes** in the G729 field. The options are: • **Yes**: Select **Yes** to enable this option. • **No**: Select **No** to disable this option. The default is **Yes**.

Table continues…

Field	Description
Discontinuous Transmission	The G.729B discontinuous transmission algorithm allows Experience Portal to access and process a far end media offer with G.729B. The Annexe B specification further reduces network bandwidth as it sends only the audio packets that contain speech data (packets that contain silence are not transmitted). **Note:** This field is enabled only if you have selected **Yes** in the G729 field. The options are: • **Yes**: Select **Yes** to enable this option. • **No**: Select **No** to disable this option. With this option Annex B is not used. **Note:** The G.729 offers may still be accepted.

QoS Parameters group

Quality of Service (QoS) is used in network routing to improve performance for certain data streams. For example, RTP negotiated by various signaling protocols, but not the signaling itself. This is especially valuable for VoIP traffic because VoIP is susceptible to jitter caused by network delays. The QoS settings in this group are defined as per the signaling protocols parameters, but apply to the RTP streams that are the result of these signaling connections. This allows the various categories of RTP data to be prioritized independently. The QoS settings, however, do not apply to the signaling connections which are much less sensitive to latency and bandwidth limitations.

Note:

The QoS settings are not in a continuous range. Increasing or decreasing the values will disable QoS. The numbers must exactly match the configuration on the network routers for the settings to have any effect. Therefore, if you are using QoS and the defaults do not seem to be working, contact your network administrator for suggested values.

Field	Description
H.323	The H.323 QoS parameters are: • **VLAN**. The QoS settings for H.323 connections running over a virtual LAN. • **Diffserv**. The QoS settings for H.323 connections running over a network using the Differentiated Services architecture. The default for **VLAN** is 6 and the default for **Diffserv** is 46.
SIP	The Session Initiation Protocol (SIP) QoS parameters are: • **VLAN**. The QoS settings for SIP connections running over a virtual LAN. • **Diffserv**. The QoS settings for SIP connections running over a network using the Differentiated Services architecture. The default for **VLAN** is 6 and the default for **Diffserv** is 46.

Table continues…

Field	Description
RTSP	The Real-Time Streaming Protocol (RTSP) QoS parameters are: • **VLAN**. The QoS settings for Real RTSP running over a virtual LAN. • **Diffserv**. The QoS settings for RTSP running over a network using the Differentiated Services architecture. The default for **VLAN** is 6 and the default for **Diffserv** is 46.

Out of Service Threshold group

The **Trigger** settings in this group determine when an MPP server issues an event or alarm message based on the percentage of ports that have gone out of service. In all cases, once the MPP server has issued an event or alarm message, it will not issue another message until the percentage of out of service ports changes to the value set in the associated **Reset** field or below.

For example, if the **Warn Trigger** value is 10 and the **Reset** value is 0, then the MPP will respond in the following manner as the percentage of out of service ports changes:

Percentage of out of service ports	MPP server response
10%	A warning event is generated and the MPP enters the Degraded state.
8%	No event is generated.
12%	No event is generated because it has not yet fallen below the **Reset** value.
0%	No event is generated but the MPP returns to the Running state.
6%	No event is generated.
11%	An event is generated and the MPP returns to the Degraded state. **Note:** When the warning event is generated after the percentage of out of service ports reaches the trigger value, no more warning is generated until you reach reset value again.

Field	Description
Warn	The **Trigger** field determines the percentage of ports that must go out of service on an MPP before the MPP sends a warning-level event to Experience Portal and enters the Degraded state. Once the **Reset** value is reached, the MPP returns to the Running state. The **Trigger** default is 10 and the **Reset** default is 0.

Table continues…

Field	Description
Error	The **Trigger** field determines the percentage of ports that must go out of service on an MPP before the MPP sends an error-level event to Experience Portal and enters the Degraded state. Once the reset value is reached, the MPP will send another error event when appropriate, but it does not return to the Running state until the **Reset** value associated with the **Warn** field has been reached. The **Trigger** default is 20 and the **Reset** default is 10.
Fatal	The **Trigger** field determines the percentage of ports that must go out of service on an MPP before the MPP issues a fatal-level alarm and enters the Degraded state. Once the reset value is reached, the MPP will send another fatal event when appropriate, but it does not return to the Running state until the **Trigger** value associated with the **Warn** field has been reached. The **Trigger** default is 100 and the **Reset** default is 50.

Call Progress group

Field	Description
Threshold	The options are: • **Voice** — The Voice Threshold parameter is used by the call classification engine in determining whether a given frame of audio data should be interpreted as voice energy. Lower values are more inclusive and tends toward marking even white background noise as voice. Higher values will reject more noise, picking out only audio frames that are very clearly voice sounds. The range is 0.0-1.0 and the default value is 0.50 • **Tone** — The Tone Threshold parameter is used conjunctively along with Periodicity Threshold parameter by the call classification engine to determine if a given frame of audio data contains a pure telephony tone. Lower values for either or both will allow the call classification engine to accept more distorted signals as valid telephony tones, but makes certain voice sounds more likely to be detected as pure tones, for example, Talk Off. The range is 0.0-1.0 and the default value is 0.95. • **Periodicity** — The Periodicity Threshold parameter is used conjunctively with Tone Threshold by the call classification engine to determine if a given frame of audio data contains a pure telephony tone. Lower values for either or both will allow the call classification engine to accept more distorted signals as valid telephony tones, but makes certain voice sounds more likely to be detected as pure tones, for example, Talk Off. The range is 0.0-1.0 and the default is 0.97. • **Ring Count** — Ring Count Threshold detects the number of ring back cycles . The purpose is to let the call progress engine to use different timers when a call is answered “quickly”, as determined by the ring count, tailoring the parameters appropriately under the assumption that calls answered after a couple of rings are more likely to be a live person. The cycles range from 0-8 and the default value is 4.

Table continues…

Field	Description
Cut Through	The **Cut Through** time is the number of milliseconds of consecutive silence after some voice energy that must be heard to determine that a live speaker is done talking. **Note:** Setting this value lower, increases the responsiveness of the system. The system finishes Live voice detection to finish sooner and the VoiceXML dialog starts playing sooner. However, the system risks false detections for recordings where there are long gaps between speech energy. For example, a voice mail system might play a short recorded greeting, followed by a TTS name, followed by some more recorded prompts. If the silence between the recorded greeting and the TTS name is longer than the cut through time, the voice mail machine is mistakenly identified as a live person. Setting the value higher increases the likelihood that a call is properly classified. The following are the values of **Cut Through** time: • **Initial** — The Initial values are loaded first when the call classification engine is initialized for any given call. The value ranges from 200-2000 milliseconds and the default is 1100 milliseconds. • **Short** — The values for the Short timers are loaded when the call classification engine detects at least one ring back cycle . The value ranges from 200-2000 milliseonds and the default is 700 milliseconds. • **Long** — The values for the Long timers are loaded if the call classification engine detects successive ring back cycles and the count equals or exceeds the Ring Count Threshold. The value ranges from 200–2000 milliseconds and the default is 1100 milliseconds. Which value is used is determined by the number of ring back cycles heard by the call classification engine and the Ring Count Threshold. The purpose is to let the call progress engine to use different timers when a call is answered “quickly”, as determined by the ring count, tailoring the parameters appropriately under the assumption that calls answered after a couple of rings are more likely to be a live person.

Table continues…

Field	Description
Max Voice	The **Max Voice** time is the number of milliseconds of continuous voice energy except gaps of silence shorter than the **Cut Through** time that must be heard to determine that a greeting is a recorded message. **Note:** Setting this value lower biases the call classification engine toward detecting answering machines. All but very short greetings are assumed to be answering machines. Conversely, setting the value higher biases the call classification engine toward detecting live voice. For instance, a greeting must be very long to be considered an answering machine. The following are the values of **Max Voice** time: • **Initial** — The Initial value is loaded first when the call classification engine is initialized for any given call. The value ranges from 1100-4000 milliseconds and the default is 2500 milliseconds. • **Short** — The values for the Short timers are loaded when the call classification engine detects at least one ring back cycle. The value ranges from 1100–4000 milliseconds and the default is 2500 milliseconds. • **Long** — The values for the Long timers are loaded if the call classification engine detects successive ring back cycles and the count equals or exceeds the Ring Count Threshold. The value ranges from 1100–4000 milliseconds and the default is 2500 milliseconds. Which value is used is determined by the number of ring back cycles heard by the call classification engine and the Ring Count Threshold. The purpose is to let the call progress engine to use different timers when a call is answered “quickly”, as determined by the ring count, tailoring the parameters appropriately under the assumption that calls answered after a couple of rings are more likely to be a live person.

Miscellaneous group

Field	Description
Inband DTMF Detection Enabled	This option allows Experience Portal to interoperate with media gateways and SIP endpoints • **Yes**: Select **Yes** to enable this option. • **No**: Select **No** to disable this option. The default is **No**. **Note:** If you make any change to the **Inband DTMF Detection Enabled** field, you must restart the MPP for the changes to take effect.

Table continues…

Field	Description
Pre-Energy Record Time	The maximum number of milliseconds of audio data that are inserted in the recordings before the system detects the energy. • **Range**: 0 to 30000. • **Default**: 0 **Note:** If you make any change to the **Pre-Energy Record Time** field, you must restart the MPP for the changes to take effect.
H323 Force Registration	Controls the behavior of the H.323 station registration process. The settings are: • **Always**: The setting **Always** causes the MPP to forcibly register an extension, immediately bringing a port into service by, potentially, taking control from any other endpoint that may currently have the extension registered. Any calls in progress on the other endpoint are dropped when control of the station is removed. • **Never**: The default setting of **Never** causes station registration to fail if a registering extension is already in use and registered by another endpoint. The port does not immediately come into service, but the station remains in use by the other endpoint until the station is released or unregistered. The default is **Never.**

Directory details of the EPM system components

Most Experience Portal components and log files are located in the default installation directory that you specify during installation. However, several components cannot be relocated and are stored in fixed paths even if you specify a different path than the default installation directory.

The following table lists some of the components that are stored in fixed paths.

This table does not include standard RHEL packages, such as Apache and NTP, that are installed with or used by Experience Portal.

Component	Directory
Experience Portal Manager web application	/opt/Tomcat/tomcat/webapps/VoicePortal
Avaya Experience Portal Management web services	/opt/Tomcat/tomcat/webapps/axis2

Table continues…

Component	Directory
Avaya License Manager	The collocated WebLM is installed in the /opt/Tomcat/tomcat/webapps/WebLM directory. **Note:** If you use an external WebLM, the license manager can be installed in a different directory on the external system.
Experience Portal database	The Postgres files are installed in the /var/lib/pgsql directory. **Note:** Most of the database data is in the /var/lib/pgsql/data directory.
Tomcat for EPM and HTML	/opt/Tomcat
Tomcat for SMS and Email Processor	/opt/MMSServer
Apache Axis2: web services container	/opt/Tomcat/tomcat/webapps/axis2
Postgres Database	/var/lib/pgsql
Experience Portal Backup	/opt/Avaya/backup
Install Agent	/opt/Avaya/InstallAgent
Core Services	/opt/coreservices, /opt/Avaya/CoreServiceConfig, /opt/Avaya/CoreServiceInstall

Determining the installation history on an Experience Portal server

About this task

Use this procedure to check the following installation history related data on the Experience Portal server:

- The current version that is installed on the server.
- All versions that have been installed on the server since Avaya Experience Portal 8.1.

Procedure

1. Log on to Linux on the Primary or Auxiliary EPM or MPP 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.
2. Navigate to the `$AVAYA_HOME/Support/VP-Tools` directory.

3. To search for installations made in any subdirectory under `$AVAYA_HOME`, do the following:
   - For the current installation: Run the **`iaversion.php`** command.
   - For all installations: Run the **`iahistory.php`** command.

Configuring the PostgreSQL database user accounts

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. The password for this account is automatically generated. You cannot add other accounts of this type, delete this account, or change the account name. **Important:** 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. You can have any number of accounts of this type with any account names. **Important:** Contact the Avaya Services representative to modify the tables that store report data in the local VoicePortal database.
vpcommon	This account is required if you plan to configure an Auxiliary EPM server. It allows the Auxiliary EPM servers limited access to the main Experience Portal database. You can delete this account or set the password for it, but you cannot add other accounts of this type or change the account name.

With the `SetDbPassword.sh` script, you can change all account passwords and add and delete all accounts except for postgres, which cannot be deleted.

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 as described in the Reloading the Avaya Experience Portal environment variables topic in the *Implementing Avaya Experience Portal on multiple servers* guide.

Procedure

1. Log in to Linux on the Primary EPM or Auxiliary EPM 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.
2. 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.
3. Enter `bash SetDbPassword.sh` followed by the additional parameters to perform the required operation.

   For details on the supported operations, see the following table. If you want to:

View a list of all Avaya Experience Portal PostgreSQL accounts	Enter the `bash SetDbPassword.sh list` command.
Change the password for a PostgreSQL user account	• Enter the `bash SetDbPassword.sh update -u` *`username`* command, where: *`username`* is the name of the user account whose password you want to change • Type the password you want to use for this account and press `Enter`. **Note:** If you change the password for the: • postgres account, Avaya Experience Portal stops and then restarts the vpms service. • vpcommon account on the Primary EPM server, you must also change the password on the Auxiliary EPM server as well.
Generate a random password for the PostgreSQL user account postgres	Enter the `bash SetDbPassword.sh reset_postgres` command.
Add a new report user with read only privileges	• Enter the `bash SetDbPassword.sh add_report_r -u` *`username`* command, where: *`username`* is the PostgreSQL account name for the new report user • Type the password you want to use for this account and press `Enter`.

Add a new report user with read/write privileges on an Auxiliary EPM server **Note:** **You cannot add a report user with read/write privileges on the Primary EPM server.**	• Enter the `bash SetDbPassword.sh add_aux_report_w -u` *`username`* command, where: *`username`* is the PostgreSQL account name for the new report user • Type the password you want to use for this account and press `Enter`.
Delete a report account from either EPM server or delete the vpcommon account from the Primary EPM server **Note:** **You cannot delete the postgres user account.**	Enter the `bash SetDbPassword.sh delete -u` *`username`* command, where *`username`* is either vpcommon or the report account name that you want to delete. For example, to delete the report account named RptReadWrite, you would enter: `bash SetDbPassword.sh delete -u RptReadWrite`
Add the vpcommon user account on the Primary EPM server so that an Auxiliary EPM server can access the database **Note:** **You cannot add the vpcommon account to an Auxiliary EPM server.**	• Enter the `bash SetDbPassword.sh add_primary_vpcommon` command. • Type the password you want to use for this account and press `Enter`.
Verify the vpcommon user on the local database that can connect to the 'auxname' (Auxiliary EPM) **This option is applicable only on the Primary EPM.**	Enter the `bash SetDbPassword.sh verify_aux_vpcommon -a auxname` command where: -a auxname is the configured name for the Auxiliary EPM.
Verify the Primary EPM's vpcommon user. **This option is applicable only on the Auxiliary EPM.**	Enter the `bash SetDbPassword.sh verify_primary_vpcommon` command.
View the help for this command	Enter the `bash SetDbPassword.sh help` command.

After the script successfully completes the operation, the script prompts a message indicating the services to be restarted and asks if the user wants to proceed.

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

Note:

The script will not list the service that is not impacted by changing the user password.

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

   Note:

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

Secure password hashing algorithm SCRAM-SHA-256 for database users

In earlier releases of Experience Portal, Postgres could only use the default MD5 password hashing algorithm for database users. In Release 7.2.3, Postgres was updated from 9.X to 11.X to support the use of a more secure password hashing algorithm SCRAM-SHA-256.

New script to change to SCRAM-SHA-256 password hashing algorithm

The `SetDbPasswordAndHashingAlgorithm.sh` script is used to change from the default MD5 password hashing algorithm to the SCRAM-SHA-256 password hashing algorithm. This script is present in the same location as the rest of the security related scripts on EPM at `/opt/Avaya/ExperiencePortal/Support/Security-Tools/`.

This new shell script automates many of the manual steps required to switch between the password hashing algorithms. For details on how to use the script to change to the newer and more secure SCRAM-SHA-256, see Changing Postgres 11 user password hashing algorithm from MD5 to SCRAM-SHA-256 on page 111.

For the remaining steps that have to performed manually to change to the new password hashing algorithm, see Changing existing account passwords manually on page 113.

Changing Postgres 11 user password hashing algorithm from MD5 to SCRAM-SHA-256

About this task

Use this procedure to change from the default MD5 hashing algorithm to SCRAM-SHA-256 password hashing algorithm by using the `SetDbPasswordAndHashingAlgorithm.sh` script.

Note:

Prior to running the `SetDbPasswordAndHashingAlgorithm.sh` script, the `SetDbPassword.sh` script has to be run to change the default postgres user database

account. The following services are restarted when the `SetDbPassword.sh` script is executed and again when the `SetDbPasswordAndHashingAlgorithm.sh` script is run. Hence, do not run the script unless a scheduled maintenance window is set to accommodate both service restarts.

- postgressql
- vpms
- mmserver
- avpSNMPAgentSvc

Procedure

1. Log on to the local Linux console as root.

   Note:

   Only a root user can execute the script.

2. Navigate to the `/opt/Avaya/ExperiencePortal/Support/Security-Tools/` directory.
3. Run the `SetDbPassword.sh` script to modify the default postgres database user account.
   a. Enter the **`bash SetDbPassword.sh update -u postgres`** command.
   b. Enter in the password when prompted.

      Ensure that you remember the password as you will have to enter it again later.

   c. Select `Y` to restart services.
4. Enter the **`Bash SetDbPasswordAndHashingAlgorithm.sh`** command.
5. Select the password hashing algorithm that you want to apply to the Postgres database.

   The options are:

   - MD5
   - SCRAM-SHA-256

   Once you select the password hashing algorithm, the script displays the process it goes through.

   Note:

   You are prompted to enter the postgres user account password three times to facilitate the changing of the password to the new hashing algorithm.

   Example of a sample output:

```
Please select the postgres hashing algorithm to set
          1) md5
          2) scram-sha-2562
2   [In this case Option 2 was selected]
Postgres will be set to use scram-sha-256 password hashing
Changing the pg_hba.conf file to scram-sha-256 hashing algorithm
Reloading the postgresql configuration file to reflect changes made
```

```
0
Enter in the postgres user account password:
Enter Password:
Enter in the postgres user account password again:
Enter Password:
Updating the postgres default user account password
ALTER ROLE
Running the SetDbPassword.sh for the postgres account - Enter in password again
Please enter the password:
```

Next steps

The postgres user account is changed automatically when you run the script. Any additional postgres user accounts will have to be changed manually using the existing `SetDbPassword.sh` script provided.

Manual steps to change to SCRAM-SHA-256 password hashing algorithm

The postgres user account is changed automatically in the script execution. However, you need to manually change any additional postgres user accounts using the existing `SetDbPassword.sh` script.

In Avaya Experience Portal, there can be several postgres database accounts used during the operation of the solution. Database user accounts are either created by the installer, which prompts for passwords, or through scripts. For any database user account, the password can be reset using the `SetDbPassword.sh` script.

However, some of these accounts are not created by default. These accounts can be created based on the needs of the specific customer. The customer should be aware of the creation of these accounts and their passwords. For details on the various accounts that exist and their relevance to a deployment, see Configuring the PostgreSQL database user accounts on page 108.

Note:

It is necessary to change the passwords of existing accounts. Since a change has been made to the configuration files, existing users and their passwords will have to be regenerated so that they are hashed into the newly selected algorithm. Failure to change the password of existing accounts may result in loss of functionality.

Changing existing account passwords manually

About this task

Use this procedure to manually change the password for the existing database accounts by using the `SetDbPassword.sh` script. Using this script, you can change all account passwords, and add and delete all the accounts except for postgres, which cannot be deleted.

Note:

This process restarts several services and should be scheduled accordingly.

Procedure

1. Log in as cust using putty.
2. Log in to Linux as a root user.

   Or, log on remotely as a non-root user, and then change the user to root by entering the `su - root` command.
3. Run the **`bash SetDbPassword.sh`** command to change the passwords.

```
/opt/Avaya/ExperiencePortal/Support/Security-Tools/SetDbPassword.sh
[Usage displayed by entering no argument]
```

Chapter 4: Organization level access

Organization level access in Avaya Experience Portal

The multi-tenancy feature in Avaya Experience Portal allows the data maintained by the Experience Portal Manager (EPM) to be segmented for multiple organizations. This segmentation allows users within an organization to have restricted access in the EPM. You can use the **Organizations** page to configure multi-tenancy in EPM.

Important:

The **Organizations** page in EPM is accessible only if the organization level access is enabled in Experience Portal.

For more information, see Configuring organization level access in Experience Portal on page 117.

In the following EPM web pages, the organization level users can only access the data which belongs to their organization:

- Reports: Standard, Custom and Scheduled
- Users
- Roles
- Applications
- Active Calls
- Audit Log Viewer

The pre-configured organization level roles in the EPM restrict the access rights of organization level users. They can access only that data which is specific to their organization.

Organizational level access is created in Experience Portal when you:

- Add an organization in the **Organizations** page.
- Assign the users to the organization in the **Add User** page.
- Assign the applications to the organization in the **Add Application** page.
- Assign the custom reports to the organization in the **Add Custom Report** page.

For example, you create an organization called `sales`. Assign a user called `John`, an application called `test` and a custom report called `test` to the `sales` organization. The user `John` can now access only the `test` application and `test` report in EPM.

Note:

Only a user with the User Manager role can add new organizations.

When a user with the Org Administration role adds an application, a user or a custom report, the organization name and forward slash character are prefixed by default. For example, when a user belonging to the sales organization and with the Org Administration role adds a new user; John, the user name is saved as sales/John.

Organization level roles

The pre-configured organization level roles in EPM restrict the access rights of organization level users. The users can access only that data which is specific to their organization.

Note:

Custom roles are not available for organization level users. For more information, see Roles page field descriptions on page 41.

The organization level roles are:

Organization level role	Description
Org Administration	User accounts with Org Administration access can perform all system-related functions that are specific to their organization.
Org Auditor	User accounts with Org Auditor access can view the audit log entries for the users in their organization.
Org Privacy Manager	User accounts with Org Privacy Manager role can update the following for their organization: • All the Transcription related configuration under **Reporting Parameters** group for an application. • Privacy Settings for traces.
Org Reporting	User accounts with Org Reporting role can generate standard reports, and add, edit, or delete the custom and scheduled reports for their organization.

Table continues…

Organization level role	Description
Org User Manager	User accounts with Org User Manager access can do the following for their organization: • Add new users to their organization. They can change, delete, unlock, and reset the password for existing users in the organization. • Add, change, and delete custom organization roles. • Change the password longevity for the users in their organization. • Change the password longevity for their organization.
Org Web Services	User accounts with Org Web Services access can use Application Interface Web Service to launch any application that is configured on the Experience Portal system, and is assigned to their organization. They can also use Application Logging Web Service to save application logging and call flow data information for any application that is assigned to their organization.

Configuring organization level access in Experience Portal

To configure multi-tenancy in Experience Portal Manager (EPM), you need to enable organization level access in Experience Portal.

Note:

By default, organization level access is disabled.

Enabling organization level access in Experience Portal

Procedure

1. Log on to the EPM by using an administrative account, and open a command window.
2. Log on to Linux on the primary EPM 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. Enter the **`cd $AVAYA_HOME/Support/VP-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 **`EnableOrganizations`** command to enable organization level access in Experience Portal.
5. Type `Y`, and press `Enter` when prompted to restart the *vpms* service.

Result

On the EPM main menu, you can access the *Organizations* page by selecting **User Management** > **Organizations**.

Note:

For more information on creating organization level access in Experience Portal, see Organization level access in Avaya Experience Portal on page 115

Disabling organization level access in Experience Portal

About this task

Note:

By default, organization level access is disabled.

Procedure

1. Log in to the EPM using an administrative account and open a command window.
2. Log in to Linux on the primary EPM 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. Enter the `cd $AVAYA_HOME/Support/VP-Tools` command. `$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 `EnableOrganizations --disable` command to disable organization level access in Experience Portal.

   Note:

   You must delete all organizations before disabling organization level access.
5. Type `Y` and press `Enter` when prompted to restart the *vpms* service.

   The **Organizations** page is disabled in **EPM > User Management**.

Organizations page field descriptions

Use this page to add organizations to the Experience Portal Management system (EPM). You can also delete an existing organization.

Using the defined organization, you can restrict a user's access to only the data which belongs to their organization.

Field or Button	Description
Selection check box	Use this Selection check box to select which organization you want to delete.
Name	The name for the organization. **Note:** The organization name must not contain , ‘ \ < > ( ) “ & ? + = : ! / characters and cannot contain multiple spaces. You cannot change the **Organization Name** after creating it.
Zone	The zone to which an organization is allocated.
 **Zones** filter icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The system displays the **Zones** filter icon only when you create new zones. If you do not create any new zones, you do not see the icon.
Requested SIP Calls	The maximum or minimum number of requests for SIP calls within an organization.
 **Zoom lens icon**	Click this icon to view the SIP allocations within an organization.
Password Longevity (days)	You can set your password for a specified period of time. For an organization user: • If the values are not specified at the role level, the Experience Portal system uses the password longevity specified for the organization. • If the organization does not have any value specified, the Experience Portal system uses the system level password longevity.
 **Pencil icon**	Click this icon to change the password longevity.

Chapter 5: Zoning Topology

Overview

Zoning is a feature of Avaya Experience Portal introduced in release 7.0.

This feature provides an advantage to customers at geographically distributed sites and to customers that have a large system in a single location.

Zoning entails three main advantages for Experience Portal (EP) customers:

- Easy management of large systems, such as MPPs
- Effective management of WAN traffic
- Local Access and Transport Area (LATA) considerations for outbound calls

Zone architecture:

Zones are extended Avaya Experience Portal systems. All resource management and configuration are centralized in zones. Each zone is either coresident to create artificial boundaries for resource management, or is deployed remotely so that all RTP traffic is contained within the location represented by the zone. All primary EPM data traffic crosses zonal boundaries including configuration information, control, status information, and report data. SIP traffic can also cross zonal boundaries though each zone must have a configured proxy.

The zone-specific resources are:

- Auxiliary EPMs
- Media servers
- Speech servers
- VoIP configuration

  Note:

  The proxies are shared across zones but traffic routing causes certain issues. The shared proxies provide call distribution across zones. For example, on ASM, you can choose to route calls to certain numbers only to MPPs in a particular zone. You can also set it up to distribute these calls across MPPs in different zones as well. If the SIP proxy is setup to distribute calls across zones, but one of the zones does not have an application configured for that particular number, the MPPs in that zone will end up rejecting those calls.

- Multi-media configuration

The system stores the resources in the primary EPM configuration database. The primary EPM OMS Poller distributes zone-specific data to each zone. The primary EPM performs the following functions:

- Downloads zone-specific configuration to Media servers, for example:
  - ASR/TTS resources assigned to a zone
  - Proxy configuration assigned to a zone
  - H.323 configuration assigned to a zone
  - Applications assigned to a zone

  Note:

  Application servers are not configured and, therefore, are not assigned to a zone. Such Application servers are common resources.
- Polls for status and statistical data from each server.
- Manages the operational states, for example, **Starts**, **Stops**, **Restarts**, **Reboots**, and **Halts**.
- Downloads the report data, for example, the Contact Summary and Contact Detail reports.

Zonal Entities:

Zonal entities are resources that you can assign to a zone. You can add the following entities to a zone:

- Auxiliary EPM servers
- Media servers
- SMPP and HTTP connections
- Email connections
- Speech servers (ASR and TTS)
- Applications
- HTML Redirectors

Zone support:

- Zone support in H.323 deployment — Stations are not shared across zones.

  Note:

  The system assigns each Communication Manager configuration to a zone. To use Communication Manager across zones, Communication Manager requires individual configuration for each zone.
- Zone support in SIP deployment

Note:

The customer can configure the total concurrent SIP sessions that a tenant uses. This configuration includes all the zones belonging to the tenant.

Failover within a zone

Experience Portal supports Media server failover only within a zone, not across zones. In case of a Media server failover, the system redistributes the licenses of the failed Media server across the other Media servers within that zone. This redistribution ensures that the capacity allocated to the zone remains consistent.

Note:

When a zone becomes unavailable, the administrator manually reassigns the licenses to a different zone.

Real-time management

A user can configure components, collect status from components, and control the operational state of components. The EP system supports each feature, from the primary EPM to the components in all zones. Zonal boundaries only exist for configurations where operational controls and status collection is zone independent and done in parallel to provide high-performance configuration services.

The polling process consists of the following:

- Retrieving component state and status information for every component in parallel including Media servers and auxiliary EPMservers.
- Saving the state and status information of the EPM servers in the database.
- Updating the configuration of the components if the components are in a configurable state. This state depends on the type of data to be configured. The configuration data is synchronized with Media servers and uploaded from auxiliary EPM components.
  - Running states: Telephony resources for media server, ASR/TTS configuration, and Application configuration.
  - Stopped states: All configurations except Telephony for Media servers, including configurations that require a restart.

Component failure within a zone causes licenses to be redistributed within that zone. However, zone licenses are not automatically redistributed across zonal boundaries.

Licenses

Resource Allocation by Zones

In a zonal partitioned system, EP provides the means to manually allocate telephony licenses to zones.

The total number of ports configured for all zones should not exceed the total number of configured telephony licenses allocated to the entire system. When the total number of configured telephony licenses for the entire system falls below the number configured for all zones, the allocation per zone is proportionately adjusted to meet the lower system configuration. Any newly added licenses to the system are not automatically distributed to the zones but must be manually assigned.

Note:

Licenses are allocated to a zone for H.323 and SIP.

Zone licensing

Licenses are assigned to a zone and are not moved between zones unless the total number of available licenses drop below the capacity defined for all of the zones. In this case, the number of licenses are less in proportion to the licenses assigned to each zone. Excess WebLM licenses are not used when the licenses exceed the capacity of the zones.

Rounding errors are distributed to the zones in the following order:

- The remaining licenses are randomly distributed to zones with equal priorities.

Tenant Licensing

Telephony and Announcement Only licenses are taken from WebLM and the licenses are divided between SIP and H.323 in proportion to the number of SIP ports and H.323 stations configured.

```
<WebLM Licenses allocated for SIP>= Licenses x (SIP ÷ (SIP + H323))
```

Where:

- Licenses = Total WebLM Licenses (Telephony + Announcement Only)
- SIP = Maximum Simultaneous Calls (SIP configuration)
- H323 = Total Number of H.323 stations configured

H.323 stations are assigned for applications within organizations through CM hunt groups or vectors. Port groups are configured through EP Administration pages to associated stations to a specific hunt group that becomes associated to a particular application through a pilot number. The application is assigned to an organization through EP configuration web pages.

WebLM SIP licenses can be assigned to organizations and in turn taken from the organizational license pool and assigned to specific applications within organizations. There are two types of organizations:

- Default Organization – The “Default Organization” is not configured and represents applications that are not owned by an organization. This allows applications to be managed with the exception that resource usage by an application is supported. There can be only one default organization that initially has no licenses allocated but which can be configured. Any licenses assigned to the default organization are taken from the Global Common Licenses pool called WebLM Licenses (SIP).

- Configured Organization (Organization A & B) – A “Configured Organization” is created and edited through the Administration web pages. Licenses are assigned to organizations through the Administration web pages. Any licenses assigned to the organization are taken from the Global Common Licenses pool [WebLM Licenses (SIP)].

There are two license types for applications:

- Guaranteed Licenses – These are licenses which only the application can use and are not given to any other application. Applications are assigned guaranteed licenses from the pool of licenses assigned to a Configured organization or from the Default organization depending on where the application is configured. Applications can be configured with no guaranteed licenses and can be starved by other applications as the common licenses become exhausted.
- Common Licenses – These licenses are shared by all the applications after exhausting the guaranteed licenses. The guaranteed licenses are distributed across the media servers.It is possible for the guaranteed licenses to be exhausted on a media server forcing common licenses used to run the application when another media servers still have guaranteed licenses available for the application.

Zone filters

When you add or change resources or start with an application, only the zones selected by the **Zone Filter** icon are available in the **Zone** drop-down list.

The zone filter is applicable for the entire user session, that is, the web pages display the resources assigned to the selected zone till the user logs off. At any given time, the user is able to reset or change the zone filter. The zone filter is retained when the user logs off from the web pages.

Restrictions on moving resources between zones

Resources assigned to a zone can be moved from one zone to another zone. However, there are certain restrictions for moving a resource from one zone to another.

Resource	Restrictions
Applications	No applications can be moved from one zone to another.
Organizations	No applications are configured in the zone from which the resource is being moved.
Auxiliary EPM servers	If a coresident SMS processor uses an SMPP connection, which is not shared, changing zones is not possible.

Table continues…

Resource	Restrictions
Media servers	The media server being moved must be stopped.
ASR servers	All media servers are stopped in the zone from which the resource is being moved.
TTS servers	All media servers are stopped in the zone from which the resource is being moved.
H.323 connections	All media servers are stopped in the zone from which the resource is being moved.
SIP connections	All media servers are stopped in the zone from which the resource is being moved.
SMPP connections	All auxiliary EPM servers must be stopped in the zone from which the resource is being moved.
HTTP connections	All auxiliary EPM servers must be stopped in the zone from which the resource is being moved.
Email connections	All auxiliary EPM servers must be stopped in the zone from which the resource is being moved.

Adding a zone

Before you begin

- Ensure that Experience Portal is installed on your system.
- To use the Zoning feature and to add zones to the **Zones** list, buy a zone license with Experience Portal .

Note:

The Zoning feature is available only with Experience Portal 7.0 and later. If you have Experience Portal 6.0 or any earlier version of Voice Portal, upgrade to Experience Portal 8.x and later and purchase a zone license.

Procedure

1. Log on to the EPM web interface.
2. Click **System Configuration** > **Zones**.
3. On the **Zones** page, click **Add**.
4. On the Add Zone page, enter appropriate information and click **Save**.

   The EPM displays the Zones page with the zone added to the list of zones.

Changing the configuration of a zone

Procedure

1. Log on to the EPM web interface.
2. Click **System Configuration** > **Zones**.
3. Click the name of the zone that you want to change.
4. On the Change Zone page, enter appropriate information in the fields that you want to change.
5. Click **Save**.

Deleting a zone

About this task

Use this procedure to delete a zone that you added. Note that you cannot delete the Default zone.

Procedure

1. Log on to the EPM web interface.
2. Click **System Configuration** > **Zones**.
3. In the **Zones** field, select the check box for the zone that you want to delete.
4. Click **Delete**.

   The EPM deletes the selected zone.

Filtering a zone

About this task

Use this procedure to filter one or more zones and set the time zone.

Procedure

1. Log on to the EPM web interface.
2. On the right of the page, click the **Zones** filter icon .
3. On the Zone Filter page, select the check box for the name of the zone that you want to filter.
4. In the **Display Time Zone** field, select the time zone that you want to set.
5. Click **Save**.

Viewing the details of a zone

Procedure

1. Log on to the EPM web interface.
2. Click **System Configuration** > **Zones**.
3. On the **Zones** page, click the **View Zone Details** icon  .

   The EPM displays the <Zone name> details page with all the resources that are assigned to a zone.

Chapter 6: Email management

Email overview

Experience Portal 7.0 and the later versions support email as an additional communication channel.

The major features driving the email capability are:

- Sending outbound email messages.
- Receiving and processing inbound email messages.
- Sending a reply to inbound email messages.
- Handling of delivery receipts from email messages.

The major components that are enhanced or added to the system include:

- **Email Web Application** : A web application that provides a web user interface for configuring and managing the email-related components.
- **Email Processor** : A web application that interacts with an email server over the SMTP and POP3/IMAP4 protocols, routes messages to Orchestration Designer email applications, and provides methods for sending email messages.
- Orchestration Designer: A new application type called **Email** is added.
- **Application Interface Web Service** : The service is enhanced for sending multimedia messages.

Experience Portal provides additional support for the multichannel features in the following ways:

- Incoming email messages can be routed to Orchestration Designer email applications.
- Delivery receipts can be routed to Orchestration Designer email applications.
- Orchestration Designer applications of any type can send email messages. For example, a voice application can send an email message.

  Note:

  Experience Portal supports the following protocols:

  - POP3 or IMAP4 for incoming emails and SMTP for outgoing emails.
  - TCP or TLS or STARTTLS connections for inbound connections and outbound connections
- Experience Portal provides multilingual email support.
- Experience Portal supports attachments for inbound and outbound email messages.

- Experience Portal provides built-in grammar support like word spotting for text-based messages.
- The EPM system monitor displays real-time email statistics.
- Contact and Session reports display the inbound and outbound email statistics. Emails have filters and summary options.
- EPM Log Viewer, Alarm Manager, and Audit Log display voice, email, and SMS-related information.
- The EPM installation program installs the email support application
- Experience Portal provides high availability and scalability with load balancing across connections.

Email typical flow

Inbound message with reply

The flow of a typical incoming email consists of the following steps:

- The incoming email message is routed through the Internet to an email server. For example, Microsoft Exchange.
- Email Processor monitors the mailbox on the email server and detects a new message.
- Email Processor launches the Orchestration Designer email application on an application web server based on **To**, **Subject**, or **Header** as specified in the application configuration on the EPM.
- The email application can gain access to the details of the incoming message by examining a variable called **Message** that has fields related to the email message: **To**, **From**, **Subject**, **Body**, and **Attachments**. The **Message** variable is similar to the **Session** variable, but only contains fields related to a message, such as email and SMS messages.
- The Orchestration Designer application can generate a reply using the Prompt tag mechanism or generate a new outbound email by using the Orchestration Designer notification connector. Both methods trigger the Orchestration Designer runtime to send an email message to Email Processor.

Note:

Experience Portal supports two types of inbound email messages:

- Regular
- Delivery Status Notification (DSN): This type of message might be generated by any email server that processes the message before reaching the final destination.

Outbound message

The Application Interface Web service is enhanced to provide a **launchEmail** method and a **sendEmail** method.

The **launchEmail** method is a web services request that calls an email application. The **launchEmail** web service request succeeds when the Orchestration Designer application begins

to run. The launched Orchestration Designer application sends an email message by invoking the notification connector. After the message is sent, a **sendEmail** web service call is created.

The **sendEmail** method enables an application that can make web service calls to send an email message to an email server through Email Processor. The web service call succeeds when the Email Processor has accepted the message. An email application can be notified when an email message is delivered to the email server. This status is sent to the Notification URL that is specified when configuring the email application on the EPM. An application can be further notified of any errors that occur after the email server has accepted the message. These email DSN message types are sent to the application if the application was configured to support either **Delivery** or **Regular and Delivery** message types. Voice applications that call **sendEmail** must specify the name of a configured email application in order to receive error notifications.

Note:

An Email Notification Connector is a pluggable data connector that is used to send an email message from a speech application or a message application that is created for a channel other than the email channel.

Notifications are done through the configured applications. An application can be configured by short code that can have an application URL which is launched by Email Browser when notifications are received. The email server relies on the SMTP delivery status notification mechanism to support the registered delivery of email messages. The Email Processor submits the SMTP delivery notifications as requested by the client. On receiving the delivery receipt from SMTP, Email Processor stores all the information from the message in the delivery receipt record so that Email Browser can make that information available to the delivery receipt application, see the Orchestration Designer documentation.

For more information on these new web service methods, see:

- LaunchEmail method on page 664
- SendEmail method on page 676

Email processors

An email processor is an application that is hosted on the multimedia server. The multimedia server is a service that is deployed on the Primary and the Auxiliary EPMs. An email processor manages connections to one or more email servers and handles the routing of incoming messages to configured applications. The email processor additionally provides Web service interface methods that the Application Interface Web Service uses to send email messages.

Using the Email Processors web page, administrators can add, modify, and delete one or more email processors.

Configure an Auxiliary EPM before you configure an email processor to be hosted on that AuxiliaryEPM. The email processor inherits the name, host address, and zone of the EPM.

Email processor states

An email processor maintains the following states for managing the functions:

State	Description
Not Running	The server is either stopped or not started yet.
Starting	The server start request is initiated, and is in the process of initialization.
Running	The server is up and functional.
Stopping	The server shutdown is requested.
Need Configuration	The server does not find configuration.
Need Connections	The server has configuration but does not have any connections assigned or configured.
Degraded	The server has configuration and connections. However, some or all connections are not working.
Error	The server data returned has been deemed "stale" (no new data retrieved after a period of 3 minutes), or 2) unexpected return code retrieved from a poll to server.
Stopped	The server is stopped.

Adding an email processor

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **Multi-Media configuration** > **Email** > **Email Processors**.
3. On the Email Processor tab, click **Add**.

   EPM displays the Add Email Processor page.
4. In the **Name** field, click the name of the EPM server.
5. In the **Enable** field, click one of the following:
   - **Yes**
   - **No**
6. In the **Categories and Trace Levels** group, click **Custom**.

   If you select **Use Email Settings**, then EPM disables the trace level buttons.
7. In the **Email Processor** field, click one of the following to set the trace level of Email Processors:
   - **Off**
   - **Fine**

- **Finer**
- **Finest**

The default trace level setting is **Off**.

8. In the **Email Browser** field, click one of the following to set the trace level of Email Browsers:
   - **Off**
   - **Fine**
   - **Finer**
   - **Finest**

   The default trace level setting is **Off**.
9. Click **Save**.

Changing the configuration of an email processor

Procedure

1. Log on to the EPM web interface.
2. On the EPM navigation pane, click **Multi-Media configuration** > **Email** > **Email Processors**.
3. On the Email Processor tab, click the name of the email processor whose configuration you want to change.

   EPM displays the Change Email Processor page.
4. In the **Enable** field, click one of the following:
   - **Yes**
   - **No**
5. In the **Categories and Trace Levels** group, click **Custom**.

   If you click **Use Email Settings**, then EPM disables the trace level buttons.
6. In the **Email Processor** field, click one of the following to set the trace level of Email Processors:
   - **Off**
   - **Fine**
   - **Finer**
   - **Finest**

   The default trace level setting is **Off**.

7. In the **Email Browser** field, click one of the following to set the trace level of Email Browsers:
   - **Off**
   - **Fine**
   - **Finer**
   - **Finest**

   The default trace level setting is **Off**.
8. Click **Save**.

Deleting an email processor

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **Multi-Media configuration** > **Email** > **Email Processors**.
3. Select the check box for the email processor that you want to delete.
4. Click **Delete**.

   EPM deletes the selected email processor.

Email connections

You can add, modify, and delete the configuration of an email connection on the Email Connections Web page. An email connection specifies the configuration parameters an email processor uses to connect with an email server. The email processor and the email server interact over the SMTP protocol for sending messages and over the IMAP4 or POP3 protocol for receiving messages. An email connection can belong to a zone. An email processor uses the email connections that belong to the same zone as the email processor server.

In versions earlier than Experience Portal 7.0, email connections were called ‘email servers’ and facilitated only the configuration of SMTP related parameters. The capability to receive email messages over IMAP4 or POP3 was added in Experience Portal 7.0 release.

Adding an email connection

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **Multi-Media configuration** > **Email** > **Email Connections**.
3. Click **Add**.

EPM displays the Add Email Connection page.

4. In the **Zone** field, click the name of the zone.
5. In the **Organization** field, click one or more organizations.
6. In the **Name** field, enter the name of the email connection.
7. In the **Enable** field, click one of the following:
   - **Yes**
   - **No**
8. In the **Registered Delivery** field, click the type of delivery.
9. In the **Type** field, click one of the following types of email connection:
   - **Outgoing**: Enter appropriate information in the **Outgoing Mail** section.
   - **Incoming and Outgoing**: Enter appropriate information in the **Incoming Mail** section.
10. In the **Outgoing Mail (SMTP)** section, do the following:
    a. In the **Server Address** field, enter the address of the email server.
    b. In the **Transport Protocol** field, click one of the transport protocols.
       - **TCP**
       - **TLS**
       - **STARTTLS**
    c. In the **Port** field, enter the port number that is used for the email connection.
    d. In the **Sender Email Address** field, enter the email address of the sender.
    e. In the **User Name** field, enter the user name.
    f. In the **Use Authentication** field, click **Yes**.

       You can enter the password only if you select **Yes**.
    g. In the **Password** field, enter the password.
11. In the **Incoming Mail** section, do the following:
    a. In the **Protocol** field, click one of the protocols.
       - **POP3**
       - **IMAP**
    b. In the **Server Address** field, enter the address of the email server.
    c. In the **Transport Protocol** field, click one of the transport protocols.
       - **TCP**
       - **TLS**
       - **STARTTLS**

d. In the **Port** field, enter the port number that is used for the email connection.

   For POP3 , the default port number is 110.

   For IMAP, the default port number is 143.

e. In the **User Name** field, enter the user name.

f. In the **Use Authentication** field, click one of the options.

   - **Yes**
   - **No**

g. In the **Password** field, enter the password.

h. In the **Folder to check for new message** field, click one of the folders where you can check new messages.

   - **Inbox**
   - **Other**

i. In the **Expunge** field, click one of the options.

   - **Yes**
   - **No**

j. In the **Delete message after reading** field, click one of the options.

   - **Yes**
   - **No**

   If you use **POP3** protocol, this field is disabled.

k. In the **Move message after reading** field, click one of the options.

   - **Yes**
   - **No**

   If you use **POP3** protocol, this field is disabled.

l. In the **Mark message as read** field, click one of the options.

   - **Yes**
   - **No**

   If you use **POP3** protocol, this field is disabled.

m. In the **Folder to move message into** field, enter the name of the folder where you want to save the message.

12. Click **Save**.

Changing the configuration of an email connection

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **Multi-Media configuration** > **Email** > **Email Connections**.
3. In the **Name** column, click the name of the email connection whose configuration you want to change.

   EPM displays the **Change Email Connection** page.
4. In the **Zone** field, click the name of the zone.
5. In the **Organization** field, click one or more organizations.
6. In the **Enable** field, click one of the following:
   - **Yes**
   - **No**
7. In the **Registered Delivery** field, click the type of delivery.
8. In the **Type** field, click one of the following types of email connection:
   - **Outgoing**: Enter appropriate information in the **Outgoing Mail** section.
   - **Incoming and Outgoing**: Enter appropriate information in the **Incoming Mail** section.
9. In the **Outgoing Mail (SMTP)** section, do the following:
   a. In the **Server Address** field, enter the address of the email server.
   b. In the **Transport Protocol** field, click one of the transport protocols.
      - **TCP**
      - **TLS**
      - **STARTTLS**
   c. In the **Port** field, enter the port number that is used for the email connection.
   d. In the **Sender Email Address** field, enter the email address of the sender.
   e. In the **User Name** field, enter the user name.
   f. In the **Use Authentication** field, click **Yes**.

      You can enter the password only if you select **Yes**.
   g. In the **Password** field, enter the password.
10. In the **Incoming Mail** section, do the following:
    a. In the **Protocol** field, click one of the protocols.
       - **POP3**

- **IMAP**

b. In the **Server Address** field, enter the address of the email server.

c. In the **Transport Protocol** field, click one of the transport protocols.

- **TCP**
- **TLS**
- **STARTTLS**

d. In the **Port** field, enter the port number that is used for the email connection.

For POP3 , the default port number is 110.

For IMAP, the default port number is 143.

e. In the **User Name** field, enter the user name.

f. In the **Use Authentication** field, click one of the options.

- **Yes**
- **No**

g. In the **Password** field, enter the password.

h. In the **Folder to check for new message** field, click one of the folders where you can check new messages.

- **Inbox**
- **Other**

i. In the **Expunge** field, click one of the options.

- **Yes**
- **No**

j. In the **Delete message after reading** field, click one of the options.

- **Yes**
- **No**

If you use **POP3** protocol, this field is disabled.

k. In the **Move message after reading** field, click one of the options.

- **Yes**
- **No**

If you use **POP3** protocol, this field is disabled.

l. In the **Mark message as read** field, click one of the options.

- **Yes**
- **No**

If you use **POP3** protocol, this field is disabled.

m. In the **Folder to move message into** field, enter the name of the folder where you want to save the message.

11. Click **Save**.

Deleting an email connection

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **Multi-Media configuration** > **Email** > **Email Connections**.
3. Select the check box of the email connection that you want to delete.
4. Click **Delete**.

   EPM deletes the selected email connection.

Adding an email application to Experience Portal

Before you begin

Ensure that the email processor and other required connections are configured in the Experience Portal system.

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **System Configuration** > **Applications**.
3. On the Applications page, click **Add**.
4. On the Add Application page, enter appropriate information, and click **Save**.

Changing the settings of an email application

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **System Configuration** > **Applications**.
3. In the **Name** column, click the name of the application whose settings you want to change.
4. On the Change Application page, enter appropriate information, and click **Save**.

Deleting an email application

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **System Configuration** > **Applications**.
3. On the Applications page, select the check box of the application that you want to delete.
4. Click **Delete**.

   EPM deletes the selected email application.

Configuring system parameters for email browser settings

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **Multi-Media configuration** > **Email** > **Email Processors** > **Browser Settings**.
3. In the **Fetch Timeout** field, enter the maximum number of seconds that the email browser must wait for the application server to return the requested page.
4. In the **Proxy Server** field, enter the fully qualified path to the proxy server.
5. In the **Proxy Port** field, enter the port number of the proxy server.
6. In the **Number of Threads** field, enter the maximum number of threads that the email browser must use for an asynchronous fetch.

   Valid values are 1 through 500. The default is 50.
7. Click **Save**.

Configuring system parameters for email settings

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **Multi-Media configuration** > **Email** > **Email Processors** > **Email Settings**.
3. In the **Log Level** field, click the level that you want to set.

   The default is **Info**.

4. In the **Record Handling on Email** section, in the **Session Data(SDR)** and **Call Data(CDR)** fields, do the following:
   a. Select the **Enable** check box.
   b. In the **Retention Period (days)** field, type the number of days for the retention period of the records.

      Note:

      The retention period has an impact on how long Call Data Records and Session Data Records are saved in the operational database that the processor uses. The retention period does not have an impact on how long these records are saved in the reporting database.
5. In the **Categories and Trace Levels** group, do the following:
   a. In the **Email Processor** field, click one of the following to set the trace level of Email Processors:
      - **Off**
      - **Fine**
      - **Finer**
      - **Finest**

      The default trace level setting is **Fine**.
   b. In the **Email Browser** field, click one of the following to set the trace level of Email Browsers:
      - **Off**
      - **Fine**
      - **Finer**
      - **Finest**

      The default trace level setting is **Fine**.
6. Click **Save**.

Next steps

For more information about parameters and return values of the email application, see the following:

- LaunchEmail method on page 664
- SendEmail method on page 676

Multimedia Tomcat server

A new instance of Tomcat server is deployed on the Primary and the Auxiliary EPMs. This server hosts the following:

- An SMS service Web application comprising an SMS Processor and an SMS Browser
- An Email service web application comprising Email Processor and Email Browser.

This new server is another instance of Tomcat and is different from the coresident application server. The coresident application server is yet another instance of Tomcat server. The multimedia server hosts the SMS and email services.

The Tomcat multimedia server is installed in the $MMSSERVER_HOME folder and runs as a Linux service as **mmsserver**.

mmsserver service supports the following commands:

- **service mmsserver status**: for checking the status of the mmserver service
- **service mmsserver start**: for starting the mmsserver service
- **service mmsserver stop** : for stopping the mmsserver service
- **service mmsserver restart**: for restarting the mmsserver service

The multimedia service is a part of the EPM server and the commands issued to the EPM server through the EPM Manager web pages are also issued to the multimedia service.

Email reporting filters

Experience Portal 7.0 and later versions have a new media type filter for email that is added to the Contact Detail and Contact Summary reports.

The following are the main filters that are available for Email:

- Email
- Email DSN

Experience Portal 7.0 and later versions support the capability to filter the messages on Email servers. This capability consists of the number of messages sent to one or more Email servers as well as the number of messages received from one or more Email servers.

The following information is available in these reports:

- The number of messages sent
- The number of messages received
- The number of delivery receipts requested
- The number of receipts pending
- The number of receipts received

All existing filters for the Contact Detail and Contact Summary reports are applied to reporting records that are created by incoming or outbound email

Chapter 7: SMS management

SMS overview

Experience Portal 7.0 and later versions support SMS as an additional communication channel.

The major features driving the SMS capability are:

- Sending outbound SMS messages.
- Receiving and processing inbound SMS messages.
- Sending a response to inbound SMS messages.
- Handling of delivery receipts from SMS messages.

The major components that are enhanced or added to the system include:

- **SMS Web Application** : A web application that provides a web user interface for configuring and managing the SMS-related components.
- **SMS Processor** : A web application that interacts with an SMSC server over HTTP/HTTPS or the SMPP protocol , routes messages to Orchestration Designer SMS applications, and provides methods for sending SMS messages.
- Orchestration Designer: A new application type called **SMS** is added.
- **Application Interface Web Service** : The service is enhanced for sending multimedia messages.

Experience Portal provides additional support for the multichannel features in the following ways:

- Incoming SMS can be routed to Orchestration Designer SMS applications.
- Orchestration Designer SMS application can reply to an incoming SMS.
- Delivery receipts can be routed to Orchestration Designer SMS applications.
- Orchestration Designer applications of any type can send an SMS message. For example, a voice application can send an SMS message.
- Experience Portal provides support for http and https for an outbound SMS.
- Experience Portal provides support for SMPP for inbound and outbound SMS.
- Experience Portal provides multilingual SMS support.
- Experience Portal provides built-in grammar support like word spotting for text-based messages.
- The EPM system monitor displays real-time SMS statistics.
- Contact and Session reports display the inbound and outbound SMS statistics. Filters and summary options exist for SMS.

- EPM Log Viewer, Alarm Manager, and Audit Log display voice, email, and SMS-related information.
- The EPM installation program installs the SMS support application.
- Experience Portal provides high availability and scalability with load balancing across connections.

SMS typical flow

Inbound message with reply

The flow of a typical incoming SMS consists of the following steps:

- The incoming SMS message is routed to the Short Message Service Center (SMSC) that is located in the cloud. The SMSC is registered with cell phone providers as the owner of the short code or long number to which the message is addressed.
- SMS Processor maintains an open connection to the SMSC and receives a deliver event for the new message
- SMS Processor launches the Orchestration Designer SMS application on an application web server based on Short Code or Long Number and optional message content keywords as specified in the application configuration on the EPM.
- The SMS application can gain access to the details of the incoming message by examining a variable called **Message** that has fields related to the SMS message: **To**, **From**, and **Body**. The **Message** variable is similar to the **Session** variable, but only contains fields related to a message, such as email and SMS messages.
- The Orchestration Designer application can generate a reply using the Prompt tag mechanism or generate a new outbound SMS by using the notification connector. Both methods cause the Orchestration Designer runtime to communicate with the SMS Processor to send an SMS message.

Note:

Experience Portal supports three types of inbound SMS messages:

- Regular
- Notification: A Notification is received when the SMSC passes the outbound message on to the next hop.
- Delivery receipt: A Delivery receipt is received when an outbound message reaches the destination.

Outbound message

The Application Interface Web service is enhanced to provide a **launchSMS** method and a **sendSMS** method.

The **launchSMS** method is a web services request that calls an Orchestration Designer SMS application. The **launchSMS** web service request succeeds when the Orchestration Designer application begins to run. The launched Orchestration Designer application sends an SMS

message by invoking the notification connector. After the message is sent, a **sendSMS** web service call is created.

The **sendSMS** method enables an application that can make web service calls to send SMS to an SMSC through the SMS Processor. The web service call succeeds when the processor accepts the message. An SMS application can be notified when the message is delivered to the SMSC. These SMS notification messages are sent to the Notification URL that is specified when configuring the SMS application on the EPM. Voice applications that call **sendSMS** must specify the name of a configured SMS application to receive notifications. In addition, an application can send the message with a delivery receipt request. If the application is configured on the EPM to support delivery message types and if the cell phone provider of the recipient returns the delivery receipt, the message is routed to the original sending application. For more information about the notification application, see the Orchestration Designer documentation.

Note:

An SMS Notification Connector pluggable data connector (PDC) is used to send an SMS message from a speech application or a message application that is created for a channel other than the SMS channel

For more information about these new web service methods, see:

- LaunchSMS method on page 666
- SendSMS method on page 678

SMS Processors

An SMS Processor is an application that is hosted on the multimedia server. The multimedia server is a service that is deployed on the Primary EPM and the Auxiliary EPMs. An SMS Processor manages connections to one or more SMSCs. The Processor handles the routing of incoming SMS, notifications, and receipts to configured applications and also provides web service interface methods that are used by the Application Interface Web Service to send an SMS message.

The SMS Processors web page allows administrators to add, modify, and delete one or more SMS Processors.

In order to configure an SMS Processor which is hosted on Auxiliary EPM, the Auxiliary EPM must be configured before configuring the associated SMS Processor. The SMS Processor that is configured and hosted on an EPM automatically inherits the name, host address and zone of the EPM on which the SMS Processor resides.

SMS processor states

An SMS Processor maintains the following states for managing functions:

State	Description
Not Running	The server is either stopped or not started yet.
Starting	The server start request is initiated, and is in the process of initialization.
Running	The server is up and functional.
Stopping	The server shutdown is requested.
Need Configuration	The server does not find configuration.
Need Connections	The server has configuration but does not have any connections assigned or configured.
Degraded	The server has configuration and connections. However, some or all connections are not working.
Error	The server data returned has been deemed "stale" (no new data retrieved after a period of 3 minutes), or 2) unexpected return code retrieved from a poll to server.
Stopped	The server is stopped.

Adding an SMS processor

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **Multi-Media Configuration** > **SMS**.
3. On the SMS Processors tab, click **Add**.
4. In the **Name** field, click the name of the server.
5. In the **Enable** field, click one of the following:
   - **Yes**
   - **No**
6. In the **Categories and Trace Levels** group, click **Custom**.

   If you select **Use SMS Settings**, then EPM disables the trace level buttons.
7. In the **SMS Processor** field, click one of the following to set the trace level of SMS processors:
   - **Off**
   - **Fine**
   - **Finer**
   - **Finest**

   The default trace level setting is **Off**.

8. In the **SMS Browser** field, click one of the following to set the trace level of the SMS browsers:
   - **Off**
   - **Fine**
   - **Finer**
   - **Finest**

   The default trace level setting is **Off**.
9. Click **Save**.

Changing the configuration of an SMS processor

Procedure

1. Log in to the EPM web interface
2. From the EPM main menu, select Home > Multi-Media configuration > SMS > SMS Processors.
3. Select the check box next to the SMS Processor that you want to change.
4. Click the SMS Processors that you have selected. The system opens the **Change Processor** page.
5. In the **Enable** field, select either the **Yes** or **No** radio button.
6. From the **Categories and Trace Levels** group, select **Customs**.

   If you select **Use SMS Settings**, then the trace level buttons are disabled.
7. Select the trace level that you want to set for the SMS Processor.

   The options are:
   - Off
   - Fine
   - Finer
   - Finest

   The default trace level setting is **Off**.
8. Select the trace level that you want to set for the SMS Browser.
   - Off
   - Fine
   - Finer
   - Finest

   The default trace level setting is **Off**.

9. Click **Save**.

Deleting an SMS processor

Procedure

1. Log on to the EPM web interface.
2. On the EPM main menu, click **Multi-Media Configuration** > **SMS**.
3. On the SMS Processors tab, select the check box of the SMS processor that you want to delete.
4. Click **Delete**.

   EPM deletes the selected SMS processor.

Adding an SMS application to Experience Portal

Before you begin

Ensure that the SMS processor and other required connections are configured in the Experience Portal system.

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role
2. On the EPM main menu, click **System Configuration** > **Applications**.
3. On the Applications page, click **Add**.
4. On the Add Application page, enter appropriate information, and click **Save**.

Changing the settings of an SMS application

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. In the **Name** column, click the name of the application whose settings you want to change.
4. On the Change Application page, enter appropriate information, and click **Save**.

Deleting an SMS application

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role
2. On the EPM main menu, click **System Configuration** > **Applications**.
3. On the Applications page, select the check box for the SMS application that you want to delete.
4. Click **Delete**.

   EPM deletes the selected SMS application.

Configuring HTTP and SMPP connections

Adding an HTTP connection

Procedure

1. Log in to the EPM web interface.
2. From the EPM main menu, select Home > Multi-Media configuration > SMS > HTTP Connections.
3. On the **HTTP Connections** page, click **Add**. The system displays the **Add HTTP Connection** page.
4. From the **Zone** field, select the name of the zone.
5. In the **Name** field, type the name of the HTTP connection.
6. From the **Enable** field, select the relevant option.

   The options available are **Yes** and **No**.
7. Select the accurate transport protocol.

   The available options are **TCP** and **TLS**.

   Note:

   For **Avaya Zang** and **AT&T Landline Texting** connectors, select **TLS**.
8. Enter the host address of the SMSC.

   Note:

   For Avaya Zang connector, the host address is api.zang.io.
9. Enter the port number that is used for the SMS connection.

10. Enter the path of the SMSC.
11. Enter the user name.

    Note:

    For Avaya Zang connector, the user name is the Account SID on the Zang Dashboard at cloud.zang.io.
12. Enter the password.

    Note:

    For Avaya Zang connector, the password is the Auth Token on the Zang Dashboard at cloud.zang.io.
13. Enter your Application Programming Interface (API) ID to facilitate your connection to the connector.
14. In the **Connector** field, select the connector.

    The options available are **Avaya Zang**, **AT&T Landline Texting**, **AOS SMS**, **Clickatell**, **i2SMS**, **ONE WAY SMS**, **WEBTEXT**, and **Zipwhip**.
15. From the **Type** field, select the type of connector.

    The options available are **Outgoing** and **Incoming and Outgoing**.
16. From the Use **HTTP Proxy** field, select **Yes**.

    The available options are **Yes** and **No**. You can configure the subsequent fields only if you select **Yes**.
17. Enter the address of the proxy server.
18. Enter the proxy port number.

    The default port number is 8000.
19. Enter the sender ID that can be either a short code or a long number.
20. Select one or more organizations from the **Organization** list.
21. **(Optional)** Click the **Additional Entry** option and enter subsequent short codes or long numbers.
22. Click **Save**.

Add HTTP Connection Page Field Descriptions

Use this page to add the configuration of an HTTP connection.

Field or Button	Description
Zone	Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only when you create new zones. If you do not create any new zones, you do not see the drop-down box.
Name	Enter the name of the HTTP connection.
Enable	The options are: • Yes • No
Transport Protocol	The protocol used to send request to SMSC. Select the transport protocol from the drop-down list box. The options are: • **TCP** • **TLS** **Note:** For **Avaya Zang** and **AT&T Landline Texting** connectors, select **TLS**.
Host Address	The IP address of the service provider or the Short Message Service Center (SMSC) server. Enter the host address of the service provider. **Note:** For Avaya Zang connector, the host address is api.zang.io.
Port	Enter the port number to be used for the connection.
Path	Enter the path of the URL to be used for communicating with the SMSC. The default is “ ”. This is the portion of the URL which is after the host address and the port. As an example if the URL is http://hostaddress:port/location, enter location here.
User Name	Enter the user name. **Note:** For Avaya Zang connector, the user name is the Account SID on the Zang Dashboard at cloud.zang.io. This Account SID should only be used in one active connection. This means that you need to use only one EPM connection if multiple Avaya Zang short codes or long numbers are associated with the same Account SID.

Table continues…

Field or Button	Description
Password	The password for the user supplied by the service provider. Enter the password. **Note:** For Avaya Zang connector, the password is the Auth Token on the Zang Dashboard at cloud.zang.io.
API ID	The user identifier supplied by the service provider. Enter the Application Programming Interface (API) ID. **Note:** For Avaya Zang connector, do not enter any value in the **API ID** field. If you plan to share the same Account SID across multiple EP systems, then enter the API ID. To share the Account SID, enter a unique number as the API ID for each EP system. This unique API ID should be appended to the SMS Request URL that is configured at cloud.zang.io. For example, if you enter 1 as the API ID for EP system 1, and 2 as the API ID for EP system 2, the SMS Request URL for an SMS number managed by EP system 1 would be: `https://pubsub.zang.io/[Account SID]/SMS/Incoming1` , and the SMS Request URL for an SMS number managed by EP system 2 would be: `https://pubsub.zang.io/[Account SID]/SMS/Incoming2`.

Table continues…

Field or Button	Description
Connector	The HTTP mechanism supported through a connector. The options are: • Avaya Zang • AT&T Landline Texting • AOS SMS • Clickatell • i2SMS • ONE WAY SMS • WEBTEXT • Zipwhip **Note:** For **AT&T Landline Texting** and **Zipwhip**, the customer must obtain a Session Key from the Sales or Support team. The Session Key is specific to each SMS-enabled phone number, so one SMS connection is required on the EPM for each phone number. The Session Key contains a `:` character. The characters to the left of the `:` character should be entered into the **Username** field of an EPM SMS Connection and the characters to the right should be entered into the **Password** field. For example, a typical Session Key (obtained from AT&T Landline Texting or Zipwhip) looks like the following: `3d0f1dde-aaff-4ce8-b61a-af212a860abc:123456789` Where, • `3d0f1dde-aaff-4ce8-b61a-af212a860abc` is the Username. • `123456789` is the Password.

Table continues…

Field or Button	Description
Type	An HTTP Connector can be of two types. The options are: • **Outgoing**: The **Outgoing** connector is used for sending out SMS messages only. It is assigned to all SMS processors in the same zone. • **Incoming and Outgoing**: The **Incoming and Outgoing** connector is used for processing incoming SMS messages and also for sending out SMS messages. It needs to be assigned to a specific SMS processor. **Note:** This option is only available for connectors that support both incoming and outgoing SMS messages. By default, an HTTP connector can only be used for processing outgoing messages. **Note:** For Avaya Zang connections, if you select **Incoming and Outgoing** to respond to incoming SMS messages, you must configure the **SMS Request URL** at `cloud.zang.io` to forward incoming SMS messages to the `pubsub.zang.io` server. You need to log in to your zang.io account, click **Numbers** on the top of the Zang dashboard, select **Manage Numbers**, and then click the purchased SMS telephone number. For example, `https://pubsub.zang.io/ABCc8890841e5034bdf1a149c2a5b6xyz/SMS/Incoming` is the **SMS Request URL**. Where, `ABCc8890841e5034bdf1a149c2a5b6xyz` is the Account SID that displays when you log in to the zang.io console. To support incoming MMS, use the same URL in the **MMS Request URL** field on the MMS tab for the Zang SMS/MMS telephone number. **Note:** From Experience Portal 7.2.1, Avaya Zang connections must be configured to use https. You may need to install the Baltimore CyberTrust Root certificate if the connections fail to connect with an SSL error. You can download the certificate from https://www.digicert.com/CACerts/BaltimoreCyberTrustRoot.crt. To import the certificate, on the EPM web page, click **Security** > **Certificates**, and the click **Import** on the Trusted Certificates tab. Restart the EPM from the EPM Manager.
Use HTTP Proxy	The proxy setup to be used while sending the HTTP(s) request. Comma-separated values comprising of proxy protocol, proxy server, and proxy port. The options are: • Yes • No

Table continues…

Field or Button	Description
Proxy server	The proxy setup to be used while sending the HTTP(s) request. Comma-separated values comprising of proxy protocol, proxy server, and proxy port. Enter the name of the proxy server.
Proxy Port	The proxy setup to be used while sending the HTTP(s) request. Comma-separated values comprising of proxy protocol, proxy server, and proxy port. Enter the port number of the proxy server.
Short Code/Long Number **Organization**	Enter the short code or the long number provided by the SMSC. Use the Additional Entry link to specify additional short codes or long numbers. The type of organization that can use the short code. Select the relevant type from the multi-select drop-down list. The options are: • **<All>** : All organizations can use this short code. If the administrator selects multiple options in the drop-down list, only <All> is saved. • **<None>**: None of the organizations can use this short code. The administrator can select other organizations in addition to <None>. • The other organizations that are enabled in the system.

Changing the configuration of an HTTP connection

Procedure

1. Log in to the EPM web interface.
2. From the EPM main menu, select Home > Multi-Media configuration > SMS > HTTP Connections.
3. In the **Name** field, click the name of the HTTP connection. The system displays the **Change HTTP Connection** page.
4. From the **Zone** field, select the name of the zone.
5. From the **Enable** field, select the relevant option.

   The options available are **Yes** and **No**.
6. Select the accurate transport protocol.

   The available options are **TCP** and **TLS**.

   Note:

   For **Avaya Zang** and **AT&T Landline Texting** connectors, select **TLS**.
7. Enter the host address of the SMSC.

   Note:

   For Avaya Zang connector, the host address is api.zang.io.
8. Enter the port number that is used for the SMS connection.

9. Enter the path of the SMSC.
10. Enter the user name.

    Note:

    For Avaya Zang connector, the user name is the Account SID on the Zang Dashboard at cloud.zang.io.

11. Enter the password.

    Note:

    For Avaya Zang connector, the password is the Auth Token on the Zang Dashboard at cloud.zang.io.

12. Enter your Application Programming Interface (API) ID to facilitate your connection to the connector.
13. From the **Connector** field, select the connector.

    The options available are **Avaya Zang**, **AT&T Landline Texting**, **AOS SMS**, **Clickatell**, **i2SMS**, **ONE WAY SMS**, **WEBTEXT**, and **Zipwhip**.

14. From the **Type** field, select the type of connector.

    The options available are **Outgoing** and **Incoming and Outgoing**.

15. From the Use **HTTP Proxy** field, select **Yes**.

    The available options are **Yes** and **No**. You can configure the subsequent fields only if you select **Yes**.

16. Enter the address of the proxy server.
17. Enter the proxy port number.

    The default port number is 8000.

18. Enter the sender ID that can be either a short code or a long number.
19. Select one or more organizations from the **Organization** list.
20. **(Optional)** Click the **Additional Entry** option and enter subsequent short codes or long numbers.
21. Click **Save**.

Change HTTP connection page field descriptions

Use this page to change the configuration of an HTTP connection.

Field or Button	Description
Zone	Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only when you create new zones. If you do not create any new zones, you do not see the drop-down box. Changing **Zone** from the default zone to any other zone is not allowed. However, you may change the zone for connections for which the existing zone is not the default zone.
Name	The name of the HTTP connection. **Note:** This name cannot be modified
Enable	The options are: • Yes • No
Transport Protocol	The protocol used to send request to SMSC. Select the transport protocol from the drop-down list box. The options are: • **TCP** • **TLS** **Note:** For **Avaya Zang** and **AT&T Landline Texting** connectors, select **TLS**.
Host Address	The IP address of the service provider or the Short Message Service Center (SMSC) server. Enter the host address of the service provider. **Note:** For Avaya Zang connector, the host address is api.zang.io.
Port	Enter the port number to be used for the connection.
Path	Enter the path of the URL to be used for communicating with the SMSC. The default is “ ”. This is the portion of the URL which is after the host address and the port. As an example if the URL is http://hostaddress:port/location, enter location here.

Table continues…

Field or Button	Description
User Name	Enter the user name. **Note:** For Avaya Zang connector, the user name is the Account SID on the Zang Dashboard at cloud.zang.io. This Account SID should only be used in one active connection. This means that you need to use only one EPM connection if multiple Avaya Zang short codes or long numbers are associated with the same Account SID.
Password	The password for the user supplied by the service provider. Enter the password. **Note:** For Avaya Zang connector, the password is the Auth Token on the Zang Dashboard at cloud.zang.io.
API ID	The user identifier supplied by the service provider. Enter the Application Programming Interface (API) ID. **Note:** For Avaya Zang connector, do not enter any value in the **API ID** field. If you plan to share the same Account SID across multiple EP systems, then enter the API ID. To share the Account SID, enter a unique number as the API ID for each EP system. This unique API ID should be appended to the SMS Request URL that is configured at cloud.zang.io. For example, if you enter 1 as the API ID for EP system 1, and 2 as the API ID for EP system 2, the SMS Request URL for an SMS number managed by EP system 1 would be: `https://pubsub.zang.io/[Account SID]/SMS/Incoming1` , and the SMS Request URL for an SMS number managed by EP system 2 would be: `https://pubsub.zang.io/[Account SID]/SMS/Incoming2`.

Table continues…

Field or Button	Description
Connector	The HTTP mechanism supported through a connector. The options are: • Avaya Zang • AT&T Landline Texting • AOS SMS • Clickatell • i2SMS • ONE WAY SMS • WEBTEXT • Zipwhip **Note:** For **AT&T Landline Texting** and **Zipwhip**, the customer must obtain a Session Key from the Sales or Support team. The Session Key is specific to each SMS-enabled phone number, so one SMS connection is required on the EPM for each phone number. The Session Key contains a : character. The characters to the left of the : character should be entered into the **Username** field of an EPM SMS Connection and the characters to the right should be entered into the **Password** field. For example, a typical Session Key (obtained from AT&T Landline Texting or Zipwhip) looks like the following: `3d0f1dde-aaff-4ce8-b61a-af212a860abc:123456789` Where, • `3d0f1dde-aaff-4ce8-b61a-af212a860abc` is the Username. • `123456789` is the Password.

Table continues…

Field or Button	Description
Type	An HTTP Connector can be of two types. The options are: • **Outgoing**: The **Outgoing** connector is used for sending out SMS messages only. It is assigned to all SMS processors in the same zone. • **Incoming and Outgoing**: The **Incoming and Outgoing** connector is used for processing incoming SMS messages and also for sending out SMS messages. It needs to be assigned to a specific SMS processor. **Note:** This option is only available for connectors that support both incoming and outgoing SMS messages. By default, an HTTP connector can only be used for processing outgoing messages. **Note:** For Avaya Zang connections, if you select **Incoming and Outgoing** to respond to incoming SMS messages, you must configure the **SMS Request URL** at `cloud.zang.io` to forward incoming SMS messages to the `pubsub.zang.io` server. You need to log in to your zang.io account, click **Numbers** on the top of the Zang dashboard, select **Manage Numbers**, and then click the purchased SMS telephone number. For example, `https://pubsub.zang.io/ABCc8890841e5034bdf1a149c2a5b6xyz/SMS/Incoming` is the **SMS Request URL**. Where, `ABCc8890841e5034bdf1a149c2a5b6xyz` is the Account SID that displays when you log in to the zang.io console. To support incoming MMS, use the same URL in the **MMS Request URL** field on the MMS tab for the Zang SMS/MMS telephone number. **Note:** From Experience Portal 7.2.1, Avaya Zang connections must be configured to use https. You may need to install the Baltimore CyberTrust Root certificate if the connections fail to connect with an SSL error. You can download the certificate from https://www.digicert.com/CACerts/BaltimoreCyberTrustRoot.crt. To import the certificate, on the EPM web page, click **Security** > **Certificates**, and the click **Import** on the Trusted Certificates tab. Restart the EPM from the EPM Manager.
Use HTTP Proxy	The proxy setup to be used while sending the HTTP(s) request. Comma-separated values comprising of proxy protocol, proxy server, and proxy port. The options are: • Yes • No

Table continues…

Field or Button	Description
Proxy server	The proxy setup to be used while sending the HTTP(s) request. Comma-separated values comprising of proxy protocol, proxy server, and proxy port. Enter the name of the proxy server.
Proxy Port	The proxy setup to be used while sending the HTTP(s) request. Comma-separated values comprising of proxy protocol, proxy server, and proxy port. Enter the port number of the proxy server.
Short Code/Long Number **Organization**	Enter the short code or the long number provided by the SMSC. Use the Additional Entry link to specify additional short codes or long numbers. Select the relevant organization from the multi-select drop-down list. The options are: • **<All>** : All organizations can use this short code. If the administrator selects multiple options in the drop-down list, only <All> is saved. • **<None>**: None of the organizations can use this short code. The administrator can select other organizations in addition to <None>. • The other organizations that are enabled in the system.

Deleting an HTTP connection

Procedure

1. Log in to the EPM web interface.
2. From the EPM main menu, select Home > Multi-Media configuration >SMS > HTTP Connections.
3. Select the check box next to the HTTP connection that you want to delete.
4. Click **Delete**.

Adding an SMPP connection

Procedure

1. Log in to the EPM Web interface.
2. From the EPM main menu, select Home > Multi-Media configuration > SMS > SMPP Connections.
3. On the **SMPP Connections** page, click **Add**.

   The system displays the **Add SMPP Connection** page.
4. In the **Zone** field, select the name of the zone.
5. In the **Name** field, type the name of the SMPP connection.
6. In the **Enable** field, select **Yes**.

7. In the **Transport Protocol** field, select the relevant protocol.

   The options available are **TCP** and **TLS**.
8. Enter the host address of the SMS server.
9. In the **Shared** field, select the relevant option.

   The options available are **Yes** and **No**. If you select **No**, SMS processor is enabled. Otherwise, SMS processor is disabled.
10. Select the SMS processor from the drop-down box.
11. Enter the port number.
12. In the **Bind Mode** field, select the accurate Bind Mode.

    The options are Transceiver, Transmitter, and Receiver.
13. Enter the user name.
14. Enter the password.
15. Enter the address range.
16. Set the **From** field to either Short Code or Blank.
17. Enter the sender ID that can be either a short code or a long number.
18. Select one or more organizations from the **Organization** list.
19. **(Optional)** Click the **Additional Entry** option and enter subsequent short codes or long numbers.
20. Specify the values for the **Advanced Parameters** group.

    To know about the **Advanced Parameters**, on the **Add SMPP Connection** page, click **Help**.
21. Click **Save**.

Changing the configuration of an SMPP connection

Procedure

1. Log in to the EPM web interface.
2. From the EPM main menu, select Home > Multi-Media configuration > SMS >SMPP Connections.
3. In the **Name** field, click the name of the SMPP connection that you want to change. The system opens the **Change SMPP Connection** page.
4. From the **Zone** field, select the name of the zone.
5. From the **Enable** field, select the relevant option.

   The options available are **Yes** and **No**.

6. In the **Transport Protocol** field, select the relevant protocol.

   The options available are **TCP** and **TLS**.
7. Enter the host address of the SMS server.
8. From the **Shared** field, select the relevant option.

   The options available are **Yes** and **No**. If you select **No**, SMS processor is required. Otherwise, SMS processor is disabled.
9. Select the SMS processor from the drop-down box.
10. Enter the port number.
11. From the **Bind Mode** field, select the accurate bind mode.

    The options are Transceiver, Transmitter, and Receiver.
12. Enter the user name.
13. Enter the password.
14. Enter the address range.
15. Set the From field to either Short Code or Blank.
16. Enter the sender ID that can be either a short code or a long number.
17. Select one or more organizations from the **Organization** list.
18. **(Optional)** Click the **Additional Entry** option and enter subsequent short codes or long numbers.
19. Specify the values for the **Advanced Parameters** group.

    To know about the **Advanced Parameters**, on the **Change SMPP Connection** page, click **Help**.
20. Click **Save**.

Testing SMPP connections

About this task

The TestSMPPConnection script can be used to verify that the firewall is open to the SMSC and to verify proper credentials prior to configuring a SMPP connection in the EPM.

Procedure

1. Log in to Linux on the EPM server which is hosting the SMS processor.
   - 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.

2. Navigate to the `Support/VP-Tools` directory under the Experience Portal installation directory.
3. Enter the `cd $AVAYA_HOME/Support/VP-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 `TestSMPPConnection` command followed by the following parameters:

   - Host Address
   - Port
   - UserName
   - Password

   For example, `bash TestSMPPConnection 255.254.253.252 2775 smppUser smppPass`.

   One or more optional parameters may be specified, as provided by the SMSC:

   - -B BindMode where BindMode may be t for Transmitter, r for Receiver, or x for Transceiver. The default is –B x.
   - -A AddressRange
   - -S SystemType
   - -TLS to enable TLS connection

   If the script runs successfully, it returns a message stating that the operation completed without any errors. Otherwise, it returns a message stating the problem that it encountered. This script may take 30 seconds to complete.

Deleting an SMPP connection

Procedure

1. Log in to the EPM web interface.
2. From the EPM main menu, select Home > Multi-Media configuration >SMS > SMPP Connections.
3. Select the check box next to the SMPP connection that you want to delete.
4. Click **Delete**.

SMS Browser

An SMS Browser is deployed as a web application on the Multi-Media Tomcat application server. The SMS Browser processes the inbound SMS messages and supports running Orchestration Designer applications for outbound SMS messages.

At startup, the SMS Browser reads the browser configuration data from the configuration DB and initializes the text browser. SMS Browser hosts the Text Browser to analyze TextXML generated by Orchestration Designer.

The SMS Browser monitors the message table for new inbound text messages. New inbound messages are fetched in batches and passed to the text browser. The SMS Browser implements a set of callbacks from the text browser.

Text Browser

The text browser fetches and executes <Textxml> from message applications. The text browser resides on the EPM and is the link between the Message Gateway and the Orchestration Designer application. The text browser only supports running Orchestration Designer applications.

TextXML

TextXML is modeled after VoiceXML, and customized to provide text-processing capabilities. Documents generated by Orchestration Designer for message flow applications conforms to the new TextXML schema for Email and SMS handling. TextXML is modified VoiceXML to handle new challenges for working with text messages. The text browser validates each input document against TextXML schema. TextXML starts with the <TextXML> tag, and follows the same structure as VoiceXML containing forms, vars, blocks and grammars. There are some enhancements made to TextXML.

Configuring system parameters for SMS browser settings

Procedure

1. Log on to the EPM web interface.
2. In the EPM navigation pane, click **Multi-Media Configuration** > **SMS**.
3. On the SMS Processor tab, click **Browser Settings**.
4. In the **Fetch Timeout** field, enter the maximum number of seconds that the SMS browser must wait for the application server to return the requested page.
5. In the **Proxy Server** field, enter the fully qualified path to the proxy server.
6. In the **Proxy Port** field, enter the port number for the proxy server.
7. In the **Number of Threads** field, enter the maximum number of threads that the SMS browser must use for an asynchronous fetch.

   You can enter a number between 1 and 500. The default is 50.
8. Click **Save**.

Configuring system parameters for SMS settings

Procedure

1. Log on to the EPM web interface.
2. In the EPM navigation pane, click **Multi-Media Configuration** > **SMS**.
3. On the SMS Processor tab, click **SMS Settings**.
4. In the **Maximum Message Length** field, enter the maximum message length.

   The default length is 960 bytes.
5. In the **Log Level** field, click one of the following to set the log level:
   - **None**
   - **Info**
   - **Warning**
   - **Error**
   - **Fatal**

   The default level is **Info**.
6. In the **Record Handling on SMS** section, in the **Session Data(SDR)** and **Call Data(CDR)** fields, do the following:
   a. Select the **Enable** check box.
   b. In the **Retention Period (days)** field, enter the number of days for the retention of records.

      Note:

      The retention period has an impact on how long the call data records and session data records are saved in the operational database that the processor uses. The retention period does not have an impact on how long these records are saved in the reporting database.
7. In the **Categories and Trace Levels** group, do the following:
   a. In the **SMS Processor** field, click one of the following to set the trace level of the SMS Processors:
      - **Off**
      - **Fine**
      - **Finer**
      - **Finest**

b. In the **SMS Browser** field, click one of the following to set the trace level of the SMS Browser:

- **Off**
- **Fine**
- **Finer**
- **Finest**

If you select the button on top, the same trace levels are set for both **SMS Processor** and **SMS Browser** fields.

The default level is **Fine**.

8. Click **Save**.

SMS web services

EP provides a Web service that helps any client application, whether EP managed or not, to send SMS messages.

The web service facilitates the sending of an SMS message to a single recipient or a list of recipients.

In addition to sending SMS messages through a web service, EP supports the following capabilities:

- Starting stopping an SMS application.
- User name and password authentication is supported for all SMS Web services.

For information on parameters and return values of the SMS application, refer:

- LaunchSMS method on page 666
- SendSMS method on page 678

Reporting filters for SMS

Experience Portal 7.0 and later versions have a new media type filter for SMS that is added to the Contact Detail and Contact Summary reports.

The following are the main filters that are available for SMS:

- SMS
- SMS receipt

Experience Portal 7.0 and later versions support the capability to filter the messages on SMSC. This capability consists of the number of messages sent to one or more SMSCs as well as the number of messages received from one or more SMSCs.

The following information is available in these reports:

- The number of messages sent
- The number of messages received
- The number of delivery receipts requested
- The number of receipts pending
- The number of receipts received

All existing filters for the Contact Detail and Contact Summary reports can be applied to reporting records created by incoming or outbound SMS. This support includes the capability to generate reports for any number of zones defined in the system.

SMS delivery receipt flow sequence

- The client requests for SMS delivery receipt in one of the following ways:
  - The client selects the **RegisteredDelivery=1** option in web service parameter.
  - The client submits a request on a link that is configured for registered delivery.
- The SMS processor sends a request for delivery receipt to SMSC on the basis of the client's request.
- Upon receiving a delivery receipt from SMSC, the server creates a receipt record in the operational database.
- The SMS browser launches the configured delivery receipt application and sends the delivery receipt information to the application.
- Once the browser reads the receipt, the browser deletes the record.
- The application can use the message Id from the obtained receipt and can accordingly correlate the corresponding outbound SMS for processing the receipt.

SMSC success and failure responses

EP handles success and failure responses from all SMSCs. The responses are made available to the application for further evaluation and processing. In case of no connectivity with the SMSC, the SMS processor issues retries. The number of retries is not configurable and retries are infinite. The retry interval is configurable.

Other than the connectivity with the SMSC, the application has the capability of handling failures. The application can trigger a **Resend** or any other action to address the failure.

Chapter 8: HTML management

HTML overview

Avaya Experience Portal 7.2 and later versions support HTML as an additional communication channel and provide a mechanism to move a self-service interaction from a voice interface to a web interface. HTML applications are always launched by name through the Application Interface web service. As a result, there is no concept of launch criteria, launch order, and default HTML application.

Note:

Experience Portal supports HTML applications that are developed using Avaya Orchestration Designer only.

In this deployment, Experience Portal is completely isolated from the public network while the Orchestration Designer application is partially isolated from the public network by using the customer's HTTP reverse proxy server. An additional security layer is provided by isolating the internal configuration and parameters from the public network. In addition, the system provides a mechanism to make visible only established Orchestration Designer sessions to the public network by session initiation that comes through the HTML Redirector application and Experience Portal.

Note:

You must specify the host address of the reverse proxy if you are using a reverse proxy in front of the redirector or multiple redirectors for added redundancy.

You must configure and use a separate redirector for each zone on zoned systems.

The HTML feature in Experience Portal is used to create applications called Visual IVR - that is they create a visual metaphor for an IVR flow.

HTML typical flow

The flow of an incoming call and the mechanism to provide an HTML interface to the user is as follows:

- A customer calls.

- The SMS, voice, and email application is launched through the Application Interface web service.
- The application fetches the global and application-specific CAVs.
- The customer and the application interacts with each other. Voice interaction happens through MPP, whereas SMS and email interaction happens through the Primary or Auxiliary EPM.
- The customer opts for a richer interface through HTML.
- The SMS, voice, and email application opts to run the HTML mobile application .
- The customer receives an HTML link based on the interaction:
  - SMS and email applications send a message containing the HTML mobile application link through a prompt.
  - Voice applications send the HTML mobile application link as an SMS or email message.

The reference to the EPM system applies to both the Primary and Auxiliary EPM servers as both support the web services required to launch the mobile HTML application. A Redirector application handles the load balancing of the requests by distributing the incoming requests among the EPM servers. On zoned systems, the Redirector application balances the load requests among the EPM servers within a specific zone.

Data collection

Using Avaya Experience Portal, you can log report data for an Avaya Orchestration Designer HTML application session. Once the Orchestration Designer HTML application session ends, Orchestration Designer runtime invokes the web service to log report data. Orchestration Designer runtime invokes the web service irrespective of how the session has ended, either in a normal manner or due to a session timeout.

The report collects usual report data for an application and also collects specific data for an HTML application:

- Count of number of interactions with the mobile application.
- Duration for interactions. This does not include session timeouts.
- Duration for which the application was in session. This includes the application server session timeout.

Adding an HTML application to Experience Portal

Procedure

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

2. In the EPM navigation pane, click **System Configuration** > **Applications**.
3. On the Applications page, click **Add**.
4. On the Add Application page, do the following:
    a. In the **Name** field, enter the name for the application.
    b. In the **Type** field, select **HTML**.
    c. Click **Continue**.
    d. Enter appropriate information in the other fields and click **Save**.

Changing the settings of an HTML application

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. In the EPM navigation pane, click **System Configuration** > **Applications**.
3. On the Applications page, click the name of the application whose settings you want to change.
4. On the Change Application page, make the required changes and click **Save**.

Deleting an HTML application

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. In the EPM navigation pane, click **System Configuration** > **Applications**.
3. On the Applications page, select the check box for the application that you want to delete.
4. Click **Delete**.

Configuring HTML Redirector

About this task

Use this procedure to set the host address and port number for the HTML Redirector.

The HTML Redirector redirects the launch requests for HTML applications. Avaya Experience Portal stores the Redirector configuration in the database as a global CAV. Avaya Orchestration Designer runtime gets the host address of the configured Redirector from the global CAVs retrieved from the EPM. Orchestration Designer uses the configured information and the HTML application name to generate a URL to launch an HTML5 application through the Redirector.

The Redirector servlet hosts a generic URL that is the initial point of contact in launching an Orchestration Designer HTML5 application. The Redirectorservlet acts as a wrapper around the web service to provide a layer of security by isolating the EPM servers and hiding any sensitive launch configuration such as application internal IP addresses, confidential parameters, and CAVs, from direct exposure to the external browser.

Procedure

1. Log on to the EPM web interface.
2. In the EPM navigation pane, click **Multi-Media Configuration** > **HTML**.

   The EPM web interface displays the HTML Redirectors page.
3. In the **Transport Protocol** field, click one of the following transport protocols for sending requests to the Redirector:
   - TCP
   - TLS
4. In the **Host address** field, enter the host address of the Redirector.

   Note:

   The EPM system is installed with a default zone. Therefore, the HTML Redirector page initially displays the host address and port number only for the default zone. However, when an administrator configures zones in Experience Portal, the HTML Redirector page displays a host address and port number for all configured zones.

   You must configure a redirector for each zone that hosts HTML applications.
5. In the **Port** field, enter the port number for the Redirector.
6. In the **Path** field, enter the path of the URL for communicating with the Redirector.

   The path appears after the host address and the port. For example, `http://hostaddress:port/path`.
7. Click **Apply**.

Chapter 9: Configuring System Manager Single Sign-On

Prerequisites for Single Sign-On

This chapter describes the prerequisites and procedures required to enable Single Sign-On between Avaya Aura® System Manager and EPM. Customers must read and understand all the considerations and complete all the procedures in this section.

Before enabling the Single Sign-On between System Manager and EPM, you must:

- Import the System Manager certificate to EPM by using the EPM Trusted Certificates webpage, and specify the certificate type as System Manager.

  Use the URL `https://<SMGR FQDN>:443` to import the System Manager certificate.
- Both the System Manager and the primary EPM server requires a fully qualified domain name (FQDN) that can be resolved in the DNS server. The FQDN of the primary EPM server must match a part of the System Manager server's domain name.
- Copy the file `CopyEPWelcomeHTML.zip` to the System Manager. To perform this task, follow README.txt located in the`$AVAYA_HOME/Support/SMGR` directory on the primary EPM.

  You must perform this step only once.
- Synchronize the machine date and time between the System Manager and EPM systems.
- Configure the value of the maximum session timeout of System Manager as near to the session timeout configured in EPM.

Configuring the EPM System Manager Settings page

Procedure

1. Log on to the EPM web interface by using an account with the User Manager role.
2. In the EPM navigation pane, click **User Management** > **Login Options**.
3. On the Login Options page, click **System Manager Settings**.
4. Configure the parameters to enable single sign-on between the System Manager and EPM systems.

System Manager Settings page field descriptions

Use the fields on this page to establish Single Sign-on with Avaya Aura® System Manager. For more information, see Configuring System Manager Single Sign-On.

Name	Description
Enable Single Sign-On	Allows you to enable or disable Single-Sign on. The options are: • **Yes**: The Single Sign-On is enabled. • **No**: The Single Sign-On is disabled. **Note:** 1. When you click **Save** or **Apply**, Avaya Experience Portal verifies the System Manager settings only if the **Enable Single Sign-On** field is set to **Yes**. If all fields are valid, Experience Portal performs the following actions with System Manager that is configured on this page: - Register Experience Portal Resource Type, Experience Portal system roles, and Experience Portal Resource Instance. - Register navigation link. - Enable SSO client. If the **Enable Single Sign-On** field is set to **No**, Experience Portal saves the changes but does not verify the changes if there is no prior configured and enabled System Manager. 2. When you have enabled Single Sign-On, the user can only modify the Navigation Link Display, User Name, and Password. 3. If the user changes the Single Sign-In option from enabled to disabled, EPM tries to communicate with the previous configured System Manager to remove the SSO client and de-register the navigation link and Experience Portal Resource Instance. This is possible only if: - Experience Portal is able to access the previous configured System Manager. - System Manager User name and credentials configured are still valid. 4. If Experience Portal cannot access System Manager, the page displays the **Force Change** check box. Use the

Name	Description
	check box to disable Single Sign-On with the configured System Manager.

Connection Settings section

Name	Description
System Manager FQDN	The fully qualified host name of the System Manager. **Note:** 1. The EPM server must match a part of the System Manager server's domain name. For example, if the FQDN of System Manager server is `smgr.us.avaya.com`, the FQDN of EPM that can perform Single Sign-On with System Manager can be `xx.us.avaya.com` or `xx.yy.avaya.com` or `xx.avaya.com`. 2. If the System Manager FQDN entered is different than the previous configured System Manager, you must restart EPM to enable Single Sign-On with the new System Manager.
Navigation Link Display	A link display that represents the primary EPM on the System Manager webpage. You can view this Navigation Link Display on the System Manager webpage from: • **Home page** > **Elements** > **Experience Portal System.** • Resource Instance when configuring a role. Valid characters are number, letters, and any of "-", "(", ")", "/", "\", ".", "_", "{", "}". **Note:** If you have multiple EPMs that are enabled to perform Single Sign-On with the same System Manager, you must configure a unique Navigation Link Display.

Table continues…

Name	Description
User Name	A valid System Manager user who has the System Administrator role and is authorized to register Resource Type and Resource Instance with System Manager. **Note:** This user must be a System Manager user and not an EPM user. This System Manager user must be created from the User Management page in the **Users** tab in System Manager.
Password	The password of the System Manager user.

Note:

On the primary EPM, if you enable Single Sign-On with a System Manager and if you change the System Manager FQDN to a different System Manager, restart the primary EPM for Single Sign-On with the new System Manager to work properly.

Creating a System Manager user

About this task

It is recommended that you create a new Avaya Aura® System Manager user with a System Administrator role on the System Manager system.

You must use the credentials of the System Manager user when configuring the System Manager Settings page on the EPM. EPM uses these System Manager credentials to register the Experience Portal resource type, managed resources, and navigation menu items with System Manager.

Note:

Do not use the default System Manager user administrator credentials when configuring the System Manager Settings page.

Procedure

1. Log on to System Manager.
2. Navigate to the User Management page.

   If a temporary password is assigned to the user, then log on to System Manager by using this user credential and change the password.

Items created on System Manager after enabling Single Sign-on

When you enable Single Sign-on in EPM, the following items are created on Avaya Aura® System Manager:

- Built-in Experience Portal System Roles:
  - Experience Portal Administration
  - Experience Portal User Manager
  - Experience Portal Auditor
  - Experience Portal Maintenance
  - Experience Portal Privacy Manager
  - Experience Portal Reporting
  - Experience Portal Operations
- An **Experience Portal** Resource Type.
- A link **Experience Portal System** in the **Elements** tab on the System Manager home page.
- A navigation link with the name configured in the **Navigation Link Display** on the EPM System Manager Settings page.
- A managed resource with the name configured in the **Navigation Link Display** on the EPM System Manager Settings page.

Note:

If you have installed Intelligent Customer Routing (ICR) Managed App on the Experience Portal system, the system creates the following items on System Manager:

- Built-in Experience Portal ICR System Roles.
  - Experience Portal ICR Administration
  - Experience Portal ICR Reporting
- An **Experience Portal ICR** Resource Type.
- An ICR managed resource with the name configured in the **Navigation Link Display** on the EPM System Manager Settings page.

If you have installed Proactive Outreach Manager (POM) Managed App on the Experience Portal system, the system creates the following items on System Manager:

- Built-in Experience Portal POM System Roles.
  - Experience Portal POM Administration
  - Experience Portal POM Campaign Manager
  - Experience Portal POM Supervisor

  - Experience Portal POM Contact Attributes Unmask
  - Experience Portal Org POM Campaign Manager
  - Experience Portal Org POM Contact Attributes Unmask
- An **Experience Portal POM** Resource Type.
- A POM managed resource with the name configured in the **Navigation Link Display** on the EPM System Manager Settings page.

Experience Portal roles and permissions assignment

The Experience Portal permissions assigned to the System Manager user determine the EPM webpages that can be accessed by the System Manager user.

The System Manager administrator can assign any built-in Experience Portal system roles or a custom role that includes the Experience Portal permissions to any valid System Manager user.

- To map permissions to a customer role in System Manager, select **Experience Portal** in the **Element or Resource Type** field.
- In the **Element or Resource instance** field, the **EPM Navigation Link Display** configured on the System Manager Settings page appears in the list.
- Click **Next**. The Permission Mapping page shows all the available Experience Portal permissions that you can select from.

Note:

When the System Manager Administrator selects Experience Portal Resource Type to add permission mapping to a custom role, the **EPM Navigation Link** permission is selected by default. Without this permission, the System Manager user cannot click the **Experience Portal System** link in the **Elements** tab on the System Manager home page.

Single Sign-on

Single Sign-On with System Manager can be accomplished in the following three ways:

Single Sign-On from System Manager

1. Start a Browser and log in to System Manager through System Manager FQDN with a valid System Manager User credentials having Experience Portal permissions.
2. On the System Manager home page, click the **Experience Portal System** link in the **Elements** tab.
3. Expand the left menu, and click the **EPM** link.

The Browser displays the EPM home web page in another tab or in another window without prompting for credentials.

Single Sign-On from System Manager

1. Start a Browser and log in to System Manager through System Manager FQDN with a valid System Manager User credentials having Experience Portal permissions.
2. In the same Browser, start a new Window or a new tab and enter the EPM FQDN in the address bar.

   The Browser displays the EPM home web page in the new Window or another tab without prompting for credentials.

Single Sign-On from EPM

1. Start a Browser and log in to EPM through the EPM FQDN.
2. Enter valid System Manager User credentials.

   The system displays the EPM home web page.

Note:

Single Sign-On between System Manager and EPM is not supported when accessing through IP address.

To remove all configuration in the System Manager Setting page, disable Single Sign-On.

Logoff

When a Single Sign-On session is active, always click **Log off** to log out from System Manager or EPM.

When a user logs off from System Manager, the system terminates the EPM session. In this release, the EPM webpage does not automatically display the login page unless a user clicks the link on the EPM webpage.

When a user logs off from EPM, the system terminates the System Manager session. The System Manager page displays the login page in a few seconds.

Invalid login scenarios

The following System Manager Users cannot use the Single Sign-On to the EPM feature:

- A disabled System Manager user.
- A password expired System Manager user.
- A System Manager user with the same name as an existing Experience Portal web user.
- An organization System Manager administrator.

Reconfiguring the single sign-on after a System Manager upgrade

About this task

Use this procedure to ensure that the single sign-on continues to work after a the System Manager upgrade.

With the single sign-on feature, you can access the System Manager and EPM using a single sign-on. After the System Manager upgrade, the single sign-on fails if:

- Experience Portal files are not retained on the System Manager .
- System Manager certificate is modified.

Before you begin

Verify whether you are able to access System Manager using the single sign-on feature from EPM.

Procedure

1. Log on to System Manager as a root user.
2. Verify whether the `experienceportalWelcome.html` file exists at the following location: .

   `$JBOSS_HOME/server/avmgmt/deploy/ROOT.war/experienceportalWelcome.html`
3. If the file does not exist, do the following:
   a. Navigate to the `Readme.txt` file located in the `$AVAYA_HOME/Support/SMGR` directory on the primary EPM.
   b. Copy the `experienceportalWelcome.html` file to System Manager.
4. If System Manager has a new certificate after the upgrade, do the following:
   a. Import the new System Manager certificate to the EPM Trusted Certificates web pages by using the URL `https://<SMGR FQDN>:443`.
   b. Specify the certificate type as System Manager.
5. Close all existing browsers and open a new browser to access System Manager using single sign-on.

System Manager Single Sign-On limitations

The following are the limitations of Single-Sign-on:

- Cannot DELETE EP Resource Type, EP System Roles in System Manager: The Experience Portal Resource Type, ICR Resource Type, POM Resource Type, Experience Portal system

roles, POM system roles, and ICR system roles cannot be deleted in System Manager after you have created them from EPM.

- No Locale Support: This includes but is not limited to Experience Portal Resource Type, ICR Resource Type, POM Resource Type, Experience Portal system roles, POM system roles, and ICR system roles, features, and navigation links created in System Manager.
- No Organization Support: Administrators created in Tenant Management cannot access Experience Portal from the System Manager dashboard.

  In this release, there is no organizational support for System Manager Single Sign-On. Therefore, an organization System Manager administrator cannot use the Single Sign-On feature to log on to EPM. System Manager also does not support EPM organization roles and features mappings.
- No Notification Mechanism between System Manager and EPM: System Manager does not send out notifications to the EPM when a System Manager session expires, terminates, or logs out. Similarly, System Manager does not have the ability to receive notifications when the EPM session expires. Sessions are validated when the next request is made.

Chapter 10: Server and database administration

EPM server administration

Changing EPM server settings

About this task

The EPM server settings apply to both the primary EPM server and the optional auxiliary EPM server.

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** > **EPM Servers**.
3. On the EPM Servers page, click **EPM Settings**.
4. On the EPM Settings page, enter the appropriate information, and click **Save**.

Configuring an auxiliary EPM server

About this task

The auxiliary EPM server:

- Can assign outgoing calls made with the Application Interface web service to an available MPP server. Avaya Experience Portal does not provide load balancing or failover, however. You must use a third-party product for these purposes.
- Shares Application Logging web service requests when the primary EPM server is in service.

  Note:

  When using the Application Logging web service, Orchestration Designer provides failover and load balancing between the primary and auxiliary EPM servers. Applications written with other tools must provide their own load balancing and failover mechanisms for this web service.
- Handles all requests when the Primary EPM is down.

- Does *not* include the EPM web interface, therefore it cannot be used to administer the system or monitor the status of the MPP servers.

Procedure

1. To reset the password for the vpcommon PostgreSQL account:
   a. Log on to Linux on the Experience Portal Primary EPM 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.
   b. 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.
   c. Enter the `bash SetDbPassword.sh update_primary_vpcommon` command.
   d. Type the password for the vpcommon PostgreSQL account and press `Enter`.

      After the password is accepted and updated, the script prompts a message indicating the services to be restarted and asks if the user wants to proceed.

      Note:

      The script will not list the service that is not impacted by changing the user password.

      Example:

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

2. Install the auxiliary EPM software on the new server as described in the *Optional: Installing the EPM software on the auxiliary EPM server* topic of the *Implementing Avaya Experience Portal on multiple servers* guide.

   When you get to the Database Login Check for Auxiliary EPM installation screen, make sure you specify the password for the vpcommon PostgreSQL database user account.

3. When the installation has finished, add the server to the Experience Portal system:
   a. Log on to the EPM web interface.

      If Avaya Services is maintaining this system and you are an Avaya Services representative, log on to EPM by using the init EPM account that is created during the EPM software installation.

      Otherwise, log on to EPM by using an account with the Administrator user role.

   b. From the EPM main menu, select **System Configuration** > **EPM Server**.
   c. On the EPM Servers page, click **Add**.
   d. On the first Add EPM Server page, enter the appropriate information and click **Continue**.
   e. On the second Add EPM Server page, enter the appropriate information.
   f. Click **OK**.

Changing the configuration information for a EPM server

Procedure

1. Log on to the EPM web interface.

   If Avaya Services is maintaining this system and you are an Avaya Services representative, log on to EPM by using the init EPM account that is created during the EPM software installation.

   Otherwise, log on to EPM by using an account with the Administrator user role.

2. On the EPM navigation pane, click **System Configuration** > **EPM Servers**.
3. On the EPM Servers page, click the name of the EPM server whose settings you want to change.
4. On the Change EPM Server page, enter the appropriate information, and click **Save**.

   If you logged in using the init account, ensure that the LDN number specified in the **LDN** field matches the information in the Avaya Services database for this server.

Reconnecting the primary and auxiliary EPM servers

Before you begin

Ensure that you have reconnected the auxiliary EPM server. Use the **`setup_vpms.php`** command to reconnect the auxiliary EPM server.

Procedure

1. Log on to the EPM web interface.

   If Avaya Services is maintaining this system and you are an Avaya Services representative, log on to EPM by using the init EPM account that is created during the EPM software installation.

   Otherwise, log on to EPM by using an account with the Administrator user role.
2. In the EPM navigation pane, click **System Configuration** > **EPM Servers**.
3. On the EPM Servers page, click the name of the auxiliary EPM server.
4. On the Change EPM Server page, select the **Trust new certificate** check box in the **EPM Certificate** section.

   If you logged in using the init account, ensure that the LDN number specified in the **LDN** field matches the information in the Avaya Services database for this server.
5. Click **Save**.

Deleting the auxiliary EPM server

About this task

Use this procedure to delete the auxiliary EPM server.

Before you begin

Delete the managed applications installed on the auxiliary EPM server.

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. In the EPM navigation pane, click **System Configuration** > **EPM Servers**.
3. On the EPM Servers page, select the name of the auxiliary EPM server.
4. Click **Delete**.

Stopping the vpms service

About this task

You can stop the vpms service if you need to perform maintenance procedures on the server machine.

Procedure

1. Log on to Linux on the Primary or Auxiliary EPM 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.
2. Stop the *vpms* service by entering the `systemctl stop vpms` command.

Next steps

After you finish performing the maintenance procedures, restart the vpms service by entering the `/sbin/ service vpms start` command.

Associating Avaya Breeze® platform with an Experience Portal system

About this task

Avaya Experience Portal provides a mechanism to associate the Avaya Breeze® platform with an Experience Portal system. The information that is entered in Experience Portal is stored in global configurable application variables. Avaya Orchestration Designer uses this information to integrate Orchestration Designer applications with Avaya Breeze® platform workflows.

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. In the EPM navigation pane, click **System Configuration** > **EPM Servers**.
3. On the EPM Servers page, click **Data Storage Settings**.
4. On the Data Storage Settings page, expand the **Avaya Breeze™** section, and enter the appropriate information in the fields.
5. Click **Apply**.
6. Click **Save**.

Data Storage Settings page field descriptions

Use this page to configure the data storage settings for report data and conversations:

- Report Database
- Avaya Breeze® platform
- Conversations

Report Database

Field or Button	Description
Location radio buttons	The options are: • **Local**: The database resides on the local EPM server machine. • **External**: The database resides on a different server. This option is generally used when you have several Experience Portal systems that share an external database. **Note:** If you select **External**, the rest of the fields in this section become available. Contact your database administrator if you do not know the information to complete these fields.
URL	The fully-qualified path to the external database. A common URL format for Oracle connections is: `jdbc:oracle:thin:@OracleServerName:1521:DBName` A format for PDB (portable db) connections is: `jdbc:oracle:thin:@ServerName:1521/pdbName` A format for CDB (container db) connections is: `jdbc:oracle:thin:@ServerName:1521/cdbName` A common URL format for Postgres is: `jdbc:postgresql://PostgresServerName:5432/DBName` A common URL format for Microsoft SQL connections is: `jdbc:sqlserver://SQLServerName:1433;databaseName=DBName` A common URL format for MySQL connections is: `jdbc:mysql://ServerName:3306/DBName` A common URL format for MariaDB connections is: `jdbc:mariadb://ServerName:3306/DBName`

Table continues…

Field or Button	Description
JDBC Driver	The name of the Java class that implements the JDBC API to the external database. Experience Portal makes JDBC calls through this class when communicating with the external database. Experience Portal installs drivers for Oracle, Postgres and Microsoft SQL Server. For Oracle, the name is `oracle.jdbc.driver.OracleDriver`. For Postgres, the name is `org.postgresql.Driver`. For Microsoft SQL Server, the name is `com.microsoft.sqlserver.jdbc.SQLServerDriver`. For both MySQL and MariaDB, the name is `org.mariadb.jdbc.Driver`.
User Name	The user name for the external database. **Note:** For Oracle, the user name must be assigned CREATE TABLE, CREATE SESSION and CREATE SEQUENCE privileges for the database. For Microsoft SQL Server, the user name must be assigned SELECT, INSERT, UPDATE and DELETE privileges on all tables in the database. For Postgres, the user name must be assigned CONNECT, TEMPORARY ON DATABASE, SELECT, INSERT, UPDATE and DELETE privileges on all tables in the database. For both MySQL and MariaDB, the database user name for Experience Portal must be assigned SELECT, INSERT, UPDATE, DELETE privileges on all tables in the database. The CREATE TEMPORARY TABLE permission is also required. When creating the database, set a collation type of utf8_unicode_ci.
Password	The password for the external database.

Note:

The **Oracle Advanced Security Option** is available only if you set the external database to Oracle.

Field	Description
Encryption Type	Encryption algorithms transform data into a form that cannot be deciphered easily. Select an encryption type to protect sensitive information sent between the EPM and external database. The options are: • **None** • **AES128** • **AES192** • **AES256** • **RC4_40** • **RC4_56** • **RC4_128** • **RC4_256** • **DES40C** • **DES56C** • **3DES112** • **3DES168** **Note:** If you select **None**, Avaya Experience Portal sets the encryption level to rejected. For any other value, Avaya Experience Portal sets the encryption level to required.
Checksum Type	Data integrity algorithms can protect against certain network-based attacks by generating cryptographically secure message digests which are included in data packets sent between the EPM and external database. Select a checksum type you want to use. The options are: • **None** • **MD5** • **SHA1** **Note:** If you select **None**, Avaya Experience Portal sets the checksum level to rejected. For any other value, Avaya Experience Portal sets the checksum level to required.

Note:

You might need to increase **Session Timeout** from the **Home** > **User Management** > **Login Options** page for very large databases where on-demand reports might take more than 10 minutes. Scheduled reports are not subject to this timeout.

Avaya Breeze® platform

Field	Description
Platform Host Address	SIP Entity IP address of Avaya Breeze® platform.
Context Store Address	Cluster IP address of the context store on Avaya Breeze® platform.
Client Timeout	Maximum number of seconds that the Orchestration Designer application should wait for the platform or the context store to respond back to its request. Enter a number between 15 and 300. The default is 60.

Note:

When you select the context store, the application server requires proper certificates setup for mutual authentication.

Conversations

Field or Button	Description
Local EPM (SMS channel only)	A database on EPM that is processing the application that creates the conversation. Use this option for a valid SMS application. If a non-SMS application attempts to create a conversation, the operation fails. This configuration provides backward compatibility with Experience Portal 7.0.
Primary EPM (All channels)	A database on the Primary EPM server. Use this option for systems that do not contain any Auxiliary EPM servers. This option does not support high availability and the conversation data is unavailable for applications when the Primary EPM server is down.

Table continues…

Field or Button	Description
Context Store (All channels)	The Context Store of Avaya Breeze® platform. Use this option to provide configuration information to Orchestration Designer. Orchestration Designer is the application that reads/writes the conversation data whereas Experience Portal provides the configuration information to Orchestration Designer. This option supports high availability, which is optional, and is robust only if you have setup Context Store in cluster mode. • Host Address: Cluster IP address of the Context Store associated with Avaya Breeze® platform. • Client Timeout: Maximum number of seconds that the Orchestration Designer application should wait for the platform or the context store to respond back to its request. Enter a number between 15 and 300. The default is 60. **Note:** The Context Store option supports Orchestration Designer 7.1 or later. Orchestration Designer 7.0.1 SMS applications will use Local EPM for conversations even if you select the Conversation Store as Context Store.

Existing conversations can be lost when you switch from the conversation store location.

Configuring conversation repository

About this task

You can use the conversation repository feature of Avaya Experience Portal to store and share conversations in multichannel applications. A conversation is the data that a multi-turn application stores to remember its state across turns. This feature supports all media types such as HTML, Email, SMS, and Voice. It provides the option of storing conversation data at alternate locations.

Experience Portal provides the following options for storage of data:

- Local EPM
- Primary EPM
- Context Store

For more information about each location, see Data Storage Settings page field descriptions on page 189.

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. In the EPM navigation pane, click **System Configuration** > **EPM Servers**.
3. On the EPM Servers page, click **Data Storage Settings**.
4. On the Data Storage Settings page, expand **Conversations**, and enter appropriate information in the fields.
5. Click **Apply**.

6. Click **Save**.

Moving the Avaya Experience Portal software

Move the Experience Portal software to a different server machine

If required, you can move the Experience Portal software to a different server machine. In all cases, you must use the same hostname and IP address on the new server as on the old server. This reduces the number of changes you need to make to the Experience Portal system configuration.

If you want to:

- Move the EPM software to a new server in a system where the EPM and MPP software runs on different servers, see Move the EPM software to a different server machine on page 194.
- Move the MPP software to a new server in a system where the EPM and MPP software runs on different servers, see Moving an MPP to a different dedicated server on page 196.
- Move the Experience Portal software in a system where the EPM and the MPP run on the same server, see Move a single-server Experience Portal system to a different server on page 197.

Move the EPM software to a different server machine

This procedure applies to moving the primary EPM software in a dedicated server configuration. If you need to:

- Move the EPM software in a system where the EPM and the MPP software runs on the same server, see Move a single-server Experience Portal system to a different server on page 197.
- Move the auxiliary EPM software, simply install the software on the new server as described in Configuring an auxiliary server on page 184.

Important:

You must complete these steps in the order given below or you may encounter errors during the procedures.

Step	Description	✔
1	On the old EPM server, back up the Experience Portal database as described in System Backup Overview on page 215.	

Table continues…

Step	Description	✔
2	If possible, set up the new server so that it has the same IP address and hostname as the old EPM server.	
3	On the new EPM server, install the operating system and the EPM server software as if this was a new installation. If at all possible, the new EPM server should have the same hostname and IP address as the old EPM server in order to minimize the number of manual changes you will need to make. **Important:** Make sure you: • Perform all software prerequisites, such as synchronizing the time between the new EPM server and the MPP servers. • Select the same options you selected for the previous installation. • Go through the same configuration steps after you install the software. For example, if you synchronized the old EPM server with an external time source, make sure you configure the new server to use that time source as well.	
4	On the new EPM server, configure the backup and restore scripts as described in Verifying the backup server mount point on page 226. Make sure that you specify the same mount point and shared directory that you used on the old EPM server.	
5	Restore the Experience Portal database from the backup you made on the old EPM server as described in Database Restore utility and system backup on page 225.	
6	If you could not use the same hostname and IP address for the new EPM server, change the information in the Experience Portal database as described in Changing the hostname or IP address on a dedicated primary EPM server on page 208.	
7	If you could not use the same IP address and hostname for the new server, you need to connect each MPP server with the new EPM server as described in Reconnecting an existing MPP server with the EPM server on page 210.	
8	If your WebLM server ran on the old EPM server, install the Experience Portal license file on the new EPM server as described in the *Installing the license file* topic in the *Implementing Avaya Experience Portal on multiple servers* guide. Otherwise, verify that the new EPM server can contact the WebLM server by selecting **Security** > **Licensing** from the EPM main menu and clicking **Verify** on the Licensing page.	

Moving an MPP to a different dedicated server

About this task

Note:

This procedure applies to the Experience Portal system in which the MPP software runs on a dedicated server. If you need to move the MPP in a system where the EPM and the MPP run on the same server, see Move a single-server Experience Portal system to a different server on page 197.

Procedure

1. If you want to transfer the MPP log files:
   a. Log into the Media Server Service Menu as described in Logging in to the Media Server Service Menu on page 295.

      Tip:

      You can also pack the files by running the `getmpplogs.sh` script on the MPP server. For more information, see the *Administrative scripts available on the MPP* topic of the *Troubleshooting Avaya Experience Portal* guide.

   b. Go to the Diagnostics page and select **Pack Files**.
   c. On the Pack Files Options page, select **Logs** and **Transcriptions and utterances**.
   d. Click **Pack**.
   e. When the process has completed, download the `tar.gz` archive file.
2. If possible, set up the new server so that it has the identical IP address and hostname as the old MPP server. The hostname should match in all respects, including case.
3. Install the MPP software on the new server as described in the *Installing the MPP software interactively* topic of the *Implementing Avaya Experience Portal on multiple servers* guide.

   Important:

   Make sure you select the same options you selected for the previous installation.
4. If you want to transfer the MPP log files, restore them as described in Restoring packed MPP log files on page 201.
5. If you could not configure the new MPP server to use the same IP address and hostname as the old MPP server:
   a. Log on to the EPM web interface by using an account with the Administration user role.
   b. Change the hostname or IP address of the MPP on the Change MPP Server page as described in Changing an MPP on page 274.
6. Reestablish the link between the EPM and the MPP as described in Reestablishing the link between the EPM and an MPP on page 197.

Reestablishing the link between the EPM and an MPP

About this task

After you upgrade the Experience Portal software, use this procedure to reestablish the link between the MPP and the EPM by trusting the MPP's security certificate.

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** > **MPP Servers**.
3. Click the name of the MPP server.
4. On the Change MPP Server page, go to the **MPP Certificate** section and select the **Trust new certificate** check box if that check box is visible.
5. Click **Save**.
6. On the EPM navigation pane, click **System Management** > **MPP Manager**.
7. On the MPP Manager page, check the **Mode** column for this server and do the following if it displays **Offline**:
   a. Select the check box next to the name of the MPP.
   b. In the **Mode Commands** group, click **Online**.
   c. In a few seconds, click **Refresh** to verify that the **Mode** column now displays **Online**.
8. Select the check box next to the name of the MPP.
9. In the **State Commands** group, click **Start** and confirm your selection when prompted.
10. In a few minutes, click **Refresh** to verify that the current **State** is **Running**.
11. To ensure that the telephony ports were correctly allocated to the MPP server, do the following:
    a. On the EPM navigation pane, click **Real-time Monitoring** > **Port Distribution**.
    b. On the Port Distribution page, check the **Current Allocation** column to find the ports allocated to this MPP.
    c. Check the **Mode** and **State** columns to ensure that the assigned ports are ready to receive calls.

Move a single-server Experience Portal system to a different server

This procedure applies to the Experience Portal system in which the EPM software runs on the same server as the MPP software. If you need to move the EPM or MPP software in a system where the EPM and the MPP run on different servers, see Move the EPM software to a different server machine on page 194 or Moving an MPP to a different dedicated server on page 196.

Important:

You must complete the following steps in the order given below or you may encounter errors during the procedures.

Step	Description
1	On the old Experience Portal server, back up the Experience Portal database. For more information, see System Backup Overview on page 215.
2	If you want to transfer the MPP log files, pack them on the old server as described in Packing MPP logs and transcriptions in a TAR file on page 198.
3	If possible, set up the new server so that it has the same IP address and hostname as the old Experience Portal server.
4	On the new server, install the Experience Portal software. For more information, see *Installing the Avaya Experience Portal software* topic in the *Implementing Avaya Experience Portal on a single server* guide. **Important:** Make sure you select the same options you selected for the previous installation, and that you go through the same configuration steps after you install the software. For example, if Avaya Services maintains this Experience Portal system, make sure you set up the Avaya Services access requirements as described in the *Configuring the Avaya Service accounts* topic in the *Implementing Avaya Experience Portal on multiple servers* guide.
5	On the new Experience Portal server, configure the backup and restore scripts as described in Verifying the backup server mount point on page 226. Make sure that you specify the same mount point and shared directory that you used on the old server.
6	Restore the Experience Portal database from the backup you made on the old EPM server as described in Database Restore utility and system backup on page 225.
7	If you archived the MPP log files, restore them by unpacking the TAR archive created by the **`Pack`** command as described in Restoring packed MPP log files on page 201.
8	If you could not use the same hostname and IP address for the new EPM server, change the information in the Experience Portal database as described in Changing the hostname or IP address on a dedicated primary EPM server on page 208.
9	Reestablish the link between the EPM and the MPP as described in Reestablishing the link between the EPM and an MPP on page 197.
10	If your WebLM server ran on the old EPM server, install the Experience Portal license file on the new EPM server as described in the Installing the license file topic in the *Implementing Avaya Experience Portal on multiple servers*. Otherwise, verify that the new EPM server can contact the WebLM server by selecting **Security** > **Licensing** from the EPM main menu and clicking **Verify** on the Licensing page.

Packing MPP logs and transcriptions in a TAR file

About this task

You can use the Diagnostics page 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 as described in Logging in to the Media Server Service Menu on page 295.
2. On the Media Server Service Menu, click **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**.

   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, Experience Portal creates a TAR file for each MPP component with the format *<MPP component>*`_`*<hostname>*`_`*<date and time stamp>*`_MPP.tar`.

   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, 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.
2. Navigate to the MPP `bin` directory by entering the `cd $AVAYA_MPP_HOME/bin` command.

   AVAYA_MPP_HOME is the environment variable pointing to the name of the MPP installation directory specified during the Avaya Experience Portal software installation.
3. Enter the `getmpplogs.sh` command with the desired options. You can select:

Option	Purpose
--web	To run a command from the MPP Service Menu.
--logs	To export system information and MPP logs, Apache logs, and system event logs. The system information exported is: • hostname • system uptime • system CPU and memory information • network configuration • storage usage • `/etc/hosts` file • currently running processes • CPU activity information • RPM database information • 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. **Note:** 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/bin` directory, enter the `getmpplogs.sh --web --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, 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. 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/VoicePortal/MPP/tmp/AVPSupport/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/VoicePortal/MPP/logs/records' to
    '/opt/Avaya/VoicePortal/MPP/logs/records-20070424-1419'...
Restoring '/tmp/untar/logs/records' to '/opt/Avaya/VoicePortal/MPP/
logs/records'...
    Restoring directory and file permissions...
 - Restoring 'Installation logs'
    Moving existing '/opt/Avaya/VoicePortal/MPP/logs/install' to
    '/opt/Avaya/VoicePortal/MPP/logs/install-20070424-1419'...
    Restoring '/tmp/untar/logs/install' to '/opt/Avaya/
VoicePortal/MPP/logs/install'...
    Restoring directory and file permissions...
 - Restoring 'Process logs'
    Moving existing '/opt/Avaya/VoicePortal/MPP/logs/process' to
    '/opt/Avaya/VoicePortal/MPP/logs/process-20070424-1419'...
    Restoring '/tmp/untar/logs/process' to '/opt/Avaya/
VoicePortal/MPP/logs/process'...
    Restoring directory and file permissions...
 - Restoring 'Transcriptions & Utterances'
    Moving existing '/opt/Avaya/VoicePortal/MPP/logs/
transcriptions' to
    '/opt/Avaya/VoicePortal/MPP/logs/
transcriptions-20070424-1419'...
    Restoring '/tmp/untar/transcriptions' to '/opt/Avaya/
VoicePortal/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.

Packing EPM logs and transcriptions using getepmlogs.sh

About this task

The `getepmlogs.sh` script packs system information files, logs, and transcriptions into one TAR file.

Procedure

1. Log on to Linux on the Experience Portal EPM 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.
2. Run the **`cd $AVAYA_HOME/Support/VP-Tools/`** command to navigate to the `VP-Tools` directory.

   AVAYA_HOME is the environment variable pointing to the name of the EPM installation directory specified during the Avaya Experience Portal software installation.
3. Enter the `getepmlogs.sh` command with the one of the following desired options:

Option	Purpose
--EPM	To archive EPM logs from $AVAYA_HOME/logs.
--Apache	To archive the Apache logs from `/var/log/httpd`.
--Install	To archive Install logs from `$AVAYA_HOME/logs/`.
--MainTomcat	To archive MainTomcat from `$CATALINA_HOME/logs`.

Option	Purpose
--MMSTomcat	To archive MMSTomcat from `$MMSSERVER_HOME/logs`.
--ALL	To archive all of the above log files.
--help	To display the above **`getepmlogs.sh`** commands. **Note:** 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 `getepmlogs.sh` script. The types of files that are packed in the TAR file depends on the combination of the command options that you use.

Diagnostics page field descriptions

This page provides you with tools you can use to collect the MPP log files for troubleshooting purposes, and to test the MPP.

To go to the Diagnostics page, log in to the **MPP Service** menu as described in Logging in to the Media Server Service Menu on page 295.

This page contains the following links:

- **Check connections to servers**, which goes to the Check Server Connections page.
- **Pack files**, which goes to the Pack Files Options page.
- **View process messages**, which goes to the Process Messages page.
- **Version**, which goes to the Version page.

Port Distribution Report page field descriptions

Use this page for a real-time view of telephony port distribution across all Media Processing Platform (MPP) servers. You can configure the telephony resources on the VoIP Connections page.

Note:

If there is a port conflict, the text for a particular port appears in red. For more information, see the **Current Allocation** column.

Column	Description
Zone	The name of the zone within which the MPP server is configured.

Table continues…

Column	Description
Servers	The MPP servers for which you want to see the Port Distribution Report. **Note:** This field appears only if you have selected one or more servers from the **Port Distribution** page. If you select **All Servers** from the **Servers** list on the **Port Distribution** page, the system does not display this field.
Port	The Experience Portal port number associated with the port. **Note:** The port distribution report for SIP protocol displays only the highest port distribution record. For detailed port information, click the number of the port to access the Port Information window. Click the **Up** arrow in the column header to sort the ports in ascending order and the **Down** arrow to sort the ports in descending order.
Mode	The operational mode of the port. The options are: • **Online**: The port is available for normal inbound and outbound calls and is allocated to an MPP. • **Inbound**: The port is available for normal inbound calls and is allocated to an MPP. • **Test**: The port is available for calls made to one of the defined H.323 maintenance stations and is allocated to an MPP in Test mode. • **Offline**: The port is not available and is not allocated to any MPP. Click the **Up** arrow in the column header to sort the modes in ascending order and the **Down** arrow to sort the modes in descending order

Table continues…

Column	Description
State	The state of the port. The options are: • **Active:** The port has been assigned to an MPP but the MPP does not know the status of the port because the EPM and the MPP are out of sync. • **Adding:** The port has been assigned to an MPP but the MPP has not taken the port yet. • **Alerting:** The port is ringing and checking resources. • **Available:** The port is ready to be assigned to an MPP. • **Connected:** The port is in service and calls are in progress. • **Delete:** The port is in the process of being deleted from the system. It is in use until the grace period expires. • **Idle:** The port is assigned to an MPP but the MPP is not registered with the switch. The port cannot take calls. • **In Service:** The port is assigned to an MPP and the MPP is registered with the switch. The port is ready to take a call. • **None:** The assigned port is missing. • **Out of Service - Fault:** The MPP is trying to register with the port. • **Out of Service - Manual:** The port is manually taken offline from the MPP. • **Proceeding:** The port was taken offline but is currently coming back into service. • **Removing:** The port is being deleted from the MPP. It will soon be available for assignment to another MPP. • **Trying:** The MPP is trying to register with the port. **Tip:** You can hover the mouse over this column to view more information about the state, including any fault information if the port could not be registered.
Port Group	The name of the port group that the port belongs to. Port groups are administered on the System Configuration pages. Click the **Up** arrow in the column header to sort the groups in ascending order and the **Down** arrow to sort the groups in descending order
Protocol	The port protocol. **Note:** The port distribution data for SIP is consolidated to a single line in each MPP. The port distribution report for SIP protocol displays only the highest port distribution record. Click the **Up** arrow in the column header to sort the protocols in ascending order and the **Down** arrow to sort the protocols in descending order.

Table continues…

Column	Description
Current Allocation	The name of the MPP to which the port is currently allocated. If there is a port conflict, you can hover the mouse over this field to view a tooltip containing one of the following error messages: • Unconfigured port currently owned by <*MPP Name*>. • Port allocated to <*MPP1 Name*> but currently owned by <*MPP2 Name*>. • Port not yet allocated but owned by <*MPP Name*>. • Port allocated to <*MPP Name*> but not owned by it. • Port allocation not yet sent. • Waiting for confirmation of the port allocation.
Base Allocation	The options are: • " " (blank): The port is currently allocated to the optimal MPP. • An MPP name: The optimal allocation for the port. If the base allocation field is not blank, it probably means that the optimal MPP went out of service and the port was reallocated.

Changing a server hostname or IP address

Hostname or IP address changes for Experience Portal servers

If you need to change the IP address or hostname of any server running the Experience Portal software after the software has been installed, or if you need to move the software to a new server that has a different IP address and hostname, you need to change the information stored in the Experience Portal database to match the new system configuration.

After changing the hostname or IP address of the Experience Portal servers, you need to complete the following actions relating to the identity certificates of the Experience Portal servers.

- Default identity certificates: If the Experience Portal servers are using default identity certificates, then a new EP Signing Certificate must be generated or uploaded. Each Experience Portal server must be restarted to install a new identity certificate that is issued by the new EP Signing Certificate. This new identity certificate contains the new IP address and hostname of the Experience Portal server in the Common Name and Subject Alternate Names entries of the identity certificate.
- Custom identity certificates: If the Experience Portal servers are using custom identity certificates, then new custom identity certificates must be installed on the Experience Portal servers. This new custom identity certificates contains the new IP address and hostname of the Experience Portal server in the Common Name and any Subject Alternate Name entries of the identity certificate.

Prerequisites:

Before changing the hostname or IP of any EP servers, ensure to complete the following:

- If the Experience Portal servers are using custom identity certificates, new custom identity certificates must be acquired from the external Certificate Authority for any Experience Portal server whose hostname or IP address is changed.
- If the existing EP Signing Certificate is issued by an external Certificate Authority, a new EP Signing Certificate must be acquired from the external CA with the new hostname and IP address of the Primary EPM.

  Note:

  Use this procedure only if you are changing the hostname and IP address of the Primary EPM. If the EP Signing Certificate was generated by Experience Portal, then this procedure is not required.
- Server Identity Validation must be disabled before you change the hostname or IP for any Experience Portal server. For more information, see Disabling Server Identity Validation on page 598.
- If DNS is used, any required DNS entries must be added for the new FQDN's and IP addresses of the Experience Portal servers.

If you want to change the IP address or hostname of:

- The primary EPM server in a dedicated server environment, see Changing the hostname or IP address on a dedicated primary EPM server on page 208.
- The auxiliary EPM server in a dedicated server environment, see Changing the hostname or IP address on the auxiliary EPM server on page 210
- An MPP server in a dedicated server environment, see Changing the hostname or IP address for a dedicated MPP server on page 212.
- The Experience Portal server running the EPM and MPP software in a single server environment, see Changing the hostname or IP address for the Experience Portal single server system on page 213.

Changing the hostname or IP address on a dedicated primary EPM server

About this task

If you need to change the IP address or hostname of a dedicated primary EPM server after the EPM software is installed, or if you need to move the primary EPM software to a new server that has a different IP address and hostname, you need to change the information stored in the Experience Portal database to match the new system configuration.

Note:

If you want to change the IP address or hostname for a single server Experience Portal system, follow the steps in Changing the hostname or IP address for the Experience Portal single server system on page 213. If you want to change the IP address or hostname for a auxiliary EPM server, follow the steps in Changing the hostname or IP address on the auxiliary EPM server on page 210.

Procedure

1. Log on to Linux on the Experience Portal Primary EPM 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.
2. Stop the *vpms* service by entering the `systemctl stop vpms` command.
3. If you want to change the hostname or IP address of the current server, do the following:
   a. Use the nmtui tool as described in the Red Hat documentation.
   b. Open the `/etc/hosts` file in an ASCII editor and change the IP address and hostname to the values you specified with the configuration tool.
   c. Reboot the EPM server.
   d. Stop the *vpms* service by entering the `systemctl stop vpms` command.
4. Navigate to the `do_UpdateHost` script directory by entering the `$AVAYA_HOME/Support/UpdateHostAddress` command.
5. Enter the `bash do_UpdateHost` command to change the hostname in the database to the hostname of the current server.
6. Start the *vpms* service by entering the `systemctl start vpms` command.
7. If the Primary EPM hostname and IP exists as an entry in the `/etc/hosts` file on the Auxiliary EPM and MPP servers, update these entries with the new hostname and IP address of the Primary EPM

Next steps

Reconnect the existing MPP servers and Auxiliary EPM servers with the Primary EPM server. For more information, see:

- Reconnecting an existing MPP server with the EPM server on page 210
- Reconnecting the primary and auxiliary EPM servers on page 187

Reconnecting an existing MPP server with the EPM server

In a dedicated server environment, if the IP address or hostname of the EPM server changes or if you reinstalled the EPM software, you need to reconnect all MPP servers with the EPM server.

Procedure

1. Log on to Linux on the Experience Portal MPP 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.
2. Navigate to the `$AVAYA_HOME/Support/VP-Tools` directory.
3. Associate this MPP server with the EPM server by entering the `setup_vpms.php` *`myhost`* command, where *`myhost`* is the server name or IP address where the EPM software is installed.
4. Follow the on-screen prompts to install the certificate, restart Apache, and configure Network Time Protocol (NTP).

Next steps

Reestablish the link between the MPP and the EPM by trusting the MPP's security certificate. For more information, see Reestablishing the link between the and an MPP on page 197.

Changing the hostname or IP address on the auxiliary EPM server

About this task

To change the IP address or hostname of the auxiliary EPM server after the EPM software has been installed, or to move the auxiliary EPM software to a new server that has a different IP address and hostname, you must change the information stored in the Experience Portal database to match the new system configuration.

Note:

To change the IP address or hostname for the primary EPM server, follow the steps in Changing the hostname or IP address on a dedicated primary EPM server on page 208.

Procedure

1. Log on to Linux on the Auxiliary EPM 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.

2. Stop the *vpms* service by entering the `systemctl stop vpms` command.
3. To change the hostname or IP address of the current server, do the following:
   a. Use the nmtui tool as described in the Red Hat documentation.
   b. Open the `/etc/hosts` file in an ASCII editor and change the IP address and hostname to the values you specified with the configuration tool.
   c. Reboot the auxiliary EPM server.
   d. After the reboot, stop the *vpms* service by entering the `systemctl stop vpms` command.
4. Navigate to the `do_UpdateHost` script directory by entering the `cd $AVAYA_HOME/Support/UpdateHostAddress` command.
5. Enter the `bash do_UpdateHost` command.
6. Start the *vpms* service by entering the `systemctl start vpms` command.
7. Log on to Linux on the Experience Portal 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.
8. Open the `/etc/hosts` file in an ASCII editor and change the IP address and hostname to the values you specified with the configuration tool.
9. Update the Auxiliary EPM servers host details by doing the following:
   a. Log on to the EPM web interface.

      If Avaya Services is maintaining this system and you are an Avaya Services representative, log on to EPM by using the init EPM account that is created during the EPM software installation.

      Otherwise, log on to EPM by using an account with the Administrator user role.
   b. On the EPM navigation pane, click **System Configuration > EPM Servers**.
   c. On the EPM Servers page, click the name of the auxiliary EPM server.
   d. On the Change EPM Server page, update the information in the **Host Address** field.

      If you logged in using the init account, ensure that the LDN number specified in the **LDN** field matches the information in the Avaya Services database for this server.
   e. Click **Save**.

Changing the hostname or IP address for a dedicated MPP server

About this task

If you need to change the IP address or hostname of a dedicated MPP server after the MPP software has been installed, or if you need to move the MPP software to a new server that has a different IP address and hostname, you need to change the information stored in the Experience Portal database to match the new system configuration.

Note:

If your Experience Portal system consists of a single server, follow the steps in Changing the hostname or IP address for the Experience Portal single server system on page 213.

Procedure

1. Log on to Linux on the Experience Portal MPP 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.
2. Stop the `mpp` service by entering the `systemctl stop mpp` command.
3. If you want to change the hostname or IP address of the current server, do the following:
   a. Use the nmtui tool as described in the Red Hat documentation.
   b. Open the `/etc/hosts` file on the MPP server in an ASCII editor and change the IP address and hostname to the values you specified with the configuration tool.
   c. Reboot the MPP server.
   d. Log on to Linux on the Experience Portal 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.

   e. Open the `/etc/hosts` file on the primary EPM server in an ASCII editor and change the IP address and hostname for the MPP to the values you specified with the configuration tool.
4. Log on to the EPM web interface.

If Avaya Services is maintaining this system and you are an Avaya Services representative, log on to EPM by using the init EPM account that is created during the EPM software installation.

Otherwise, log on to EPM by using an account with the Administrator user role.

5. On the EPM naviagtion pane, click **System Configuration > MPP Servers**.
6. On the MPP Servers page, click on the name of the MPP whose hostname or IP address you changed.
7. On the Change MPP Server page, make sure that the information in the **Host Address** field matches the new IP address or hostname.

   If you logged in using the init account, ensure that the LDN number specified in the **LDN** field matches the information in the Avaya Services database for this server.
8. Click **Save**.

Changing the hostname or IP address for the Experience Portal single server system

About this task

If you need to change the IP address or hostname of the Experience Portal server after the EPM and MPP software has been installed, or if you need to move the Experience Portal software to a new server that has a different IP address and hostname, you need to change the information stored in the Experience Portal database to match the new system configuration.

Note:

If your Experience Portal system consists of one or more dedicated servers, follow the steps in Changing the hostname or IP address on a dedicated primary EPM server on page 208.

Procedure

1. Log on to Linux on the Primary EPM 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.
2. Stop the *vpms* service by entering the `systemctl stop vpms` command.
3. Stop the `mpp` service by entering the `systemctl mpp stop` command.
4. If you want to change the hostname or IP address of the current server, do the following:
   a. Use the nmtui tool as described in the Red Hat documentation.
   b. Open the `/etc/hosts` file in an ASCII editor and change the IP address and hostname to the values you specified with the configuration tool.

c. Reboot the Experience Portal server.

5. Stop the `vpms` service by entering the `systemctl stop vpms` command.
6. Stop the `mpp` service by entering the `systemctl stop mpp` command.
7. Navigate to the do_UpdateHost script directory by entering the `cd $AVAYA_HOME/Support/UpdateHostAddress` command.
8. Enter the `bash do_UpdateHost` command to change the hostname in the database to the hostname of the current server.
9. Start the `vpms` service by entering the `systemctl start vpms` command.
10. Start the `mpp` service by entering the `systemctl start mpp` command.
11. If the Primary EPM hostname and IP exists as an entry in the `/etc/hosts` on the Auxiliary EPM and MPP servers, update these entries with the new hostname and IP address of the Primary EPM.
12. If the application server is co-resident with the Experience Portal single server system, verify and change the hostname or IP address referenced in the Applications page.
    a. On the EPM navigation pane, click **System Configuration** > **Applications**.
    b. Verify the hostname or IP address.

Next steps

Reconnect the existing MPP server and Auxiliary EPM servers with the Primary EPM server.

For more information, see the following:

- Reconnecting an existing MPP server with the EPM server on page 210
- Reconnecting the primary and auxiliary EPM servers on page 187

Installing new Identity Certificates after changing hostname and IP address

After updating the hostnames and IP addresses of the Experience Portal servers, new identity certificates need to be installed on the Experience Portal servers.

The Common Name and any Subject Alternate Name entries in the existing identity certificates for the Experience Portal servers contains the old hostname and IP address which is incorrect. The Common Name and Subject Alternate Name entries are used to validate a network entities identity during the setup of secure communications with that network entity.

Default Identity Certificates

If Experience Portal is using default identity certificates, you need to generate or upload a new EP Signing Certificate.

- If using an EP Signing Certificate that was generated by Experience Portal, you need to generate a new EP Signing Certificate. For more information, see Generating a new EP Signing Certificate on page 569.

- If using an EP Signing Certificate that was issued by an external CA, you need to upload a new EP Signing Certificate. For more information, see Uploading the EP Signing Certificate on page 570.

Custom Identity Certificates

If Experience Portal is using custom identity certificates, new identity certificates need to be installed for each Experience Portal server that has a change in their hostname and IP address.

The new custom identity certificates must have the Common Name and any Subject Alternate Name entries based on the new hostname and IP address of the Experience Portal server. The custom identity certificates are acquired from an external Certificate Authority.

For more information on installing custom identity certificates, see Uploading Identity Certificates on page 579.

Re-enabling Server Identity Validation

After updating the hostname, IP address, and identity certificates for the Experience Portal servers, you can re-enable Server Identity Validation.

For more information, see Enabling Server Identity Validation on page 598.

Local database maintenance

System Backup

System Backup Overview

You can use the System Backup feature in the Experience Portal Manager (EPM) to regularly back up the data in a local Experience Portal database and the associated properties files.

Note:

Before you can use the System Backup feature in EPM, you must complete the tasks in Database backup prerequisites on page 216.

The System Backup web page in EPM allows you to perform the following backup tasks:

- Configure the backup server and verify the backup server connectivity. For more information, see Backup Server page field descriptions on page 222.
- Perform on-demand backup directly on the web page or configure backup schedule to perform backup on a periodic basis. For more information, see Backup Scheduler page field descriptions on page 224.
- Back up Experience Portal database which includes the associated default properties files, and the specified custom files. You can also optionally configure additional files and directories that need to be backed up. For more information, see User Components page field descriptions on page 224.

- Configure the number of backups to retain in the backup server. You can also retain more than one backup data package and select preferred package for data restore operation. For more information, see Backup Server page field descriptions on page 222.
- View the backup history.

  The System Backup feature verifies the current package list in the backup folder against the set number of backups to retain, and removes the older packages based on the timestamp.

The System Backup copies the Experience Portal database and the property files from the EPM server to the local backup folder, or to a Linux or Windows backup server across the network. Refer to the *Local database configuration for System Backup* section for further information on the backup server.

For information on the backup procedure, see Backing up an Avaya Experience Portal system from System Backup menu in EPM on page 218.

Tip:

You should backup your data at periodic intervals to capture any incremental changes to the database.

Local database configuration

Database backup prerequisites

You must complete the following tasks before you can use the System Backup feature in EPM.

✔	Description
	Make sure that there is enough disk space to store a copy of the database.
	Set up the Linux or Windows backup server. For details, see: • Setting up a Linux backup server on page 216 • Setting up a Windows backup server on page 217

Setting up a Linux backup server

Procedure

1. Log in to Linux on the backup server with the user account that Experience Portal uses while performing the backup operation.
2. Enter the `id` command to obtain the UID of the account with which you are currently logged in.

   The system displays the UID. For example: $>id backupuser uid=500(backupuser) gid=500(backupuser) groups=500(backupuser) context=user_u:system_r:unconfined_t
3. Create the backup directory where you want to save the backup packages. For example, if you want Experience Portal to store the backups in the `/home/experienceportal/backup` directory, enter the `mkdir /home/experienceportal/backup` command.

4. Enter the `su -` command to gain temporary root level access.
5. Open the `/etc/exports` file in a text editor.
6. Add a new entry for the new directory, to be shared with Experience Portal, using the following format:

   `<BackupDir> <ExperiencePortalAddress>(rw,sync,all_squash,anonuid=<UID>)` where

   - `<BackupDir>` is the name of the directory to be shared. For example, `/home/experienceportal/backup`.
   - `<ExperiencePortalAddress>` is the IP address of the Primary EPM server that accesses the backup directory.
   - `<UID>` is the ID of the user account that Experience Portal uses when accessing the backup directory.
7. Save and close the file.
8. Enter the **`#>service nfs restart`** command to restart the NFS service.
9. If the backup server is installed on Red Hat Enterprise Linux 5.x, restart the portmap service by entering the **`#>service portmap restart`** command.

   Note:

   If the backup server is installed on Red Hat Enterprise Linux 6, you do not need to restart the rpcbind service.

Setting up a Windows backup server

About this task

You can set up shared directories between the main Experience Portal server and a Windows server.

Note:

Since the Experience Portal server is installed on Linux, you cannot connect to a Windows server unless you have Samba or any other connection utility. For details, see the Red Hat website, http://www.redhat.com.

Procedure

1. Log in to the Windows back up server using an Administrator account.
2. **(Optional)** Add a new user account that the Experience Portal system uses when backing up files to the server. For more information on adding a new Windows user, see the Microsoft Windows documentation.
3. Create the directory that you want to share with the Experience Portal server.
4. To set the shared permissions, right-click on the directory in Windows Explorer and click **Sharing and Security**.
5. In the <folder name> Properties dialog box, click the **Sharing** tab.

6. Click **Share this folder**.
7. Click **Permissions**.
8. In the Permissions dialog box, click **Add**.
9. In the **Enter the object names to select** list box, add the appropriate user name in the format *backup_server_name**user_name*, where:
   - *backup_server_name* is the name of the Windows backup server.
   - *user_name* is the name of a Windows user that currently exists on the backup server.

   For example, if the backup server name is `BackupEPMServer` and the Windows user name is `user`, you need to enter `BackupEPMServer\user`.
10. To return to the Permissions dialog box, click **OK** .
11. In the **Group or user names** list box, select the user you just added.
12. In the **Allow** column for that user, enable the **Change** and **Read** check boxes.

    The **Full Control** permission is optional.
13. To return to the <folder name> Properties dialog box and to save your changes, click **OK**.
14. Click **OK**.

Backing up an Avaya Experience Portal system from System Backup menu in EPM

Before you begin

Before you use the System Backup feature in EPM, you must complete the tasks in Database backup prerequisites on page 216.

Procedure

1. Log in to the EPM web interface.
2. On the EPM navigation pane, click **System Management** > **System Backup**.
3. Click the **Backup Server** icon .
4. On the **Backup Server** page, update the configuration details, and click **Verify**.

   Important:

   Ensure that the backup is stored on a server that is not part of the Experience Portal system.

   EPM verifies if the backup folder exists and can be mounted using the specified parameters such as server address and backup folder, and displays the details in the Verify Backup Server window.
5. On the Verify Backup Server window, click **Close Window** .
6. On the **Backup Server** page, click **Save** .

7. On the **System Backup** page, click the **Backup Schedule** icon if you want to specify a schedule for the backup procedure.
8. On the **Backup Scheduler** page, configure the backup schedule, and click **Save**.
9. Click the **User Components** icon .
10. On the **User Components** page, configure user components for the backup operation, and click **Save**.
11. Click **Backup Now** to initiate an on-demand backup.

Result

When the backup is complete, the **System Backup** page displays the backup completed message.

Note:

Click **Refresh** to check if the backup completed message is displayed.

Next steps

On the **Backup History** section of the **System Backup** page:

- Verify that the package is created
- Verify the Date/Time details of the package

Note:

The package list is not displayed if the backup server is not configured properly.

System Backup page field descriptions

Use this page to perform the backup operation and configure the backup servers, backup schedule, and the files and folder for backup operation.

This page contains the following sections:

- Backup Server section on page 219
- Backup Scheduler section on page 220
- Backup Components section on page 220
- Backup History section on page 220
- Buttons section on page 221

Backup Server section

Field	Description
Server Type	Type of the backup server type. The options are:
Server Address	Network address of the backup server.

Table continues…

Field	Description
Backup Folder	Name of the folder where the backup data is stored.
Number of Backup(s) to Retain	Number of backup data packages to be retained in the backup server.
Backup Server icon 	Opens the Backup Server page for configuring the backup server.

Backup Scheduler section

Field	Description
Backup Schedule	Configured schedule for backup.
Backup Schedule icon 	Opens the Backup Scheduler page for configuring the backup schedule.

Backup Components section

Field	Description
EP Database/ Properties	Experience Portal data that includes the Experience Portal database and the associated properties files.
User Components	Number of files and folders specified for backup.
Backup Components icon 	Opens the User Components page for configuring the backup schedule.

Backup History section

Field	Description
Packages	List of existing backup packages saved in the backup server. The package list is not displayed if the backup server is not configured properly.
Date/Time	Date and time when each data package was backed up.

Buttons section

Button	Description
Backup Now	Initiates the on-demand backup for the specified components on the configured server. **Tip:** Verify the backup server details before initiating the on demand backup. Select the **Backup Server>Verify** web page to verify that the backup folder exists and can be mounted using the specified username and password. For more information, see Verify Backup Server page field descriptions on page 223 On initiating the on-demand backup, the **Backup Now** button changes to **Cancel Backup** till the backup operation is in progress.
Cancel Backup	Stops the backup operation in progress.

View System Backup page field descriptions

Use this page to view the backup configuration, backup schedule, and the files and folder for backup operation.

This page contains the following sections:

- Backup Server section on page 221
- Backup Scheduler section on page 221
- Backup Components section on page 222
- Backup History section on page 222

Backup Server section

Field	Description
Server Type	Type of the backup server type. The options are:
Server Address	Network address of the backup server.
Backup Folder	Name of the folder where the backup data is stored.
Number of Backup(s) to Retain	Number of backup data packages to be retained in the backup server.

Backup Scheduler section

Field	Description
Backup Schedule	Configured schedule for backup.

Backup Components section

Field	Description
EP Database/ Properties	Experience Portal data that includes the Experience Portal database and the associated properties files.
User Components	Number of files and folders specified for backup.

Backup History section

Field	Description
Packages	List of existing backup packages saved in the backup server. The package list is not displayed if the backup server is not configured properly.
Date/Time	Date and time when each data package was backed up.

Backup Server page field descriptions

Use this page to configure the backup servers, mount point and the authentication information to connect and mount the backup server.

This page contains the following sections:

- Backup Server section on page 222
- Number of Backup(s) to Retain section on page 223
- State Commands on page 223

Backup Server section

Field	Description
Server Type	Type of the backup server. The options are:
Server Address	Network address of the backup server. If the backup server is a Windows 7 or Windows 2008 R2 server, enter a valid Fully qualified domain name (FQDN). For all other servers, enter a valid IP address. You can use 127.0.0.1 or localhost as the host/IP address to use the local system as a backup server.

Table continues…

Field	Description
Backup Folder	Name of the folder where the backup data is stored. The backup folder name on Linux must have the syntax: `/<Folder name>` where, `<Folder name>` indicates a shared directory that is used to store the backup files in the backup server. **Note:** For a local backup, verify that the avayavp and avayavpgroup linux users have the read, write, and execute permissions for the backup folder. The backup folder name on Windows must have the syntax: `/<Folder name>` or `\<Folder name>`. where, `<Folder name>` indicates a shared directory that is used to store the backup files in the backup server. For example, the default is `C:\Avaya\backup`.
Username	The user name used to mount the backup server.
Password	The password used to connect and mount the backup server.
Verify	Verifies that the backup folder exists and can be mounted using the specified parameters such as server address and backup folder.

Number of Backup(s) to Retain section

Field	Description
Number of Backup(s) to Retain	Number of backup data packages to be retained in the backup server. The existing packages are deleted if the limit is exceeded. The maximum limit of backups to retain is 5.

State Commands

Button	Description
Save	Saves the new settings and navigates to the **System Backup** page.
Apply	Saves the new settings.
Cancel	Cancels the changes and navigates to the **System Backup** page.

Verify Backup Server page field descriptions

Use this page to verify that the backup folder exists and can be mounted.

Field	Description
Server Type	Type of the backup server. The options are:

Table continues…

Field	Description
Server Address	Network address of the backup server.
Backup Folder	Name of the folder where the backup data is stored.
Username	The user name used to mount the backup server. This field is displayed only when the backup server type selected is **PC Windows** and the **Server Address** is not a local server.
Result	Shows whether the backup server was configured successfully or not. For Example: • Backup server was verified successfully. • null mount: mount to NFS server <IP address> failed: System Error: No route to host.

Backup Scheduler page field descriptions

Use this page to schedule the backup operation to run on a periodic or one time basis.

Select Backup Schedule section

Field	Description
None	Disables the backup scheduling.
One time at	Performs backup operation only on the specified date and time.
Daily at	Performs backup operation every day at the specified time.
Weekly on	Performs backup operation every week on the specified day and time.
Monthly on	Performs backup operation every month on the specified day and time.

Note:

If the backup schedule is reached and the previous backup operation is still in progress, the backup action is dropped till its next cycle allowing the backup in progress to complete.

State Commands

Button	Description
Save	Saves the new properties and navigates to the **System Backup** page.
Apply	Saves the new properties.
Cancel	Cancels the changes and navigates to the **System Backup** page.

User Components page field descriptions

Use this page to configure user components for the backup operation. You can configure more than one file and folder that you want to backup.

Field	Description
Folder	Name and the path of the folder that you want to backup. The path must an absolute path. For example: For Linux, `/opt/coreservices/dss`, indicates that you want to backup the contents of `dss` folder located in the `/opt/coreservices` directory. For Windows, you can use forward slash (/), back slash (\), as well as the drive name in the path.
File	Name and the path of the file that you want to backup. You can specify the file name with file extension or with asterisk (*). For example, you can specify file names like *.xml or common.*.

Note:

For Linux, verify that the avayavp and avayavpgroup linux users have the read permission for the folder and file that you want to backup.

If you specify a valid folder name but the file field is empty, all the files from the specified folder are backed up. However, the subfolders are not considered for the back up.

You cannot add duplicate entries. If you try to add the same details suffixed or prefixed with an extra space, that too is treated as a duplicate entry.

State Commands

Button	Description
Save	Saves the new properties and navigates to the **System Backup** page.
Apply	Saves the new properties.
Cancel	Cancels the changes and navigates to the **System Backup** page.
Add	Adds the new properties.
Delete	Deletes the new properties.

Database Restore utility

Database Restore utility and system backup

You can use the Database Restore utility to restore your Experience Portal database from a backup created through the **System Backup** web page in EPM.

To restore your Experience Portal database that is installed on Linux:

- Ensure the backup server mount point is updated in the `do_MntDrv` script. For more information, see Verifying the backup server mount point on page 226.
- Use the do_RestoreData script for restoring data. For more information, see Restoring data backed up from System Backup on page 227.

Important:

If your primary Experience Portal server fails and cannot be recovered, you must first reinstall the EPM software on a new server. Then you can restore your Experience Portal database using the Database Restore utility.

For details about the **System Backup** feature in EPM, see System Backup Overview on page 215.

Verifying the backup server mount point

About this task

The Database Backup utility `do_MntDrv` script, used during the restore procedure, creates a shared directory at the mount point on the Experience Portal server and connects that shared directory with the Linux or Windows backup server.

Note:

You cannot connect to a Windows server unless you have Samba or other connection utility. For details, see the Red Hat Web site, http://www.redhat.com.

The `do_MntDrv` script is updated automatically with the backup server details configured in the **System Backup>Backup Server** EPM web page.

Important:

Before you can run this script, you must verify your system details. If the system details are not updated in the script, edit the details as described below.

Procedure

1. Log on to Linux on the Experience Portal Primary EPM 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.
2. Navigate to the backup directory located in $AVAYA_HOME by entering the cd `$AVAYA_HOME/Support/Database/DBbackup` command.
3. Open the `do_MntDrv` script in an ASCII text editor.

   This file contains a sample mount drive command.

   `bash MntDrive pc ipAddress backupServerFolder backupUserName` where

   - `[type]` is either `linux` or `pc` based on the type of back up server you are using. Sample command displays **pc** as type.
   - *`[host address]`* is the backup server name or IP address. Sample command displays **ipAddress** as host address.

- *shared_dir* is the name of the shared directory on the backup server. For Linux, this must be the full path. For Windows, this must be the shared directory name. Sample command displays **backupServerFolder** as shared directory.
- *[Windows_user]* is used only when the backup server is a Windows machine. Replace this parameter with the name of the Windows user that is authorized to access the database. The default is `postgres`. Sample command displays **backupUserName** as Windows user.

4. Verify your backup server details.
   - If you configure the Linux system `voiceportal-linux-backup` as the backup server and set up `/misc/dbbackup` as the shared directory in the **System Backup>Backup Server** EPM web page, verify the `do_MntDrv` script is as follows:

     ```
     bash MntDrive linux voiceportal-linux-backup /misc/dbbackup
     ```
   - If you configure the Windows XP system `voiceportal-xp-backup` as the backup server and set up `c:\temp\EP_dbbackup` as the shared directory in the **System Backup>Backup Server** EPM web page, verify the `do_MntDrv` script is as follows:

     ```
     bash MntDrive pc voiceportal-xp-backup VP_dbbackup postgres
     ```

     For example: `bash MntDrive pc <IP Address> VP_bu postgres`.
5. Save and close the file if `do_MntDrv` is updated.

Restoring data backed up from System Backup

Before you begin

The Experience Portal software version must be the same version that was used to create the backup.

Verify the `do_MntDrv` script. For further information, see Verifying the backup server mount point on page 226.

For more information, see Backup Server page field descriptions on page 222.

Procedure

1. Log on to Linux on the Experience Portal Primary EPM 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.
2. Stop the vpms service by entering the `/sbin/service vpms stop` command.
3. Stop the avpSNMPAgentSvc service by entering the `/sbin/service avpSNMPAgentSvc stop` command.
4. If there is an application server installed on the system, enter the `/sbin/service appserver stop` command to stop the application server.

5. Navigate to the backup directory located in $AVAYA_HOME by entering the cd `$AVAYA_HOME/Support/Database/DBbackup` command.
6. If the backup package is on a remote server:
   a. Enter the `bash do_MntDrv` command.
   b. Restore the database by entering the `bash do_RestoreData` command.

   If the backup package is on a local server:

   Enter the `do_RestoreData -f <backup file name>` command. For example, enter the `do_RestoreData -f /opt/Avaya/backup` which indicates that you want to restore the contents of *backup* folder located in the `/opt/Avaya` directory.

   Note:

   The command will first clean the database.

   The list of existing backup packages saved in the backup server is displayed.
7. Select the package for Experience Portal data restore.
8. Press Enter to continue.

   The script completes the restore process.
9. If the script displays a message to restart the postgresql service for the changes to take effect, then manually restart the postgresql service by running the **`/sbin/service postgresql restart`** command.
10. Perform the following steps if the hostname or IP address of the server running the EPM or MPP software has changed since you created the database backup:
    a. To navigate to the `do_UpdateHost` script directory, enter the `cd $AVAYA_HOME/Support/UpdateHostAddress` command.
    b. To change the hostname in the database to the hostname of the current server, enter the `bash do_UpdateHost` command .
11. Restart the vpms service by entering the `/sbin/service vpms start` command.
12. Restart the `avpSNMPAgentSvc` service by entering the `/sbin/service avpSNMPAgentSvc start` command.
13. If there is an application server installed on the system, restart the application server by entering the `/sbin/service appserver start` command.
14. Reconnect each MPP server with the EPM server.
15. Reestablish the link between the MPP and the EPM by trusting the MPP's security certificate.
16. Reconnect each auxiliary EPM server with the primary EPM server as described in Reconnecting the primary and auxiliary EPM servers on page 187.
17. If you are restoring your Experience Portal database to a new server, you need to install a new license file on the server. For further information, see Installing the license file section

in the *Implementing Experience Portal on multiple servers* or the *Implementing Avaya Experience Portal on single server* guide.

Note:

This step is not required if you are using a remote WebLM.

18. To unmount the shared directory, enter the `bash UmntDrive` command.

Resetting report data positions using the local database

About this task

Use this procedure to reset report data positions in the local database after you run the restore scripts.

Although you must always run the script mentioned in this procedure on the primary EPM, you might need to run the script multiple times. You must specify different EPM names each time you restore the EPM. If you restore multiple EPMs, then you must run the script once for each of those EPM names.

Note:

If you do not run the script on the primary EPM, Experience Portal does not collect email and SMS report data from the primary or auxiliary EPM.

Procedure

1. Log on to Linux on the Experience Portal 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. On the primary EPM, for each configured EPM name that has a SMS or Email processor, run the **`./ResetEmailSMSLocalDB <EPM_Name>`** command.
4. Reboot the primary EPM server.

Purging report data from a local Experience Portal database

About this task

The `PurgeReportDataLocalDB` script purges all report data from the `VoicePortal` database. This data includes all:

- Application Detail Records (ADRs) stored in the `vpapplog` table
- Contact Detail Records (CDRs) stored in the `cdr` table
- Performance records stored in the `vpperformance` table
- Session Detail Records (SDRs) stored in the `sdr` table

Important:

After you run this script, users cannot generate reports through the EPM until the EPM has downloaded the current report data from the Media Servers.

Procedure

1. Make sure that the EPM is not currently downloading report data from the Media Servers.
   a. Log on to the EPM web interface by using an account with the Administration user role.
   b. From the Media Server Service Menu, select **System Configuration > EPM Servers > Report Data**.
   c. Go to the display text box in the **Download and Maintenance Schedules** group and make sure that no downloads are scheduled for the current time.
2. Log in to Linux on the Primary or Auxiliary EPM 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. Navigate to the `Support/VP-Tools` directory under the Experience Portal installation directory.
4. Enter the `cd $AVAYA_HOME/Support/VP-Tools` command. `$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`.
5. Enter the `bash PurgeReportDataLocalDB` command.

   Important:

   The system may take some time to purge the data depending on the amount of data in the database tables.

   If the script runs successfully, it returns a message stating that the data was purged from the database. Otherwise, it returns a message stating the problem that it encountered.

Masking a contact number in the local Experience Portal database

About this task

Use this procedure to mask a specified contact number in all CDR records in the local Experience Portal database.

The `MaskContactNumberLocalDB` script examines all CDR records in the local Experience Portal database and replaces all instances of the specified contact number with a new contact

number. The script searches both the Originating Number field and the Destination Number field in each CDR record. For example, any reference to sip:4085551212 can be replaced with sip:408******* or just ****.

Procedure

1. Log on to Linux on the Primary EPM 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.
2. Navigate to the `Support/VP-Tools` directory under the Experience Portal installation directory.
3. Enter the **`cd $AVAYA_HOME/Support/VP-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 MaskContactNumberLocalDB "current contact number" "new contact number"`** command.

   Ensure to enclose any value that contains non alphanumeric characters with quotation marks. For example, **`bash MaskContactNumberLocalDD "sip:4085551212" "****"`**

   Note that the system may take some time to mask the data depending on the amount of data in the CDR database table.

   If the script runs successfully, it returns a message stating how many records were updated. Otherwise, it returns a message stating the problem that it encountered.

External database configuration

Shared external database configuration for multiple Experience Portal systems

If you have multiple Experience Portal systems, you may want to set up a shared external database so that you can log into the EPM for one system and:

- See the status of all systems in the shared database
- Create reports that include data from all systems in the shared database

Once you connect the Experience Portal system to the external database, that system stores all its report data in the external database from that point forward. The report data includes:

- Contact Detail Records (CDRs)
- Session Detail Records (SDRs)
- Application Detail Records (ADRs)
- Performance report records

Important:

You must back up the external database manually using your database administration tools. You cannot use the Avaya Experience Portal Database Backup utility to back up an external database.

External database requirements

The performance of the Experience Portal internal database degrades when 5 to 10 million records exist in any table. When you expect the number of calls or number of application-generated report records to exceed these values, you must use an external database.

The external database can be a new or existing database created in:

- Microsoft SQL Server 2010 and greater
- MySQL 5.6 and greater
- MariaDB 10.5 and greater
- Oracle 11g and greater
- PostgresSQL 9.6.x and greater

Note:

Avaya has tested Experience Portal with Oracle and SQLServer reporting databases containing approximately 50 million total records without any issues. Due to variances in database hardware and network performance, Avaya cannot provide a finite maximum number of records before the database reaches its practical limit. Scheduled reports are not subject to timeouts and can be used when on-demand report generation begins to time out. However, record insertions must be completed within 60 seconds to avoid web service time-outs and perpetual retries. Increasing the web service time-outs is not recommended. When insert time-outs occur regularly, Avaya recommends that you lower the record retention periods in the Report Data Configuration page. Fewer records mean faster insertions and faster report generation.

Important:

The administration and maintenance of the external reporting database and the periodic maintenance of the indexes is a customer responsibility.

Creating the required tables in the external database

In order to create the tables that Experience Portal requires in the shared database, you need to run the scripts provided on the Experience Portal Installation DVD against an Oracle, Postgres, Microsoft SQL Server, MySQL or MariaDB database.

Before you begin

If you use an existing database, Experience Portal appends its required tables to that database without altering any of the existing data.

The Experience Portal data requires approximately 4 GB of space per million calls handled.

Note:

If you use a Microsoft SQL Server external database that needs to support multibyte characters, you need to create a new Microsoft SQL Server database and select the appropriate collation for the desired language. For instance, for Microsoft SQL Server Management Studio 2008 you need to perform the following steps during database creation:

- Click **Options** under the **Select a page** section.
- Select the appropriate collation for the desired language in the **Collation** field.
- Ensure that the collation you select is of the case-insensitive type. Case-insensitive types contain the letters CI. For example, Japanese_CI_AI.

Note:

Experience Portal adds tables to the database without changing any existing data. Therefore Experience Portal can share an existing external database with other applications as long as the database meets the version requirements.

Important:

Ensure that the external database is not installed on any Experience Portal server.

Procedure

1. Insert the Experience Portal installation DVD into the DVD device of the server on which you want to create the database.
2. If you are using:
   - Oracle, change to the Oracle support directory `Support/ExternalDB/Oracle/InstallScripts/`.
   - Postgres, change to the Postgres support directory `Support/ExternalDB/Postgres/InstallScripts/`.
   - Microsoft SQL, change to the SQL Server support directory `/Support/ExternalDB/MSSQL/InstallScripts/`.
   - MySQL or MariaDB, change to the MySQL or MariaDB support directory `/Support/ExternalDB/MySQL/InstallScripts/`.

3. Use your database administration tool to run all of the scripts containing the database schema in the appropriate `Support/ExternalDB` directory.

   These scripts create the required tables in the external database.

   Note:

   For Oracle, the database user name for Experience Portal must be assigned CREATE TABLE and CREATE SESSION privileges for the database.

   For Microsoft SQL Server, the database user name for Experience Portal must be assigned SELECT, INSERT, UPDATE and DELETE privileges on all tables in the database.

   For both MySQL and MariaDB, the database user name for Experience Portal must be assigned SELECT, INSERT, UPDATE, DELETE privileges on all tables in the database. The CREATE TEMPORARY TABLE permission is also required. When creating the database, set a collation type of utf8_unicode_ci.

Next steps

Connect your Experience Portal systems to the external database as described in Connecting the Experience Portal system to a shared external database on page 234

Connecting the Experience Portal system to a shared external database

About this task

After you connect the Experience Portal system to an external database, the system copies all the report data that is currently on all MPPs in that system, into the external database. Users can then generate reports that include that data. However, they cannot include any data that resides in the local Experience Portal database.

Note:

The amount of data available on each MPP depends on the settings for the fields in the **Record Handling on MPP** group on the MPP Settings page.

Before you begin

Ensure that you have created the required tables in the external database as described in Creating the required tables in the external database on page 233.

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** > **EPM Servers**.
3. On the EPM Servers page, click **Data Storage Settings**.
4. On the Data Storage Settings page, in the **Report Database** group, select **External** .
5. In the **URL** field, enter the path to the external database.

A common URL format for Oracle connections is:
`jdbc:oracle:thin:@OracleServerName:1521:DBName`

A format for PDB (portable db) connections is:
`jdbc:oracle:thin:@`*`ServerName`*`:1521/`*`pdbName`*

A format for CDB (container db) connections is:
`jdbc:oracle:thin:@`*`ServerName`*`:1521/`*`cdbName`*

A common URL format for Postgres is: `jdbc:postgresql://PostgresServerName:5432/DBName`

A common URL format for Microsoft SQL connections is: `jdbc:sqlserver://SQLServerName:1433;databaseName=DBName`

A common URL format for MySQL connections is: `jdbc:mysql://`*`ServerName`*`:3306/`*`DBName`*

A common URL format for MariaDB connections is: `jdbc:mariadb://`*`ServerName`*`:3306/`*`DBName`*

6. In the **JDBC Driver** field, enter the name of the Java class that implements the JDBC API to the external database.

   For Oracle, the name is `oracle.jdbc.driver.OracleDriver`.

   For Postgres, the name is `org.postgresql.Driver`.

   For Microsoft SQL Server, the name is `com.microsoft.sqlserver.jdbc.SQLServerDriver`.

   For both MySQL and MariaDB, the name is `org.mariadb.jdbc.Driver`.

7. In the **User Name** and **Password** fields, enter the user name and password for the external database.
8. Click **Apply**.

Result

- If Experience Portal can connect to the new database, the system scheduler begins saving all the report data that is currently on all MPPs in that system into the external database.
- If Experience Portal cannot connect to the database, it displays an error message on the page. Experience Portal cannot write to the external database until you fix the error.

Disconnecting the Experience Portal system from a shared external database

About this task

When you disconnect the Experience Portal system from a shared external database, the system scheduler begins saving all report data, that are currently on all the MPPs in that system, into the local Experience Portal database.

After you disconnect the system, users can generate reports that include the current data that resided on the MPPs along with any older data that previously existed in the local database. However, they cannot include any data that resides in the external database.

Note:

The amount of data available on each MPP depends on the settings for the fields in the **Record Handling on MPP** group on the MPP Settings page.

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** > **EPM Servers**.
3. On the EPM Servers page, click **Data Storage Settings**.
4. On the Data Storage Settings page, in the **Report Database** group, select **Local**.
5. Click **Apply**.

Result

Experience Portal records all the data in the local Experience Portal database from this point forward.

However, it does not delete any data from the external database. If you reconnect the system later, users can once again access the old data unless it has been purged.

Purging Experience Portal report data from an external database

About this task

The `PurgeReportDataExtDB` script purges the report data from the external database for any inactive Experience Portal system. This data includes all:

- Application Detail Records (ADRs) stored in the `vpapplog` table
- Contact Detail Records (CDRs) stored in the `cdr` table
- Performance records stored in the `vpperformance` table
- Session Detail Records (SDRs) stored in the `sdr` table
- System information such as the unique identifier for each Media Server associated with the Experience Portal system

Procedure

1. Make sure that the Experience Portal system whose data you want to purge is inactive. To do so:
   a. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
   b. From the EPM main menu, select **Real-time Monitoring** > **System Monitor** and go to the Summary tab.

c. Make sure the **State** column says **Inactive**. To change the system status to Inactive, disconnect the system from the shared external database. For more information, see Disconnecting the Experience Portal system from a shared external database on page 235

2. Log in to Linux on the primary or auxiliary EPM 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. Enter the `cd $AVAYA_HOME/Support/VP-Tools` command. `$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 PurgeReportDataExtDB "Ext_DB_URL" JDBC_Driver Ext_DB_Username EP_System_Name` command.

   Where:
   - *"Ext_DB_URL"* is the fully-qualified path to the external database.

     Note:

     The quotation marks are used around the first parameter when purging data from an external database. For example, the *Ext_DB _URL* parameter is surrounded with the quotation marks while running the script.
   - *JDBC_Driver* is the name of the Java class that implements the JDBC API to the external database.
   - *Ext_DB_Username* is the user name for the external database.
   - *EP_System_Name* is the name of an **Inactive** Experience Portal system.

   Note:

   Database URLs containing semi-colons need to be enclosed within quotes. For example, 'jdbc:sqlserver://<db ip address>:<port>;databaseName=<db name>'.

   The values specified for these parameters should match the values specified on the EPM Settings page in the EPM.

   Important:

   The system may take some time to purge the data depending on the amount of data in the database tables.
5. Enter the external database password.
6. At the prompt, press **Enter** to continue.

If the script runs successfully, it returns a message stating that the data was purged from the database. Otherwise, it returns a message stating the problem that it encountered. For example, the script will return an error message if you specify the name of an active system or if the system name you specify does not exactly match one of the systems in the external database.

Masking a contact number in the external Experience Portal database

About this task

Use this procedure to mask a specified contact number in all CDR records in the external Experience Portal database.

The `MaskContactNumberExtDB` script examines all CDR records in the external Experience Portal database and replaces all instances of the specified contact number with a new contact number. The script searches both the Originating Number field and the Destination Number field in each CDR record. For example, any reference to sip:4085551212 can be replaced with sip:408******* or just ****.

Note that only CDR records belonging to the specified Experience Portal system are updated.

Procedure

1. Log on to Linux on the Primary EPM 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.
2. Navigate to the `Support/VP-Tools` directory under the Experience Portal installation directory.
3. Enter the **`cd $AVAYA_HOME/Support/VP-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 MaskContactNumberExtDB "current contact number" "new contact number" "Ext_DB_URL" JDBC_Driver Ext_DB_Username EP_System_Name`** command.

   Where,
   - “current contact number” is the contact number to be replaced.
   - “new contact number” is the replacement value for the contact number.
   - “Ext_DB_URL” is the fully-qualified path to the external database.

- JDBC_Driver is the name of the Java class that implements the JDBC API to the external database.
- Ext_DB_Username is the user name for the external database.
- EP_System_Name is the name of an Experience Portal system.

Ensure to enclose any value that contains non-alphanumeric characters with quotation marks. For example, **bash MaskContactNumberExtDB "sip:4085551212" "****" "jdbc:oracle:thin:@148.147.6.139:1521:ep" "oracle.jdbc.driver.OracleDriver" voiceportal scaaep134**.

Note that the system may take some time to mask the data depending on the amount of data in the CDR database table.

5. Enter the external database password.
6. At the prompt, click **Enter** to continue.

   If the script runs successfully, it returns a message stating how many records were updated. Otherwise, it returns a message stating the problem that it encountered.

Resetting report data positions using external databases

About this task

Use this procedure to reset report data positions in external databases after the restore scripts are run.

Though the script that is mentioned in the procedure is executed always on the primary EPM, the script may need to be executed multiple times. You will need to specify different EPM names each time it is restored. If you restore multiple EPMs then the script needs to be run once for each of those EPM names.

Note:

The Email and SMS report data is not collected from the primary or auxiliary EPM, if the procedure is not run on the primary EPM.

Procedure

1. Log on to Linux on the Experience Portal 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. On the primary EPM, for each configured EPM name that has an SMS or Email processor, run the following command: **./ResetEmailSMSExtDB "<Database_URL>" <JDBC_Driver> <Database_User_Name> <Experience_Portal_Name> <EPM_Name>**

Where,

- "<Database_URL>" is the URL of the external database as it appears on the **Report Database Settings** page of the EPM web interface.
- <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.
- <EPM_name> is the name of the Primary or Auxiliary EPM as it appears on the **EPM Servers** page of the EPM web interface.

4. Reboot the Primary EPM server.

EPM Servers page field descriptions

Use this page to configure the EPM servers on this Experience Portal system.

Column	Description
Selection check box	Indicates which auxiliary EPM servers you want to delete. **Note:** You cannot delete the primary EPM server.
Zone	The name of the zone where the EPM server is configured.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. . **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
Name	The name of the EPM server.
Type	The options are: • **Primary**: This is the primary EPM server for this system. • **Auxiliary**: This is the backup EPM server for this system.
Host Address	The hostname or IP address of the EPM server.

Table continues…

Column	Description
Add	Opens the Add EPM Server page so that you can specify the location of the auxiliary EPM server, if one is configured for your system. **Note:** You can add one or more auxiliary EPM servers to the Experience Portal system.
Delete	Deletes the selected auxiliary EPM servers.
EPM Settings	Opens the EPM Settings page.
Event Handlers	Opens the Event Handlers page so you can change the global event handlers and prompts for all MPP servers.
Privacy Settings	Opens the Privacy Settings page. **Note:** **Privacy Settings** is available in EPM only when the media server is MPP and when you log in to EPM with a **Privacy Manager** user role.
Data Storage Settings	Opens the Data Storage Settings page.
Report Data	Opens the Report Data Configuration page.
Alarm Codes	Opens the Alarm Codes page.
Alarm/Log Options	Opens the Alarm/Log Options page.
Syslog Settings	Opens the Syslog Settings page.

EPM Settings page field descriptions

Use this page to set the options that affect the primary EPM server

This page contains the:

General section

Field	Description
Experience Portal Name	The name of this Experience Portal system. Experience Portal displays this name on the Summary tab of the System Monitor page.

Table continues…

Field	Description
Number of Application Server Failover Logs	The number of backup logs to retain on the application server in case the application server cannot communicate with the Experience Portal database. Each log file can be up to 100MB in size. The number of failover logs determines how much data the server can send to the EPM when the connection is restored. If the number of failover logs is exceeded, the application server deletes the oldest log file and begins recording data in a new file. When that file is full, the application server deletes the oldest log file and opens a new file. This process is repeated until contact with the Experience Portal database is restored and the application server can write its logs to that database.
Commands to Retain in Configuration History	The number of media server configuration changes that Experience Portal should save in the database. This value determines the number of entries on the <Media Server Name> Configuration History page.

Resource Alerting Thresholds (%) group

Field	Description
Disk	The low water threshold determines when the EPM generates an event, warning you, that disk usage is getting high. The high water threshold determines when the EPM generates an alarm, warning you, that disk usage is getting dangerously high. • **High Water**: Enter a whole number from 0 to 100. The default is 90. • **Low Water**: Enter a whole number from 0 to 100. The default is 80.
HTML Units	The HTML usage threshold determines when the system approaches the licensed usage limit. The administrator can configure the HTML usage threshold that triggers an alarm when the system approaches the licensed usage limit. The threshold is displayed in percentage.

Note:

If the system is configured to use the local postgres database, the Call Data Handler (CDH) scheduler stops downloading report data from media server when the disk space on the EPM is below the configured high water alerting threshold.

Web Service Authentication group

Important:

If you change the user name or password, there will be a delay of two-minute before these changes propagate across the system. Any request for web services made with the new user name and password will fail until that propagation is complete.

Note:

If these fields are not displayed, click the group heading to expand the group.

Field	Description
Application Reporting section	
User Name	The user name to send to the Application Logging web service for Digest Authentication. **Note:** • The user name must not contain the : ! ( ) characters. • You cannot use the same user name for both the Application Logging web service and the Application Interface web service.
Password	The password associated with the specified user name.
Verify Password	The associated password again for verification purposes.
Outcall section **Note:** The **Outcall** section is available in EPM only if the media server is MPP.	
User Name	The user name to send to the Application Interface web service. **Note:** You cannot use the same user name for both the Application Logging web service and the Application Interface web service.
Password	The password associated with the specified user name.
Verify Password	The associated password again for verification purposes.

Miscellaneous group

Field	Description
License Re-allocation Wait Time (minutes)	The number of minutes the system waits before reallocating the licenses from a media server that is out of service to other media servers in the system. Enter a whole number from 0 to 1440. The default is 10.
Operational Grace Period (minutes)	The number of minutes Experience Portal waits for processing to complete before it terminates the remaining EP activities for any of the following Primary EPM, Auxiliary EPM, and MPP commands: • Stop • Reboot • Halt Enter a whole number of minutes between 0 and 999 in this field. **Important:** Ensure that the grace period is long enough for the media server to complete any existing activity before it invokes one of the EP Media Server commands mentioned above.

Table continues…

Field	Description
Event Level Threshold to Send to EPM	Besides Fatal alarms, which are always sent, the lowest level of events and alarms to be included in the tracing log that is sent to the EPM. The options are: • **Error**: Fatal alarms and Error alarms are sent. • **Warning**: Fatal alarms, Error alarms, and Warning events are sent. • **Info**: All events and alarms are sent. **Note:** Selecting the **Info** option can cause performance problem as all events and alarms are sent from the media server to EPM.
Multi-Media Server Numeric ID Range	Experience Portal assigns a numeric ID for each MPP server, Email processor, and SMS processor in the Experience Portal system from the number range given in this field. This numeric ID identifies the MPP in the Experience Portal database and becomes part of the Universal Call Identifier (UCID) associated with every call processed on that MPP server, Email processor, or SMS processor. **Tip:** The ID assigned to a specific MPP server is displayed in the **Unique ID** field on the <MPP name> Details page for that server. Enter a range between 1 and 32,767. The default range is 10,000 to 19,999. **Important:** You should only change this value if other components in your call center create Universal Call Identifier (UCID) values that conflict with the default Experience Portal values. If you do change the value, ensure that you specify a range that covers all MPP servers, Email processors, and SMS processors in your Experience Portal system.
Maximum Number of Conversations per Server	The maximum number of conversations that can be stored at any given time on either a Primary EPM or an Auxiliary EPM. Enter a range between 0 and 1000000. The default value is 500000.

Adding additional disk space to the Experience Portal system

About this task

You can expand the amount of space in the root file system of Experience Portal. The root file system is where `/opt/Avaya` is installed which includes log partition.

You can enable additional disk space for the following:

- Systems deployed using one of the 8.x OVA's (Primary, Auxiliary, or MPP)
- Systems deployed from the 8.x AVL ISO using the fresh installation option

Note:

You cannot enable disk expansion on any system upgraded from Experience Portal 6.x or 7.x.

Use this procedure to expand the size of the root partition to add additional disk space to the Experience Portal system.

Procedure

1. Deploy Experience Portal OVA/AVL.

   For more details on deploying the Experience Portal virtual application, see the *Deploying Experience Portal in an Avaya Customer Experience Virtualized Environment* guide.

2. Power down the system.
3. Using a hypervisor tool (such as VMware), dynamically increase the size of the disk.

   Note:

   You can only increase the existing disk size, but not decrease the disk size.

   VMware does not allow the expansion of disk size when there are snapshots present.

4. Power on the system.
5. Log on to the Experience Portal server as a user with root privileges.
6. Run the **`df /`** command to check the partition size.

   If the disk is full, there may be system instability. You need to enable expansion before running out of space.

7. Run the **`/opt/Avaya/LinuxInstaller/bin/expand_root.sh`** command and monitor the messages the system displays on the screen.

   For example,

   ```
   [AEP ~]# /opt/Avaya/LinuxInstaller/bin/expand_root.sh
   ok to expand, let's keep processing...
   Let's expand the space by 640716802 sectors.
   Space expanded
   ```

   The `expand_root.sh` script verifies the ability for the disk to expand. If there are any reasons to prevent expansion, the system displays a message and exits.

   For example:

   - `Expand only supported when '/' is the last partition on the drive`
   - `Expand only supported for new builds, not updates from AAEP 7.x`
   - `Stop: the disk is fully utilized, nothing to do.`

8. Do the following to reboot the system to enforce the new drive size in all locations:

Note:

If EPM/MPP is not yet installed on the server, you can directly reboot the system.

a. Log into the Primary EPM web interface as a user with the Administration role.
b. If the MPP was expanded, do the following:
   - Click **System Management** > **MPP Manager**.
   - On the MPP Manager page, reboot the MPP server.
c. If the EPM was expanded, do the following:
   - Disable the EPM server.
     - If the EPM server contains an email processor, use the Email page to disable the EPM server.
     - If the EPM server contains an SMS processor, use the SMS page to disable the EPM server.
   - Click **System Management** > **EPM Manager**.
   - On the EPM Manager page, reboot the MPP server.

     Note:

     After rebooting the Primary EPM server, you need to log into the EPM web interface again.
   - Enable the EPM server.
     - If the EPM server contains an email processor, use the Email page to enable the EPM server.
     - If the EPM server contains an SMS processor, use the SMS page to enable the EPM server.

9. Log on to the Experience Portal server as a user with root privileges.
10. Run the `df /` command to check the partition size.

    You can view the system with the new increased disk size.

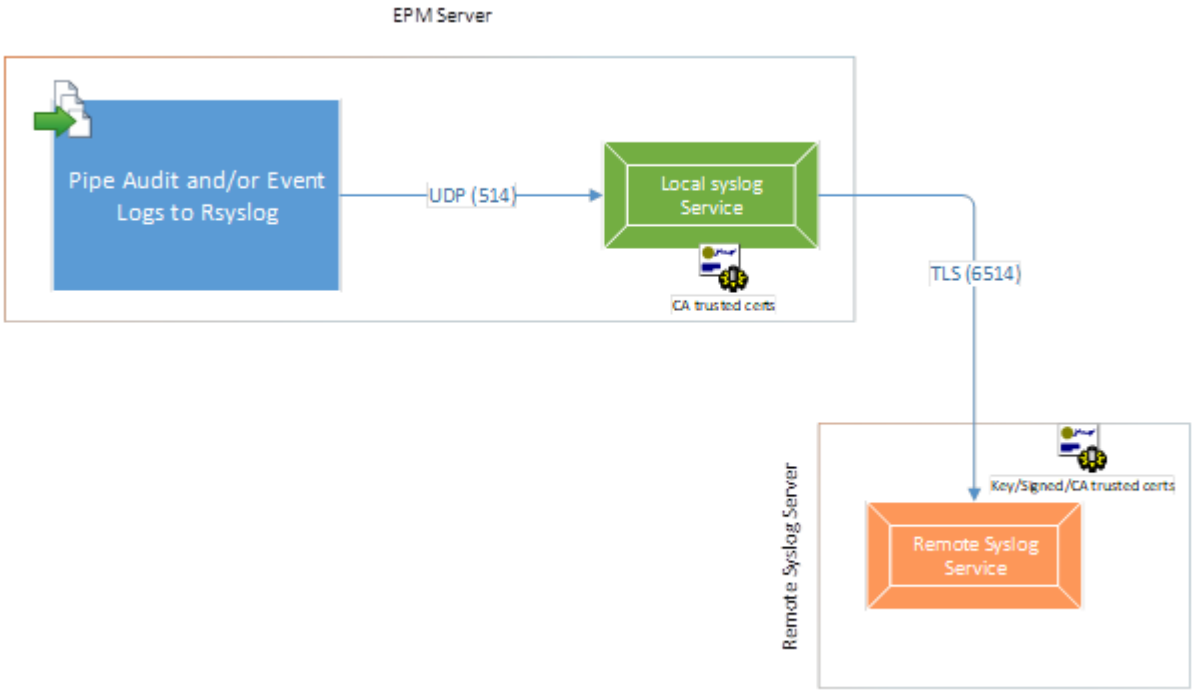
Syslog communication to external syslog servers

In Avaya Experience Portal 8.x, logs directed to external syslog servers are secured when leaving the Experience Portal system. The primary EPM sends audit logs, event logs, and alarms to a syslog server using secure connections.

The following diagram depicts the flow of logs from the Primary EPM to a remote syslog server.

- Primary EPM server forwards logs to a local syslog server over UDP and Port 514 (configurable) - This is internal to the Primary EPM server.

- Primary EPM syslog server then forwards the logs via TLS over port 6514 (configurable) to the external syslog server.



Configuring Primary EPM server to write to the local syslog server

About this task

When directing audit or event logs to a syslog server, instead of specifying an external syslog server in the EPM web interface, you can direct the logs to the Primary EPM local syslog server over any UDP port. The default syslog port is 514.

Procedure

1. Log on to the EPM web interface.
2. On the EPM navigation pane, click **System Configuration** > **EPM Servers**.
3. Click **Syslog Settings**.
4. In the Syslog Settings page, do the following to specify what logs are to be written to a syslog server:
   a. In the **Send Audit Logs to Syslog** field, select Yes.
   b. In the **Send Event Logs to Syslog** field, select Yes.
   c. In the **Syslog Server IP Address** field, enter the local IP address of the Primary EPM server.

d. In the **Syslog Server Port** field, enter the port number of the Primary EPM server.

   Ensure that the firewall policy allows the communication of this port.

   Make a note of the port as you have to manually configure this in the Primary EPM `syslog.conf` file so it can listen to the logs being sent to it.

5. Click **Apply** and **Save**.

Next steps

Configure the Primary EPM syslog server with a forwarding rule to divert securely to an external syslog server.

Configuring secure syslog communication on Primary EPM server

To secure syslog communication from the primary EPM, the primary EPM uses the local EPM Server syslog software, to establish a secure connection to an external syslog server. EPM communicates with the local syslog server, which in turn establishes a secure connection to an external syslog server.

The remote syslog server must be configured to do the following:

- Listen on port 6514 (Default syslog port for TLS communication).
- Forward logs to the external syslog server using TLS over 6514.
  - Firewall on the remote syslog server must allow communication on port 6514.
- Access the trusted Certificate Authority (CA) public certificate. This is used to configure security certificates on the remote syslog server on the EPM server to facilitate TLS handshaking.
  - Ensure that the PKI certificates are in place on the remote syslog server as per the syslog setup documentation.

Listening on UDP Port

About this task

When communicating to the local syslog server from Primary EPM, ensure that the Primary EPM is configured to listen on port 514 over UDP.

Procedure

1. Go to your Primary EPM Server.
2. Open the `vi /etc/rsyslog.conf` file.
3. Look for the following lines and ensure that they are not commented out:

   For RHEL 7:

   ```
   # Provides UDP syslog reception
   ```

```
$ModLoad imudp
$UDPServerRun 514
```

For RHEL 8:

```
# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")
```

Forwarding rule

About this task

After checking that the local syslog server is listening on port 514 and is receiving EPM log messages, the next step is to forward the logs to the external syslog server using TLS over 6514.

Procedure

1. Go to the Primary EPM Server.
2. Open the `vi /etc/rsyslog.conf` file.
3. At the end of the file, append the following line:

   `*. * @@XXX.XXX.XXX.XXXX:6514`

   Where,

   - `XXX.XXX.XXX.XXXX` is the IP address of the remote syslog server
   - `@@` Denotes TCP (Recommended)
   - `@` Denotes UDP

   If the remote log server is configured to listen only on TCP connections, or if you want to use a reliable transport network protocol such as TCP, add another `@` character before the remote host.

```
# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding rule. They
belong together, do NOT split them. If you create multiple forwarding rules,
duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is down,
messages are spooled to disk and sent when it is up again.
#$WorkDirectory /var/lib/rsyslog # where to place spool files
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
#*.* @10.129.187.100:514
*.* @@XXX.XXX.XXX.XXX:6514
# ### end of the forwarding rule ###
```

Accessing trusted certificates

About this task

The local syslog server needs to have access to the Certificate Authority (CA) trusted certificate used to generate the certificates for the remote syslog server.

Procedure

1. Go to your Primary EPM Server.
2. Open the `vi /etc/rsyslog.conf` file.
3. In the `rsyslog.conf` file, place the certificate in the default location as shown below:

   ```
   #### GLOBAL DIRECTIVES ####

   # certificate files

   $DefaultNetstreamDriver gtls

   $DefaultNetstreamDriverCAFile /etc/rsyslog-keys/ca.pem
   ```

   Where, `ca.pem` is the trusted certificate authority public certificate.

   Note:

   If the directory does not exist, you can create the directory and place the certificate in it.

Chapter 11: SNMP agents and traps

SNMP Agents and Traps

The Avaya Experience Portal Simple Network Management Protocol (SNMP) network includes agents, traps, and managers.

SNMP agents

You can configure Experience Portal to act as an *SNMP agent* so that a third party network management software can retrieve the Experience Portal system status.

An SNMP agent is a software module that resides on a device, or node, in an SNMP-managed network. The SNMP agent collects and stores management information and makes this information available to *SNMP managers*. SNMP agent communication can be:

- Solicited by an SNMP manager.
- Initiated by the SNMP agent if a significant event occurs. This type of communication is called an *SNMP trap*.

The commands and queries that the SNMP agent can use, along with information about the target objects that the SNMP agent can interact with using these commands and queries, is stored in a Management Information Base (MIB) that resides on the managed device.

SNMP traps

An SNMP trap is an unsolicited notification of a significant event from an SNMP agent to an SNMP manager. When an internal problem is detected, the SNMP agent immediately sends one of the traps defined in the MIB.

Important:

If you configure Experience Portal to send SNMP traps, you must configure the appropriate SNMP managers to receive those traps.

SNMP managers

SNMP managers collect information from SNMP agents. SNMP managers are usually used to display status information in a type of graphical user interface (GUI).

For Experience Portal, the SNMP manager can be an Avaya Services Security Gateway (SSG) or a Network Management System (NMS) station such as HP *OpenView* or IBM *Tivoli*. SNMP traps sent to the Avaya SSG contain specific information that generates Initialization and Administration System (INADS) notifications, which in turn generate customer trouble tickets.

Note:

You can only configure the Experience Portal SNMP agent and SNMP trap destinations if you are an administrator.

Configuring Avaya Experience Portal as an SNMP agent

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** > **SNMP**.
3. On the SNMP page, click **SNMP Agent Settings**.
4. On the SNMP Agent Settings page, enter appropriate information, and click **Save**.
5. **(Optional)** If you changed the port number, restart the SNMP Agent.

Viewing existing SNMP traps

Procedure

1. Log on to the EPM web interface by using an account with one of the following user roles:
   - Administration
   - Operations
   - Maintenance
2. On the EPM navigation pane, click **System Configuration** > **SNMP**.

   The EPM displays the SNMP page. On this page, authorized users can add, change, or delete SNMP trap destinations.

Adding an SNMP trap

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPMnavigation pane, click **System Configuration** > **SNMP**.
3. On the SNMP page, click **Add**.
4. On the Add SNMP Trap Configuration page, enter the appropriate information, and click **Save**.

Changing an SNMP trap

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** > **SNMP**.
3. On the SNMP page, in the **Host Address** column, click the SNMP Manager IP address or host name.
4. On the Change SNMP Trap Configuration page, enter appropriate information, and click **Save**.

Disabling SNMP traps

About this task

Use this procedure to disable SNMP traps.

You can disable an SNMP trap instead of deleting it, if you want a particular SNMP trap to stop sending SNMP notifications but want to save the configuration information for future reference.

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** > **SNMP**.
3. On the SNMP page, in the **Host Address** column, click the SNMP manager IP address or host name.
4. On the Change SNMP Trap Configuration page, in the **Enable** field, click **No**.
5. Click **Save**.

Testing SNMP traps

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** > **SNMP**.
3. On the SNMP page, click **Test**.

   Experience Portal sends a test message to each SNMP trap that is configured on the system.

Next steps

When you test the SNMP traps, Experience Portal automatically generates an alarm. You should retire this alarm as soon as possible so that it does not get confused with a real SNMP trap alarm.

Deleting SNMP traps

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** > **SNMP**.
3. On the SNMP page, do one of the following:
   - To delete individual SNMP traps: Select the check box for the SNMP trap destination that you want to delete.
   - To delete all SNMP trap destinations: Select the selection check box in the header row of the table, which automatically selects all rows in the SNMP traps table.
4. Click **Delete**.

Configuring IBM Tivoli or HP OpenView with Experience Portal

Procedure

For details about configuring Experience Portal with IBM's *Tivoli* or HP's *OpenView*, see the configuration files on the Experience Portal installation DVD. For:

- IBM Tivoli, see `Support/NMS-Configuration/IBM-Tivoli/ibm-config-steps.txt`
- HP OpenView, see `Support/NMS-Configuration/HP-Openview/hp-config-steps.txt`

SNMP page field descriptions

Use this page to view information about any SNMP trap configurations already administered on the Experience Portal system and to access the SNMP Agent settings. You can also use this page to add or change SNMP traps.

Column or Button	Description
Add	Opens the Add SNMP Trap Configuration page.

Table continues…

Column or Button	Description
Delete	Deletes the selected SNMP traps.
Test	Sends a test alarm notification to all servers so that you can verify the functionality of the traps.
SNMP Agent Settings	Opens the SNMP Agent Settings page.
SNMP Device Notification Settings	Opens the SNMP Device Notification Settings page where you can change how device notifications are sent.

Note:

The system displays the following columns only if you add an SNMP Trap.

Column or Button	Description
Selection check box	Indicates which SNMP traps you want to delete.
Host Address	The IP address or fully qualified domain name of the SNMP manager that receives the SNMP traps. To change settings for an SNMP trap configuration, click the name or address in this field. Experience Portal opens the Change SNMP Trap Configuration page.
Enable	Whether this SNMP trap is active.
Device	The options are: • **SSG/SAL**: Experience Portal sends SNMP traps to an Avaya Services Security Gateway (SSG)/Secure Access Link (SAL). **Note:** Experience Portal sends only Initialization and Administration System (INADS) traps to the SSG. • **NMS**: Experience Portal sends SNMP traps to a customer-provided Network Management System (NMS). **Note:** The Experience Portal system does not send INADS traps to the NMS.
Transport Protocol	The options are: • **UDP**: The transport protocol is set to User Datagram Protocol (UDP). • **TCP**: The transport protocol is set to Transmission Control Protocol (TCP).
Port	The port number the Experience Portal system uses to send SNMP traps.

Table continues…

Column or Button	Description
Type	The options are: • **Trap**: Experience Portal sends notifications with the SNMP `trap` command. • **Inform**: Experience Portal sends notifications with the SNMP `inform` command.
SNMP Version	The options are: • **1**: The SNMP agent uses SNMP Version 1 to send notifications. • **2c**: The SNMP agent uses SNMP Version 2c to send notifications. • **3**: The SNMP agent uses SNMP Version 3 to send notifications.
Security Name	The character string the Experience Portal SNMP agent uses as the identification name for the configuration.
Authentication Protocol	If the **SNMP Version** field is set to **3**, this can be: • **None**: The system performs no authentication and you cannot use an Authentication Password. If you select this option, you must also set the **Privacy Protocol** field to **None**. • **MD5**: Authentication is performed using the Message Digest 5 (MD5) protocol. This is the default. • **SHA**: Authentication is performed using the Secure Hash Algorithm (SHA) protocol.
Privacy Protocol	If the **SNMP Version** field is set to **3**, this can be: • **None**: The system performs no message encryption and you cannot set a Privacy Password. You must select this option if the **Authentication Protocol** field is set to **None**. • **DES**: The Data Encryption Standard (DES) protocol is used to encrypt SNMP Version 3 messages. • **AES128**: The Advanced Encryption Standard 128 (AES128) protocol is used to encrypt SNMP Version 3 messages. This is the default. • **AES192**: The Advanced Encryption Standard 192 (AES192) protocol is used to encrypt SNMP Version 3 messages. • **AES256**: The Advanced Encryption Standard 256 (AES256) protocol is used to encrypt SNMP Version 3 messages.

SNMP Agent Settings page field descriptions

Use this page to view or configure the SNMP agent settings for this Experience Portal system.

This page contains the:

SNMP Version 1 group

Field	Description
Enable SNMP Version 1	To configure the Experience Portal SNMP agent to receive and respond to SNMP Version 1 messages, select this check box.
Security Name	If you enabled version 1 messages, enter an alphanumeric name for the Experience Portal SNMP agent in this field. The agent only accepts message strings that include this name. You cannot leave this field blank or use the strings "public" or "private".

SNMP Version 2c group

Field	Description
Enable SNMP Version 2c	To configure the Experience Portal SNMP agent to receive and respond to SNMP Version 2c messages, select this check box.
Security Name	If you enabled version 2c messages, enter an alphanumeric name for the Experience Portal SNMP agent in this field. The agent only accepts message strings that include this name. You cannot leave this field blank or use the strings "public" or "private".

SNMP Version 3 group

Field	Description
Enable SNMP Version 3	To configure the Experience Portal SNMP agent to receive and respond to SNMP Version 3 messages, select this check box.
Security Name	If you enabled version 3 messages, enter an alphanumeric name for the Experience Portal SNMP agent in the **Security Name** field. The agent only accepts message strings that include this name. You cannot leave this field blank or use the strings "public" or "private".

Table continues…

Field	Description
Authentication Protocol	If the **SNMP Version** field is set to 3, select one of the following options as the **Authentication Protocol**. The options are: • **None**: The system does not perform any authentication and you cannot use an Authentication Password. If you select this option, you must also set the **Privacy Protocol** field to **None**. • **MD5**: The system performs an authentication using the Message Digest 5 (MD5) protocol. • **SHA**: The system performs an authentication using the Secure Hash Algorithm (SHA) protocol. The default option is **MD5**. **Note:** If the **Authentication Protocol** is set to **None**, the **Privacy Protocol** must also be set to **None**.
Authentication Password	Enter a character string to be used as the authentication password for SNMP Version 3 messages. This password must contain at least 8 characters. If the **Authentication Protocol** field is set to **None**, the **Authentication Password** field is not used and cannot be set.
Privacy Protocol	If the **SNMP Version** field is set to 3, select one of the following options as the **Privacy Protocol**: The options are: • **None**: The system does not perform any message encryption and you cannot set a Privacy Password. You must select this option if the **Authentication Protocol** field is set to **None**. • **DES**: The Data Encryption Standard (DES) protocol is used to encrypt SNMP Version 3 messages. • **AES128**: The Advanced Encryption Standard 128 (AES128) protocol is used to encrypt SNMP Version 3 messages. • **AES192**: The Advanced Encryption Standard 192 (AES192) protocol is used to encrypt SNMP Version 3 messages. • **AES256**: The Advanced Encryption Standard 256 (AES256) protocol is used to encrypt SNMP Version 3 messages. The default option is **AES128**. **Note:** If the **Authentication Protocol** is set to **None**, the **Privacy Protocol** must also be set to **None**.

Table continues…

Field	Description
Privacy Password	Enter a character string to be used as the privacy password for SNMP Version 3 messages. This password must contain at least 8 characters. If the **Privacy Protocol** field is set to **None**, the **Privacy Password** field is not used and cannot be set.

Authorized for SNMP Access group

Field	Description
Allow All IP Addresses	Allows any SNMP manager access to the Experience Portal SNMP agent. This is the default.
Allow Only the Following	Allows up to five specified SNMP managers access to the Experience Portal SNMP agent. If you select this field, specify one or more SNMP managers in the **IP Address/ Hostname** fields.

Transport Protocol group

The only currently supported transportation protocol is the User Datagram Protocol (UDP).

Port Number group

Field	Description
Default Port Number	Specifies that the Experience Portal SNMP agent communicates with SNMP managers using the default port number for UDP, which is 161.
Custom Port Number	Specifies that the Experience Portal SNMP agent communicates with SNMP managers using a non-default port number. If you select this option, enter a port number from 0 to 65535 in the associated text field.

Add SNMP Trap Configuration page field descriptions

Use this page to add a new Simple Network Management Protocol (SNMP) trap.

Column	Description
Enable	Whether this SNMP trap is active. The default is **Yes**, which means the trap is active.

Table continues…

Column	Description
Device	The options are: • **SSG/SAL**: Experience Portal sends SNMP traps to an Avaya Services Security Gateway (SSG)/Secure Access Link (SAL). **Note:** Experience Portal sends only Initialization and Administration System (INADS) traps to the SSG. • **NMS**: Experience Portal sends SNMP traps to a customer-provided Network Management System (NMS). **Note:** The Experience Portal system does not send INADS traps to the NMS. The default is **SSG/SAL**.
Transport Protocol	The options are: • **UDP**: The transport protocol is set to User Datagram Protocol (UDP). • **TCP**: The transport protocol is set to Transmission Control Protocol (TCP). The default is **UDP**.
Host Address	The IP address or fully qualified domain name of the SNMP manager that receives the SNMP traps.
Port	The port number the Experience Portal system uses to send SNMP traps. The default is 162.
Type	The options are: • **Trap**: Experience Portal sends notifications with the SNMP `trap` command. The receiver does not verify that the command was received. This notification type can be used with all versions of SNMP. • **Inform**: Experience Portal sends notifications with the SNMP `inform` command. This option can be used only with SNMP versions 2c and 3. When an SNMP manager receives an SNMP message with the `inform` command, the SNMP manager sends a response back to the SNMP agent indicating that it received the notification. The default is **Trap**.
SNMP Version	The options are: • **1**: The SNMP agent uses SNMP Version 1 to send notifications. • **2c**: The SNMP agent uses SNMP Version 2c to send notifications. • **3**: The SNMP agent uses SNMP Version 3 to send notifications. The default is **3**.

Table continues…

Column	Description
Security Name	The character string the Experience Portal SNMP agent uses as the identification name for the configuration. For devices configured to use SNMP Version 1 or 2c, this string is used as the `Community Name`. For devices configured to use SNMP Version 3, this string is used as the `Security Name`. You cannot leave this field blank or use the strings `public` or `private`.
Authentication Protocol	If the **SNMP Version** field is set to **3**, this can be: • **None**: The system performs no authentication and you cannot use an Authentication Password. If you select this option, you must also set the **Privacy Protocol** field to **None**. • **MD5**: Authentication is performed using the Message Digest 5 (MD5) protocol. This is the default. • **SHA**: Authentication is performed using the Secure Hash Algorithm (SHA) protocol.
Authentication Password	If the **Authentication Protocol** field is set to something other than **None**, the password that the system uses to authenticate SNMP Version 3 messages. The password must contain at least 8 characters.
Privacy Protocol	If the **SNMP Version** field is set to **3**, this can be: • **None**: The system performs no message encryption and you cannot set a Privacy Password. You must select this option if the **Authentication Protocol** field is set to **None**. • **DES**: The Data Encryption Standard (DES) protocol is used to encrypt SNMP Version 3 messages. • **AES128**: The Advanced Encryption Standard 128 (AES128) protocol is used to encrypt SNMP Version 3 messages. This is the default. • **AES192**: The Advanced Encryption Standard 192 (AES192) protocol is used to encrypt SNMP Version 3 messages. • **AES256**: The Advanced Encryption Standard 256 (AES256) protocol is used to encrypt SNMP Version 3 messages. **Note:** For the **AES192** or **AES256** options, the system must be configured for a high encryption level. These options are not enabled during a standard OS installation and are controlled under U.S. federal export laws. The default is **AES128**.
Privacy Password	If the **Privacy Protocol** field is set to something other than **None**, the password that the system is to use for encrypted SNMP Version 3 messages. The password must contain at least 8 characters.

Change SNMP Trap Configuration page field descriptions

Use this page to change an existing Simple Network Management Protocol (SNMP) trap.

Column	Description
Enable	Whether this SNMP trap is active. The default is **Yes**, which means the trap is active.
Device	The options are: • **SSG/SAL**: Experience Portal sends SNMP traps to an Avaya Services Security Gateway (SSG)/Secure Access Link (SAL). **Note:** Experience Portal sends only Initialization and Administration System (INADS) traps to the SSG. • **NMS**: Experience Portal sends SNMP traps to a customer-provided Network Management System (NMS). **Note:** The Experience Portal system does not send INADS traps to the NMS. The default is **SSG/SAL**.
Transport Protocol	The options are: • **UDP**: The transport protocol is set to User Datagram Protocol (UDP). • **TCP**: The transport protocol is set to Transmission Control Protocol (TCP). The default is **UDP**.
Host Address	The IP address or fully qualified domain name of the SNMP manager that receives the SNMP traps.
Port	The port number the Experience Portal system uses to send SNMP traps. The default is 162.
Type	The options are: • **Trap**: Experience Portal sends notifications with the SNMP `trap` command. The receiver does not verify that the command was received. This notification type can be used with all versions of SNMP. • **Inform**: Experience Portal sends notifications with the SNMP `inform` command. This option can be used only with SNMP versions 2c and 3. When an SNMP manager receives an SNMP message with the `inform` command, the SNMP manager sends a response back to the SNMP agent indicating that it received the notification. The default is **Trap**.

Table continues…

Column	Description
SNMP Version	The options are: • **1**: The SNMP agent uses SNMP Version 1 to send notifications. • **2c**: The SNMP agent uses SNMP Version 2c to send notifications. • **3**: The SNMP agent uses SNMP Version 3 to send notifications. The default is **3**.
Security Name	The character string the Experience Portal SNMP agent uses as the identification name for the configuration. For devices configured to use SNMP Version 1 or 2c, this string is used as the `Community Name`. For devices configured to use SNMP Version 3, this string is used as the `Security Name`. You cannot leave this field blank or use the strings `public` or `private`.
Authentication Protocol	If the **SNMP Version** field is set to **3**, this can be: • **None**: The system performs no authentication and you cannot use an Authentication Password. If you select this option, you must also set the **Privacy Protocol** field to **None**. • **MD5**: Authentication is performed using the Message Digest 5 (MD5) protocol. This is the default. • **SHA**: Authentication is performed using the Secure Hash Algorithm (SHA) protocol.
Authentication Password	If the **Authentication Protocol** field is set to something other than **None**, the password that the system uses to authenticate SNMP Version 3 messages. The password must contain at least 8 characters.

Table continues…

Column	Description
Privacy Protocol	If the **SNMP Version** field is set to **3**, this can be: • **None**: The system performs no message encryption and you cannot set a Privacy Password. You must select this option if the **Authentication Protocol** field is set to **None**. • **DES**: The Data Encryption Standard (DES) protocol is used to encrypt SNMP Version 3 messages. • **AES128**: The Advanced Encryption Standard 128 (AES128) protocol is used to encrypt SNMP Version 3 messages. This is the default. • **AES192**: The Advanced Encryption Standard 192 (AES192) protocol is used to encrypt SNMP Version 3 messages. • **AES256**: The Advanced Encryption Standard 256 (AES256) protocol is used to encrypt SNMP Version 3 messages. **Note:** For the **AES192** or **AES256** options, the system must be configured for a high encryption level. These options are not enabled during a standard OS installation and are controlled under U.S. federal export laws. The default is **AES128**.
Privacy Password	If the **Privacy Protocol** field is set to something other than **None**, the password that the system is to use for encrypted SNMP Version 3 messages. The password must contain at least 8 characters.

View SNMP Device Notification Settings page field descriptions

Use this page to view how SNMP notifications are sent on the Avaya Experience Portal system

This page contains the following groups:

- NMS group on page 265
- SSG/SAL group on page 265
- Last Time All Alarms Retired group on page 266

NMS group

Section or Field	Description
Notification options	The SNMP notifications that Avaya Experience Portal sends to the Network Management System (NMS) . The options are: • **All Minor, Major, and Critical notifications will be sent.** • **First Minor will be sent. All Major and Critical notifications will be sent.** • **First Minor and Major will be sent. All Critical notifications will be sent.** • **First Minor, Major, and Critical notifications will be sent.**
Highest severity notification sent	If any option except **All Minor, Major, and Critical notifications will be sent.** is selected in the Notification options section, this field displays: • " " (blank) if no notification has been sent since the last time the old alarms were retired. • The highest notification that has been sent to this system since the last time the status of all alarms was set to Retired. No more notifications below this level will be sent to the NMS until the status of all current alarms has been set to Retired.

SSG/SAL group

Section or Field	Description
Notification options	The SNMP notifications that Avaya Experience Portal sends to the Service Selection Gateway (SSG). The options are: • **All Minor, Major, and Critical notifications will be sent.** • **First Minor will be sent. All Major and Critical notifications will be sent.** • **First Minor and Major will be sent. All Critical notifications will be sent.** • **First Minor, Major, and Critical notifications will be sent.**
Highest severity notification sent	If any option except **All Minor, Major, and Critical notifications will be sent.** is selected in the Notification options section, this field displays: • " " (blank) if no notification has been sent since the last time the old alarms were retired. • The highest notification that has been sent to this system since the last time the status of all alarms was set to Retired. No more notifications below this level will be sent to the SSG until the status of all current alarms has been set to Retired.

Last Time All Alarms Retired group

Displays the last time that the status of all alarms was set to Retired, thereby resetting the notification triggers.

Chapter 12: Media Processing Platforms

Media Processing Platform server overview

A Media Processing Platform (MPP) server is a server machine running the Avaya Experience Portal MPP software.

The MPP software:

- Runs on Avaya Enterprise Linux or Red Hat Enterprise Linux.
- Uses Voice over IP (VoIP) protocols to communicate with the telephone network.
- Uses the Media Resource Control Protocol (MRCP) protocol to communicate with the speech servers.
- Runs Voice eXtensible Markup Language (VoiceXML) speech applications deployed on the application server.
- Runs Call Control eXtensible Markup Language (CCXML) applications

Note:

Experience Portal uses the Oktopous™ ccXML Interpreter.

Multiple MPP servers

When a system is configured with multiple MPP servers:

- An individual MPP server is not aware of any other MPP servers in the system, nor can it communicate directly with them.
- The Experience Portal Manager (EPM) web interface allows administrators to control any MPP server in the system.

Data storage

The Experience Portal system is designed so that all persistent data is stored on the primary EPM server. For example, all configuration information is stored on the primary EPM server and downloaded to the MPP when required.

Any persistent data created on the MPP server is uploaded to the EPM either on-demand or through scheduled jobs. For example:

- The EPM regularly polls the MPP server's status.
- Event and alarm data is delivered to the EPM on demand.
- Report data, including Contact Detail Records (CDRs) and Session Detail Records (SDRs), are delivered to the EPM according to a schedule that you administer.

The MPP has additional data that can be used for debugging, but is not required to be persistent. For example:

- Trace data and MPP-specific log files.
- Session transcriptions and utterances.

MPP server components

The MPP server consists of the following components:

- System Manager
- Web services
- Session Manager
- Avaya Voice Browser
- CCXML Browser
- Speech proxies
- Telephony
- Event Manager

System Manager component

The System Manager component works in conjunction with the EPM to keep the MPP functioning in an optimal state. In addition, System Manager provides the following functions:

Function	Description
State management	Starts and stops all processes in response to start or stop commands from the EPM. Monitors the health of the processes and attempts to restart any processes that exit prematurely, appear deadlocked, have stopped responding.
Configuration management	The EPM downloads configuration information to the MPP during startup. Configuration updates can also be downloaded to the MPP while it is running. The System Manager transfers the information to the other MPP components of the change, if needed.
License management	The EPM manages port licensing for each MPP and passes that information during MPP startup and later if licenses need to be redistributed. The EPM downloads all licensing changes to the MPP.
Resources monitor	The EPM monitors CPU usage, memory usage, and disk usage for each MPP. The EPM checks the state of these resources at predetermined intervals during EPM polling operations. If at any time the use of these resources crosses thresholds set on the EPM, Resource monitor issues an alert. The System Manager also monitors for network errors between the MPP and the EPM.

The Web services component

The EPM accesses the web services of the MPP to monitor and control the MPP. The Apache Web server implements the web services and ensures that communication between the EPM and the web services is secure. The MPP web services are:

Service name	Description
Call Data Handler (CDH) service	The EPM uses the CDH service to transfer Application Detail Records (ADRs), Contact Detail Records (CDRs), and Session Detail Records (SDRs) from the MPP. The EPM stores the record data in the Experience Portal database and uses this information to generate the call and session reports.
MPP Management Service (MMS)	The EPM uses the MMS to send heartbeat requests, configuration changes, and commands. The MMS then forwards these requests to the System Manager for execution.
Application Interface web service	Also known as the “Outcall web service”, using this Web services the developers can: • Start a CCXML or VoiceXML application that has been added to Experience Portal. • Send an event to a specific application session running on an MPP. • Query the system for the total number of: - Used and unused outbound resources available - Unused SIP outbound resources - Unused H.323 outbound resources • Send an SMS or Email message using Experience Portal resources. • Start an SMS or Email application that has been added to Experience Portal.
TransService	This process uploads any transcription data to the Experience Portal database.

The Session Manager component

A *session* covers the time between the start of the inbound or outbound call and the completion of that call.

When the MPP initiates a call or is assigned a call, the Session Manager:

1. Starts a new session.
2. Assigns the session a unique ID.
3. Associates the call with the appropriate Call Control eXtensible Markup Language (CCXML) or Voice eXtensible Markup Language (VoiceXML) application.

4. Depending on the MPP settings, the administrator selects for the MPP, records all or some of the following data during the session:
   - Contact Detail Records (CDRs)
   - Application Detail Records (ADRs)
   - Session transcriptions
   - Performance trace information

The MPP Session Manager also coordinates all interactions between the MPP and:

- Any Automatic Speech Recognition (ASR) servers
- Any Text-to-Speech (TTS) servers
- Any telephony components
- The Avaya Voice Browser
- The CCXML Browser

The Avaya Voice Browser component

The Avaya Voice Browser is a Voice eXtensible Markup Language (VoiceXML) interpreter that communicates with the application servers to interpret the VoiceXML documents of a speech application.

For each incoming call:

1. Session Manager starts a new Avaya Voice Browser session and passes the Universal Resource Indicator (URI) of the VoiceXML application to the new session.
2. The Avaya Voice Browser contacts the application server and waits for the VoiceXML page to be returned.
3. After the application starts, the Avaya Voice Browser is responsible for:
   - Interpreting the VoiceXML page returned by the application server.
   - Managing the user interaction including playing prompts and interpreting input from the caller through Dual-tone multi-frequency (DTMF) or Automatic Speech Recognition (ASR).

The CCXML Browser component

The CCXML Browser component is responsible for providing low level call control support including the setup, monitoring, and tear-down of telephone calls.

For VoiceXML applications, Experience Portal includes a default CCXML application that provides the basic call control functionality. If you want to use advanced features such as call merging and all conferencing, you need to create a custom CCXML application.

Speech proxy component

The MPP speech proxy component integrates third-party media resources, such as Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) speech servers, into the Experience Portal system by employing Media Resource Control Protocol (MRCP).

When a speech application requests ASR or TTS resources, the speech proxy component communicates with the speech servers and selects the appropriate server to provide those resources. The MRCP proxy reports the state of the speech servers to the MPP System Manager.

If directed by the EPM, the speech proxy component can also add or remove communication ports between an MPP and any speech server in the system.

The Telephony component

The MPP Telephony component provides all telephony services required by the Experience Portal system, including call control and media processing.

The telephony subsystem can be connected to:

- Direct connection to Communication Manager, a VoIP-based PBX gateway, using either the International Standard for Multimedia Communication Over Packet-switched Networks (H.323) or Session Initiation Protocol (SIP) for signaling and Real-time Transport Protocol (RTP) to transport the actual audio data stream in a connection.
- Proxied SIP connection through Avaya Aura Session Manager to Communication Manager, Communication Server 1000, the Avaya G860 Media Gateway or Third-party SIP gateways.

Setting the global grace period and trace level parameters

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. To set the global grace period, do the following:
    a. On the EPM navigation pane, click **System Configuration** > **EPM Servers**.
    b. On the EPM Servers page, click **EPM Settings**.
    c. On the EPM Settings page, in the Miscellaneous section, do the following:
        - In the **Operational Grace Period (minutes)** field, enter the number of minutes Experience Portal waits for the processing to complete before it terminates all the remaining Experience Portal activities and begins changing the following states of the Primary EPM, Auxiliary EPM, and MPP:
            - Halting

- Rebooting
- Restarting
- Stopping

- In the **Event Level Threshold to Send to EPM** drop-down list, select the lowest level of events to be included in the performance tracing log that is sent to the EPM.

3. To set the trace level parameters, do the following:
   a. On the EPM navigation pane, click **System Configuration** > **MPP Servers**.
   b. On the MPP Servers page, click **MPP Settings**.
   c. On the MPP Settings page, click the Categories and Trace Levels section header to view the complete table of options.
   d. Click the performance trace level you want to use as the default for each component.

      The options are:

      - **Off**
      - **Fine**
      - **Finer**
      - **Finest**

      Important:

      Performance tracing is a valuable troubleshooting tool, but it can adversely impact Experience Portal system performance if you set the trace level for all categories to **Finest** on a busy production system. If you need to troubleshoot a particular area, you must set specific categories to **Fine** and examine the resulting output to see if you can locate the issue. If not, set the level to **Finer** and repeat the process. If you still need more data, then set the level to **Finest** and keep a close watch on system resource usage.

Viewing all MPP servers

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. To view the current status of all MPP servers and to get detailed information about any alarms they have generated, click **Real-time Monitoring** > **System Monitor**and go to the <System name> Details tab.

   The information on this page refreshes automatically if you leave the browser window open.

3. To view the MPP configuration, click **System Configuration** > **MPP Servers** to access the MPP Servers page.

   In general, the MPP servers shown on these pages should be identical. Occasionally, however, there may be more MPP servers on the <System name> Details tab on the System Monitor page. For example, when an administrator deletes an MPP server, Experience Portal immediately removes it from the MPP Servers but leaves it on the <System name> Details tab until the ports allocated to the MPP server can be reassigned.

Viewing details for a specific MPP

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **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. If you want to view the configuration history of the MPP, on the <MPP name> Details page, click the **History** link next to the **Configuration** group.

   Note:

   If you are logged in with the Administration user role, you can access the Media Server Service Menu for the MPP by clicking the **Service Menu** link in the **Miscellaneous** group.

Adding an MPP

Procedure

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

   If Avaya Services is maintaining this system, and you are an Avaya Services representative, log on to EPM by using the init EPM account that is created during the EPM software installation.
2. On the EPM navigation pane, click **System Configuration** > **MPP Servers**.
3. On the Add MPP Server page, click **Add**.
4. On the first Add MPP Server page, enter the appropriate information and click **Continue**.
5. On the second Add MPP Server page, enter the appropriate information and click **Save**.

If you logged in using the init account, ensure that you enter the appropriate LDN number for the server in the **LDN** field. If you do not specify an LDN number, Experience Portal uses the default value (000)000-0000.

Note:

Ensure that you verify the displayed security certificate by clicking the **MPP Certificate** section, and then checking the **Trust new certificate** check box. You cannot save the MPP unless you select this check box.

Changing an MPP

About this task

You can change all MPP options except the name of the MPP.

Procedure

1. Log on to the EPM web interface.

   If Avaya Services is maintaining this system and you are an Avaya Services representative, log on to EPM by using the init EPM account that is created during the EPM software installation.

   Otherwise, log on to EPM by using an account with the Administrator user role.
2. On the EPM navigation pane, click **System Configuration** > **MPP Servers**.
3. On the MPP Servers page, in the **Name** column, click the name of the MPP you want to reconfigure.
4. On the Change MPP Server page, enter appropriate information, and click **Save**.

   If you logged in using the init account, ensure that the LDN number specified in the **LDN** field matches the information in the Avaya Services database for this server.

MPP server capacity

The number of telephony ports and the maximum number of simultaneous calls that an MPP server can handle depend on many factors, including the hardware characteristics of the MPP server and the complexity of the applications that the Avaya Experience Portal system is running. 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.

When configuring your Avaya Experience Portal system, make sure that you have enough MPP servers to handle the telephony ports that you purchase. Ideally, you should have enough reserve

capacity so that when one MPP server goes out of service, all of your telephony ports can be handled by the remaining MPP servers. You must have enough MPP servers so that the sum of the maximum simultaneous calls is larger than the number of configured ports.

For example, if your Avaya Experience Portal system needs to handle 400 simultaneous calls, you must purchase 400 telephony port licenses and configure a sufficient number of MPP servers to run that many simultaneous calls.

If your Avaya Services representative or Avaya Business Partner determines that each one of your MPP servers can handle a maximum of 100 simultaneous calls, you could configure:

- 4 MPP servers, each with the **Maximum Simultaneous Calls** parameter set to 100. When Avaya Experience Portal initializes, it distributes the 400 available telephony ports across the 4 servers so that each server is running at the maximum capacity of 100 calls each and the entire system can process 400 simultaneous calls. In this configuration there is no failover capability. If an MPP goes out of service, Avaya Experience Portal cannot reassign the ports because the other 3 servers are already running 100 simultaneous calls. This means that the total number of simultaneous calls the system can handle drops to 300.
- 5 MPP servers, each with the **Maximum Simultaneous Calls** parameter set to 100. When Avaya Experience Portal initializes, it distributes the 400 available telephony ports across the 5 servers so that each server is assigned 80 telephony ports and the entire system can process 400 simultaneous calls. In this configuration, if an MPP goes out of service, Avaya Experience Portal can reassign the 80 ports to the other 4 servers, bringing those 4 servers up to their maximum capacity of 100 ports. The entire system remains capable of processing 400 simultaneous calls.

For more information about capacity and scalability specification, see *Avaya Experience Portal Overview and Specification.*

MPP operational modes

Mode	Description
Offline	The MPP is unavailable to handle customer calls or test calls. It is not currently being polled, but its last known status is displayed on the MPP Manager page. The MPP will *not* respond to state change commands issued through the EPM, but you can change the mode to Online or Test.
Online	The MPP is available to handle customer calls. It is being polled, and its updated status is displayed on the MPP Manager page. The MPP will respond to state change commands issued through the EPM.
Test	The MPP is *not* available to handle customer calls but is available to handle test calls made using an H.323 connection that has at least one maintenance station defined. If your site does not have any configured H.323 connections or defined maintenance stations, then an MPP in Test mode will not respond to any VoIP requests. The MPP will respond to state change commands issued through the EPM.

Changing the operational mode of an MPP

Procedure

1. Log on to the EPM web interface by using an account with the Administration or Operations user role.
2. On the EPM navigation pane, click **System Management** > **MPP Manager**.
3. On the MPP Manager page, in the MPP server table, select the check box for the MPP that you want to change.
4. In the **Mode Commands** group, click one of the following desired operational state buttons:
   - **Offline** if the MPP server is currently in Online or Test mode.
   - **Test** if the MPP server is currently in Offline or Online mode.
   - **Online** if the MPP server is currently in Offline or Test mode.
5. After you finish setting the operational mode, click **Refresh** to ensure the mode is now what you selected.

MPP operational states

State	Description
Booting	The MPP is in the process of restarting and is not yet ready to take new calls. It is not responding to heartbeats and last MPP state was Rebooting. If the MPP remains in this state for more than 10 minutes, the state changes to Not Responding.
Degraded	The MPP is running but it is not functioning at full capacity. This usually means that: • Some of the H.323 or SIP telephony resources assigned to the MPP are not registered with the switch. For more information on viewing telephony port distribution, see *Administering Avaya Experience Portal*. • Enough ports have gone out of service to trigger a fatal alarm. The percentage of out of service ports that trigger such an alarm is specified in the **Out of Service Threshold** group on the VoIP Settings page. • A critical process has stopped on the MPP server. If an MPP has issued a fatal event and remains in that state for three minutes, Experience Portal automatically restarts the MPP in an attempt to fix the problem. If the problem persists after the restart, Experience Portal tries to restart the MPP up to two more times. If after three restarts the MPP is still encountering fatal errors, the state changes to Error.

Table continues…

State	Description
Error	The MPP has encountered a severe problem and cannot recover.
Halted	The MPP is no longer responding to heartbeats because it received a **Halt** command. The MPP cannot be restarted until its server machine has been manually restarted.
Halting	The MPP is responding to heartbeats but is not taking new calls. Experience Portal shuts down the corresponding server machine after all calls in progress are completed or the grace period ends, whichever comes first. Once an MPP has halted, you must manually turn on the corresponding server machine before the MPP can be restarted.
Never Used	The MPP has never successfully responded to a heartbeat request. New MPPs start to receive heartbeat requests during the next polling interval after they have been configured. This state occurs when an MPP has either not yet been sent a heartbeat request after it was added or the MPP did not respond to the heartbeat request.
Not Responding	The MPP is not responding to heartbeat requests and it has not received a **Restart** or **Halt** command. You should manually check the MPP server machine.
Rebooting	The MPP is responding to heartbeats but is not taking new calls. Experience Portal reboots the corresponding server machine after all calls in progress are completed or the grace period ends, whichever comes first.
Recovering	The MPP has encountered a problem and is attempting to recover.
Restart Needed	This state is most often reached when the MPP has encountered a problem that it cannot recover from and it requires a manual restart. However, it may also appear for an MPP when the EPM software has been upgraded and the MPP software has not. In that case, the state should update automatically when you upgrade the MPP software.
Running	The MPP is responding to heartbeat requests and is accepting new calls.
Starting	The MPP is responding to heartbeats but not taking new calls because it is transitioning from the Stopped state to the Running state.
Stopped	The MPP is responding to heartbeats but is not taking new calls. The MPP enters this state while it initializes after it restarts or when a **Stop** command is received. Experience Portal will restart the MPP automatically if the MPP: • Stopped unexpectedly and the **Auto Restart** option is selected for that MPP. In this case, Experience Portal restarts the MPP immediately. • Has a specified restart schedule. In this case, Experience Portal restarts the MPP when the scheduled restart time arrives whether the MPP stopped because of an explicit **Stop** command or because the MPP encountered a problem and was not configured to restart automatically.
Stopping	The MPP is responding to heartbeats but is not taking new calls. Experience Portal stops the corresponding server machine after all calls in progress are completed or the grace period ends, whichever comes first.

Checking the operational state for one or more MPPs

Procedure

1. Log on to the EPM web interface by using an account with the Administration or Operations user role.
2. On the EPM navigation pane, click **System Management** > **MPP Manager**.
3. On the MPP Manager page, see the **State** column for the MPPs whose state you want to check.

   The options are:

   - **Booting**: The Media Server is in the process of restarting and is not yet ready to take new calls.
   - **Degraded**: The Media Server is running but it is not functioning at full capacity.
   - **Error**: The Media Server has encountered a severe problem and cannot recover.
   - **Halted**: The Media Server is no longer responding to heartbeats because it received a **`Halt`** command.
   - **Halting**: The Media Server is responding to heartbeats but is not taking new calls.
   - **Need Configuration**: An Email or SMS processor residing on the Media Server has not yet been configured.
   - **Need Connections**: No connections (SMPP or HTTP) have been configured or assigned to an Email/SMS processor residing on the Media Server.
   - **Never Used**: The Media Server has never successfully responded to a heartbeat request.
   - **Not Installed**: The Media Server is missing files required for heartbeat requests to occur.
   - **Not Responding**: The Media Server is not responding to heartbeat requests and it has not received a **`Restart`** or **`Halt`** command.
   - **Partially Running**: (EPM only) The Media Server is in the process of starting up, and not all individual components of the service, for example: Tomcat, SL, ActiveMQ, have come up yet.
   - **Rebooting**: The Media Server is responding to heartbeats but is not taking new calls.
   - **Recovering**: The Media Server has encountered a problem and is attempting to recover.
   - **Restart Needed**: This state is most often reached when the Media Server has encountered a problem that it cannot recover from and it requires a manual restart. However, it can also appear for an MPP when the EPM software has been upgraded and the MPP software has not. In that case, the state should update automatically when you upgrade the MPP software.

- **Running**: The Media Server is responding to heartbeat requests and is accepting new calls.
- **Starting**: The Media Server is responding to heartbeats but not taking new calls because it is transitioning from the Stopped state to the Running state.
- **Stopped**: The Media Server is responding to heartbeats but is not taking new calls. The Media Server enters this state while it initializes after it restarts or when a **Stop** command is received.
- **Stopping**: The Media Server is responding to heartbeats but is not taking new calls.
- **Unknown**: The Media Server is in the Offline mode.

Changing the operational state for one or more MPPs

Procedure

1. Log on to the EPM web interface by using an account with the Administration or Operations user role.
2. On the EPM navigation pane, click **System Management** > **MPP Manager**.
3. On the MPP Manager page, in the MPP server table, select the check box for the MPP server that you want to change.
4. If you selected multiple servers, in the **Restart/Reboot Options** group, select one of the following options to either restart or reboot the servers:
   - **One server at a time**
   - **All servers**
5. In the **State Commands** group, click the desired operational state button and confirm your selection when prompted.

   The options are:
   - Start
   - Stop
   - Restart
   - Reboot
   - Halt
   - Cancel
6. Click **Refresh** to ensure that the operational state is what you selected.

   Tip:

   You can also verify the change in state by clicking **Real-time Monitoring** > **System Monitor** and going to the <System name> Details tab. The information on this page refreshes automatically if you leave the browser window open.

Setting the license reallocation time

About this task

When you stop or restart an MPP, the EPM waits for the specified license reallocation time before taking the telephony ports away from that MPP and redistributing them to the other MPPs in the Experience Portal system. The reallocation time needs to be longer than the MPP grace period so that the MPP has time to finish any active calls, stop, and then restart.

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPMnavigation pane, click **System Configuration** > **EPM Servers**.
3. On the EPM Servers page, click **EPM Settings**.
4. On the EPM Settings page, go to the **Miscellaneous** group.
5. In the **License Re-allocation Wait Time** field, enter the number of minutes that the EPM has to wait.
6. Click **Save**.

MPP processes

The following table provides an overview of the processes that run on the MPP.

Process Name	Descriptive Name	Notes
`ccxml`	CCXML Interpreter	Controls all call handling behavior for each VoiceXML application that runs on the MPP. CCXML Interpreter also controls each request to obtain or release a telephony resource for a given VoiceXML application.
`CdhService`	Call Data Handler (CDH)	A web service that runs when the EPM is downloading Contact Detail Records (CDRs) and Session Detail Records (SDRs).
`EventMgr`	Event Manager	Collects events from other MPP processes and sends them to the network log web service on the EPM.
`httpd`	Apache Web Server	Enables the other web services running on the MPP. The first Apache Web Server process started by the daemon runs as root. The root process starts nine other processes that run as the `avayavp` user in the avayavpgroup group.
`MmsServer`	MPP Management Service (MMS)	With a Web service interface, the EPM server sends commands to the MPP server. MMS runs only when the EPM is polling or sending commands to the MPP.

Table continues…

Process Name	Descriptive Name	Notes
mppmaint	MPP Maintenance Utility	The cron process runs the MPP Maintenance Utility daily at 4 am to purge CDRs, SDRs, and transcriptions data based on the retention period specified in the EPM.
mppmon	MPP Monitor	Runs as root and monitors the httpd service, restarting them if necessary.
mppsysmgr	System Manager	Handles the majority of tasks required to manage the MPP. 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. When instructed by the EPM, the System Manager starts or stops all MPP processes and distributes EPM configuration updates to all MPP processes as updates occur.
SessionManager	Session Manager	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	Transcription Service	Uploads any transcription data to the Experience Portal database.
vxmlmgr	VoiceXML Manager	Works with the Session Manager to run multiple VoiceXML dialog sessions. VoiceXML Manager also interfaces with the CCXML, telephony, ASR, and TTS subsystems. The VoiceXML Manager and the Session Manager communicates through 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.

Software Upgrade

Software Upgrade overview

The Software Upgrade page in Experience Portal allows you to upgrade the software version of the MPPs running on your Experience Portal system. The Software Upgrade page lists only those software versions which have the .iso image set in the `$AVAYA_IA_HOME/download` directory. Before you start the upgrade process from the Software Upgrade page in EP, make sure you:

- Run the **`/opt/Avaya/InstallAgent/bin/DownloadPK.bash`** <*EPM_Hostname, or EPM IP address*> command on the MPPs to authorize the software upgrades through EPM. For more information see the *Authorizing the EPM to upgrade the MPP* section in the *Implementing Avaya Experience Portal on multiple servers* guide.

- Copy the `.iso` image of the updated software versions in the `$AVAYA_IA_HOME/download` directory.
- Have a corresponding `.sig` for every .iso image.

Note:

Delete files from the `$AVAYA_IA_HOME/download` directory when they are not required.

Software Upgrade page field descriptions

Use this page to upgrade the software version of the MPPs running on your Experience Portal system.

This page contains the:

- Software Upgrade server table on page 282
- Upgrade Commands group on page 284

Software Upgrade server table

Field	Version Description
Selection check box	Indicates the MPPs you want to upgrade. To select all MPPs, click the check box in the header row. **Note:** If there is no Selection check box next to an MPP, it can be because: • The user does not have the permission to upgrade an MPP. • There is no .iso image or tar.gz patch file available in the `$AVAYA_IA_HOME/download` directory. • An MPP is already being upgraded. • The MPP version is not Experience Portal 6.0 or higher. • The MPP is on the same server as the primary EPM. If you select all MPPs, the upgrade process skips MPPs which meet any of the conditions mentioned above.
Zone	The zone where the MPPs are configured.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon
Server Name	The name of the MPP.

Table continues…

Field	Version Description
Mode	The MPP operational mode. The options are: • **Online**: The Media Server is available. • **Offline**: The Media Server is unavailable and is not being polled by the EPM server. • **Test**: (MPP only) The Media Server is available to handle calls made to one of the defined H.323 maintenance stations. **Tip:** To view the date and time that this mode was first reached, hover the mouse over this column.
State	The operational state of the MPP. **Tip:** To view the date and time that this state was first reached, hover the mouse over this column.
Config	The MPP configuration state. The options are: • **Need ports**: The MPP has been configured and is waiting for ports to be assigned • **None**: The MPP has never been configured • **OK**: The MPP is currently operating using the last downloaded configuration • **Restart needed**: The MPP must be restarted to enable the downloaded configuration • **Reboot needed**: The MPP must be rebooted to enable the downloaded configuration
Active Calls	This field displays: • **In**: The number of active incoming calls in the system • **Out**: The number of active outgoing calls in the system
Current Version	The MPP version.

Table continues…

Field	Version Description
Upgrade Status	The MPP upgrade status. The options are: • **Upgrade Pending**: The MPP is selected for an upgrade and is waiting for the upgrade process to start. • **Upgrade Not Needed**: The current version of the MPP is higher than the requested upgrade version. • **Upgrade Not Requested**: The MPP is not selected for upgrade. • **Upgrade Not Possible**: Requested version of upgrade is not supported. • **Downloading**: The requested upgrade version is in the process of downloading. During this process, the MPP continues to be in the **Running** state. • **Downloaded**: Download process is complete and the MPP is waiting for upgrade. • **Recovery Needed**: The upgrade process is interrupted before completion. **Note:** This upgrade status is displayed when the EPM server reboots while the MPP is being upgraded. The upgrade of this MPP continues while the EPM is out of service. However, you must restart the upgrade process for any other MPPs that still needs to be upgraded. • **Upgrade In Progress**: The MPP upgrade is in progress. Once this process starts: - The MPP **State** changes to **Stopped** - The MPP is out of service and the MPP mode changes to **Upgrading** • **Completed Successfully**: The MPP upgrade is completed successfully. • **Failed**: The MPP upgrade process is unsuccessful. **Note:** If there is a problem in upgrading an MPP, the upgrade for all MPPs is stopped. The other MPPs continue to run the software version they had prior to the start of the upgrade. For more information on the upgrade error, you can use the Log Viewer page. • **Cancelled**: The MPP upgrade process is cancelled.
Certificate Algorithm	The Certificate Signing Algorithm of the MPP server certificate.

Upgrade Commands group

Note:

These buttons are greyed out until you select one or more MPPs using the Selection check box in the MPP server table.

Button	Description
New Version	The new versions available for upgrade. **Note:** • Only those versions which have the .iso image or a tar.gz patch file available in the `$AVAYA_IA_HOME/download` directory are available for selection. • Ensure that each .iso has a corresponding .sig in the `$AVAYA_IA_HOME/download` directory. • Manually delete files from the `$AVAYA_IA_HOME/download` directory when they are no longer needed.
Upgrade	Starts the upgrade for the selected MPPs. **Note:** When selected, the button is greyed out until the upgrade is complete.
Cancel	Stops the upgrade for the selected MPPs. It allows an ongoing download or upgrade process to complete before cancelling the upgrade command.

Upgrading all MPP servers

Before you begin

Run the **`/opt/Avaya/InstallAgent/bin/DownloadPK.bash`** <*EPM_Hostname, or EPM IP address*> command on the MPPs to authorize the software upgrades through EPM.

For more information, see the Authorizing the EPM to upgrade the MPP section in the *Implementing Avaya Experience Portal on multiple servers* guide.

Procedure

1. Log on to the EPM web interface.

   If Avaya Services is maintaining this system and you are an Avaya Services representative, log on to EPM by using the init EPM account that is created during the EPM software installation.

   Otherwise, log on to EPM by using an account with the Administrator user role.
2. On the EPM navigation pane, click **System Management** > **Software Upgrade**.
3. In the MPP server table, select the check box in the header row of the first column to select all MPP servers.

Note:

The upgrade process skips an MPP if:

- You do not have permission to upgrade an MPP.
- There is no `.iso` image or tar.gz patch file available in the `$AVAYA_IA_HOME/download` directory.
- An MPP is already being upgraded.
- The MPP version is not Experience Portal 6.0 or higher.
- The MPP is on the same server as the primary EPM.

4. In the **New Version** field, select the required upgrade version.

   Note:

   Only those versions that have the `.iso` image or tar.gz patch file available in the directory `$AVAYA_IA_HOME/download` (default = `/opt/Avaya/InstallAgent/download`) are available for selection.

5. In the **Upgrade Commands** group, click **Upgrade** and confirm your selection when prompted.

   Experience Portal upgrades the MPP servers. This process can take several minutes depending on how many servers are there in your system.

   Note:

   The selection boxes are greyed out and you cannot start another upgrade until the current one completes.

6. After a few minutes, click **Refresh** and verify the following states for all MPP servers:

   - **Mode** is **Online**.
   - **State** is **Running**.
   - **Config** is **OK**.

   Note:

   If there is an error, you can view the details in the **Log Viewer** page.

7. Check that the version numbers are correctly allocated to the MPP servers by verifying the **Current Version** column.

Upgrading an MPP server

Procedure

1. Log on to the EPM web interface.

If Avaya Services is maintaining this system and you are an Avaya Services representative, log on to EPM by using the init EPM account that is created during the EPM software installation.

Otherwise, log on to EPM by using an account with the Administrator user role.

2. On the EPM navigation pane, click **System Management** > **Software Upgrade**.
3. Select the selection check box of the MPP server you want to upgrade.

   Note:

   If there is no selection check box next to an MPP, it can be because:

   - The user does not have the permission to upgrade an MPP.
   - There is no .iso image or tar.gz patch file available in the `$AVAYA_IA_HOME/download` directory.
   - An MPP is already being upgraded.
   - The MPP version is not Experience Portal 6.0 or higher.
   - The MPP is on the same server as the primary EPM.
4. In the **New Version** field, select the required upgrade version.

   Note:

   Only those versions that have the .iso image or tar.gz patch file available in the directory `$AVAYA_IA_HOME/download` (default = `/opt/Avaya/InstallAgent/download`) are available for selection.
5. In the **Upgrade Commands** group, click **Upgrade** and confirm your selection when prompted.

   Experience Portal upgrades the MPP server. This process can take several minutes depending on how many servers there are in your system.

   Note:

   The selection boxes are greyed out and you cannot start another upgrade until the first one completes.
6. After a few minutes, click **Refresh** and verify that the:
   - **Mode** is **Online**.
   - **State** is **Running**.
   - **Config** is **OK**.
7. Check that the version number is correctly allocated to the MPP server by verifying the **Current Version** column.

Starting all MPP servers

Procedure

1. On the EPM navigation pane, click **System Management** > **MPP Manager**.
2. On the MPP Manager page, ensure that the **Mode** column shows **Online** for all servers. If any server is **Offline**, do the following:
   a. Select the check box next to each Offline MPP server.
   b. Click **Online** in the **Mode Commands** group and confirm your selection when prompted.
3. Select the check box in the first column header of the MPP server table to select all MPP servers.
4. Click **Start** in the **State Commands** group and confirm your selection when prompted.

   Experience Portal starts the MPP servers. This process can take several minutes depending on how many servers are there in your system.
5. After a few minutes, click **Refresh** and verify the following states for all MPP servers:
   - **Mode** is **Online**.
   - **State** is **Running**.
   - **Config** is **OK**.
6. **(Optional)** Do the following to ensure that all the licensed telephony ports are correctly allocated to the MPP servers:
   a. On the EPM navigation pane, click **Real-time Monitoring** > **Port Distribution**.
   b. On the Port Distribution page, examine the **Mode** and **State** columns.

Starting an MPP server

Procedure

1. On the EPM navigation pane, click **System Management** > **MPP Manager**.
2. On the MPP Manager page, ensure that the **Mode** column says **Online** for the server you want to start. If the mode is **Offline**, do the following:
   a. Click the selection check box next to the Offline MPP server.
   b. Click the **Online** button in the **Mode Commands** group and confirm your selection when prompted.
3. Click the selection check box next to the MPP server you want to start.
4. Click **Start** in the **State Commands** group and confirm your selection when prompted.

5. After a few minutes, click **Refresh** and verify the following:
   - **Mode** is **Online**.
   - **State** is **Running**.
   - **Config** is **OK**.
6. **(Optional)** To ensure that all licensed telephony ports are correctly allocated to the MPP server, do the following:
   a. On the EPM navigation pane, click **Real-time Monitoring** > **Port Distribution**.
   b. On the Port Distribution page, examine the **Mode** and **State** columns.

Restarting one or more MPP servers

Procedure

1. Log on to the EPM web interface by using an account with the Administration or Operations user role
2. On the EPM navigation pane, click **System Management** > **MPP Manager**.
3. On the MPP Manager page, in the MPP server table, do one of the following:
   - To restart individual MPP servers, select the check box for the MPP server that you want to restart.
   - To restart all MPP servers, click the check box in the header row of the MPP server table.
4. In the **Restart/Reboot Options** group, select one of the following options if you selected multiple servers and want to either restart or reboot them:
   - **One server at a time**
   - **All servers**
5. In the **State Commands** group, click **Restart**.
6. Confirm that you want to restart the selected MPP servers when prompted.
7. After the grace period for the MPP servers has expired, click **Refresh** to ensure that the servers are restarting.

Setting the restart options for an MPP

Procedure

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

2. On the EPM navigation pane, click **System Management** > **MPP Manager**.
3. To change the action Experience Portal takes if an MPP stops unexpectedly, do the following:
   a. Click the pencil icon in the **Auto Restart** column.
   b. Select the check box in the Auto Restart <MPP Name> page.
4. To schedule a one time restart during the current day, do the following:
   a. Click the pencil icon under **Restart Today** in the **Restart Schedule** column.
   b. Enter appropriate information in the Restart <MPP Name> Today page.
5. To specify that the MPP should be automatically restarted on a regular basis, do the following:
   a. Click the pencil icon under **Recurring** in the **Restart Schedule** column.
   b. Enter appropriate information in the Restart Schedule for <MPP Name> page.
6. Click **Save** to return to the MPP Manager page.

Viewing MPP configuration history

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **Real-time Monitoring** > **System Monitor**.
3. On the <System name> Details tab, in the **Server Name** column of the system status table, click the name of the MPP whose configuration history you want to view.
4. On the <MPP name> Details page, click the **History** link next the **Configuration** group.

   You can now view the MPP configuration history.
5. If you want to view or save an XML document detailing a specific configuration change, go to the <MPP Name> Configuration History page, click the link in the **Configuration** column for that change, and follow the prompts.

   Note:

   The number of configuration changes that are displayed depends on the setting for the **Commands to Retain in Configuration History** field on the EPM Settings page.
6. If you want to view or save an XML document showing the complete current configuration for the MPP, click **Export** and follow the prompts.

Configuring Experience Portal to use the Test operational mode

You can test any MPP in the Experience Portal system if there is at least one maintenance station assigned to an H.323 connection and a speech application is available to handle a call made from the maintenance station.

Before you begin

If desired, on the Communication Manager PBX for the system, create a special hunt group for maintenance numbers. For information about setting up the hunt group on the Communication Manager, see *Avaya Configuration Note 3910* on the Avaya online support Web site, http://support.avaya.com.

Make sure that at least one H.323 station has been defined as a maintenance number as described in Defining maintenance stations for an H.323 connection on page 69.

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, look at the **Launch** column and make sure 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 as described in Adding a speech application to Experience Portal on page 342, making sure that 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 as described in Changing speech application settings through Avaya Experience Portal on page 342, making sure that you specify the maintenance stations in the **Application Launch** group on the Change Application page.

Using the Test operational mode

The Test operational mode allows you to send a test call to one or more MPPs in the Experience Portal system.

Before you begin

Configure one or more H.323 connections to use the Test operational mode as described in Configuring Experience Portal to use the Test operational mode on page 291.

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 the MPPs you want to test.

   If you select multiple MPPs, keep in mind that the number of available test ports is equal to the number of defined maintenance numbers. If you put more MPPs into Test mode than you have defined maintenance numbers, some of the MPPs will not be assigned a port and therefore will not be tested.
4. If any of the MPPs are running:
   a. In the **State Commands** group, click **Stop** and confirm your selection when prompted.
   b. After allowing the MPP to finish processing, click **Refresh** to ensure that the state is Stopped.
   c. Use the appropriate Selection check boxes to reselect the MPPs you want to test.
5. In the **Mode Commands** group, click **Test**.
6. Click **Refresh** to ensure the **Mode** is now **Test**.
7. Use the appropriate Selection check boxes to reselect the MPPs you want to test.
8. In the **State Commands** group, click **Start** or **Restart** and confirm your selection when prompted.

   Experience Portal assigns a Test mode port to each MPP as soon as it starts. If the number of MPPs currently in Test mode is:

   - Less than or equal to the number of defined maintenance stations, Experience Portal assigns one Test mode port to each MPP.
   - Greater than the number of defined maintenance stations, Experience Portal randomly assigns the associated Test mode ports to a subset of the selected MPPs. To determine which MPPs were selected, see Viewing telephony port distribution on page 61.
9. Initiate a call using a unique maintenance station for each MPP you placed in Test mode.
10. Verify the results of each call using the Experience Portal reports and MPP logs for additional information if needed.
11. When you have finished testing:
    a. Use the appropriate Selection check boxes to reselect the MPPs you want to put into Online mode.
    b. In the **State Commands** group, click **Stop** and confirm your selection when prompted.
    c. After allowing the MPP to finish processing, click **Refresh** to ensure that the **State** is **Stopped**.
    d. Use the appropriate Selection check boxes to reselect the MPPs.
    e. In the **Mode Commands** group, click **Online**.

f. Use the appropriate Selection check boxes to reselect the MPPs.

g. In the **State Commands** group, click **Start** or **Restart** and confirm your selection when prompted.

h. Click **Refresh** to ensure the **Mode** is now **Online** and the **State** is **Running**.

Reestablishing the link between the EPM and an MPP

About this task

After you upgrade the Experience Portal software, use this procedure to reestablish the link between the MPP and the EPM by trusting the MPP's security certificate.

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** > **MPP Servers**.
3. Click the name of the MPP server.
4. On the Change MPP Server page, go to the **MPP Certificate** section and select the **Trust new certificate** check box if that check box is visible.
5. Click **Save**.
6. On the EPM navigation pane, click **System Management** > **MPP Manager**.
7. On the MPP Manager page, check the **Mode** column for this server and do the following if it displays **Offline**:
   a. Select the check box next to the name of the MPP.
   b. In the **Mode Commands** group, click **Online**.
   c. In a few seconds, click **Refresh** to verify that the **Mode** column now displays **Online**.
8. Select the check box next to the name of the MPP.
9. In the **State Commands** group, click **Start** and confirm your selection when prompted.
10. In a few minutes, click **Refresh** to verify that the current **State** is **Running**.
11. To ensure that the telephony ports were correctly allocated to the MPP server, do the following:
    a. On the EPM navigation pane, click **Real-time Monitoring** > **Port Distribution**.
    b. On the Port Distribution page, check the **Current Allocation** column to find the ports allocated to this MPP.
    c. Check the **Mode** and **State** columns to ensure that the assigned ports are ready to receive calls.

Deleting MPP servers

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** > **MPP Servers**.
3. On the MPP Servers page, do one of the following:
   - To delete individual MPP servers: Select the check box for the MPP name that you want to delete.
   - To delete all MPPs: Select the check box in the header row of the MPP server table, which automatically selects all MPP servers.
4. Click **Delete**.

   Experience Portal removes the MPP from the MPP Servers page but leaves the MPP on the <System name> Details tab of the System Monitor page until the association between the MPP and all H.323 ports and SIP channels are removed.

MPPServiceMenu

The Media Server Service Menu provides details about the status of an MPP and of the calls running on that MPP.

Note:

You must be logged into the EPM as a user with the Administration user role to access the Media Server Service Menu.

Name	Description
Home	Displays the MPP Service Menu home page, which shows an overview of the MPP status.
Activity	Displays the Page Activity page, which shows details about call and telephony activity currently taking place on the MPP.
Calls	Displays the Active Calls page, which shows details about all calls running on the MPP.
Sessions	Displays the Active Sessions page, which shows details about all sessions running on the MPP.
Applications	Displays the Applications page, which shows details about all applications running on the MPP.
Statistics	Displays the Application Statistics page, which shows statistics for all applications running on the MPP.

Table continues…

Name	Description
Certificates	Displays the Certificates page, which displays a list of the certificates available on the MPP.
Configuration	Displays the Configuration page, which shows the configuration file for this MPP.
Diagnostics	Displays the Diagnostics page, which lets you: • Check the connectivity between the MPP and the other servers in the Experience Portal system. • Create a compressed file containing the logs stored on this MPP. • View process messages. • View the current and previous version of the MPP software installed on this server.
Logs	Displays the Log Directories page, which shows the logs created on the MPP.
Resources	Displays the Resources page, which shows a summary of the Automatic Speech Recognition (ASR), Text-to-Speech (TTS), and telephony resources are being used by the applications running on the MPP.
ASR	Displays the ASR Resources page, which displays details about the ASR resources being used by the MPP.
TTS	Displays the TTS Resources page, which displays details about the TTS resources being used by the MPP.
Speech Servers	Displays the Speech Servers page, which displays the status of the speech servers available to the MPP.
Telephony	Displays the Telephony Resources page, which displays details about the telephony resources being used by the MPP.
Networking	Displays the Networking page, which displays details about the telephony resources being used by the MPP.
Users	Displays the Users page, which shows the EPM user accounts that have the Administration user role and are therefore authorized to access the Media Server Service Menu.

Logging in to the Media Server Service Menu

About this task

If you are logged in to the EPM with the Administration user role, you can also log in to the Media Server Service Menu for a specific MPP.

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 **Real-time Monitoring** > **System Monitor**.

3. On the System Monitor page, go to the <System name> Details tab, 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. Click the name of an MPP in the **Server Name** column.
5. On the <MPP name> Details page, in the **Miscellaneous** group, click **Service Menu** .

   If the EPM does not automatically open the Media Server Service Menu, there may be a problem with the proxy server settings. For details, see Using the Media Server Service Menu with a proxy server on page 296.

Using the Media Server Service Menu with a proxy server

About this task

If your browser uses a proxy server, you need to add the host address of the MPP to the list of addresses for which a proxy server is not required. You should then be able to access the Media Server Service Menu from the appropriate <MPP name> Details page.

Procedure

1. Open Internet Explorer.
2. Select **Tools** > **Internet Options** > **Connections**.
3. Click **LAN Settings**, then click **Advanced**.
4. In the **Exceptions** text box, enter the host addresses of the MPP whose Media Server Service Menu you want to access.

   You can use the * (asterisk) wildcard to specify multiple MPPs with similar addresses.

   Tip:

   To determine the host address of a particular MPP, look at the <MPP name> Details for that MPP.

   To view the host addresses for all MPPs, from the EPM main menu, select **System Configuration** > **MPP Servers**.
5. Click **OK** three times to close the Proxy Settings dialog, the LAN Settings dialog, and the Internet Options dialog.

Next steps

Log into the Media Server Service Menu as described in Logging in to the Media Server Service Menu on page 295.

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. 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 the 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 be at least as large 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, refer to Man pages on Linux for the **`Mount`** command

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 Manager 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. 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, 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.
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 Manager page, click the Selection check box next to the name of the MPP you want to start.
   c. Click **Restart** in the **State Commands** group
   d. Wait until the operational state becomes Running. To check this, click **Refresh** and look at the **State** field.

Add MPP Server page field descriptions

Use these pages to add a new Media Processing Platform (MPP) to the Experience Portal system.

Add MPP Server page (page 1 of 2)

Field	Description
Zone	The name of the zone where the MPP server is configured. Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only if you have created zones on your Experience Portal system. If you do not create any new zones, you do not see the drop-down box.

Table continues…

Field	Description
Name	The unique identifier for the MPP server on the Experience Portal system. This name is used only in the EPM web interface and cannot be changed after you save the new MPP.
Host Address	The network address, or location, of the computer on which the MPP server resides. The EPM uses this address to communicate with the MPP server. This address can be a fully qualified domain name or an IP address, but the address must be unique on this Experience Portal system and the machine must already have the MPP software installed on it. You cannot use any of the following hostnames: `127.0.0.1`, `localhost`, or `localhost.local.domain`.
Continue	Submits the name and host address to Experience Portal for verification. Experience Portal verifies the host address by attempting to download the Secure Sockets Layer (SSL) certificate from the designated MPP. If the SSL certificate fails to download, Experience Portal prompts you to correct the **Host Address** field entry and try again. When the SSL certificate downloads successfully, Experience Portal displays the second Add MPP Server page.

Add MPP Server page (page 2 of 2)

This page contains the:

- General section on page 299
- MPP Certificate section on page 301
- Categories and Trace Levels section on page 301

General section

Field	Description
Name	The name you entered on the first Add MPP page. **Note:** This field cannot be changed.

Table continues…

Field	Description
Host Address	The network address, or location, of the computer on which the MPP server resides. The EPM uses this address to communicate with the MPP server. This address can be a fully qualified domain name or an IP address, but the address must be unique on this Experience Portal system and the machine must already have the MPP software installed on it. You cannot use any of the following hostnames: `127.0.0.1`, `localhost`, or `localhost.local.domain`. **Important:** If you entered an incorrect host address on the first Add MPP page, Experience Portal displays an error message in red next to this field. You must correct this error before you can save the new MPP.
Network Address (VoIP)	The IP address the telephony servers must use to communicate with the MPP.
Network Address (MRCP)	The IP address the speech proxy servers must use to communicate with the MPP when processing ASR and TTS requests. **Tip:** This address is usually the same as the host IP address.
Network Address (AppSvr)	The IP address the application servers must use to communicate with the MPP. **Tip:** This address is usually the same as the host IP address.
Maximum Simultaneous Calls	The maximum number of calls that this MPP can handle at any one time. It is equivalent to the maximum number of ports that Experience Portal will allocate to this MPP. Enter an integer in this field. **Note:** 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 *Avaya Experience Portal Overview and Specification* on http://support.avaya.com.

Table continues…

Field	Description
Restart Automatically	The options are: • **Yes**: If the MPP stops unexpectedly, Experience Portal brings it back online automatically. • **No**: If the MPP stops, it must be manually restarted. **Note:** This option also affects an MPP that has received an **`explicit Reboot or Halt`** command. For details about issuing a **`Halt`** command and changing the operational state of one or more MPPs, see *Administering Avaya Experience Portal* on http://support.avaya.com.
Listed Directory Number (LDN)	This field is only shown when you are logged into the EPM using the Avaya Services init account created when the Avaya Service accounts were configured. If you are logged into the EPM using the init account, enter the LDN number for this server as it appears in the Avaya Services database. If an LDN number is not specified for this server, Experience Portal uses the default value (000)000-0000.

MPP Certificate section

Field	Description
Certificate display box	The SSL certificate issued by the MPP. The displayed certificate must exactly match the certificate that was established when the MPP was first installed.
Trust new certificate	If this MPP has just been installed or upgraded, this check box is displayed in this section. If you see this check box, make sure the certificate is valid and then select the check box. You cannot save the MPP until the certificate is accepted.

Categories and Trace Levels section

Performance tracing is a valuable troubleshooting tool, but it can adversely impact Experience Portal system performance if you set all categories to **Finest** on a busy production system. If you need to troubleshoot a particular area, you must set specific categories to **Fine** and examine the resulting output to see if you can locate the issue. If not, set the level to **Finer** and repeat the process. If you still need more data, then set the level to **Finest** and keep a close watch on system resource usage.

Note:

If these fields are not displayed, click the group heading to expand the group.

Field or Radio Button	Description
Trace level settings radio buttons	The options are: • **Use MPP Settings**: The MPP uses the default settings for all MPPs set on the MPP Settings page. • **Custom**: The MPP uses the trace level settings in the table in this section. **Note:** If you want to set any of the trace levels, you must select the **Custom** radio button first.
Off	Sets trace logging for all categories to off.
Fine	Sets trace logging for all categories to fine.
Finer	Sets trace logging for all categories to finer.
Finest	Sets trace logging for all categories to finest.
ASR	The amount of trace logging done on the Automatic Speech Recognition (ASR) server. Select **Off**, **Fine**, **Finer**, or **Finest**.
CCXML Browser	The amount of trace logging done for Call Control eXtensible Markup Language (CCXML). Select **Off**, **Fine**, **Finer**, or **Finest**.
Event Manager	The amount of trace logging for the Event Manager. This component collects events from other MPP processes and sends them to the network log web service on the EPM. Select **Off**, **Fine**, **Finer**, or **Finest**.
Media Endpoint Manager	The amount of trace logging done for the Media End Point Manager. This trace component controls the logging for the media endpoint interface in the MediaManager process. The media endpoint interface controls the RTP (audio, video) flow through the MediaManager and to the external servers. Select **Off**, **Fine**, **Finer**, or **Finest**.
Media Manager	The amount of trace logging done for the Media Manager. This trace component controls the logging for the start and shutdown of the MediaManager process. Select **Off**, **Fine**, **Finer**, or **Finest**.

Table continues…

Field or Radio Button	Description
Media Video Manager	The amount of trace logging done for the Media Video Manager. This trace component controls the logging for the video interface in the MediaManager process. The video interface handles: • Downloading of any files (.txt, .jpg, .3pg and so on.) referenced in the Synchronized Multimedia Integration Language (SMIL) from the application server • Rendering video based on the video configuration from EPM and commands from SessionManager **Note:** SMIL parsing is done in SessionManager and low level video commands are sent to this component. Select **Off**, **Fine**, **Finer**, or **Finest**.
MPP System Manager	The amount of trace logging done for the MPP System Manager. Select **Off**, **Fine**, **Finer**, or **Finest**.
MRCP	The amount of trace logging done on the speech proxy server. Select **Off**, **Fine**, **Finer**, or **Finest**.
Reporting	The amount of trace logging done for the Call Data Handler (CDH). Select **Off**, **Fine**, **Finer**, or **Finest**.
Session Manager	The amount of trace logging done for the MPP Session Manager. Select **Off**, **Fine**, **Finer**, or **Finest**.
SIP Messages Tracing	The amount of trace logging done for the SIP Messages. Select **Off**, **Fine**, **Finer**, or **Finest**. This component logs the Global Session ID (GSID) in the trace files when you set the tracing level to **Finest**.
Telephony	The amount of trace logging done on the telephony server. Select **Off**, **Fine**, **Finer**, or **Finest**.
Trace Logger	The amount of trace logging done for the Web Service Trace. The Trace Logger uploads the MPP traces requested by the trace client that runs on EPM. This trace component controls the logging for the activities of trace retrieval in the Trace Web Service. Select **Off**, **Fine**, **Finer**, or **Finest**.
TTS	The amount of trace logging done on the Text-to-Speech (TTS) server. Select **Off**, **Fine**, **Finer**, or **Finest**.

Table continues…

Field or Radio Button	Description
Voice Browser Client	The amount of trace logging done for the Avaya Voice Browser (AVB) client. This component connects the Voice eXtensible Markup Language (VoiceXML) interpreter to the MPP. Its logs: • Indicate the progress of VoiceXML execution and any exceptions or errors from VoiceXML documents • Contain the status and errors from platform initialization and interpreter initialization Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser INET	The amount of trace logging done for the AVB INET. This component manages: • Downloading content such as VoiceXML and prompts from the application server • Storing this content in the local VoiceXML interpreter cache Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Interpreter	The amount of trace logging done for the AVB interpreter. This component parses and interprets the VoiceXML commands and controls the flow of the application based on Dual-tone multi-frequency (DTMF) or recognition results. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Java Script Interface	The amount of trace logging done for the AVB Javascript Interface. This component perform the ECMAScript execution from the VoiceXML documents. Its logs contain the status of script execution and any ECMAScript semantic errors. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Object	The amount of trace logging done for the AVB. This component is the interface to the platform module that performs VoiceXML element execution. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Platform	The amount of trace logging done for the AVB. This component handles messages from the MPP `vxmlmgr` process, the wrapper for the VoiceXML interpreter. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Prompt	The amount of trace logging done for the AVB prompt. This component controls queuing, converting, and playing prompts. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Recognition	The amount of trace logging done for the AVB recognition function. This component controls queuing, loading, and unloading grammars. Select **Off**, **Fine**, **Finer**, or **Finest**.

Table continues…

Field or Radio Button	Description
Voice Browser Telephony	The amount of trace logging done for the AVB telephony interface. This component is the interface to the telephony system of the MPP. It handles features such as features as disconnect, blind transfer, and bridge transfer. In addition, its log also contains any channel initialization errors that the system encounters. Select **Off**, **Fine**, **Finer**, or **Finest**.

Restart Automatically <MPP Name> page field descriptions

Field	Description
Restart Automatically	Determines whether Experience Portal automatically restarts an MPP if it stops unexpectedly. If this check box is: • Selected, Experience Portal brings the MPP back online automatically • Not selected, you must manually restart the MPP if it stops **Note:** This option also affects an MPP that has received an **`explicit Reboot or Halt`** command. For details about issuing a **`Halt`** command and changing the operational state of one or more MPPs, see *Administering Avaya Experience Portal* on http://support.avaya.com.

Change MPP Server page field descriptions

Use this page to change an existing Media Processing Platform (MPP).

This page contains the:

General section

Field	Description
Zone	The name of the zone where the MPP server is configured. Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only if you have created zones on your Experience Portal system. If you do not create any new zones, you do not see the drop-down box.
Name	The unique identifier for the MPP server on the Experience Portal system. **Note:** This field cannot be changed.
Host Address	The network address, or location, of the computer on which the MPP server resides. The EPM uses this address to communicate with the MPP server. This address can be a fully qualified domain name or an IP address, but the address must be unique on this Experience Portal system and the machine must already have the MPP software installed on it. You cannot use any of the following hostnames: `127.0.0.1`, `localhost`, or `localhost.local.domain`. **Note:** This field cannot be changed.
Network Address (VoIP)	The IP address the telephony servers must use to communicate with the MPP. To use the IP address associated with the address in the **Host Address** field, enter `<Default>` in this field.
Network Address (MRCP)	The IP address the speech proxy servers must use to communicate with the MPP when processing ASR and TTS requests. **Tip:** This address is usually the same as the host IP address. To use the IP address associated with the address in the **Host Address** field, enter `<Default>` in this field.
Network Address (AppSvr)	The IP address the application servers must use to communicate with the MPP. **Tip:** This address is usually the same as the host IP address. To use the IP address associated with the address in the **Host Address** field, enter `<Default>` in this field.

Table continues…

Field	Description
Maximum Simultaneous Calls	The maximum number of calls that this MPP can handle at any one time. It is equivalent to the maximum number of ports that Experience Portal will allocate to this MPP. Enter an integer in this field. **Note:** 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 *Avaya Experience Portal Overview and Specification* on http://support.avaya.com.
Restart Automatically	The options are: • **Yes**: If the MPP stops unexpectedly, Experience Portal brings it back online automatically. • **No**: If the MPP stops, it must be manually restarted. **Note:** This option also affects an MPP that has received an **`explicit Reboot or Halt`** command. For details about issuing a **`Halt`** command and changing the operational state of one or more MPPs, see *Administering Avaya Experience Portal* on http://support.avaya.com.
Listed Directory Number (LDN)	This field is only shown when you are logged into the EPM using: • The Avaya Services init account created when the Avaya Service accounts were configured. In this case, you can enter a value in this field. • Any other EPM user account and an Avaya Services representative has previously set the LDN value. In this case, the field is read only. If you are logged into the EPM using the init account, enter the LDN number for this server as it appears in the Avaya Services database. If an LDN number is not specified for this server, Experience Portal uses the default value (000)000-0000.

MPP Certificate section

Field	Description
Certificate display box	The SSL certificate issued by the MPP. The displayed certificate must exactly match the certificate that was established when the MPP was first installed. **Note:** The MPP certificate cannot be edited on this page.
Trust new certificate	If this MPP has just been installed or upgraded, this check box is displayed in this section. If you see this check box, make sure the certificate is valid and then select the check box. You cannot save the MPP until the certificate is accepted.

Categories and Trace Levels section

Performance tracing is a valuable troubleshooting tool, but it can adversely impact Experience Portal system performance if you set all categories to **Finest** on a busy production system. If you need to troubleshoot a particular area, you must set specific categories to **Fine** and examine the resulting output to see if you can locate the issue. If not, set the level to **Finer** and repeat the process. If you still need more data, then set the level to **Finest** and keep a close watch on system resource usage.

Note:

If these fields are not displayed, click the group heading to expand the group.

Field or Radio Button	Description
Trace level settings radio buttons	The options are: • **Use MPP Settings**: The MPP uses the default settings for all MPPs set on the MPP Settings page. • **Custom**: The MPP uses the trace level settings in the table in this section. **Note:** If you want to set any of the trace levels, you must select the **Custom** radio button first.
Off	Sets trace logging for all categories to off.
Fine	Sets trace logging for all categories to fine.
Finer	Sets trace logging for all categories to finer.
Finest	Sets trace logging for all categories to finest.
ASR	The amount of trace logging done on the Automatic Speech Recognition (ASR) server. Select **Off**, **Fine**, **Finer**, or **Finest**.
CCXML Browser	The amount of trace logging done for Call Control eXtensible Markup Language (CCXML). Select **Off**, **Fine**, **Finer**, or **Finest**.
Event Manager	The amount of trace logging for the Event Manager. This component collects events from other MPP processes and sends them to the network log web service on the EPM. Select **Off**, **Fine**, **Finer**, or **Finest**.
Media Endpoint Manager	The amount of trace logging done for the Media End Point Manager. This trace component controls the logging for the media endpoint interface in the MediaManager process. The media endpoint interface controls the RTP (audio, video) flow through the MediaManager and to the external servers. Select **Off**, **Fine**, **Finer**, or **Finest**.

Table continues…

Field or Radio Button	Description
Media Manager	The amount of trace logging done for the Media Manager. This trace component controls the logging for the start and shutdown of the MediaManager process. Select **Off**, **Fine**, **Finer**, or **Finest**.
Media Video Manager	The amount of trace logging done for the Media Video Manager. This trace component controls the logging for the video interface in the MediaManager process. The video interface handles: • Downloading of any files (.txt, .jpg, .3pg and so on.) referenced in the Synchronized Multimedia Integration Language (SMIL) from the application server • Rendering video based on the video configuration from EPM and commands from SessionManager **Note:** SMIL parsing is done in SessionManager and low level video commands are sent to this component. Select **Off**, **Fine**, **Finer**, or **Finest**.
MPP System Manager	The amount of trace logging done for the MPP System Manager. Select **Off**, **Fine**, **Finer**, or **Finest**.
MRCP	The amount of trace logging done on the speech proxy server. Select **Off**, **Fine**, **Finer**, or **Finest**.
Reporting	The amount of trace logging done for the Call Data Handler (CDH). Select **Off**, **Fine**, **Finer**, or **Finest**.
Session Manager	The amount of trace logging done for the MPP Session Manager. Select **Off**, **Fine**, **Finer**, or **Finest**.
SIP Messages Tracing	The amount of trace logging done for the SIP Messages. Select **Off**, **Fine**, **Finer**, or **Finest**. This component logs the Global Session ID (GSID) in the trace files when you set the tracing level to **Finest**.
Telephony	The amount of trace logging done on the telephony server. Select **Off**, **Fine**, **Finer**, or **Finest**.
Trace Logger	The amount of trace logging done for the Web Service Trace. The Trace Logger uploads the MPP traces requested by the trace client that runs on EPM. This trace component controls the logging for the activities of trace retrieval in the Trace Web Service. Select **Off**, **Fine**, **Finer**, or **Finest**.

Table continues…

Field or Radio Button	Description
TTS	The amount of trace logging done on the Text-to-Speech (TTS) server. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Client	The amount of trace logging done for the Avaya Voice Browser (AVB) client. This component connects the Voice eXtensible Markup Language (VoiceXML) interpreter to the MPP. Its logs: • Indicate the progress of VoiceXML execution and any exceptions or errors from VoiceXML documents • Contain the status and errors from platform initialization and interpreter initialization Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser INET	The amount of trace logging done for the AVB INET. This component manages: • Downloading content such as VoiceXML and prompts from the application server • Storing this content in the local VoiceXML interpreter cache Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Interpreter	The amount of trace logging done for the AVB interpreter. This component parses and interprets the VoiceXML commands and controls the flow of the application based on Dual-tone multi-frequency (DTMF) or recognition results. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Java Script Interface	The amount of trace logging done for the AVB Javascript Interface. This component perform the ECMAScript execution from the VoiceXML documents. Its logs contain the status of script execution and any ECMAScript semantic errors. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Object	The amount of trace logging done for the AVB. This component is the interface to the platform module that performs VoiceXML element execution. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Platform	The amount of trace logging done for the AVB. This component handles messages from the MPP `vxmlmgr` process, the wrapper for the VoiceXML interpreter. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Prompt	The amount of trace logging done for the AVB prompt. This component controls queuing, converting, and playing prompts. Select **Off**, **Fine**, **Finer**, or **Finest**.

Table continues…

Field or Radio Button	Description
Voice Browser Recognition	The amount of trace logging done for the AVB recognition function. This component controls queuing, loading, and unloading grammars. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Telephony	The amount of trace logging done for the AVB telephony interface. This component is the interface to the telephony system of the MPP. It handles features such as features as disconnect, blind transfer, and bridge transfer. In addition, its log also contains any channel initialization errors that the system encounters. Select **Off**, **Fine**, **Finer**, or **Finest**.

<MPP name> Details page field descriptions

Use this page to view detailed information about the Media Processing Platform (MPP) *<MPP Name>*.

Note:

This page is called the <EPM Name>/<MPP Name> Details page if the EPM and MPP server are installed on the same machine.

General Information group

Field	Description
Zone	The name of the zone within which the MPP is configured.
Server Name	The unique name for this MPP.
Unique ID	The ID number used for this MPP in the database. Experience Portal selects this number from the range given in the **MPP Numeric ID Range** field on the MPP Settings page.
Host Address	The hostname of the MPP.
IP Address	The IP address of the MPP.
Version	The version number of the MPP software.
Last Successful Poll	The last date and time that the EPM polled the MPP successfully.

Operational State group

Field or Button	Description
Current State	The operational state of the Media Server. The options are: • **Booting**: The Media Server is in the process of restarting and is not yet ready to take new calls. • **Degraded**: The Media Server is running but it is not functioning at full capacity. • **Error**: The Media Server has encountered a severe problem and cannot recover. • **Halted**: The Media Server is no longer responding to heartbeats because it received a **`Halt`** command. • **Halting**: The Media Server is responding to heartbeats but is not taking new calls. • **Need Configuration**: An Email or SMS processor residing on the Media Server has not yet been configured. • **Need Connections**: No connections (SMPP or HTTP) have been configured or assigned to an Email/SMS processor residing on the Media Server. • **Never Used**: The Media Server has never successfully responded to a heartbeat request. • **Not Installed**: The Media Server is missing files required for heartbeat requests to occur. • **Not Responding**: The Media Server is not responding to heartbeat requests and it has not received a **`Restart`** or **`Halt`** command. • **Partially Running**: (EPM only) The Media Server is in the process of starting up, and not all individual components of the service, for example: Tomcat, SL, ActiveMQ, have come up yet. • **Rebooting**: The Media Server is responding to heartbeats but is not taking new calls. • **Recovering**: The Media Server has encountered a problem and is attempting to recover. • **Restart Needed**: This state is most often reached when the Media Server has encountered a problem that it cannot recover from and it requires a manual restart. However, it can also appear for an MPP when the EPM software has been upgraded and the MPP software has not. In that case, the state should update automatically when you upgrade the MPP software. • **Running**: The Media Server is responding to heartbeat requests and is accepting new calls. • **Starting**: The Media Server is responding to heartbeats but not taking new calls because it is transitioning from the Stopped state to the Running state.

Table continues…

Field or Button	Description
	• **Stopped**: The Media Server is responding to heartbeats but is not taking new calls. The Media Server enters this state while it initializes after it restarts or when a `Stop` command is received. • **Stopping**: The Media Server is responding to heartbeats but is not taking new calls. • **Unknown**: The Media Server is in the Offline mode.
Requested State	If the MPP is in the process of changing states, this field shows the state that the user requested and the time at which the request was made.

Operational Mode group

Field or Button	Description
Current Mode	The operational mode of the MPP. The options are: • **Online**: The Media Server is available. • **Offline**: The Media Server is unavailable and is not being polled by the EPM server. • **Test**: (MPP only) The Media Server is available to handle calls made to one of the defined H.323 maintenance stations.
Configure	Opens the Change MPP Server page so you can change the MPP configuration.

Configuration group

Field or Link	Description
History	Click this link to view the MPP configuration history.
Current State	The current configuration state.
Last Modified	The date and time when the MPP configuration was last changed.

Call Status group

Field	Description
Current Capacity	The number of calls that the system is ready to accept.
Licenses Allocated	The number of licenses allocated to the MPP.
Maximum Call Capacity	The maximum call capacity for the MPP.
Active Calls	The number of calls that are currently active on the MPP.
Calls Today	The number of calls handled by the MPP today.

Resource Status group

Field	Description
CPU	The percentage of CPU utilization for the MPP.
Memory	The percentage of memory utilization for the MPP.
Disk	The percentage of hard disk utilization for the MPP.

Miscellaneous group

This group contains a link to the Media Server Service Menu. To access this menu, click **Service Menu**.

MPP Manager page field descriptions

Use this page to change the operational state and mode of the MPPs running on your Experience Portal system.

The page contains the:

- MPP server table on page 314
- State Commands group on page 316
- Restart/Reboot Options group on page 318
- Mode Commands group on page 318

MPP server table

Field	Description
Selection check box	Indicates the MPPs whose operational state or mode you want to change. To select all MPPs, click the check box in the header row.
Zone	The name of the zone where the MPP is configured.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon
Server Name	The name of the MPP.

Table continues…

Field	Description
Mode	The MPP operational mode and the date and time that mode took effect. The options are: • Online: The MPP is available to handle normal call traffic. • Offline: The MPP is unavailable to handle any calls and is not being polled by the Experience Portal server. • Test: The MPP is available to handle calls made to one of the defined H.323 maintenance stations. • Upgrading: The MPP upgrade is in process and the MPP is temporarily unavailable. **Tip:** To view the date and time that this mode was first reached, hover the mouse over this column.
State	The operational state of the MPP. **Tip:** To view the date and time that this state was first reached, hover the mouse over this column.
Active Command	This column is displayed if one or more MPPs are currently in transition from their current state to a new user-requested state. For each transitional MPP, this column displays the requested, or final, state. For any other MPPs in the system, this field displays **None**.
Config	The MPP configuration state. The options are: • **Need certificates**: The Primary EPM certificate must be downloaded to the MPP by running the `setup_vpms.php` script on the MPP • **Need ports**: The MPP has been configured and is waiting for ports to be assigned • **None**: The MPP has never been configured • **OK**: The MPP is currently operating using the last downloaded configuration • **Restart needed**: The MPP must be restarted to enable the downloaded configuration • **Reboot needed**: The MPP must be rebooted to enable the downloaded configuration
Auto Restart	The options are: • **Yes** if the MPP will restart automatically if it fails • **No** if the MPP must be manually restarted if it fails

Table continues…

Field	Description
Restart Schedule	This field displays: • **Today**: Displays **Yes at *time*** if the MPP is administered to restart today. Displays **No** otherwise. To change this, click the pencil icon. • **Recurring**: Displays the recurring restart schedule, or **None** if there is no schedule defined. To change this, click the pencil icon.
Active Calls	This field displays: • **In**: The number of active incoming calls in the system • **Out**: The number of active outgoing calls in the system

State Commands group

Note:

These buttons are greyed out until you select one or more MPPs using the Selection check box in the MPP server table.

Important:

Ensure that the Operational Grace Period is long enough for the MPP to complete any existing calls before it stops, restarts, reboots, or halts. Calls are terminated when the Operational Grace Period is reached. For more information on the Operational Grace Period, see Setting the global grace period and trace level parameters on page 271.

Button	Description
Start	Starts the MPP. The operational state changes to Starting until the MPP is back online, after which the state changes to Running. **Important:** When you start an MPP, the Experience Portal system experiences a brief disruption in service while it reallocates the licensed ports. To avoid the disruption, start MPPs during off-peak hours.
Stop	Stops the MPP. The operational state changes to Stopping until all active calls have disconnected or the grace period expires, whichever comes first. At that time, the state changes to Stopped. Experience Portal will only restart the MPP if: • You issue an explicit `Start` command • The MPP has a specified restart schedule **Note:** For more information, see Setting the global grace period and trace level parameters on page 271.

Table continues…

Button	Description
Restart	Restarts the MPP software, but does not affect the server machine. The operational state changes to Stopping until all active calls have disconnected or the grace period expires, whichever comes first. After the MPP stops, it starts again automatically, and the operational state changes to Starting until the MPP is ready to take calls again. At that point, the state changes to Running. **Important:** Before you click this button, make sure you select the appropriate option in the **Restart/Reboot Options** group.
Reboot	Reboots the MPP server machine. The operational state changes to Rebooting until all active calls have disconnected or the grace period expires, whichever comes first. At that time, the MPP server machine shuts down and automatically restarts. The state changes to Starting until the MPP is ready to take calls again. At that point, the state changes to Running. **Note:** If the EPM resides on the same server as the MPP, it will be rebooted as well. In that case, you need to wait several minutes after the system has rebooted for Tomcat to restart and reinitialize its web applications before you can log back into the Experience Portal. **Important:** Before you click this button, make sure you select the appropriate option in the **Restart/Reboot Options** group.
Halt	Halts the MPP and turns off the server machine on which the MPP is running. The operational state changes to Halting until all active calls have disconnected or the grace period expires, whichever comes first. After that, the state changes to Halted when the MPP server machine has powered down. **Important:** If the EPM resides on the same server as the MPP, it will be halted as well. The MPP cannot be restarted until after the MPP server machine is restarted. Once the server machine has finished booting, the MPP software is automatically started and the MPP enters the Stopped state. At that point: • If the **Auto Restart** option is enabled, Experience Portal automatically starts the MPP. • You can manually restart the MPP using the **Start** button on this page.
Cancel	If you have issued a restart or reboot request and selected **One server at a time** in the **Restart/Reboot Options** group, you can cancel that request for any MPP servers that have not yet been restarted or rebooted. You cannot cancel a restart or reboot request that is already in process.

Restart/Reboot Options group

The options are:

- **One server at a time**. If you select this option, Experience Portal restarts or reboots one of the selected MPPs and waits until that MPP has completely restarted and been assigned its ports before it goes on to restart or reboot the next MPP on the list.
- **All servers**.

Mode Commands group

Note:

These buttons are grayed out until you select one or more MPPs using the Selection check box in the MPP server table.

Button	Description
Offline	Sets the operational mode to Offline. No further polling is done.
Test	Sets the operational mode to Test. Once you start or restart the MPP, only calls made to one of the defined H.323 maintenance stations will be accepted. For details, see Using the Test operational mode on page 291.
Online	Sets the operational mode to Online. Once you start or restart the MPP, it will be ready to handle normal call traffic.

MPP Servers page field descriptions

Use this page to view, add, change, and delete the Media Processing Platform (MPP) servers currently administered on the Experience Portal system.

Field	Description
Selection check box	Indicates which MPP servers you want to delete.
Zone	The name of the zone where the MPP servers are configured.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
Name	The unique identifier for the MPP server on the Experience Portal system.
Host Address	The network address, or location, of the computer on which the MPP server resides. The EPM uses this address to communicate with the MPP server.

Table continues…

Field	Description
Network Address (VoIP)	The IP address the telephony servers must use to communicate with the MPP. The options are: • **<Default>**: The servers use the IP address specified in the **Host Address** field. • A specific IP address.
Network Address (MRCP)	The IP address the speech proxy servers must use to communicate with the MPP when processing ASR and TTS requests. The options are: • **<Default>**: The servers use the IP address specified in the **Host Address** field. • A specific IP address.
Network Address (AppSvr)	The IP address the application servers must use to communicate with the MPP. The options are: • **<Default>**: The servers use the IP address specified in the **Host Address** field. • A specific IP address.
Maximum Simultaneous Calls	The maximum number of calls that this MPP can handle at any one time. It is equivalent to the maximum number of ports that Experience Portal will allocate to this MPP.
Trace Level	The options are: • **Use MPP Settings**: The MPP uses the default trace settings specified on the MPP Settings page. • **Custom**: The MPP uses the trace settings specified for the specific MPP. To view these settings, click the server name in the **Name** column.
Add	Opens the Add MPP Server page so that you can add a new MPP server.
Delete	Deletes the selected MPP servers.
MPP Settings	Opens the MPP Settings page so you can change the global settings for all MPP servers.
Browser Settings	Opens the Browser Settings page so you can change the global Avaya Voice Browser settings for all MPP servers.
Video Settings	Opens the Video Settings page to configure system parameters that affect video.
VoIP Settings	Opens the VoIP Settings page so you can change the global Voice over IP settings for all MPP servers.

MPP Settings page field descriptions

Use this page to configure options that affect all MPPs on the Experience Portal system.

Resource Alerting Thresholds group

Field	Description
CPU	The low water threshold determines when the MPP generates an event warning you that CPU usage is getting high. The high water threshold determines when the MPP generates an alarm warning you that CPU usage is getting dangerously high. • **High Water**: Enter a whole number from 0 to 100. The default is 70. • **Low Water**: Enter a whole number from 0 to 100. The default is 60.
Memory	The low water threshold determines when the MPP generates an event warning you that RAM usage is getting high. The high water threshold determines when the MPP generates an alarm warning you that RAM usage is getting dangerously high. • **High Water**: Enter a whole number from 0 to 100. The default is 80. • **Low Water**: Enter a whole number from 0 to 100. The default is 70.
Disk	The low water threshold determines when the MPP generates an event warning you that disk usage is getting high. The high water threshold determines when the MPP generates an alarm warning you that disk usage is getting dangerously high. • **High Water**: Enter a whole number from 0 to 100. The default is 80. • **Low Water**: Enter a whole number from 0 to 100. The default is 60.

Trace Logger group

Field	Description
Log File Maximum Size	The maximum size, in megabytes, that the log file can be. Once the log file reaches this size, the system starts a new log file. If starting a new log file causes the number of logs to exceed the **Number of Logs to Retain** setting, the system deletes the oldest file before it starts the new file. Enter a whole number from 1 to 100. The default is 10. **Note:** Due to the volume of trace messages from the following components, the number of log files retained by the system are set higher than the number you specify in this field. The actual size is as follows: • Endpoint Manager ($AVAYA_MPP_HOME/logs/process/MediaMgr/EndPointMgr): 5x • Media Manager ($AVAYA_MPP_HOME/logs/process/MediaMgr/MediaManager): 2x • Session Manager ($AVAYA_MPP_HOME/logs/process/SessMgr/*): 2x

Table continues…

Field	Description
Number of Logs to Retain	The maximum number of log files the system can retain, including the current one. Once this number of log files exists, the system deletes the oldest log file before starting a new one. Enter a whole number from 1 to 5. The default is 2. **Note:** Due to the volume of trace messages from the following components, the number of log files retained by the system are set higher than the number you specify in this field. The actual size is as follows: • Endpoint Manager ($AVAYA_MPP_HOME/logs/process/MediaMgr/EndPointMgr): 5x • Media Manager ($AVAYA_MPP_HOME/logs/process/MediaMgr/MediaManager): 2x • Session Manager ($AVAYA_MPP_HOME/logs/process/SessMgr/*): 2x

Transcription group

Field	Description
Transcriptions Retention Period	How long an MPP keeps detailed session transcriptions for the sessions that it handles. Enter a whole number from 0 to 999. The default is 14.

Record Handling on MPP group

Field	Description
Session Data	Whether an MPP keeps detailed records about the sessions that it handles. Experience Portal uses this data to create the Session Detail report and Session Summary report. • **Enable**: Select this check box to record session data on all MPPs. • **Retention Period**: The number of days to retain the session data. Enter a whole number from 1 to 999. The default is 14.
Call Data	Whether an MPP keeps detailed records about the calls that it handles. Experience Portal uses this data to create the Contact Detail report and Contact Summary report. • **Enable**: Select this check box to record call data on all MPPs. • **Retention Period**: The number of days to retain the session data. Enter a whole number from 1 to 999. The default is 14.

Table continues…

Field	Description
VoiceXML/CCXML Log Tags	Whether an MPP keeps the CCXML and VoiceXML Log tag data from the application sessions transacted on that server. If desired, Experience Portal can download the Log tag data and display it in the Application Detail report and Application Summary report. • **Enable**: Select this check box to record application on all MPPs. • **Retention Period**: The number of days to retain the session data. Enter a whole number from 1 to 999. The default is 14.

Categories and Trace Levels section

Performance tracing is a valuable troubleshooting tool, but it can adversely impact Experience Portal system performance if you set all categories to **Finest** on a busy production system. If you need to troubleshoot a particular area, you must set specific categories to **Fine** and examine the resulting output to see if you can locate the issue. If not, set the level to **Finer** and repeat the process. If you still need more data, then set the level to **Finest** and keep a close watch on system resource usage.

Note:

If these fields are not displayed, click the group heading to expand the group.

Field or Radio Button	Description
Off	Sets trace logging for all categories to off.
Fine	Sets trace logging for all categories to fine.
Finer	Sets trace logging for all categories to finer.
Finest	Sets trace logging for all categories to finest.
ASR	The amount of trace logging done on the Automatic Speech Recognition (ASR) server. Select **Off**, **Fine**, **Finer**, or **Finest**.
CCXML Browser	The amount of trace logging done for Call Control eXtensible Markup Language (CCXML). Select **Off**, **Fine**, **Finer**, or **Finest**.
Event Manager	The amount of trace logging for the Event Manager. This component collects events from other MPP processes and sends them to the network log web service on the EPM. Select **Off**, **Fine**, **Finer**, or **Finest**.
Media Endpoint Manager	The amount of trace logging done for the Media End Point Manager. This trace component controls the logging for the media endpoint interface in the MediaManager process. The media endpoint interface controls the RTP (audio, video) flow through the MediaManager and to the external servers. Select **Off**, **Fine**, **Finer**, or **Finest**.

Table continues…

Field or Radio Button	Description
Media Manager	The amount of trace logging done for the Media Manager. This trace component controls the logging for the start and shutdown of the MediaManager process. Select **Off**, **Fine**, **Finer**, or **Finest**.
Media Video Manager	The amount of trace logging done for the Media Video Manager. This trace component controls the logging for the video interface in the MediaManager process. The video interface handles: Select **Off**, **Fine**, **Finer**, or **Finest**.
MPP System Manager	The amount of trace logging done for the MPP System Manager. Select **Off**, **Fine**, **Finer**, or **Finest**.
MRCP	The amount of trace logging done on the speech proxy server. Select **Off**, **Fine**, **Finer**, or **Finest**.
Reporting	The amount of trace logging done for the Call Data Handler (CDH). Select **Off**, **Fine**, **Finer**, or **Finest**.
Session Manager	The amount of trace logging done for the MPP Session Manager. Select **Off**, **Fine**, **Finer**, or **Finest**.
SIP Messages Tracing	The amount of trace logging done for the SIP Messages. Select **Off**, **Fine**, **Finer**, or **Finest**. This component logs the Global Session ID (GSID) in the trace files when you set the tracing level to **Finest**.
Telephony	The amount of trace logging done on the telephony server. Select **Off**, **Fine**, **Finer**, or **Finest**.
Trace Logger	The amount of trace logging done for the Web Service Trace. The Trace Logger uploads the MPP traces requested by the trace client that runs on EPM. This trace component controls the logging for the activities of trace retrieval in the Trace Web Service. Select **Off**, **Fine**, **Finer**, or **Finest**.
TTS	The amount of trace logging done on the Text-to-Speech (TTS) server. Select **Off**, **Fine**, **Finer**, or **Finest**.

Table continues…

Field or Radio Button	Description
Voice Browser Client	The amount of trace logging done for the Avaya Voice Browser (AVB) client. This component connects the Voice eXtensible Markup Language (VoiceXML) interpreter to the MPP. Its logs: • Indicate the progress of VoiceXML execution and any exceptions or errors from VoiceXML documents • Contain the status and errors from platform initialization and interpreter initialization Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser INET	The amount of trace logging done for the AVB INET. This component manages: • Downloading content such as VoiceXML and prompts from the application server • Storing this content in the local VoiceXML interpreter cache Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Interpreter	The amount of trace logging done for the AVB interpreter. This component parses and interprets the VoiceXML commands and controls the flow of the application based on Dual-tone multi-frequency (DTMF) or recognition results. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Java Script Interface	The amount of trace logging done for the AVB Javascript Interface. This component perform the ECMAScript execution from the VoiceXML documents. Its logs contain the status of script execution and any ECMAScript semantic errors. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Object	The amount of trace logging done for the AVB. This component is the interface to the platform module that performs VoiceXML element execution. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Platform	The amount of trace logging done for the AVB. This component handles messages from the MPP `vxmlmgr` process, the wrapper for the VoiceXML interpreter. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Prompt	The amount of trace logging done for the AVB prompt. This component controls queuing, converting, and playing prompts. Select **Off**, **Fine**, **Finer**, or **Finest**.
Voice Browser Recognition	The amount of trace logging done for the AVB recognition function. This component controls queuing, loading, and unloading grammars. Select **Off**, **Fine**, **Finer**, or **Finest**.

Table continues…

Field or Radio Button	Description
Voice Browser Telephony	The amount of trace logging done for the AVB telephony interface. This component is the interface to the telephony system of the MPP. It handles features such as features as disconnect, blind transfer, and bridge transfer. In addition, its log also contains any channel initialization errors that the system encounters. Select **Off**, **Fine**, **Finer**, or **Finest**.

Restart <MPP Name> Today page field descriptions

Use this page to schedule a one time restart for the MPP.

Field	Description
Restart Today	Indicates that you want the MPP to restart today. When the specified time is reached, the EPM restarts the MPP and clears this check box. The EPM only restarts the MPP again if a regular restart schedule is defined on the Restart Schedule for <MPP Name> page.
Time	After you select the **Restart Today** check box, enter the time at which you want the MPP to restart using a 24 hour clock. For example, to have the MPP restart at midnight, enter `00:00`. To have it restart at 10:30 p.m., enter `22:30`.

Restart Schedule for <MPP Name> page field descriptions

Use this page to set up a restart schedule if you want Experience Portal to periodically stop and then restart the MPP.

Note:

The Restart MPP schedule option is available only on the **MPP Manager** page.

Field	Description
None	If you do not want to set up a schedule for restarting the MPP, select this button.
Daily at	If you want the MPP to restart each day, select this button and enter the time you want the MPP to restart using the 24 hour time format `hh:mm`. For example, to have the MPP restart at midnight, enter `00:00`. To have it restart at 10:30 p.m., enter `22:30`.

Table continues…

Field	Description
Weekly on	If you want the MPP to restart once a week, select this button, select a day of the week from the drop-down list, and enter the time you want the MPP to restart using the 24 hour time format `hh:mm`.
Monthly on	If you want the MPP to restart once a month, select this button, select a day of the month from the drop-down list, and enter the time you want the MPP to restart using the 24 hour time format `hh:mm`. If you select a day that does not occur in a given month, Experience Portal takes the number of days between the end of the month and the restart date and restarts the MPP that many days into the next month. For example, if you select 31 for this field and there are only 28 days in February, Experience Portal actually restarts the MPP three days after the end of the month, on the 3rd of March. It will restart the MPP again on the 31st of March. Similarly, April only has 30 days, so Experience Portal will restart the MPP on the 1st of May and again on the 31st of May.

<System name> Details tab on the System Monitor page field descriptions

Use this tab for a detailed view of the health and status of the EPM and each MPP in the Experience Portal system named in <*System Name*>. The information on this page refreshes automatically if you leave the browser window open.

Note:

If the EPM server needs to be restarted, Experience Portal displays the message "EPM needs to be restarted." in red text just above the system status table.

Column	Description
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
Zone	The zone where the EPM and the MPP servers are configured.
Server Name	The options are: • The name of the EPM server. Click this name to view the <EPM Name> Details page. • The name of an MPP running on the system. Click this name to view the <MPP name> Details page. • *<EPM Name>/<MPP Name>*, if an MPP resides on the same server as the EPM. Click this name to view the <MPP name> Details page.

Table continues…

Column	Description
Type	The options are: • **EPM**: The Experience Portal Manager • **MPP**: A Media Processing Platform **Tip:** To verify whether the associated server is a primary or auxiliary EPM server, hover the mouse over the EPM field.
Mode	The operational mode of the Media Server. The options are: • **Online**: The Media Server is available. • **Offline**: The Media Server is unavailable and is not being polled by the EPM server. • **Test**: (MPP only) The Media Server is available to handle calls made to one of the defined H.323 maintenance stations. **Tip:** To view the date and time that this mode was first reached, hover the mouse over this column.

Table continues…

Column	Description
State	The operational state of the Media Server. The options are: • **Booting**: The Media Server is in the process of restarting and is not yet ready to take new calls. • **Degraded**: The Media Server is running but it is not functioning at full capacity. • **Error**: The Media Server has encountered a severe problem and cannot recover. • **Halted**: The Media Server is no longer responding to heartbeats because it received a **`Halt`** command. • **Halting**: The Media Server is responding to heartbeats but is not taking new calls. • **Need Configuration**: An Email or SMS processor residing on the Media Server has not yet been configured. • **Need Connections**: No connections (SMPP or HTTP) have been configured or assigned to an Email/SMS processor residing on the Media Server. • **Never Used**: The Media Server has never successfully responded to a heartbeat request. • **Not Installed**: The Media Server is missing files required for heartbeat requests to occur. • **Not Responding**: The Media Server is not responding to heartbeat requests and it has not received a **`Restart`** or **`Halt`** command. • **Partially Running**: (EPM only) The Media Server is in the process of starting up, and not all individual components of the service, for example: Tomcat, SL, ActiveMQ, have come up yet. • **Rebooting**: The Media Server is responding to heartbeats but is not taking new calls. • **Recovering**: The Media Server has encountered a problem and is attempting to recover. • **Restart Needed**: This state is most often reached when the Media Server has encountered a problem that it cannot recover from and it requires a manual restart. However, it can also appear for an MPP when the EPM software has been upgraded and the MPP software has not. In that case, the state should update automatically when you upgrade the MPP software. • **Running**: The Media Server is responding to heartbeat requests and is accepting new calls. • **Starting**: The Media Server is responding to heartbeats but not taking new calls because it is transitioning from the Stopped state to the Running state. • **Stopped**: The Media Server is responding to heartbeats but is not taking new calls. The Media Server enters this state while it initializes after it restarts or when a **`Stop`** command is received. • **Stopping**: The Media Server is responding to heartbeats but is not taking new calls.

Table continues…

Column	Description
	• **Unknown**: The Media Server is in the Offline mode. **Tip:** To view the date and time that this state was first reached, hover the mouse over this column.
Active Command	This column is displayed if one or more Media Servers are currently in transition from their current state to a new user-requested state. For each transitional Media Server, this column displays the requested, or final, state. For any other Media Servers in the system, this field displays **None**.
Config	The configuration state of the Auxiliary EPM/MPP. The options are: • **Need certificates**: The Primary EPM certificate must be downloaded to the Auxiliary EPM/MPP by running the **`setup_vpms.php`** script on the Auxiliary EPM/MPP. • **Need ports**: The MPP has been configured and is waiting for ports to be assigned. • **None**: The MPP has never been configured. • **OK**: The Auxiliary EPM/MPP is currently operating using the last downloaded configuration. • **Restart needed**: The MPP must be restarted to enable the downloaded configuration. • **Reboot needed**: The MPP must be rebooted to enable the downloaded configuration. • **Upgrade needed**: The Auxiliary EPM must be upgraded to the same version of the software as on the Primary EPM. • **Unknown**: The MPP is either not responding or is in the Offline mode.
Call Capacity	This field displays: • **Current**: The number of calls that can be currently handled by the system. • **Licensed**: The number of licenses allocated to this system. • **Maximum**: The maximum number of simultaneous calls that the MPPs in this system can handle. This value is obtained by adding together the maximum number of calls set for each of the MPPs in the system. **Note:** This value can be larger than the number of licenses allocated to the system, but it should never be smaller. If it is smaller, then some of your licenses will never be used.

Table continues…

Column	Description
Active Calls	This field displays: • **In**: The number of active incoming calls in the system. • **Out**: The number of active outgoing calls in the system. Clicking the number displayed under the **Active Calls In** column displays all the active incoming calls for the media servers. Clicking the number displayed under the **Active Calls Out** column displays all the active outgoing calls for the media servers.
Calls Today	The number of calls handled during the current day.
Alarms	The alarm status indicators for the EPM, each MPP, and the overall Experience Portal system. The options are: • Green: There are no active major or critical alarms • Yellow: There are one or more active minor alarms • Red: There are one or more active major or critical alarms **Tip:** You can click any red or yellow alarm indicator to view the Alarm report for that system.
Summary	The total number of calls based on **Contact Summary** and **Active Calls**. On the Summary line, clicking the number displayed under the **Active Calls In** column displays all the active incoming calls for the media servers. On the Summary line, clicking the number displayed under the **Active Calls Out** column displays all the active outgoing calls for the media servers.

Email, HTML and SMS processors section

Column	Description
Zone	The zone where the Email and SMS processors are configured. The summary reports within a zone are: • **Email Summary**: Summary of the incoming and outgoing email messages in the last 24 hours. • **SMS Summary**: Summary of the incoming and outgoing SMS messages in the last 24 hours. • **HTML Summary**: Summary of the incoming HTML messages in the last 24 hours.
Server Name	The name of the EPM on which the Email, SMS and HTML processors are configured.

Table continues…

Column	Description
Type	The options are: • Email processor • HTML processor • SMS processor
State	The operational state of the email/SMS/HTML processors. The options are: • **Not Running**: The server is either stopped or not started yet. • **Starting**: The server start request is initiated, and is in the process of initialization. • **Running**: The server is up and functional. • **Stopping**: The server shutdown is requested. • **Need Configuration**: The server does not find configuration. • **Need Connections**: The server has configuration but does not have any connections assigned or configured. • **Degraded**: The server has configuration and connections. However, some or all connections are not working. • **Error**: The server data returned has been deemed "stale" (no new data retrieved after a period of 3 minutes), or 2) unexpected return code retrieved from a poll to server. • **Stopped**: The server is stopped.
Usage (Today)	Displays the number of messages processed during the current day. The Summary row also shows the maximum number of messages allowed per day.
Messages (Last 24 hours)	The options are: • Incoming: The number of incoming messages processed in the last 24 hours. • Outgoing: The number of outgoing messages processed in the last 24 hours. **Note:** Clicking on the **Last 24 hours** text, lets the user to change the number of messages displayed for the following time frames: • Last hour • Last 3 hours • Last 6 hours • Last 12 hours • Last 24 hours
Timeline Graph 	Displays a graph icon. Clicking this graph icon displays the number of messages processed in a graphical form.

Summary tab on the System Monitor page field descriptions

Use this tab for a consolidated view of the health and status of the Experience Portal system. The information on this page refreshes automatically if you leave the browser window open.

Note:

If the EPM server needs to be restarted, Experience Portal displays the message "EPM needs to be restarted." in red text just above the system status table.

Column	Description
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
System Name	The name of the Experience Portal system, as specified in the **Avaya Experience Portal Name** field on the EPM Settings page. If your installation consists of multiple Experience Portal systems that share a common external database, this column contains: • The name of the local system that you currently logged into. The **Type** for this system will always be **EP**. • The name of the another Experience Portal system in the shared external database. The **Type** will always be **Remote EP**. Click the system name to log into the EPM web interface for the remote system.
Type	If your installation consists of a single Experience Portal system, the type will always be **EP**. If your installation consists of multiple Experience Portal systems that share a common external database, this column contains: • **EP**: This type indicates that you are currently logged into the EPM for this system. Any system commands you issue will affect this EPM and any media servers assigned to this system. The <System name> Details tab for this system shows the assigned media servers. • **Remote EP**: This type indicates that this is an active Experience Portal system, but it is *not* the system you are currently logged into. To affect the EPM or media servers assigned to a remote system, you must first log into that system by clicking the remote system name in the **System Name** column.

Table continues…

Column	Description
State	Displays the operational state of the Experience Portal system. The options are: • **Active**: This Experience Portal system is updating its information in the database on a regular basis. • **Inactive**: A remote Experience Portal system of **Type** is **Remote EP** is no longer updating information in the shared database. Click the system name to log into the EPM on that system and troubleshoot the problem locally. • **Stale**: It has been over an hour since this Experience Portal system has updated its summary information in the database. Create an Alarm report to view the error messages generated by the system. **Note:** If you are using an external database, the time difference between your Experience Portal systems is too great. For more information, see the *Time Synchronization between external database and EPM servers* topic in the *Troubleshooting Avaya Experience Portal* guide. **Tip:** To view the date and time that this state was first reached and on which it was last changed, hover the mouse over this column.
Call Capacity	This field displays: • **Current**: The number of calls that can be currently handled by the system. • **Licensed**: The number of licenses allocated to this system. • **Maximum**: The maximum number of simultaneous calls that the media servers in this system can handle. This value is obtained by adding together the maximum number of calls set for each of the media servers in the system. This value can be larger than the number of licenses allocated to the system, but it should never be smaller. If it is smaller, then some of your licenses will never be used.
Active Calls	When the number of active calls (In or Out) is greater than zero, the number displayed on the System Monitor is displayed as a link. Clicking on this link takes the user to the Active Calls web page.
Alarms	This field displays one of the following alarm status indicators: • Green: There are no active major or critical alarms • Yellow: There are one or more active minor alarms • Red: There are one or more active major or critical alarms For a system whose **Type** is **EP**, you can click any red or yellow alarm indicator to view an associated Alarm report. To view the alarms for a system whose **Type** is **Remote EP**, you must first log into the remote system by clicking the name in the **System Name** column.

<Media server Name> Configuration History page field descriptions

Use this page to view information about the history of configuration changes for the media server installed on the server.

Column	Description
Time	The date and time the media server configuration change occurred.
Command	A summary of the media server configuration change.
Configuration	Click the link to open or save an XML file with detailed information about media server configuration changes.

Chapter 13: Speech applications in Avaya Experience Portal

Speech applications in Avaya Experience Portal

Speech applications are the “directors” of Avaya Experience Portal system operations. When a caller dials in to the system, the Media Processing Platform (MPP) accesses the appropriate speech application to control the call. From that point on, the speech application directs the flow of the call until the caller hangs up or the application is finished.

Experience Portal systems can have more than one application active and available at a time. The MPP that takes the call accesses the appropriate application based on the Dialed Number Identification Service (DNIS).

Note:

An application does not have to have a DNIS assigned to it. In this case, such an application handles any call that comes in to the system by means of a DNIS that is not assigned to any other application on the system. However, you can only have one such application on the system. If you attempt to configure a second application without a DNIS, the system generates an error.

In addition, if the speech application requires Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) resources, the MPP contacts the appropriate ASR or TTS server through an Media Resource Control Protocol (MRCP) proxy server.

Multiple speech recognition vendor

In earlier releases of Experience Portal , only a single speech vendor type could be utilized during a call. From Release 7.2.2, customers can select multiple speech recognition vendor types for the same call.

The application in Experience Portal can be assigned to more than one speech recognition vendor. Each speech recognition vendor which is assigned to the application, has individual settings for vendor specific parameters such as Languages, and Acquire and Release control.

Applications such as Orchestration Designer or VXML, must specify the speech recognition vendor that must be used when requesting speech recognition. This is accomplished by defining a

new VXML property that must be in the VXML scope wherever recognition grammars are defined. This VXML property instructs Experience Portal to load the grammar on a specific speech recognition vendor, and therefore determines which speech recognition vendor will perform the recognition.

Note:

Only one speech recognition vendor can perform recognition at a time.

Specifying the vendor in multi-vendor applications

Applications can specify the speech recognition vendor by using the following VXML property:

```
<property name="com.avaya.asr.vendor" value="" />
```

The valid values for this property are:

- nuance osr
- loquendo
- googleasr
- dialogflowasr

These values are not case-sensitive. However, ensure that you use white spaces wherever present.

The grammars fail to load if there are any invalid or empty values for this property, or if the vendor specified in this property is not assigned to the application.

Speech grammars:

For speech recognition, the vendor property must be in scope when the VXML interpreter runs any VXML element that represents a speech grammar.

This includes the <grammar>, <option> and <choice> elements. For the complete list of all possible elements that can represent a voice grammar, see the VXML specification.

DTMF grammars:

If remote DTMF processing is enabled on the application, the vendor property must be in scope when the VXML interpreter runs any VXML element that represents a DTMF grammar.

The following are some examples of VXML elements for DTMF. For the complete list of all possible elements that can represent a DTMF grammar, see the VXML specification.

- <choice> element
- <option> element
- <link> element with the dtmf attribute
- DTMF <grammar> element
- <record> element with the ‘dtmfterm’ attribute set to true

If remote DTMF processing is not enabled on the application, then the vendor property is not required for DTMF grammars. In such cases, Experience Portal internally performs DTMF recognition. A speech recognition vendor is not required.

For applications that are configured with a single speech recognition vendor, you do not need to specify the vendor property in VXML.

Note:

These guidelines also apply for all OD applications. The property name and valid values are the same as that of VXML applications. In OD applications, the property is created as an external property.

Application design recommendations

The following table lists the application design recommendations for developing an application that uses multiple speech recognition vendors.

Note:

The term grammar refers to a VXML <grammar> element. It also refers to any VXML element that the VXML interpreter translates to a grammar.

Type	Description	Design recommendation
VXML scope of vendor property	The vendor property, that is in the VXML scope at the time the interpreter runs a grammar, defines which speech recognition vendor the grammar is be loaded on. It defines which speech recognition vendor will perform the recognition. If multiple vendors are in use within the same VXML document, it is possible to accidentally load two grammars on two speech recognition vendors. This is solely dependent on the scope of both the VXML vendor property and the grammars. **Note:** Only one speech recognition vendor can perform recognition at a time. Therefore, loading grammars on multiple vendors simultaneously, results in some grammars not being active during the recognition. This is because the grammars are loaded on another speech recognition vendor.	• Define the vendor property at a document level (in the document scope), where possible. • Define a single recognition vendor property per document. The outcome of this design is that all grammars in a VXML document are loaded on a single speech recognition vendor. Defining the property at the form or field level can complicate the design of the application.

Table continues…

Type	Description	Design recommendation
Application root documents	If the application is designed with an application root document, defining grammars in the application root document introduces complications regarding the following: • The grammars that are currently in scope • The grammars that are currently active • The speech recognition vendor that the grammars are loaded on	If the application root document defines grammars which need to be common across all speech recognition vendors, ensure that these application root grammars are defined for each speech recognition vendor that is used by the application. For example, an application root document defines a common *return* grammar that allows the user to speak a return command that brings them back to the start of the application. The application uses both Nuance and Loquendo speech recognition in different sections and there is a leaf document per recognition vendor. To load and activate the common *return* grammar on both Nuance and Loquendo speech recognition vendors, the grammar must be defined twice in the application root document (per vendor). This can be accomplished by defining a <form> per vendor with the document scope in the application root document. • For Nuance, define a form element containing: - A vendor property of ‘nuance osr’ - The return <grammar> • For Loquendo, define a form element containing: - A vendor property of ‘loqendo’ - The return <grammar>
Event handler documents	Like the application root document, defining grammars in the event handler documents can introduce complications.	If the application defines grammars within event handler documents, ensure that the grammar is defined for all required speech recognition vendors.

Note:

The multiple speech recognition vendor feature does not support the override of the ASR server or ASR languages in CCXML.

Reporting

The speech events in the transcription data of the Session detail record contain the ASR server, where the recognition is performed, and the ASR session ID.

A new event `ASRVendorChange` is added to Transcriptions to identify when a different speech recognition vendor begins recognition on a session.

Call flow example

This call flow example shows how the Experience Portal system interacts with other systems to handle an automated telephone transaction.

1. A caller from the Public Switched Telephone Network (PSTN) dials a telephone number.
2. The PSTN routes the call to the Private Branch Exchange (PBX) associated with that number.
3. Using Voice over IP (VoIP), the PBX breaks the voice data into packets and sends them over the LAN to a Media Processing Platform (MPP) server in the Experience Portal system.
4. The MPP server looks at the Dialed Number Identification Service (DNIS) for the incoming call and uses the configuration information downloaded from the EPM server to match the number to a speech application that has been added to Experience Portal.
5. The MPP starts an Avaya Voice Browser session and passes it the Universal Resource Indicator (URI) specified for the selected speech application.
6. The Avaya Voice Browser contacts the application server and passes it the URI.
7. The application server returns a VoiceXML page to the Avaya Voice Browser.
8. Based on instructions on the VoiceXML page, the MPP uses prerecorded audio files, Text-to-Speech (TTS), or both to play a prompt to start interaction with the caller. For TTS, the MPP establishes a connection to a TTS server and the ASCII text in the speech application is forwarded for processing. The TTS server renders the text as audio output in the form of synthesized speech which the MPP then plays for the caller.

   Note:

   This connection requires one TTS license, which can be released as soon as processing is complete.
9. If the caller responds by:
   - Entering Dual-tone multi-frequency (DTMF) digits, the results can be processed locally by the MPP or passed to the ASR server for remote processing. The administrator selects local or remote DTMF processing when the application is configured. The digits entered are then returned to the application for further action.
   - Speaking, the MPP establishes a connection to an Automatic Speech Recognition (ASR) server and sends the caller's recorded voice response to the ASR server for processing. The ASR server then returns the results to the application for further action.

     Note:

     This connection requires one ASR license, which is *not* released until the entire call is complete.

10. If errors are encountered during the call, how these errors are handled depend on the type of grammar used by the application. If the application grammar is:
    - Dynamic, or In-line, the speech server gets the grammar directly from Experience Portal and any error messages are passed back to Experience Portal.
    - External or static, the speech server asks for the grammar using the URL specified in the application. If the URL points to an application server, the speech server interacts directly with that application server. Because Experience Portal is not involved in this communication, any error messages passed back by the application server may not be passed back to Experience Portal.
11. The application terminates the call when it finishes execution or when the caller hangs up.
12. When the call ends, the PSTN clears the call from the PBX and releases the ASR license if one was required.

Deploying a speech application

About this task

Before you can add a speech application to Experience Portal, you must deploy the speech application to an application server connected to your Experience Portal.

Procedure

1. Create the speech application.

   For design guidelines, see Design for user experience on page 366.

2. Package the application for deployment.

   For more information about packaging applications for deployment on Apache Tomcat or IBM WebSphere, see Tomcat and WebSphere speech application deployment guidelines on page 341.

3. Copy the speech application package file to the application server from which the application will run.

   Security alert:

   Observe appropriate security measures when copying application package files to the application server.

Next steps

Some application server environments require that you take additional steps to deploy the speech application after you copy the application files to the application server. The additional steps might include installing any run-time support files that the application requires. For more information about support files required by your application server, see the documentation for your server.

Tomcat and WebSphere speech application deployment guidelines

You can deploy Orchestration Designer speech applications on a Tomcat or WebSphere application server. If you want to use a different application server, consult your server documentation for deployment requirements.

Supported application servers

- Tomcat versions 7.0, 8.0, 8.5, and 9.0
- Boss Application Server 7
- Websphere 8.5.5 application server - with Java 7 support
- Websphere 8.5 application server - with Java 6 suuport by default, but has Java 7 option – see the Websphere documentation for details
- Websphere 9 application server - with Java 8 support
- Oracle Weblogic 10.3.6, 11g, and 12c

Apache Tomcat deployment guidelines

To deploy a speech application to an Apache Tomcat application server, you must package the application within a standard Web Archive (WAR) file. A WAR file is a compressed set of files, similar to a ZIP file. The WAR file format is specified by the J2EE specification and all J2EE-compliant application servers should support this format. The Tomcat servlet engine is optimized to handle WAR files. For more information about WAR file requirements for speech applications on your Apache Tomcat system, see the documentation for your system.

When you transport the WAR files to your Apache Tomcat application server, copy them to the directory *TomcatHome*\webapps\, where *TomcatHome* is the directory in which your Apache Tomcat application server software is installed.

Then, when you next start Tomcat, Tomcat automatically installs and deploys the application.

Important:

If you are redeploying an existing application, make sure the original application is not running before you deploy the new version on the server. If the original application is running, there could be conflicts with the log files.

IBM WebSphere deployment guidelines

In order to deploy a speech application on an IBM WebSphere or WebSphere Express application server, you must package the application within a standard Enterprise ARchive (EAR) file or Web ARchive (WAR) file with the JDK source level set to 15. These files are compressed sets of files, similar to a ZIP file. IBM WebSphere servlet engines can use either EAR or WAR file formats. For more information about EAR or WAR file requirements for speech applications on your IBM WebSphere system, see the documentation for your system.

When you transport the EAR or WAR files to your IBM WebSphere application server, make note of the directory to which you copy them. Then later, use the WebSphere Administrative Console to actually deploy the application from this location. For more information, see your IBM WebSphere documentation.

Important:

If you are redeploying an existing application, make sure the original application is not running before you deploy the new version on the server. If the original application is running, there could be conflicts with the log files.

Adding a speech application to Experience Portal

Before you begin

Ensure that the:

- Required speech servers are added to the Experience Portal system. For more information, see Speech servers in Avaya Experience Portal on page 428.
- Speech application is deployed to the application server.

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. On the Applications page, click **Add**.
4. On the Add Application page, enter appropriate information, and click **Save**.

Changing speech application settings through Avaya Experience Portal

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. On the Applications page, click the application name in the **Name** column.
4. On the Change Application page, enter appropriate information, and click **Save**.

Viewing speech applications added to the Experience Portal system

Procedure

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

2. On the EPM navigation pane, click **System Configuration** > **Applications**.

   The EPM displays the Applications page, which lists all of the speech applications added to Experience Portal. The options that are displayed on this page depend on your user role.

Deleting speech applications from Avaya Experience Portal

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. On the Applications page, do one of the following:
   - To delete individual applications: Select the check box of the name of the application in the applications table.
   - To delete all applications: Select the check box in the header row of the table, which automatically selects all rows in the applications table.
4. Click **Delete**.
5. **(Optional)** Remove the application from the Application server as well.

Speech application priority

Because you can specify wildcards in the **Called URI** field for an application, you could end up with a situation in which an incoming call could match more than one application. In this case, Experience Portal uses the first application listed on the Applications page to handle an incoming call from that URI. If you want Experience Portal to use a different application for given URI, you must change that application's priority by changing its position in the list.

For example, if you have the following:

Application name	Specified Called URI value
`all_555`	\+1-212-555-xxxx
`1212_specific`	\+1-212-555-1212

When you get a call from 1-212-555-1212, that call matches both applications because of the wildcards specified in `all_555`. If `all_555` is above `1212_specific` in priority, then Experience Portal will always run `all_555` and never run `1212_specific`.

Changing speech application priority

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. On the Applications page, click **Launch Order** .
4. In the Application Launch Order window, click the name of the application whose priority you want to change, and then click one of the following:
   - Up arrow: To move the application up in priority.
   - Down arrow: To move the application down in priority.
5. Click **Save**.

Specifying the default application for inbound calls

About this task

You can specify a default application for Experience Portal to use when the system receives a call from a telephone number that is not associated with any other application.

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. On the Applications page, do one of the following:
   - To add a new application and designate it as the default: Click **Add** and enter the appropriate information in all sections of the Add Application page *except* the **Application Launch** group.
   - To designate an existing application as the default: Click the application name in the **Name** column. The EPM displays the Change Application page.
4. On the Add Application or Change Application page, go to the **Application Launch** group.
5. In the **Type** field, select **Inbound Default** .
6. Click **Save** .

Accessing VoiceXML and CCXML Log tag data through Experience Portal

If you include VoiceXML or CCXML Log tags in an application and you want to view that information in the Experience Portal application reports, you need to make sure that the data is being collected on the MPP and downloaded to the Experience Portal database.

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. To specify that the MPP servers should collect and store Log tag data:
   a. On the EPM navigation pane, click **System Configuration** > **MPP Servers**.
   b. On the MPP Servers page, click **MPP Settings**.
   c. On the MPP Settings page, make sure that the **Enable** check box is checked for the **VoiceXML/CCXML Log Tags** option in the **Record Handling on MPP** group.
   d. Click **Apply**.
3. To download the Log tag data to the Experience Portal database:
   a. From the EPM main menu, select **System Configuration** > **EPM Servers** > **Report Data**.
   b. On the Report Data Configuration page, make sure that the following fields are set to **Yes**:
      - **Download VoiceXML Log Tags**
      - **Download CCXML Log Tags**
   c. Click **Apply**.
4. To view the Log tag data available in the Experience Portal database:
   a. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
   b. From the EPM main menu, select **Reports** > **Standard** or **Reports** > **Application Detail**.
   c. Click **more >>** to expand the **Optional Filters** group.
   d. In the **Activity Type** field, make sure that the check boxes for **VoiceXML Log Tag** and **CCXML Log Tag** are selected.
   e. Click **OK**.

Viewing application transcription data

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **Reports** > **Standard** > **Session Detail** .
3. On the Session Detail page, click the **more >>** link to display the rest of the optional filters.
4. Enter the criteria you want to use for the report.

   Tip:

   If you want to limit the report to those sessions that have transcription information, select **Yes** in the **Session Transcription** field.
5. Click **OK**.

   The EPM displays the Session Detail Report page.
6. Locate the session for which you want to view the transcription data and click the **View Session Details** icon at the end of the appropriate row.

   Experience Portal displays the Session Details page, which shows both the session and transcription data grouped by the information category.

Vendor specific parameters

Users can set vendor specific parameters in VoiceXML applications. Vendor specific parameters can be set for Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with. This is accomplished by defining new VXML properties for ASR and TTS resources that must be in the VXML scope. These properties should specify valid prefixes for ASR and TTS vendor specific parameters which will be set and sent to speech servers. The properties must also be in the scope of all cases where vendor specific parameters are set.

Configuring vendor specific parameters

About this task

Use this procedure to configure vendor specific parameters in VoiceXML applications.

Users can use the following VoiceXML properties to set vendor specific parameters:

- `com.avaya.asr.valid.prefix` - Specifies valid prefixes for ASR vendor specific parameters which are set and sent to ASR speech server.

- `com.avaya.tts.valid.prefix` - Specifies valid prefixes for TTS vendor specific parameters which are set and sent to TTS speech server.

These properties are configured in the `<property>` element with string value in the VoiceXML application scope where the vendor specific parameters are set.

Procedure

1. On the MPP server, do the following to configure valid prefixes for ASR and TTS vendor specific parameters to be used in the VoiceXML application:
   a. Add valid vendor prefixes to `<parameter name="mpp.vendor.valid.prefix.list">` in the `$MPP/config/mppconfig.xml` file.
   b. Restart the MPP server.
2. In the VoiceXML application, do the following:
   a. Specify valid vendor prefixes for ASR and TTS vendor specific parameters.
      - For ASR vendor specific parameters, set the `com.avaya.asr.valid.prefix` property.
      - For TTS vendor Specific parameters, set the `com.avaya.tts.valid.prefix` property.
   b. Set the vendor specific parameters which will be applied and sent to vendor.

Note:

If the `com.avaya.asr.valid.prefix` or `com.avaya.tts.valid.prefix` properties are not configured, all the vendor specific parameters that are specified in the VoiceXML application will be ignored, except the vendor specific parameters which are already supported by the voice browser by default.

```
$MPP/config/mppconfig.xml:

…
<parameter
name="mpp.vendor.valid.prefix.list">swi;com.ibm.voice.server;com.lumenvox</
parameter>
…

VoiceXML application:
<?xml version="1.0" encoding="UTF-8"?>
<vxml xmlns="http://www.w3.org/2001/vxml"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.w3.org/2001/vxml
   http://www.w3.org/TR/voicexml20/vxml.xsd"
   version="2.0">
  <property name="com.avaya.asr.valid.prefix" value="com.lumenvox."/>
  <property name="com.lumenvox.secure_context" value="1"/>
  <form>
  <field name="drink">
     <prompt>Would you like coffee, tea, milk, or nothing?</prompt>
     <grammar src="drink.grxml" type="application/srgs+xml"/>
  </field>
  <block>
     <submit next="http://www.drink.example.com/drink2.asp"/>
  </block>
```

```
 </form>
</vxml>
```

3. In the `$MPP/logs/process/SessMgr` directory, open SessionManager.log and verify that the required vendor specific parameter is sent in MRCP SET-PARAMS request to the vendor.

```
$MPP/logs/process/SessMgr/SessionManager.log:

…

FINEST|MRCP|22977|FileName=mrcpv2/Mrcpv2Connection.cpp,LineNumber=300|~Msg:
Sending: MRCP/2.0 220 SET-PARAMS 3
Channel-Identifier: 47@speechrecog
confidence-threshold: 0.500000
dtmf-term-timeout: 0
input-modes: dtmf voice
logging-tag: ep-pepm-51-2018310121209-1
n-best-list-length: 1
no-input-timeout: 7000
save-waveform: false
sensitivity-level: 0.800000
speech-complete-timeout: 0
speech-language: en-US
speed-vs-accuracy: 0.500000
vendor-specific-parameters: com.lumenvox.secure_context=”1”;
swirec_application_name=”Test”;swirec_company_name="Avaya";swi.rec.logValue=”ANII=
419001|DNIS=60504”
…
```

Nuance call logs and ASR applications

Users can identify the Nuance call logs that are created for each session (call), with the ASR application that is running on Experience Portal.

The Nuance call logs that are created on the Nuance speech server side can be identified with the ASR application by the Call-Id of the SIP incoming call originated for this application.

Note:

This feature supports MRCPv2 ASR sessions and SIP calls only.

Identifying Nuance call log with ASR application

About this task

Use this procedure to identify the Nuance call log with the running ASR application.

Users can use the `mpp.mrcp.pass_callid=true` property to identify the Nuance call log with the running ASR application.

Procedure

1. Log on to the EPM web interface.

2. On the EPM main menu, click **System Configuration** > **Applications**.
3. On the Applications page, click the deployed application whose configuration you want to change.
4. On the Change Application page, do the following to change the configuration of the application:
   a. In the **Speech Parameters** group for **ASR**, add the new property `mpp.mrcp.pass_callid=true` in the **Vendor Parameters** field.
   b. Click **Apply** and **Save**.

The Nuance call log that is created for the selected ASR application has the following filename format:

```
NUAN-$mm-$ss-$host-$hostname_of_EP-ASR-$Call-
ID_of_SIP_incoming_call-LOG
```

Where:

- `$mm` is the number of minutes into the current hour.
- `$ss` is the number of seconds into the current minute.
- `$host` is the name of the host writing the log record.
- `$hostname_of_EP` is the name of the Experience Portal host where the ASR application is running.
- `$Call-ID_of_SIP_incoming_call` is the Call-Id of the SIP incoming call originated for ASR application.

Note:

If `mpp.mrcp.pass_callid` is not configured or set to false, the Nuance call log is created with the default Nuance call log name:

```
NUAN-$mm-$ss-$host-$sid-$appsessionid-LOG
```

Where:

- `$mm` is the number of minutes into the current hour.
- `$ss` is the number of seconds into the current minute.
- `$host` is the name of the host writing the log record.
- `$sid` is the unique session identifier created by the system.
- `$appsessionid` is the unique session identifier created by the application, if one is set.

For example, a SIP incoming call with Call-Id `1094a326dde241e8ac2305056a21888` for the ASR application running on Experience Portal with `ep-pepm-51` as hostname, the Nuance call log `NUAN-$mm-$ss-$host-ep-pepm-51-ASR-1094a326dde241e8ac2305056a21888-LOG` is created on the Nuance speech server side.

Google Speech recognition

Avaya Experience Portal supports Google as a speech recognition engine. Google Cloud Speech-to-Text, which is also referred to as Google Speech, is a cloud-based speech transcription service which transcribes speech into text. It does not perform conventional speech recognition which matches inputted speech to specified intents.

Experience Portal communicates with Google through the Google Cloud Speech-to-Text API's. To use Google Speech, you must create a service account on Google and enable the Google Speech-to-Text API on this account. A speech server with the Google engine type can then be added to Experience Portal specifying the credentials that are provided by Google (JSON format).

By default, Google Speech provides recognition for all the languages that Google supports. There is no language selection within Experience Portal for Google, either for Speech Servers or Application ASR selection.

Google Speech integration with VXML

In Experience Portal, an application (Orchestration Designer or VXML) can request speech recognition from Google by defining a specific VXML grammar. The VXML grammar must have a type attribute of `application/avaya-ep-csr`.

Google Speech does not support standard grammar specifications such as SRGS or SISR.

The content of a VXML grammar for Google Speech is formatted as a CDATA section that encapsulates a JSON string. The JSON contains the properties that are related to this recognition request and are sent to Google through the Google Cloud Speech-to-Text API.

Note:

Only a single JSON string is supported within a grammar when a Speech-to-Text transcription is complete.

The following is an example of a VXML grammar for Google Speech:

```
<grammar mode="voice" type ="application/avaya-ep-csr" xml:lang=”en-us”>
            <![CDATA[
             { "provider": "google", "profanity-filter": false, "chunkSize": 8192,
"phrases": [“work”,”avaya”] }
        ]]>
</grammar>
```

Grammar property definitions for Google

“`provider`” – (Mandatory) The name of the cloud speech recognition provider. Currently there is only one valid value `google`. This is a required property for Experience Portal. It is not a Google property.

“`chunkSize`” – (Optional) The size in bytes of the audio segments that are sent to Google for recognition. In the example above, the 8kb value requests Experience Portal to send 8kb chunks of audio data to Google. This property can be given a default value when adding the Speech Server for Google. Note that changing the default value may influence speech recognition quality.

"profanity-filter" – (Optional) The filter that controls whether inappropriate content should be filtered out by Google. This property can be given a default value when adding the Speech Server for Google.

"phrases" – (Optional) A set of words or phrases that are likely to be spoken. Such a set of words and phrases can be used to customise Speech recognition to a specific context. This property can be given a default value per application. This is accomplished by adding a phrases parameter to the vendor parameters for Google in the application, in the following format:

```
phrases=["work","avaya"]
```

Accessing speech recognition results

The speech recognition results for Google Speech recognition are available in VoiceXML through the shadow variables similar to other speech vendors.

The following is an example of the format of these result variables:

```
application.lastresult$.utterance
```

Google Speech with multiple speech recognition vendors

Google Speech is supported with applications using multiple speech recognition vendors.

For these applications, when defining a grammar for Google Speech recognition, a VXML property `com.avaya.asr.vendor` must be in scope with the value `googleasr`. This ensures that the Google Speech service is used for speech recognition.

As mentioned in the Multiple speech recognition vendor topic, if Google is the only speech recognition vendor in an application, you do not need to specify the vendor VXML property. For more information, see Multiple speech recognition vendor on page 335.

Google Speech with the Acquire and Release resource

The Acquire and Release resource control setting in the application is not configurable for the Google Speech recognition engine.

By default, Google Speech uses the **Acquire and Release as Needed** option. The communication with Google Speech is opened and closed each time a speech recognition attempt is requested.

Licensing

For Google Speech support, Experience Portal has a new Google ASR Connections license. Instances of this license are required to enable speech recognition with Google.

Limitations

The following are the limitations of Google Speech support:

- Google Speech recognition does not support VXML grammars within Event Handler and Application Root documents.
- Only a single VXML grammar for Google Speech can be in VXML scope at any one time within an application.
- Google Speech does not support DTMF recognition. Therefore, a grammar cannot be defined for Google with a mode of `dtmf`. Hence, Google Speech does not support the remote DTMF processing feature of Experience Portal.
- Google Speech does not support standard grammars specifications such as SRGS or SISR.
- Only a single Google account is supported per Experience Portal deployment.
- Unlike grammar specifications such as SRGS, a grammar for Google Speech cannot specify a variable to be assigned the recognition result.
- Google Speech integration supports some of the Generic Speech Recognizer Properties defined in the VoiceXML specification such as confidencelevel, completetimeout, incompletetimeout, and maxspeechtimeout. All other properties such as sensitivity and speedvsaccurracy are not supported with Google Speech recognition.
- Google Speech has a maximum speech silence timeout of 10 seconds. Therefore, any relevant VXML timeout properties that are configured higher than this value will be overridden.

Troubleshooting and recommendations

Ensure that the EPM servers time is synchronized with a public NTP server. This is mandatory for communication with Google. Communication issues arise if there are time differences between Experience Portal and Google.

Ensure that the `speech.google.com` fully qualified domain name can be contacted from the MPP servers.

Ensure that there are no issues communicating with Google. Run the Google Cloud Speech sample application (provided by Google) on the MPP machine. This sample application is available at https://github.com/GoogleCloudPlatform/cpp-docs-samples/blob/master/speech/api/streaming_transcribe_singlethread.cc

Google Dialogflow

Avaya Experience Portal supports full native integration of Google Dialogflow. With this feature, customers can access Cloud AI based automation for voice calls using Experience Portal.

Dialogflow speech recognition extracts intents from customer conversations. Dialogflow then uses these intents to automate processes such as room booking, reservations, and find relevant answers from FAQs. These bots are developed on the Google Cloud platform through https://dialogflow.com/.

Experience Portal provides the telephony gateway and call management functionality to compliment Dialogflow. Avaya Experience Portal streams audio from a caller to Google Dialogflow using the open source gRPC and acts on responses from Dialogflow such as transfer call, collect DTMF, and play audio file/DTMF.

Experience Portal provides out of the box integration with Google Dialogflow for voice applications through a default VXML application on MPP. This is the main interface for integrating Avaya Experience Portal with any Dialogflow bot. No changes are needed to the default Dialogflow application on MPP.

Avaya Experience Portal Dialogflow integration supports the following capabilities:

- Audio streaming between Avaya Experience Portal and Dialogflow
- VXML transfer (bridge, blind, and consultative transfers) and notification of transfer complete or failure (bridge transfers)
- DTMF transfer using feature access codes, such as playing DTMF into call
- DTMF dial pad collection by MPP using TELEPHONY_DTMF event
- SIP Header and avaya-session-telephone session parameters using contexts in Welcome event
- VXML privacy support
- VXML timer support
  - Dialogflow can set no_input_timeout (VXML property: `timeout`) and speech_complete_timeout (VXML Property: `completetimeout`).
- Controlled number of attempts
  - MPP sends NO_INPUT when VXML silence is detected - this is used by the bot to control the number of attempts.
- Fetch audio support
  - Playing audio files for an unspecified amount of time until the follow up event is received from Dialogflow.
- Invalid prompt (No match).
- Barge-in control.
- Playing of pre-recorded prompts.
- Sending call disconnect event (Hangup) to Dialogflow when the caller hangs up.

Integration with Dialogflow for voice applications

In Avaya Experience Portal, an application (Orchestration Designer or VXML) can connect to a Dialogflow bot by using a defined grammar. The VXML grammar must have a type attribute of `application/avaya-ep-csr`.

Google Dialogflow does not support standard grammar specifications such as SRGS or SISR. The content of a VXML grammar for Google Dialogflow is formatted as a CDATA section that encapsulates JSON objects. The JSON contains the properties that are related to this recognition request and are sent to Google using the Dialogflow V2Beta APIs. The JSON is used to send events and context from Avaya Experience Portal to Dialogflow.

The following grammar is an example of the initial grammar sending the Welcome event with `sip-hdrs` and `avaya-session-telephone` context. Here the default language, en-us, is overridden with the language en-gb (key/value pair defined in the JSON object).

```
<grammar mode="voice" type ="application/avaya-ep-csr" xml:lang=”en-us”>
<![CDATA[
     {"provider": "dialogflow_v2beta1",
      "event_input":{"name":"Welcome"},
      "language":"en-gb",
      "contexts":[
          {
              "name":"sip-hdrs", "lifespanCount":1,
              "parameters":
              {
                  "callid":"3ffdc4d6555541e98159050568f34fb",
                  "requestmethod":"INVITE",
                  "requesturi":"sip:2141280@sipccgal.com",
                  "requestversion":"SIP/2.0"
              }
          },
          {
              "name":"avaya-session-telephone", "lifespanCount":1,
              "parameters":
              {
                  "aai":"00FA08000E04E35CA37458;encoding=hex",
                  "ani":"8140971",
                  "callid":"mpp248-EPMPP224SM-1-2019092144217",
                  "dnis":"2141280",
                  "early_media":"false"
              }
          }]
     }
]]>
</grammar>
```

Experience Portal interaction with Dialogflow

Avaya Experience Portal interacts with Dialogflow using defined events and custom payloads.

For more details on how the defined events or custom payloads are used to deliver the bot telephony features, see the AAEP Dialogflow white paper.

Events from Avaya Experience Portal to Dialogflow

Avaya Experience Portal sends the following events to Dialogflow:

AAEP to Dialogflow event	Description
Welcome	The initial event that is sent to Dialogflow containing sip-hdrs and avaya-session-telephone context. `"event_input":{ "name":"Welcome" }`
Hangup	The event that is sent when AAEP detects caller hanging up. `"event_input":{ "name":"Hangup" }`
TELEPHONY_DTMF	When a bot instructs Experience Portal to collect dial pad DTMF, this event is used to send the DTMF collected from Experience Portal to the bot. `"event_input":{ "name":"TELEPHONY_DTMF", "parameters":{ "telephony_dtmf_digits":"590227" } }` Where, `"590227"` is the digits collected by Experience Portal.
TELEPHONY_XFER_COMPLETE	The event that is sent when bridge transfer is finished successfully. This event also contains one of the following reason parameter values: • near_end_disconnect, far_end_disconnect • maxtime_disconnect, network_disconnect `"event_input":{ "name":"TELEPHONY_XFER_COMPLETE", "parameters":{ "reason":"far_end_disconnect" } }`
TELEPHONY_XFER_FAILED	The event that is sent when transfer fails. This event also contains one of the following reason parameter values: • busy • network_busy • noanswer • unknown `"event_input":{ "name":"TELEPHONY_XFER_FAILED", "parameters":{ "reason":"noanswer" } }`

Table continues…

AAEP to Dialogflow event	Description
NO_INPUT	The event that is sent when AAEP detects no input (silence). This event can be used by the bot to implement **number of attempts** functionality. `"event_input":{ "name":"NO_INPUT" }`
Custom followup_event	The event that is specified in the followup_event custom payload sent to AAEP. This event allows AAEP to play music until the bot signals, using this event, to proceed to the next recognition. `"event_input":{ "name":"eventname_of_followup" }` Where, `"eventname_of_followup"` is the followup event specified in custom payload

Custom payloads from Dialogflow to Avaya Experience Portal

Dialogflow sends the following custom payloads to Avaya Experience Portal:

- **telephony_read_dtmf**: Dialogflow instructs AAEP to use this payload for local DTMF detection to detect DTMF entered using dial pad.
- **avaya_telephony**: Dialogflow uses this payload for all other features such as VXML transfer, play WAV file or DTMF into call, control bargein and so on.

Dialogflow to AAEP custom payload	JSON keys	Description
telephony_read_dtmf	max_digits	The payload sent by Dialogflow to collect maximum number of digits. This maps to VXML property: `maxlength`.
	finish_digit	The terminating character one of DTMF_STAR, DTMF_POUND, DTMF_ONE…. This maps to VXML property: `termchar`.
	listen_to_speech	The boolean to control whether audio will be streamed to Dialogflow.
	max_duration	Ignored (no equivalent in VXML)
avaya_telephony	transfer	The payload that is used performs VXML transfer.

Table continues…

Dialogflow to AAEP custom payload	JSON keys	Description
	bargein	The boolean that is used to control bargein. **Note:** If bargein is not specified in custom payload, then the default is to have bargein enabled. However, for usability, the default is changed to disabled for the first intent. This can be overridden by specifying bargein=true in the first intent custom payload.
	reply_audio_uri	The payload that overrides Dialogflow generated audio and play a single or array of wav files.
	no_input_timeout	The payload that specifies the amount of silence time after a prompt is played after which a no input event is thrown in VXML. The default is 7 seconds. This maps to VXML property: `timeout`.
	speech_complete_timeout	The payload that specifies the period of silence required after user speech to determine that speaker has finished talking. The default is 0.25 seconds. This maps to VXML property: `speechtimeout`.
	set_language_code	The payload that is used to change the language to a supported Dialogflow language (IETF language code, en-us, es-es, es-419). This language is used for all interactions after this command. This code needs to match with what you are using in Google Dialogflow.
	private	The payload that enables or disables the VXML privacy feature for processing current responds. This maps to VXML property: `private`

Custom payload examples

This following are examples of some custom payloads sent by Dialogflow to AAEP.

Example of telephony_read_dtmf custom payload

This payload is sent by Dialogflow to collect a maximum of five digits using dial pad only terminating with * (`listen_to_speech` is false).

```
"telephony_read_dtmf": {
        "max_duration": "10s",
        "max_digits": 5,
        "listen_to_speech": false,
        "finish_digit": "DTMF_STAR"
  }
```

Example of avaya_telephony custom payload to play audio files and DTMF

This payload is sent by Dialogflow to instruct AAEP to play three audio files and then play DTMF digits: *991611. The audio files cannot be interrupted by speech (`bargein` is false)

```
"avaya_telephony": {
  "bargein": false,
  "reply_audio_uri": [
     "http://1.2.3.4/prompts/HelloRoomBookingAgent.wav",
     "http://1.2.3.4/prompts/HowCanIHelp.wav",
     "file:///opt/Avaya/EP/MPP/web/misc/dialogflowapp/prompts/test/Test.wav",
     "builtin://senddigit/*991611"
  ]
}
```

Example of avaya_telephony custom payload to perform a VXML transfer

This payload is sent by Dialogflow to instruct AAEP to perform a VXML bridge transfer to 8141270, with SIP headers and AAI data to be sent to the caller through SIP INVITE. The music.wav file will play until the callee answers. The transfer disconnects after 15 seconds if the callee does not answer (`connecttimeout`: 15s). The bridge call disconnects 30 seconds after connecting (`maxtime`: 30s).

```
"avaya_telephony": {
    "transfer": {
          "dest": "tel:1234",
          "type": "bridge",
          "transferaudio": "http://1.2.3.4/prompts/music.wav",
          "connecttimeout": "15s",
          "maxtime": "30s",
          "aai": "FA,2901000246DEE275",
          "sip_headers": {
              "unknownhdr[0].name": "Random",
              "unknownhdr[0].value": "This is an unknown header"
          }
    }
}
```

Dialogflow intent indicating end of conversation

An intent in Dialogflow can be marked as **end of conversation**. If the intent is set to end of conversation, Dialogflow then sets the key/value pair `endInteraction` to True in the Intent object of the response. This key/value pair in the intent response can be checked to see if the conversation with the Dialogflow bot is finished. The out of the box Dialogflow application checks this field to determine when to finish. The Dialogflow ASR resource is released when the `endInteraction` boolean is set to True.

For more details on Dialogflow ASR resources, see Dialogflow with the Acquire and Release resource on page 362.

Out of the box integration with Dialogflow for voice applications

Avaya Experience Portal provides out of the box integration with Google Dialogflow for voice applications via VXML. This is provided through a default VXML application on MPP which is the main interface for integrating with Dialogflow.

This VXML application sends the initial Welcome event and then loops handling responses from Dialogflow that are returned in the recognition result. For example, playing audio responses from Dialogflow, collecting DTMF locally, DTMF transfer and so on. It also checks for endInteraction key/value pair being set to true in the response whereby the def_dialogflow VXML application will exit or return, if it is called as a sub-dialog.

This application named `def_dialogflow.vxml` is located on MPP at `$MPP/web/misc/dialogflowapp`. It is accessed using the following URL:

`http://xx.xx.xx.xx/mpp/misc/dialogflowapp/def_dialogflow.vxml`.

Where, xx.xx.xx.xx is the IP address or FQDN of the MPP server.

If you use the FQDN of the MPP, all the traffic will be served from that MPP, which will break failover. Hence, it is recommended that you use the localhost.

Invoking default VXML application as a sub-dialog

The def_dialogflow.vxml application can be invoked directly or invoked as a VXML sub-dialog.

A sample application is provided on MPP mentioning how this is done. The sample application is called `invoke_def_dialogflow.vxml` and is located on MPP at `$MPP/web/misc/dialogflowapp/test`.

The following parameters must be passed to the default VXML application by the calling VXML application:

```
<param name="calledAsSubDialog" value="true"/>
<param name="sipInfoFromParent" value="session.connection.protocol.sip"/>
```

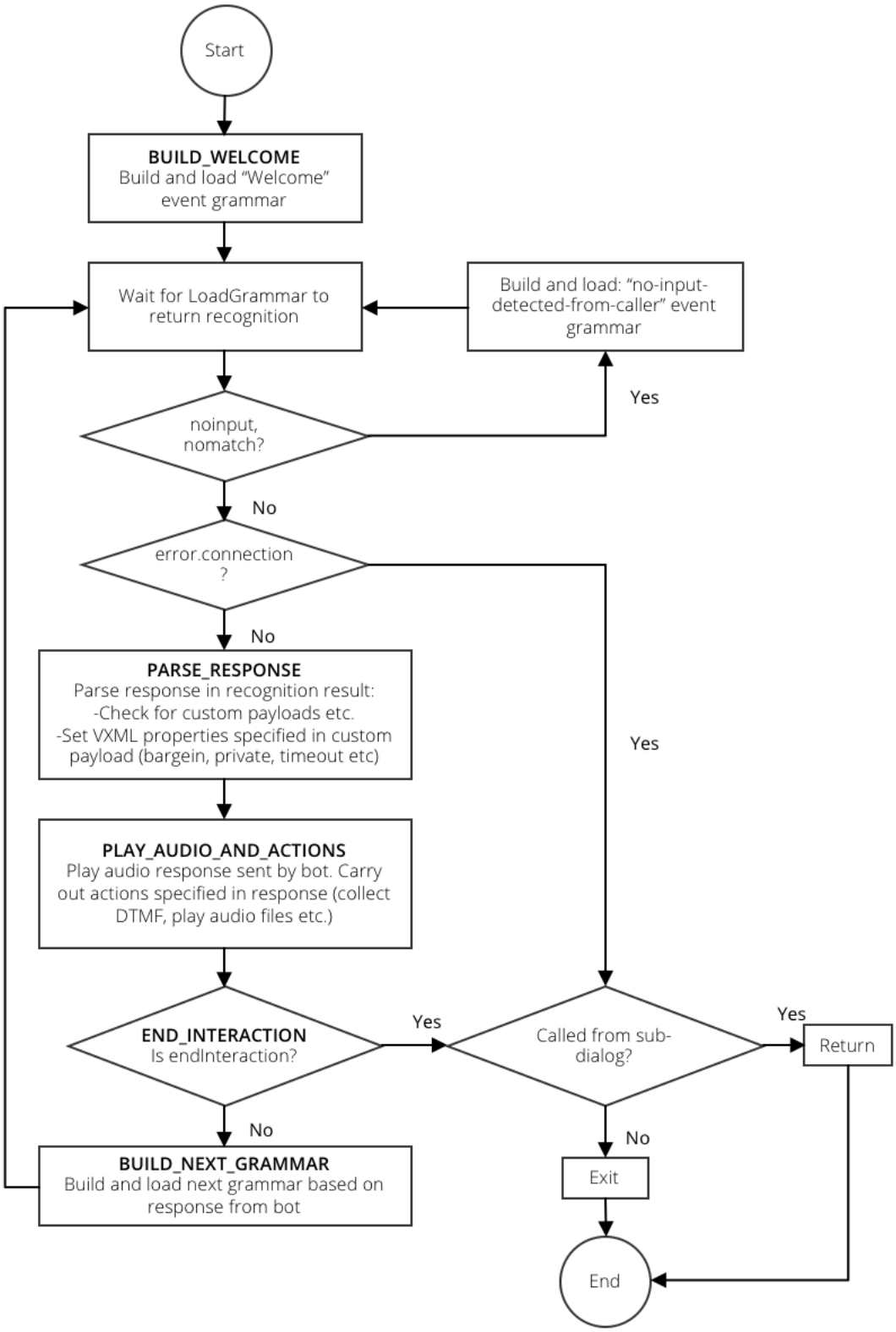
The def_dialogflow.vxml application returns an array of responses received from Google Dialogflow.

Default Dialogflow VXML interaction with Google Dialogflow

This simple bot, which explains the interactions between Experience Portal and Dialogflow bot, does the following:

- Triggers the Welcome intent “Hello, Welcome. Please use dial pad to enter five digits.”
- Instructs Experience Portal to collect five DTMF digits.
- Plays the collected digits back to the user “The digits entered are: 12345” and sets this as the end of conversation.

The following image displays the interaction between `def_dialogflow.vxml` and the Dialogflow bot. It shows that the VXML starts recognition with Dialogflow, and then waits for a response from the Dialogflow bot on what needs to be done.


Start
BUILD_WELCOME
Build and load "Welcome" event grammar
Wait for LoadGrammar to return recognition
Build and load: "no-input-detected-from-caller" event grammar
noinput, nomatch?
Yes
No
error.connection ?
No
Yes
PARSE_RESPONSE
Parse response in recognition result:
-Check for custom payloads etc.
-Set VXML properties specified in custom payload (bargein, private, timeout etc)
PLAY_AUDIO_AND_ACTIONS
Play audio response sent by bot. Carry out actions specified in response (collect DTMF, play audio files etc.)
END_INTERACTION
Is endInteraction?
Yes
Called from sub-dialog?
Yes
Return
No
Exit
No
BUILD_NEXT_GRAMMAR
Build and load next grammar based on response from bot
End

The flow of interactions between Experience Portal and Dialogflow bot consists of the following steps:

1. `BUILD_WELCOME`: Experience Portal sends the Welcome event to the Dialogflow bot.
2. The bot receives the event, triggers the Welcome intent, and responds with the audio: “Hello, Welcome. Please use dial pad to enter five digits”.

   The bot also adds the following custom payload:

   ```
   "telephony_read_dtmf": {
           "max_duration": "10s",
           "max_digits": 5,
           "listen_to_speech": false,
           "finish_digit": "DTMF_STAR"
     }
   ```

3. `PARSE_RESPONSE`: Experience Portal parses the response and determines that the bot has instructed Experience Portal to collect five DTMF digits.
4. `PLAY_AUDIO_AND_ACTIONS`: Experience Portal plays the audio “Hello, Welcome. Please use dial pad to enter five digits” sent back from bot and then sets up local DTMF collection for five digits. Note that Experience Portal also stops sending voice to Dialogflow as `listen_to_speech` is false.
5. The user enters five digits: 590227 followed by *.
6. `BUILD_NEXT_GRAMMAR`: Experience Portal detects DTMF and sends `TELEPHONY_DTMF` event to the bot.

   ```
   “event_input”:{
       “name”:”TELEPHONY_DTMF”,
       “parameters”:{
           “telephony_dtmf_digits”:”590227”
       }
   }
   ```

7. The bot receives the `TELEPHONY_DTMF` event and sends audio to Experience Portal.

   ```
   “Got DTMF via dialpad: #TELEPHONY_DTMF.telephony_dtmf_digits”
   ```

   Note:

   This intent is also marked as End of conversation.

8. `PARSE_RESPONSE` and `PLAY_AUDIO_AND_ACTIONS`: Experience Portal plays the audio sent by the bot “Got DTMF via dialpad 590227”.
9. `END_INTERACTION`: Experience Portal checks if `endInteraction` is set to true.
10. VXML exits or returns (if called as a sub-dialog) to finish the interaction.

Note:

The dialogflowapp directory is overwritten during MPP patch installation and upgrades. If custom changes are required, then the dialogflowapp directory must be copied and changes must be made within this copied directory.

The MPP connects to Dialogflow using a TLS connection on port 443 to FQDN `dialogflow.googleapis.com`

Google Dialogflow with multiple speech recognition vendors

Google Dialogflow is supported with applications using multiple speech recognition vendors.

For these applications, when defining a grammar for Google Dialogflow, a VXML property `com.avaya.asr.vendor` must be in scope with the value `dialogflowasr`. This ensures that the Google Dialogflow service is used for speech recognition.

Licensing

For Google Dialogflow support, Experience Portal has a new Google Dialogflow Connections license. Instances of this license are required to enable Dialogflow connections.

Configuration

Dialogflow is added as a new ASR server Engine Type option for Dialogflow support.

Credentials

Avaya Experience Portal requires credentials to access the Dialogflow bot. These are Google IAM permissions. They are generated as part of the Avaya process to onboard the customer onto the Avaya account. These credentials are generated in Dialogflow.

Credentials can be configured in the application page of Avaya Experience Portal or the Dialogflow ASR server page. Application credentials are used if they are configured, otherwise speech server credentials are used.

Dialogflow credentials can be dynamically updated without the need to restart the MPP. This means the credentials can be changed mid call (in both the application and the speech server) and these new credentials will be used for the next VXML load grammar.

Dialogflow with the Acquire and Release resource

The Acquire and Release resource control setting in the application is not configurable for the Google Dialogflow recognition engine.

By default, Dialogflow uses the **Acquire and Release as Needed** option. The Dialogflow ASR resource is acquired when the first grammar is loaded (to send the Welcome event). The Dialogflow ASR resource is released when AAEP detects an error communicating with Google or when the response from Google contains the JSON intent object with the `endInteraction` key/value pair set to true.

Reporting

Reports with transcriptions and utterances are fully supported for Dialogflow. The ASR Session ID that is displayed is the Google Dialogflow conversation identifier. Speech events display the full JSON response received from Dialogflow. Speech events do not capture the actual audio sent by Dialogflow, however the fulfillmentText entry displays the text form of this audio.

Limitations

The following are the limitations of Google Dialogflow support:

- Google Dialogflow recognition does not support VXML grammars within Event Handler and Application Root documents.
- Only a single VXML grammar for Google Dialogflow can be in VXML scope at any one time within an application.
- Google Dialogflow does not support standard grammars specifications such as SRGS or SISR.
- Experience Portal supports one Google account per application since the credentials are specified there.
- Unlike grammar specifications such as SRGS, a grammar for Google Speech cannot specify a variable to be assigned the recognition result.
- In Dialogflow reporting, def_dialogflow.vxml builds dynamic VXML pages in order to interact with Dialogflow. This means that the VoiceXMLLoad event is listed but does not display the Dynamic VXML.

Troubleshooting and recommendations

- Ensure that there are no issues communicating with Google. The Google Dialogflow project has the proper permissions for the Google CC-AI functionality that is being used.
- Ensure that the EP and MPP servers time is synchronized with a public NTP server. This is mandatory for communication with Google Dialogflow. Communication issues arise if there are time differences between Experience Portal and Google.
- Ensure that the `dialogflow.googleapis.com` fully qualified domain name can be contacted from the MPP servers. This means that the customer's firewalls and proxies are configured to enable connectivity from the MPP to `dialogflow.googleapis.com`.

REST API for key rotation

About this task

From Avaya Experience Portal 7.2.3, cloud ASR customers can rotate credentials using a new REST API. Experience Portal supports rotation on DialogFlow and Google Speech. To ensure safety, Google recommends its customers to shuffle the keys periodically.

Use this procedure to rotate the credentials through the new REST API.

Before you begin

Ensure the following:

- Customers follow the Avaya Experience Portal REST docs to prepare the environment.
- Customers have an administrator account for Google cloud.

Procedure

1. Generate a new key JSON file from Google Cloud control panel.
2. Go to the following URL to complete the REST authorization process:

   `https://BaseURL/EPWebServices/rest/management/asrservers/credentials/<asrName>`.

   Where,

   - `BaseURL` is the default IP address of your main EPM.
   - `<asrName>` is name of the ASR server for which you want to replace the keys.

   Note:

   This REST API only supports Google Speech and DialogFlow ASR servers. Any existing MRCP solution is rejected.

3. Send a PUT call request to the above address with the json request body.

   For example,

```
{
  "credentials": "
{\"type\":\"service_account\",\"project_id\":\"aaep-sample-bot-sv
\",\"private_key_id\":\"36b87603a5abd6764463422c20adfbc43efeb564\",\"private_key
\":\"-----BEGIN PRIVATE KEY-----\\nKEYContent\\n-----END PRIVATE KEY-----\\n
\",\"client_email\":\"dialogflow-vcotni@aaep-sample-bot-sv.iam.gserviceaccount.com
\",\"client_id\":\"107673866867627177364\",\"auth_uri\":\"https://
accounts.google.com/o/oauth2/auth\",\"token_uri\":\"https://oauth2.googleapis.com/
token\",\"auth_provider_x509_cert_url\":\"https://www.googleapis.com/oauth2/v1/
certs\",\"client_x509_cert_url\":\"https://www.googleapis.com/robot/v1/metadata/
x509/dialogflow-vcotni%40aaep-sample-bot-sv.iam.gserviceaccount.com\"}
",
"credentialFileName": "test2.json"
}
```

   The json request body should contain the following mandatory parameters:

   - `credentialFileName`: Any string is fine. This is used to identify a key.

- `Credentials`: Should contain the whole json credential file content download from Google. Ensure that it is transformed so that it can be treated as a string value in json format.

The json request body should have all `"` and `\` escaped to ensure that the json body is processed correctly as a string, and special characters are not misinterpreted or cause a format error.

4. At the prompt, enter your user name and password for authentication.

   You must use the credentials that you use to login to the EPM.

   Note:

   The cloud provider controls the creation and deletion of the key. Avaya Experience Portal only needs to know which key MPP uses. After key rotation, you must still manually disable and delete the key.

Result

On successful completion, customers receive a 200 response containing the request body. If the process fails, customers receive a 400 or 500 response containing the error message used for the debugging.

Speech application design guidelines

Best practices for speech application design

Sound files

High quality stereo sound files may appear to be the perfect way to communicate with your customers, but you must remember that these files will be played over a telephone line which has only 8 KHz bandwidth. Most of the higher frequencies are lost when a recording is played over the telephone.

When you record sound files:

- Record monaural rather than stereo.
- Use 16 bit-depth A-to-D conversion.
- Use a quality audio editing program to normalize the amplitude of your various phrases and convert to mu-LAW or A-LAW PCM.

When you have finished recording, listen to each recording in its final format. If you use the above guidelines, the way they sound at this point will be very close to how they sound over the telephone.

Supported wav file formats

Audio Format	Media Type
Raw (headerless) 8kHz 8-bit mono mu-law [PCM] single channel (G.711)	audio/basic
Raw (headerless) 8kHz 8 bit mono A-law [PCM] single channel (G.711)	audio/x-alaw-basic
WAV (RIFF header) 8kHz 8-bit mono mu-law [PCM] single channel	audio/x-wav
WAV (RIFF header) 8kHz 8-bit mono A-law [PCM] single channel	audio/x-wav
WAV (RIFF header) 8kHz 16-bit mono linear PCM single channel	audio/x-wav

Design for user experience

The best first step in planning an application is to envision exactly what you want the caller to experience when calling in to your system. Do not consider how to set up the application. Simply ask and try to answer as many questions as you can.

For example, ask and try to answer the following questions:

- What options do you want to offer callers?
- Do you want to offer callers the opportunity to interact in more than one language?
- What means do you want to offer callers to respond to options? By voice? By using touchtone keys on the telephone? By recording their answers or other short messages?
- What voice gender do you want to use in presenting your prompts?
- Do you need to use Text-to-Speech (TTS) technology to provide the caller a way to hear text-based information?
- What about hearing- or speech-impaired callers? How do you want to provide for their special needs?

Again, the idea is to ask as many questions as you possibly can. Create sample scenarios for the various situations you think callers might require help with. Try to be as comprehensive as possible.

Design for potential problems

One of the most important steps in planning a good speech application is to plan for any potential problem and error condition you can think of and to include error handlers that can deal with these issues. For example, how should the system respond when one of these problem situations arises?

- Technical or hardware limitations. What if the caller does not have a touchtone telephone? How does your system respond to TTY or TDD requests?
- Accessibility for callers with physical limitations. Have you allowed for the extra time it can take for callers with physical handicaps or other limitations?

- Language limitations. Is it likely that a caller will need to interact using a different language than the primary language? Do you have the necessary Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) servers and software to accommodate them?
- Personal preferences. Have you allowed for the personal preferences of your callers? Some people would rather interact with the system verbally, while others can prefer to use touchtone, or Dual-tone multi-frequency (DTMF) , responses. Other people prefer to interact with a live attendant no matter how good your Interactive Voice Response (IVR) speech application is. How easy is it for such users to get to a live attendant?

If an application encounters an error that is not handled by its own error handlers, or if an application cannot be started due to problems with the application server or the speech servers, Experience Portal uses the error handlers installed on the MPP server. In addition to designing the speech applications, you should also design the error handlers that Experience Portal uses in these cases.

For example, you want your default event handler to:

1. Play a prompt explaining that there was a problem and that the customer is being redirected to an agent immediately.
2. Transfer the call to a special number reserved for such issues.

A call coming in on this special number alerts the agent that the caller has encountered and error in Experience Portal, and that the agent should find out what the customer was doing when the error occurred. The call center can then track these exceptions and fix areas that encounter frequent problems.

For more information, see Experience Portal event handlers on page 367.

Experience Portal event handlers

When a CCXML speech application tries to access an HTML page that cannot be found or a VoiceXML application encounters an unexpected event, the application responds with an exception error message. A well-designed speech application includes exception handlers that deal with these messages and help the application recover so that it can continue processing the call.

Experience Portal uses the error handlers defined in the application whenever possible. However, if an exception error message occurs that is not handled by the application, or if there is a problem running the application due to issues with the application server or the speech servers, Experience Portal uses one of the event handlers installed on the MPP server.

The event handler Experience Portal uses depends on the state of the speech application. If an application:

- Was successfully started and there is a call in progress, Experience Portal uses the event handler associated with that application when it was added to the Experience Portal system.
- Could not be started, Experience Portal looks at the type of application that was requested and uses the appropriate default CCXML or VoiceXML event handler.

When you install the software, Experience Portal automatically installs default event handlers for CCXML and VoiceXML, as well as an event handler prompt that is played by the default event handlers.

To customize the way Experience Portal reacts to a problem, you can add your own event handlers and prompts, and then designate which ones Experience Portal should use as the default. Customers can review and update the messages to match their voice and to say something more user-friendly than *The system is experiencing technical difficulty*.

For example, you want your default event handler to:

1. Play a prompt explaining that there was a problem and that the customer is being redirected to an agent immediately.
2. Transfer the call to a special number reserved for such issues.

A call coming in on this special number alerts the agent that the caller has encountered and error in Experience Portal, and that the agent should find out what the customer was doing when the error occurred. The call center can then track these exceptions and fix areas that encounter frequent problems.

Design for application flow

You have envisioned the experience you want your callers to have. You have tried to foresee and plan for any problem contingency that might arise. Now you are ready to start actually mapping the flow of your speech application. A number of methods can serve you well in this effort, but here are a couple of the more common approaches:

- Describe the flow verbally. Talk through each of your scenarios verbally. Make sure you take note of where the prompts occur and what you want callers to say or do. Record these verbal “walkthroughs”.
- Use a flow diagram. As you work through your scenarios, you can create a flow diagram to show the major points in the call flow. Use this diagram to show such things as:
  - Where you want to offer options to callers
  - Where you want them to listen to the entire prompt and where they can interrupt, or "barge in", and cut the prompt off
  - Where you require a response from callers and what the valid responses will be
  - Where you want or need to access databases to retrieve or record customer data
  - How and where you want to access a Web service to respond to a customer request

Again, the idea is to be as complete and comprehensive as possible. Try and foresee every eventuality, and map how the system will respond.

Design for modularity

When you are planning your speech application, be alert to places where you can reuse parts of the application in two or more places. Then, when designing and building the application, you can create these parts as modules that you can reuse wherever you need that functionality.

If you plan for these modules ahead of time, you can also develop them before developing your main application project file. That way, they are already available when you create your main application.

For example, you might want to collect bank account or credit card numbers from callers at several points in the call flow. You have figured out that it is the same basic process each time you need to collect such numbers. Therefore, you might want to create a speech project module that you can reuse in your master application whenever you need to collect this type of information from callers.

Using this modular approach to application design has several advantages:

- You can "develop once, use many times." This can be a tremendous advantage, especially if you have certain actions or options you want to offer in several places to your callers.
- It is easier to maintain the overall application, even if you are not reusing much of the code. When you use a modular approach, you can change one part of the application without necessarily having to rebuild the entire application.
- It can make it easier to debug your applications, by making it possible to isolate the trouble spots where errors are occurring.

A team of developers can work on separate pieces of an application separately and then merge their efforts.

Design for application resources

As a final step in planning your speech application, you must attempt to identify and list all the application resources you will need to develop the application. Application resources include components such as Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) servers, prerecorded phrases that the system plays back as prompts, and so on.

If you have planned the flow completely, keeping in mind all the resources you will need, you can list those application resources before you actually start to develop the application. Then you can create or import those resources before creating the call flow.

In the case of phrases, for example, if you know exactly what phrases you want to use, and if you plan to have those phrases recorded by a professional talent, you can list all the phrases and have them recorded as WAV files before you start to develop the actual application. Then, when you get to the points in the application where you need the phrases, you can import the prerecorded files.

CCXML and VoiceXML considerations

Keeping CCXML application sessions active until the MPP grace period expires

About this task

When you stop, restart, or halt an MPP, any CCXML application currently running on that MPP is sent a `ccxml.kill` event. This event notifies the application that the MPP is shutting down when the grace period expires.

If you do not define an error handler for this event in your CCXML application, the application exits immediately, even if it still processing a call.

Procedure

To keep the CCXML application active until the grace period has expired or until the application encounters an `</exit>` tag, add the following event handler to your CCXML application:

```
<transition event="ccxml.kill">
<!-- Do nothing.  Platform will kill session
after grace period-->
</transition>
```

Restrictions for dialogs attached to CCXML conference calls

Dialogs attached to conference calls may only play audio or text-to-speech prompts. If an attached dialog attempts to perform speech recognition processing, each attempt will result in a `no resource` error.

If you need speech recognition capabilities, you must attach the dialog to one of the calls that is part of the conference. In this case, however, the dialog can only process the speech that comes from the call to which it is attached.

Speech recognition results and VoiceXML applications

VoiceXML provides shadow variables accessible within a page to access recognition results such as `application.lastresult$`. While this includes a mechanism for presenting multiple possible semantic matches (n-best results whose presence can be determined by inspecting `application.lastresult$.length`), unfortunately the specification does not describe how to present a result that contains multiple interpretations for a given semantic match.

Avaya Experience Portal addresses the issue of a result containing multiple interpretations for a given semantic match by exposing the shadow variable `application.lastresult $.interpretation$`. To test for the presence of multiple interpretations in a result, examine `application.lastresult$.interpretation$.length`.

If the VoiceXML page containing that grammar uses the `maxnbest` property of `2`, then the recognition results arising from a caller saying “star gazer” would be accessed as follows in the VoiceXML specification:

```
application.lastResult$.length              2
application.lastResult$[0].confidence       0.83
application.lastResult$[0].utterance        Stargazer
application.lastResult$[0].interpretation   eyes
application.lastResult$[1].confidence       0.12
application.lastResult$[1].utterance        starchaser
application.lastResult$[1].interpretation   legs
```

Even though the recognition results contain the additional interpretations “look” and “run”, the VoiceXML specification makes no provisions for making those additional interpretations available to the application. To accomplish this, Avaya Experience Portal extends this list of shadow variables as:

```
application.lastResult$[0].interpretation$.length   2
application.lastResult$[0].interpretation$[0]       eyes
application.lastResult$[0].interpretation$[1]       look
application.lastResult$[1].interpretation$.length   2
application.lastResult$[1].interpretation$[0]       legs
application.lastResult$[1].interpretation$[1]       run
```

Privacy feature support for VoiceXML applications

In VoiceXML applications, you can declare a form or field to be private using the following property statement:

```
<property name="private" value="true"/>
```

While a private form or field is executing, Experience Portal does not write any speech recognition results, DTMF results, or TTS strings into the session transcription logs or into any alarms that may be generated during execution. Once the private form or field has finished executing, Experience Portal resumes logging these items as normal.

Note:

If tracing is turned on for the MPP, Experience Portal ignores the privacy property and writes the requested debugging information into the MPP trace logs.

Server Name Indication

The CCXML or VoiceXML browser examines the certificate that the server sends. It compares the name that the server is trying to connect to with the name included in the certificate. If the name matches, the browser continues the connection. Otherwise, it stops the connection.

DTMF digits sending by a VoiceXML application

Experience Portal allows VoiceXML applications to send DTMF digits. This feature is most commonly used when an application running on Experience Portal communicates with an automated system and not with a human being. This is also used when applications communicate with network routing, such as Cisco ICM for "tack back and transfer" applications. Previously, the only way for Experience Portal applications to send DTMF digits was to play an audio file that contained a recording of the digits to be sent.

Example

The following is a sample VoiceXML application that demonstrates how to send the digits 1 2 3 4:

```
<?xml version="1.0" encoding="UTF-8"?>
<vxml version="2.1"
xmlns="http://www.w3.org/2001/vxml"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.w3.org/2001/vxml
http://www.w3.org/TR/2007/REC-voicexml21-20070619/vxml.xsd">
<form>
    <field>
        <prompt>
             <audio src="builtin://senddigit/1234"/>
             </prompt>
         </field>
      </form>
   </vxml>
```

CCXML elements and attributes

Elements	Attributes	Supporting information on Limitations and Extensions
<accept>	• connectionid • hints	For details on each specific instance of the **hints** attribute, see CCXML hints on page 379.
<assign>	• name • expr	If the CCXML compliance flag is set to **true**, the session variables like session* is checked for **read only**.
<cancel>	sendid	
<ccxml>	• version • xml:base • xsi:schemaLocation	For more information on the **xsi:schemaLocation** attribute, visit the following websites: • http://www.w3.org/2002/09/ccxml. • http://www.w3.org/TR/ccxml/ccxml.xsd.
<createcall>	• dest • connectionid • aai • callerid • hints • timeout • joinid • joindirection	For details on each specific instance of the **hints** attribute, see CCXML hints on page 379.

Table continues…

Elements	Attributes	Supporting information on Limitations and Extensions
<createccxml>	• next • namelist • fetchparam • parameters • method • sessionid • timeout • maxage • maxstale • enctype	
<createconference>	• conferenceid • confname • reservedtalkers • reservedlisteners • hints	
<destroyconference>	• conferenceid • hints	
<dialogprepare>	• src • type • namelist • parameters • dialogid • connectionid • conferenceid • mediadirection • maxage • maxstale • enctype • method • hints	For details on each specific instance of the **hints** attribute, see CCXML hints on page 379.

Table continues…

Elements	Attributes	Supporting information on Limitations and Extensions
<dialogstart>	• src • preparedialogid • type • namelist • parameters • dialogid • connectionid • conferenceid • mediadirection • maxage • maxstale • enctype • method • hints	• If the compliance flag is set to **true**, the flag checks if **maxage** is used with **preparedialogid**. In such a case, an error event is generated. • If the compliance flag is set to **true**, the flag checks if **maxstale**is used with **preparedialogid**. In such a case, an error event is generated. • If the compliance flag is set to **true**, the flag checks if **enctype** is used with **preparedialogid**. In such a case, an error event is generated. • If the compliance flag is set to **true**, the flag checks if **method** is used with **preparedialogid**. In such a case, an error event is generated. For details on each specific instance of the **hints** attribute, see CCXML hints on page 379.
<dialogterminate>	• dialogid • immediate • hints	EP does not support the **hints** attribute.
<disconnect>	• connectionid • reason • hints	
<else>		
<elseif>	cond	
<eventprocessor>	statevariables	

Table continues…

Elements	Attributes	Supporting information on Limitations and Extensions
<exit>	• expr • namelist	For EPM reporting, the following namelists are used: • avayaExitReason • avayaExitInfo1 • avayaExitInfo2 • avayaExitInfo5 • avayaExitInfo6 • avayaExitInfo7 • avayaExitInfo8 • avayaExitInfo9 • avayaExitPreferredPath • avayaExitCustomerId • avayaExitTopic
<fetch>	• next • type • namelist • method • fetchid • timeout • maxage • maxstale • timeout • mode	
<goto>	fetchid	
<if>	cond	

Table continues…

Elements	Attributes	Supporting information on Limitations and Extensions
<join>	• id1 • id2 • duplex • hints • entertone • exittone • autoinputgain • autooutputgain • dtmfclamp • toneclamp	For details on each specific instance of the **hints** attribute, see CCXML hints on page 379.
<log>	• label • expr	
<merge>	• connectionid1 • connectionid2 • hints	<Merge> is only supported by SIP, not by H.323.
<meta>	• name • http-equiv • content	
<metadata>		
<move>	• source • event • sessionid	
<redirect>	• connectionid • dest • reason • hints	For details on each specific instance of the **hints** attribute, see CCXML hints on page 379.
<reject>	• connectionid • reason • hints	For details on each specific instance of the **hints** attribute, see CCXML hints on page 379.

Table continues…

Elements	Attributes	Supporting information on Limitations and Extensions
<script>	• src • fetchid • timeout • maxage • maxstale • charset	• If the compliance flag is set to **true**, the src string should not include a single quote. In all other cases, the single quote is required. The following is an example of a noncompliant src string:`<script src="'http://<IP Address>:8080/FetchTestCCXML/jsp/updateaccount.js'"/>` The following is an example of a compliant src string:`script src="'http://<IP Address>:8080/FetchTestCCXML/jsp/updateaccount.js'"/>` • If the compliance flag is set to **true**, the charset string should not include a single quote. In all other cases, the single quote is required. The following is an example of a noncompliant charset string:`<script src=”script_utf_8.es”charset="'UTF-8'"/>` The following is an example of a compliant charset string: `<script src=”script_utf_8.es”charset="'UTF-8"/>`

Table continues…

Elements	Attributes	Supporting information on Limitations and Extensions
<send>	• target • targettype **Note:** The extra Avaya types are: - avaya_platform - avaya_plaform.web_service - SIPEndpoint • sendid • delay • name **Note:** If **name** is avaya.launchresponse, then **status** and **failed_status** can be used. The values for **status** and **failed_status** are: - success - no resource - busy - no answer - invalid telephony uri - network refuse - invalid application uri - appliction server failure - fax detected - network failed before connect - near end disconnect before connect - far end disconnect before connect - transferred before connect	For details on each specific instance of the **hints** attribute, see CCXML hints on page 379.

Table continues…

Elements	Attributes	Supporting information on Limitations and Extensions
	- unknown failure before connect - call disconnected before application started • namelist • hints	
<transition>	• state • event • cond	
<unjoin>	• id1 • id2 • hints	
<var>	• name • expr	

CCXML hints

<accept/>

Hint	Description
hints.enable_call_classification	Has the following values: • true • false Call classification is received in connection.signal events.
hints.call_classification_timeout	Specifies the timeout for call classification in milliseconds. For example, 20000 = 20 seconds.

<createcall/>

To change the ANI of a SIP call, set the callerid field. Hints are not needed. This does not work for H323 as there is no way to change the ANI for H323.

Hint	Description
hints.disable_cdr_logging	Disables CDR Logging on Voice Portal if the value is true.
hints.disable_video	Disables video on Voice Portal if the value is true.

Table continues…

Hint	Description
hints.enable_call_classification	Has the following values: • true • false Call classification is received in connection.signal events.
hints.call_classification_timeout	Specifies the timeout for call classification in milliseconds. For example, 20000 = 20 seconds.
hints.call_classification_recorded_msg_timeout	Specifies the timeout for call classification recorded message in milliseconds. For example, 20000 = 20 seconds. The timer starts after the call progress detects an answering machine greeting. That is the application receives a connection.signal event with the recorded_msg parameter. It is used to limit the amount of time that the call progress waits for the end of the answering machine message. If the timer fires, the application receives a connection.signal event with the session.connection.callprogress value set to timeout. The default is 30 seconds.
hints.sip.from.displayname	Sets the Display Name field in the From: header of the generated INVITE.
hints.sip.to.displayname	Sets the Display Name field in the To: header of the generated INVITE.
hints.sip.call-info	Sets the Call-Info: header in the INVITE.
hints.sip.organization	Sets the Organization: header in the INVITE.
hints.sip.subject	Sets the Subject: header in the INVITE.
hints.sip.priority	Sets the Priority: header in the INVITE.
hints.sip.replaces	Sets the Replaces: header in the INVITE.
hints.sip.x-nt-gslid	Adds a URL parameter named x-nt-gslid to the sip URI in the To: header and request line. This hint is used in propagating a GSLID on transfers and so on.
hints.sip.passertedid.displayname	Sets the Display Name field of the P-Asserted-Identity: header in the INVITE.
hints.sip.passertedid.uri	Sets the URI for the P-Asserted-Identity: header in the INVITE.

Table continues…

Hint	Description

hints.sip.historyinfo	Controls the history info headers in the generated INVITE request.
	`var hints = new Object();`
	`hints.sip = new Object();`
	`hints.sip.historyinfo = new Array();`
	`hints.sip.historyinfo[0] = new Object();`
	`hints.sip.historyinfo[0].user = "5551101";`
	`hints.sip.historyinfo[0].host = "avaya.com";`
	`hints.sip.historyinfo[0].index = "1";`
	`hints.sip.historyinfo[1] = new Object();`
	`hints.sip.historyinfo[1].displayname = "VDN1";`
	`hints.sip.historyinfo[1].user = "5551101";`
	`hints.sip.historyinfo[1].host = "avaya.com";`
	`hints.sip.historyinfo[1].optheader =`
	`"Reason=SIP;cause=302;text=\"Moved Temporarily\"";`
	`hints.sip.historyinfo[1].index = "1.1";`
	`hints.sip.historyinfo[2] = new Object();`
	`hints.sip.historyinfo[2].displayname = "Skill1";`
	`hints.sip.historyinfo[2].user = "5552101";`
	`hints.sip.historyinfo[2].host = "avaya.com";`
	`hints.sip.historyinfo[2].optheader =`
	`"Reason=SIP;cause=480;text=\"Temporarily Unavailable\"";`
	`hints.sip.historyinfo[2].index = "1.2";`

hints.sip.media	Controls whether an RTP stream should be negotiated for the call.
	It is used in SIP call scenarios like Best Service Routing (BSR) polling and call queueing that only require call signaling.
	`// Set media type empty so there is no media (rtp stream)`
	`var hints = new Object();`
	`hints.sip = new Object();`
	`hints.sip.media = new Array();`
	`hints.sip.media[0] = new Object();`
	`hints.sip.media[0].type = "empty";`

hints.sip.unknownhdr	Allows the setting of arbitrary headers in the generated INVITE.
	`var hints = new Object();`
	`hints.sip = new Object();`
	`hints.sip.unknownhdr = new Array();`
	`hints.sip.unknownhdr[0] = new Object();`
	`hints.sip.unknownhdr[0].name = "X-AnyHeader";`
	`hints.sip.unknownhdr[0].value = "Value for header";`

hints.call_classification_connectWhen	Has the following values: • OnConnect • OnProgress
hints.ConnectWhen	Has the following values: • OnConnected • OnProceeding • OnAlerting OnConnected is the default state if not specified. For more details, see ConnectWhen on page 383.

<dialogprepare/> or <dialogstart/>

Hint	Description
hints.ASRRequired	Overrides the setting in VPMS. The value could be true or false.
hints.ASRLanguages	Specifies the language used in ASR. For example, en-US or en-SG. **Note:** Check VPMS on Speech Servers for the list of all languages.

<join/>

Hint	Description
hints.clamp_dtmf_duplex	Blocks DTMF (DTMF clamping) in either full duplex or half duplex direction. It is used only when dtmfclamp join parameter is `true`. Has the following values: • half: Clamps DTMF from id1 to id2, and allows DTMF from id2 to id1. • full: Clamps DTMF in both directions.

The following is an example of using clamp dtmf half duplex:

```
< join id1="confid" id2="agentid" dtmfclamp="'true'" duplex="'full'"
hints="{clamp_dtmf_duplex:'half'}"/>
```

This blocks DTMF from conference to agent, but allows DTMF from agent to conference.

<merge/>

Hint	Description
hints.MergeTimeout	Sets a time limit for the merge to complete, specified in milliseconds. If the underlying REFER w/Replaces operation doesn't complete within the time limit, the merge will fail.
hints.DestinationURI	Sets the URI in the ReferTo: header of the REFER w/Replaces request.

<redirect/>

Hint	Description
hints.ConnectWhen	Contains the following values: • OnConnected • OnProceeding • OnAlerting OnProceeding is the default state if not specified. For more details, see ConnectWhen on page 383.
hints.TransferTimeout	Indicates the time interval of finishing the transfer.

Table continues…

Hint	Description
hints.AAI	Specifies the application to application info. AAI is a string containing data sent to an application on the far-end, available in the session variable session.connection.aai. For details on the <transfer/> element, see VoiceXML elements and attributes on page 385.

<reject/>

Hint	Description
hints.sip.respcode	Sets the numeric value of the SIP status code. This allows the application to override the default of 302.
hints.sip.resptext	Sets the string value of the SIP reason phrase. This allows the application to override the default of Moved Temporarily.

For more details, see Sample method for passing AAI as UUI on page 384.

<send/>

Hint	Description
hints.h323	Specifies H323 call info.
hints.uui	Sets UUI info.
session.connection.protocol.sip.requestmethod	Contains the following values: • info • options • update These three values can be used with targettype "SIPEndpoint" on <send/> to determine the SIP request message.
session.connection.protocol.sip.body[xx].type	Specifies the content type for the multipart message body of the SIP request.
session.connection.protocol.sip.body[xx].msg	Specifies the content for the multipart message body of the SIP request.

For more details, see Sample method for sending a SIP INFO message on page 384.

ConnectWhen

ConnectWhen is a field that indicates when a transfer should be considered complete.

ConnectWhen only works in the redirect tag and when the call that is being redirected is in the connected state. The connected state is where a transfer can be performed.

ConnectWhen contains the following values:

- OnConnected: OnConnected is a supervised transfer, where the transfer is not considered successful until the outgoing call is answered. The ConnectWhen hint will be ignored if it is used in any other context.

- OnProceeding: OnProceeding tells the platform to consider the transfer successful when the outgoing call reaches the proceeding state. The proceeding state is where the switch has accepted the transfer. This is called a blind transfer.
- OnAlerting: OnAlerting tells the platform to consider the transfer successful when the outgoing call reaches the alerting state. The alerting state is where the call rings. This is a transfer to a ringing type operation.

Note:

On createcall, ccxml passes the ConnectWhen hint to Session Manager, however Telephony might ignore it.

Sample method for sending a SIP INFO message

The following is an example for sending a SIP INFO message:

```
<transition event="dialog.exit"  state="in_dialog">
        <log expr="'-- ' + event$.name +' -- [' + state +']'"/>
        <log expr="'   eventdata... \n' + objectToString(event$)"/>
        <!--
         Save return values and log
         -->
        <assign name="dialogresult" expr="event$.values.dialogresult" />
        <assign name="collecteddigits" expr="event$.values.collecteddigits" />
        <log expr="'  dialogresult : ' + dialogresult"/>
        <log expr="'  collecteddigits : ' + collecteddigits"/>
        <if cond="dialogresult == 'CANCEL'">
         <log expr="'User quit application exiting'" />
         <disconnect connectionid="in_connectionid"/>
        </if>

        <!-- Construct a SIP INFO message to send the collected digits -->
        <script>
     var hints = new Object();
     hints.sip = new Object();
     hints.sip.requestmethod = 'INFO';
     hints.sip.body = new Array(1);
     hints.sip.body[0] = new Object();
     hints.sip.body[0].type = 'application/vnd.nortelnetworks.digits';
     hints.sip.body[0].msg = 'p=Digit-Collection\ny=Digits\nd=Digits%3D'+
collecteddigits;
 </script>
 <send name="''" target="in_connectionid" targettype="'SIPEndpoint'" hints="hints"/>

        <log expr="'Program quit application exiting'" />
        <disconnect connectionid="in_connectionid"/>
    </transition>
```

Sample method for passing AAI as UUI

The following is an example for passing AAI as UUI:

```
    <transition state="in_dialog init incoming_sip" event="dialog.transfer">
<var name="dialog_values" expr="event$.values"/>
<assign name="dialog_values.AAI" expr="event$.aai"/>
      <redirect connectionid="main_connectionid" dest="event$.uri"
hints="dialog_values"/>
    </transition>
```

Note:

If the customer is using default.ccxml in a SIP environment, then the hints to pass AAI as UUI will already be applied if using a VXML transfer.

VoiceXML elements and attributes

Tag	Attributes	Available in VoiceXML 2	Available in VoiceXML 2.1	Available in VoiceXML 3.0	Limitation or Extensions, Supporting information
<assign>	• name • expr	Yes	Yes		Supports all attributes.
<audio>	• src • fetchtimeout • fetchhint • maxage • maxstale • expr	Yes	Yes		Supports all other attributes except **fetchhint**.
<block>	• name • expr • cond	Yes	Yes		Supports all attributes.
<catch>	• event • count • cond	Yes	Yes		Supports all attributes.

Table continues…

Tag	Attributes	Available in VoiceXML 2	Available in VoiceXML 2.1	Available in VoiceXML 3.0	Limitation or Extensions, Supporting information
<choice>	• dtmf • accept • next • expr • event • eventexpr • message • messageexpr • fetchaudio • fetchhint • fetchtimeout • maxage • maxstale	Yes	Yes		Supports all attributes except **message**, **messageexpr**, and **fetchhint**.
<clear>	• namelist	Yes	Yes		Supports the **namelist** attribute.
<initial>	• name • expr • cond	Yes	Yes		Supports all attributes.
<disconnect>	• namelist	No	Yes		Supports the **namelist** attribute.
<else>	• name • expr • cond	Yes	Yes		Supports all attributes.
<error>	count cond	Yes	Yes		Supports all attributes.
<exit>	expr namelist	Yes	Yes		Supports all attributes.

Table continues…

Tag	Attributes	Available in VoiceXML 2	Available in VoiceXML 2.1	Available in VoiceXML 3.0	Limitation or Extensions, Supporting information
<field>	• name • expr • cond • type • slot • modal	Yes	Yes		Supports all attributes.
<filled>	• mode • namelist	Yes	Yes		Supports all attributes.
<form>	• id • scope	Yes	Yes		Supports all attributes.
<goto>	• next • expr • nextitem • expritem • fetchaudio • fetchint • fetchtimeout • maxage • maxstale	Yes	Yes		Supports all attributes.

Table continues…

Tag	Attributes	Available in VoiceXML 2	Available in VoiceXML 2.1	Available in VoiceXML 3.0	Limitation or Extensions, Supporting information
<grammar>	• version • xml:lang • mode • root • tag-format • xml:base • src • scope • type • weight • fetchhint • fetchtimeout • maxage • maxstale • srcexpr	Yes	Yes		Supports all attributes except **fetchhint**.
<help>	• count • cond	Yes	Yes		Supports all attributes.
<if> (optional <else> and <elseif> elements)		Yes	Yes		Supports the **if** element.

Table continues…

Tag	Attributes	Available in VoiceXML 2	Available in VoiceXML 2.1	Available in VoiceXML 3.0	Limitation or Extensions, Supporting information
<link>	• next • expr • eventexpr • message • messageexpr • dtmf • fetchaudio • fetchhint • fetchtimeout • maxage • maxstale	Yes	Yes		Supports all attributes except **fetchhint**.
<log>	• label • expr	Yes	Yes		Supports all attributes.
<mark> (an SSML element)	• name • nameexpr • markname • marktime	• name — Yes • nameexpr — No • markname — No • marktime — No	Yes		Supports **name** and **nameexpr** only. **Note:** In VoiceXML 2.0, the ,<mark> element was ignored by VoiceXML platforms.
<media>	• src • srcexpr • clipBegin • clipEnd • repeatDur • repeatCount	No	No	Yes	soundLevel not supported.

Table continues…

Tag	Attributes	Available in VoiceXML 2	Available in VoiceXML 2.1	Available in VoiceXML 3.0	Limitation or Extensions, Supporting information
<menu>	• id • scope • dtmf • accept	Yes	Yes		Supports all attributes.
<meta>	• name • content • http-equiv	Yes	Yes		Currently inactive.
<metadata>	• creator • rights • subject	Yes	Yes		Currently inactive.
<noinput>	• count • cond	Yes	Yes		Supports all attributes.
<nomatch>	• count • cond	Yes	Yes		Supports all attributes.
<object>	• name • expr • cond • classid • codebase • codetype • data • type • archive • fetchhint • fetchtimeout • maxage • maxage	Yes	Yes		Currently inactive.
<option>	• dtmf • accept • value	Yes	Yes		Currently inactive.

Table continues…

Tag	Attributes	Available in VoiceXML 2	Available in VoiceXML 2.1	Available in VoiceXML 3.0	Limitation or Extensions, Supporting information
<param>	• name • expr • value • valuetype • type	Yes	Yes		• Currently inactive — **valuetype** and **type**. • Supports all the other attributes.
<prompt>	• bargein • bargeintype • cond • count • timeout • xml:lang • xml:base	Yes	Yes		Supports all attributes.
<property>	• name • value	Yes	Yes		Supports all attributes.
<record>	• name • expr • cond • modal • beep • maxtime • finalsilence • dtmfterm • type	Yes	Yes		Supports all attributes.
<reprompt>		Yes	Yes		Supports the <reprompt> element.
<return>	• event • eventexpr • message • messageexpr • namelist	Yes	Yes		Supports all attributes.

Table continues…

Tag	Attributes	Available in VoiceXML 2	Available in VoiceXML 2.1	Available in VoiceXML 3.0	Limitation or Extensions, Supporting information
<script>	• src • charset • fetchhint • fetchtimeout • maxage • maxstale • srcexpr	• srcexpr — No • Rest of the attributes— Yes	Yes		Supports all attributes except **fetchhint**.
<subdialog>	• name • expr • cond • namelist • srcexpr • method • enctype • fetchaudio • fetchtimeout • maxage • maxstale	Yes	Yes		Supports all attributes.
<submit>	• next • expr • namelist • method • enctype • fetchaudio • fetchhint • fetchtimeout • maxage • maxstale	Yes	Yes		Supports all attributes except **fetchhint**.

Table continues…

Tag	Attributes	Available in VoiceXML 2	Available in VoiceXML 2.1	Available in VoiceXML 3.0	Limitation or Extensions, Supporting information
<throw>	• event • eventexpr • message • messageexpr	Yes	Yes		Supports all attributes.
<transfer>	• name • expr • cond • dest • destexpr • bridge • connecttimeout • maxtime • transferaudio • aai • aaiexpr • type	• type — No • Rest of the attributes — Yes	Yes		Supports all attributes.
<value>	expr	Yes	Yes		Supports the attribute.
<var>	• name • expr	Yes	Yes		Supports all attributes.
<vxml>	• version • xmlns • xml:base • xml:lang_d • application	Yes	Yes		Supports all attributes.

Table continues…

Tag	Attributes	Available in VoiceXML 2	Available in VoiceXML 2.1	Available in VoiceXML 3.0	Limitation or Extensions, Supporting information
<data>	• src • name • srcexpr • method • namelist • enctype • fetchaudio • fetchhint • fetchtimeout • maxage • maxstale	No	Yes		Supports all attributes except fetchhint.
<foreach>	• array • item	No	Yes		Supports all attributes.
<receive>	• fetchaudio • fetchaudioexpr • maxtime • maxtimeexpr	No	No	Yes	Only works from launching the CCXML application to the launched application.

Table continues…

Tag	Attributes	Available in VoiceXML 2	Available in VoiceXML 2.1	Available in VoiceXML 3.0	Limitation or Extensions, Supporting information
<send>	• async • asyncexpr • body • bodyexpr • contenttype • contenttypeexpr • event • eventexpr • fetchaudio • fetchaudioexpr • namelist • timeout • timeoutexpr	No	No	Yes	Only works from launching the CCXML application to the launched application. The target and targetexpr attributes must not be specified.

Call classification in speech applications

Call classification overview

Call classification, or call progress, is a method for determining who or what is on the other end of a call by analyzing the audio stream. When the analysis determines a probable match, the CCXML page receives a `connection.signal` event which contains the result in the `event $.info.callprogress` variable. Depending on the results of the analysis, call classification may continue for the duration of the call. In that case, the CCXML page will may receive multiple `connection.signal` events.

Call classification falls into two categories:

- Tone-based classification. This category has a high degree of accuracy because it is easy for the system to detect busy signals or fax machine signals.
- Speech-based classification. This category as a much lower degree of accuracy because it can be difficult to tell a human being's speech from an answering machine's recorded message.

Experience Portal uses speech-based classification when it detects an amount of energy in a frequency consistent with human speech. When it detects human speech, it differentiates between a live human being and an answering machine based on the length of the utterance. Generally, if a live human being answers, the utterance is relatively short while answering machine greetings are usually much longer.

For example, a live human might just say “Hello.” while an answering machine message might say “Hello. I can't come to the phone right now. Please leave your message after the beep.”

However, some people may answer the phone with a much longer greeting while others have recorded a very short answering machine greeting. In both of these cases, the call classification algorithm will incorrectly identify the call and assume the long greeting is a recorded message while the short greeting is a live human being.

To use call classification in your applications, make sure you design the application so that it takes such mistakes into account.

If you configure Experience Portal system to use H.323 connections and outcall applications, you must have Communication Manager with the SA8874 feature to detect that the call has been answered. Without the SA8874 feature, Experience Portal incorrectly detects that the call is answered even if the call is not answered.

If you configure Experience Portal system to use outcall applications, and want the Experience Portal system to differentiate human vs. answering machine, you require the Enhanced Call Classification license.

Call classification analysis results

When Experience Portal classifies the call, it sends a `connection.signal` event to the CCXML page. This event includes the results of the classification in the `event$.info.callprogress` variable.

Value of `event$.info.callprogress`	Applies to	Description
`start_of_voice`	Outbound calls only	The call is answered and Experience Portal detects a voice on the line. EP determines whether the voice is from a human being or from an answering machine. A `Start_of_voice` classification is followed by either a `live_voice` or `recorded_msg` classification.
`live_voice`	Outbound calls only	The call is probably connected to a human being. No further classifications will be sent for this call.
`busy_tone`	Outbound calls only	A busy tone was received. This is commonly referred to as the “slow busy” tone. No further classifications will be sent for this call.

Table continues…

Value of `event $.info.callprogress`	Applies to	Description
`reorder`	Outbound calls only	A switch error, such as all circuits being busy, has occurred. This is commonly referred to as the “fast busy” tone. No further classifications will be sent for this call.
`sit_tone`	Outbound calls only	A special information tone was received which indicates that the call could not be completed. This is the three frequency tone that is often followed by a spoken message. No further classifications will be sent for this call.
sit_tone_reorder		A call-disposition category for a call processing failure. (Incomplete digits, internal office or feature failure – local office) and (Call failure, no wink or partial digits received – distant office).
sit_tone_vacant		A call-disposition category for a call attempt to an unassigned NPA (numbering plan area) or NXX (Central Office exchange code).
sit_tone_no_circuit		A SIT (special information tone) classification for call attempts that fail to find an available Local/long distance. Service Provider outgoing trunk. (All circuits busy – local office).
sit_tone_ineffective		General misdialing, coin deposit required, or other failure.
sit_tone_intercept		Number changed or disconnected.
`recorded_msg`	Outbound calls only	An answering machine was detected and a recorded message has just started. A `recorded_msg` classification will always be followed by either a `msg_end` or `timeout` classification. No further classifications will be sent for this call.
`msg_end`	Outbound calls only	The end of a recorded message, such as that played by an answering machine, was detected. No further classifications will be sent for this call.
`fax_calling_tone`	Inbound calls only	A fax machine was detected as the initiator of an inbound call. No further classifications will be sent for this call.
`fax_answer_tone`	Outbound calls only	A fax machine was detected as the recipient of an outbound call. No further classifications will be sent for this call.
`ringing`	Outbound calls only	A “ring back” tone was detected. One or more of these classifications may be received by the application, but they are always followed by one of the other applicable classifications.

Table continues…

Value of `event $.info.callprogress`	Applies to	Description
`timeout`	Inbound and outbound calls	The classification algorithm failed to classify the call before the allotted time ran out. By default, the allotted time is 20 seconds (or 20000 milliseconds). The default value can be overridden for outbound calls by setting the `call_classification_timeout` parameter in the `hints` attribute on the `<createcall>` tag to the desired number of milliseconds before call classification analysis should time out. No further classifications will be sent for this call.
`error`	Inbound and outbound calls	An internal error occurred during the classification analysis and the call could not be properly classified. No further classifications will be sent for this call.
`early_media`	Outbound calls only	Early media refers to media that is exchanged before a particular session is accepted by the called user. For example, for outbound calls, the caller ring tone is detected as early_media by call classification.

Call classification for inbound calls

The only call classification provided for inbound calls is the ability to detect an incoming fax. It is extremely difficult to differentiate between a live human being and a recorded message for an incoming call because you cannot assume the initial greeting will be as short for an incoming call as it is for an outgoing call. Therefore, any classification for an incoming call other than `fax_calling_tone` should be treated as if a live human being was detected.

If fax tone is detected when using VoiceXML applications, Experience Portal stops the application and transfers the call to a fax machine.

If fax tone is detected when using CCXML applications, Experience Portal sends the fax_calling_tone event to the application. The call treatment is then decided by the rules which the application designer has configured on the application.

When you add an application to Experience Portal using the EPM web interface, the following parameters in the **Advanced Parameters** group on the Add Application page determine what happens when an incoming fax machine call is detected:

Parameter	Description
Fax Detection Enabled	The options are: • **Yes**: The application should attempt to identify whether the caller is a fax machine and route any fax machine calls to the telephone number specified in **Fax Phone Number**. • **No**: The application should not attempt to identify whether the caller is a fax machine. The default is **No**.
Fax Phone Number	If **Fax Detection Enable** is set to **Yes**, this is the telephone number or URI to which fax machines calls should be routed.

Call classification for outbound calls

Classification of human vs. answering machine for outbound call is done by Experience Portal. The classification is based on the length of the voice energy that is detected after the call is answered. You require the Enhanced Call Classification license on the Experience Portal system to differentiate human vs. answering machine. The classification is done only if the application sends a classification request to Experience Portal.

Note:

In the VoiceXML <TRANSFER> outcall method, the human vs. answering machine classification is never done.

Detection of answer, busy, RNA, and so on classification is done by Communication Manager and not by Experience Portal. Communication Manager needs the SA8874 feature to detect this classification. The detection is done on all outcalls except for blind transfers.

The application designer needs to enable call classification for outbound calls. If the call is going to be invoked by the Application Interface web service `LaunchVXML` method, you can specify the call classification parameters when you invoke the web service, as described in Call classification with the LaunchVXML method on page 672.

Otherwise, the application designer has to set `enable_call_classification=true` in the `hints` attribute of the `<createcall>` tag.

When call classification is enabled, a call will receive one or more `connection.signal` events containing the `event$.info.callprogress` field. This field will have one of the values described in Call classification for outbound calls on page 399.

Note:

Remember that the page may receive `connection.signal` events that do *not* contain the `callprogress` field. It is up to the page to determine if the`callprogress` field exists and to take the appropriate course of action based on the value of this field.

The default timeout for outbound call classification is 20 seconds (or 20000 milliseconds). The default value can be overridden for outbound calls by setting the

`call_classification_timeout` parameter in the `hints` attribute on the `<createcall>` tag to the desired number of milliseconds before call classification analysis should time out.

The following example shows a simple `connection.signal` handler page that first determines whether this is a `connection.signal` event bearing classification data. If it is, the handler assesses the data to determine what action to take. If the classification is `live_voice`, then it returns a status of `success` and the page continues to run. Otherwise, a it returns the failure status `no answer`.

```
<transition event="connection.signal">
    <if cond="typeof(event$.info) != 'undefined'">
        <if cond="typeof(event$.info.callprogress) != 'undefined'">
            <var name="call_classification" expr="event$.info.callprogress"/>
            <var name="status"/>
            <if cond="call_classification == 'live_voice'">
                <assign name="status" expr="'success'"/>
                <send name="'avaya.launchresponse'" targettype="'avaya_platform'"
                        target="session.id" namelist="status"/>
            <else/>
                <assign name="status" expr="'no answer'"/>
                <send name="'avaya.launchresponse'" targettype="'avaya_platform'"
                        target="session.id" namelist="status"/>
            </if>
        </if>
    </if>
</transition>
```

Call classification with the LaunchVXML method

Call classification allows the VoiceXML application to return the appropriate status code based on whether a human, an answering machine, or a fax machine answers an outbound call.

Call classification parameters for the LaunchVXML method

The following call classification name-value pairs can be passed as parameters with the `LaunchVXML` method. For both parameters the default is `false`, which means that you must specify the name-value pair in order to enable the associated functionality.

Name-value pair	Description
`enable_call_classification=true`	This required parameter enables call classification.
`detect_greeting_end=true`	This optional parameter instructs the VoiceXML application to identify the end of a recorded greeting if an answering machine answers the outbound call.
`call_classification_recorded_msg_timeout = in mili secs (e.g. 30000 is 30 sec)`	This Optional parameter is to set wait timeout for “end of recorded greeting”, if an answering machine answers the outbound call. Default is 30 sec.

Table continues…

Name-value pair	Description
`call_classification_connectWhen = ( OnConnect or OnProgress)`	This optional parameter is to start the CPA engine (call classification) on either OnConnect or OnProgress. By default it is set to OnProgress. In case the engine is started before connect, early media will also be captured for call classification.
`call_classification_timeout=value`	This optional parameter indicates how long the call classification function will run if it is unable to determine the classification. The value specified should be in milliseconds. If the value is not provided, the default timeout is 20 sec.
`call_classification_timeout = in mili secs (e.g. 20000 is 20 sec)`	Timeout for outbound call classification from engine. Default is 20 sec.

Call classifications

If you enable call classification, the VoiceXML application sends one of the following classifications to the application server using the query arguments on the URL:

Classification	Description
`live_voice`	If a human being answers the call, the application starts the previously-prepared VoiceXML dialog. **Note:** This is the default classification assigned to the VoiceXML session before the call is placed. If a human being does not answer the call, this classification must be changed.
`recorded_msg`	If the `LaunchVXML` method was invoked with `detect_greeting_end=false` or if the `detect_greeting_end` parameter was not specified and an answering machine answers the call, the application terminates the previously-prepared VoiceXML dialog and starts a new dialog by sending the classification `recorded_msg` to the application server.
`msg_end`	If the `LaunchVXML` method was invoked with `detect_greeting_end=true` and an answering machine answers the call, the application terminates the previously-prepared VoiceXML dialog and starts a new dialog by sending the classification `msg_end` to the application server.
`fax_answer_tone`	If a fax machine answers the call, the application terminates and returns the error code `fax detected (8206)` to the Application Interface web service.
`timeout`	If the VoiceXML application does not send a classification change message to the CCXML page within a given period of time, the CCXML applications assumes that a live person has answered the phone and it starts the previously-prepared VoiceXML dialog.
`*`	All other classifications result in the status code for `no answer ()` being returned the Application Interface web service.

SIP application support

User-to-User Interface (UUI) data passed in SIP headers

When you add an application to Experience Portal using the EPM web interface, you also specify how User-to-User Interface (UUI) information will be passed to the application if it uses a SIP connection using the **Operation Mode** field in the **Advanced Parameters** group on the Add Application page.

The options are:

- Service Provider: Experience Portal passes the UUI data along as a single block to the application without making any attempt to interpret data.

  If you select this option, the application must handle the UUI data on its own.

- Shared UUI: Experience Portal takes the UUI data and parses it into an array of IDs and their corresponding values. It then passes the application both the fully encoded UUI data and the parsed array with only the values still encoded..

  If you select this option, the UUI data must conform to the Avaya UUI specifications listed below.

UUI data format in CCXML applications

For a CCXML application, the UUI data is organized in a tree format. For example:

```
avaya.ucid = '####################'
avaya.uui.mode = "shared uui"
avaya.uui.shared[0].id = "FA"
avaya.uui.shared[0].value = "#################"
avaya.uui.shared[1].id = "BG"
avaya.uui.shared[1].value = "#################"
```

Each connection has its own tree associated with it, and the values for that connection can be accessed using the format `session.connections['`*connection_number*`'].avaya.`*element_name*.

For example, if you want to declare two variables called `ucid` and `mode`, and you wanted to set those variables to be equal to the corresponding values for connection 1234, you would specify:

```
<var name="ucid" expr="session.connections['1234'].avaya.ucid"/>
<var name="mode" expr="session.connections['1234'].avaya.uui.mode"/>
```

UUI data format in VoiceXML applications

In VoiceXML, there is only one active call so the UUI information is organized into a similar tree format and placed into a session variable at the start of the dialog. The tree structure looks like this:

```
session.avaya.ucid
session.avaya.uui.mode
session.avaya.uui.shared[]
```

With the Shared UUI mode, you must send UUI/AAI data as name-value pairs in the following format:

```
<id0>,<value0>;<id1>,<value1>;<id2>,<value2>; ...
```

When you specify the name-value pairs:

- Each name must be set to the hexadecimal encoded ID stored in the `shared[]` array.
- Each value must be set to the encoded value stored in the `shared[]` array.
- Each name in the pair must be separated from its value by a `,` (comma).
- Each name-value pair must be separated from the next name-value pair by a `;` (semi-colon).

For example, if you wanted to send a UCID using UUI/AAI, you might specify: `aai = "FA,2901000246DEE275"`

Universal Call Identifier (UCID) values included in UUI data

The Universal Call Identifier (UCID) is an Avaya-proprietary call identifier used to help correlate call records between different systems. This identifier can either be generated by the Experience Portal MPP server or it can be passed to Experience Portal through an application's SIP headers if the application uses a SIP connection and the application's **Operation Mode** is set to **Shared UUI**.

Note:

If the application uses an H.323 connection, Experience Portal can receive UCID from Communication Manager. This feature is supported in Communication Manager 5.2.

To enable this feature, you need to administer ucid-info on button 10 on the 7434ND stations used by Experience Portal.

A UCID consists of 20 decimal digits in three groups. Before the UCID is added to the UUI data, Experience Portal encodes each group as a hexadecimal value and concatenates the three groups together. The:

- First group of 5 digits represents a 2 byte network node identifier assigned to the Communication Manager. In the UUI data, this group is encoded as 4 hexadecimal digits.
- Second group of 5 digits represents a 2 byte sequence number. This group is encoded as 4 hexadecimal digits.
- Third group of 10 digits represents a 4 byte timestamp. This group is encoded as 6 hexadecimal digits.

For example, the UCID 00001002161192633166 would be encoded as `000100D84716234E`.

When Experience Portal passes the UCID 00001002161192633166 to the application, it would look like this:

```
avaya.ucid = '00001002161192633166'
avaya.uui.mode = 'shared uui'
avaya.uui.shared[0].id = 'FA'
avaya.uui.shared[0].value = '000100D84716234E'
```

Note:

The identifier for the UCID is always 250, which becomes FA in hexadecimal in the UUI `shared[]` array.

Experience Portal application parameters affecting the UUI data

When you add an application to Experience Portal using the EPM web interface, the following parameters in the **Advanced Parameters** group on the Add Application page affect the contents of the SIP UUI data:

Parameter	Description
Generate UCID	The Universal Call Identifier (UCID) is an Avaya-proprietary call identifier used to help correlate call records between different systems. The options are: • **Yes**: If the CM does not pass a UCID to Experience Portal, the MPP server generates a UCID. • **No**: The MPP does not generate a UCID.
Operation Mode	The SIP header for each call can contain User-to-User Interface (UUI) information that the switch can either pass on as a single block or attempt to parse so that the information can be acted on. This field determines how Experience Portal treats the UUI data. The options are: • **Service Provider**: Experience Portal passes the UUI data as a single block to the application without making any attempt to interpret data. If you select this option, the application must handle the UUI data on its own. • **Shared UUI**: Experience Portal takes the UUI data and parses it into an array of IDs and their corresponding values. It then passes the application both the fully encoded UUI data and the parsed array with only the values still encoded. If you select this option, the UUI data must conform to the Avaya UUI specifications described in User-to-User Interface (UUI) data passed in SIP headers on page 402.
Transport UCID in Shared Mode	If **Operation Mode** is set to **Shared UUI** and **Generate UCID** is set to **Yes**, this field determines whether Experience Portal encodes the Experience Portal-generated UCID and adds it to the UUI data for all outbound calls. The default is **No**, which means that a UCID is only passed as part of the UUI information if that UCID was passed to Experience Portal by the application.
Maximum UUI Length	The maximum length of the UUI data that can be passed in the SIP header. If this length is exceeded and Experience Portal generated a UCID for the call, the UCID is removed from the UUI data. If the result still exceeds this value, or if the UCID was passed to Experience Portal by the application, Experience Portal does *not* send any UUI data. Instead, it leaves the entire field blank because it has no way to determine what can be left out.

SIP header support for CCXML and VoiceXML applications

Session Initiation Protocol (SIP) headers can provide additional information about a call that a CCXML or VoiceXML application can use to determine what processing needs to be done for that call. Experience Portal uses a collection of session variables to present this information to the application. However, not all SIP headers are accessible and many accessible headers are read only.

The following table lists the session variables that may accompany an inbound SIP INVITE. In the table, `<sip>` is the variable access string used to access the variables in a particular context. The valid strings are:

Variable access string	Description
`session.connection.protocol.sip`	This access string can be used by either CCXML or VoiceXML applications.
`event$.info.protocol.sip`	This access string can used when variables arrive in the `info` map for a transition. These variables are only valid within the transition in which they arrived.
`session.connections['`*`SessionID`*`'].protocol.sip` where *SessionID* is the session ID.	This access string can be used to retrieve the variables from the connection object in the session variable space. The variables exist between transitions but can be overwritten by new data at any time.

If you want to use a variable in your application, you must use the complete text in your code.

For example, if you want to access the `<sip>.callid` variable in a session with the session ID *1234*, you would code one of the following, depending on the context in which you want to access the variable:

- `session.connection.protocol.sip.callid`
- `event$.info.protocol.sip.callid`
- `session.connections['1234'].protocol.sip.callid`

Session Variable	SIP Header	Notes
<sip>.callid	Call-ID	Uniquely identifies a particular invitation or all registrations of a particular client.
<sip>.contact[array].displayname <sip>.contact[array].uri	Contact	Provides the display name, a URI with URI parameters, and header parameters.

Table continues…

Session Variable	SIP Header	Notes
<sip>.from.displayname <sip>.from.uri <sip>.tag	From	The initiator of the request.
<sip>.historyinfo[array].displayname <sip>.historyinfo[array].user <sip>.historyinfo[array].host <sip>.historyinfo[array].opthheader	History-Info	This field is typically used to inform proxies and User Agent Clients and Servers involved in processing a request about the history or progress of that request.
<sip>.passertedid[array].displayname <sip>.passertedid[array].uri	P-asserted Identity	The verified identity of the user sending the SIP message. This field is typically used among trusted SIP intermediaries to prove that the initial message was sent by an authenticated source.
<sip>.require	Require	The options that the User Agent Client (UAC) expects the User Agent Server (UAS) to support in order to process the request.
<sip>.supported[array].option	Supported	All extensions supported by the UAC or UAS.
<sip>.to.displayname <sip>.to.host <sip>.to.uri <sip>.to.user	To	The logical recipient of the request.
<sip>.unknownhdr[array].name <sip>.unknownhdr[array].value	Unknown	All headers not understood by Avaya Experience Portal are passed to the application through this array.
<sip>.useragent[array]	User-Agent	Contains information about the UAC originating the request.
<sip>.via[array].sentaddr <sip>.via[array].sentport <sip>.via[array].protocol <sip>.via[array].branch	Via	The path taken by the request to this point along with the path that should be followed in routing responses.
<sip>.name		This variable returns “sip” when the SIP protocol is used.
<sip>.version		This variable returns the SIP protocol version when the SIP protocol is used.

Table continues…

Session Variable	SIP Header	Notes
<sip>.requestmethod <sip>.requestversion <sip>.requesturi <sip>.request.user <sip>.request.host <sip>.requestparams[array].name <sip>.requestparams[array].value	“request”	The various components of the request URI (INVITE). For example, this variable includes the parameters, user and host part of the URI, and the request method.
<sip>.respcode		The results of a transaction. The actual contents varies by transaction type.
<sip>.resptext		The results of a transaction. The actual contents varies by transaction type.

Sample VoiceXML page logging SIP headers

The following VoiceXML page logs various SIP headers using the Experience Portal session variables.

```
<?xml version="1.0"?>
<vxml version="2.0" xmlns="http://www.w3.org/2001/vxml" xml:lang="en-us">
<property name="promptgender" value="female"/>
<property name="timeout" value="4s"/>
<property name="maxspeechtimeout" value="15s"/>
 <form id="form0">
  <block>
    <log>session.connection.protocol.sip <value
    expr="session.connection.protocol.sip"/></log>
    <log>session.connection.protocol.name: <value
    expr="session.connection.protocol.name"/></log>
    <log>session.connection.protocol.version: <value
    expr="session.connection.protocol.version"/></log>
    <log>session.connection.protocol.sip.requesturi: <value
    expr="session.connection.protocol.sip.requesturi"/></log>
    <log>session.connection.protocol.sip.requestmethod: <value
    expr="session.connection.protocol.sip.requestmethod"/></log>
    <log>session.connection.protocol.sip.requestversion: <value
    expr="session.connection.protocol.sip.requestversion"/></log>
    <log>session.connection.protocol.sip.request.user: <value
    expr="session.connection.protocol.sip.request.user"/></log>
    <log>session.connection.protocol.sip.request.host: <value
    expr="session.connection.protocol.sip.request.host"/></log>
    <log>session.connection.protocol.sip.requestparams[0].name: <value
    expr="session.connection.protocol.sip.requestparams[0].name"/></log>
    <log>session.connection.protocol.sip.requestparams[0].value: <value
    expr="session.connection.protocol.sip.requestparams[0].value"/></log>
    <log>session.connection.protocol.sip.to.uri: <value
    expr="session.connection.protocol.sip.to.uri"/></log>
    <log>session.connection.protocol.sip.to.displayname: <value
    expr="session.connection.protocol.sip.to.displayname"/></log>
    <log>session.connection.protocol.sip.to.user: <value
```

```
    expr="session.connection.protocol.sip.to.user"/></log>
    <log>session.connection.protocol.sip.to.host: <value
    expr="session.connection.protocol.sip.to.host"/></log>
    <log>session.connection.protocol.sip.from.uri: <value
    expr="session.connection.protocol.sip.from.uri"/></log>
    <log>session.connection.protocol.sip.from.displayname: <value
    expr="session.connection.protocol.sip.from.displayname"/></log>
    <log>session.connection.protocol.sip.from.tag: <value
    expr="session.connection.protocol.sip.from.tag"/></log>
    <log>session.connection.protocol.sip.from.user: <value
    expr="session.connection.protocol.sip.from.user"/></log>
    <log>session.connection.protocol.sip.from.host: <value
    expr="session.connection.protocol.sip.from.host"/></log>
    <log>session.connection.protocol.sip.useragent[0]: <value
    expr="session.connection.protocol.sip.useragent[0]"/></log>
    <log>session.connection.protocol.sip.contact[0].displayname: <value
    expr="session.connection.protocol.sip.contact[0].displayname"/></log>
    <log>session.connection.protocol.sip.contact[0].uri: <value
    expr="session.connection.protocol.sip.contact[0].uri"/></log>
    <log>session.connection.protocol.sip.via[0].sentaddr: <value
    expr="session.connection.protocol.sip.via[0].sentaddr"/></log>
    <log>session.connection.protocol.sip.via[0].protocol: <value
    expr="session.connection.protocol.sip.via[0].protocol"/></log>
    <log>session.connection.protocol.sip.via[0].sentport: <value
    expr="session.connection.protocol.sip.via[0].sentport"/></log>
    <log>session.connection.protocol.sip.via[1].sentaddr: <value
    expr="session.connection.protocol.sip.via[1].sentaddr"/></log>
    <log>session.connection.protocol.sip.via[1].protocol: <value
    expr="session.connection.protocol.sip.via[1].protocol"/></log>
    <log>session.connection.protocol.sip.via[1].sentport: <value
    expr="session.connection.protocol.sip.via[1].sentport"/></log>
    <log>session.connection.protocol.sip.supported: <value
    expr="session.connection.protocol.sip.supported"/></log>
    <log>session.connection.protocol.sip.require: <value
    expr="session.connection.protocol.sip.require"/></log>
  </block>
 </form>
</vxml>
```

Support for unknown headers

If Experience Portal receives an INVITE with a header it does not recognize, it saves the name and value of the header in the `session.connection.protocol.sip.unknownhdr` session variable array.

For example, if Experience Portal receives an INVITE with the following unknown headers:

```
new_header: "helloworld"
another_new_header: "howareyou"
```

Experience Portal adds the following entries to the `session.connection.protocol.sip.unknownhdr` array:

```
session.connection.protocol.sip.unknownhdr.unknownhdr[0].name = "new_header"
session.connection.protocol.sip.unknownhdr.unknownhdr[0].value = "helloworld"
session.connection.protocol.sip.unknownhdr.unknownhdr[1].name = "another_new_header"
session.connection.protocol.sip.unknownhdr.unknownhdr[1].value = "howareyou"
```

RFC 3261 SIP headers

You can set a limited number of SIP headers independently for applications that initiate an outbound call with one of the following:

- A REFER as a result of a blind or consultative transfer
- An INVITE as a result of bridged transfer or a CCXML outbound call

Note:

Not all headers that are available to be set on an INVITE are available to be set on a REFER.

You can set the following headers with the VoiceXML `<property>` element before `<transfer>` element. In the table, `<sip_prop>` represents `AVAYA_SIPHEADER.session.connection.protocol.sip`.

Note:

If you want to set a header in your application, you must use the complete text in your code. For example, code `<sip_prop>.callid` as `AVAYA_SIPHEADER.session.connection.protocol.sip.callid`.

SIP Header	<property>	Notes
Call-Info	<sip_prop>.callinfo	Provides additional information about the source or target of the call, depending on whether it is found in a request or response.
To.displayname	<sip_prop>.to.displayname	Displays the name of the call's target.
From.displayname	<sip_prop>.from.displayname	Displays the name of the call's source.
P-asserted Identity	<sip_prop>.passertedid.displayname <sip_prop>.passertedid.uri	The unique identifier of the source sending the SIP message. This identifier is used for authentication purposes if your SIP configuration requires trusted connections. **Note:** If you define the **P-Asserted-Identity** parameter for the SIP connection through the EPM, Experience Portal ignores any attempt by an application to change this identity.
Subject	<sip_prop>.subject	A summary of the call.
Organization	<sip_prop>.organization	The name of the organization to which the SIP element issuing the request or response belongs.
Priority	<sip_prop>.priority	The priority of the request.

Creating a custom header

Procedure

In the`session.connection.protocol.sip.unknownhdr` session variable array, add a name and value pair.

Example

To create a custom header with the name as `new_header` and value as `mycustomheader`, add the following to the `session.connection.protocol.sip.unknownhdr` array:

```
AVAYA_SIPHEADER.session.connection.protocol.sip.unknownhdr[0].name = "new_header"
AVAYA_SIPHEADER.session.connection.protocol.sip.unknownhdr[0].value = "mycustomheader"
```

Sample VoiceXML page setting SIP headers in a VoiceXML application

The following VoiceXML page sets various SIP headers on a bridged transfer.

```
<?xml version="1.0" ?>
<vxml version="2.0" xmlns="http://www.w3.org/2001/vxml" xml:lang="en-us" >
<form id="form0">
  <property name="AVAYA_SIPHEADER.session.connection.protocol.sip.from.displayname"
   value="kong, king"/>
  <property name="AVAYA_SIPHEADER.session.connection.protocol.sip.to.displayname"
  value="godzilla"/>
  <property
name="AVAYA_SIPHEADER.session.connection.protocol.sip.passertedid.displayname"
  value="authority"/>
  <property name="AVAYA_SIPHEADER.session.connection.protocol.sip.passertedid.uri"
  value="sip:1234@123.321.123.321"/>
  <property name="AVAYA_SIPHEADER.session.connection.protocol.sip.unknownhdr[0].name"
  value="Random"/>
  <property name="AVAYA_SIPHEADER.session.connection.protocol.sip.unknownhdr[0].value"
  value="This is an unknown header"/>
  <transfer name="t1" type="bridge" dest="tel:1234"/>
</form>
</vxml>
```

SIP UPDATE method

The SIP UPDATE method, as per RFC 3311, allows you to update parameters of a session. While a call is in a queue, Experience Portal allows the SIP UPDATE method to update the following parameter of the call:

- User-to-User Interface data

You can send multiple UPDATE messages after the initial INVITE is established and before the final response to the INVITE.

Note:

Experience Portal supports SIP UPDATE method only if the Allow header indicates support.

Sample SIP UPDATE Method

The following is an example of the SIP UPDATE method:

```
Via: SIP/2.0/UDP pc33.<domain_name>.com;branch=<branch id>
;received=<ip_address>
To: <sip: email id>;tag=<tag number>
From: <name>
<sip:email id>;tag= <tag number>
 Call-ID: <call_id>
 CSeq: 63104 OPTIONS
 Contact: <sip: email id>
 Contact: <mailto: email id>
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE
 Accept: application/sdp
 Accept-Encoding: gzip
 Accept-Language: en
 Supported: foo
 Content-Type: application/sdp
 Content-Length: 274
```

Experience Portal event handlers

When a CCXML speech application tries to access an HTML page that cannot be found or a VoiceXML application encounters an unexpected event, the application responds with an exception error message. A well-designed speech application includes exception handlers that deal with these messages and help the application recover so that it can continue processing the call.

Experience Portal uses the error handlers defined in the application whenever possible. However, if an exception error message occurs that is not handled by the application, or if there is a problem running the application due to issues with the application server or the speech servers, Experience Portal uses one of the event handlers installed on the MPP server.

The event handler Experience Portal uses depends on the state of the speech application. If an application:

- Was successfully started and there is a call in progress, Experience Portal uses the event handler associated with that application when it was added to the Experience Portal system.
- Could not be started, Experience Portallooks at the type of application that was requested and uses the appropriate default CCXML or VoiceXML event handler.

When you install the software, Experience Portal automatically installs default event handlers for CCXML and VoiceXML, as well as an event handler prompt that is played by the default event handlers.

If you want to customize the way Experience Portal reacts to a problem, you can add your own event handlers and prompts and then designate which ones Experience Portal should use as the default.

For example, you want your default event handler to:

1. Play a prompt explaining that there was a problem and that the customer is being redirected to an agent immediately.
2. Transfer the call to a special number reserved for such issues.

A call coming in on this special number alerts the agent that the caller has encountered and error in Experience Portal, and that the agent should find out what the customer was doing when the error occurred. The call center can then track these exceptions and fix areas that encounter frequent problems.

Adding application event handlers and prompts

You can install custom event handlers and prompts that you can use either as the system default or as the event handler for a specific application.

Before you begin

Ensure that you test all event handlers thoroughly before you add them to the system.

Important:

Experience Portal does not validate the code in an uploaded event handler. If the event handler has a syntax error, it will not be detected until Experience Portal tries to use the event handler to process a call.

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** > **EPM Servers**, and then click **Event Handlers**.
3. Do the following to add a VoiceXML event handler:
   a. Go to the VoiceXML tab.
   b. Verify that an event handler with the filename you intend to use does not already exist.

      If you install an event handler with the same filename as an existing event handler, Experience Portal overwrites the old event handler with the new file without requiring confirmation.
   c. Click **Add**.
   d. On the Add VoiceXML Event Handler page, enter the appropriate information and click **Install**.

      You can specify any file with the extension VXML.

4. Do the following to add a CCXML event handler:
    a. Go to the CCXML tab.
    b. Verify that an event handler with the filename you intend to use does not already exist.

       If you install an event handler with the same filename as an existing event handler, Experience Portal overwrites the old event handler with the new file without requiring confirmation.
    c. Click **Add**.
    d. On the Add CCXML Event Handler page, enter the appropriate information and click **Install**.

       You can specify any file with the extension CCXML.
5. Do the following to add an event handler prompt:
    a. Go to the Prompts tab.
    b. Verify that an event handler prompt with the filename you intend to use does not already exist.

       If you install an event handler prompt with the same filename as an existing prompt, Experience Portal overwrites the old prompt with the new file without requiring confirmation.
    c. Click **Add**.
    d. On the Add Event Handler Prompt page, enter the appropriate information and click **Install**.

       You can specify any file with the extension WAV, ALAW, or ULAW. After you add a prompt, it can be used by any of the installed VoiceXML or CCXML event handlers.

Setting the default application event handlers

About this task

If an application encounters a problem and no specific event handler has been associated with that application, you can define a default CCXML and VoiceXML event handler, along with a default event handler prompt.

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **System Configuration** > **EPM Servers** and click **Event Handlers**.
3. To specify the default VoiceXML event handler:
    a. Go to the VXML tab.

b. In the **Default** column, click the **Default** link associated with the VoiceXML handler you want to use as the default.

4. To specify the default CCXML event handler:
   a. Go to the CCXML tab.
   b. In the **Default** column, click the **Default** link associated with the CCXML handler you want to use as the default.

Avaya Voice Browser overview

A voice browser is a web browser that presents an interactive voice user interface to the user. In addition, it typically provides an interface to the PSTN or a PBX. Just as a visual web browser works with HTML pages, a voice browser operates on pages that specify voice dialogues. These pages are usually written in VoiceXML, but other proprietary voice dialogue languages remain in use.

TheAvaya Voice Browser is a VoiceXML interpreter. The Avaya Voice Browser performs the following functions:

- Fetches VoiceXML and ECMA script documents.
- Parses, translates, and stores VoiceXML documents. Stores parsed VoiceXML pages in memory.
- Loads and switches Execution context.
- Loads, activates, and unloads Grammars. Supports SRGS 1.0 and simple JSGF 1.0.
- Browses through VoiceXML elements and interprets them.
- Translates <Prompt> elements to SSML 1.0 format and collects user inputs.
- Reports events (throws exceptions) according to VoiceXML specification.

Setting Avaya Voice Browser options

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** > **MPP Servers**.
3. On the MPP Servers page, click **Browser Settings**.
4. On the AVB Settings page, enter appropriate information, and click **Save**.

AVB-specific VoiceXML events

The Avaya Voice Browser may issue any of the following Experience Portal-specific VoiceXML events:

AVB event name	Description
`error.badfetch.applicationuri`	The targeted application could not be found.
`error.badfetch.baddialog`	The targeted dialog could not be found. For example, it cannot match the specified `<form>` id or `<field>` name.
`error.badfetch.baduri`	A bad URI was encountered during a fetch attempt.
`error.grammar`	An unknown grammar was received from a speech server.
`error.grammar.choice`	An unknown grammar error was received from a speech server while processing a `<choice>` statement.
`error.grammar.inlined`	An unknown grammar was received from a speech server while processing inline grammars for `<field>` or `<link>`.
`error.grammar.option`	An unknown grammar error was received from a speech server while processing an `<option>` statement.
`error.internalerror`	An internal error was encountered.
`error.max_loop_count_exceeded`	The maximum number of document pages allowed for a session has been exceeded. **Note:** This is usually an indication of an infinite loop detected in an application execution path.
`error.noresource.asr`	No ASR resources are currently available.
`error.noresource.tts`	No TTS resources are currently available.
`error.recognition`	An unknown recognition error was received from a speech server.
`error.semantic.ecmascript`	A semantic error was encountered while processing a ECMA script.
`error.semantic.no_event_in_throw`	An empty "event" attribute was encountered. For example, a `<throw>` was defined with no associated event.
`error.semantic.recordparameter`	A semantic error was encountered while processing recording-related parameters.
`error.transfer`	An unknown error was encountered during a transfer attempt.

Browser Settings page field descriptions

Use this page to configure the Browser settings that affect all MPPs in the Experience Portal system.

This page contains the:

- VoiceXML Properties group on page 416
- VoiceXML Browser Properties group on page 418
- CCXML Browser Properties group on page 420

Note:

Click the group heading to expand or collapse the group.

To restore the default settings for all the fields, click **Reset All to Default**.

VoiceXML Properties group

Note:

Most of these default values can be overridden either in the VoiceXML application itself or in the application parameters when you add the application to Experience Portal.

Field	Description
Language	The default application language. The available choices depend on the ASR application languages installed on your Experience Portal system.
Confidence Threshold	The default confidence level below which the ASR engine rejects the input from the caller. This value is mapped to whatever scale the ASR engine uses to compute the confidence level. In the case of ASR engines that use MRCP, this value is mapped in a linear fashion to the range 0 to 100. Enter a number in the range 0.0 to 1.0. The default is 0.5.
Sensitivity Level	How loud an utterance must be for the ASR engine to start speech recognition. The higher the sensitivity level, the lower the input volume required to start speech recognition. This value is mapped to whatever scale the ASR engine uses to compute the sensitivity level for speech recognition. Enter a number in the range 0.0 to 1.0. The default is 0.5.

Table continues…

Field	Description
Speed vs. Accuracy	The balance between speed of recognition and accuracy of recognition. This value is mapped to whatever scale the ASR engine uses to compute the balance between speed and accuracy of recognition. Enter a number in the range 0.0 to 1.0. The default is 0.5. If you are using ASR servers *without* MRCP and want to: • Decrease the time it takes to recognize an utterance at the expense of recognition accuracy, enter a lower number in this field. • Increase the likelihood that an utterance is correctly recognized at the expense of recognition speed, enter a higher number in this field. If you are using ASR servers *with* MRCP and want to: • Decrease the time it takes to recognize an utterance at the expense of recognition accuracy, enter a higher number in this field. • Increase the likelihood that an utterance is correctly recognized at the expense of recognition speed, enter a lower number in this field.
N Best List Length	The maximum number of recognition results that the ASR engine can return. Enter a number in the range 1 to 100. The default is 1.
Fetch Timeout	The maximum number of seconds that the VoiceXML browser should wait for the application server to return the requested page.
Output Modes	Select the output mode for a media track. The options are: • **Audio**—Selects the audio track for playback. • **Video**—Selects the video track for playback. • **Audio/Video**—Selects the audio and video tracks for playback.
Maximum Recording Duration	The maximum recording time allowed. If recording time exceeds the limit, event message containing this information is sent. Enter a number in the range 0 to 65535. The default is 10800.
Alarm Event Interval	The interval, in seconds, that determines the number of times the same type of error is logged to Log Viewer. If the same type of error occurs more than once in the specified interval, the error is logged to Log Viewer only once. This functionality ensures that the number of repetitive errors logged to Log Viewer are reduced. Enter a value in the range 0 to 86,400. The default is 3600.
Maximum Cache Age section	

Table continues…

Field	Description
Document	The maximum length of time that a document can be in the cache before the application considers it to be stale and forces the MPP to download the document again. Enter a whole number of seconds in this field. The default is 3600.
Grammar	The maximum length of time that an utterance can be in the cache before the application considers it to be stale and forces the MPP to download the utterance again. Enter a whole number of seconds in this field. The default is 3600. **Note:** This value is the same as the **Maximum Grammar Cache Age** application parameter, and Experience Portal uses it in conjunction with the **Maximum Grammar Staleness** and **Minimum Grammar Freshness Time** application parameters in order to determine whether to force the MPP to download the utterance again.
Audio	The maximum length of time that an audio file can be in the cache before the application considers it to be stale and forces the MPP to download the audio file again. Enter a whole number of seconds in this field. The default is 3600.
Script	The maximum length of time that a script can be in the cache before the application considers it to be stale and forces the MPP to download the script again. Enter a whole number of seconds in this field. The default is 3600.
Data	The maximum length of time that data can be in the cache before the application considers it to be stale and forces the MPP to download the data again. Enter a whole number of seconds in this field. The default is 3600.

VoiceXML Browser Properties group

Field	Description
Maximum Branches	Maximum number of JavaScript branches for each JavaScript evaluation, that are used to interrupt infinite loops from (possibly malicious) scripts. Enter a value in the range 1 to 999999. The default is 100000.
Cache section	
Total Size	The maximum size for the AVB cache. Once this size is reached, Experience Portal cleans the cache until size specified in the **Low Water** field is reached. The default is 40.
Low Water	The size that you want the AVB cache to be after it is cleaned. The default is 10.

Table continues…

Field	Description
Maximum Entry Size	The maximum individual file size to cache. This field has to be less than **Total Size** value. File that exceeds the size limit is not fetched. Enter a value in the range 0 to 65535. The default is 4 MB.
Entry Expiration Time	You should obtain the lock before reading or writing files in the cache. If the lock is not available, the entry expiration time is used to periodically check its availability. Enter a value in the range 0 to 65535. The default is 5 seconds.
Interpreter section	
Maximum Documents	The maximum number of pages that the AVB can access in a single session. Enter a number between 250 and 10000. The default is 500.
Maximum Execution Context Stack Depth	The maximum number of scripting context threads that can be stored simultaneously in the AVB. Enter a number between 1 and 128. The default is 10. **Tip:** If you set this value too high, your system could run out of memory if the applications initiate an unexpectedly large number of threads. You should specify the highest number of threads that can run simultaneously without seriously taxing the resources available on the MPP server.
Maximum Loop Iterations	Prevents voice browser from entering into an infinite loop while handling VXML events. If number of entries to event handling function exceeds the limit, the application exits. Enter a number between 1 and 2000. The default is 1000.
INET section	
Proxy Server	If your site uses an INET Proxy server, the fully qualified path to the proxy server.
Proxy Port	If your site uses an INET Proxy server, the port number for the proxy server. The default is 8000.

Table continues…

Field	Description
SSL Verify	The options are: • **Yes**: If an application is configured to use https and this option is set to Yes, Experience Portal verifies the connection from the MPP to the application server using the appropriate application certificate. **Important:** If a suitable certificate cannot be found, the connection to the application server will fail and the application will not run. • **No**: Experience Portal does not verify the connection from the MPP to the application server regardless of the specified application protocol.
Connection Persistent	Whether a new connection is established for each HTTP request. The options are: • **Yes**: Same connection is used for each HTTP request. • **No**: A new connection is used for each HTTP request. The default is **Yes**.

CCXML Browser Properties group

Field	Description
Fetch Timeout	The maximum number of seconds that the CCXML browser should wait for the application server to return the requested page. If this time elapses with no response from the application server, the CCXML browser cancels the request and runs the application's default error page. Enter a number between 1 and 65535. The default is 15.
Number of Threads for Asynchronous Fetch	The maximum number of threads that the CCXML browser should use for an asynchronous fetch. Enter a number between 1 and 500. The default is 5.
Maximum Branches	Maximum number of JavaScript branches for each JavaScript evaluation, that are used to interrupt infinite loops from (possibly malicious) scripts. Enter a value in the range 1 to 999999. The default is 100000.

INET and cache Interface

The INET and Cache modules provide the interface for fetching resources from the internet and control the caching scheme based on the configuration of several elements. Attributes of the INET and Cache interface include:

- Supports HTTP, HTTPS and FILE protocols.
- Caches responses to GET requests.
- Supports HTTPS through OpenSSL.
- Supports Cookies to enable sessions in the web server.
- Provides caching based on server caching policy.
- Validates cache based on maxage and maxstale setting in the application.
- Configures cache folder, size and low watermark level.

Cache control mechanisms

There are three basic mechanisms for controlling caches: freshness, validation, and invalidation.

- **Freshness** allows a response to be used without rechecking it on the original server, and can be controlled by both the server and the client. For example, the Expires response header gives a date when the document becomes stale, and the maxage directive tells the cache how many seconds the response is fresh for.
- **Validation** can be used to check whether a cached response is still good after it becomes stale. For example, if the response has a Last-Modified header, a cache can make a conditional request using the If-Modified-Since header to see if it has changed. The ETag (entity tag) mechanism also allows for both strong and weak validation.
- **Invalidation** is usually a side effect of another request that passes through the cache. For example, if a URL associated with a cached response subsequently gets a **POST**, **PUT** or **DELETE** request, the cached response will be invalidated.

ETag Directives

An ETag or entity tag is one of several mechanisms that HTTP provides for cache validation. ETags are used by servers and browsers to validate cached components. ETags enable a client to make conditional requests.

An ETag is an identifier assigned by a web server or a browser to a specific version of a resource. If the resource content ever changes, a new and different ETag is assigned. Used in this manner, ETags are similar to fingerprints and can be compared to determine if two versions of a resource are the same or not.

The use of ETags in the HTTP header is optional.

Avaya Voice Browser supports the use of ETags. For information on disabling ETag directives, see http://www-01.ibm.com/support/docview.wss?uid=swg21566450.

Component details of a request

HTTP Header Setting (Request Headers)

Requests can be made using the GET or POST HTTP method. A **GET** command checks if an updated version of a document exists using the configuration settings to determine whether to fetch the document or use the cached version. A **POST** command forces a new fetch of the document irrespective of the configuration settings and bypasses the Cache Validator step. The header settings can be controlled from within the application (for a given document), at the application server level, and at the ASR speech server level for grammars. Common headers include the following:

- **Host:** Host information.
- **Accept:** Acceptable media types.
- **Referrer:** Referring URL.
- **Connection:** Connection type, persistent or non-persistent, use close for non-persistent.
- **Cache-Control:** maxage, maxstale, no-cache, no-store.
- **Cookie**: If Cookies are enabled.
- **If-Modified-Since:** Last-Modified from pervious fetch (**GET** only).
- **Expect:** Waiting for continue (**POST** only).
- **Content-Length:** Media size that is used to allocate buffer for fetching documents. Memory allocation is done block by block, if not set.
- **Content-Type**: Media type that is used to decide the MIME type of the audio and is set according to the extension/MIME type mapping on the server.

POST requests support multipart or form-data to submit audio to the application server.

Example

```
accept: */*
host: avb-linux.sv.avaya.com:8080
user-agent: AvayaVXI/2.0
referrer: http://avb-linux.sv.avaya.com:8080/test_promptFile.vxml
connection: close
cache-control: max-age=3600
method=GET
protocol=HTTP/1.1
```

URL Parsing

In this step, the protocol, the machine name, the port number, and the absolute path of the requested document is determined. This is setup through the IR or EP Administration interface when deploying the application.

Fetch versus Cache

A fetch will be performed rather than using the cache under the following conditions:

- No maxage configured
- No cache validator present
- Validator has expired (or no expiration time is set)
- An error encountered when reading the cache

The default maxage and maxstale values are configured through the EPM for Experience Portal. The expiration of the cache or the validator is configured on the application server. If expiration is not sent from the application server, the entry expires.

HTTP Header Settings (Response Headers)

- Pragma: no cache — Do not cache
- Cache-Control:
  - no-cache, no-store or private — Do not cache
  - maxage, s-maxage — use the max age given in the header
  - must-revalidate — Do not cache
- Expires:
  - When does this entry expire — no conditional gets before the entry expires
- Last-Modified
- Date

Example

In this example, the expiration date is later than the current date, so the cache entry is still valid and will be used. If the “Expires” header is absent, AVB will send conditional HTTP GET with If-Modified-Since and If-None-Match headers to check if the resources has been updated.

```
HTTP/1.1 200 OK
 Date: Tue, 23 May 2006 22:30:45 GMT
 Server: Apache/2.0.46 (Red Hat)
 Last-Modified: Tue, 28 Feb 2006 17:43:35 GMT
 ETag: "6090ec-29b-5dd53fc0"
 Accept-Ranges: bytes
 Content-Length: 667
 Cache-Control: max-age=86400
 Expires: Wed, 24 May 2006 22:30:45 GMT
 Keep-Alive: timeout=15, max=100
 Connection: Keep-Alive
 Content-Type: text/xml
```

Example

In this example due to the no-cache settings and 0 value for expiration, no entry will be added to the cache for future requests thus forcing a fetch of the document for each request.

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=65F51939A8D2D86E2D31919FFF5A2DED; Path=/pizza
Cache-Control: no-cache
Pragma: no-cache
Expires: 0
```

```
Content-Type: text/xml;charset=UTF-8
Date: Tue, 23 May 2006 23:14:53 GMT
Connection: close
```

Cache Validation

If a document has previously been fetched and the header response information indicates that the document should be cached, the next time this document is requested, a cache entry will be found and evaluated. The cache validation logic is as follows and uses the maxage and maxstale values. These values can be specified for each individual cacheable resource such as document page, prompt and grammar in the application or on the EP and IR systems (defaults are provided). For EP, they are configured through the EPM and on IR, they are configured by editing the defaults.xml file.

Note:

The maxage and maxstale defined for speech grammars are used by speech servers and the speech server can define and override the behavior of the settings.

Freshness Life Time = maxage from header or “Expires” – “Date”

Staleness = Current Age – Freshness Life Time

Must Revalidate = “must-revalidate” from “Cache-Control”

If Current Age > maxage then the document is Expired

If Staleness < 0 then the document is Not Expired

If Must Revalidate is set then the document is treated as Expired

If Staleness is > maxstale then the document has Expired

If No Freshness Life Time is less than or equal to 0 then the document has Expired

Connections

The method of configuring connections impact performance. Persistent connections saves the time spent in parsing the URL and resolves the hostname using DNS. Configurations that use load balancers or any mechanism that changes host name to IP address mapping of application servers may not use persistent connections. Make sure persistent connections works in your environment before utilizing this option.

Persistent versus Non-Persistent

- Persistent connections reuses existing sockets within the same call instance.
- Non-Persistent will open a new socket connection for every request.
- This is configurable at the process level with the default being persistent.
- Persistent mode uses a connection table to get a Connection for a host.
- Persistent and Non-persistent modes resolve host names using DNS and support multiple IPs.

Secured versus Non-Secured

- Based on the protocol specified in the URL (HTTP or HTTPS)
- Trusted client certificates are supported
- OpenSSL is used for Secured Connections

Cookie Support

The AVB supports the use of Cookies as follows:

- Can be enabled and disabled at the process level
- Can not be shared across sessions
- Collects cookies from the server
- Ensures Expires, Domain and Path cookie attribute matches
- Does not match request port number

Example

```
Client requests a document, and receives in the response:
-    Set-Cookie: CUSTOMER=WILE_E_COYOTE; path=/; expires=Wednesday, 09-Nov-99 23:12:40
GMT
When client requests a URL in path "/" on this server, it sends:
-    Cookie: CUSTOMER=WILE_E_COYOTE
Client requests a document, and receives in the response:
Set-Cookie: PART_NUMBER=ROCKET_LAUNCHER_0001; path=/
When client requests a URL in path "/" on this server, it sends:
Cookie: CUSTOMER=WILE_E_COYOTE; PART_NUMBER=ROCKET_LAUNCHER_0001
Client receives:
Set-Cookie: SHIPPING=FEDEX; path=/foo
When client requests a URL in path "/foo" on this server, it sends:
Cookie: CUSTOMER=WILE_E_COYOTE; PART_NUMBER=ROCKET_LAUNCHER_0001; SHIPPING=FEDEX
```

Cache performance factors

There are several factors to consider when making decisions on the configuration settings for a given application or customer environment. These include:

- **Security:** The connections between the Application Server and the AVB (platform) and the Application Server and the server hosting the secured resources must be secure.
- **Persistent Connections:** If you use persistent connections, you save the time spent on parsing the URL and resolving the host name using DNS.

  Note:

  Configurations that use load balancers or any mechanism that changes host name to IP address mapping of application servers may not lend themselves to using persistent connections. So make sure persistent connections work properly in your environment before utilizing this option.
- **Dynamic URLs:** Pages that use dynamic URLs should not be cached.
- **Cache Size:** The browser cache size should be configured to ensure all cacheable files from an application (or set of applications) can be stored in the cache. The number and size of cacheable resources will determine the correct size of the cache. The default is set to 40 megabytes and can be configured through the EPM for EP or by editing the defaultsx.cfg file on IR(where x is the VXI instance number). This may need to be adjusted if you are running multiple applications, if the length of the prompts is measured in minutes, or if there are an unusually large number of prompts, pages and grammars in the application. The quickest way to size it is to run through the application (or set of applications that will coreside) a few

times and cover as many application execution paths as possible, and then check the cache folder size.

- **Expiration frequency:** If feasible, a 24–hour or longer expiration timeframe is recommended. The AVB will still use the cached copy if it has exceeded its expiration time by no more than maxstale seconds. A shorter expiration timeframe will cause more conditional GETs to be performed by AVB given the same maxage or maxstale settings. Use the HTTP Expires header to set the expiration time.
- When a load balancer is used it is essential to keep ETags and last modified records the same across all servers, otherwise AVB performs many unnecessary cache updates. The AVB generates f-Match/If-None-Match headers while refreshing a resource with an ETag that was previously retrieved.
- The **POST** method should be used in cases where caching is not useful to prevent unnecessary overhead.
- Understand the default and tunable parameters for your application server. For example, Tomcat does not set the HTTP Expires header for static files such as audio files and grammar files. The absence of the HTTP Expires header will force the browser to do a conditional get to the server on every access to the static file. It is possible to use Tomcat in combination with an http server, such as Apache or IIS, which then allows the server to generate the HTTP Expires header setting.

Using a secure connection between the MPP and the application server

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. For each application that you want to use as a secure connection, verify that the URL in the **URL** column starts with `https`.

   If the URL does not start with `https`, click the name of the application to open the Change Application page and specify a URL that begins with `https`.
4. On the EPM navigation pane, click **Security** > **Certificates** and go to the Trusted Certificates tab.
5. Verify that a security certificate exists for each application server that Experience Portal can trust.

   Important:

   If Experience Portal cannot find a suitable application certificate, it will not be able to establish a secure connection to the application server, and all `https` applications will fail.

6. Click **Add** to install a security certificate using the Add Application Certificate page.
7. On the EPM navigation pane, click **System Configuration** > **MPP Servers** and click **Browser Settings**.
8. On the Browser Settings page, ensure that **SSL Verify** is set to **Yes**.

Chapter 14: Speech servers in Avaya Experience Portal

Speech servers in Avaya Experience Portal

The Avaya Experience Portal system integrates with two types of third-party speech servers:

- Automatic Speech Recognition (ASR): This technology enables an interactive voice response (IVR) system to collect verbal responses from callers.
- Text-to-Speech (TTS): This technology enables an IVR system to render text content into synthesized speech output according to algorithms within the TTS software.

For more information, see *Avaya Experience Portal Overview and Specification.*

Mixed Protocols for configuring speech servers

When the Media Processing Platform (MPP) software receives a call, the MPP software uses the Media Resource Control Protocol (MRCP) protocol to communicate with the speech servers. Using Experience Portal, you can configure multiple MRCP options for each speech server depending on the protocols the speech vendor supports.

For example, Experience Portal enables you to configure the following MRCP protocols for the Nuance speech server in the Experience Portal system:

- MRCP V1
- MRCP V2 TCP
- MRCP V2 TLS

In such a configuration, the MPP software uses the speech servers in a round-robin way. For example, if you configure a Nuance Vocalizer to use MRCPV1 and a Nuance Recognizer server to use MRCPv2 with TLS, the MPP software uses the Nuance Vocalizer MRCPv1 server for the first call, the Nuance Recognizer MRCPv2 with TLS for the second call, and so on.

Important:

- Using EPM, you can configure various MRCP options for different types of speech servers. However, you need to contact your speech server vendor for information on the

MRCP options supported by each speech server. For example, the Nuance Recognizer server supports all options (MRCPv1, MRCPv2+TCP, and MRCPv2+TLS).

- To configure TLS on any ASR or TTS speech server, you must restart the MPP server to reauthorize the certificates.

ASR servers in Avaya Experience Portal

ASR servers in Avaya Experience Portal

The Automatic Speech Recognition (ASR) technology enables an Interactive Voice Response (IVR) system to collect verbal responses from callers. The IVR system then interprets these verbal responses according to algorithms within the ASR software. Avaya Experience Portal integrates with third-party ASR servers to provide this capability in speech applications.

When the Experience Portal Media Processing Platform (MPP) software receives a call, MPP starts the associated speech application that controls the call flow. If the speech application uses ASR resources, MPP also starts a session with an ASR server configured to use *all* the languages defined in the speech application.

Note:

You can switch languages within a single speech application, provided all the required languages are configured on the same ASR server. If a speech application is configured to use more languages than those configured for any single ASR server, Experience Portal sends a `No ASR Resource` exception to the application. What happens afterward depends on the event handler that the application uses.

As the call progresses, MPP directs any speech recognition requests from the application to the designated ASR server. The ASR server processes the input collected from the caller and returns the results to the speech application for further action.

Note:

You need one ASR license for each call that requires ASR resources. The license is unavailable until the call is complete.

On the EPM web interface, administrators can enable speech server utterance recording on a per application basis, only when the Nuance ASR servers are used. This feature is available on all supported versions of Nuance.

ASR acquire and release resource control

In earlier releases of Experience Portal, if ASR was enabled for an application, the ASR resource was acquired at the start of the call and released at the end of the call, regardless of whether speech recognition was invoked on the call. However, from Release 7.2.2, applications can delay the acquisition of the ASR resource and provide an early release of the ASR resource based on its requirement on the call.

Here, the ASR resource refers to the ASR port, the communication channel to the speech server for recognition, and the ASR license.

Each application has the following three options to control the acquisition and release of the ASR resource:

- Acquire on call start and retain
- Acquire on first use and retain
- Acquire and release as needed

Option	Description
Acquire on call start and retain	When you select this option, the ASR resource is acquired at the start of the call and is released at the end of the call. The application maintains the ASR resource acquisition and release behavior of the previous Experience Portal releases. This is the default option for all applications.
Acquire on first use and retain	When you select this option, Experience Portal delays the acquisition of the ASR resource until the application requires and requests speech recognition. After the ASR resource is acquired, it is retained until the end of the call, and then released.
Acquire and release as needed	When you select this option, Experience Portal delays the acquisition of the ASR resource until the application requires and requests speech recognition. After the ASR resource is acquired, it is released during the call as needed. The ASR resource is released after all the VXML elements that require speech recognition resources are out of the VXML application scope. This occurs when all the grammars, loaded to the speech recognition server for this application, are unloaded from the speech recognition server. Grammars are generally unloaded after they are out of VXML scope. **Note:** The term 'grammar' refers to all VXML elements translated or interpreted as a grammar, not only the grammar element. For more details, see the ASR resource usage section.

Viewing existing ASR servers

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **System Configuration** > **Speech Servers**.
3. Click the ASR tab.

   The options that you see on this page depends on your user role.

Adding ASR servers

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** > **Speech Servers**.
3. On the Speech Servers page, on the **ASR** tab , click **Add**.
4. On the Add ASR Server page, enter appropriate information in the fields.

   If you logged in using the init account, ensure that you enter the appropriate LDN number for the server in the **LDN** field. If you do not specify an LDN number, Experience Portal uses the default value (000)000-0000.
5. Click **Save**.

   After you save the changes, the **System Monitor** webpage and the **MPP Manager** webpage on EPM displays the **Restart Required** configuration status for MPPs in the **Running** state.
6. Restart only the MPP servers that belong to the affected zone.

Changing ASR servers

Procedure

1. Log in to the EPM web interface.
2. In the EPM navigation pane, click **System Configuration** > **Speech Servers**.
3. On the ASR tab of the Speech Servers page, the **Name** column, click the name of the server.
4. On the Change ASR Server page, enter appropriate information in the fields.

   If you logged in using the init account, ensure that the LDN number specified in the **LDN** field matches the information in the Avaya Services database for this server.

5. Click **Save**.

   After you save the changes, the **System Monitor** webpage and the **MPP Manager** webpage on EPM displays the **Restart Required** configuration status for MPPs in the **Running** state.

6. Restart only the MPP servers that belong to the affected zone.

Deleting ASR servers

Before you begin

Important:

All ASR-enabled applications on the Experience Portal system have associated ASR languages. Before you delete a server, look at the **Languages** column. Ensure that all the languages that the server supports are also supported by at least one other ASR server. If the server you plan to delete is the only one that supports a given language, you must assign that language to another ASR server. You can also change any applications that use the old language.

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** > **Speech Servers**.
3. On the Speech Servers page, click the **ASR** tab.
4. On the ASR page, do the following:
   - To delete each ASR servers: Select the check box for the server that you want to delete.
   - To delete all servers: Select the selection check box in the header row of the table, which automatically selects all rows in the table.
5. Click **Delete**.

   If the server is currently in use, Experience Portal deletes it after the server finishes processing any active calls.

   After you save the changes, the **System Monitor** webpage and the **MPP Manager** webpage on EPM displays the **Restart Required** configuration status for MPPs in the **Running** state.

6. Restart only the MPP servers that belong to the affected zone.

Adding a third-party ASR Server type

About this task

By default, Experience Portal supports a set of ASR Servers. The list of ASR Servers is displayed in the ASR Server list drop-down when configuring an ASR Server or selecting an ASR Server to

an application. It is possible to add another third-party ASR Server to the list of supported ASR Servers as long as the third-party ASR Server can mimic one of the supported ASR Servers.

Procedure

1. Log in to Linux on the Experience Portal server in one of the following ways:
   - Log on to the local Linux console as root.
   - 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 config directory by running the **`cd $CATALINA_HOME/lib/config`** command.
3. Take a backup of the existing `asrCustom.properties` file.
4. Open the `asrCustom.properties` file and follow the instructions given in the file.

   The file also includes an example.
5. After the file is updated, restart the vpms service by running the **`systemctl restart vpms`** command.

   Note:

   You must also restart the vpms service once during off-hours.

   The new ASR Server is available in the **Engine Type** drop-down on the ASR Servers web page and the application configuration web page.

ASR tab on the Speech Servers page field descriptions

Use this tab to view information about the Automatic Speech Recognition (ASR) servers currently administered on the Experience Portal system, add a new ASR server, or change an existing server, and add or delete different languages and language codes.

Column or Button	Description
Selection check box	Use this Selection check box to select which ASR servers you want to delete.
Zone	The name of the zone where the ASR servers are configured.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.

Table continues…

Column or Button	Description
Name	The unique identifier for this ASR server on the Experience Portal system. To change the parameters for an ASR server, click the name of the server in the table. Experience Portal opens the Change ASR Server page.
Enable	Whether this ASR server is available for use by the Experience Portal system.
Network Address	The network address, or location, of the ASR server.
Engine Type	The type of ASR software engine the server uses. **Note:** To add a third-party ASR server type that mimics an existing ASR server, see Adding a third-party ASR Server type on page 432.
MRCP	The MRCP protocol used for allocating the media processing server resources (ASR).
Base Port	The port number on the ASR server to which requests for ASR services are sent. The ASR server must be configured to receive and process requests through this port.
Total Number of Licensed ASR Resources	The total number of licensed ASR resources that will be used by the Experience Portal system. Experience Portal uses this information to determine the total number of ASR resources available to the Experience Portal system.
Languages	The languages that the ASR server can recognize.
Add	Opens the Add ASR Server page.
Delete	Deletes the ASR servers whose Selection check box has been checked. After you delete the servers, the **System Monitor** web page and the **MPP Manager** web page on EPM display the **Restart needed** configuration status for affected MPPs that are in the **Running** state. You must restart affected MPPs before the deleted ASR servers will be removed from the MPP's configuration.
Customize	Opens the ASR Custom Languages page. Using this page you can add custom languages and their respective language codes to the Automatic Speech Recognition (ASR) servers currently administered on the Experience Portal system. You can also delete the existing custom configured languages and their respective codes.

Add ASR Server page field descriptions

Use this page to add a new Automatic Speech Recognition (ASR) server to the Experience Portal system.

After you save the changes, the **System Monitor** web page and the **MPP Manager** web page on EPM display the **Restart needed** configuration status for the affected MPPs that are in the **Running** state. You must restart the affected MPPs before the applications can use the new ASR server.

This page contains the:

Note:

The SRTP and the Configured SRTP List sections are available only if the Transport Protocol field is set to TLS.

General Section

Field	Description
Zone	The name of the zone where the ASR servers are configured. Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only if you have created zones on your Experience Portal system. If you do not create any new zones, you do not see the drop-down box.
Name	The unique identifier for this ASR server on the Experience Portal system. If you are using a Nuance server, this name must be between 1 and 32 characters. **Note:** Once you save the ASR server, this name cannot be changed.
Enable	Whether this ASR server is available for use by the Experience Portal system. The default is **Yes**, which means the server is available.

Table continues…

Field	Description
Engine Type	The type of ASR software engine the server uses. The options are: • **Loquendo** • **Nuance** • **Google Speech** • **Dialogflow** The selection of an engine type in this field affects what the EPM displays as the defaults in the **Base Port**, **New Connection per Session**, **Languages** and **RTSP URL** fields. **Note:** Once you save the ASR server, this type cannot be changed. **Note:** To add a third-party ASR server type that mimics an existing ASR server, see Adding a third-party ASR Server type on page 432.
Credentials	The authentication credentials for communicating with a Google Speech or Dialogflow Engine. This field is displayed only when you select **Google Speech** or **Dialogflow** in the **Engine Type** field. For more information on the authentication credentials, refer to the Google Speech or Dialogflow Engine documentation.
Profanity Filter	The filter that indicates whether the speech recognition engine should filter out profane words or not. The options are: • Yes • No This field is displayed only when you select **Google Speech** in the **Engine Type** field.
Audio Chunk Size	The size of each chunk of audio data, specified in kilobytes, that is transmitted to the speech engine. Enter a number in the range 1 to 128. The default value is 8. This field is displayed only when you select **Google Speech** or **Dialogflow** in the **Engine Type** field.
Network Address	The network address, or location, of the ASR server. This must be a valid network address in the form of a fully qualified hostname or an IP address. When you enter an address in this field, the EPM automatically inserts the address as part of the **RTSP URL** field.

Table continues…

Field	Description
Base Port	The port number on the ASR server to which requests for ASR services are sent. The default value for this field depends on which engine type and MRCP protocol you select: • For Loquendo, the default is 554 • For Nuance, the default is port 4900 The default port value changes to 5060 if you select MRCPV2 (TCP) protocol and to 5061 for MRCPV2 (TLS) protocol. **Important:** These values are set to the default port numbers on the respective ASR servers. Unless you have manually changed the default settings on the ASR server, you should not have to change them here.
Total Number of Licensed ASR Resources	The total number of licensed ASR resources that will be used by the Experience Portal system. Experience Portal uses this information to determine the total number of ASR resources available to the Experience Portal system.
New Connection per Session	Whether Experience Portal opens a new connection for each call session. If you are using: • Loquendo, the default is **Yes**. • Nuance, the default is **No**. **Important:** You must use the above settings for this parameter.

Table continues…

Field	Description
Languages	Displays all the languages that ASR servers can use on this system. The selected languages are the ones that this ASR server can recognize. Select an individual entry in this list by clicking on it, or use `Ctrl+Click` and `Shift +Click` to select multiple entries. Then, click the button to move the selected languages to the **Selected Languages** field. To move the languages back from the **Selected Languages** field to the **Languages** field, click on the button. This list is prepopulated with the list of the languages that were available for the designated ASR engine type when Experience Portal was released. It is maintained in a special file on the Experience Portal system and is not automatically updated. You must verify that the languages you select here are actually installed and available on the target ASR server. You can add more languages to this list by clicking **Configuration>Speech Servers** from the EPM menu and selecting **Customize** in the ASR tab. **Note:** If a speech application is configured to use more languages than are configured for any single ASR server, Experience Portal sends a `No ASR Resource` exception to the application. What happens then depends on the event handler that the application uses.
Selected Languages	All language(s) that you select in the **Languages** pane appear in this pane.
Listed Directory Number (LDN)	This field is only shown when you are logged into the EPM using the Avaya Services init account created when the Avaya Service accounts were configured. If you are logged into the EPM using the init account, enter the LDN number for this server as it appears in the Avaya Services database. If an LDN number is not specified for this server, Experience Portal uses the default value (000)000-0000.

MRCP Section

Field	Description
Ping Interval	When a speech application requires ASR resources, the MPP establishes a connection to the ASR server at the beginning of a session. Experience Portal sends periodic "heartbeat" messages to the ASR server to make sure the connection is not terminated prematurely. This field specifies the number of seconds the Experience Portal system waits between heartbeat messages. Enter an integer in this field. The default is 15.
Response Timeout	The number of seconds to allow for the ASR server to respond to a request for ASR resources before timing out. Enter an integer in this field. The default is 4.

Table continues…

Field	Description
Protocol	The MRCP protocol used for allocating the media processing server resources (ASR). The options are: • **MRCP V1** • **MRCP V2** — This option is shown only when you select Nuance in the **Engine Type** field **Note:** If you have installed Avaya Aura® Media Server on the system, the only option available is **MRCP V1**. The default is MRCP V1.
RTSP URL	The URL of the Real-Time Streaming Protocol (RTSP) server. The RTSP server is the network remote control for the Experience Portal multimedia servers. The default path depends on: • The network address as set in the **Network Address** field. If you change the network address, the default RTSP URL updates to reflect the change. • Which ASR engine type you have selected in the **Engine Type** field. If you change the engine type, the default RTSP URL updates to reflect the change. **Tip:** If you want to change the default URL, make sure you specify the network address and select the ASR engine type first. Otherwise, Experience Portal will overwrite your changes when you enter a new network address or change the engine type.
Enable Session XML	Displays when you select the MRCP V2 option in the **Protocol** field. Parameters specified in the `session.xml` file supersede vendor-specific parameters specified on the Applications webpage. The options are: • Yes: `Session.xml` specified for each voice application is sent to the speech server. If `Session.xml` is not specified for the voice application, the system generates and sends a `session.xml` file that consists of an organization and application name. • No: `Session.xml` is not sent to the speech server for any voice application.

Table continues…

Field	Description
Transport Protocol	This field is only shown when you select the MRCP V2 protocol under the MRCP section. The transport protocol used for transporting the real-time data. The options are: • **TCP** • **TLS** The default is TCP. The TLS option is shown only when you select Nuance in the **Engine Type** field. **Important:** • If you select TLS, ensure that the CA certificate that signed the identity certificate of the speech server is installed on Experience Portal as a trusted certificate. On the EPM navigation pane, click **Security > Certificates > Trusted Certificates**. Ensure that the required trusted certificate of the speech server is installed. If it is not uploaded, upload the certificate. • Click **System Maintenance > Log Viewer** to check for speech server connection errors.
Listener Port	This field is only shown when you select the MRCP V2 protocol under the MRCP section. Enter an integer value in the range 1 – 65535. The default is 5060 if you select MRCPV2 (TCP) protocol and 5061 for MRCPV2 (TLS) protocol.

SRTP Section

Note:

This group only appears if the **Transport Protocol** field is set to **TLS**.

Field	Description
Enable	The options are: • **Yes** : This connection uses SRTP. • **No** : This connection does not use SRTP.
Encryption Algorithm	The options are: • **AES_CM_128**: This connection uses 128 key encryption. • **None**: Messages sent through this connection are not encrypted.
Authentication Algorithm	The options are: • **HMAC_SHA1_80**: Authentication is done with HMAC SHA-1 which uses 80 bit key for the authentication. • **HMAC_SHA1_32**: Authentication is done with HMAC SHA-1 which uses 32 bit key for the authentication.
RTCP Encryption Enabled	The options are: • **Yes:** This connection uses RTP Control Protocol encryption. • **No:** This connection does not use RTP Control Protocol encryption.

Table continues…

Field	Description
RTP Authentication Enabled	The options are: • **Yes:** This connection uses Real-time Transport Protocol authentication. • **No:** This connection does not use Real-time Transport Protocol authentication.
Add	Adds the SRTP configuration to the **Configured SRTP List**.

Configured SRTP List group

This group displays any SRTP configurations defined for the connection.

Note:

This group only appears if the Transport Protocol field is set to TLS.

Field	Description
Display list box	Displays the SRTP configurations for this connection.
Remove	Removes the association between the SRTP configuration selected in the display text box and the SIP connection.

Change ASR Server page field descriptions

Use this page to change an existing Automatic Speech Recognition (ASR) server to the Experience Portal system.

For all ASR changes except for Enable/Disable, after you save the changes, the **System Monitor** web page and the **MPP Manager** web page on EPM display the **Restart needed** configuration status for affected MPPs that are in the **Running** state. You must restart the affected MPPs before applications can use the modified configuration.

This page contains the:

General Section

Field	Description
Zone	The name of the zone where the ASR servers are configured. Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only if you have created zones on your Experience Portal system. If you do not create any new zones, you do not see the drop-down box.
Name	The unique identifier for this ASR server on the Experience Portal system. If you are using a Nuance server, this name must be between 1 and 32 characters. **Note:** Once you save the ASR server, this name cannot be changed.
Enable	Whether this ASR server is available for use by the Experience Portal system. The default is **Yes**, which means the server is available. **Note:** When you change this value from **Yes** to **No**, no new calls will use this server. However, any calls in progress may continue to use the speech server. You must let the ongoing calls to complete before taking the speech server out of service to avoid application errors.
Engine Type	The type of ASR software engine the server uses. The options are: • **Loquendo** • **Nuance** • **Google Speech** • **Dialogflow** The selection of an engine type in this field affects what the EPM displays as the defaults in the **Base Port**, **New Connection per Session**, **Languages** and **RTSP URL** fields. **Note:** Once you save the ASR server, this type cannot be changed. **Note:** To add a third-party ASR server type that mimics an existing ASR server, see Adding a third-party ASR Server type on page 432.

Table continues…

Field	Description
Credentials	The authentication credentials for communicating with a Google Speech or Dialogflow Engine. This field is displayed only when you select **Google Speech** or **Dialogflow** in the **Engine Type** field. For more information on the authentication credentials, refer to the Google Speech or Dialogflow Engine documentation.
Profanity Filter	The filter that indicates whether the speech recognition engine should filter out profane words or not. The options are: • Yes • No This field is displayed only when you select **Google Speech** in the **Engine Type** field.
Audio Chunk Size	The size of each chunk of audio data, specified in kilobytes, that is transmitted to the speech engine. Enter a number in the range 1 to 128. The default value is 8. This field is displayed only when you select **Google Speech** or **Dialogflow** in the **Engine Type** field.
Network Address	The network address, or location, of the ASR server. This must be a valid network address in the form of a fully qualified hostname or an IP address. When you enter an address in this field, the EPM automatically inserts the address as part of the **RTSP URL** field.
Base Port	The port number on the ASR server to which requests for ASR services are sent. The default value for this field depends on which engine type and MRCP protocol you select: • For Loquendo, the default is 554 • For Nuance, the default is port 4900 The default port value changes to 5060 if you select MRCPV2 (TCP) protocol and to 5061 for MRCPV2 (TLS) protocol. **Important:** These values are set to the default port numbers on the respective ASR servers. Unless you have manually changed the default settings on the ASR server, you should not have to change them here.
Total Number of Licensed ASR Resources	The total number of licensed ASR resources that will be used by the Experience Portal system. Experience Portal uses this information to determine the total number of ASR resources available to the Experience Portal system.

Table continues…

Field	Description
New Connection per Session	Whether Experience Portal opens a new connection for each call session. If you are using: • Loquendo, the default is **Yes** • Nuance, the default is **No** **Important:** You must use the above settings for this parameter.
Languages	Displays all the languages that ASR servers can use on this system. The selected languages are the ones that this ASR server can recognize. Select an individual entry in this list by clicking on it, or use `Ctrl+Click` and `Shift +Click` to select multiple entries. Then, click the button to move the selected languages to the **Selected Languages** field. To move the languages back from the **Selected Languages** field to the **Languages** field, click on the button. This list is prepopulated with the list of the languages that were available for the designated ASR engine type when Experience Portal was released. It is maintained in a special file on the Experience Portal system and is not automatically updated. You must verify that the languages you select here are actually installed and available on the target ASR server. You can add more languages to this list by clicking **Configuration>Speech Servers** from the EPM menu and selecting **Customize** in the ASR tab. **Note:** If a speech application is configured to use more languages than are configured for any single ASR server, Experience Portal sends a `No ASR Resource` exception to the application. What happens then depends on the event handler that the application uses.
Selected Languages	All languages that you select in the **Languages** pane appear in this pane.
Listed Directory Number (LDN)	This field is only shown when you are logged into the EPM using the Avaya Services init account created when the Avaya Service accounts were configured. If you are logged into the EPM using the init account, enter the LDN number for this server as it appears in the Avaya Services database. If an LDN number is not specified for this server, Experience Portal uses the default value (000)000-0000.

MRCP Section

Field	Description
Ping Interval	When a speech application requires ASR resources, the MPP establishes a connection to the ASR server at the beginning of a session. Experience Portal sends periodic "heartbeat" messages to the ASR server to make sure the connection is not terminated prematurely. This field specifies the number of seconds the Experience Portal system waits between heartbeat messages. Enter an integer in this field. The default is 15.
Response Timeout	The number of seconds to allow for the ASR server to respond to a request for ASR resources before timing out. Enter an integer in this field. The default is 4.
Protocol	The MRCP protocol used for allocating the media processing server resources (ASR). The options are: • **MRCP V1** • **MRCP V2** — MRCPv2 option is shown only when you select Nuance in the **Engine Type** field. **Note:** If you have installed Avaya Aura® Media Server on the system, the only option available is **MRCP V1**. The default is MRCP V1.
RTSP URL	The URL of the Real-Time Streaming Protocol (RTSP) server. The RTSP server is the network remote control for the Experience Portal multimedia servers. The default path depends on: • The network address as set in the **Network Address** field. If you change the network address, the default RTSP URL updates to reflect the change. • Which ASR engine type you have selected in the **Engine Type** field. If you change the engine type, the default RTSP URL updates to reflect the change. **Tip:** If you change the default URL, make sure you specify the network address and select the ASR engine type first. Otherwise, Experience Portal will overwrite your changes when you enter a new network address or change the engine type.

Table continues…

Field	Description
Enable Session XML	Displays when you select the MRCP V2 option in the **Protocol** field. Parameters specified in the `session.xml` file supersede vendor-specific parameters specified on the Applications webpage. The options are: • Yes: `Session.xml` specified for each voice application is sent to the speech server. If `Session.xml` is not specified for the voice application, the system generates and sends a `session.xml` file that consists of an organization and application name. • No: `Session.xml` is not sent to the speech server for any voice application.
Transport Protocol	This field is only shown when you select the MRCP V2 protocol under the MRCP section. The transport protocol used for transporting the real-time data. The options are: • **TCP** • **TLS** The default is TCP. The TLS option is shown only when you select Nuance in the **Engine Type** field. **Important:** • If you select TLS, ensure that the CA certificate that signed the identity certificate of the speech server is installed on Experience Portal as a trusted certificate. On the EPM navigation pane, click **Security > Certificates > Trusted Certificates**. Ensure that the required trusted certificate of the speech server is installed. If it is not uploaded, upload the certificate. • Click **System Maintenance > Log Viewer** to check for speech server connection errors.
Listener Port	This field is only shown when you select the MRCP V2 protocol under the MRCP section. Enter an integer value in the range 1 – 65535. The default is 5060 if you select MRCPV2 (TCP) protocol and 5061 for MRCPV2 (TLS) protocol.

SRTP Section

Note:

This group only appears if the **Transport Protocol** field is set to **TLS**.

Field	Description
Enable	The options are: • **Yes**: This connection uses SRTP. • **No**: This connection does not use SRTP.
Encryption Algorithm	The options are: • **AES_CM_128**: This connection uses 128 key encryption. • **None**: Messages sent through this connection are not encrypted.

Table continues…

Field	Description
Authentication Algorithm	The options are: • **HMAC_SHA1_80**: Authentication is done with HMAC SHA-1 which uses 80 bit key for the authentication.. • **HMAC_SHA1_32**: Authentication is done with HMAC SHA-1 which uses 32 bit key for the authentication..
RTCP Encryption Enabled	The options are: • **Yes:** This connection uses RTP Control Protocol encryption. • **No:** This connection does not use RTP Control Protocol encryption.
RTP Authentication Enabled	The options are: • **Yes:** This connection uses Real-time Transport Protocol authentication. • **No:** This connection does not use Real-time Transport Protocol authentication.
Add	Adds the SRTP configuration to the **Configured SRTP List**.

Configured SRTP List group

This group displays any SRTP configurations defined for the connection.

Note:

This group only appears if the Transport Protocol field is set to TLS.

Field	Description
Display list box	Displays the SRTP configurations for this connection.
Remove	Removes the association between the SRTP configuration selected in the display text box and the SIP connection.

TTS servers in Avaya Experience Portal

TTS servers in Experience Portal

The Text-to-Speech (TTS) technology enables an Interactive Voice Response (IVR) system to render text content into synthesized speech output, according to algorithms within the TTS software. Avaya Experience Portal integrates with third-party TTS servers to provide this capability in speech applications.

When the Experience Portal Media Processing Platform (MPP) software receives a call, MPP starts the associated speech application that controls the call flow. If the speech application uses TTS resources, MPP also starts a session with a TTS server that is configured to use *all* the language and voice combinations defined in the speech application.

Note:

You can switch languages within a single speech application, provided all the required languages are configured on the same TTS server. If a speech application is configured to use more language/voice combinations than are configured for any single TTS server, Experience Portal sends a `No TTS Resource` exception to the application. What happens then depends on the event handler that the application uses.

As the call progresses, MPP directs any requests for speech synthesis from the application to the designated TTS server. The TTS server then renders the text content as audible speech output.

Note:

You need one TTS license for each call that requires TTS resources. The license is unavailable until the call is complete and becomes available to other calls after the current call ends.

Viewing existing TTS servers

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **System Configuration** > **Speech Servers**.
3. Click the TTS tab.

   The options that you see on this page depend on your user role.

Adding TTS servers

Procedure

1. Log on to the EPM web interface.

   If Avaya Services is maintaining this system and you are an Avaya Services representative, log on to EPM by using the init EPM account that is created during the EPM software installation.

   Otherwise, log on to EPM by using an account with the Administrator user role.
2. In the EPM main menu, select **System Configuration** > **Speech Servers**.
3. On the **TTS** tab of the Speech Servers page, click **Add**.
4. On the Add TTS Server page, enter the appropriate information and click **Save**.

   If you logged in using the init account, ensure that you enter the appropriate LDN number for the server in the **LDN** field. If you do not specify an LDN number, Experience Portal uses the default value (000)000-0000.

After you save the changes, the **System Monitor** webpage and the **MPP Manager** webpage on EPM displays the **Restart Required** configuration status for MPPs in the **Running** state.

5. Restart only the MPP servers that belong to the affected zone.

Changing TTS servers

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** > **Speech Servers**.
3. On the Speech Servers page, on the **TTS** tab, in the **Name** column, click the server name.
4. On the Change TTS Server page, enter appropriate information, and click **Save**.

   If you logged in using the init account, ensure that the LDN number specified in the **LDN** field matches the information in the Avaya Services database for this server.

   After you save the changes, the **System Monitor** webpage and the **MPP Manager** webpage on EPM displays the **Restart Required** configuration status for MPPs in the **Running** state.
5. Restart only the MPP servers that belong to the affected zone.

Deleting TTS servers

Before you begin

Important:

All TTS-enabled applications on the Experience Portal system have associated TTS languages and voices. Before you delete a server, look at the **Voices** column. Ensure that all the languages or voices that the server supports are also supported by at least one other TTS server. If the server you plan to delete is the only one that supports a given language or voice, you must assign that language or voice to another TTS server. You can also change any applications that use the old language or voice.

Procedure

1. Log on to the EPM web interface by using an account with the Administration user role.
2. In the EPM main menu, select **System Configuration** > **Speech Servers**.
3. On the Speech Servers page, click the **TTS** tab.
4. For each TTS server that you want to delete, select the **Selection** check box to the left of the server name in the table.

Tip:

To delete all servers, select the **Selection** check box in the header row of the table. The system automatically selects all rows in the table.

5. Click **Delete**.

   If the server is currently in use, Experience Portal deletes it after the server finishes processing any active calls.

   After you save the changes, the **System Monitor** webpage and the **MPP Manager** webpage on EPM displays the **Restart Required** configuration status for MPPs in the **Running** state.

6. Restart only the MPP servers that belong to the affected zone.

Adding a third-party TTS Server type

About this task

By default, Experience Portal supports a set of TTS Servers. The list of TTS Servers is displayed in the TTS Server list drop-down when configuring a TTS Server or selecting an TTS Server to an application. It is possible to add another third-party TTS Server to the list of supported TTS Servers as long as the third-party TTS Server can mimic one of the supported TTS Servers.

Procedure

1. Log in to Linux on the Experience Portal server in one of the following ways:
   - Log on to the local Linux console as root.
   - 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 config directory by running the **`cd $CATALINA_HOME/lib/config`** command.
3. Take a backup of the existing `ttsCustom.properties` file.
4. Open the `ttsCustom.properties` file and follow the instructions given in the file.

   The file also includes an example.

5. After the file is updated, restart the vpms service by running the **`systemctl restart vpms`** command.

   Note:

   You must also restart the vpms service once during off-hours.

   The new TTS Server is available in the **Engine Type** drop-down on the TTS Servers web page and the application configuration web page.

Custom RealSpeak TTS dictionaries

Adding custom dictionaries for Nuance Vocalizer

An application that uses the Nuance Vocalizer server can use a custom dictionary. You can create as many custom dictionaries as you require. You can pass the dictionary as a vendor specific parameter switts.ssftrs_dict_enable or define the dictionary using parameter dictionaries in the Nuance Vocalizer configuration file *baseline.xml*.

Procedure

1. Create the custom dictionaries, as described in the Nuance Vocalizer documentation. Nuance Vocalizer doesn't support text-based dictionary format (DCT or TDC files) anymore, only binary user dictionary format, BDC or DCB files, is supported. The binary dictionary format has also changed.
2. Convert the old text format dictionary (.dct or .tdc) to the new Vocalizer text format dictionary (.txt) with the following command:

   ```
   dictmigrate –i <old-dictionary> -o <new_dictionary>
   ```

   For example:

   ```
   dictmigrate -i DictionaryName.dct –o DictionaryName.txt
   ```

   Note:

   Skip this step if you've already created a new text format dictionary.
3. Compile text format dictionary (.txt) to binary format dictionary, .bdc or .dcb, with the following command:

   ```
   dictcpl –o <BinaryFilename.bdc> <TextName.txt>
   ```

   For example:

   ```
   dictcpl -o DictionaryName.bdc DictionaryName.txt
   ```

If the user dictionary will be accessed from the application server through HTTP, you must map the dictionary extensions that you are using to the appropriate MIME type.

4. On each Nuance Vocalizer HTTP server, open the *mime.types* file.

   The default file location on Linux is in the `/etc/` directory. The default locations on Windows are:

   - For a 32 bit system:

     ```
     C:\Program Files\Apache Software Foundation\Apache2.2\conf
     ```

   - For a 64 bit system:

     ```
     C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf
     ```

5. Add the following lines to mime.types to associate text and binary dictionaries with the correct file extensions:

   application/octet-stream bdc

   application/octet-stream dcb

   application/octet-stream dct

   application/octet-stream tdc

6. Save and close the file.
7. Upload the custom dictionaries as described in the Nuance Vocalizer documentation.

Next steps

Associate the dictionary with the application.

Associating a custom dictionary with an application through Experience Portal

Procedure

1. Follow the steps described in Adding a speech application to Experience Portal on page 342 or Changing speech application settings through Avaya Experience Portal on page 342.
2. When you get to the **TTS** section in the **Speech Parameters** group, go to the **TTS** field and:
   - If your Vocalizer server is on Linux, add the `swittts.ssftrs_dict_enable="file:///opt/ttsdict/<dictionary name>.<extension>"` parameter.
   - If your Vocalizer server is on Windows, add the `swittts.ssftrs_dict_enable="file://<drive>/<full path>/<dictionary name>.<extension>"` parameter.
3. Click **Save**.

Example

On Windows, if your dictionary is stored in a file called `C:/custom/ttsdict/my_dictionary.bdc`, specify the following:

```
swittts.ssftrs_dict_enable="file://C:/custom/ttsdict/my_dictionary.bdc"
```

Associating a custom dictionary with an application using the lexicon tag

About this task

Avaya Orchestration Designer does not currently support the `lexicon` tag, but if you want to use it in your custom application, place it within the `prompt` tag.

Procedure

If you are using:

- Linux, add the tag using the format `<lexicon uri="file:///<fully qualified file path>/<filename>.<extension>/">`
- Windows, add the tag using the format `<lexicon uri="file://<drive>/<full path>/<filename>.<extension>/">`

Example

On Windows you could specify:

```
<prompt bargin="false">
<lexicon uri="file://c:/mydictionary.dct/">
Welcome to Avaya Inc.
</prompt>
```

Sample custom dictionary for Vocalizer

The following shows a sample text-base dictionary for US English:

```
[Header]

[SubHeader]
Language = ENU
Content=EDCT_CONTENT_ORTHOGRAPHIC
Representation=EDCT_REPR_SZ_STRING
[Data]
DLL     "Dynamic Link Library"
Hello  "Welcome to the demonstration of the American English Text-to-Speech system.
TTS     "Text To Speech."
info    Information
```

```
[SubHeader]
Language = ENU
Content = EDCT_CONTENT_BROAD_NARROWS
Representation = EDCT_REPR_SZZ_STRING
[Data]
addr   // '@.dR+Es
avaya  // $.'v@.j$
```

The `[Data]` sections contain the abbreviations or phonetic expressions you want to add to your custom dictionary.

Phonetic expressions allowed in a custom dictionary

Phonetic Symbols	Orthographic Example	Phonetic Example
i	f(ee)l	'fil
I	f(i)ll	'fIl
E	f(e)ll	'fEl
@	c(a)t	'k@t
A	g(o)t	'gAt
^	c(u)t	'k^t

Table continues…

Phonetic Symbols	Orthographic Example	Phonetic Example
O	f(a)ll	'fOl
U	f(u)ll	'fUl#\
u	f(oo)l	'ful
E0	c(u)rt	'kE0R+t
e&I	f(ai)l	'fe&Il
O&I	f(oi)l	'fO&Il
a&I	f(i)le	'fa&Il
a&U	f(ou)l	'fa&Ul
o&U	g(oa)l	'go&Ul
j	(y)es	'jEs
w	(wh)y	'wa&I
R+	(r)ip	'R+Ip
l	(l)ip	'lIp
p	(p)it	'pIt
t	(t)op	'tAp
k	(c)at	'k@t
b	(b)it	'bIt
d	(d)ig	'dIg
g	(g)ot	'gAt
?	()illness	'?Il.nIs
f	(f)at	'f@t
T	(th)in	'TIn
s	(s)eal	'sil
S	(sh)ip	'SIp
v	(v)at	'v@t
D	(th)en	'DEn
z	(z)eal	'zil
Z	lei(s)ure	'li.Z$R+”
h	(h)at	'h@t
t&S	ca(tch)	'k@t&S
d&Z	(j)ourney	'd&ZE0R+.ni
m	(m)an	'm@n
n	(n)ut	'n^t
nK	ri(ng)	'R+InK
.	syllable break	

Table continues…

Phonetic Symbols	Orthographic Example	Phonetic Example
'	primary stress	
'2	secondary stress	
“	sentence accent	
#	silence (pause)	
_	word delimiter	
*.	end of declarative	
*,	comma	
*!	end of exclamation	
*?	end of question	
*;	semicolon	
*:	colon	
$	(a)llow	$.'la&U
l%)	batt(le)	'b@.r6l%)
n%)	did(n’)t	'dI.dn%)t
r6	bu(tt)er	'b^.r6$R+

TTS tab on the Speech Servers page field descriptions

Use this tab to view information about the Text-to-Speech (TTS) servers currently administered on the Experience Portal system, add a new TTS server, or change an existing server, and add or delete different voices and voice codes.

Column or Button	Description
Selection check box	Use this Selection check box to select which servers you want to delete.
Zone	The name of the zone where the TTS server is configured.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
Name	The unique identifier for this TTS server on the Experience Portal system. To change the parameters for a TTS server, click the name of the server in the table. Experience Portal opens the Change TTS Server page.
Enable	Whether this TTS server is available for use by the Experience Portal system.

Table continues…

Column or Button	Description
Network Address	The network address, or location, of the TTS server you want to use.
Engine Type	The type of TTS software engine the server uses. **Note:** To add a third-party TTS server type that mimics an existing TTS server, see Adding a third-party TTS Server type on page 450.
MRCP	The MRCP protocol used for allocating the media processing server resources (TTS).
Base Port	The port number on the TTS server to which requests for TTS services are to be sent. The TTS server must be configured to receive and process requests through this port.
Total Number of Licensed TTS Resources	The total number of licensed TTS resources that is used by the Experience Portal system. Experience Portal uses this information to determine the total number of TTS resources available to the Experience Portal system.
Voices	The voices that this TTS server is configured to use.
Add	Opens the Add TTS Server page.
Delete	Deletes the TTS servers whose Selection check box has been checked. After you delete the servers, the **System Monitor** web page and the **MPP Manager** web page on EPM display the **Restart needed** configuration status for affected MPPs that are in the **Running** state. You must restart affected MPPs before the deleted TTS servers will be removed from the MPP's configuration.
Customize	Opens the **TTS Custom Voices** page. Using this page you can add custom voices and their respective language codes to the Text-to-Speech (TTS) servers currently administered on the Experience Portal system. You can also delete the existing custom configured voices and their respective language codes.

Add TTS Server page field descriptions

Use this page to add a new Text-to-Speech (TTS) server to the Experience Portal system.

After you save the changes, the **System Monitor** web page and the **MPP Manager** web page on EPM display the **Restart needed** configuration status for affected MPPs that are in the **Running** state. You must restart the affected MPPs before the applications can use the new TTS server.

This page contains the:

Note:

The SRTP and the Configured SRTP List sections are available only if the Transport Protocol field is set to **TLS**.

General Section

Field	Description
Zone	The name of the zone where the TTS server is configured. Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only if you have created zones on your Experience Portal system. If you do not create any new zones, you do not see the drop-down box.
Name	The unique identifier for this TTS server on the Experience Portal system. If you are using a Nuance server, this name must be between 1 and 32 characters. **Note:** You cannot change this name once you save the TTS server.
Enable	Whether this TTS server is available for use by the Experience Portal system. The default is **Yes**, which means the server is available.
Engine Type	The type of TTS software engine the server uses. The options are: • **Loquendo** • **Nuance** The selection of an engine type in this field affects what the EPM displays as the defaults in the **Base Port**, **New Connection per Session**, **Voices** and **RTSP URL** fields as well. **Note:** Once you save the TTS server, this engine type cannot be changed. **Note:** To add a third-party TTS server type that mimics an existing TTS server, see Adding a third-party TTS Server type on page 450.
Network Address	The network address, or location, of the TTS server you want to use. This must be a valid network address in the form of a fully qualified hostname or an IP address. When you enter a network address in this field, the EPM automatically inserts the address as part of the **RTSP URL** field.

Table continues…

Field	Description
Base Port	The port number on the TTS server to which requests for TTS services are to be sent. The value for this field depends on the selected engine type and the MRCP protocol: • For Loquendo, the default is 554 • For Nuance, the default is port 4900 The default port value changes to 5060 if you select MRCPV2 (TCP) protocol and to 5061 for MRCPV2 (TLS) protocol. **Important:** These values are set to the default port numbers on the respective TTS servers. Unless you have manually changed the default settings on the TTS server, you should not have to change them here.
Total Number of Licensed TTS Resources	The total number of licensed TTS resources that is used by the Experience Portal system. Experience Portal uses this information to determine the total number of TTS resources available to the Experience Portal system.
New Connection per Session	Whether Experience Portal establishes a new connection on the TTS server for each call session. If you are using: • Loquendo, set this to **Yes** • Nuance, set this to **No**
Voices	Displays all voices that TTS servers can use on this system. Select an individual entry in this list by clicking on it, or use `Ctrl+Click` and `Shift+Click` to select multiple entries. Then, click the button to move the selected voices to the **Selected Voices** field. To move the voices back from the **Selected Voices** field to the **Voices** field, click on the button. This list of voices in the **Voices** field is prepopulated with the list of the voices that were available for the designated TTS engine type when Experience Portal was released. It is maintained in a special file on the Experience Portal system and is not automatically updated. You must verify that the voices you select here are actually installed and available on the target TTS server. You can add more voices to this list by clicking **Configuration>Speech Servers** from the EPM menu and selecting **Customize** in the TTS tab. **Note:** If a speech application is configured to use more language/voice combinations than are configured for any single TTS server, Experience Portal sends a `No TTS Resource` exception to the application. What happens then depends on the event handler that the application uses.

Table continues…

Field	Description
Selected Voices	All voices that you select in the **Voices** pane appear in this pane.
Listed Directory Number (LDN)	This field is only shown when you are logged into the EPM using the Avaya Services init account created when the Avaya Service accounts were configured. If you are logged into the EPM using the init account, enter the LDN number for this server as it appears in the Avaya Services database. If an LDN number is not specified for this server, Experience Portal uses the default value (000)000-0000.

MRCP Section

Field	Description
Ping Interval	When a speech application requires TTS rendering, the MPP establishes a connection to the TTS server at the beginning of a session. Experience Portal sends periodic "heartbeat" messages to the TTS server to make sure the connection is not terminated prematurely. This field specifies the number of seconds the Experience Portal system waits between the heartbeat messages. Enter an integer in this field. The default is 15. **Note:** The value specified in this field does not affect TTS timeout.
Response Timeout	An integer value specifying the number of seconds to wait for the TTS server to respond to a request for TTS before timing out. The default is 4.
Protocol	The MRCP protocol used for allocating the media processing server resources (TTS). The options are: • **MRCP V1** • **MRCP V2** — MRCPv2 option is shown only when you select Nuance in the **Engine Type** field. **Note:** If you have installed Avaya Aura® Media Server on the system, the only option available is **MRCP V1**. The default is MRCP V1.

Table continues…

Field	Description
RTSP URL	The URL of the Real-Time Streaming Protocol (RTSP) server. The RTSP server is the network remote control for the Experience Portal multimedia servers. The default path depends on which TTS engine type you select in the **Engine Type** field. If you change the **Engine Type**, this field also changes to a new default. To change the default path, first select the TTS engine type and then overwrite the default value in this field.
Enable Session XML	Displays when you select the MRCP V2 option in the **Protocol** field. Parameters specified in the `session.xml` file supersede vendor-specific parameters specified on the Applications webpage. The options are: • Yes: `Session.xml` specified for each voice application is sent to the speech server. If `Session.xml` is not specified for the voice application, the system generates and sends a `session.xml` file that consists of an organization and application name. • No: `Session.xml` is not sent to the speech server for any voice application.
Transport Protocol	This field is only shown when you select the MRCP V2 protocol under the MRCP section. The transport protocol used for transporting the real-time data. The options are: • **TLS** • **TCP** The default is TCP. The TLS option is shown only when you select Nuance in the **Engine Type** field. **Important:** • If you select TLS, ensure that the CA certificate that signed the identity certificate of the speech server is installed on Experience Portal as a trusted certificate. On the EPM navigation pane, click **Security > Certificates > Trusted Certificates**. Ensure that the required trusted certificate of the speech server is installed. If it is not uploaded, upload the certificate. • Click **System Maintenance > Log Viewer** to check for speech server connection errors.
Listener Port	This field is only shown when you select the MRCP V2 protocol under the MRCP section. Enter an integer value in the range 1 – 65535. The default is 5060 if you select MRCPV2 (TCP) protocol and 5061 for MRCPV2 (TLS) protocol.

SRTP Section

Note:

This group only appears if the **Transport Protocol** field is set to **TLS.**.

Field	Description
Enable	The options are: • **Yes** : This connection uses SRTP. • **No** : This connection does not use SRTP.
Encryption Algorithm	The options are: • **Yes** : AES_CM_128: This connection uses 128 key encryption. • **No** : None: Messages sent through this connection are not encrypted.
Authentication Algorithm	The options are: • **HMAC_SHA1_80**: Authentication is done with HMAC SHA-1 which uses 80 bit key for the authentication. • **HMAC_SHA1_32**: Authentication is done with HMAC SHA-1 which uses 32 bit key for the authentication.
RTCP Encryption Enabled	The options are: • **Yes:** This connection uses RTP Control Protocol encryption. • **No:** This connection does not use RTP Control Protocol encryption.
RTP Authentication Enabled	The options are: • **Yes:** This connection uses Real-time Transport Protocol authentication. • **No:** This connection does not use Real-time Transport Protocol authentication.
Add	Adds the SRTP configuration to the connection.

Configured SRTP List group

This group displays any SRTP configurations defined for the connection.

Note:

This group only appears if the Transport Protocol field is set to TLS.

Field	Description
Display list box	Displays the SRTP configurations for this connection.
Remove	Removes the association between the SRTP configuration selected in the display text box and the SIP connection.

Change TTS Server page field descriptions

Use this page to change an existing Text-to-Speech (TTS) server.

For all TTS changes except for Enable/Disable, after you save the changes, the **System Monitor** web page and the **MPP Manager** web page on EPM display the **Restart needed** configuration status for affected MPPs that are in the **Running** state. You must restart the affected MPPs before the applications can use the modified configuration.

This page contains the:

- General Section on page 462
- MRCP Section on page 465
- SRTP Section on page 467
- Configured SRTP List group on page 468

General Section

Field	Description
Zone	The name of the zone where the TTS server is configured. Select the name of the zone from the drop-down box. **Note:** The **Zone** drop-down box appears only if you have created zones on your Experience Portal system. If you do not create any new zones, you do not see the drop-down box.
Name	The unique identifier for this TTS server on the Experience Portal system. If you are using a Nuance server, this name must be between 1 and 32 characters. **Note:** You cannot change this name once you save the TTS server.

Table continues…

Field	Description
Enable	Whether this TTS server is available for use by the Experience Portal system. The default is **Yes**, which means the server is available. **Note:** When you change this value from **Yes** to **No**, no new calls will use this server. However, any calls in progress may continue to use the speech server. You must let the ongoing calls to complete before taking the speech server out of service to avoid application errors.
Engine Type	The type of TTS software engine the server uses. The options are: • **Loquendo** • **Nuance** The selection of an engine type in this field affects what the EPM displays as the defaults in the **Base Port**, **New Connection per Session**, **Voices** and **RTSP URL** fields as well. **Note:** Once you save the TTS server, this engine type cannot be changed. **Note:** To add a third-party TTS server type that mimics an existing TTS server, see Adding a third-party TTS Server type on page 450.
Network Address	The network address, or location, of the TTS server you want to use. This must be a valid network address in the form of a fully qualified hostname or an IP address. When you enter a network address in this field, the EPM automatically inserts the address as part of the **RTSP URL** field.
Base Port	The port number on the TTS server to which requests for TTS services are to be sent. The value for this field depends on the selected engine type and the MRCP protocol: • For Loquendo, the default is 554 • For Nuance, the default is port 4900 The default port value changes to 5060 if you select MRCPV2 (TCP) protocol and to 5061 for MRCPV2 (TLS) protocol. **Important:** These values are set to the default port numbers on the respective TTS servers. Unless you have manually changed the default settings on the TTS server, you should not have to change them here.

Table continues…

Field	Description
Total Number of Licensed TTS Resources	The total number of licensed TTS resources that is used by the Experience Portal system. Experience Portal uses this information to determine the total number of TTS resources available to the Experience Portal system.
New Connection per Session	Whether Experience Portal establishes a new connection on the TTS server for each call session. If you are using: • Loquendo, set this to **Yes** • Nuance, set this to **No** **Important:** You must use the above settings for this parameter.
Voices	Displays all voices that TTS servers can use on this system. Select an individual entry in this list by clicking on it, or use `Ctrl+Click` and `Shift +Click` to select multiple entries. Then, click the button to move the selected voices to the **Selected Voices** field. To move the voices back from the **Selected Voices** field to the **Voices** field, click on the button. This list of voices in the **Voices** field is prepopulated with the list of the voices that were available for the designated TTS engine type when Experience Portal was released. It is maintained in a special file on the Experience Portal system and is not automatically updated. You must verify that the voices you select here are actually installed and available on the target TTS server. You can add more voices to this list by clicking **Configuration>Speech Servers** from the EPM menu and selecting **Customize** in the TTS tab. **Note:** If a speech application is configured to use more language/voice combinations than are configured for any single TTS server, Experience Portal sends a `No TTS Resource` exception to the application. What happens then depends on the event handler that the application uses.
Selected Voices	All voices that you select in the **Voices** pane appear in this pane.
Listed Directory Number (LDN)	This field is only shown when you are logged into the EPM using the Avaya Services init account created when the Avaya Service accounts were configured. If you are logged into the EPM using the init account, enter the LDN number for this server as it appears in the Avaya Services database. If an LDN number is not specified for this server, Experience Portal uses the default value (000)000-0000.

MRCP Section

Field	Description
Ping Interval	When a speech application requires TTS rendering, the MPP establishes a connection to the TTS server at the beginning of a session. Because there is no way to know when the connection will be used during the session, Experience Portal sends periodic "heartbeat" messages to the TTS server to make sure the connection is not terminated prematurely. This field specifies the number of seconds the Experience Portal system waits between the heartbeat messages. Enter an integer in this field. The default is 15. **Note:** The value specified in this field does not affect TTS timeout.
Response Timeout	An integer value specifying the number of seconds to wait for the TTS server to respond to a request for TTS before timing out. The default is 4.
Protocol	The MRCP protocol used for allocating the media processing server resources (TTS). The options are: • **MRCP V1** • **MRCP V2** — MRCPv2 option is shown only when you select Nuance in the **Engine Type** field. **Note:** If you have installed Avaya Aura® Media Server on the system, the only option available is **MRCP V1**. The default is MRCP V1.

Table continues…

Field	Description
RTSP URL	The URL of the Real-Time Streaming Protocol (RTSP) server. The RTSP server is the network remote control for the Experience Portal multimedia servers. The default path depends on which TTS engine type you select in the **Engine Type** field. If you change the **Engine Type**, this field also changes to a new default. To change the default path, first select the TTS engine type and then overwrite the default value in this field.
Enable Session XML	Displays when you select the MRCP V2 option in the **Protocol** field. Parameters specified in the `session.xml` file supersede vendor-specific parameters specified on the Applications webpage. The options are: • Yes: `Session.xml` specified for each voice application is sent to the speech server. If `Session.xml` is not specified for the voice application, the system generates and sends a `session.xml` file that consists of an organization and application name. • No: `Session.xml` is not sent to the speech server for any voice application.

Table continues…

Field	Description
Transport Protocol	This field is only shown when you select the MRCP V2 protocol under the MRCP section. The transport protocol used for transporting the real-time data. The options are: • **TCP** • **TLS** The default is TCP. The TLS option is shown only when you select Nuance in the **Engine Type** field. **Important:** • If you select TLS, ensure that the CA certificate that signed the identity certificate of the speech server is installed on Experience Portal as a trusted certificate. On the EPM navigation pane, click **Security > Certificates > Trusted Certificates**. Ensure that the required trusted certificate of the speech server is installed. If it is not uploaded, upload the certificate. • Click **System Maintenance > Log Viewer** to check for speech server connection errors.
Listener Port	This field is only shown when you select the MRCP V2 protocol under the MRCP section. Enter an integer value in the range 1 – 65535. The default is 5060 if you select MRCPV2 (TCP) protocol and 5061 for MRCPV2 (TLS) protocol.

SRTP Section

Note:

This group only appears if the **Transport Protocol** field is set to **TLS**.

Field	Description
Enable	The options are: • **Yes** : This connection uses SRTP. • **No** : This connection does not use SRTP.
Encryption Algorithm	The options are: • **AES_CM_128**: This connection uses 128 key encryption. • **None**: Messages sent through this connection are not encrypted.

Table continues…

Field	Description
Authentication Algorithm	The options are: • **HMAC_SHA1_80**: Authentication is done with HMAC SHA-1 which uses 80 bit key for the authentication. • **HMAC_SHA1_32**: Authentication is done with HMAC SHA-1 which uses 32 bit key for the authentication.
RTCP Encryption Enabled	The options are: • **Yes** : This connection uses RTP Control Protocol encryption. • **No** : This connection does not use RTP Control Protocol encryption.
RTP Authentication Enabled	The options are: • **Yes** : This connection uses Real-time Transport Protocol authentication. • **No** : This connection does not use Real-time Transport Protocol authentication.
Add	Adds the SRTP configuration to the **Configured SRTP List.**

Configured SRTP List group

This group displays any SRTP configurations defined for the connection.

Note:

This group only appears if the **Transport Protocol** field is set to **TLS**.

Field	Description
Display list box	Displays the SRTP configurations for this connection.
Remove	Removes the association between the SRTP configuration selected in the display text box and the SIP connection.

Chapter 15: Application Server Manager

Application Server Manager in Avaya Experience Portal

Using the Application Server web page in the Experience Portal Manager (EPM), you can start and stop the Application server co-resident with the primary EPM.

You can also use this page to navigate to the Tomcat Manager web interface where users can deploy, undeploy, start, and stop applications on the Application server.

To access the Tomcat Manager web interface from EPM, you need the Tomcat user name created during the Tomcat application installation.

Important:

The Application Server page is displayed only when Avaya Experience Portal is installed on a single server and has a Tomcat application server installed. For more information, see the *Implementing Avaya Experience Portal on a single server* guide.

Application Server page field descriptions

Use the Application Server page to start and stop the application server co-resident with the primary Experience Portal Manager (EPM). You can also use this page to navigate to the Tomcat Manager web page where users can deploy, undeploy, start, and stop applications on the application server.

Important:

The Application Server page is displayed only when Avaya Experience Portal is installed on a single server and has a Tomcat application server installed on it. For details, see the *Implementing Avaya Experience Portal on a single server* guide.

This page contains the:

Application Server table

Field	Description
Selection check box	Indicates the application servers in the Experience Portal system. To select all application servers, click the check box in the header row.
Host Address	The application server host address. To access the Tomcat Manager web page, click the host address of the server. Experience Portal displays the Tomcat Manager web page in a separate window. **Note:** The link to the Tomcat Manager web page is enabled when the application server state is **Running**.
State	The operational state of the application server.

State Commands group

Note:

The system enables these buttons when you select one or more application servers using the selection check box in the Application Server table.

Button	Description
Start	Starts the application server and changes the operational state to Running.
Stop	Stops the application server and changes the operational state to Stopped. **Note:** All applications available on the application server are stopped.

Starting Application server

Procedure

1. On the EPM navigation pane, click **System Management** > **Application Server**.
2. Select the check box for the application server you want to start.
3. In the **State Commands** group, click **Start** and confirm your selection when prompted.
4. After a few minutes, click **Refresh** and verify that the **State** is **Running**.

Logging in to the Tomcat Manager web interface from Avaya Experience Portal

About this task

Using the Experience Portal Manager (EPM) web interface, you can navigate to the *Tomcat Web Application Manager* page, where users can deploy, remove, start, and stop applications on the application server.

The login account for accessing the Tomcat Manager web interface is different from your EPM user name.

Procedure

1. Log in to the EPM web interface.
2. On the EPM navigation pane, click **System Management** > **Application Server**.
3. Click the host address of the server.

   EPM opens a new browser window and displays the login dialog box for the Tomcat Manager web interface.
4. On the **Tomcat Manager** login page, in the **User Name** field, enter your Tomcat user name.

   The user name is case-sensitive. It must exactly match an existing Tomcat account name.
5. In the **Password** field, enter your login password.

   The password is case-sensitive. It must exactly match the password assigned to the specified user name.
6. Click **OK**.

   If your user name and password:

   - Matches an authorized Tomcat user account, the Tomcat Web Application Manager page is displayed in a new browser window.
   - Does not match an authorized Tomcat user account, the login dialog box is displayed again.

Chapter 16: Managed Applications in Avaya Experience Portal

Overview

Managed applications are special classes of applications that derive the licensing, administration framework, manageability, and accessibility from the Avaya Experience Portal management system.

Experience Portal is the single point of management for managed applications.

For example, Avaya Proactive Outreach Manager is a managed application that runs on Experience Portal. Avaya Proactive Outreach Manager uses the Experience Portal platform to create and deliver automated campaigns to support Finance, Marketing, and Healthcare needs for automation.

Note:

For more information, see the documentation delivered with the managed applications.

Experience Portal provides the following capabilities for managed applications:

- Acquire and maintain licenses on page 472
- Add managed application to EPM on page 473
- Role-based access on page 474
- Multi-tenancy on page 474
- Logging and Alarming on page 474
- Reports related to managed applications on page 475

Managed applications related menus, web pages, and associated online help are installed and integrated into the EPM by the managed application installer.

Acquire and maintain licenses

The managed application installer adds the licensing information to the licensing tables in the Experience Portal database. Experience Portal retrieves this information from the database and acquires the licenses for the managed applications from the license server.

Experience Portal also handles the license expiry and grace period for the managed application licenses. Experience Portal provides a thirty-day grace period under the following conditions:

- Managed application is installed, and the managed application license is not available on the license server. Durng the installation, the managed application specifies the licensed values allowed during the grace period.
- License server is not available or accessible from the EPM.
- Managed application license has expired.

Note:

Experience Portal generates appropriate alarms for these conditions.

Experience Portal generates an alarm seven days before the managed application license expiry.

Once a grace period is initiated, EPM generates an alarm every day till the issue is resolved or the grace period expires.

Managed applications periodically retrieve the license information from the EPM and take appropriate actions based on the licensed values.

When the grace period expires:

- The licensed features of the managed application are reset to zero.
- The configuration and management web pages of the managed application are still available in EPM, but they do not function.

You can view and configure the license details of the managed application from the Licensing web page in EPM.

For more information on acquiring and maintaining licenses of the managed application, see the documentation delivered with the managed application.

Add managed application to EPM

The managed application installer adds additional pages and fields to the EPM. The user roles determine which pages and fields the user can see and what actions the user can perform. A managed application may add additional fields to existing EPM pages or new pages with new fields.

A managed application may also add an additional application type during installation. This application type is available in the Add Application page as an option in the **Type** field.

For more information about the pages and fields related to the managed application, see the documentation delivered with the managed application.

Note:

You must log in to the EPM web interface on the primary EPM server to perform any managed application related administrative tasks.

Role-based access

The managed application installer may add new features to existing roles or additional roles and features to the EPM.

Experience Portal enables you to create custom roles that are based on existing roles and managed application roles. The user roles determine which pages the user can see and what actions the user can perform in EPM.

You can create new users and assign them managed application based roles and Experience Portal based roles.

For more information on roles and features related to the managed application, see the documentation delivered with the managed application.

Note:

The EPM administrator role can access managed application features when the managed application is installed on Experience Portal.

Multi-tenancy

The multi-tenancy feature in Experience Portal allows the configuration data and reports maintained by the Experience Portal Manager (EPM) to be segmented for multiple organizations. Managed applications can take advantage of the multi-tenancy feature and segment their data for multiple organizations.

For more information on multi-tenancy, see Organization level access in Avaya Experience Portal on page 115.

For more information on the multi tenancy feature related to managed applications, see the documentation delivered with the managed application.

Logging and Alarming

Avaya Experience Portal enables you to view audit logs, event logs, and alarms generated by managed applications.

The managed application installer may add the following additional categories:

- Audit log categories: These categories are available on the **Audit Log Viewer** EPM web page with the EPM audit log categories. You can use the Audit log categories for filtering the audit logs.
- Event log categories: These categories are available on the **Log Viewer** EPM web page with the EPM event log categories. You can use the Event log categories for filtering the event logs.
- Alarm categories: These categories are available on the **Alarm Manager** EPM web page with the EPM alarm categories. You can use the Alarm categories for filtering the alarms.

Note:

The retention of the audit logs, event logs, and alarms is based on the purge and retention settings specified on the **Alarm/Log Options** EPM web page.

For more information on logging and alarming related to managed applications, see the documentation delivered with the managed application.

Reports related to managed applications

The managed application installer adds additional standard reports to Experience Portal which are available on the Standard Reports page of the EPM web page. You can create and schedule custom reports based on these standard reports.

For more information about standard reports related to managed applications, see the documentation delivered with the managed application.

Chapter 17: Intelligent Customer Routing (ICR) functionality in Avaya Experience Portal

Intelligent Customer Routing overview

Intelligent Customer Routing (ICR) derives the licensing, administration framework, manageability, and accessibility from Avaya Experience Portal.

ICR uses the Experience Portal platform to identify and determine caller intent through simple, intelligent, customer conversations using speech and self-service, and, when necessary, routes the call to a relevant call center across applicable geographic locations. Using Avaya Call Center Best Services Routing (BSR) infrastructure, ICR routes calls to the most preferred resource available. Once a route decision is made, the call is either transferred directly to the selected location, or a virtual call is placed and parked on the Experience Portal and enhanced wait treatment is performed.

Note:

For more information, see the ICR documentation library posted on the Avaya support site at http://support.avaya.com under the appropriate release in the Intelligent Customer Routing product category.

ICR related menus, web pages, and associated online help are installed and integrated into the EPM by the ICR installer.

Acquire and maintain licenses

The ICR installer adds the licensing information to the licensing tables in the Experience Portal database. Experience Portal retrieves this information from the database and acquires the licenses for ICR from the license server.

Experience Portal also handles the license expiry and grace period for the ICR licenses. Experience Portal provides a thirty day grace period under the following conditions:

- ICR is installed and the ICR license is not available on the license server. The licensed values allowed during the grace period are specified by ICR during installation.

- License server is no longer available or accessible from the EPM.
- ICR license has expired.

Note:

Experience Portal generates appropriate alarms for these conditions.

Experience Portal generates an alarm, seven days prior to the ICR license expiry.

Once a grace period is initiated, EPM generates an alarm every day till the issue is resolved or the grace period expires.

ICR periodically retrieve the license information from the EPM and take appropriate actions based on the licensed values.

When the grace period expires:

- The licensed features of ICR are reset to zero.
- The configuration and management web pages of ICR are still available in EPM but they do not function.

You can view and configure the license details of ICR from the Licensing web page in EPM.

Note:

For more information, see the ICR documentation library posted on the Avaya support site at http://support.avaya.com under the appropriate release in the Intelligent Customer Routing product category.

Configure ICR in EPM

The ICR installer adds new pages and fields to the EPM. The user roles determine which pages and fields the user can see and what actions the user can perform.

ICR adds an additional application type during the installation. This application type is available in the **EPM > System Configuration > Applications > Add Application** page as an option in the **Type** field.

You must login to the EPM web interface on the primary EPM server to perform any ICR related administrative tasks.

Note:

For more information, see the ICR documentation library posted on the Avaya support site at http://support.avaya.com under the appropriate release in the Intelligent Customer Routing product category.

Role-based access

The ICR installer adds new features to existing roles and an additional role to the EPM.

Experience Portal enables you to create custom roles which are based on existing roles and managed application roles. The user roles determine which pages the user can see and what actions the user can perform in EPM.

You can create new users and assign them ICR based roles as well as Experience Portal based roles.

Note:

For more information, see the ICR documentation library posted on the Avaya support site at http://support.avaya.com under the appropriate release in the Intelligent Customer Routing product category.

The EPM administrator role can access ICR features when ICR is installed on Experience Portal.

Multi-tenancy

The multi-tenancy feature in Experience Portal allows the configuration data and reports maintained by the Experience Portal Manager (EPM) to be segmented for multiple organizations. ICR can take advantage of the multi-tenancy feature and segment the data for multiple organizations.

For more information on multi-tenancy, see Organization level access in Avaya Experience Portal on page 115.

Database Backup and Restore

Using the System Backup feature in EPM, you can regularly back up data in a local Experience Portal database and the associated properties files. System Backup takes both EP and ICR database backup.

For more information, see System Backup Overview on page 215.

Using Database Restore utility, you can restore the Experience Portal database, including ICR data, from a backup created through the System Backup web page in EPM.

For more information, see Database Restore utility and system backup on page 225.

Logging and Alarming

Experience Portal enables you to view audit logs, event logs, and alarms generated by ICR.

The ICR installer adds the following additional categories:

- Audit log categories. These categories are available in the **Audit Log Viewer** EPM web page along with the EPM audit log categories and can be used for filtering the audit logs.
- Event log categories. These categories are available in the **Log Viewer** EPM web page along with the EPM event log categories and can be used for filtering the event logs.
- Alarm categories. These categories are available in the **Alarm Manager** EPM web page along with the EPM alarm categories and can be used for filtering the alarms.

Note:

The retention of the audit logs, event logs, and alarms is based on the purge and retention settings specified in the **Alarm/Log Options** EPM web page.

Note:

For more information, see the ICR documentation library posted on the Avaya support site at http://support.avaya.com under the appropriate release in the Intelligent Customer Routing product category.

Reports related to ICR

The ICR installer adds additional standard reports to Experience Portal. These additional standard reports are available under **Standard Reports** on the EPM web page. You can create and schedule custom reports based on these standard reports.

Note:

For more information, see the ICR documentation library posted on the Avaya support site at http://support.avaya.com under the appropriate release in the Intelligent Customer Routing product category.

Chapter 18: Integrated Voice and Video Response

The Integrated Voice and Video Response (IVVR) is an extension to the voice support capabilities of the Avaya Experience Portal system. It combines the standard Experience Portal audio processing with video streaming between two endpoints.

IVVR uses the 3G video enabled devices and SIP-based video phones to deliver multi-modal communication capabilities to end users. IVVR supports video streaming, in addition to static and dynamic menu creation, and audio prompting.

You can use the following VoiceXML tags when designing a video enabled application:

- `<media>`: This tag is used to specify a new definition of non-audio media content such as video.
- `<seq>`: This is a control tag used to queue up media files for playback in a sequential order.
- `<para>`: This is a control tag used to queue up items to be played in parallel.

Note:

Video streaming is supported only in SIP based deployments.

The video server that supports the IVVR is available on the MPP. However, to use the IVVR feature, you must have the **Video Server Connections** license. This license enables or disables the support for the video server.

You can configure the IVVR feature by specifying the **Video Enable** option value to **Yes** or **No** while configuring the application. To enable the video server, set the license value to a non-zero number. To disable the video server, set the license value to zero.

Chapter 19: Avaya Experience Portal system events

Viewing Avaya Experience Portal system status

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **Real-time Monitoring** > **System Monitor**.
3. On the System Monitor page, do one of the following:
   - To view the overall status for all Avaya Experience Portal systems in the network: Go to the Summary tab.
   - To view the status for the EPM and all MPPs in the local Experience Portal system: Go to the <System name> Details tab.
   - To view detailed information for an MPP: Go to the <System name> Details tab, in the **Server Name** column, click the name of the MPP.
   - To view detailed alarm information: Click any yellow or red alarm indicator.

   Tip:

   The information on this page refreshes automatically if you leave the browser window open.
4. **(Optional)** On the EPM navigation pane, click **Real-time Monitoring** > **Active Calls**to check the resources being used by all current applications in the system.

Summary tab on the System Monitor page field descriptions

Use this tab for a consolidated view of the health and status of the Experience Portal system. The information on this page refreshes automatically if you leave the browser window open.

Note:

If the EPM server needs to be restarted, Experience Portal displays the message "EPM needs to be restarted." in red text just above the system status table.

Column	Description
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
System Name	The name of the Experience Portal system, as specified in the **Avaya Experience Portal Name** field on the EPM Settings page. If your installation consists of multiple Experience Portal systems that share a common external database, this column contains: • The name of the local system that you currently logged into. The **Type** for this system will always be **EP**. • The name of the another Experience Portal system in the shared external database. The **Type** will always be **Remote EP**. Click the system name to log into the EPM web interface for the remote system.
Type	If your installation consists of a single Experience Portal system, the type will always be **EP**. If your installation consists of multiple Experience Portal systems that share a common external database, this column contains: • **EP**: This type indicates that you are currently logged into the EPM for this system. Any system commands you issue will affect this EPM and any media servers assigned to this system. The <System name> Details tab for this system shows the assigned media servers. • **Remote EP**: This type indicates that this is an active Experience Portal system, but it is *not* the system you are currently logged into. To affect the EPM or media servers assigned to a remote system, you must first log into that system by clicking the remote system name in the **System Name** column.

Table continues…

Column	Description
State	Displays the operational state of the Experience Portal system. The options are: • **Active**: This Experience Portal system is updating its information in the database on a regular basis. • **Inactive**: A remote Experience Portal system of **Type** is **Remote EP** is no longer updating information in the shared database. Click the system name to log into the EPM on that system and troubleshoot the problem locally. • **Stale**: It has been over an hour since this Experience Portal system has updated its summary information in the database. Create an Alarm report to view the error messages generated by the system. **Note:** If you are using an external database, the time difference between your Experience Portal systems is too great. For more information, see the *Time Synchronization between external database and EPM servers* topic in the *Troubleshooting Avaya Experience Portal* guide. **Tip:** To view the date and time that this state was first reached and on which it was last changed, hover the mouse over this column.
Call Capacity	This field displays: • **Current**: The number of calls that can be currently handled by the system. • **Licensed**: The number of licenses allocated to this system. • **Maximum**: The maximum number of simultaneous calls that the media servers in this system can handle. This value is obtained by adding together the maximum number of calls set for each of the media servers in the system. This value can be larger than the number of licenses allocated to the system, but it should never be smaller. If it is smaller, then some of your licenses will never be used.
Active Calls	When the number of active calls (In or Out) is greater than zero, the number displayed on the System Monitor is displayed as a link. Clicking on this link takes the user to the Active Calls web page.
Alarms	This field displays one of the following alarm status indicators: • Green: There are no active major or critical alarms • Yellow: There are one or more active minor alarms • Red: There are one or more active major or critical alarms For a system whose **Type** is **EP**, you can click any red or yellow alarm indicator to view an associated Alarm report. To view the alarms for a system whose **Type** is **Remote EP**, you must first log into the remote system by clicking the name in the **System Name** column.

<System name> Details tab on the System Monitor page field descriptions

Use this tab for a detailed view of the health and status of the EPM and each MPP in the Experience Portal system named in <*System Name*>. The information on this page refreshes automatically if you leave the browser window open.

Note:

If the EPM server needs to be restarted, Experience Portal displays the message "EPM needs to be restarted." in red text just above the system status table.

Column	Description
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
Zone	The zone where the EPM and the MPP servers are configured.
Server Name	The options are: • The name of the EPM server. Click this name to view the <EPM Name> Details page. • The name of an MPP running on the system. Click this name to view the <MPP name> Details page. • *<EPM Name>/<MPP Name>*, if an MPP resides on the same server as the EPM. Click this name to view the <MPP name> Details page.
Type	The options are: • **EPM**: The Experience Portal Manager • **MPP**: A Media Processing Platform **Tip:** To verify whether the associated server is a primary or auxiliary EPM server, hover the mouse over the EPM field.

Table continues…

Column	Description
Mode	The operational mode of the Media Server. The options are: • **Online**: The Media Server is available. • **Offline**: The Media Server is unavailable and is not being polled by the EPM server. • **Test**: (MPP only) The Media Server is available to handle calls made to one of the defined H.323 maintenance stations. **Tip:** To view the date and time that this mode was first reached, hover the mouse over this column.

Table continues…

Column	Description
State	The operational state of the Media Server. The options are: • **Booting**: The Media Server is in the process of restarting and is not yet ready to take new calls. • **Degraded**: The Media Server is running but it is not functioning at full capacity. • **Error**: The Media Server has encountered a severe problem and cannot recover. • **Halted**: The Media Server is no longer responding to heartbeats because it received a **`Halt`** command. • **Halting**: The Media Server is responding to heartbeats but is not taking new calls. • **Need Configuration**: An Email or SMS processor residing on the Media Server has not yet been configured. • **Need Connections**: No connections (SMPP or HTTP) have been configured or assigned to an Email/SMS processor residing on the Media Server. • **Never Used**: The Media Server has never successfully responded to a heartbeat request. • **Not Installed**: The Media Server is missing files required for heartbeat requests to occur. • **Not Responding**: The Media Server is not responding to heartbeat requests and it has not received a **`Restart`** or **`Halt`** command. • **Partially Running**: (EPM only) The Media Server is in the process of starting up, and not all individual components of the service, for example: Tomcat, SL, ActiveMQ, have come up yet. • **Rebooting**: The Media Server is responding to heartbeats but is not taking new calls. • **Recovering**: The Media Server has encountered a problem and is attempting to recover. • **Restart Needed**: This state is most often reached when the Media Server has encountered a problem that it cannot recover from and it requires a manual restart. However, it can also appear for an MPP when the EPM software has been upgraded and the MPP software has not. In that case, the state should update automatically when you upgrade the MPP software. • **Running**: The Media Server is responding to heartbeat requests and is accepting new calls. • **Starting**: The Media Server is responding to heartbeats but not taking new calls because it is transitioning from the Stopped state to the Running state. • **Stopped**: The Media Server is responding to heartbeats but is not taking new calls. The Media Server enters this state while it initializes after it restarts or when a **`Stop`** command is received. • **Stopping**: The Media Server is responding to heartbeats but is not taking new calls.

Table continues…

Column	Description
	• **Unknown**: The Media Server is in the Offline mode. **Tip:** To view the date and time that this state was first reached, hover the mouse over this column.
Active Command	This column is displayed if one or more Media Servers are currently in transition from their current state to a new user-requested state. For each transitional Media Server, this column displays the requested, or final, state. For any other Media Servers in the system, this field displays **None**.
Config	The configuration state of the Auxiliary EPM/MPP. The options are: • **Need certificates**: The Primary EPM certificate must be downloaded to the Auxiliary EPM/MPP by running the **`setup_vpms.php`** script on the Auxiliary EPM/MPP. • **Need ports**: The MPP has been configured and is waiting for ports to be assigned. • **None**: The MPP has never been configured. • **OK**: The Auxiliary EPM/MPP is currently operating using the last downloaded configuration. • **Restart needed**: The MPP must be restarted to enable the downloaded configuration. • **Reboot needed**: The MPP must be rebooted to enable the downloaded configuration. • **Upgrade needed**: The Auxiliary EPM must be upgraded to the same version of the software as on the Primary EPM. • **Unknown**: The MPP is either not responding or is in the Offline mode.
Call Capacity	This field displays: • **Current**: The number of calls that can be currently handled by the system. • **Licensed**: The number of licenses allocated to this system. • **Maximum**: The maximum number of simultaneous calls that the MPPs in this system can handle. This value is obtained by adding together the maximum number of calls set for each of the MPPs in the system. **Note:** This value can be larger than the number of licenses allocated to the system, but it should never be smaller. If it is smaller, then some of your licenses will never be used.

Table continues…

Column	Description
Active Calls	This field displays: • **In**: The number of active incoming calls in the system. • **Out**: The number of active outgoing calls in the system. Clicking the number displayed under the **Active Calls In** column displays all the active incoming calls for the media servers. Clicking the number displayed under the **Active Calls Out** column displays all the active outgoing calls for the media servers.
Calls Today	The number of calls handled during the current day.
Alarms	The alarm status indicators for the EPM, each MPP, and the overall Experience Portal system. The options are: • Green: There are no active major or critical alarms • Yellow: There are one or more active minor alarms • Red: There are one or more active major or critical alarms **Tip:** You can click any red or yellow alarm indicator to view the Alarm report for that system.
Summary	The total number of calls based on **Contact Summary** and **Active Calls**. On the Summary line, clicking the number displayed under the **Active Calls In** column displays all the active incoming calls for the media servers. On the Summary line, clicking the number displayed under the **Active Calls Out** column displays all the active outgoing calls for the media servers.

Email, HTML and SMS processors section

Column	Description
Zone	The zone where the Email and SMS processors are configured. The summary reports within a zone are: • **Email Summary**: Summary of the incoming and outgoing email messages in the last 24 hours. • **SMS Summary**: Summary of the incoming and outgoing SMS messages in the last 24 hours. • **HTML Summary**: Summary of the incoming HTML messages in the last 24 hours.
Server Name	The name of the EPM on which the Email, SMS and HTML processors are configured.

Table continues…

Column	Description
Type	The options are: • Email processor • HTML processor • SMS processor
State	The operational state of the email/SMS/HTML processors. The options are: • **Not Running**: The server is either stopped or not started yet. • **Starting**: The server start request is initiated, and is in the process of initialization. • **Running**: The server is up and functional. • **Stopping**: The server shutdown is requested. • **Need Configuration**: The server does not find configuration. • **Need Connections**: The server has configuration but does not have any connections assigned or configured. • **Degraded**: The server has configuration and connections. However, some or all connections are not working. • **Error**: The server data returned has been deemed "stale" (no new data retrieved after a period of 3 minutes), or 2) unexpected return code retrieved from a poll to server. • **Stopped**: The server is stopped.
Usage (Today)	Displays the number of messages processed during the current day. The Summary row also shows the maximum number of messages allowed per day.
Messages (Last 24 hours)	The options are: • Incoming: The number of incoming messages processed in the last 24 hours. • Outgoing: The number of outgoing messages processed in the last 24 hours. **Note:** Clicking on the **Last 24 hours** text, lets the user to change the number of messages displayed for the following time frames: • Last hour • Last 3 hours • Last 6 hours • Last 12 hours • Last 24 hours
Timeline Graph 	Displays a graph icon. Clicking this graph icon displays the number of messages processed in a graphical form.

Events and alarms

Events and alarms

The Experience Portal Manager (EPM) or Media Processing Platform (MPP) software generates an *event* when it encounters any of the following:

- A minor problem
- A change to the system
- A change to the system resources

If a specific event is repeated several times in succession, or if the EPM or an MPP encounters a serious problem, the system raises an *alarm*. All alarms have an associated event, but not all events have an associated alarm.

Events and alarms are:

- Divided into categories based on the component that generated them
- Assigned a severity so that you can quickly find the critical issues

In addition, alarms have a status that you can change to indicate that the issue described in the alarm message has been dealt with.

You cannot control the events and alarms generated by the EPM or an MPP, but you can control:

- When Experience Portal notifies you about high CPU, RAM, and disk space usage
- How long the system stores event and retired alarm records

Event and alarm categories

Every event and alarm is part of one of the following categories:

Column	Description
EP Administration	Messages related to administration activities on the Experience Portal Manager (EPM).
EP Application Interface Service	Messages related to the Application Interface REST web service. This web service runs on the EPM server and allows customer applications to send multi-media messages and starts multi-media applications.
EP Application Interface WS	Messages related to the Application Interface SOAP web service. This web service runs on the EPM server and allows customer applications to initiate outbound calls, send multi-media messages, and starts multi-media applications.

Table continues…

EP Application Interface WS 2.0	Messages related to the Application Interface SOAP web service 2.0. This version is functionally equivalent to the previous one. While there is a single username or password for the former, the new version provides the added facility of allowing multiple users to access the web service.
EP Application Logger	Messages related to the Experience Portal application logger. The application logger is a web service running on Experience Portal which allows Orchestration Designer applications to log messages to the EPM.
EP ASR	Messages related to Automatic Speech Recognition (ASR).
EP Backup	Messages related to the EP Backup subsystem, which provides the means to perform on-demand or scheduled backup operation.
EP Carrier Service	Messages related to the Carrier REST web service, which allows you to retrieve mobile related information from a carrier.
EP CCXML Browser	Messages related to the Call Control eXtensible Markup Language (CCXML) browser, which controls all call handling for all Voice eXtensible Markup Language (VoiceXML) applications.
EP Event Manager	Messages related to the Event Manager, which collects events from other Media Processing Platform (MPP) processes and sends them to the network log web service on the EPM.
EP Licensing	Messages related to port licensing.
EP Listener	Messages related to the Alarm Codes Destinations types (Listeners) where the alarm notification is delivered.
EP Management Service	Messages related to the Experience Portal Management REST web service, which allows you to configure and manage an EPM.
EP Management WS	Messages related to the Experience Portal Management SOAP web service. This web service runs on the EPM server and allows you to configure and manage a EPM.
EP Media Manager	Messages related to audio and video Real-time Transport Protocol (RTP) connections.
EP MMS	Messages related to the MPP Management Service (MMS), which stores configuration information and controls the initialization and operation of an MPP.
EP Media Server Manager	Messages related to the MPP management subsystem, which provides the means to start and stop call processing.
EP MPP System Manager	Messages related to the MPP System Manager process, which manages and monitors MPP processes, configuration, licensing, and system resources.
EP MRCP	Messages related to Media Resource Control Protocol (MRCP), which is an open standard for speech interfaces.
EP Reporting	Messages related to the collection of report data and the generation of reports.
EP Session Manager	Messages related to the MPP Session Manager, which coordinates the low-level interactions between the ASR, TTS, and telephony components and the VoiceXML and CCXML browsers.
EP SNMP Agent	Messages related to the SNMP agent, which collects and stores management information and makes this information available to SNMP managers.

Table continues…

EP Telephony	Messages related to the H.323 connections and Voice over IP (VoIP) telephony interfaces.
EP Trace	Messages related to the EP trace reports. It provides the means to collect trace data from EPM or specific MPP.
EP TTS	Messages related to Text-to-Speech (TTS).
EP Upgrade Manager	Messages related to software upgrades for MPPs running on the EPM.
EP Email Processor	Messages related to the EP Email Processor.
EP SMS Processor	Messages related to the EP SMS Processor.
EP Text Browser	Messages related to the EP Text Processor.

Event severities

Event Severity	Description
Info	Informational message about the system or its resources.
Warning	Indicates that no immediate action is necessary, but the system condition needs to be monitored.
Error	Indicates a potentially serious problem that needs to be fixed soon.
Fatal	Indicates a problem that is interrupting service. Immediate action is needed.

Alarm severities

Alarm Severity	Description
Minor	Indicates that no immediate action is necessary, but the system condition needs to be monitored.
Major	Indicates a potentially serious problem that needs to be fixed soon.
Critical	Indicates a problem that is interrupting service. Immediate action is needed.

Alarm statuses

Status	Description
Unacknowledged	When an event or alarm is issued, Experience Portal sets the alarm status to Unacknowledged to indicate that the alarm is new. Experience Portal deletes Unacknowledged alarms from the database depending on the alarm retention period that you specify in the Alarm/Log Options page.

Table continues…

Status	Description
Acknowledged	You can set the event or alarm status to Acknowledged to indicate that you have seen the information but want to refer back to the event or alarm at a later point. Experience Portal deletes Acknowledged alarms from the database depending on the alarm retention period that you specify in the Alarm/Log Options page.
Retired	You can set the event or alarm status to Retired to indicate that you no longer need to refer to the alarm. Experience Portal deletes Retired alarms from the database depending on the alarm retention period that you specify in the Alarm/Log Options page.

Resource thresholds for events and alarms

When the use of system resources exceeds certain levels, the performance of the system as a whole can be impaired. Therefore, you want the system to issue an alarm when these levels are exceeded so that you can take appropriate action before the situation becomes critical.

For Experience Portal, you can specify a high water and low water setting for CPU, memory, and disk usage.

- **High Water**: When a resource exceeds its high water setting for the first time, the system generates an alarm. Experience Portal does not generate another alarm for this resource until the resource usage goes back down below the low water setting and then rises back above the high water setting.

  You can view high water alarms by generating an alarm report.

- **Low Water**: When a resource exceeds its low water setting at any time, the system generates an informational event with a severity of **Info**.

  If your system is configured to send informational events to the EPM, you can view low water events by generating an event report. Otherwise, you need to see the System Manager process log, which is accessible from the Log Directories page on the Media Server Service Menu.

For information on:

- Setting the level of events that are sent to the EPM, see Setting the resource thresholds for events and alarms on page 493.
- Setting which events are available in an event report, see Setting the global grace period and trace level parameters on page 271.

Setting the resource thresholds for events and alarms

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** > **MPP Servers**.
3. On the MPP Servers page, click **MPP Settings**.

4. On the MPP Settings page, go to the **Resource Alerting Thresholds (%)** section.
5. For the **CPU** field, enter the following information:
    a. **High Water**: Enter the percentage of the CPU that the system must exceed before an alarm is generated.

       The system generates one alarm each time the CPU percentage goes from being below the low water threshold to being above the high water threshold. In other words, once a high water alarm is generated, another alarm does not occur until the CPU percentage falls back down below the low water setting and then rises above the high water setting again. The default is 70.

    b. **Low Water**: Enter the percentage of the CPU that the system must fall below before an event is generated.

       The system generates one event each time the CPU percentage goes from being above the low water threshold to being below it. In other words, once a low water event is generated, another event does not occur until the CPU percentage rises above the low water setting and then falls below it again. The default is 60.
6. For the **Memory** field, enter the following information:
    a. **High Water**: Enter the percentage of the available RAM that the system must exceed before an alarm is generated.

       The system generates one alarm each time the percentage of the available RAM goes from being below the high water threshold to being above it. The default is 50.

    b. **Low Water**: Enter the percentage of the available RAM that the system must fall below before an event is generated.

       The system generates one event each time the percentage of the available RAM goes from being above the low water threshold to being below it. The default is 40.
7. For the **Disk** field, enter the following information:
    a. **High Water**: Enter the percentage of disk space that the system must exceed before an alarm is generated.

       The system generates one alarm each time the percentage of disk space being used goes from being below the high water threshold to being above it. The default is 80.

    b. **Low Water**: Enter the percentage of disk space that the system must fall below before an event is generated.

       The system generates one event each time the percentage of disk space being used goes from being above the low water threshold to being below it. The default is 60.

Setting log data retention periods

About this task

The Experience Portal viewer setting parameters determine whether event, retired alarms, and audit log records are automatically deleted from the database when the specified retention period expires.

Note:

Experience Portal only purges Retired alarms. Experience Portal does not automatically remove Unacknowledged and Acknowledged alarms from the database.

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** > **EPM Servers** > **Alarm/Log Options**.
3. On the Alarm/Log Options page, enter appropriate information, and click **Save**.

Creating an event report

About this task

The following fields on the Alarm/Log Options page can affect the event report:

- The **Logs** group fields determine whether old events are automatically deleted from the database and how long these events remain in the database.
- The **Maximum Report Pages** field in the **Alarms/Logs/Audit Logs Report Size** group affects the length of time that elapses before Experience Portal displays the report. You can set how many pages Experience Portal generates before it displays the first page.

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **System Maintenance** > **Log Viewer**.
3. On the Log Viewer page, enter the filter criteria that you want to use, and click **OK**.

   The EPM displays the Log Report page. The Log Report only displays the first 10,000 entries that match the specified criteria as generating this report can take a long time if the Experience Portal database contains a large number of event records.

Next steps

You can view any available exception information for an event by clicking the **More** link in the **Event Message** field.

Creating an alarm report

About this task

The amount of data available for this report depends on the **Retention Period** setting in the **Alarms** group on the Alarm/Log Options page.

For example, if this value is set to 14, you can enter a start date that is two weeks prior to the current date. If the value is set to 7, you can only check for the previous week.

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **System Maintenance** > **Alarm Manager**.
3. On the Alarm Manager page, enter the filter criteria that you want to use, and click **OK**.

   The EPM displays the Alarm Report page.
4. In the **Event Code** column, click the link to view the associated event details for an alarm.

   The EPM displays the Log Report for Event page.

Viewing alarms by alarm category

About this task

The **Alarms** column displays one of the following alarm status indicators for the EPM, MPP, and the overall Experience Portal system:

- Green: There are no active major or critical alarms
- Yellow: There are one or more active minor alarms
- Red: There are one or more active major or critical alarms

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **Real-time Monitoring** > **System Monitor**.
3. On the System Monitor page, click the <System name> Details tab.
4. To view the alarms in each alarm category for EPM, MPP, or the overall Experience Portal system, click any red or yellow alarm indicator at the end of the appropriate row.

   The EPM displays the Alarm Monitor page.
5. To view an alarm report for a given category, on the Alarm Monitor page, in the **Status** column, click any red or yellow alarm indicator.

   The EPM displays the Alarm Report page showing all alarms in the selected category.

6. To view the associated event details for an alarm, click the link in the **Event Code** column.

   The EPM displays the Log Report for Event page.

Changing the status of an alarm

Procedure

1. Log on to the EPM web interface by using an account with the Administration or Operations user role.
2. On the EPM navigation pane, click **System Maintenance** > **Alarm Manager**.
3. On the Alarm Manager page, enter the filter criteria that you want to use and click **OK**.
4. On the Alarm Report page, select the alarms that you want to change the status of.
5. In the **Change Alarm Status** group at the bottom of the page, select one of the following:
   - **Selected alarms on this page**: To change the status of only the alarms you selected.
   - **All alarms on this report**: To change the status of all alarms in this report regardless of which alarms are selected.
6. In the **New Status** field, click one of the following status to assign to the alarms:
   - **ACK**: To set the alarm status to Acknowledged.
   - **RETIRED**: To set the alarm status to Retired.
7. Click **Submit**.

Viewing the status changes made to an alarm

Procedure

1. Log on to the EPM web interface by using an account with the Administration or Operations user role.
2. On the EPM navigation pane, click **System Maintenance** > **Alarm Manager**.
3. On the Alarm Manager page, enter the filter criteria that you want to use and click **OK**.
4. On the Alarm Report page, in the **Alarm Status** column, select one of the following:
   - **ACK**
   - **RETIRED**

   The EPM displays the Alarm History window.

Alarm Manager page field descriptions

Use this page to select filtering options and alarm categories and severities when creating an alarm report.

This page contains the:

General section

Field	Description
Zones	Select the name of the zone from the drop-down box. You can filter the records based on the zone that you select. **Note:** The **Zones** drop-down box appears only when you create new zones. If you do not create any new zones, you do not see the drop-down box.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon
Servers	The name of the system for which you want to view alarms. The options are: • **All servers** • The EPM • A specific MPP • A combination of systems by selecting the first system and then using `Shift+Click` to select a range of systems or `Ctrl+Click` to select individual systems. The default is **All servers**.

Table continues…

Field	Description
Search Keywords	The text to search for in the alarm records. The search is case insensitive and based on a substring match, not a whole string match. For example, “Acknowledged” matches “acknowledged”, “ACKNOWLEDGED”, and “unacknowledged”. The search uses a logical OR when combining keywords. You can separate multiple entries with a comma, and use the tilde character (~) to indicate NOT. For example, if you enter `login, logoff, ~user=admin`, the report displays any records that contain the string “login” or “logoff” for all users *except* those user accounts that start with the string “admin”. If you enter `login, logoff, ~ADMIN`, the report displays any records that contain the string “login” or “logoff” but that do *not* contain the string “admin” anywhere within the record.
Status	The options are: • **Unacknowledged** • **Acknowledged** • **Retired** • **All** The default is **Unacknowledged**.
Alarm Codes	One or more alarm codes to search for. Separate multiple alarm codes with a comma or a space. For example, to search for alarm codes QADMN00001 and QADMN00002, enter `QADMN00001,QADMN00002` or `QADMN00001 QADMN00002`.
Sort By	This can be: • **Time: newest first** • **Time: oldest first** • **Severity: highest first** • **Severity: lowest first** • **Server Name** • **Status** The default is **Time: newest first**.

Date and Time group

Button	Description
Predefined Values	The options are: • **All Dates and Times** • **Today** • **Yesterday**
Last	Limits the report to a given number of days or hours. Enter that number of days or hours in the associated text field, then select **Days** or **Hours** from the associated drop-down list. You can enter a whole number from 1 to 99. The number of days is calculated from midnight to 11:59 p.m. For example, if the current time is 3:00 p.m. on Wednesday and you enter a 3 in this field and select **Days** from the drop-down, the report will include all activity starting on Monday at midnight through the end of the current day.
Between	Limits the report to a specified range of dates. The default range covers a seven day time span that ends with the current date and time. If you want a different range of dates:

Note:

The amount of data available for this report depends on the **Retention Period** setting in the **Alarms** group on the Alarm/Log Options page.

For example, if this value is set to 14, you can enter a start date that is two weeks prior to the current date. If the value is set to 7, you can only check for the previous week.

Categories and Severities group

This group lists all the alarm categories and severities available in the report. Use the check boxes to show or hide the alarms for a given category or with a given severity.

Note:

If these fields are not displayed, click the group heading to expand the group.

Column	Description
All Categories	The check box in this column indicates which alarm categories to include in the alarm report. For more information, see Event and alarm categories on page 490.
Critical	Critical alarms describe problems that are interrupting service and require immediate action.
Major	Major alarms describe serious problems that need to be fixed as soon as possible.
Minor	Minor alarms describe problems that do not require immediate action but need monitoring.

EP Administration	Messages related to administration activities on the Experience Portal Manager (EPM).

EP Application Interface WS	Messages related to the Application Interface web service. This web service runs on the EPM server and allows customer applications to initiate outbound calls.
EP Application Interface WS 2.0	Messages related to the Application Interface web service 2.0. This version is functionally equivalent to the previous one. While there is a single username or password for the former, the new version provides the added facility of allowing multiple users to access the web service.
EP Application Logger	Messages related to the Experience Portal application logger. The application logger is a web service running on Experience Portal which allows Orchestration Designer applications to log messages to the EPM.

EP ASR	Messages related to Automatic Speech Recognition (ASR).
EP Backup	Messages related to the EP Backup subsystem, which provides the means to perform on-demand or scheduled backup operation.
EP Carrier Service	Messages related to the Carrier REST web service, which allows you to retrieve mobile related information from a carrier.
EP CCXML Browser	Messages related to the Call Control eXtensible Markup Language (CCXML) browser, which controls all call handling for all Voice eXtensible Markup Language (VoiceXML) applications.
EP Event Manager	Messages related to the Event Manager, which collects events from other Media Processing Platform (MPP) processes and sends them to the network log web service on the EPM.
EP Licensing	Messages related to port licensing.
EP Listener	Messages related to the Alarm Codes Destinations types (Listeners) where the alarm notification is delivered.
EP Management WS	Messages related to the Experience Portal Management web service. This web service runs on the EPM server and allows you to configure and manage a EPM.
EP Media Manager	Messages related to audio and video Real-time Transport Protocol (RTP) connections.
EP MMS	Messages related to the MPP Management Service (MMS), which stores configuration information and controls the initialization and operation of an MPP.
EP Media Server Manager	Messages related to the MPP management subsystem, which provides the means to start and stop call processing.
EP MPP System Manager	Messages related to the MPP System Manager process, which manages and monitors MPP processes, configuration, licensing, and system resources.
EP MRCP	Messages related to Media Resource Control Protocol (MRCP), which is an open standard for speech interfaces.
EP Reporting	Messages related to the collection of report data and the generation of reports.
EP Session Manager	Messages related to the MPP Session Manager, which coordinates the low-level interactions between the ASR, TTS, and telephony components and the VoiceXML and CCXML browsers.

Table continues…

EP SNMP Agent	Messages related to the SNMP agent, which collects and stores management information and makes this information available to SNMP managers.
EP Telephony	Messages related to the H.323 connections and Voice over IP (VoIP) telephony interfaces.
EP Trace	Messages related to the EP trace reports. It provides the means to collect trace data from EPM or specific MPP.
EP TTS	Messages related to Text-to-Speech (TTS).
EP Upgrade Manager	Messages related to software upgrades for MPPs running on the EPM.
EP Email Processor	Messages related to the EP Email Processor.
EP SMS Processor	Messages related to the EP SMS Processor.
EP Text Browser	Messages related to the EP Text Processor.

Note:

Additional categories may be available if you have installed managed application on Experience Portal. For more information on managed application based categories, see the documentation delivered with the managed application.

Alarm Report page field descriptions

Use this page to view, print, or export an alarm report, or to view the history of alarm state changes and information about associated event codes.

This page contains the:

- Alarm report table on page 502
- Change Alarm Status group on page 503

Alarm report table

Field	Description
Selection check box	Use this check box to select the alarms whose status you want to change. **Note:** This check box is only available if you are logged in with the Administration or Operations System Manager user role
Timestamp	The date and time that the alarm message was generated.
Alarm Status	The options are: • **UNACK**: The alarm is active and has not been acknowledged. • **ACK**: The alarm is active and was acknowledged. • **RETIRED**: The alarm is retired. If the alarm status is **ACK** or **Retired**, click the status to view the Alarm History window that details the changes to the alarm's status.

Table continues…

Field	Description
Server Name	The options are: • The name of the primary or auxiliary EPM server • The name of the Media Server that generated the event
Category	Indicates which Experience Portal component generated the alarm.
Alarm Severity	Indicates how severe the problems surrounding the alarm were.
Alarm Code	The unique identification code associated with the alarm.
Event Code	The unique identification code associated with the event. Click this event code to view the Log Report for Event page.
Alarm Message	A brief explanation of the problem or error that caused the alarm.

Change Alarm Status group

Note:

This group is only available if there are Unacknowledged or Acknowledged alarms in the report and you are logged in with the Administration or Operations System Manager user role.

Field or Button	Description
Alarm selection radio buttons	The options are: • **Selected alarms on this page**: Changes the status of the selected alarms only. • **All alarms on this report**: Changes the status of all alarms. regardless of the current selection.
New Status	The options are: • **ACK**: Change the status to Acknowledged. • **RETIRED**: Change the status to Retired. Experience Portal may be configured to automatically delete retired alarms after a specified length of time, based on the **Purge Enabled** setting in the **Alarms** group on the Alarm/Log Options page.
Submit	Changes the status of the selected alarms.

Trace Viewer

The Trace Viewer enables you to view and generate trace reports more effectively using the EPM interface. Using the trace viewer, you can generate trace reports for the traces that are retrieved from MPPs or the primary EPM, more effectively and securely. With a similar interface as the log viewer and the alarm manager for filtering and reports, the trace viewer provides better debugging capabilities on the Experience Portal system.

The Trace Viewer feature has the following enhancements:

- A separate tab to configure the filters and retrieve trace records for MPP traces.

- A separate tab to configure the filters and retrieve trace records for EPM traces.
- Ready-to-use details of trace information of specific components or processes that occurr in a selected MPP or EPM server.
- Enhanced debugging capabilities through well formatted outputs on the trace report. You can easily analyze the process activities and efficiently identify the root cause if any unexpected issue occurs.

You can use Trace viewer by clicking the **Trace viewer** link under **System Maintenance** on the navigation pane.

Important:

You must have the same version of EPM and MPP installed to use the trace viewer feature.

If any of the incompatible MPPs are connected to EPM, the trace client detects the incorrect version and reports an error on the log report. This distinguishes the MPP connection failures due to incompatibility and failure due to Trace WS.

MPP Traces tab on Trace Viewer page field descriptions

Use this page to configure the filters and retrieve trace records for MPP traces.

This page contains the:

- General section on page 504
- Select Trace File section on page 506
- Date and Time section on page 508

General section

Field	Description
Zone	Select the name of the zone from the drop-down box. You can filter the records based on the zone that you select. **Note:** The **Zone** drop-down box appears only when you create new zones. If you do not create any new zones, you do not see the drop-down box.
	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon
Servers	Select the name of the MPP server for which you want to view the trace details. For a single box system, the MPP name is displayed. If there are no MPPs configured, a message `No MPPs configured` is displayed.

Table continues…

Field	Description
Search Keywords	Enter text to search for in the trace records. You can specify multiple search keywords separated by commas. The search is case insensitive and based on a substring match, not a whole string match. For example, “Acknowledged” matches “acknowledged”, “ACKNOWLEDGED”, and “unacknowledged”. The search uses a logical OR when combining keywords. You can separate multiple entries with a comma, and use the tilde character (~) to indicate NOT. For example, if you enter `login, logoff, ~user=admin`, the report displays any records that contain the string “login” or “logoff” for all users *except* those user accounts that start with the string “admin”. If you enter `login, logoff, ~ADMIN`, the report displays any records that contain the string “login” or “logoff” but that do *not* contain the string “admin” anywhere within the record.
Components	Select the process components for which you want to view the trace details. The options are: • **Administration** • **Call Data Handler WS** • **CCXML Browser** • **Event Manager** • **Media Manager** • **MMS** • **Outcall WS** • **Session Manager** • **SIP** • **System Manager** • **Transcript WS** • **Voice Browser** The default is **Administration**. For details about the components, see Event and alarm categories on page 490.

Table continues…

Field	Description
Trace Level	Select one or multiple levels on traces report. The options are: • **All Levels** • **FATAL** • **ERROR** • **WARN** • **INFO** • **FINE** • **FINER** • **FINEST** The default is **All Levels**. **Note:** You can select multiple trace levels by using *Shift+Click* to select a range of systems or *Ctrl+Click* to select individual systems.

Note:

The amount of data available for this report depends on the **Retention Period** setting in the **Logs** group on the Viewer Settings page.

For example, if this value is set to 14, you can enter a start date that is two weeks prior to the current date. If the value is set to 7, you can only check for the previous week.

Select Trace File section

Note:

This section is available only if you select one of the following **Components**:

- **CCXML Browser**
- **Media Manager**
- **Session Manager**
- **Voice Browser**

The fields in this section vary with the component selection.

Select Trace File fields for Media Manager	
Field	**Description**
EndPointMgr	Select this option to access the EndPointMgr.log file produced by the MediaManager process. This log file contains the traces regarding media end point management (RTP) and end point control messages exchanged between the MediaManager process and the SessionManager.
Media Manager	Select this option to access the MediaManager.log file produced by the MediaManager process. This log file contains the log traces associated with basic management of the MediaManager process including the start up, configuration, and shutdown messages.
VideoMgr	Select this option to access the VideoMgr.log file produced by the MediaManager process. This log file contains the traces regarding video rendering and video control messages exchanged between the MediaManager process and the SessionManager.
Session Slot	Select the session slot number. The session slot number is used by Avaya Experience Portal to uniquely identify the session. This slot number is included in the name of the associated logs on the MPP. The session slots are numeric values in the range 1 to 9,999.

Select Trace File fields for Session Manager	
Field	**Description**
Session Manager	Select this option to access the log files produced by the Session Manager. The session manager contains the following log files: • SessionManager.log– Contains data related to events that are not specifically associated with a single session • SessionSlot-###.log– Where ### represents a unique log identifier. Contains data related to Session Manager operations for individual sessions. **Tip:** You can use ### to find related CCXML interpreter and Avaya Voice Browser logs. **Note:** The Session Manager component can be parsed with Categories. If you select **All Categories**, the system displays the records for all existing categories.
Session Slot	Select the session slot number. The session slot number is used by Avaya Experience Portal to uniquely identify the session. This slot number is included in the name of the associated logs on the MPP. The session slots are numeric values in the range 1 to 9,999.

Select Trace File fields for SIP	
Field	**Description**
Session ID	Select this option to enter the unique identifier for the SIP call sessions.
Contact ID	Select this option to enter the unique identifier for a single call.
SIP Call-ID **From Tag**	Select this option to specify values so that the system displays messages that have the matching values in both the SIP Call-ID header and the tag parameter of the From header.

Select Trace File fields for CCXML Browser and Voice Browser	
Field	**Description**
GlobalProcess	Select the global process ID from the drop down box. The global process ID is a numeric value in the range 0 to 9.
Session Slot	Select the session slot number. The session slot number is used by Avaya Experience Portal to uniquely identify the session. This slot number is included in the name of the associated logs on the MPP. The session slots are numeric values in the range 1 to 9,999.

Date and Time section

Button	Description
Predefined Values	The options are: • **All Dates and Times** • **Today** • **Yesterday**
Last	Limits the report to a given number of days or hours. Enter that number of days or hours in the associated text field, then select **Days** or **Hours** from the associated drop-down list. You can enter a whole number from 1 to 99. The number of days is calculated from midnight to 11:59 p.m. For example, if the current time is 3:00 p.m. on Wednesday and you enter a `3` in this field and select **Days** from the drop-down, the report will include all activity starting on Monday at midnight through the end of the current day.

Table continues…

Button	Description
Between	Limits the report to a specified range of dates. The default range covers a seven day time span that ends with the current date and time. If you want a different range of dates: • In the beginning of the **Start Date/Time** field, enter the start date using the format `mmm-dd-yyyy` or click the calendar icon to select the date from a pop-up calendar. After the start date, enter the start time using a 24-hour format and the same timezone as the EPM. For example, you could enter `Mar-03-2007 16:26:10`. The default for this field is one week prior to the current date at time 00:00:00. • In the beginning of the **End Date/Time** field, enter the end date using the format `mmm-dd-yyyy` or click the calendar icon to select the date from a pop-up calendar. After the end date, enter the end time using a 24-hour format and the same timezone as the EPM. For example, you could enter `Mar-10-2007 16:26:10`. The default for this field is the day prior to the current date at time 23:59:59.

MPP Trace Report page field descriptions

Use this page to view, print, or export the formatted trace reports for the traces that are retrieved from MPPs, or to view the information about associated event codes.

Field	Description
Timestamp	The date and time that the log record was generated.
Server Name	The name of the MPP from which the traces are retrieved.
Category	The Experience Portal component that generated the log record.
Trace Level	The severity of the log record.
Event Code	The event code associated with the event. Click the event code to view detailed information about the event.
Trace Message	A brief explanation of the trace. If trace information is available for the trace, you can click the **Detail** link in this column to display detailed trace information of system server on the Experience Portal system.

EPM Traces tab on Trace Viewer page field descriptions

Use this page to configure the filters and retrieve trace records for primary EPM traces.

General section

Field	Description
Zone	The name of the default zone. **Note:** The **Zone** field appears only if zones are defined on EPM.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
Server Names	The primary EPM.
Search Keywords	Enter text to search for in the trace records. You can specify multiple search keywords separated by commas. The search is case insensitive and based on a substring match, not a whole string match. For example, “Acknowledged” matches “acknowledged”, “ACKNOWLEDGED”, and “unacknowledged”. The search uses a logical OR when combining keywords. You can separate multiple entries with a comma, and use the tilde character (~) to indicate NOT. For example, if you enter `login, logoff, ~user=admin`, the report displays any records that contain the string “login” or “logoff” for all users *except* those user accounts that start with the string “admin”. If you enter `login, logoff, ~ADMIN`, the report displays any records that contain the string “login” or “logoff” but that do *not* contain the string “admin” anywhere within the record.

Table continues…

Field	Description
Components	Select the process components for which you want to view the trace details. The options are: • **Application Interface WS** • **Application Interface WS 2.0** • **Application Logger** • **Email** • **EP Backup** • **EP Management WS** • **EPM** • **Listener** • **SMS** • **SNMP Agent** • **SUM Upgrade WS** • **Text** The default is **Application Interface WS**. For details about the components, see Event and alarm categories on page 490.
Trace Level	Select one or multiple levels on traces report. The options are: • FATAL • ERROR • WARN • INFO • FINE • FINER • FINEST

Note:

The amount of data available for this report depends on the **Retention Period** setting in the **Logs** group on the Alarm/Log Options page.

For example, if this value is set to 14, you can enter a start date that is two weeks prior to the current date. If the value is set to 7, you can only check for the previous week.

Date and Time section

Button	Description
Predefined Values	The options are: • **All Dates and Times** • **Today** • **Yesterday**
Last	Limits the report to a given number of days or hours. Enter that number of days or hours in the associated text field, then select **Days** or **Hours** from the associated drop-down list. You can enter a whole number from 1 to 99. The number of days is calculated from midnight to 11:59 p.m. For example, if the current time is 3:00 p.m. on Wednesday and you enter a 3 in this field and select **Days** from the drop-down, the report will include all activity starting on Monday at midnight through the end of the current day.
Between	Limits the report to a specified range of dates. The default range covers a seven day time span that ends with the current date and time. If you want a different range of dates:

EPM Trace Report page field descriptions

Use this page to do the following:

- View, print, or export the formatted trace reports for the traces that are retrieved from the primary EPM
- View the information about associated event codes

Field	Description
Timestamp	The date and time that Experience Portal generates the log record.
Server Name	The EPM from which the traces are retrieved.
Category	The Experience Portal component that generates the log record.
Trace Level	The severity of the log record.
Event Code	The event code associated with the event. Click the event code to view detailed information about the event.
Trace Message	A brief explanation of the trace. If the trace information is available for the trace, you can click the **Detail** link in this column to display the detailed trace information of system server on the Experience Portal system.

Log Viewer page field descriptions

Use this page to create an event report.

This page contains the:

General information section

Field	Description
Zones	Select the name of the zone from the drop-down box. You can filter the records based on the zone that you select. **Note:** The **Zones** drop-down box appears only when you create new zones. If you do not create any new zones, you do not see the drop-down box.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon appears only when you create new zones. If you do not create any new zones, you do not see the icon.
Servers	Select the name of the system for which you want to view events. The options are: • **All servers** • EPM / MPP • EPM • MPP The default is **All servers**. **Note:** The **MPP** option is available in EPM only if the media server is MPP.

Table continues…

Field	Description
Search Keywords	Enter text to search for in the event records. The search is case insensitive and based on a substring match, not a whole string match. For example, “Acknowledged” matches “acknowledged”, “ACKNOWLEDGED”, and “unacknowledged”. The search uses a logical OR when combining keywords. You can separate multiple entries with a comma, and use the tilde character (~) to indicate NOT. For example, if you enter `login, logoff, ~user=admin`, the report displays any records that contain the string “login” or “logoff” for all users *except* those user accounts that start with the string “admin”. If you enter `login, logoff, ~ADMIN`, the report displays any records that contain the string “login” or “logoff” but that do *not* contain the string “admin” anywhere within the record.
Sort By	Select one of the following options: • **Time: newest first** • **Time: oldest first** • **Severity: highest first** • **Severity: lowest first** • **Server Name** The default is **Time: newest first**.
Event Codes	Enter one or more event codes to search for in the log records. Separate event codes with a comma or a space. For example, to search for event codes PADMN00001 and PADMN00002, enter `PADMN00001,PADMN00002` or `PADMN00001 PADMN00002`

Date and Time group

Button	Description
Predefined Values	The options are: • **All Dates and Times** • **Today** • **Yesterday**

Table continues…

Button	Description
Last	Limits the report to a given number of days or hours. Enter that number of days or hours in the associated text field, then select **Days** or **Hours** from the associated drop-down list. You can enter a whole number from 1 to 99. The number of days is calculated from midnight to 11:59 p.m. For example, if the current time is 3:00 p.m. on Wednesday and you enter a `3` in this field and select **Days** from the drop-down, the report will include all activity starting on Monday at midnight through the end of the current day.
Between	Limits the report to a specified range of dates. The default range covers a seven day time span that ends with the current date and time. If you want a different range of dates:

Note:

The amount of data available for this report depends on the **Retention Period** setting in the **Logs** group on the Alarm/Log Options page.

For example, if this value is set to 14, you can enter a start date that is two weeks prior to the current date. If the value is set to 7, you can only check for the previous week.

Categories and Severities group

This group lists all the event categories and severities available in the report.

Use the check boxes to show or hide the alarms for a given category or with a given severity. Use the **Check all** or **Uncheck all** links to the right of the group header to select or clear all category and severity check boxes.

Note:

If these fields are not displayed, click the group heading to expand the group.

Column	Description
All Categories	The check box in this column indicates which event categories to include in the report. For details about the categories, see Event and alarm categories on page 490.
Fatal	Fatal events describe problems that are interrupting service and require immediate action.
Error	Error events describe serious problems that need to be fixed as soon as possible.
Warning	Warning events describe problems that are not currently interrupting service but which should be monitored.
Info	Info events are informational messages about the system or system resources.

Log Report page field descriptions

Use this page to do the following:

- View, print, or export a log report.
- View exception information for an event.

Field	Description
Timestamp	The date and time that Experience Portal generates the event message.
Server Name	The name of the server. The options are: • **EPM** • The name of the media server that generates the event **Note:** If you sort the report by this field, the EPM actually sorts by the name of the server in the Experience Portal database, not the name displayed in this field. Therefore the sort results may be different from what you expect.
Category	Indicates which Experience Portal component generated the event. For more information, see Event and alarm categories on page 490.
Event Severity	Indicates the severity of the problems surrounding the event. For more information, see Event severities on page 492.
Event Code	The event code associated with the event. Click the event code to view detailed information about the event.
Event Message	A brief explanation of the event or condition. If the exception information is available for the event, a link labeled **More** appears in this column. Click **More** to display the exception information.

<System name> Details tab on the System Monitor page field descriptions

Use this tab for a detailed view of the health and status of the EPM and each MPP in the Experience Portal system named in <*System Name*>. The information on this page refreshes automatically if you leave the browser window open.

Note:

If the EPM server needs to be restarted, Experience Portal displays the message "EPM needs to be restarted." in red text just above the system status table.

Column	Description
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
Zone	The zone where the EPM and the MPP servers are configured.
Server Name	The options are: • The name of the EPM server. Click this name to view the <EPM Name> Details page. • The name of an MPP running on the system. Click this name to view the <MPP name> Details page. • *<EPM Name>/<MPP Name>*, if an MPP resides on the same server as the EPM. Click this name to view the <MPP name> Details page.
Type	The options are: • **EPM**: The Experience Portal Manager • **MPP**: A Media Processing Platform **Tip:** To verify whether the associated server is a primary or auxiliary EPM server, hover the mouse over the EPM field.
Mode	The operational mode of the Media Server. The options are: • **Online**: The Media Server is available. • **Offline**: The Media Server is unavailable and is not being polled by the EPM server. • **Test**: (MPP only) The Media Server is available to handle calls made to one of the defined H.323 maintenance stations. **Tip:** To view the date and time that this mode was first reached, hover the mouse over this column.

Table continues…

Column	Description
State	The operational state of the Media Server. The options are: • **Booting**: The Media Server is in the process of restarting and is not yet ready to take new calls. • **Degraded**: The Media Server is running but it is not functioning at full capacity. • **Error**: The Media Server has encountered a severe problem and cannot recover. • **Halted**: The Media Server is no longer responding to heartbeats because it received a **`Halt`** command. • **Halting**: The Media Server is responding to heartbeats but is not taking new calls. • **Need Configuration**: An Email or SMS processor residing on the Media Server has not yet been configured. • **Need Connections**: No connections (SMPP or HTTP) have been configured or assigned to an Email/SMS processor residing on the Media Server. • **Never Used**: The Media Server has never successfully responded to a heartbeat request. • **Not Installed**: The Media Server is missing files required for heartbeat requests to occur. • **Not Responding**: The Media Server is not responding to heartbeat requests and it has not received a **`Restart`** or **`Halt`** command. • **Partially Running**: (EPM only) The Media Server is in the process of starting up, and not all individual components of the service, for example: Tomcat, SL, ActiveMQ, have come up yet. • **Rebooting**: The Media Server is responding to heartbeats but is not taking new calls. • **Recovering**: The Media Server has encountered a problem and is attempting to recover. • **Restart Needed**: This state is most often reached when the Media Server has encountered a problem that it cannot recover from and it requires a manual restart. However, it can also appear for an MPP when the EPM software has been upgraded and the MPP software has not. In that case, the state should update automatically when you upgrade the MPP software. • **Running**: The Media Server is responding to heartbeat requests and is accepting new calls. • **Starting**: The Media Server is responding to heartbeats but not taking new calls because it is transitioning from the Stopped state to the Running state. • **Stopped**: The Media Server is responding to heartbeats but is not taking new calls. The Media Server enters this state while it initializes after it restarts or when a **`Stop`** command is received. • **Stopping**: The Media Server is responding to heartbeats but is not taking new calls.

Table continues…

Column	Description
	• **Unknown**: The Media Server is in the Offline mode. **Tip:** To view the date and time that this state was first reached, hover the mouse over this column.
Active Command	This column is displayed if one or more Media Servers are currently in transition from their current state to a new user-requested state. For each transitional Media Server, this column displays the requested, or final, state. For any other Media Servers in the system, this field displays **None**.
Config	The configuration state of the Auxiliary EPM/MPP. The options are: • **Need certificates**: The Primary EPM certificate must be downloaded to the Auxiliary EPM/MPP by running the **`setup_vpms.php`** script on the Auxiliary EPM/MPP. • **Need ports**: The MPP has been configured and is waiting for ports to be assigned. • **None**: The MPP has never been configured. • **OK**: The Auxiliary EPM/MPP is currently operating using the last downloaded configuration. • **Restart needed**: The MPP must be restarted to enable the downloaded configuration. • **Reboot needed**: The MPP must be rebooted to enable the downloaded configuration. • **Upgrade needed**: The Auxiliary EPM must be upgraded to the same version of the software as on the Primary EPM. • **Unknown**: The MPP is either not responding or is in the Offline mode.
Call Capacity	This field displays: • **Current**: The number of calls that can be currently handled by the system. • **Licensed**: The number of licenses allocated to this system. • **Maximum**: The maximum number of simultaneous calls that the MPPs in this system can handle. This value is obtained by adding together the maximum number of calls set for each of the MPPs in the system. **Note:** This value can be larger than the number of licenses allocated to the system, but it should never be smaller. If it is smaller, then some of your licenses will never be used.

Table continues…

Column	Description
Active Calls	This field displays: • **In**: The number of active incoming calls in the system. • **Out**: The number of active outgoing calls in the system. Clicking the number displayed under the **Active Calls In** column displays all the active incoming calls for the media servers. Clicking the number displayed under the **Active Calls Out** column displays all the active outgoing calls for the media servers.
Calls Today	The number of calls handled during the current day.
Alarms	The alarm status indicators for the EPM, each MPP, and the overall Experience Portal system. The options are: • Green: There are no active major or critical alarms • Yellow: There are one or more active minor alarms • Red: There are one or more active major or critical alarms **Tip:** You can click any red or yellow alarm indicator to view the Alarm report for that system.
Summary	The total number of calls based on **Contact Summary** and **Active Calls**. On the Summary line, clicking the number displayed under the **Active Calls In** column displays all the active incoming calls for the media servers. On the Summary line, clicking the number displayed under the **Active Calls Out** column displays all the active outgoing calls for the media servers.

Email, HTML and SMS processors section

Column	Description
Zone	The zone where the Email and SMS processors are configured. The summary reports within a zone are: • **Email Summary**: Summary of the incoming and outgoing email messages in the last 24 hours. • **SMS Summary**: Summary of the incoming and outgoing SMS messages in the last 24 hours. • **HTML Summary**: Summary of the incoming HTML messages in the last 24 hours.
Server Name	The name of the EPM on which the Email, SMS and HTML processors are configured.

Table continues…

Column	Description
Type	The options are: • Email processor • HTML processor • SMS processor
State	The operational state of the email/SMS/HTML processors. The options are: • **Not Running**: The server is either stopped or not started yet. • **Starting**: The server start request is initiated, and is in the process of initialization. • **Running**: The server is up and functional. • **Stopping**: The server shutdown is requested. • **Need Configuration**: The server does not find configuration. • **Need Connections**: The server has configuration but does not have any connections assigned or configured. • **Degraded**: The server has configuration and connections. However, some or all connections are not working. • **Error**: The server data returned has been deemed "stale" (no new data retrieved after a period of 3 minutes), or 2) unexpected return code retrieved from a poll to server. • **Stopped**: The server is stopped.
Usage (Today)	Displays the number of messages processed during the current day. The Summary row also shows the maximum number of messages allowed per day.
Messages (Last 24 hours)	The options are: • Incoming: The number of incoming messages processed in the last 24 hours. • Outgoing: The number of outgoing messages processed in the last 24 hours. **Note:** Clicking on the **Last 24 hours** text, lets the user to change the number of messages displayed for the following time frames: • Last hour • Last 3 hours • Last 6 hours • Last 12 hours • Last 24 hours
Timeline Graph 	Displays a graph icon. Clicking this graph icon displays the number of messages processed in a graphical form.

Alarm/Log Options page field descriptions

Use this page to view or change the retention period for alarm and log records as well as the maximum number of report pages Experience Portal generates before it displays the first page of the report to the user.

This page contains the:

- Alarms group on page 522
- Logs group on page 522
- Audit Logs group on page 523
- Alarms/Logs/Audit Logs/Traces Report Size group on page 523

Note:

For purging the alarms, logs, and audit logs, the purge start time is 00:00 hours (midnight) by default. This implies that the purge period is not triggered until midnight regardless the time that you specify in the retention period.

For example, if you set the purge period to 1 day at 10:00 hours today, the purge does not occur until the third day morning at 00:01 hours.

Alarms group

Note:

You can only change the values in this group if your user account has the Administration user role.

Field	Description
Purge Enabled	The options are: • **Yes**: Experience Portal deletes Retired alarms once the retention period is exceeded. • **No**: Experience Portal leaves the Retired alarms in the database indefinitely. The default is **Yes**. **Note:** Experience Portal never automatically purges Acknowledged or Unacknowledged alarms.
Retention Period	The number of days that alarm records are retained if **Purge Enabled** is set to **Yes**. Enter an integer between 1 and 365. The default is 30.

Logs group

Note:

You can only change the values in this group if your user account has the Administration user role.

Field	Description
Purge Enabled	The options are: • **Yes**: Experience Portal deletes event log records once the retention period is exceeded. • **No**: Experience Portal leaves the event log records in the database indefinitely. The default is **Yes**.
Retention Period	The number of days that log records are retained if **Purge Enabled** is set to **Yes**. Enter an integer between 1 and 365. The default is 15.

Audit Logs group

Note:

You can only change the values in this group if your user account has the Auditor user role.

Field	Description
Purge Enabled	The options are: • **Yes**: Experience Portal deletes event log records once the retention period is exceeded. • **No**: Experience Portal leaves the event log records in the database indefinitely. The default is **Yes**
Retention Period	The number of days that audit log records are retained if **Purge Enabled** is set to **Yes**. Enter an integer between 1 and 365. The default is 180.

Alarms/Logs/Audit Logs/Traces Report Size group

Note:

You can only change the values in this group if your user account has the Administration user role.

Field	Description
Maximum Report Pages	The number of report pages Experience Portal generates before it displays the first page of the report to the user. Enter an integer between 1 and 100. The default is 10. For example, if this field is set to 20, Experience Portal retrieves enough data to fill the first 20 pages of the report before it displays the first page of the report. When the user reaches the end of page 20 and clicks **Next**, Experience Portal does not display page 21 until it has retrieved the data for pages 21-40.

Alarm History window field descriptions

Use this window to view the history of alarm state changes for Acknowledged or Retired alarms.

This window contains the:

- Alarm information section on page 524
- Alarm status change table on page 524

Alarm information section

Field	Description
Alarm Code	The unique identification code associated with the alarm.
Timestamp	The date and time that the alarm message was generated.
Server Name	The options are: • The name of the primary or auxiliary EPM server • The name of the Media Server that generated the event
Alarm Severity	Indicates how severe the problems surrounding the alarm were.
Alarm Message	A brief explanation of the problem or error that caused the alarm.

Alarm status change table

Field	Description
Timestamp	The date and time that the alarm status was changed.
Status Changed To	The status that the alarm was changed to. This can be: • **ACK**: The alarm status is now Acknowledged. • **RETIRED**: The alarm status is now Retired.
By	The user name of the user who changed the alarm status.

Creating an Audit Log report

About this task

The Audit Log report shows all the actions performed by all users logged into the EPM. It does *not* show any system configuration or backup activities performed by running Experience Portal scripts or other changes outside the EPM web interface.

Note:

The length of time that events remain in the database depends on the retention period set in the **Audit Logs** group on the Alarm/Log Options page.

Procedure

1. Log on to the EPM web interface by using an account with the Auditor user role.
2. On the EPM navigation pane, click **System Maintenance** > **Audit Log Viewer**.
3. On the Audit Log Viewer page, enter the filter criteria that you want to use, and click **OK**.

The EPM displays the Audit Log Report page.

Audit Log Viewer page field descriptions

Use this page to create an Audit Log report, which provides details on the administration activity that has occurred on this system.

This page contains the:

General section

Field	Description
Zones	Select the name of the zone from the drop-down box. You can filter the records based on the zone that you select. **Note:** The **Zones** drop-down box appears only when you create new zones. If you do not create any new zones, you do not see the drop-down box.
 **Zones filter** icon	To filter zones, click this icon located at the right side of the page. The system opens the **Zone filter** window for selecting one or more zones. **Note:** The **Zones filter** icon only appears when you create new zones. If you do not create any new zones, you do not see the icon.
Categories	The categories used to filter the audit log report.
Search Keywords	The text to search for in the audit log records. The search is case insensitive and based on a substring match, not a whole string match. For example, “Acknowledged” matches “acknowledged”, “ACKNOWLEDGED”, and “unacknowledged”. The search uses a logical OR when combining keywords. You can separate multiple entries with a comma, and use the tilde character (~) to indicate NOT. For example, if you enter `login, logoff, ~user=admin`, the report displays any records that contain the string “login” or “logoff” for all users *except* those user accounts that start with the string “admin”. If you enter `login, logoff, ~ADMIN`, the report displays any records that contain the string “login” or “logoff” but that do *not* contain the string “admin” anywhere within the record.
Sort By	The options are: • **Time: newest first** • **Time: oldest first**
Actions	The actions to be included in the audit log report.

Date and Time group

Button	Description
Predefined Values	The options are: • **All Dates and Times** • **Today** • **Yesterday**
Last	Limits the report to a given number of days or hours. Enter that number of days or hours in the associated text field, then select **Days** or **Hours** from the associated drop-down list. You can enter a whole number from 1 to 99. The number of days is calculated from midnight to 11:59 p.m. For example, if the current time is 3:00 p.m. on Wednesday and you enter a 3 in this field and select **Days** from the drop-down, the report will include all activity starting on Monday at midnight through the end of the current day.
Between	Limits the report to a specified range of dates. The default range covers a seven day time span that ends with the current date and time. If you want a different range of dates:

Note:

The amount of data available for this report depends on the setting in the **Retention Period** field in the **Audit Logs** group on the Alarm/Log Options page.

For example, if this value is set to 14, you can enter a start date that is two weeks prior to the current date. If the value is set to 7, you can only check for the previous week.

Audit Log Report page field descriptions

Use this page to view, print, or export an Audit Log report.

Column	Description
Timestamp	The date and time the user made the log entry.
User	The user name used to log in to the EPM to make the change.
Category	The EPM audit log category that is used for filtering the audit log.
Action	The action related to the user or category in the audit log report.
Zone	The zone where the audit log is located.
Component	The affected component.
Property	The affected property.
From	The value before the change was made.
To	The value after the change was made.

Chapter 20: Reports

Configuring report data settings

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** > **MPP Servers**.
3. On the MPP Servers page, click **MPP Settings**.
4. On the MPP Settings page, in the **Transcription** group, enter in the desired retention period.
5. In the **Record Handling on MPP** group, do the following:
   a. For each data type that you want each MPP to collect, verify that the **Enable** check-box for that data type is selected.
   b. In the associated **Retention Period** field, enter the number of days the data should be kept on the MPP.

   The data types are:

   - **Session Data**: Avaya Experience Portal uses this data to create the Session Detail and Session Summary reports.
   - **Call Data Record**: Experience Portal uses this data to create the Contact Detail and Contact Summary reports.
   - **VoiceXML/CCXML Log Tags**: Experience Portal can download the Log tag data and display it in the Application Detail report and Application Summary report.
6. Click **Save**.
7. To configure how often the EPM collects report data from each MPP, and how long the EPM keeps the report data in the Experience Portal database, do the following:
   a. On the EPM navigation pane, click **System Configuration** > **EPM Servers** > **Report Data**.
   b. On the Report Data Configuration page, enter appropriate information, and click **Save**.
8. To create application reports for speech applications running on the Experience Portal system, do the following to set the reporting options for each application:
   a. On the EPM navigation pane, click **System Configuration** > **Applications**.

b. On the Applications page, click the name of the application for which you want to create reports.

c. On the Change Application page, go to the **Reporting Parameters** group and enter appropriate information.

d. Click **Save**.

Printing reports

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **Reports** > **Standard** or **Reports** > **Custom**.
3. In the **View Report** column, click  for the report you want to generate.
4. At the top of the report page, click the **Print** icon.
5. Follow the prompts and do the following:
   - Ensure that the page orientation is Landscape, since some columns of the report may not print in Portrait orientation.
   - Select the browser option to print background colors and to include the same shading in the columns and rows as the online report.

Exporting reports

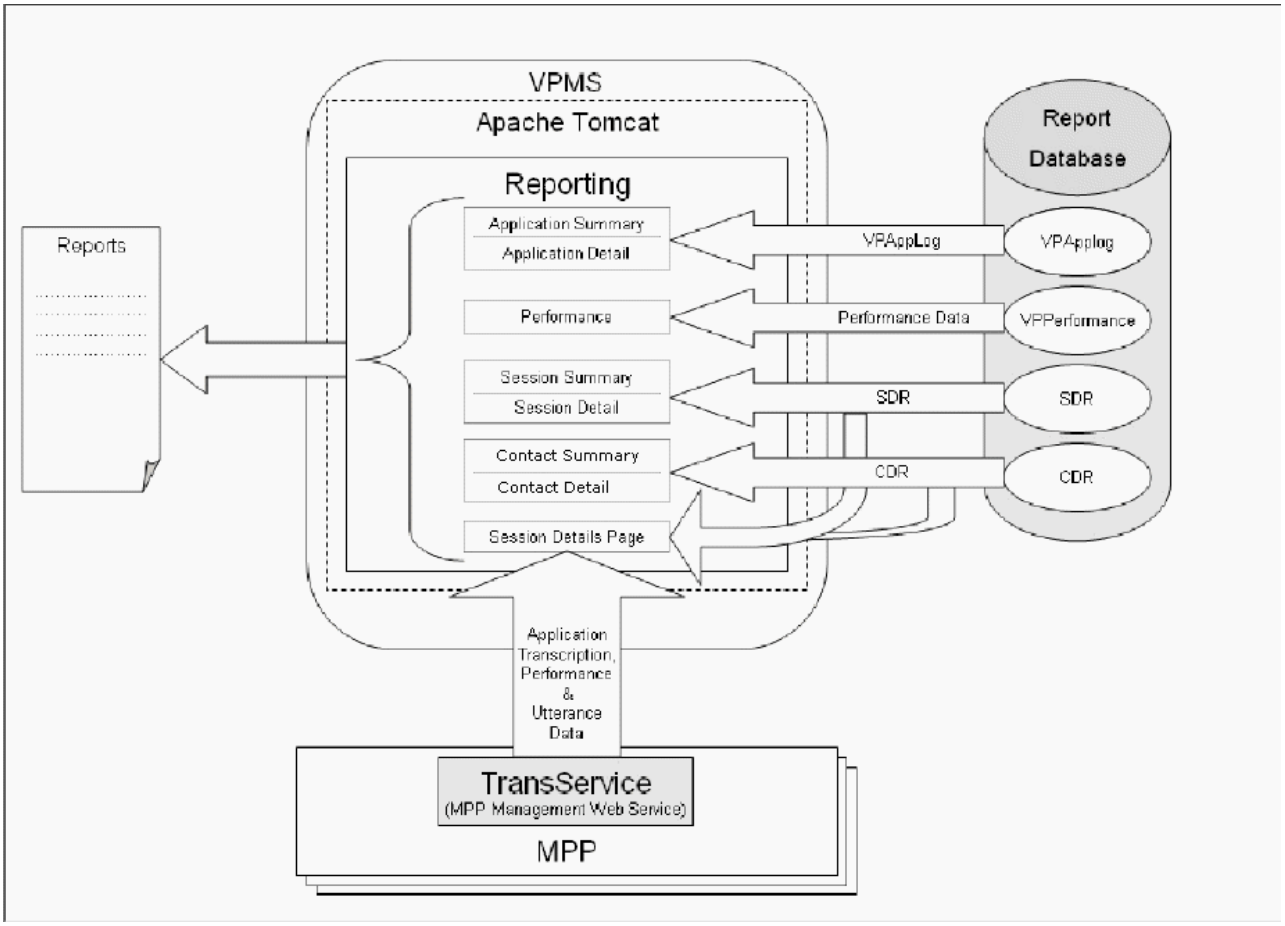
Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **Reports** > **Standard** or **Reports** > **Custom**.
3. In the **View Report** column, click  for the report you want to generate.
4. At the top of the report page, click the **Export** icon to export the data from the report.
5. Select one of the following export options and follow the prompts:
   - Export as XLS format
   - Export as PDF format

   Experience Portal creates a spreadsheet (XLSX file format) or a PDF containing the details shown in the report along with any additional report information available for up to 10,000 data records.

Report generation flow diagram

The following figure shows how the EPM generates reports.



Application activity reports

The available application activity reports are the following:

- Application Summary report
- Application Detail report

These application activity reports display:

- Activities and messages generated by the Orchestration Designer applications added to the Experience Portal system.
- Voice eXtensible Markup Language (VoiceXML) and Call Control eXtensible Markup Language (CCXML).

Log Tag messages from all the speech applications added to the Experience Portal system, if Log Tag messages are stored on and downloaded from the MPP.

The amount of data available for these reports depend on:

- The length of time since the application finished processing.

  The EPM downloads Application Detail Records (ADRs) within five minutes after an application finishes. If an application is not included in your report, make sure the application has finished processing and try running the report again.
- The **Retention Period** setting for the **Application Retention Period** field on the Report Data Configuration page.

  For example, if this value is set to 14, you can enter a start date that is two weeks prior to the current date. If the value is set to 7, you can only check for the previous week.
- You can specify the settings for the report parameters for each individual application in the **Reporting Parameters** group on the Change Application page.

Creating an Application Summary report

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **Reports** > **Standard**.
3. On the Standard Reports page, in the **Report Name** column, click the **Application Summary** link.

   Note:

   To generate the report with the default selections of filters, you can click  next to Application Summary link.
4. On the Application Summary page, enter the filter criteria that you want to use.

   Tip:

   Click the **more >>** link to display the rest of the optional filters.
5. Click **OK**.

   The EPM displays the Application Summary Report page.

Creating an Application Detail report

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 **Reports** > **Standard**.
3. On the Standard Reports page, click **Application Detail** link under the **Report Name** column.
4. Optionally, click  next to **Application Detail** link to generate the report with the default selections of filters.
5. On the Application Details page, enter the filter criteria that you want to use.

   Tip:

   Click the **more >>** link to display the rest of the optional filters.
6. Click **OK**.

   The EPM displays the Application Detail Report page.

   Tip:

   If the width of the activity type exceeds the width of the **Type** column, then the activity type appears as **...**. Hover the mouse over the **...** to view a tool tip with the complete type name.

Call activity reports

Contact activity reports

The following reports track call activity in the Experience Portal system:

Contact Summary report : Provides summary information about all calls handled by the specified MPPs and applications for the specified time period.

Contact Detail report : Provides detailed information about all calls handled by the specified MPPs and applications for the specified time period.

Session Summary report : Provides summary information about call-handling sessions for the specified MPPs and applications for the specified time period.

Session Detail report: Provides detailed information about all call-handling sessions for the specified MPPs and applications for the specified time period. This report also provides access to any transcription information saved for the applications.

The amount of data available for these reports depends on the **Retention Period** setting for the **Contact Data Record** and **Session Data** fields on the MPP Settings page.

For example, if this value is set to 14, you can enter a start date that is two weeks prior to the current date. If the value is set to 7, you can only check for the previous week.

Creating a Contact Detail report

About this task

The Contact Detail report provides detailed information about all calls handled by the specified MPPs and applications for the specified time period.

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 .**Reports** > **Standard**.
3. On the Standard Reports page, click **Contact Detail** link under the **Report Name** column.
4. Optionally, click  next to **Contact Detail** link to generate the report with the default selections of filters.
5. On the Contact Detail Report page, enter the filter criteria that you want to use.

   Tip:

   Click the **more >>** link to display the rest of the optional filters.
6. Click **OK**.
7. On the Contact Detail Report page, if you want to:
   - View the messages generated by one of the Orchestration Designer applications listed in the table, click the appropriate name in the **Application** column. The EPM displays the Application Detail Report page detailing the messages generated during the associated call session.
   - Get more information about how a call ended, hover the mouse over a value in the **End Type** column. Information about how a call ended is displayed in a pop-up window.
   - View details about the session that handled the call, click the **View Session Details** icon  in the appropriate row. The EPM displays the Session Details page.

Creating a Contact Summary report

About this task

The Contact Summary report provides summary information about all calls based on the specified filtering options.

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 **Reports** > **Standard**.
3. On the Standard Reports page, click **Contact Summary** link under the **Report Name** column.

   Note:

   You can also click  next to **Contact Summary** link to generate the report using the default selections of filters.
4. Optionally, click next to **Contact Summary** link to generate the report with the default selections filters.
5. On the Contact Summary page, enter the filter criteria that you want to use.

   Tip:

   Click the **more >>** link to display the rest of the optional filters.
6. Click **OK**.

   The EPM displays the Contact Summary Report page.

Creating a Session Detail report

About this task

The Session Detail report provides detailed information about the call-handling sessions for the specified Media Processing Platform (MPP) servers and applications for the specified time period. A session starts with the initial inbound or outbound call and ends with the termination of the CCXML page that resulted from the call.

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 **Reports** > **Standard**.
3. On the Standard Reports page, click **Session Detail** link under the **Report Name** column.
4. Optionally, click  next to **Session Detail** link to generate the report using the default selections of filters.
5. On the Session Detail (Filters) page, enter the filter criteria that you want to use.

   Tip:

   Click the **more >>** link to display the rest of the optional filters.
6. Click **OK**.

   The EPM displays the Session Detail Report page.

7. If you want to view more information about a particular session, click the **View Session Details** icon  in the appropriate row.

   Experience Portal displays the Session Details page.

Creating a Session Summary report

About this task

The Session Summary report provides summary information about call handling sessions for the specified Media Processing Platform (MPP) servers and applications for the specified time period. A session starts with the initial inbound or outbound call and ends with the termination of the CCXML or VoiceXML page that resulted from the call.

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 **Reports** > **Standard**.
3. Optionally, click  next to **Session Summary** link to generate the report with the default selections of filters.
4. On the Standard Reports page, click **Session Summary** link under the **Report Name** column.
5. On the Session Summary (Filters) page, enter the filter criteria that you want to use.

   Tip:

   Click the **more >>** link to display the rest of the optional filters.
6. Click **OK**.

   The EPM displays the Session Summary Report page.

Viewing application transcription data

Procedure

1. Log on to the EPM web interface by using an account with the Administration, Operations, or Maintenance user role.
2. On the EPM navigation pane, click **Reports** > **Standard** > **Session Detail** .
3. On the Session Detail page, click the **more >>** link to display the rest of the optional filters.
4. Enter the criteria you want to use for the report.

Tip:

If you want to limit the report to those sessions that have transcription information, select **Yes** in the **Session Transcription** field.

5. Click **OK**.

   The EPM displays the Session Detail Report page.

6. Locate the session for which you want to view the transcription data and click the **View Session Details** icon at the end of the appropriate row.

   Experience Portal displays the Session Details page, which shows both the session and transcription data grouped by the information category.

Show/Hide the Extended Exit Info #3 to Info #10 filters/columns in reports

By default, the Extended Exit Info #3 to Info #10 filters and columns are not shown in the Session Summary and Session Detail reports. To show/hide these filters and columns in EPM, you must run the **`enableExtendedExitFields`** command on the Experience Portal server.

Showing the Extended Exit Info #3 to Info #10 filters/columns in the Session Summary and Session Details reports

About this task

Note:

By default, the EnableExtendedExitFields feature is disabled.

Procedure

1. Log in to Linux on the Primary or Auxiliary EPM 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.
2. Navigate to the `Support/VP-Tools` directory under the Experience Portal installation directory.

   Enter the `cd $AVAYA_HOME/Support/VP-Tools` command. `$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`.

3. Type `Y` and press `Enter` when prompted to restart the *vpms* service.

Hiding the Extended Exit Info #3 to Info #10 filters/columns in the Session Summary and Session Details reports

Procedure

1. Log in to Linux on the Primary or Auxiliary EPM 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.
2. Navigate to the `Support/VP-Tools` directory under the Experience Portal installation directory.

   Enter the `cd $AVAYA_HOME/Support/VP-Tools` command. `$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`.
3. To run the script:

   Enter the `./EnableExtendedExitFields --disable` command to hide the extended exit fields in the Session Summary and Session Details reports.
4. Type `Y` and press `Enter` when prompted to restart the *vpms* service.

Creating a Performance report

About this task

The Performance report provides information about resource utilization on the specified Media Processing Platform (MPP) servers for the specified time period.

The amount of data available for this report depends on the **Performance Retention Period** field on the Report Data Configuration page.

For example, if this value is set to 14, you can enter a start date that is two weeks prior to the current date. If the value is set to 7, you can only check for the previous week.

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 **Reports** > **Standard**.
3. On the Standard Reports page, click **Performance** link under the **Report Name** column.

4. Optionally, click  next to **Performance** link to generate the report with the default selections of filters
5. On the Performance (Filters) page, enter the filter criteria that you want to use.
6. Click **OK**.
7. In the Performance Report page, if you want to:
   - View additional performance data in graphical format, click **View Summary Graph** above the last column in the table. All graphs show one bar for each MPP. The bars are color-coded to show average and peak usage for each category.
   - View port utilization information, click the magnifying glass icon in the **Port Utilization %** column. The EPM displays the Port Utilization Details page.
   - View resource utilization over time combined with the call volume over time, click the icon in the **Timeline Graph** column.

Advanced reporting in Experience Portal

The Experience Portal solution offers a variety of reports which enable you to analyze call volumes, trends, and effectiveness of your VoiceXML and CCXML applications.

The major new features added to the existing reporting feature are:

- Custom Reports on page 537
- Scheduled Reports on page 537
- Data Export reports on page 537

Custom Reports

With the custom reporting feature you can use any standard Experience Portal report as a base for generating a custom report. A custom report uses the filter settings defined in the selected base report. However, you can change the filter settings to create a different set of filters and configure the columns that you want to use for generating the report. You can also save this configuration for later reference.

Scheduled Reports

You can schedule the generation of the standard or the custom reports to occur on a periodic basis. You can receive the report output as an email attachment, or access it through the secure links in the email notification, RSS feeds or by logging into the Experience Portal Manager (EPM). You can optionally set Record Threshold restriction value when scheduling a report. Setting this restriction generates a notification only when the total record count reaches the specified minimum value.

Data Export reports

You can use the Data Export report to export the data from the Experience Portal reporting database, including the detailed call flow information stored on the MPP server. The call flow

information includes the session transcription files containing user experience, performance data, and optionally the caller's utterances stored in wave files.

Data Export report

Data Export reports

You can use the Data Export Report to request a bulk download of the raw report data for application tuning analysis. The raw data includes the session transcription XML files with or without the performance traces block of tags, utterance wave files, SDR, CDR, or ADR records.

Note:

- The Data Export Report does not include the session transcriptions and utterance wave files that reside on MPPs managed by a different EPM, that is, the MPPs that are in another Experience Portal system.
- The Data Export Report does not include transcriptions and/or utterances from MPPs that are in an Offline state.

Only one Data Export report request can be processed at a time.

The filters used in the Data Export report are based on the Session Detail report. However, the **Session Transcription** filter in the **Optional Filters** section is by default set to **All values**. If you are exporting Session Transcriptions and want to skip sessions that do not have transcriptions enabled, then select **Yes** in the **Session Transcription** filter. This ensures that only the sessions with transcriptions are considered for generating the report.

Creating a Data Export report

Procedure

1. Log into the EPM web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the EPM main menu, select **Reports** > **Standard**.
3. On the **Standard Reports** page, click **Data Export** link under the **Report Name** column.
4. Optionally, click  next to Data Export link to generate the report with the default selections of filters.
5. On the **Data Export (Filter)** page, enter the filter criteria that you want to use.

Tip:

Click the **more>>** link to display the rest of the optional filters

6. Click **OK**.

   The EPM displays the Data Export Report page.

Generating Custom reports using third-party software

Generating Custom reports using third-party software

You can use third party reporting tools to create reports using some of the raw application, call, and session data collected by the Experience Portal system and stored in the reporting database. Most of the data is protected by the system for security reasons, but you can use the database report user account created during EPM installation to access the information in the:

- Application Detail Records (ADRs) stored in the `vpapplog` table. For more information, see Custom application activity reports on page 539.
- Contact Detail Records (CDRs) stored in the `cdr` table. For more information, see Custom Contact Detail report on page 542.
- Session Detail Records (SDRs) stored in the `sdr` table. For more information, see Custom Session Detail report on page 548.

Note:

All data that you can access to create customized reports is Read-Only data.

Custom application activity reports

You can create custom application reports using the data stored in the `vpapplog` table of the PostgreSQL `VoicePortal` database. Experience Portal applications are designed to write log entries during their execution, much as other software applications do. Those log entries are composed of standard fields, some of which allow free-form string expressions. The occurrence and content of log entries is therefore subject to the design of the application. For each log entry, there is one row in the table. The columns of each row correspond to the standard fields. Rows are created after the controlling session completes and the data is pushed from the application server to a database updating web service on the EPM. Rows are deleted according to an administrable data retention limit.

Table 1: Primary Key column

This comprises of a collection of 5 columns:

Name
VPID
SessionID
MsgTimestamp
SessionIndex
Logtype

Table 2: Columns

Column	Data Type	Description
ActivityDuration	INTEGER	The number of seconds that have elapsed since the start of the activity. The start time for an activity is the time at which a record with `ActivityName <name>` and `LogType Start` is logged.
ActivityName	VARCHAR (1024)	Application generated value used to group report or log entries. For example, "Buy Ticket" or "Rent Car".
ApplicationID	VARCHAR (512)	*<Application Name>* where entry was logged.
AppServerAddress	VARCHAR (512)	Host name or IP address of the application server where the application was initially invoked.
InsertID	BIGSERIAL, NUMBER(20,0) BIGINT_ IDENTITY, BIGINT UNSIGNED	Unique sequence number which is automatically incremented by the database for each row that is inserted into the table. This field exists to permit easy access by extract, transform, and load (ETL) processes that are used by other Avaya products such as Avaya IQ.
LogLevel	VARCHAR (512)	Application specified level of log entry "Info", "Warning", "Error", "Fatal".
LogTimestamp	TIMESTAMP (62)	Date and time the log entry was generated in the time zone of the EPM.

Table continues…

Column	Data Type	Description
LogType	VARCHAR (512)	Type of log (generated by application). The possible values are: • `Start`: Beginning of an activity. • `End`: End of an activity. • `In Progress`: General log entry. • `Cancel`: Canceling of an activity. • `Cancel All`: Cancel all started activities in session. • `Node Entry`: Generated automatically by the DD framework if the collection of 'Call Flow Data' is enabled when the application is configured on the EPM. The node that is being entered (destination node) is listed in the ModuleIDNodeID field. The previous node (Exit node or Source node) is listed in the `Message` field. • `Module Exit`: Generated automatically by the DD framework if the collection of 'Call Flow Data' is enabled when the application is configured on the EPM. The module name that is exiting is listed in the ModuleIDNodeID field. • `Application Exit`: Generated automatically by the DD framework if the collection of 'Call Flow Data' is enabled when the application is configured on the EPM.
Message	VARCHAR (1024)	Application-defined, free-format text.
ModuleIDNodeID	VARCHAR	The node name that is being entered when LogType is Node Entry. The module and node identifiers in the format `[Module Id]:Node Id`, where `Module Id` is only specified if it is *not* the same as the application name. For example, if the application name is `CollectTicketInfo` and it contains the `CollectTicketInfo` module with the node `StartTicket` and the `GetPayment` module with the node `StartPay`, you would specify them as `:StartTicket` and `GetPayment:StartPay`.
MsgTimestamp	TIMESTAMP	Date and time the log entry was generated in GMT time zone.
NoInputCount	INTEGER	The number of times that no input was received prior to entering this node. This field is only populated for LogType of Node Entry and only when the previous node was a menu.
NoMatchCount	INTEGER	The number of times that no match events occurred prior to entering this node. This field is only populated for LogType of Node Entry and only when the previous node was a menu.

Table continues…

Column	Data Type	Description
RecConf	INTEGER	The confidence reported by the speech recognition engine. This field is only populated for LogType of Node Entry and only when the previous node was a menu. Values will range from 0 to 99.
SessionID	VARCHAR (512)	Session ID generated by the media server.
SessionIndex	INTEGER	This log entry's position within the session, where `1` indicated the first log entry, `2` indicates the second log entry, and so on.
SessionLabel	VARCHAR (1024)	A unique identifier set by the application designer. **Note:** An application designer can change the session label at any point while processing a single call. This field shows the label that was in effect when the log entry was made.
VarName	VARCHAR (1024)	A user-defined Dialog Designer application variable associated with this log entry by the application designer.
VarValue	VARCHAR (1024)	Value of variable defined in the column VarName when the log entry was made.
VPID	INTEGER	Identifies the EP system within a cluster of multiple EP systems that merge their data into the same external database. If there is only one EP system at your installation, this field will always be 1.

Custom Contact Detail report

You can create a custom Contact Detail report using the data stored in the `cdr` table of the PostgreSQL `VoicePortal` database. Experience Portal applications respond to incoming calls and can place outgoing calls. The details of each such call are recorded in this table. Call records are numbered sequentially by the database across each MPP and the Experience Portal system. Each call is further identified by a distinct universal identifier (UCID) received from the switch for communicating with other call handling systems. SessionID can be used to link a CDR record with its corresponding SDR and vpapplog records. This table has one row for each call handled by the Experience Portal cluster. Rows are created after the controlling session completes and the scheduled data download has occurred. Rows are deleted according to an administrable data retention limit.

Table 3: Primary Key Column

Name
InsertID

Table 4: Columns

Column	Data Type	Description
ApplicationName	VARCHAR (255)	Application name as configured in EPM.
AreaCode	INTEGER	The area code as extracted from the OriginatingNumber field based on rules defined in areacode.properties.
AudioCodec	VARCHAR (32)	Audio codec used in the call.
CallID	VARCHAR (255)	Unique call identifier assigned by the MPP. Value is unique within the Experience Portal cluster.
CallStartDate	INTEGER	Date the call started in YYYYMMDD format for the GMT timezone.
CallStartTime	INTEGER	Time in the day that the call started in HHMMSS format for the GMT timezone.
CallTimestamp	TIMESTAMP	Time in the day that the call started stored in a single Timestamp column. Based on GMT timezone.
CallType	INTEGER	Type of call: • 0: Inbound call. • 1: Outbound call.
ConnectLatency	INTEGER	The number of milliseconds until the call was connected.
DestinationNumber	VARCHAR (255)	DNIS - Pilot number of the application.
EMLEntryId	BIGINT, NUMBER(20,0)	Stores the primary key of the CDR record from the operational database for the email processor component. Contains 0 when CDR is from another source.
Duration	INTEGER	Call length in seconds.

Table continues…

Column	Data Type	Description
EndDetails	VARCHAR (255)	Additional information to **End Type** on how the contact ended. For example, you can specify the `Busy` filter to view all outbound contacts that received a busy signal. The options are: • Application exited • Busy • Hangup • Insufficient Media Server Resources • Insufficient Telephony Resources • Internal Error • Invalid Called URI • Network Busy • No Answer • SessionTerminated • SIT (Special Information tone) for disconnected number • tel: transferdestination# • Unknown Disconnect Reason
EndType	INTEGER	How the call completed: • 1: The call completed successfully; Near End Disconnect • 2: Transfer • 3: Far End Disconnect • 4: Interrupted • 5: Not Routed • 6: No Resource • 7: Session Manager Error • 8: Redirected • 9: Rejected • 10: Merged • 11: TimeOut
FirstPromptLatency	INTEGER	The amount of time after the call connected and before the first prompt was played, in milliseconds.

Table continues…

Column	Data Type	Description
InsertID	BIGSERIAL, NUMBER(20,0) BIGINT_ IDENTITY, BIGINT UNSIGNED	Unique sequence number which is automatically incremented by the database for each row that is inserted into the table. This field exists to permit easy access by extract, transform, and load (ETL) processes that are used by other Avaya products such as, Avaya IQ.
MediaType	INTEGER	Voice=0 (default), Video=1, SMSDelivery=2, SMS=3 EmailDSN=4, Email=5, HTML=6
MPP	VARCHAR (255)	The name of the MPP name that handled this session. This name is configured in the EPM.
OriginatingNumber	VARCHAR (255)	ANI - The caller's number.
PortID	INTEGER	The switch station for H.323.
ProviderName	VARCHAR(65)	The name of the Email or SMS provider that handled the message. The name is configured on the **Connections** tab for Email and Sms Processors in the EPM. For HTML contacts: It contains the browser-reported operating system and vendor information. For example, “Windows Desktop;Firefox;44.0” or “IPhone;Safari;8.0”. The user's web browser determines the content and format.
ProviderMessage	VARCHAR(160)	For SMS, this is the SMS message. For Email, this is either the subject or body of the email as specified under Reporting Parameters when the application is configured on the EPM. **Note:** • Only the first n characters are shown, as controlled by the Privacy section under Reporting Parameters when the application is configured on the EPM. The default is 0 characters. • The latter section can only be configured by an administrator who has the Privacy Manager role.

Table continues…

Column	Data Type	Description
ProviderStatus	INTEGER	The status of the message from the provider. For SMPP, this column will store the 'command_status' from the submit_sm response. A value of 0 indicates Success. A value of -1 indicates that a status was not received within the configured timeout period. The following are the Status values for emails with a MediaType of EmailDSN(4): • 0: Indicates that the message was successfully delivered to the recipient address specified by the sender, which includes "delivery" to a mailing list exploder. It does not indicate that the message has been read. This is a terminal state and no further DSN for this recipient should be expected. • 1: Indicates that 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 should be expected. • 2: Indicates that the message has been relayed or gatewayed into an environment that does not accept responsibility for generating DSNs upon successful delivery. • 3: Indicates that the Reporting MTA has so far been unable to deliver or relay the message, but it will continue to attempt to do so. Additional notification messages may be issued as the message is further delayed or successfully delivered, or if delivery attempts are later abandoned. • 4: Some other unknown error occurred. The details might be in the DSN message
ReasonCode	VARCHAR (255)	Reason code from a transferred call.
ReceiptRequested	INTEGER	0 = contact was not sent with a delivery receipt request. 1 = contact was sent with a delivery receipt request.
RecordDate	INTEGER	The date on which the record was written on the MPP. The format is YYYYMMDD and is always in GMT.
RecordID	INTEGER	CDR entry count by day.
RedirectedNumber	VARCHAR (255)	The number of the extension that the call is transferred from when calls are transferred to Experience Portal.
RtpRcvJitter	INTEGER	An estimate of the statistical variance of the RTP data packet inter-arrival time, measured in timestamp units and expressed as an unsigned integer.

Table continues…

Column	Data Type	Description
RtpRcvLost	INTEGER	The total number of RTP data packets from source that have been lost since the beginning of reception. This is the number of packets expected minus the number of packets actually received, where the number of packets received includes any which are late or duplicates.
RTPRcvPackets	INTEGER	The total number of RTP data packets received from the source.
RTPRoundTripTime	INTEGER	The delay, expressed in units of 1/65536 seconds, between receiving the last SR packet from source SSRC_*n* and sending this reception report block. If no SR packet has been received yet from SSRC_*n*, the DLSR field is set to zero.
RTPSendJitter	INTEGER	The Jitter reported from the far end of the RTP stream.
RTPSendLost	INTEGER	The total RTP data packets lost as reported by the far end of the RTP stream.
RTPSendPackets	INTEGER	The total number of RTP data packets transmitted by the sender.
SessionID	VARCHAR (255)	Dialog ID generated by MPP .
SMSEntryId	BIGINT, NUMBER(20,0)	Stores the primary key of the CDR record from the operational database for the SMS processor component. Contains 0 when CDR is from another source.
SwitchOrProxy	VARCHAR (255)	Name of the Switch as configured by the EPM.
TelMediaEncryption	VARCHAR(255)	The media encryption used during the call, if any.
TelProtocol	VARCHAR (255)	Telephony protocol use. This can be: • H.323 • SIP • SIPS
UCID	VARCHAR (255)	The Universal Call ID.
VideoBitRate	VARCHAR (32)	Video bit rate used in the call.
VideoCodec	VARCHAR (32)	Video codec used in the call.
VideoFrameRate	INTEGER	Video frame rate used in the call in Frame Per Second (FPS).
VideoScreenSize	VARCHAR(32)	Video screen resolution delivered on the call.
VPID	INTEGER	The ID number of the EP system that handled the call. If there is only one EP system at your installation, the value of this field will always be 1.
ZoneID	INTEGER	Identifies the Zone of the component creating this record. This value can be used as a key into the vpZones table.

Custom Session Detail report

You can create a custom Session Detail report using the data stored in the `sdr` table of the PostgreSQL `VoicePortal` database. Experience Portal supports both simple VoiceXML applications, which have exactly one dialog per session, and general CCXML applications, which can have zero to many dialogs per session. This table describes details of each session and of each dialog. For simple VoiceXML applications there is one row describing both the session and its single dialog. For general CCXML applications, there is a separate row describing the overall session plus one additional row for each dialog that was invoked during that session. These three types of records are distinguished by the RecordType field. Records in this table are uniquely identified across MPP and Experience Portal systems by a sequential number created by the database. SessionID can be used to link a SDR record with its corresponding CDR and vpapplog records. This table has one or more rows for each session handled by the Experience Portal cluster, as described above. Rows are created after the controlling session completes and the scheduled data download has occurred. Rows are deleted according to an administrable data retention limit.

Table 5: Primary Key Column

Name
InsertID

Table 6: Columns

Column	Data Type	Description
ApplicationName	VARCHAR(255)	Application name as configured in EPM.
AppServer	VARCHAR(255)	Initial URL as configured in EPM that triggered the application.
ASRPercent	INTEGER	Speech recognition percentage for the page with the lowest recognition. This value is computed using the values for: • The number of recognized utterances on the page with the worst recognition, as shown in the UttCntRecWPage column. • The number of total utterances received on the page, as shown in the UttCntWPage column. The formula is: `(UttCntRecWPage/UttCntWPage)*100`
ASRServer	VARCHAR(255)	IP address of the ASR server used by the session.
AverageASRpercent	INTEGER	The average ASR percentage for the session, based on the total number of utterances and the total number of recognized utterances.

Table continues…

Column	Data Type	Description
AverageLatency	INTEGER	The average time, in milliseconds, after the caller issued a speech command before the subsequent prompt began playing.
AverageRecConf	INTEGER	The average confidence level across all recognized utterances in this session.
DialogID	VARCHAR(255)	The unique ID that describes a specific VXML dialog associated with a particular session.
Duration	INTEGER	The total length of the session, in seconds.
EMLEntryId	BIGINT, NUMBER(20,0)	Stores the primary key of the SDR record from the operational database for the email processor component. Contains 0 when SDR is from another source.
ExitCustomerID	VARCHAR(65)	Optional Information set by the application (through session.exitCustomerID variable in DD or manually through the Exit tag)
ExitPreferredPath	INTEGER	This field is determined by the DD framework: • 0 - if a node that has been flagged by the application developer as unpreferred, is ran in this session. • 1 – if no unpreferred nodes are ran in this session.
ExitTopic	VARCHAR(65)	Optional Information set by the application (through session.exitTopic variable in DD or manually through the Exit tag)
HasPerformanceTrace	INTEGER	This can be: • 0: No performance data was captured for this session. • 1: The performance data was captured for this session.
HasTranscription	INTEGER	This can be: • 0: No transcription data was captured for this session. • 1: Transcription data was captured for this session. **Note:** By default, the DD nodes are “Preferred”.
InsertRecordID	INTEGER	An uniquely sequential number that resets to 1 when the InsertDate changes.
LatAnswer	INTEGER	The time after which the call was connected and before the first prompt was played, in milliseconds.
LatencyHistogram1	INTEGER	The number of speech application pages that took less than one second to load.
LatencyHistogram2	INTEGER	The number of speech application pages that took between one and two seconds to load.
LatencyHistogram3	INTEGER	The number of speech application pages that took between two and three seconds to load.

Table continues…

Column	Data Type	Description
LatencyHistogram4	INTEGER	The number of speech application pages that took between three and four seconds to load.
LatencyHistogram5	INTEGER	The number of speech application pages that took more than four seconds to load.
LatWPage	INTEGER	Longest length of time that it took for any page to load, in milliseconds.
LatWPageName	VARCHAR (512)	URL of the page that took the longest time to load.
MaxConsecutiveRecErrors	INTEGER	The maximum number of times in a row that an utterance was not recognized during a session. This value tracks the maximum consecutive number of recognition errors, not the total number of recognition errors for a given utterance. For example, if the caller had to repeat the word "brokerage": • Twice on the first menu • Three times on the second menu This field would display 3.
MPP	VARCHAR(255)	The name of the MPP name that handled this session. This name is configured in the EPM.
MRCPSessionIDASR	VARCHAR(255)	The Session ID on the ASR server. This is the MRCP session ID if the ASR server uses the MRCP protocol. **Note:** When multiple ASR servers are used, the ASR Session ID field contains only the first Session ID. To find all of the ASR Session IDs, examine the Speech events in the Session Transcription.
MRCPSessionIDTTS	VARCHAR(255)	The Session ID on the Text-to-Speech (TTS) server. This is the MRCP session ID if the TTS server uses the MRCP protocol.
PageReqCacheHits	INTEGER	Number of VXML page cache hits.
PageReqTotal	INTEGER	Number of VXML page requests.
ParentID	VARCHAR(255)	Session ID of parent session, “root”.
RecordDate	INTEGER	The date on which the record is written on the MPP. The format is YYYYMMDD and is always in GMT.
RecordID	INTEGER	SDR entry count by day.

Table continues…

Column	Data Type	Description
RecordType	INTEGER	This can be: • 0: maintains statistics for an entire session and all dialogs within the session • 1: maintains statistics for a single dialog when multiple dialogs exist within a session • 2: maintains statistics for a session containing only a single dialog.
SessionID	VARCHAR(255)	Session ID generated by the media server .
SessionTimestamp	TIMESTAMP	Date and Time of the start of the session stored in a single Timestamp column. Based on GMT time zone.
Slot	INTEGER	MPP slot number that handled the call. This is related to the MPP session log generation.
SMSEntryId	BIGINT, NUMBER(20,0)	Stores the primary key of the SDR record from the operational database for the SMS processor component. Contains 0 when SDR is from another source.

Table continues…

Column	Data Type	Description
Source	VARCHAR(255)	Cause of the session startup This can be: • Inbound: specifies session was generated from inbound call or an outbound call. • LaunchCCXML: specifies that the session was generated as an outbound call from LaunchVXML. • LaunchVoiceXML: specifies that the session was generated as an outbound call from LaunchCCXML. • SMSInbound: The session was generated by an incoming SMS. • SMSReceipt: The session was initiated by a SMS delivery receipt. • EmailInbound: The session was generated by an incoming Email. • EmailReceipt: The session was initiated by an Email DSN. • LaunchSMS: The session was initiated through the LaunchSMS method on the outcall webservice. That is, through the SMS application. • LaunchEmail: The session was initiated through the LaunchEmail method on the outcall webservice. That is, through the Email application. LaunchHTML: The session was initiated through the LaunchHTML method on the outcall webservice. For example, called by the HTML Redirector app in response to a request from a mobile web browser.
StartDate	INTEGER	Date the session started in YYYYMMDD format. Based on GMT timezone.
StartPageName	VARCHAR(512)	URL of initial page loaded when call started.
StartTime	INTEGER	Time of day that the call started in HHMMSS format for GMT timezone.
TerminationInfo1	VARCHAR(64)	Optional Information set by the application (through the Exit tag or the session.exitInfo1 variable in DD).
TerminationInfo2	VARCHAR(64)	Optional Information set by the application (through the Exit tag or the session.exitInfo2 variable in DD)
TerminationInfo3	VARCHAR(64)	Optional Information set by the application (through the Exit tag*)
TerminationInfo4	VARCHAR(64)	Optional Information set by the application (through the Exit tag*)

Table continues…

Column	Data Type	Description
TerminationInfo5	VARCHAR(64)	Optional Information set by the application (through the Exit tag*)
TerminationInfo6	INTEGER	Optional Information set by the application (through the Exit tag*)
TerminationInfo7	INTEGER	Optional Information set by the application (through the Exit tag*)
TerminationInfo8	INTEGER	Optional Information set by the application (through the Exit tag*)
TerminationInfo9	INTEGER	Optional Information set by the application (through the Exit tag*)
TerminationInfo10	INTEGER	Optional Information set by the application (through the Exit tag*)
TerminationPageName	VARCHAR(512)	The VoiceXML or CCXML page where the disconnect event occurred.
TerminationPageName Short	VARCHAR(255)	The VoiceXML or CCXML page where the disconnect event occurred. Similar to terminationpagename column except contains only the page name and the file extension, rather than the full URL.
TerminationReason	VARCHAR(64)	Reason call terminated as set by the application (through the Exit tag). If an application does not set a value, the system defines the default value as Application exited.
TTSServer	VARCHAR(255)	IP address of the TTS server used by the session.
UttCntRecWPage	INTEGER	Number of recognized utterances received on the page with the worst recognition
UttCntTot	INTEGER	Total number of utterances in session.
UttCntTotRec	INTEGER	Total number of recognized utterances in session.
UttCntRecWPage	INTEGER	Nmber of recognized utterances made on the page with the lowest percentage of correctly recognized utterances.
UttCntWPage	INTEGER	Total number of utterances made on the page with the lowest percentage of correctly recognized utterances.
VPID	INTEGER	Identifies the EP system within a cluster of multiple EP systems that merge the data into the same external database. If there is only one EP system at an installation, this field is always 1.
ZoneID	INTEGER	Identifies the Zone of the component creating this record. This value can be used as a key into the vpZones table. Added in EP 7.0

VPApplication table

Experience Portal is a platform on which customer defined web applications control call flow based on your information provided through voice dialogs. Applications are identified by name on each Experience Portal system in a cluster. The system invokes an application through its URL in order to handle a call. There is one row in this table for each application in a cluster.

Table 7: Primary key columns

Name
VPID
AppName

Table 8: Columns

Column	Data Type	Description
VPID	INTEGER	Identifies the EP system within a cluster of multiple EP systems that merge the data into the same external database. If there is only one EP system at an installation, this field is always 1.
APPName	VARCHAR2(256)	A text string identifying the application within a particular Experience Portal system.
AppURL	VARCHAR2(2048)	The invocation URL of the application.
DeleteDate	VARCHAR2(64)	Currently unused.

Custom VPPerformance Reports

The vpperformance report contains performance statistics for each MPP in the Experience Portal system. This information is obtained from the MPP heartbeat request and is aggregated over a configured period (5 minutes by default). Statistics are identified by the ResourceID and apply to a specific time interval and a specific MPP server in the cluster. This table has one row for each statistic, for each MPP in a cluster, for each time interval in which an MPP heartbeat response was received. Rows are created upon completion of each aggregation period. Rows are deleted according to an administrable data retention limit.

Table 9: Primary key columns

Name
VPID
MPP
Time
ResourceID
ComponentID

Table 10: Columns

Column	Data Type	Description
VPID	INTEGER	Identifies the EP system , within a cluster of multiple EP systems that merge the data into the same external database. If there is only one EP system at an installation, this field will always be 1.
MPP	VARCHAR2(256)	The unique name assigned to this MPP through the EPM.
Time	VARCHAR2(64)	Timestamp of the aggregated statistic.
ResourceID	VARCHAR2(256)	Name of the statistic to which this row applies: • CPU - Percentage of CPU utilization • Disk - Percentage of disk utilization • Memory - Percentage of memory in use • Port - Percentage of licensed telephony resources currently in use • Inbound Calls - Total active inbound calls • Outbound Calls - Total active outbound calls
Duration	INTEGER	Time period that the data represents in milliseconds.
Sum	INTEGER	Sum of all the statistics taken in the aggregation period.
Count	INTEGER	Number of statistics taken in the aggregation period (number of heartbeats).
Peak	INTEGER	Largest statistic taken in the aggregation period.
Minimum	INTEGER	Smallest statistic taken in the aggregation period.
CurrentResource	INTEGER	Last value received from the heartbeat in aggregate period.
SourceType	INTEGER	Type of system resource is from: • 0 = MPP • 1 = EPM Primary • 2 = EPM Secondary • 3 = Overall Experience Portal • 4 = OM Stat
ComponentID	INTEGER	The component ID from AMS for OM statistic. The value in this column is populated when the value of SourceType is equal to 4. This column was added in Experience Portal 6.0.

VPMpps table

Each Experience Portal system in a cluster is supported by one or more media servers; the number being configured to support the anticipated system load. When a media server receives a call from a PBX, it invokes a VoiceXML application on an application server and communicates with ASR and TTS servers to process the call. Media servers are identified by name on each Experience Portal system in a cluster. There is one row in this table for each media server in the Experience Portal cluster.

Table 11: Primary key columns

Name
VPID
MPPName

Table 12: Columns

Column	Data Type	Description
VPID	INTEGER	Identifies the Experience Portal system within a cluster of multiple Experience Portal systems that merge the data into the same external database. If there is only one Experience Portal system at an installation, this field is always 1.
MPPName	VARCHAR2(256)	The unique name assigned to the media server through the EPM.
DeleteDate	VARCHAR2(64)	Currently unused.

VPSystems table

Multiple Experience Portal systems store their reporting data in the same external database even though those systems are autonomous in all respects. Together these multiple Experience Portal systems are said to form the Experience Portal cluster. To ensure that the data from separate systems can be distinguished, each system is assigned a unique numeric identifier (the VPID) in addition to having a unique system name (the VPName).

This table has one row for each Experience Portal system in the Experience Portal cluster.

Note:

This data model differs slightly from the actual implementation. The model lists VPID as the primary key to illustrate the logical relationships between tables. In the actual implementation the primary key is VPName with VPID as an attribute.

Table 13: Primary key columns

Name
VPID

Column	Data Type	Description
VPID	INTEGER	Identifies the EP system , within a cluster of multiple EP systems that merge the data into the same external database. If there is only one EP system at an installation, this field is always 1.
VPName	VARCHAR2(512)	The administered name of this Experience Portal system.
TimeZoneDrift	INTEGER	Offset in milliseconds of the Experience Portal system from GMT.
AdminURL	VARCHAR2(2048)	IP address of the Experience Portal system.
CreateDate	VARCHAR2(64)	Timestamp of the time the Experience Portal system was first added to the cluster.
LastUpdate	VARCHAR2(64)	Timestamp of the time that configuration data changed in the table.
LicensedTelephony	INTEGER	Total telephony licenses purchased for the Experience Portalsystems.
LicensedASR	INTEGER	Nonzero if ASR is licensed for the Experience Portal system.
LicensedTTS	INTEGER	Nonzero if TTS is licensed for the Experience Portal system.
CallCapacity	INTEGER	Total Telephony resources concurrently configured to take calls across all media servers for this EP system. The number can be less than the sum of the individual media server maximum port configuration represented by TotalCapacity column.
LicensesAllocated	INTEGER	Telephony resources assigned to MPPs.
TotalCapacity	INTEGER	Total of the maximum call capacity of all the MPPs in an EP system.
DatabaseFail	TIMESTAMP	Currently unused.
IncomingCalls	INTEGER	Number of currently active inbound calls.
OutgoingCalls	INTEGER	Number of currently active outbound calls made from Experience Portal system.

Table continues…

Column	Data Type	Description
AlarmStatus	INTEGER	Current alarm status of the Experience Portal system: • 0 = none • 1 = Minor • 2 = Major • 3 = Critical Corresponds to EPM Status Monitor Alarm icons : • 0 - green • 1 - yellow • 2 - red
StatusUpdate	VARCHAR2(64)	Timestamp of when the last status update occurred (Licensing and call info).
SystemType	INTEGER	Primary or secondary
RecordStatus	VARCHAR2(32)	Set to 'Active' if the Experience Portal system participates in the cluster. Set to 'Inactive' if the Experience Portal system left the cluster.
Version	VARCHAR(32)	The version of the software that is currently running on the system.

Note:

The supplied scripts to create the reporting tables will use the appropriate data types for the selected database vendor.

VPUCIDMap table

This report maps each MPP within a cluster to a unique numeric identifier, MPPID, which is included in UCID strings identifying calls originated by that media server. This table is just an extension of the VPMPPs table. There is one row in this table for each MPP server in an EP cluster.

The primary keys are:

- VPID
- MPPName

Column	Data Type	Description
VPID	INTEGER	Identifies the EP system , within a cluster of multiple EP systems that merge the data into the same external database.
MPPName	VARCHAR2(256)	The unique name assigned to the MPP through the EPM.

Table continues…

Column	Data Type	Description
MPPID	INTEGER	Internally generated ID assigned to each MPP which is unique across the cluster. The ID is used to generate UCID.

Generating Custom reports using Experience Portal Manager

Custom Reports using EPM

You can use the Custom Reports feature to generate reports for your specific requirements. You must select a standard report or an existing custom report format as a base for generating the custom report. The custom report uses the standard set of filters defined by the Experience Portal system for the selected base report. You can then change the selection of filters to suite your requirements.

You can run the Custom Report on-demand by clicking the View Report icon. Prior to generating a report, you can also click the Report Name link on the Custom Reports page to view and edit the saved filter and column values.

Note:

You cannot change the source report and the name of the report while editing the custom report filters.

Generating a Custom report using EPM

About this task

The custom report provides summary information about all the filtering options specified in the source report that you used for generating the report.

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 **Reports** > **Custom**.
3. On the Custom Reports page, click **Add**.
4. Optionally, click  next to the existing custom report name link to generate the report.

Tip:

Placing the mouse pointer over the existing custom report name displays a tooltip that lists the user ID of the user who created the custom report.

5. On the Add Custom Report (Filters) page, select a source report from the **Standard Reports** or the **Custom Reports** lists. On selecting a source report, the filters get refreshed to correspond to the selected source report.
6. To create a custom report with organization level access, select an organization from the **Organizations** list. If you do not select an organization, this indicates that the user does not belong to any organization.

   Note:

   This field is displayed only if organization level access is enabled in the Avaya Experience Portal system and you have logged in as a user not assigned to any organization. For more information on organization level access, see Organization level access in Avaya Experience Portal on page 115.

   If you select an organization for a custom report, the option to select an application is enabled. Only those applications are listed which belong to the organization.
7. Specify a name for the report.

   Note:

   If you have selected an organization in the field above, the selected organization and forward slash character are automatically prefixed to the report name.
8. Enter the filter criteria that you want to use.

   Tip:

   Click the **more >>** link to display the rest of the optional filters.
9. Click **OK**.

   The EPM displays the report.
10. Optionally, click **Save** to save the filter settings without generating the report.

Trending By report

Use the Contact Summary Report to produce a trending report to compare different categories of information over a period of time. You can define custom reports that display activities of your interest and use the trending report feature in Contact Summary Report to see how the activity levels varied from day to day. You can compare five such items in a single report.

The report displays the output in both tabular and graph format. The tabular format displays the daily summary and contains a row for every day in the specified time range. The graph displays

hourly data and starts with the first hour that contains data and ends with the last hour that contains data.

Each metric displayed in the Contact Trending table and graph is represented by an Experience Portal custom report. Each custom report must contain the filter values that produce a single metric when that report is run. The Trending By option in the Contact Summary filter page provides all eligible custom reports. You can select multiple custom reports to generate the output. Experience Portal uses the name of the custom report as the metric name in the Trending By output table and graph.

The following custom reports are not supported and not displayed for selection:

- Custom reports based on Performance Reports
- Custom reports that contain Trending By reports

Note:

Application reports that contain vxml or ccxml log tags are not currently supported. However, reports populated by the Orchestration Designer call flow data or Orchestration Designer report nodes are supported.

Scenario

A car rental business wants to track and compare certain types of car size rentals over a period of time.

Method

- Set the car size in either an SDR exit variable or log it through the Report Node to the vpAppLog table through the Orchestration Designer application.
- Create two custom reports:
  - One with the filter values to restrict the output of that report to only sessions where small cars were rented. For example, a Session Summary report with **ExitInfo1** set to `small`.
  - Another with sessions where midsize cars were rented. For example, a Session Summary report with **ExitInfo1** set to `midsize`.
- Select both custom reports in the **Trending By** field.

Analysis

The report displays how many contacts each day were associated with the sessions in each of the custom reports. Click the View Graph link to display a timeline graph of hourly contacts that met the criteria in the custom report. The Contact Trending report might show that during the past 90 days rentals of midsize cars trended 20% higher as compared to a relatively flat number of rentals for small cars.

Scheduled reports

Scheduled Reports

You can schedule the generation of the standard or the custom reports to occur on a periodic or one time basis. You can receive the report output as an email attachment, or access it through the secure links in the email notification, RSS feeds or by logging into the Experience Portal Manager (EPM). You can optionally set **Record Threshold** restriction value when scheduling a report. Setting this restriction generates a notification only when the total record count reaches the specified minimum value.

Using the Scheduled Reports page, you can add, edit, or delete a scheduled report. You can also view and export the report output for a specified report or all the reports.

The Scheduled Reports page is distributed in two tabs:

- Schedules
- Outputs

Use the **Schedules** tab to view, add, edit, or delete a scheduled report. You can also view and export the details regarding the output and history for a specific scheduled reports by clicking the **Output** folder icon on this tabbed page. You can also subscribe for change notifications by clicking the  icon under **Notification Method** column.

Use the **Outputs** tab to view the details regarding the output and history for all the scheduled reports. You can export the report outputs by clicking the **Export** icon on this tabbed page.

Scheduling a Report

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 **Reports** > **Scheduled**.
3. On the Scheduled Reports page, click **Add**.
4. On the Add Scheduled Report page, select a source report that you want to schedule, from the **Standard Reports** or the **Custom Reports** lists.
5. Enter the filter criteria that you want to use.
6. Specify the date and time for the scheduling, notification method that you want to use, and the record threshold restriction value.
7. Specify the **Output Type** for the scheduled report. You can select one of the **xls**, **pdf**, and **csv** options.

8. Click **Save**.

   The EPM displays the scheduled report entry on the Scheduled Reports page.

SQL queries for the EPM reports

When the EPM generates a report, it sends one or more SQL queries to the Experience Portal database and displays the result as a EPM page. This topic shows the:

Note:

For all reports, user-entered dates and times are converted from the local EPM server timezone to the GMT timezone prior to performing the SQL query.

Application Detail report query

```
SELECT * FROM vpapplog
WHERE (LogTimestamp >= 'yyyy-mm-dd hh:mm:ss.0' AND LogTimestamp <= 'yyyy-mm-dd
hh:mm:ss.0')
ORDER BY logtimestamp DESC, sessionindex DESC LIMIT 10000;
```

Application Summary report queries

```
SELECT {SummarizeByField}, count(*) as TotalCount FROM  vpapplog
WHERE (LogTimestamp >= 'yyyy-mm-dd hh:mm:ss.0' AND LogTimestamp <= 'yyyy-mm-dd
hh:mm:ss.0')
GROUP BY {SummarizeByField} ORDER BY TotalCount DESC;
CREATE TEMP TABLE tmpADR AS
SELECT DISTINCT sessionid, {SummarizeByField} FROM vpapplog
WHERE (LogTimestamp >= 'yyyy-mm-dd hh:mm:ss.0' AND LogTimestamp <= 'yyyy-mm-dd
hh:mm:ss.0')
GROUP BY by sessionid, {SummarizeByField};
+
SELECT {SummarizeByField}, count(*)as CallCount FROM tmpADR
GROUP BY {SummarizeByField} ORDER BY CallCount desc;
```

Where *{SummarizeByField}* can be any of the following:

- loglevel
- message
- activityname
- logtype
- varname & varvalue

Contact Detail report query

```
SELECT * FROM  CDR
WHERE  ( (CALLSTARTDATE > yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME >=
hhmmss )) AND
 ( CALLSTARTDATE < yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME <= hhmmss)) )
ORDER BY CALLSTARTDATE ASC, CALLSTARTTIME ASC, RECORDID ASC LIMIT 10000;
```

Contact Summary report queries

```
SELECT Count(DURATION) as totalcalls, Sum(DURATION) as totalsum, ENDTYPE as etype FROM
CDR
WHERE  ( (CALLSTARTDATE > yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME >=
hhmmss )) AND
( CALLSTARTDATE < yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME <= hhmmss)) )
GROUP BY ENDTYPE;
SELECT Count(DURATION) as totalcalls, Sum(DURATION) as totalsum, applicationname FROM
CDR
    WHERE  ( (CALLSTARTDATE > yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME
>= hhmmss )) AND
 ( CALLSTARTDATE < yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME <= hhmmss)) )
GROUP BY applicationname ORDER BY Count(DURATION) desc;
SELECT Count(*) as totalcalls, Sum(DURATION) as totalsum, MPP as mppcolumn FROM  CDR
WHERE  ( (CALLSTARTDATE > yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME >=
hhmmss )) AND
( CALLSTARTDATE < yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME <= hhmmss)) )
GROUP BY MPP ORDER BY COUNT(MPP) DESC;
SELECT Count(MPP) as totalcalls, Sum(DURATION) as totalsum, MPP as mppcolumn, PORTID as
portidcolumn FROM  CDR
WHERE  ( (CALLSTARTDATE > yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME >=
hhmmss )) AND
( CALLSTARTDATE < yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME <= hhmmss)) )
GROUP BY MPP, PORTID ORDER BY COUNT(MPP) DESC;
SELECT callstartdate, callstarttime, recordid FROM  CDR
WHERE ( (CALLSTARTDATE > yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME >=
hhmmss )) AND
( CALLSTARTDATE < yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME <= hhmmss)) )
ORDER BY CALLSTARTDATE ASC, CALLSTARTTIME ASC, RECORDID ASC;
SELECT duration/60 AS BUCKET, count(duration) AS BUCKETCOUNT FROM CDR
WHERE ( (CALLSTARTDATE > yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME >=
hhmmss )) AND
( CALLSTARTDATE < yyyymmdd OR (CALLSTARTDATE = yyyymmdd AND CALLSTARTTIME <= hhmmss)) )
GROUP BY duration/60 ORDER BY BUCKET DESC;
```

Performance report queries

```
SELECT Max(Peak) as peak, sum(sum) as sum, sum(count) as count, mpp, resourceid FROM
vpperformance
WHERE  (time >='yyyy-mm-dd hh:mm:ss.0' AND time < 'yyyy-mm-dd hh:mm:ss.0')
GROUP BY mpp, resourceid ORDER BY mpp;
SELECT peak/10 as util_buckets, sum(duration) as duration FROM vpperformance
where time >='yyyy-mm-dd hh:mm:ss.0' AND time < 'yyyy-mm-dd hh:mm:ss.0' AND resourceid
= 'PORT'
GROUP BY util_buckets ORDER BY util_buckets;
```

Session Detail report query

```
SELECT * FROM SDR
WHERE ( (STARTDATE > yyyymmdd OR (STARTDATE = yyyymmdd AND STARTTIME >= hhmmss )) AND
( STARTDATE < yyyymmdd OR (STARTDATE = yyyymmdd AND STARTTIME <= hhmmss)) )
ORDER BY STARTDATE ASC, STARTTIME ASC, RECORDID ASC LIMIT 10000;
```

Session Summary report queries

```
SELECT count(recordid) as totalcalls, avg(timetillanswer) as timetillanswer,
avg(latanswer) as latanswer,
avg(duration) as duration, avg(uttcnttot) as uttcnttot, avg(uttcnttotrec) as
uttcnttotrec, avg(pagereqcachehits) as pagereqcachehits,
```

```
avg(pagereqtotal) as pagereqtotal FROM SDR
WHERE  ( (STARTDATE > yyyymmdd OR (STARTDATE = yyyymmdd AND STARTTIME >= hhmmss )) AND
( STARTDATE < yyyymmdd OR (STARTDATE = yyyymmdd AND STARTTIME <= hhmmss)) );
SELECT latwpage as latwpage, latwpagename as latwpagename, mpp as mpp FROM SDR
WHERE  ( (STARTDATE > yyyymmdd OR (STARTDATE = yyyymmdd AND STARTTIME >= hhmmss )) AND
 ( STARTDATE < yyyymmdd OR (STARTDATE = yyyymmdd AND STARTTIME <= hhmmss)) )
ORDER BY latwpage desc;
SELECT uttcntwpage as uttcntwpage, uttcntrecwpage as uttcntrecwpage, uttwpagename, mpp
as mpp, asrpercent FROM SDR
WHERE  ( (STARTDATE > yyyymmdd OR (STARTDATE = yyyymmdd AND STARTTIME >= hhmmss )) AND
 ( STARTDATE < yyyymmdd OR (STARTDATE = yyyymmdd AND STARTTIME <= hhmmss)) )
ORDER BY asrpercent asc;
SELECT Count(*) as totalsessions, vpid, applicationname, terminationpagenameshort
FROM SDR WHERE ( (STARTDATE > yyyymmdd OR (STARTDATE = yyyymmdd AND STARTTIME >=
hhmmss )) AND
( STARTDATE < yyyymmdd OR (STARTDATE = yyyymmdd AND STARTTIME <= hhmmss)) )
GROUP BY vpid, applicationname, terminationpagenameshort order by vpid,
applicationname, totalsessions desc
```

Chapter 21: Certificates

Overview

Experience Portal servers use the TLS protocol for all inbound and outbound secure communication which includes:

- Communication from one Experience Portal server to another Experience Portal server
- Communication from an Experience Portal server to external network entities (such as Application Servers, SMGR, SIP Proxies, Speech Servers, and so on.)

Experience Portal servers refers to Primary EPM, Auxiliary EPM, or MPP. The TLS protocol requires the exchange and validation of identity certificates to provide secure communication.

There are three types of security certificates in Experience Portal:

- EP Signing Certificate
- Identity Certificates
- Trusted Certificates

EP Signing Certificate (EP Root Certificate)

The EP Signing Certificate is the Certificate Authority Root Certificate for Experience Portal. It is installed by default on the Primary EPM.

The purpose of the EP Signing Certificate is to allow the Primary EPM server to act as the Certificate Authority for all Experience Portal servers. The Primary EPM uses the EP Signing Certificate to issue and sign identity certificates to all the Experience Portal servers.

The EP Signing Certificate is enabled only when the default identity certificates are in use by the Experience Portal servers. If externally signed identity certificates are in use by Experience Portal servers, the EP Signing Certificate must be disabled.

Identity Certificates

Each Experience Portal server has a single identity certificate that it uses to establish secure communication with other network entities.

Experience Portal servers can use either of the following certificates:

- **Default identity certificates:** Identity certificates that are issued and signed by the EP Certificate Authority (signed by the EP Signing Certificate).
- **Externally signed identity certificates:** Custom identity certificates that are signed by an external Certificate Authority (CA). External CA's are also known as third-party CA's and refer to commercial Certificate Authorities, an enterprise Certificate Authority, an SMGR or any on-premise Certificate Authority.

Trusted Certificates

Trusted certificates are Certificate Authority (CA) certificates. These certificates are used to validate identity certificates that are received by the Experience Portal servers during the setup of TLS communication.

Generally, a trusted certificate can be a single certificate (usually the Root certificate of the CA) or a chain of certificates (CA intermediate certificates and Root certificate).

If Experience Portal receives an identity certificate which was issued and signed by a trusted certificate that is installed on Experience Portal, the identity certificate is deemed trusted.

There are different types of trusted certificates in Experience Portal that determine what communication links they will be used to validate identity certificates for. For example, Application-type trusted certificates are used to validate secure communication between Experience Portal servers and external Application Servers.

Certificate Authorities

With default identity certificates, the Primary EPM acts as a Certificate Authority for the Experience Portal servers. The EP Signing Certificate is used by the primary EPM to issue and sign identity certificate for all the Experience Portal servers.

If Experience Portal uses custom identity certificates, the EP Signing Certificate must be disabled. The custom identity certificates for the Experience Portal servers must then be issued and signed by an external Certificate Authority.

An external or third-party Certificate Authority refers to any of the following:

- Commercial Certificate Authorities
- An enterprise Certificate Authority
- The Certificate Authority of System Manager (SMGR)
- Any Certificate Authority outside Experience Portal

Viewing Certificates

Procedure

1. Log on to the EPM web interface.
2. On the EPM navigation pane, click **Security** > **Certificates**.

   This Certificates page displays all the certificates including the EP Signing certificate, EPM identity certificates, MPP identity certificates, and all the trusted certificates that are currently installed on Experience Portal.

Certificates page field descriptions

Use this page to:

- View, Upload, Generate, or Disable signing of the EP Signing certificate.
- Upload or Generate a Certificate Signing Request for the EP Signing certificate.
- View identity certificates for EPM servers.
- View identity certificates for MPP servers.
- Import, Upload, or Delete Trusted Certificates.
- View or Edit Security Settings.

Name	Description
EP Signing Certificate	Contains two tabs: • Certificate tab: Displays the current installed EP Signing certificate. • Certificate Signing Request tab: Displays the current generated Certificate Signing Request.
EPM Identity Certificates	Displays the identity certificates that are currently installed on the EPM servers.
MPP Identity Certificates	Displays the identity certificates that are currently installed on the MPP servers.
Trusted Certificates	Displays the trusted certificates that are currently installed on Experience Portal.
Security Settings	Opens the Security Settings page. For details, see Security Settings page field descriptions on page 598.

EP Signing Certificate

On the EP Signing Certificate tab on the Certificates page, there are two sub-tabs:

- **Certificate** tab: Displays the current installed EP Signing certificate.
- **Certificate Signing Request** tab: Displays the current generated Certificate Signing Request.

Certificate tab on the EP Signing Certificate tab of the Certificates page field descriptions

Use this tab to view the currently installed EP Signing Certificate that is used in the issuing of identity certificates for Experience Portal servers. You can also upload or generate a new EP Signing Certificate.

Field or Button	Description
Security Certificate	Displays the current EP Signing Certificate.
Upload	Opens the Upload EP Signing Certificate page.
Generate	Generates a new EP Signing Certificate.
Disable Signing	Removes the EP Signing Certificate from the system. The identity certificates signed by this EP Signing Certificate will continue to work until one of the following: • The identity certificates are replaced by externally signed identity certificates. For more information, see Externally signed identity certificates on page 577. • A new EP Signing Certificate is installed.

Generating a new EP Signing Certificate

About this task

You can generate a new EP Signing Certificate if required. However, it is not recommended to make this a frequent operation.

Generating a new EP Signing Certificate will force all Experience Portal servers to replace their current identity certificate with a new identity certificate signed by the new EP Signing Certificate. This will happen on the next restart of the Experience Portal servers' services.

Important:

After generating a new EP Signing Certificate, restart the Experience Portal servers. On the EPM web interface, go to **System Management** > **EPM Manager** or **MPP Manager**, and restart the servers in the following order:

1. MPP servers
2. Auxiliary EPM servers
3. Primary EPM servers

Note:

Do not generate the EP Signing Certificate multiple times without restarting all the Experience Portal servers. This will potentially cause loss of communication between the Experience Portal servers. In case this happens, do the following to regain communication between the servers:

- Reconnect all MPP servers with the EPM server

- Reconnect the primary and auxiliary EPM servers
- Restart the Primary EPM.

For more information, see Reconnecting an existing MPP server with the EPM server on page 210 and Reconnecting the primary and auxiliary EPM servers on page 187.

Procedure

1. Log on to the EPM web interface.
2. On the EPM navigation pane, click **Security** > **Certificates**.
3. Click the EP Signing Certificate tab.
4. Click the Certificate tab.
5. Click **Generate** to generate a new EP Signing Certificate.

Uploading the EP Signing Certificate

About this task

Use this page to upload an external CA issued EP Signing Certificate if the external CA generated the CSR and private key. However, it is not recommended to make this a frequent operation.

When uploading a new EP Signing Certificate, the EP Signing Certificate must be issued by an external Certificate Authority. The uploaded EP Signing Certificate must have Basic Constraints with a CA value set to true.

Uploading a new EP Signing Certificate will force all Experience Portal servers to replace their current identity certificate with a new identity certificate signed by the new externally signed EP Signing Certificate. This will happen on the next restart of the Experience Portal servers' services.

Important:

After uploading a new EP Signing Certificate, restart the Experience Portal servers. On the EPM web interface, go to **System Management** > **EPM Manager** or **MPP Manager**, and restart the servers in the following order:

1. MPP servers
2. Auxiliary EPM servers
3. Primary EPM servers

Note:

Do not upload the EP Signing Certificate multiple times without restarting all the Experience Portal servers. This will potentially cause loss of communications between the Experience Portal servers. In case this happens, do the following to regain communication between the servers:

- Reconnect all MPP servers with the EPM server
- Reconnect the primary and auxiliary EPM servers
- Restart the Primary EPM.

For more information, see Reconnecting an existing MPP server with the EPM server on page 210 and Reconnecting the primary and auxiliary EPM servers on page 187.

Note:

If you are importing an EP Signing Certificate signed by an external Certificate Authority, ensure the following:

- The certificate must be formatted as a PKCS#12 file. A PKCS#12 file always includes a certificate and its corresponding key. The certificate is encrypted and requires a password. The PKCS#12 file must include all CA certificates.
- The EP Signing certificate must include the standard extension Basic Constraints with the CA:true attribute. This allows the EP Signing Certificate to issue and sign identity certificates.
- If the Extended Key Usage is specified in the X509.V3 certificate extension, specify `Server Authentication` (serverAuth), and `Client Authentication` (clientAuth) for the usage.

Procedure

1. Log on to the EPM web interface.
2. On the EPM navigation pane, click **Security** > **Certificates**.
3. Click the EP Signing Certificate tab.
4. Click the Certificate tab.
5. Click **Upload** to upload a new EP Signing Certificate.
6. On the Upload EP Signing Certificate page, click **Choose File**, and select the certificate file in the dialog box.
7. In the **Password** field, enter the password for the PKCS#12 file
8. Click **Install**.

Certificate Signing Request tab on the EP Signing Certificate tab of the Certificates page field descriptions

Use this tab to configure a certificate signing request (CSR). After the CSR is signed, the signed certificate can be uploaded as the EP Signing Certificate of the Primary EPM.

You can also do the following on this page:

- Upload the signed certificate (EP Signing Certificate).
- Generate a new certificate signing request.
- Export the certificate signing request in the Base-64 encoded PEM format and submit it to an external CA to create and sign the security certificate (EP Signing Certificate).

Name	Description
Certificate Signing Request Details	Displays the current certificate signing request details that include the following information: • Subject • Signature Algorithm • Public Key Size • Public Key Algorithm • Basic Constraints • Extended Key Usages • Key Usage • Subject Alternate Name
Upload	Opens the Upload Signed Certificate page to upload the EP Signing Certificate.
Generate	Opens the Generate Certificate Signing Request page.

View Certificate Signing Request tab on the Certificates page field descriptions

Use this tab to view a certificate signing request (CSR). After the CSR is signed by an external Certificate Authority, the externally signed certificate can be uploaded as the EP Signing Certificate of the Primary EPM.

Name	Description
Certificate Signing Request Details	Displays the current certificate signing request details that include the following information: • Subject • Signature Algorithm • Public Key Size • Public Key Algorithm • Basic Constraints • Extended Key Usages • Key Usage • Subject Alternate Name

Uploading a Signed Certificate

About this task

Use this page to upload an external CA issued EP Signing Certificate if a CSR was generated on Experience Portal through the Certificate Signing Request tab and provided to the external CA. The uploaded certificate file must include the complete chain of certificates in PEM format. These include the public certificates of all external CA's involved in the signing process (Intermediate and

Root CA's) and the EP Signing Certificate that was signed by the external CA. The external CA uses the certificate signing request generated from the EPM to generate the EP Signing Certificate.

Uploading a new EP Signing Certificate will force all Experience Portal servers to replace their current identity certificate with a new identity certificate signed by the new externally signed EP Signing Certificate. This will happen on the next restart of the Experience Portal servers' services.

Important:

After uploading a new EP Signing Certificate, restart the Experience Portal servers. On the EPM web interface, go to **System Management** > **EPM Manager** or **MPP Manager**, and restart the servers in the following order:

1. MPP servers
2. Auxiliary EPM servers
3. Primary EPM servers

Note:

Do not upload the EP Signing Certificate multiple times without restarting all the Experience Portal servers. This will potentially cause loss of communications between the Experience Portal servers. In case this happens, do the following to regain communication between the servers:

- Reconnect all MPP servers with the EPM server
- Reconnect the primary and auxiliary EPM servers
- Restart the Primary EPM.

For more information, see Reconnecting an existing MPP server with the EPM server on page 210 and Reconnecting the primary and auxiliary EPM servers on page 187.

Procedure

1. Log on to the EPM web interface.
2. On the EPM navigation pane, click **Security** > **Certificates**.
3. Click the EP Signing Certificate tab.
4. Click the Certificate Signing Request tab.
5. Click **Upload** to upload a new EP Signing Certificate.
6. On the Upload Signed Certificate page, click **Choose File**, and select the certificate file in the dialog box.
7. Click **Continue**.
8. Click **Save**.

Upload Signed Certificate page field descriptions

Use this page to an external CA issued EP Signing Certificate if a CSR was generated on Experience Portal through the Certificate Signing Request tab and provided to the external CA. The uploaded certificate file must include the complete chain of certificates in PEM format. These

include the public certificates of all external CA's involved in the signing process (Intermediate and Root CA's) and the EP Signing Certificate that was signed by the external CA. The external CA uses the certificate signing request generated from the EPM to generate the EP Signing Certificate.

Note:

The uploaded EP Signing certificate is validated against the private key stored in the database. If the EP Signing certificates are valid, they will replace the existing EP Signing Certificate on the primary EPM.

Name	Description
Security Certificate File	The option to browse for the file name of the EP Signing Certificate chain file.
Continue	The option to submit the location of the signed security certificate to Avaya Experience Portal for verification. Avaya Experience Portal downloads the SSL (Secure Sockets Layer) certificate from the designated location. If the SSL certificate fails to download, Avaya Experience Portal asks you to correct the Location field entry and try again. When the SSL certificate downloads successfully, Avaya Experience Portal will validate the uploaded signed certificate with the private key stored in the database. If the signed certificate matches the private key in the database, Avaya Experience Portal displays the second Upload Signed Certificate page.
Cancel	The option to cancel the changes made. If you click **Cancel**, you will navigate to the Certificate Signing Request page.

(Save) Upload Signed Certificate page field descriptions

Use this page to save the uploaded EP Signing Certificate.

Name	Description
Display text box	The text of the uploaded signed certificates.
Save	The option to install and replace the current EP Signing Certificate on the EPM.
Cancel	The option to cancel the changes made. If you click **Cancel**, you will navigate to the Certificate Signing Request page.

Generating a Certificate Signing Request

Procedure

1. Log on to the EPM web interface.
2. On the EPM navigation pane, click **Security** > **Certificates**.
3. Click the EP Signing Certificate tab.
4. Click the Certificate Signing Request tab.

5. Click **Generate** .
6. On the Generate Certificate Signing Request page, enter the appropriate details in the fields to generate a new certificate signing request.
7. Click **Save**.

Generate Certificate Signing Request page field descriptions

Use this page to generate a Certificate Signing Request for the EP Signing Certificate which can be sent to an external CA to request a signed certificate.

By default, the certificate signing request has the following characteristics:

- 2048-bits length public key and private key
- SHA256 Signature Algorithm
- X509 V3 extension:
  - Basic Constraints: CA:True
  - Extended Key Usages: serverAuth, clientAuth
  - Key Usage: DigitalSignature, key_CertSign
  - Subject Alternative Name: DNSName, IPAddresses

Note:

- Before generating a new certificate signing request, it is highly recommended to check with the third-party CA on what guideline to follow when generating a certificate signing request. For example, some external CAs may not allow special characters or punctuation characters when creating the certificate signing request.
- The certificate signing request and the associated private key will be saved in the database. If the user decides to generate the certificate signing request again, the previously generated certificate signing request and private key will be replaced with the new one.

Name	Description
Common name	The full qualified domain name (FQDN) for the EPM server. Valid characters for this field can only contain: • Alphanumeric characters • Special characters: ' = ( ) + , - . / : ? and space.
Business/ Organization	The exact legal name of the organization. The name must be registered with some authority at the national, state, or city level. For example, EP Corp. Valid characters for this field can only contain: • Alphanumeric characters • Special characters: ' = ( ) + , - . / : ? and space.

Table continues…

Name	Description
Depart/Organization Unit	A section of the organization. For example, Marketing. Valid characters for this field can only contain: • Alphanumeric characters • Special characters: ' = ( ) + , - . / : ? and space.
City/ Locality	The city where the organization is legally located. For example, San Jose. Valid characters for this field can only contain: • Alphanumeric characters • Special characters: ' = ( ) + , - . / : ? and space.
State/Province/Region/Country	The State, Province, Region, or Country where the organization is legally located. For example, California. Valid characters for this field can only contain • Alphanumeric characters • Special characters: ' = ( ) + , - . / : ? and space.
Country (two-letter code)	The two-letter ISO abbreviation for your country code. For example, US.
Save	The option to save the changes made. If you click **Save**, you will navigate to the Certificate Signing Request page to display the new Certificate Signing Request details.
Cancel	The option to cancel the changes made. If you click **Cancel** , you will navigate to the Certificate Signing Request page.

Identity Certificates

EPM Identity Certificates tab on the Certificates page field descriptions

Use this tab to view or upload the identity certificates for EPM servers in Experience Portal.

Field	Description
Server Name	Lists all the primary and auxiliary EPM servers that are configured. Select the EPM server from the drop-down to display it's current identity certificate. The default value is None.
Identity certificate for EPM secure communication	Displays the identity certificate of the selected EPM server.
Upload	Opens the Upload Identity Certificate page. Allows the upload of a new identity certificate for an EPM server.

MPP Identity Certificates tab on the Certificates page field descriptions

Use this tab to view or upload the identity certificates for MPP servers in Experience Portal.

Field	Description
Server Name	Lists all the MPP servers that are configured. Select the MPP server from the drop-down list to display it's current identity certificate. The default value is None.
Identity certificate for MPP secure communication	Displays the identity certificate of the selected MPP server.
Upload	Opens the Upload Identity Certificate page. Allows the upload of a new identity certificate for a MPP server.

Externally signed identity certificates

Externally signed identity certificates for Experience Portal servers are identity certificates that are signed and issued by an external certificate authority.

These identity certificates when imported will overwrite the identity certificates that were signed and issued by the EP Signing Certificate.

Once imported, the externally signed identity certificates is used for all secure communication from the Experience Portal servers. This includes communication between Experience Portal servers as well as communication to external servers.

You must perform the installation procedures on each Experience Portal server to replace the identity certificates signed by the EP Signing certificate.

Pre-requisites for importing custom identity certificates

Ensure to do the following before importing custom identity certificates on the Experience Portal servers:

- Remove the EP Signing Certificate
- Upload the external CA Certificates as Platform type Trusted Certificate

Removing the EP Signing Certificate

About this task

Before importing custom identity certificates on the Experience Portal servers, the EP Signing Certificate must be removed.

Procedure

1. Log on to the EPM web interface.
2. On the EPM navigation pane, click **Security** > **Certificates**.
3. Click the EP Signing Certificate tab.
4. Click **Disable Signing** .

   At the prompt, confirm the removal of the EP signing certificate.

Uploading external CA certificates as a Platform type trusted certificate

About this task

Before importing custom identity certificates on the Experience Portal servers, the external CA public certificates that signed the Experience Portal server's identity certificates must be uploaded as a Platform type Trusted Certificate.

The Platform certificate file can be in PEM format or in PKCS#12 format.

If all the Experience Portal servers are signed by the same external CA, then the PKCS#12 file that contains the Primary EPM Identity Certificate can be uploaded as the Platform certificate. The external CA public certificate chain will be extracted from the PKCS#12 file and installed as a Trusted Certificate.

Note:

If all the Experience Portal servers are not signed by the same external CA, then the public certificates of each external CA that signed the identity Certificate of an Experience Portal server would need to be uploaded as a Platform type Trusted Certificate.

Procedure

1. Log on to the EPM web interface.
2. On the EPM navigation pane, click **Security** > **Certificates**.
3. Click the Trusted Certificates tab.
4. Click **Upload** to upload a trusted certificate.

5. On the Upload Trusted Certificate page, do the following:
   a. **Name**: Enter a unique name for the Platform certificate.
   b. **Type**: Select **Platform**.
   c. **Security Certificate File**: Choose the file to upload.

      Note:

      - If the certificate file is in the PKCS#12 format, the system displays the Password field.
      - If the certificate file is in the PEM format, the system does not display the Password field.
6. Click **Continue**.
7. Click **Save** to upload the certificates.

Uploading Identity Certificates

Uploading a Primary EPM server identity certificate

About this task

Use this procedure to upload an identity certificate for the Primary EPM through the Experience Portal web admin interface without re-installing the Experience Portal software. The identity certificate for the Primary EPM is issued by an external Certificate Authority.

Before you begin

- Ensure that the Primary EPM server is not processing any multi-channel messages such as Emails, SMS, or HTML.
- If a managed application is installed, you might need to perform additional steps before and after the identity certificate is updated. For more information, see the documentation of the managed application.
- Ensure that you complete the Pre-requisites for importing custom identity certificates on page 578.
- Ensure that the Primary EPM is in the Running state.

Important:

- The uploaded certificate file must be in the PKCS12 format. This includes an identity certificate, CA public certificates and the corresponding private key. This certificate is encrypted and requires a password. The password is chosen during the creation of the PKCS#12 file by the designated CA.
- If **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication` which is also called serverAuth, and `Client Authentication` which is also called clientAuth, for the usage.

- The certificate must have a valid Common Name that represents the EP server host name.
- If the Subject Alternate Name is specified in the X509 V3 certificate extension, the certificate must contain valid DNS and IP Address entries that are associated with the EP server host name.

Procedure

1. Log on to the EPM web interface.
2. Click **Security** > **Certificates**.
3. Click the **EPM Identity Certificates** tab.
4. On the **EPM Identity Certificates** tab, click **Upload**.
5. On the Upload Identity Certificate page, do the following:
   a. In the **Server Name** field, click the name of the Primary EPM server.
   b. In the **Security Certificate File** field, click **Choose File** and choose the PKCS#12 formatted security file for the Primary EPM server.
   c. In the **Password** field, enter the password of the chosen PKCS#12 formatted security file.
   d. Click **Continue**.
6. On the Save Identity Certificate page, do the following:
   a. Review the warning that the Primary EPM services will be automatically restarted to install the identity certificate.
   b. Review the identity certificate text that is displayed to ensure it is the correct certificate to install for the Primary EPM server.
   c. Click **Save** to install the identity certificate on the Primary EPM.

      Note:

      The Primary EPM services will automatically restart. Therefore, the Experience Portal web admin site may not render pages correctly until the restart is completed. The user will then be asked to login again.

Next steps

If you have not completed the Pre-requisites for importing custom identity certificates on page 578 , do the following to accept and trust the new Primary EPM identity certificate on all Auxiliary EPMs and MPPs:

1. On each auxiliary EPM and MPP, log in to the console as a `root` user.
2. Navigate to the `$AVAYA_HOME/Support/VP-Tools` directory.
3. Run the **`./setup_vpms.php <Primary EPM>`** command, where <Primary EPM> is the IP address or hostname of the Primary EPM.
4. Type `Y`, and press `Enter` to accept the new certificate.

   For NTP service, type `Y`, and press `Enter` to use the Primary EPM.

Uploading an Auxiliary EPM server identity certificate

About this task

Use this procedure to upload an identity certificate for the Auxiliary EPM through the Experience Portal web admin interface without re-installing the Experience Portal software. The identity certificate for the Auxiliary EPM is issued by an external Certificate Authority.

Before you begin

- Ensure that the Auxiliary EPM server is not processing any multi-channel messages such as Email, SMS, or HTML.
- If a managed application is installed, you might need to perform additional steps before and after the identity certificate is updated. For more information, see the documentation of the managed application.
- Ensure that you complete the Pre-requisites for importing custom identity certificates on page 578.
- Ensure that the Auxiliary EPM is in either the Stopped or Running state.

Important:

- The imported certificate file must be in PKCS#12 format. This includes an identity certificate, CA public certificates and the corresponding private key. This certificate file is encrypted and requires a password. The password is chosen during the creation of the PKCS#12 file by the designated CA.
- If **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication` which is also called serverAuth, and `Client Authentication` which is also called clientAuth, for the usage.
- The certificate must have a valid Common Name that represents the EP server host name.
- If the Subject Alternate Name is specified in the X509 V3 certificate extension, the certificate must contain valid DNS and IP Address entries that are associated with the EP server host name.

Procedure

1. Log on to the EPM web interface.
2. Click **Security** > **Certificates**.
3. Click the **EPM Identity Certificates** tab.
4. On the **EPM Identity Certificates** tab, click **Upload**.
5. On the Upload Identity Certificate page, do the following:
   a. In the **Server Name** field, click the name of the Auxiliary EPM server.
   b. In the **Security Certificate File** field, click **Choose File** and choose the PKCS#12 formatted security file for the Auxiliary EPM server.
   c. In the **Password** field, enter the password of the chosen PKCS#12 formatted security file.

d. Click **Continue**.

6. On the Save Identity Certificate page, do the following:

   a. Review the warning that the Auxiliary EPM services will be automatically restarted to install the identity certificate if the Auxiliary EPM is in the Running state.

      Note:

      If the Auxiliary EPM is in the Stopped state before this procedure, it will remain in the Stopped state after the new identity certificate is installed. The Auxiliary EPM needs to be manually started through **System Management** > **EPM Manager** to apply the new identity certificate on the Auxiliary EPM.

   b. Review the identity certificate text that is displayed to ensure it is the correct certificate to install for the Auxiliary EPM server.

   c. Click **Save** to install the identity certificate on the Auxiliary EPM.

Next steps

If you have not completed the Pre-requisites for importing custom identity certificates on page 578 , do the following to re-establish the link between the Primary EPM and the Auxiliary EPM:

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **System Configuration** > **EPM Servers**.
3. Click the name of the Auxiliary EPM server.
4. On the Change EPM Server page, navigate to the **Auxiliary EPM Certificate** section, and select the **Trust new certificate** check box if the check box is visible.
5. Click **Save**.
6. On the EPM main menu, click **Real-Time Monitoring** > **System Monitor**.
7. If the Config of the MPP displays **Restart needed**, restart the MPP.

Uploading an MPP server identity certificate

About this task

Use this procedure to upload an identity certificate for the MPP server through the Experience Portal web admin interface without re-installing the Experience Portal software. The identity certificate for the MPP server is issued by an external Certificate Authority.

Before you begin

- Ensure that the MPP server is not handling any calls.
- You may need to perform additional steps before and after the identity certificate is updated, if a managed application is installed. For more information, see the documentation of the managed application.
- Ensure that you complete the Pre-requisites for importing custom identity certificates on page 578.
- Ensure that the MPP is in the Stopped or Running state.

Important:

- The imported certificate file must be in the PKCS#12 format. This includes an identity certificate, CA public certificates, and the corresponding private key. This certificate file is encrypted and requires a password. The password is chosen during the creation of the PKCS#12 file by the designated CA.
- If **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication`, which is also called serverAuth, and `Client Authentication`, which is also called clientAuth, for the usage.
- The certificate must have a valid Common Name that represents the EP server host name.
- If the Subject Alternate Name is specified in the X509 V3 certificate extension, the certificate must contain valid DNS and IP Address entries that are associated with the EP server host name.

Procedure

1. Log on to the EPM web interface.
2. Click **Security** > **Certificates**.
3. Click the **MPP Identity Certificates** tab.
4. On the **MPP Identity Certificates** tab, click **Upload**.
5. On the Upload Identity Certificate page, do the following:
   a. In the **Server Name** field, click the name of the MPP server.
   b. In the **Security Certificate File** field, click **Choose File** and choose the PKCS#12 formatted security file for the MPP server.
   c. In the **Password** field, enter the password of the chosen PKCS#12 formatted security file.
   d. Click **Continue**.
6. On the Save Identity Certificate page, do the following:
   a. Review the warning that the MPP services will be automatically restarted to install the identity certificate if the MPP is in the Running state.

      Note:

      If the MPP is in the *Stopped* state before this procedure, it will remain in the *Stopped* state after the new identity certificate is installed. The MPP needs to be manually started through **System Management** > **EPM Manager** to apply the new identity certificate on the MPP.

   b. Review the identity certificate text that is displayed to ensure it is the correct certificate to install for the MPP server.
   c. Click **Save** to install the identity certificate on the MPP.

Next steps

If you have not completed the Pre-requisites for importing custom identity certificates on page 578 , do the following to re-establish the link between the Primary EPM and the MPP:

1. Log on to the EPM web interface by using an account with the Administration user role.
2. On the EPM main menu, click **System Configuration** > **MPP Servers**.
3. Click the name of the MPP server.
4. On the Change MPP Server page, navigate to the **MPP Certificate** section, and select the **Trust new certificate** check box.
5. Click **Save**.

Uploading a Single server identity certificate

About this task

Use this procedure to upload an identity certificate for the Primary EPM and coresident MPP through the Experience Portal web admin interface without re-installing the Experience Portal software. The identity certificate for the Primary EPM and coresident MPP is issued by an external Certificate Authority.

Before you begin

- Ensure that the Single EP server is not processing any multi-channel messages such as Emails, SMS, or HTML.
- Ensure that the MPP is not processing any traffic.
- If a managed application is installed, you might need to perform additional steps before and after the identity certificate is updated. For more information, see the documentation of the managed application.
- Ensure that you complete the Pre-requisites for importing custom identity certificates on page 578.
- Ensure that the Primary EPM is in the Running state.
- Ensure that the MPP server is in either the Stopped or Running state.

Important:

- The uploaded certificate file must be in PKCS#12 format. This includes an identity certificate, CA public certificates and the corresponding private key. This certificate is encrypted and requires a password. The password is chosen during the creation of the PKCS#12 file by the designated CA.
- If **Extended Key Usage** is specified in the X509.V3 certificate extension, specify `Server Authentication` which is also called serverAuth, and `Client Authentication` which is also called clientAuth, for the usage.
- The certificate must have a valid Common Name that represents the EP server host name.
- If the Subject Alternate Name is specified in the X509 V3 certificate extension, the certificate must contain valid DNS and IP Address entries that are associated with the EP server host name.

Procedure

1. Log on to the EPM web interface.
2. Click **Security** > **Certificates**.
3. Click the **EPM Identity Certificates** tab.
4. On the **EPM Identity Certificates** tab, click **Upload**.
5. On the Upload Identity Certificate page, do the following:
   a. In the **Server Name** field, click the name of the Primary EPM server.
   b. In the **Security Certificate File** field, click **Choose File** and choose the PKCS#12 formatted security file for the Primary EPM server.
   c. In the **Password** field, enter the password of the chosen PKCS#12 formatted security file.
   d. Click **Continue**.
6. On the Save Identity Certificate page, do the following:
   a. Review the warning that the Primary EPM services will be automatically restarted to install the identity certificate.

      Note:

      The coresident MPP services will also automatically be restarted if the MPP is in the Running state.

      If the coresident MPP is in the Stopped state before this procedure, it will remain in the Stopped state after the new identity certificate is installed. The MPP will need to be manually started through **System Management** > **MPP Manager** to apply the new identity certificate on the MPP.

   b. Review the identity certificate text that is displayed to ensure it is the correct certificate to install for the Primary EPM server and the coresident MPP.
   c. Click **Save** to install the identity certificate on the Primary EPM and coresident MPP.

      Note:

      The Primary EPM services will automatically restart. Therefore, the Experience Portal web admin site may not render pages correctly until the restart is completed. The user will then be asked to login again.

Next steps

If you have not completed the Pre-requisites for importing custom identity certificates on page 578 , do the following to accept the new certificate on the MPP:

1. Log in to the console as a `root` user.
2. Navigate to the `$AVAYA_HOME/Support/VP-Tools` directory.
3. Run the **`./setup_vpms.php <Primary EPM>`** command, where <Primary EPM> is the IP address or hostname of the Primary EPM.

4. Type `Y`, and press `Enter` to accept the new certificate.

   For NTP service, type `Y`, and press `Enter` to use the Primary EPM.

Upload Identity Certificate page field descriptions

Name	Description
Server name	Lists all the Experience Portal servers (EPM and MPP) that are configured. Select the Experience Portal server from the drop-down list to upload a new identity certificate. The default value is None.
Security Certifcate File	The file name of the encrypted PKCS#12 formatted security file that contains the identity certificate, private key, and the CA chain to upload. Click **Choose File** to open the **File Upload** dialog box and select a security file. After you click **Continue**, this path cannot be changed.
Password	The password of the encrypted PKCS#12 security file. This field is mandatory. The password for the file is set during the creation of the PKCS#12 file.
Continue	Submits the security certificate file to Avaya Experience Portal for verification and validation. On successful validation, Avaya Experience Portal displays the Save Identity Certificate page.
Cancel	Cancels the upload operation and navigates back to the **Security** > **Certificates** page.

Save Identity Certificate page field descriptions

Name	Description
Server Name	The name of the selected Experience Portal server (EPM or MPP) that the new identity certificate is installed on.
Certificate Text	Displays the uploaded identity certificate text for review before installation. After you click **Save**, the identity certificate and its corresponding private key is installed on the selected Experience Portal server.

Table continues…

Name	Description
Save	Installs the identity certificate, corresponding private key, and the CA chain on the selected Experience Portal server. The identity certificate and its corresponding private key is now used in the setup of secure communications by the Experience Portal server.
Cancel	Cancels the upload operation and navigates back to the **Security** > **Certificates** page. If you click **Cancel**, the identity certificate is not installed on the selected Experience Portal server.

Custom Identity Certificate Expiration

When the identity certificate of the Experience Portal server is nearing it's expiration date, alarms are generated to notify the administrators that the identity certificate need to be replaced.

If a custom identity certificate for an Experience Portal server (EPM or MPP) does expire, the Experience Portal server will transition into one of the following states:

- Not Responding: If the EP server is the Auxiliary EPM or MPP
- Partially Running: If the EP server is the Primary EPM

The Experience Portal server will not be operational and secure communications cannot be established until a valid identity certificate is installed.

Secure communications need to be re-established on the Experience Portal server before a new custom identity certificate can be uploaded through the Experience Portal web admin interface. To do this, a temporary self-signed identity certificate must be generated on the EP server.

Generating a self-signed identity certificate

About this task

Use this procedure to generate a temporary self-signed identity certificate on the Experience Portal server.

Procedure

1. Log on to Linux on the Experience Portal server in one of the following ways:
   - Root user: Log on to the local Linux console as a root user if you are an Avaya Services representative, and use Avaya Enterprise Linux, or if the Avaya Service accounts are installed on this server.
   - Non-root user: Log on remotely as a non-root user, then enter the `su - root` command to change the user to root.
2. Navigate to `$AVAYA_HOME/Support/Security-Tools directory`.
3. Enter the **`bash SetupServerCertificate.sh -generate`** command.

A new self-signed identity certificate is generated for the Experience Portal server.

The system displays a message indicating that the services will be restarted and asks if you want to proceed.

Note:

If any service is not configured on the server while the script is running, the script will not restart these services after a new certificate is installed.

4. Enter **Y** to proceed.

   A new self-signed identity certificate is generated.

   The system displays a message asking if you would like to install the certificate.

5. Enter **Y** to proceed.

   The Experience Portal server services will restart.

Trusting the self-signed identity certificate for the Primary EPM server on the Auxiliary EPM and MPP servers

About this task

If the identity certificate has expired on the Primary EPM and a temporary self-signed identity certificate was generated, you need to authenticate the temporary self-signed certificate for the Primary EPM.

Use this procedure to trust the new temporary self-signed certificate for the Primary EPM on each of the Auxiliary EPM and MPP servers.

Procedure

1. On each auxiliary EPM and MPP, log in to the console as a root user.
2. Navigate to the `$AVAYA_HOME/Support/VP-Tools` directory.
3. Run the **`./setup_vpms.php <Primary EPM>`** command.

   Where, <Primary EPM> is the IP address or hostname of the Primary EPM.

4. Type **Y**, and press **Enter** to accept the new certificate.

Trusting the self-signed identity certificate for the Auxiliary EPM server

About this task

If the identity certificate has expired on the Auxiliary EPM and a temporary self-signed identity certificate was generated, you need to authenticate the temporary self-signed certificate for the Auxiliary EPM.

Use this procedure to trust the new temporary self-signed certificate for the Auxiliary EPM.

Procedure

1. Login to the EPM web interface by using an account with the Administration user role.
2. Browse to **System Configuration** > **EPM Servers**.

3. Click the name of the Auxiliary EPM server.
4. On the Change EPM Server page, in the **Auxiliary EPM Certificate** section, review the downloaded identity certificate and select the **Trust new certificate** checkbox.
5. Click **Save**.

Trusting the self-signed identity certificate for the MPP server

About this task

If the identity certificate has expired on the MPP and a temporary self-signed identity certificate was generated, you need to authenticate the temporary self-signed certificate for the MPP.

Use this procedure to trust the new temporary self-signed certificate for the MPP server.

Procedure

1. Login to the EPM web interface by using an account with the Administration user role.
2. Browse to **System Configuration** > **MPP Servers**.
3. Click the name of the MPP server.
4. On the Change MPP Server page, in the **MPP Certificate** section, review the downloaded identity certificate and select the **Trust new certificate** checkbox.
5. Click **Save**.

Next steps

After re-establishing secure communications and the Experience Portal server is back to the Running state, you can complete the following standard procedures to install a new custom identity certificate:

- Uploading a Primary EPM server identity certificate on page 579
- Uploading an Auxiliary EPM server identity certificate on page 581
- Uploading an MPP server identity certificate on page 582
- Uploading a Single server identity certificate on page 584

Trusted Certificates

Trusted Certificates tab on the Certificates page field descriptions

Use this tab to view the trusted certificates that are installed on Experience Portal. You can also import or upload new certificates from this page.

Column or Button	Description
Selection check box	Indicates the certificates you want to delete.
Name	The name of the certificate.
Type	The options are: • Application • CRL File • LDAP Server • SIP Connection • Speech Server • Platform • User • System Manager
Certificate	The text of the certificate.
Import	Opens the **Import Trusted Certificate** page. **Note:** This option is disabled if FIPS is enabled for the system.
Upload	Opens the **Upload Trusted Certificate** page.
Delete	Deletes the selected security certificates. **Note:** You cannot delete a User type of certificate if it is currently assigned to an Experience Portal web user.

Upload Trusted Certificate page field descriptions

Use the two Upload Trusted Certificate pages to upload a certificate for:

- Application server: These certificates allow Avaya Experience Portal to use a secure connection between the MPPs and the application server.
- LDAP server: These certificates allow Avaya Experience Portal to use a secure connection between the Primary EPM server and the LDAP server.
- SIP Connection: These certificates allow a secure connection between Avaya Experience Portal and the VoIP servers.
- Speech server: These certificates are used by the MPP for communicating with the speech servers when using MRCP V2 TLS protocol.
- User: These certificates are used by the EPM to perform certificate based authentication for the web users.
- System Manager: These certificates allow the EPM to Single Sign-On with the System Manager.

- Platform: These trusted certificates are used to setup a trust relationship between the Experience Portal servers for secure communication when externally signed identity certificates are in use.
- CRL File: This trusted certificate type is a Certificate Revocation List (CRL) which will be checked against certificates in Experience Portal for any revoked certificates.

Upload Trusted Certificate page (page 1 of 2)

Field	Description
Name	The name of this certificate on the Avaya Experience Portal system. Once you click **Continue**, this name cannot be changed.
Type	The options are: • Application • CRL File • LDAP Server • SIP Connection • Speech Server • Platform • User • System Manager
Security Certificate File	The file name of the security certificate. Experience Portal supports certificate files in PKCS#12 format. Once you click **Continue**, this path cannot be changed. **Important:** If you select Speech server in the **Type** field, please ensure: • The MRCP v2/TLS connection requires certificates and only the Nuance speech server supports this connection. So you need to add details in this field only for the Nuance speech server. • The Nuance certificate must be formatted as a .pem file. The following 4 certificates must reside in a certificate folder in Nuance speech server; domain_cert_localdomain.pem and _cert.pem, domain_key_localdomain.pem and _key.pem files. • Select only the _cert.pem certificate. If you select User in the **Type** field, please ensure: • To include a whole chain of certificates. • Ensure the Client Authentication (clientAuth) is specified if the Extneded Key Usage is included in the X509 V3 extension of the certificate. Click the **Browse** field if you want to select the certificate file from the **Choose File to Upload** dialog box.

Table continues…

Field	Description
Continue	Submits the location to Avaya Experience Portal for verification. Avaya Experience Portal downloads the SSL (Secure Sockets Layer) certificate from the designated location. If the SSL certificate fails to download, Avaya Experience Portal prompts you to correct the **Location** field entry and try again. When the SSL certificate downloads successfully, Avaya Experience Portal displays the second Upload Trusted Certificate page.

Upload Trusted Certificate page (page 2 of 2)

The fields on this page are presented for confirmation purposes only. If you want to make any changes, you need to cancel this submission and repeat the process from the beginning.

Field	Description
Name	The name of this certificate on the Avaya Experience Portal system.
Display text box	The text of the security certificate.
Save	Installs the displayed certificate on the EPM.

Installing trusted certificate for TLS authentication with Avaya Aura® Session Manager

About this task

Configure the Avaya Aura® Session Manager and Experience Portal to communicate over TLS.

Before you begin

To configure TLS as the Proxy Transport for SIP signaling between Experience Portal, Avaya Aura® Session Manager , and Communication Manager, the following certificate management steps are required:

- The CA certificate that signed the Experience Portal server’s identity certificate must be imported as a trusted certificate on Avaya Session Manager.
  - If the Experience Portal servers are using default identity certificates, then the EP Signing Certificate (Root) must be installed as a trusted certificate on Avaya Session Manager.
  - If the Experience Portal servers are using externally signed identity certificates, then the trusted certificate of the CA that signed the Experience Portal server’s identity certificate must be installed as a trusted certificate on Avaya Session Manager.
- The CA certificate that signed the Avaya Session Manager’s identity certificate must imported as a trusted certificate on Experience Portal.

The identity and trusted certificates establish a mutually authenticated secure connection with Avaya Session Manager.

Procedure

1. If using Default identity certificates, do the following:
   a. Log on to the EPM web interface.
   b. On the EPM navigation pane, click **Security** > **Certificates**.
   c. On the **EP Signing Certificate** tab, click **Export** and follow the prompts accordingly.
   d. Log on to System Manager and add the Experience Portal trusted certificate to Avaya Session Manager.

      For information on how to add trusted certificates, see Administering Avaya Aura® Session Manager on http://support.avaya.com.
2. If using Externally signed identity certificates, do the following:
   a. Acquire the public certificates of the external CA that signed the Experience Portal server's identity certificate.
   b. Log on to System Manager and add the certificates as trusted certificates to Avaya Session Manager.

Next steps

1. Import the public certificate of the CA that signed the Avaya Session Manager's identity certificate as a *SIP Connection type* Trusted Certificate on Experience Portal. This is done through the Experience Portal web interface on the **Security** > **Certificates** > **Trusted Certificates** page.
2. Log on to the System Manager console and configure the ASM Entity Link for TLS on port 5061.
3. Log on to EPM, configure a SIP connection for TLS on port 5061, and restart the MPP.

Chapter 22: Security

Enabling password protection for Single User Mode on Avaya Enterprise Linux

About this task

Booting the Avaya Enterprise Linux system in a Single User Mode without password protected is a security risk. Use this procedure to enable password protection for a Single User Mode logon to the Avaya Enterprise Linux system for security reasons.

Note:

By default, the system does not ask for a password of a root user trying to log on in a Single User Mode in the Avaya Enterprise Linux system.

Procedure

1. To enable password requirement in the `/etc/sysconfig/init` file:
   a. Log on using a secure shell session (SSH) to the Avaya Enterprise Linux system as a user with root privileges.
   b. Open the `/etc/sysconfig/init` file and replace `SINGLE=/sbin/subshell` with `SINGLE=/sbin/sulogin`.
2. To set password for the root user to enable password protection for the Single User Mode:

   By default, the `root` user is disabled from logging into the Avaya Enterprise Linux for security reasons.
   a. Using a secure shell session (SSH), log on to the Avaya Enterprise Linux system as a user with root privileges.
   b. On the command prompt, enter `passwd root`.
   c. In New password, type the new password and press **Enter**.
   d. In Retype new password, reenter the new password and press **Enter**.
3. To boot the Avaya Enterprise Linux system in a Single User Mode:
   a. Log on to the Avaya Enterprise Linux system using a secure shell session (SSH) .
   b. On the command line, enter `init 1` to boot the system in a Single User Mode.
   c. Enter the root password when the system asks for a **root password**.

Disabling MPP core files

About this task

The core dump files on the MPP server can contain sensitive data. You can disable the generation of core files to prevent logging of sensitive data. However, if you disable the core files, you cannot troubleshoot MPP failures when processes terminate unexpectedly.

Procedure

1. Log on to Linux on the Experience Portal MPP server.
2. Navigate to the `MPP config` directory by entering the `cd $AVAYA_MPP_HOME/config` command.

   AVAYA_MPP_HOME is the environment variable pointing to the name of the MPP installation directory specified during the Experience Portal software installation.
3. Edit the `mpp` file and make the following changes:

   `Change ULIMIT_COREFILE="unlimited" to ULIMIT_COREFILE="0"`
4. Repeat this procedure on each MPP server.

Enabling legacy TLS protocols

From Experience Portal 7.2, all servers are updated to use TLS 1.2 to maximize system security. If servers external to the EPMs and MPPs cannot be updated to use TLS 1.2, then during the transition period, the TLS 1.0 and TLS 1.1 protocols can be manually enabled on the Experience Portal servers. The script used to enable these legacy TLS protocols is `$AVAYA_HOME/Support/Security-Tools/ConfigureLegacyTLS.sh`.

It is highly recommended that once the external servers are updated to use TLS 1.2, the TLS 1.0 and TLS 1.1 protocols should be disabled on all the Experience Portal servers.

The following commands are run using the ConfigureLegacyTLS.sh script:

- **`bash ConfigureLegacyTLS.sh disable`** command: To disable legacy TLS 1.0 and TLS 1.1 protocols in httpd configuration, providing greater security
- **`bash ConfigureLegacyTLS.sh enable`** command: To enable legacy TLS 1.0 and 1.1 protocols in httpd configuration, lowering system security but providing backward compatibility with systems requiring these legacy TLS protocols.
- **`bash ConfigureLegacyTLS.sh status`** command: To display the current status of the legacy TLS protocols in httpd configuration.

A reinstallation or upgrade of Experience Portal may automatically disable these legacy TLS protocols. If backward compatibility needs to be retained across upgrades, the ConfigureLegacyTLS.sh script needs to be rerun to enable legacy TLS protocols after each Experience Portal upgrade.

To maximize security, it is suggested that these legacy TLS protocols remain disabled if possible.

Note:

Running either the enable or disable commands will automatically reload the Apache (httpd) daemon if it is running.

Server Identity Validation

Server Identity Validation is a security feature in Experience Portal. During a normal TLS handshake between the client and server, the TLS client verifies the validity, trusted CA, and valid signature of the server certificate. Optionally the TLS client performs an additional security check which is to authenticate the server's identity against the server certificate during the TLS handshake. The TLS client authenticates the server by verifying that the server is located at the same network address specified by the domain name and/or IP address in the server certificate.

When Server Identity Validation is enabled, all the components of Experience Portal that act as a TLS client will verify the identity of the remote server that it is establishing a connection with, is asserted by the server's identity certificate presented during the TLS handshake. TLS clients verify that the certificate asserts an identity in the certificate's Subject Common Name and/or Subject Alternate Name that matches the FQDN of the established connection. If it does not match, the connection is dropped.

The following table lists the Experience Portal components that establish secure connections and performs additional security check if Server Identify Validation is enabled:

Client	Server	Capability
Primary EPM	LDAP server	LDAP Settings web page LDAP User authentication
Primary EPM	System Manager	System Manager Settings web page System Manager Single Sign-On authentication
Primary EPM and Auxiliary EPM	Email Server	Email TLS Connections (SMTP, IMAP4 & POP3)
Primary EPM and Auxiliary EPM	SMS SMPP Gateway	SMPPS Connections
Primary EPM and Auxiliary EPM	SMS HTTP Server	HTTPS Connections
Primary EPM and Auxiliary EPM	Application Server	HTTPS Connections
Primary EPM	Auxiliary EPM	HTTPS Connections
Primary EPM	MPP	HTTPS Connections
MPP	Speech Server	MRCP V2 Connections
MPP	Application Server	HTTPS Connections
MPP	Session Manager	SIP TLS Connections

Best practices for Server Identity Validation

Enable Server Identity Validation

To avoid man-in-the-middle (MITM) attack, it is strongly recommended to enable Server Identity Validation when Experience Portal components use TLS connections to connect to external servers.

Note:

Server Identity Validation is a global setting which applies to the entire Experience Portal system. It is a good approach to disable Server Identity Validation temporarily to avoid interruption of services if some external servers are still sending valid certificates lacking valid Common Name or Subject Alternate Name. Then contact external server vendors for correction of its certificates.

External server's identity certificate requirement

For Experience Portal to successfully validate an external server's identity, the identity certificates of the external servers must have the following attributes:

- Valid Subject Common Name that represents the external server fully qualified hostname.
- The X509 V3 Subject Alternate Name (SAN) extension should include valid DNS and IP Address entries associated with the external server domain name and actual IP address.

  Note:

  - For Speech server, SIP Proxy server, and Application server, the SAN extension with both valid DNS and IP Address entries are required to pass the Server Identity Validation.
  - The DNS entry in the Subject Alternate Name extension can contain the wildcard * (asterisk) character which can match any single domain name component or component fragment. For example, *.avaya.com matches ep.avaya.com, but it does not match bar.ep.avaya.com. e*.com matches ep.com but it does not match bar.com
  - Wildcard in DNS entry is not valid for SIP server.

Basic troubleshooting for Server Identity Validation

The following steps provide some troubleshooting guidelines to help identify TLS connection failures between only EP servers or between EP servers and external servers when Server Identity Validation is enabled:

- Disable the Server Identity Validation setting and check if the TLS connections with external servers are working.
- Examine the EPM/MPP event logs, alarms, and EPM/MPP debug logs to check if the issue might be caused by the server identity validation failure
- If you see the following error message when trying to add an MPP, Auxiliary EPM, or LDAP server connection:

```
Cannot verify identity of server(< hostname>) as there is no valid
DNS Name in the SubjectAltNames nor matching Common Name of the
server certificate
```

It means the server identity certificate did not pass the server identity validation check. That is the Common Name of the certificate is not valid and there is no valid DNS name in the SubjectAltNames extension of the certificate.

- Use the openssl command **`openssl s_client -showcerts -connect <server hostname>:<port>`** to connect to the server to receive and examine the server certificate.
- Monitor the traffic between the Experience Portal system and the external server. For example, use tcpdump and examine the server certificate sent by the server during the TLS handshake.

Enabling Server Identity Validation

Procedure

1. Click **Security** > **Certificates** > **Security Settings**.
2. In the **Enable Server Identity Validation** field, select **Yes**.

Disabling Server Identity Validation

Procedure

1. Click **Security** > **Certificates** > **Security Settings**.
2. In the **Enable Server Identity Validation** field, select **No**.

Security Settings page field descriptions

Use this page to configure the security settings for the Experience Portal system. For more information, see Server Identity Validation on page 596

Name	Description
Enable Server Identity Validation	The option to enable or disable Server Identity Validation. The options are: • **Yes**: Enable Server Identity Validation. • **No**: Disable Server Identity Validation. If you enable Server Identity Validation, see Server Identity Validation on page 596 for details on which Experience Portal components will perform Server Identity Validation. The default setting for Server Identity Validation is: • Enabled: For freshly installed systems. • Disabled : For upgraded systems. This is to avoid service disruption of existing deployed systems. **Note:** Server Identity Validation is a global setting.
Certificate Expiration Threshold (days)	The number of days before a certificate is set to expire. The system generates a daily alarm notification for the number of days that you set here. Enter an integer between 30 and 120. The default is 60. **Note:** Certificate Expiration Threshold is a global setting.
Save	The option to save the changes made.
Apply	The option to apply the changes.
Cancel	The option to cancel the changes made. If you click **Cancel**, you will navigate to the Certificates page.

View Security Settings page field descriptions

Name	Description
Enable Server Identity Validation	To view whether the Experience Portal system has enabled Server Identity Validation. The options are: • **Yes**: Server Identity Validation is enabled. • **No**: Server Identity Validation is disabled. The default setting for Server Identity Validation is: • Enabled: For freshly installed systems. • Disabled: For upgraded systems. This is to avoid service disruption of existing deployed systems. **Note:** Server Identity Validation is a global setting.
Certificate Expiration Threshold (days)	The number of days before a certificate is set to expire. The system generates a daily alarm notification for the set number of days. Enter an integer between 30 and 120. The default is 60. **Note:** Certificate Expiration Threshold is a global setting.

Server Name Indication

Best practices for Server Name Indication

To turn on Server Name Indication on the Avaya Voice browser or the Avaya CCXML browser, the application server side needs to support the extension of Server Name Indication on Transport Layer Security.

Basic troubleshooting for Server Name Indication

The following step provides a troubleshooting guideline to help identify if the Server Name Indication of the TLS connection failure happened between the Avaya Voice browser or CCXML browser and external application servers:

- Use the openssl command **`openssl s_client -connect <server ip address>:<port> -servername <server name>`** to connect to the server to receive and examine the server certificate.

Configuring AIDE

Advanced Intrusion Detection Environment

Advanced Intrusion Detection Environment (AIDE) is a file integrity checker and intrusion detection program. AIDE can be run for checking the integrity of files to ensure the critical files have not been changed in an unauthorized manner. AIDE does this by creating a baseline database of files on an initial run, and then checks this database against the system on subsequent runs.

In Avaya Experience Portal Avaya Enterprise Linux, the AIDE package is installed in `/usr/sbin/aide`. Only a Linux user with root privilege can run AIDE.

The following is the AIDE installed package information:

```
Name        : aide
Version     : 0.14
Release     : 8.el6
Install Date: Tue 12 Jul 2016 06:38:29 AM PDT
Group       : Applications/System
Size        : 303714
Signature   : RSA/8, Mon 22 Feb 2016 12:33:43 AM PST
Relocations: (not relocatable)
Vendor: Red Hat, Inc.
Build Date: Mon 18 Jan 2016 05:12:26 AM PST
Build Host: x86-031.build.eng.bos.redhat.com
Source RPM: aide-0.14-8.el6.src.rpm
License: GPLv2+
Key ID 199e2f91fd431d51
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
URL         : http://sourceforge.net/projects/aide
Summary     : Intrusion detection environment
Description: AIDE (Advanced Intrusion Detection Environment) is a file
integrity checker and intrusion detection program.
```

Note:

This section provides a high level description of the AIDE package. It is not intended to describe the details of the scanning and reporting rules, or to dictate what files or directories and monitoring schedule to run against the AIDE tool, or to describe procedures, for example, how to setup a cron job to run the AIDE.

It is strongly recommended to review the default AIDE configuration file and make any necessary customized changes to correctly match the customer server environment before running the AIDE tool.

Using AIDE

Typically a system administrator will create an initial AIDE database on a system after Avaya Experience Portal is installed. The administrator then sets up a cron job to reproduce a daily or weekly report depending on the system needs. The first AIDE database is a snapshot of the system in its normal state by which all subsequent updates and changes will be measured. This notifies you within, at most, 24 hours of when any file was changed, added, or removed. It also helps establishing an audit trail in the event your site is compromised.

For security reasons, it is a good practice to store the AIDE configuration file on a read-only removable media instead of the default location. If the system is comprised, intruders can not just read the AIDE configuration file and look for directories that are skipped for AIDE monitoring, but also can alter the URL of the output database in order to trick subsequent AIDE scans. For similar reasons, it may also be a good practice to store the AIDE's output database on the read/write removable media, then subsequently copy the new database to a read-only media.

Default AIDE configuration file

`/etc/aide.conf` is the default configuration file installed by the AIDE package.

`/etc/aide.conf` does the following:

- Controls the default scanning and reporting rules.
- Contains the run time configuration AIDE uses to initialize or check the AIDE database.
- Determines whether and how AIDE should report a file or directory as having changed, and which attributes AIDE should consider when scanning.

Checklist for running AIDE

The following steps describe how to run AIDE:

No.	Task	Description	Notes	✔

1	Initialize the AIDE Database.	The value of **database_out** as defined in the AIDE configuration file specifies the URL to which the new database is written.
		`@@define DBDIR /var/lib/aide`
		`database_out=file:@@{DBDIR}/aide.db.new.gz`
		Run the **aide --init** command to create a new AIDE database called `aide.db.new.gz` for all the directories defined in aide.conf under the `/var/lib/aide` directory.
		Example:
		`# aide --config /etc/aide.conf --init`
		`AIDE, version 0.14`
		`### AIDE database at /var/lib/aide/aide.db.new.gz initialized.`		

2	Check the system against baseline database.	The value of **database** as defined in the AIDE configuration file specifies the URL from which the database is read while running the **aide --check** command to check for inconsistencies. Run the **cp /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz** command to copy the baseline database to the file that is specified in the AIDE configuration file. When you run AIDE with **--check** option, it will check the system against the baseline database.		
3	Update the baseline database.	In some cases, the monitored files may have to be updated for legal reasons. For example, Avaya Experience Portal system upgrade or patch install. When you run AIDE with the **--update** option, it will run a scan and update the database non-interactively. AIDE saves the new database at the URL (database_out) specified in the configuration.		

Table continues…

No.	Task	Description	Notes	✔

4	View the output report	The value of **report_url** as defined in the AIDE configuration file specifies the URL to which the AIDE output is written. Though there can be multiple instances of this parameter, output is written to all of them. However, the default is stdout.
		The following shows the default **report_url** value as defined in the AIDE configuration file.
		`@@define LOGDIR /var/log/aide`
		`report_url=file:@@{LOGDIR}/aide.log`
		`report_url=stdout`
		When you run the AIDE tool, the output report is shown on the screen as well as the debug log located at `/var/log/aide/aide.log`.		

Avaya Experience Portal files or directories recommended to monitor

The following are the files or directories that are recommended to be monitored:

Primary EPM and Auxiliary EPM Servers

`/etc/httpd/conf`

`/etc/httpd/conf.d`

`/etc/pki/tls/private`

`/etc/pki/tls/cert`

`/var/lib/pgsql/data/postgresql.conf`

`/var/lib/pgsql/data/postmaster.opts`

`/opt/Tomcat/tomcat/bin`

`/opt/Tomcat/tomcat/common`

`/opt/Tomcat/tomcat/conf`

`/opt/Tomcat/tomcat/lib`

`/opt/Tomcat/tomcat/shared`

`/opt/Tomcat/tomcat/webapps`

`/opt/MMSServer/tomcat/bin`

`/opt/MMSServer/tomcat/conf`

`/opt/MMSServer/tomcat/lib`

`/opt/MMSServer/tomcat/webapps`

`/opt/Avaya/ExperiencePortal/Support`

```
/opt/Avaya/ExperiencePortal/Documentation
/opt/Avaya/ExperiencePortal/_uninst
/opt/Avaya/ExperiencePortal/VPMS/web/ssl.crt
/opt/Avaya/ExperiencePortal/VPMS/CompMgrService/bin
/opt/Avaya/ExperiencePortal/VPMS/CompMgrService/include
/opt/Avaya/ExperiencePortal/VPMS/CompMgrService/scripts/webservices/
CompMgrWS
/opt/Avaya/ExperiencePortal/VPMS/webservices/CompMgrWS
/opt/Avaya/ExperiencePortal/pki/
```

MPP Servers

```
/etc/httpd/conf
/etc/httpd/conf.d
/etc/pki/tls/private
/etc/pki/tls/cert
/opt/Avaya/ExperiencePortal/Support
/opt/Avaya/ExperiencePortal/MPP/bin
/opt/Avaya/ExperiencePortal/MPP/bin/tools
/opt/Avaya/ExperiencePortal/MPP/config/web/ssl.crt
/opt/Avaya/ExperiencePortal/pki/
```

Avaya Experience Portal files or directories recommended to be excluded from monitoring

It is not recommended to monitor files or directories that are changing frequently. For example, debug log files, mail spools, process file systems, user's home directories, or temporary directories. Adding `!` to a file or directory name in the AIDE configuration file will prevent AIDE from monitoring those specific files or directories.

The following are the files or directories that are recommended to be excluded from monitoring:

Primary EPM and Auxiliary EPM Servers

```
/var/log
/var/lib/pgsql/pgstartup.log
/var/lib/pgsql/data
/opt/Tomcat/tomcat $CATALINA_HOME/logs
/opt/Tomcat/tomcat $CATALINA_HOME/temp
/opt/Tomcat/tomcat $CATALINA_HOME/work
/opt/MMSServer/tomcat $MMSSERVER_HOME/logs
```

```
/opt/MMSServer/tomcat $MMSSERVER_HOME/temp
/opt/MMSServer/tomcat $MMSSERVER_HOME/work
/opt/Avaya/ExperiencePortal/logs
/opt/Avaya/ExperiencePortal/VPMS $AVAYA_VPMS_HOME//logs
/opt/Avaya/ExperiencePortal/VPMS $AVAYA_VPMS_HOME/transcriptions
/opt/Avaya/ExperiencePortal/VPMS/CompMgrService/status
/opt/Avaya/ExperiencePortal/VPMS/CompMgrService/tmp
```

MPP servers

```
/var/log
/opt/Avaya/ExperiencePortal/MPP/logs
/opt/Avaya/ExperiencePortal/MPP/tmp
/opt/Avaya/ExperiencePortal/MPP/AVB
/opt/Avaya/ExperiencePortal/MPP/VideoMgr
/opt/Avaya/ExperiencePortal/MPP$AVAYA_MPP_HOME/web/handlers
/opt/Avaya/ExperiencePortal/MPP$AVAYA_MPP_HOME/web/prompts
/opt/Avaya/ExperiencePortal/MPP/web/promptsImpl
```

AIDE manual pages

You can view detailed information for the following:

- aide: For information on the aide tool, type `man aide` on the Linux command line.
- aide.conf: For information on the aide configuration file, type `man aide.conf` on the Linux command line.
- AIDE manual: For the detailed AIDE manual, see http://aide.sourceforge.net/stable/manual.html. You can also view detailed description of the AIDE configuration file.

Sample AIDE run

The following is a sample of the AIDE run:

```
[root@AIDETestPRI aide]# aide -c /etc/aide.conf --check
AIDE found differences between database and filesystem!!
Start timestamp: 2017-01-09 16:05:20
Summary:
  Total number of files:        56561
  Added files:                  1
  Removed files:                0
  Changed files:                30


---------------------------------------------------
Added files:
---------------------------------------------------
added: /bin/test.out

---------------------------------------------------
```

```
Changed files:
---------------------------------------------------

changed: /usr/sbin
changed: /usr/lib
changed: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/lib
changed: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/lib/amd64/jli
changed: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/bin
changed: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib
changed: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib/amd64/jli
changed: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/bin
changed: /usr/lib/nss/unsupported-tools
changed: /usr/lib/cups/filter
changed: /usr/lib64
changed: /usr/lib64/nss/unsupported-tools
changed: /usr/lib64/perl5/CORE
changed: /usr/lib64/sa
changed: /usr/lib64/gettext
changed: /usr/lib64/pm-utils/bin
changed: /usr/lib64/graphviz
changed: /usr/bin
changed: /usr/libexec
changed: /usr/libexec/getconf
changed: /usr/libexec/gcc/x86_64-redhat-linux/4.4.4
changed: /usr/libexec/awk
changed: /usr/libexec/gstreamer-0.10
changed: /usr/libexec/utempter
changed: /lib
changed: /lib/udev
changed: /lib64
changed: /lib64/dbus-1
changed: /bin
changed: /sbin

---------------------------------------------------
Detailed information about changes:
---------------------------------------------------


Directory: /usr/sbin
  Mtime    : 2017-01-09 12:09:33              , 2017-01-09 16:03:32
  Ctime    : 2017-01-09 12:09:33              , 2017-01-09 16:03:32

Directory: /usr/lib
  Mtime    : 2017-01-09 12:09:33              , 2017-01-09 16:03:32
  Ctime    : 2017-01-09 12:09:33              , 2017-01-09 16:03:32

Directory: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/lib
  Mtime    : 2017-01-09 12:09:37              , 2017-01-09 16:03:36
  Ctime    : 2017-01-09 12:09:37              , 2017-01-09 16:03:36

Directory: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/lib/amd64/jli
  Mtime    : 2017-01-09 12:09:37              , 2017-01-09 16:03:37
  Ctime    : 2017-01-09 12:09:37              , 2017-01-09 16:03:37

Directory: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/bin
  Mtime    : 2017-01-09 12:09:38              , 2017-01-09 16:03:37
  Ctime    : 2017-01-09 12:09:38              , 2017-01-09 16:03:37

Directory: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib
  Mtime    : 2017-01-09 12:09:38              , 2017-01-09 16:03:37
  Ctime    : 2017-01-09 12:09:38              , 2017-01-09 16:03:37

Directory: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib/amd64/
jli
```

```
  Mtime    : 2017-01-09 12:09:40              , 2017-01-09 16:03:39
  Ctime    : 2017-01-09 12:09:40              , 2017-01-09 16:03:39

Directory: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/bin
  Mtime    : 2017-01-09 12:09:40              , 2017-01-09 16:03:39
  Ctime    : 2017-01-09 12:09:40              , 2017-01-09 16:03:39

Directory: /usr/lib/nss/unsupported-tools
  Mtime    : 2017-01-09 12:09:40              , 2017-01-09 16:03:39
  Ctime    : 2017-01-09 12:09:40              , 2017-01-09 16:03:39

Directory: /usr/lib/cups/filter
  Mtime    : 2017-01-09 12:09:40              , 2017-01-09 16:03:40
  Ctime    : 2017-01-09 12:09:40              , 2017-01-09 16:03:40

Directory: /usr/lib64
  Mtime    : 2017-01-09 12:10:03              , 2017-01-09 16:04:02
  Ctime    : 2017-01-09 12:10:03              , 2017-01-09 16:04:02

Directory: /usr/lib64/nss/unsupported-tools
  Mtime    : 2017-01-09 12:10:05              , 2017-01-09 16:04:04
  Ctime    : 2017-01-09 12:10:05              , 2017-01-09 16:04:04

Directory: /usr/lib64/perl5/CORE
  Mtime    : 2017-01-09 12:10:06              , 2017-01-09 16:04:04
  Ctime    : 2017-01-09 12:10:06              , 2017-01-09 16:04:04

Directory: /usr/lib64/sa
  Mtime    : 2017-01-09 12:10:06              , 2017-01-09 16:04:04
  Ctime    : 2017-01-09 12:10:06              , 2017-01-09 16:04:04

Directory: /usr/lib64/gettext
  Mtime    : 2017-01-09 12:10:06              , 2017-01-09 16:04:05
  Ctime    : 2017-01-09 12:10:06              , 2017-01-09 16:04:05

Directory: /usr/lib64/pm-utils/bin
  Mtime    : 2017-01-09 12:10:08              , 2017-01-09 16:04:06
  Ctime    : 2017-01-09 12:10:08              , 2017-01-09 16:04:06

Directory: /usr/lib64/graphviz
  Mtime    : 2017-01-09 12:10:08              , 2017-01-09 16:04:06
  Ctime    : 2017-01-09 12:10:08              , 2017-01-09 16:04:06

Directory: /usr/bin
  Mtime    : 2017-01-09 12:10:15              , 2017-01-09 16:04:13
  Ctime    : 2017-01-09 12:10:15              , 2017-01-09 16:04:13

Directory: /usr/libexec
  Mtime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14
  Ctime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14

Directory: /usr/libexec/getconf
  Mtime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14
  Ctime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14

Directory: /usr/libexec/gcc/x86_64-redhat-linux/4.4.4
  Mtime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14
  Ctime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14

Directory: /usr/libexec/awk
  Mtime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14
  Ctime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14

Directory: /usr/libexec/gstreamer-0.10
  Mtime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14
```

```
  Ctime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14

Directory: /usr/libexec/utempter
  Mtime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14
  Ctime    : 2017-01-09 12:10:16              , 2017-01-09 16:04:14

Directory: /lib
  Mtime    : 2017-01-09 12:10:17              , 2017-01-09 16:04:15
  Ctime    : 2017-01-09 12:10:17              , 2017-01-09 16:04:15

Directory: /lib/udev
  Mtime    : 2017-01-09 12:10:19              , 2017-01-09 16:04:17
  Ctime    : 2017-01-09 12:10:19              , 2017-01-09 16:04:17

Directory: /lib64
  Mtime    : 2017-01-09 12:10:22              , 2017-01-09 16:04:20
  Ctime    : 2017-01-09 12:10:22              , 2017-01-09 16:04:20

Directory: /lib64/dbus-1
  Mtime    : 2017-01-09 12:10:22              , 2017-01-09 16:04:20
  Ctime    : 2017-01-09 12:10:22              , 2017-01-09 16:04:20

Directory: /bin
  Mtime    : 2017-01-09 12:10:48              , 2017-01-09 16:05:08
  Ctime    : 2017-01-09 12:10:48              , 2017-01-09 16:05:08

Directory: /sbin
  Mtime    : 2017-01-09 12:10:24              , 2017-01-09 16:04:22
  Ctime    : 2017-01-09 12:10:24              , 2017-01-09 16:04:22
```

FIPS 140–2 mode

The operating system of Avaya Experience Portal is FIPS 140-2 compliant. With this feature, Experience Portal has the ability to enable or disable the use of FIPS 140-2 compliant modules or ciphers.

Enabling FIPS

About this task

Use this procedure to enable FIPS 140–2 mode.

Important:

The following are some limitations that arise when FIPS is enabled:

1. Secure connections between AEP and WebLM cannot be established:

   Avaya Experience Portal in FIPS mode cannot establish secure communications with a remote or local WebLM server using existing WebLM packaged certificates. This is due to the WebLM packaged certificates using SHA-1 1024-bit certificates. FIPS expects certificates to use a FIPS-compliant signature and key algorithms. This issue can only be resolved by replacing the existing WebLM packaged certificates with certificates that use a FIPS-compliant signature and key algorithms.

For more information on how to replace the WebLM certificates, see the *WebLMCertificateConfiguration.pdf* document available on the AEP server at `$AVAYA_HOME/VPMS/Support/WebLM/` or on the Avaya Support site at support.avaya.com.

Note that if you are using the local WebLM server that is installed on the AEP server, you can change the License Server URL to use `http` URL instead of `https` URL.

2. Default identity certificates issued by the EP Signing Certificate are no longer supported:

   You must disable the EP Signing Certificate and install the custom identity certificates on the Experience Portal servers.

For more information, see the following sections:

- Pre-requisites for importing custom identity certificates on page 578
- Uploading Identity Certificates on page 579

Procedure

1. Do the following from a local Linux console as a root user:
   a. Enable FIPS at OS level by running the `fips-mode-setup --enable` command.

      Note:

      Software-only customers using RHEL 7 can follow the procedure that is provided in the Red Hat customer portal for controlling FIPS mode in the operating system. For details, see How can I make RHEL 6/7/8 FIPS 140-2 compliant?

   b. Reboot the system by running the `reboot` command.

      Note:

      Rebooting the system enables FIPS at the JVM level.

2. Re-login and verify if FIPS is active by running the following commands:

   ```
   cat /proc/sys/crypto/fips_enabled
   ```

   ```
   sysctl crypto.fips_enabled
   ```

   If the output for both of the commands is 1, then FIPS is enabled.

   ```
   cat /proc/sys/crypto/fips_enabled
    see: "1"

   sysctl crypto.fips_enabled
    see "crypto.fips_enabled = 1"

   grep "JVM FIPS" $CATALINA_HOME/logs/catalina.out | tail -n 1
   ```

   If FIPS is enabled, `catalina.out` will have the following log:

   ```
   VPServlet::initialize JVM FIPS is enabled
   ```

Disabling FIPS

About this task

Use this procedure to disable FIPS 140–2 mode.

Procedure

1. Do the following from a local Linux console as a root user:
   a. Disable FIPS at the OS level by running the following command:

      fips-mode-setup --disable

      Note:

      Software-only customers using RHEL 7 can follow the procedure that is provided in the Red Hat customer portal for controlling FIPS mode in the operating system. For details, see How can I make RHEL 6/7/8 FIPS 140-2 compliant?

   b. Disable FIPS at the JVM level by running the following command:

      bash /opt/Avaya/ExperiencePortal/Support/Security-Tools/AAEP_FIPS_remove.sh

   c. Reboot the system by running the `reboot` command.
2. Re-login and verify if FIPS is inactive by running the following commands:

   `cat /proc/sys/crypto/fips_enabled`

   `sysctl crypto.fips_enabled`

   If the output for both of the commands is 0, then FIPS is disabled.

```
cat /proc/sys/crypto/fips_enabled
 see: "0"

sysctl crypto.fips_enabled
 see "crypto.fips_enabled = 0"

grep "JVM FIPS" $CATALINA_HOME/logs/catalina.out | tail -n 1
```

   If FIPS is disabled, `catalina.out` will have the following log:

```
VPServlet::initialize JVM FIPS is NOT enabled
```

Chapter 23: Enhanced Access Security Gateway

Enhanced Access Security Gateway (EASG)

EASG provides a secure method for Avaya services personnel to access Avaya Experience Portal both remotely and on-site. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management, and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

The EASG authentication method is based on cryptographic signature verification of responses using the certificates issued by Avaya.

The following are the key points for EASG implementation:

- The old ASG (Avaya Security Gateway) is obsolete. The ASG RPM (asgtools) is removed during the Avaya Experience Portal installation process.
- The Avaya Service Account authentication file is no longer used to control access to services logins.
- Avaya Services Logins supported in Avaya Experience Portal EASG are init, inads, craft, and sroot. EASG does not affect the permissions associated with Avaya Services Logins. For more information, see Avaya Services Logins supported by EASG on page 612.

Note:

The rasaccess account is disabled and not supported.

Avaya Service Logins supported by EASG

User name	Group	Purpose
sroot	root, avayavpgroup	Avaya Services root access
craft	susers, avayavpgroup	Avaya Services non-root access
init	susers	Avaya Services non-root access
inads	susers	Avaya Services non-root access

Table continues…

User name	Group	Purpose
init	Administration, Auditor, User manager, Privacy manager roles	EPM service user account

Avaya Experience Portal product certificate

Avaya Experience Portal installer installs a dedicated Avaya Experience Portal 8.x product certificate at the `/etc/asg/Product.p7b` directory in each server. The product certificate is x509v3 compliant and is derived from Avaya IT Root CA. It uniquely identifies the major releases of Avaya Experience Portal to the Avaya EASG backend server.

Product certificate contents

To view the contents of the product certificate, you must run the `EASGProductCert --certInfo` command.

Example:

```
EASGProductCert --certInfo
Subject: CN=Avaya Experience Portal  8.1, OU=EASG, O=Avaya Inc.
Serial Number: 10001
Expiration: Jul 27 04:00:00 2031 GMT
Trust Chain:
1. O=Avaya, OU=IT, CN=AvayaITrootCA2
2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
4. CN=Product EASG Intermediate CA, OU=EASG, O=Avaya Inc.
5. CN=Avaya Experience Portal  8.1, OU=EASG, O=Avaya Inc.
```

Product certificate update

Every major release requires the generation of a new EASG product certificate. The Avaya Experience Portal 8.x product certificate that is shipped with the 8.x release is the EASG product certificate for all Avaya Experience Portal 8.x releases.

If the product certificate is deleted, modified, or replaced illegally, Avaya can no longer provide remote access support to the customer.

If the Avaya Experience Portal 8.x product certificate is revoked by the Avaya backend server, only a software patch or new software release can replace the revoked certificate.

Product certificate monitoring

The Avaya Experience Portal 8.x EASG product certificate is valid for 15 years. The primary EPM raises major alarms when the product certificate approaches the following expiration days:

- EASG Product certificate expiration pending:
  - 365 days
  - 180 days
  - 30 days
- EASG Product Certificate expired.

EASG Acceptance of Terms

Avaya Experience Portal displays the following EASG Acceptance of Terms during the installation of the primary EPM of Avaya Experience Portal. The message displays only if the user has not configured EASG on the primary EPM or when `EASGConfigure.sh` script is run on any Avaya Experience Portal server.

Enable (recommended)

```
By enabling Avaya Logins you are granting Avaya access to your system. This is
necessary to maximize the performance and value
of your Avaya support entitlements, allowing Avaya to resolve product issues in a
timely manner.
In addition to enabling the Avaya Logins, this product should be registered with Avaya
and technically onboarded for
remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/
registration) for additional
information for registering products and establishing remote access and alarming.
```

Disable

```
By disabling Avaya Logins you are preventing Avaya access to your system. This is not
recommended, as it impacts Avaya's
ability to provide support for the product. Unless the customer is well versed in
managing the product themselves,
Avaya Logins should not be disabled.
```

Important:

The EASG selection you make during the primary EPM installation is applied to other systems within the Experience Portal system including new MPPs and auxiliary EPMs which are subsequently installed.

EASG states

The following are the valid EASG states:

- Enabled EASG: The state that the user selects to enable EASG during the primary EPM installation or run the EASGConfigure.sh script provided by Experience Portal to enable EASG. When EASG is enabled, access to all Avaya Services Logins will be EASG protected.
- Disabled EASG: The state that the user selects to disable EASG during the primary EPM installation or run the EASGConfigure.sh script provided by Experience Portal to disable EASG. When EASG is disabled, it will not be possible to login to the Avaya Experience Portal server with any Avaya Services Login.

Important:

- The user uses the EASGConfigure.sh script to enable or disable EASG after installing Experience Portal.
- Users with root privileges or users who belong to the susers group can run the EASGConfigure.sh script to enable or disable EASG.

Note:

The primary EPM software installation will always display the Acceptance of Terms prompt to enable or disable EASG, if EASG is not installed. The auxiliary EPM and MPP software installation will query the primary EPM EASG state and set the same EASG state, if EASG is not installed.

Enabling EASG

About this task

Use the EASGConfigure.sh script to enable EASG on an Avaya Experience Portal server. After EASG is enabled, the Avaya Services Logins accounts are EASG protected. Use the challenge-response authentication to log in to the Avaya Experience Portal server.

Note:

- Using EASGConfigure.sh script to enable EASG on an Avaya Experience Portal server does not enable EASG on other existing servers in the Avaya Experience Portal system. To enable EASG on other servers, run the script on each server.
- Users with root privileges or users who belong to the susers group can run the EASGConfigure.sh to enable EASG.

Before you begin

- Ensure that the server has a non-Avaya service account with root privilege or a user that belongs to the susers group to run the EASGConfigure.sh script.
- You cannot log in to the Experience Portal server with an Avaya Services Login account if the current state of the server is disabled.

Procedure

1. Log on to the Avaya Experience Portal Linux server locally as a user with root privilege or as a user who belongs to the susers group. Or, log in remotely as a non-root user and then change the user to a user with root privileges or a user that belongs to the susers group by entering the **`su -`** command.
2. Navigate to the `$AVAYA_HOME/Support/Security-Tools/EASG` directory where the script is located.
3. Run the **`bash EASGConfigure.sh --enable`** command. The script displays the Acceptance of terms prompt for enabling EASG.

   Example:

```
bash EASGConfigure.sh --enable
Invocation at Tue Apr 25 16:35:50 PDT 2017
LOG FILE: /opt/Avaya/ExperiencePortal/logs/EASGConfigure/
EASGConfigure.sh.2017-04-25.log
Enhanced Access Security Gateway (EASG)
EASG is disabled
By enabling Avaya Services Logins you are granting Avaya access to your system.
This is required to maximize the performance and
 value of your Avaya support entitlements, allowing Avaya to resolve product
```

```
issues in a timely manner. The product must be
registered using the Avaya Global Registration Tool (GRT, see https://
grt.avaya.com) to be eligible for Avaya remote
connectivity. Please see the Avaya support site (https://support.avaya.com/
registration) for additional information for
registering products and establishing remote access and alarming.
Do you want to enable EASG [yes/no]?
```

4. Type one of the following:
   - `yes` to accept the EASG terms.
   - `no` to cancel.
5. Review the output and debug log from the `/opt/Avaya/ExperiencePortal/logs/EASGConfigure` directory to ensure that the script completes successfully.

Disabling EASG

About this task

Use the EASGConfigure.sh script to disable EASG on an Avaya Experience Portal server.

After EASG is disabled:

- Avaya Services Logins accounts will be blocked from logging in to the Avaya Experience Portal server.
- EPM service account init will be blocked from logging in to the primary EPM.

Note:

- Using the EASGConfigure.sh script to disable EASG on an Avaya Experience Portal server does not disable EASG on other existing servers in the Avaya Experience Portal system. To disable EASG on other servers, run the script on each server.
- Users with root privileges or users who belong to the susers group can run the EASGConfigure.sh to disable EASG.

Before you begin

Ensure that the server has a non-Avaya service account with root privilege or a user that belongs to susers group to run the EASGConfigure.sh script.

Procedure

1. Log on to the Avaya Experience Portal Linux server locally as a user with root privileges or as a user who belongs to the susers group. Or, log in remotely as a non-root user and then change the user to a user who belongs to the susers group by entering the **`su -`** command.
2. Navigate to the `$AVAYA_HOME/Support/Security-Tools/EASG` directory where the script is located.
3. Run the **`bash EASGConfigure.sh --disable`** command. The script displays the Acceptance of terms prompt for disabling EASG.

Example:

```
bash EASGConfigure.sh --disable
Invocation at Tue Apr 25 16:39:51 PDT 2017
LOG FILE: /opt/Avaya/ExperiencePortal/logs/EASGConfigure/
EASGConfigure.sh.2017-04-25.log
Enhanced Access Security Gateway (EASG)
EASG is enabled
By disabling Avaya Services Logins you are denying Avaya access to your system.
This is not recommended, as it can impact
Avaya's ability to provide support for the product. Unless the customer is well
versed in managing the product themselves,
Avaya Services Logins should not be disabled.
```

4. Type one of the following:
   - `yes` to accept the EASG terms.
   - `no` to cancel.
5. Review the output and debug log from `/opt/Avaya/ExperiencePortal/logs/EASGConfigure` directory to ensure that the script completes successfully.

Displaying EASG status

About this task

Use the EASGConfigure.sh script to display the current EASG state on an Avaya Experience Portal server. The current EASG state can be either enabled or disabled.

Before you begin

If the current EASG state of the Avaya Experience Portal server is disabled, it will not be possible to log into the Experience Portal server with any Avaya Services Login accounts. Ensure that the server has a non-Avaya service account with root privilege or a user that belongs to the susers group to run the EASGConfigure.sh script.

Procedure

1. Log on to the Avaya Experience Portal Linux server locally as root or as a user who belongs to the susers group. 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 `$AVAYA_HOME/Support/Security-Tools/EASG` directory where the script is located.
3. Run one of the following commands:
   - **`bash EASGConfigure.sh`**
   - **`bash EASGConfigure.sh --status`**

   The script displays the current EASG state.

EASG built-in utilities

Note:

You must always use the Avaya Experience Portal wrapper script EASGConfigure.sh to enable or disable EASG.

EASGProductCert

The EASGProductCert script is available to all users by default. It has two modes of operation:

- The script can print details about the product certificate.
- The script can check for product certificate expiration.

The following is a sample screen shot of the EASGProductCert command line arguments usage:

```
EASGProductCert --lessThanDays <number_of_days>
EASGProductCert --certInfo
Where:
--lessThanDays:
Determines if the certificate will expire within the number of days indicated by
<number_of_days>.  A return code of 1 indicates
 that the EASG Product Certificate will expire within <number_of_days>. A return code
of 0 indicates that the EASG Product
Certificate will not expire in <number_of_days>.  Finally, if an error is encountered,
a return code of 2 is issued.
--certInfo:
Display information about the EASG Product Certificate.
```

The following is a sample screen shot of running EASGProductCert with **`--certInfo`**:

```
EASGProductCert --certInfo
Subject: CN=Avaya Experience Portal  3.1, OU=EASG, O=Avaya Inc.
Serial Number: 10001
Expiration: Jul 27 04:00:00 2031 GMT
Trust Chain:
1. O=Avaya, OU=IT, CN=AvayaITrootCA2
2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
4. CN=Product EASG Intermediate CA, OU=EASG, O=Avaya Inc.
5. CN=Avaya Experience Portal  8.1, OU=EASG, O=Avaya Inc.
```

EASG Status

The EASGStatus script is available to all users by default. It displays the current EASG state as enabled or disabled.

EASGSiteCertManage

The EASGSiteCertManage is restricted to root access or users who belong to the susers group. Users who belong to the susers group can use **`sudo EASGSiteCertManage`** to run the script. The site certificates are primarily used by on-site technicians who do not have access to Avaya network when they are on the customer's premises. The **`EASGSiteCertManage`** command can be run with no options to get documentation about its usage.

EASG Challenge-Response Authentication

EASG challenge generation

When EASG is enabled, an attempt to access the product via an Avaya Service Login will result in providing the following information:

- Challenge String: The new EASG Challenge String is the legacy ASG challenge format with the Product Certificate ID appended at the front. The Product Certificate ID is the serial number of the Avaya Experience Portal product certificate.
- Product ID String: The new Product ID string is a GUID (globally unique identifier) which is generated by the EASG RPM, with the EASG RPM version number appended at the end.

The following is a sample screen shot of the challenge and Product ID when trying to access the system using Avaya service account:

```
Challenge: 10001-85132972
Product ID: 09f2c551f32e4c808b7fd3c544365a8f01
Response:
```

EASG response generation

The Avaya EASG Web Mobile interface has been enhanced to accept all the existing challenge inputs for both ASG and EASG challenges. Avaya EASG Web Mobile then provides this information to the Avaya EASG backend server and displays the appropriate responses to the user.

The new EASG response strings can reach up to a maximum 512 bytes strings. There is a Copy Response to Clipboard button on the Avaya EASG Web Mobile web page which the user can use to copy the response string and paste it to the Linux login shell.

EASG response validation

If an EASG Response is not submitted to the product within 5 minutes of the EASG Challenge String being provided, the challenge shall expire. Any EASG response submitted against an expired challenge fails validation and the login will fail.

If the EASG Response validation succeeds, then the Avaya service account user is allowed access to the system with the permissions associated with the Avaya Service Login name. The Linux system log `/var/log/messages` will record an authentication through the success message of the product certificate.

If the EASG Response validation fails, the user will be denied access to the system and the challenge is depreciated. Any subsequent login attempt needs a new challenge. The Linux system log `/var/log/messages` will record an authentication failed message.

EASG Site Certificate Management

Avaya technicians use the EASG Site Certificate when they do not have access to Avaya network to generate responses. The technicians generate the EASG Site Certificate by using the EASG Site Manager tool. After the technician generates the EASG Site Certificate successfully, the

technician usually sends it to the customer with the instructions on how to install the Site Certificate.

Note:

The EASG Site Manager tool is based on version 7 and later.

Generating a site certificate

About this task

Use this procedure to generate a site certificate on the EASG site manager tool. The EASG site manager tool can issue only a single valid site certificate per technician at a given time. A new site certificate request will overwrite any previously valid site certificate if one exists.

Note:

The EASG site certificate will expire 2 weeks from the date of creation.

Procedure

1. Click the EASG Site Cert tab on the EASG Site Manager tool.
2. Click the **New** button to generate a new EASG Site Certificate.

   Once you generate the site certificate successfully, a message displays at the bottom of EASG Site Manager window. The message shows how long the site certificate is valid and where it is located.

Installing the Site Certificate

About this task

Use this procedure to install the EASG Site Certificate on the Avaya Experience Portal server.

The Linux system log `/var/log/messages` will record a successful Site Certificate installation message.

Procedure

1. Log on to the Avaya Experience Portal Linux server locally as root or a user who belongs to the susers group. Or log in remotely as a non-root user and then change the user to root by entering the **`su -`** command.
2. Upload the site certificate to the Avaya Experience Portal Linux server.
3. Run the EASG built-in tool **`EASGSiteCertManage`** to install the uploaded site certificate.
4. Run the **`(sudo) EASGSiteCertManage --add <filename> --saf <SAF>`** command.

   Where,

   - sudo: If the user who runs this command belongs to the susers group, **`sudo`** needs to be added in front of EASGSiteCertManage. If the user is a root privilege user, there is no need to add **`sudo`**.

- Filename: The location of the Site Certificate.
- SAF: The Site Authentication Factor code which is a 10 to 20 character alphanumeric string. The SAF is required for technician access when the technician later generates a response.

Example:

```
[root@EP72PRI voiceportal]# EASGSiteCertManage --add
/home/voiceportal/test.p7b --saf 1234567890
Site Certificate installed successfully.
```

Displaying the site certificate content

About this task

Use this procedure to display all the installed EASG Site Certificates on the Avaya Experience Portal server and to display the content of an installed EASG Site Certificate.

Procedure

1. Log on to the Avaya Experience Portal Linux server locally as root or a user who belongs to the susers group. Or, log in remotely as a non-root user and then change the user to root by entering the **su -** command.
2. To display a list of installed site certificates, run the **(sudo) EASGSiteCertManage --list** command.

   If the user who runs this command belongs to the susers group, **sudo** needs to be added in front of EASGSiteCertManage. If the user is a root privilege user, there is no need to add **sudo**.

   Example:

   ```
   [root@EASG voiceportal]# EASGSiteCertManage --list
   Valid Site Certificates:
     1. test.p7b
   ```

3. To display the content of a Site Certificate, run the **(sudo) EASGSiteCertManage --show <SiteCertName>** command.

   Where,

   - sudo: If the user who runs this command belongs to the susers group, **sudo** needs to be added in front of EASGSiteCertManage. If the user is a root privilege user, there is no need to add **sudo**.
   - SiteCertName: The name of the Site Certificate

   Example:

   ```
   [root@EASG voiceportal]# EASGSiteCertManage --show test.p7b

   Subject: CN=Avaya Technician test, OU=EASG, O=Avaya Inc.
   User Name: test
   Expiration: Feb 16 00:51:39 2017 GMT
   Trust Chain:
   ```

1. O=Avaya, OU=IT, CN=AvayaITrootCA2
2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
4. CN=Site EASG Intermediate CA, OU=EASG, O=Avaya Inc.
5. CN=Avaya Technician dchen, OU=EASG, O=Avaya Inc.

Deleting a Site Certificate

About this task

The expired EASG Site Certificates are automatically deleted by the Avaya Experience Portal system. Use this procedure to manually delete the installed EASG Site Certificate.

The Linux system log `/var/log/messages` records a Site Certificate deletion message.

Procedure

1. Log on to the Avaya Experience Portal Linux server in one of the following ways:
   - Log in locally as root, or as a user who belongs to the `susers` group.
   - Log in remotely as a non-root user, and then change the user to root by entering the **`su -`** command.
2. Run the **`(sudo) EASGSiteCertManage --delete <SiteCertName>`** command.

   Where,

   - sudo: If the user who runs this command belongs to the susers group, **`sudo`** must be added in front of `EASGSiteCertManage`. If the user is a root privilege user, there is no need to add **`sudo`**
   - SiteCertName: The name of the Site Certificate.

   For example:

   ```
   [root@EASG voiceportal]# EASGSiteCertManage --delete test.p7b
   Successfully removed Site Cert: test.p7b
   ```

Generating a Site Certificate response

About this task

Use this procedure to generate a Site Certificate response on the EASG Site Manager tool.

Procedure

1. Log in to the Avaya Experience Portal system using one of the Avaya Service Logins.

   The login shell displays the Challenge and Product ID.
2. On the EASG Site Manager tool, click the Authenticate tab.
3. Select **EASG (Certificate Based Authentication)** and click **OK**.

   The EASG Authentication window appears.
4. Enter the appropriate information in the fields.

5. Click **Generate Response** to create the response.
6. Click **Copy Response** to copy the response to the computer clipboard.
7. Paste the response into the login shell.

   The login is successful.

   The Linux system log `/var/log/messages` will record an authentication through the site certificate success message.

EASG Authentication field descriptions

Name	Description
Equipment	The Product ID that displays in the login shell when you log in to the Avaya Experience Portal system using one of the Avaya Service Logins.
EquipLogin	The Avaya Service Login accounts (init, inads, craft, or sroot).
SAF PIN	The SAF code that the customer enters when the Site Certificate is installed.
Challenge	The challenge that displays in the login shell when you log in to the Avaya Experience Portal system using one of the Avaya Service Logins.
Response	The response that displays after you generate the response.

Chapter 24: Experience Portal Manager main menu customizations

EPM main menu customizations

Avaya Experience Portal offers those users who need additional functionality in the Experience Portal Manager (EPM) main menu the ability to modify and customize the EPM main menu by changing the associated configuration files.

The EPM main menu consists of menu groups and menu items associated with each group.

Examples of the menu groups in the EPM include the **User Management** and **System Maintenance** groups.

Examples of menu items under the **System Maintenance** group include **Trace Viewer**, **Log Viewer**, and **Alarm Manager**.

You can add menu items to existing menu groups, or add entire menu groups with their own menu items to the EPM main menu.

The EPM main menu configuration files

Note:

You must define the groups and items in all four `configuration` files before they will display properly in the EPM main menu.

configuration menu.xml file

This file defines the groups and items that can appear in the main menu. It is located in the *`TomcatHome`*`/lib/config` directory, where *`TomcatHome`* is the directory in which the Tomcat servlet engine software is installed. The default is `/opt/Tomcat/tomcat`.

display menu.properties file

This file defines the text that the EPM displays for the groups and items defined in the configuration `menu.xml` file. The display `menu.properties` file is located in the *`TomcatHome`*`/lib/messages` directory, where *`TomcatHome`* is the directory in which the Tomcat servlet engine software is installed. The default is `/opt/Tomcat/tomcat`.

features.xml file

This file defines which user roles can see the menu groups and items defined in the configuration `menu.xml` file. The `features.xml` file is located in the *`TomcatHome`*`/lib/config` directory, where *`TomcatHome`* is the directory in which the Tomcat servlet engine software is installed. The default is `/opt/Tomcat/tomcat`.

features.properties file

This file defines the text that the EPM displays on the Roles web pages for the features defined in the configuration `features.xml` file. The `features.properties` file is located in the *`TomcatHome`*`/lib/messages` directory, where *TomcatHome* is the directory in which the Tomcat servlet engine software is installed. The default is `/opt/Tomcat/tomcat`.

Add a new menu group and items

To add a new menu group, complete the following procedures:

Step	Task	✔
1	Define a unique extensions directory as described in Defining a unique extensions directory on page 638.	
2	Define the new menu group and its items in the configuration `menu.xml` file as described in Defining a new menu group and its items on page 625.	
3	Define the labels that will be displayed for the menu group and its items in the display `menu.properties` file as described in Defining labels for the new menu group and its items on page 627.	
4	Set the access permissions by defining the user roles that can see the menu group and each of its items in the `features.xml` file as described in Setting user access permissions for the new menu group and its items on page 628.	
5	Define the labels that will be displayed for the features in the display `feature.properties` file as described in Defining labels for the features in the new menu group and its items on page 631.	

Defining a new menu group and its items

About this task

The configuration `menu.xml` file specifies the location of and properties for your new menu group and the menu items.

Procedure

1. In an ASCII text editor, create a configuration `menu.xml` file in the *`TomcatHome`*`/lib/extensions/UniqueDirectoryName/config` directory, where *`TomcatHome`* is the directory in which the Tomcat servlet engine software is installed and

UniqueDirectoryName is the directory defined as described in Defining a unique extensions directory on page 638. The default is `/opt/Tomcat/tomcat`.

2. Create the basic template for the menu.xml by adding the following tags:

```
<?xml version="1.0" encoding="UTF-8"?>
<navigationmenu
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:noNamespaceSchemaLocation="menu.xsd">
</navigationmenu>
```

3. For each menu group to be defined, add the <menu> and </menu> tags just before the </navigationmenu> tag.

Note:

A menu group is defined by a <menu> tag followed by one or more <item> tags. The <menu> tag must end with a </menu> tag.

4. For each menu tag you add for defining a group, specify the following menu attributes:

Attributes	Example	Description
`type="group"`, where *type* defines the type of the menu.	To specify the type of the menu as `group`, specify `type="group"`	This attribute defines the type of the menu tag.
`render=[true|false]`, where `render` is either `true` or `false`.	To instruct the EPM to display the menu group, specify `render=true`	If you set this property to `false`, the EPM does not display the menu group.
`tag="groupTag"`, where *groupTag* is the identifier the system uses to identify the group.	To assign the name specify, `tag="newMenuGroupIdentifier"`	The identifier of the menu group. This identifier must be unique across all menu groups and menu items in the configuration `menu.xml` file.

5. For each menu item you want to add, specify the <item> tag after the <menu> tag but before the corresponding </menu> tag and specify the following attributes:.

Note:

A menu item within a menu group is defined by an <item> tag.

Attributes	Example	Description
`type="item"`, where *type* defines the type of the item.	To specify the type of the menu item as `item`, specify `type="item"`.	This attribute defines the type of the item tag.
`render=[true|false]`, where `render` is either `true` or `false`.	To instruct the EPM to display the item in the menu group, specify `render=true`	If you set this property to `false`, the EPM does not display the menu group.

Table continues…

Attributes	Example	Description
`tag=itemTag`, where `itemTag` is the identifier the system uses to identify the item.	Specify `tag="newMenuItemIdentifier"`	The identifier of the menu item. This identifier must be unique across all menu groups and menu items in the configuration `menu.xml` file.
`action=displayURL`, where `displayURL` is the URL that you want the system to display when a user clicks this item.	To instruct the EPM to open `admin.ops.page.html` when the user clicks on the second item of the fifth menu group, specify `action="http://my.site.com/custom_pages/admin.ops.page.html"`	Determines what page Experience Portal displays when the user selects the menu item. **Important:** Experience Portal does not validate this URL
`newWindow="[true|false]"`, where `newWindow` is either `true` or `false`.	To instruct the EPM to open a new page when the user clicks on the menu item of the menu group, specify `newWindow=true`	If this option is set to `true`, Experience Portal opens the specified URL in a new browser window. If you do not specify this property, it defaults to `false`.

6. For each new <item> tag, specify a </item> tag to end the menu item definition.
7. Save and close the file.

Example

For example, if you have a group called `myMenuGroup` with menu items `myUsersItem`, `myAdminItem`, and `myUserMgrItem`, the entire section could look like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<navigationmenu
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:noNamespaceSchemaLocation="menu.xsd">
<menu type="group" render="true" tag="myMenuGroup">
   <item type="item" render="true" tag="myUsersItem"
      action="http://my.site.com/custom/users.page.html" newWindow="true">
   </item>
   <item type="item" render="true" tag="myAdminItem"
      action="http://my.site.com/custom/admin.page.html" newWindow="true">
   </item>
   <item type="item" render="true" tag="myUserMgrItem"
      action="http://my.site.com/custom/usermgr.page.html" newWindow="true">
   </item>
</menu>
</navigationmenu>
```

Defining labels for the new menu group and its items

About this task

The display `menu.properties` file specifies the labels that the EPM displays to the end user.

Procedure

1. In an ASCII text editor, open the display `menu.properties` file in the *TomcatHome*`/lib/extensions/UniqueDirectoryName/messages` directory, where *TomcatHome* is the directory in which the Tomcat servlet engine software is installed and UniqueDirectoryName is the directory as described in Defining a unique extensions directory on page 638. The default is `/opt/Tomcat/tomcat`.
2. Add a section for each menu group that you added to the configuration `menu.xml` file as shown below:

   ```
   myMenuGroup=groupDisplayText
   myMenuItem=itemDisplayText
   ```

   where:

   - `myMenuGroup` is the menu group identifier specified in the `menu.xml` configuration file.
   - `myMenuItem` is the menu item identifier specified in the `menu.xml` configuration file.
   - *`groupDisplayText`* is the group label that Experience Portal displays in the EPM main menu.
   - *`itemDisplayText`* is the item label that Experience Portal displays in the EPM main menu.
3. Save and close the file.

Example

For example:

```
myMenuGroup=My Menu Group
myUsersItem=Users
myAdminItem=Administrator
myUserMgrItem=User Manager
```

Setting user access permissions for the new menu group and its items

About this task

The `features.xml` file specifies which user roles have access to a menu group and each item in the group.

Procedure

1. In an ASCII text editor, create a `configuration features.xml` file in the *TomcatHome*`/lib/extensions/UniqueDirectoryName/config` directory, where *TomcatHome* is the directory in which the Tomcat servlet engine software is installed and UniqueDirectoryName is the directory as described in Defining a unique extensions directory on page 638. The default is `/opt/Tomcat/tomcat`.

2. Create the basic template for features.xml by adding the following tags:

```
<?xml version="1.0" encoding="UTF-8"?>
<features
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:noNamespaceSchemaLocation="features.xsd">
</features>
```

3. For each menu group to be defined in configuration menu.xml, add the <category> and </category> tags just before the </features> tag.

Note:

For each new menu group defined in the `menu.xml` confiugratiion file, you needs to define the <category> and </category> tags in the `features.xml` file.

4. For each <category> tag added, specify the following attributes:

Attributes	Example	Description
`name="groupTag"`, where *`groupTag`* is the identifier defined for the menu group in the `menu.xml` configuration file.	Specify `name="newMenuGroupIdentifier"`	The identifier of the menu group defined in the configuration `menu.xml` file.

5. Specify a <feature> tag for each new menu item after the <category> and before the corresponding </category> tags.

Note:

For each new menu item defined in the `menu.xml` configuration file, you need to define a <feature> tag within the corresponding <category> tag in the `features.xml` file.

6. For each <feature> tag added, specify the following attributes:

Attributes	Example	Description
`name="itemTag"`, where *`itemTag`* is the identifier defined for the menu item in the `menu.xml` configuration file.	Specify `name="newMenuItemIdentifier".`	The identifier of the menu item defined in the configuration `menu.xml` file.

Table continues…

Attributes	Example	Description
`allow="roles"`, where *roles* is a combination of any of the following roles separated by commas: • administration • maintenance • operations • usermanager • auditor	To define that this menu group is accessible only to the administrator and user manager roles , specify `allow= "administration, usermanager".`	This attribute defines the roles that have permission to view this menu group.

Note:

Make sure that any user role specified for a menu item is also specified for the entire group.

7. Make sure each of the new <feature> tags have a corresponding</feature> tag.
8. Save and close the file.

Example

For example, if you have a group called `myMenuGroup` with menu items `myUsersItem`, `myAdminItem`, and `myUserMgrItem`, and you want to specify that:

- Users with any user role can see the `myMenuGroup` and `myUsersItem` groups.
- Only the users with the Administration user role can see the `myAdminItem` group.
- Users with the User Manager user role can see the `myUserMgrItem` group.

You would specify:

```
<?xml version="1.0" encoding="UTF-8"?>
<features
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:noNamespaceSchemaLocation="feature.xsd">
<category name="myMenuGroup"
  <feature name="myUsersItem"
allow="administration,operations,maintenance,auditor,usermanager">
  </feature>
  <feature name="myAdminItem" allow="administration"/>
  </feature>
  <feature name="myUserMgrItem" allow="administrator, usermanager"/>
  </feature>
</category>
</features>
```

Defining labels for the features in the new menu group and its items

About this task

The display `feature.properties` file specifies the labels that the EPM displays to the end user on the Roles page.

Procedure

1. In an ASCII text editor, open the display `feature.properties` file in the *`TomcatHome`*`/lib/extensions/UniqueDirectoryName/messages` directory, where *`TomcatHome`* is the directory in which the Tomcat servlet engine software is installed and UniqueDirectoryName is the directory defined as described in Defining a unique extensions directory on page 638. The default is `/opt/Tomcat/tomcat`.
2. Create the basic template for the features.properties by adding the following tags:

   ```
   #{{START:FEATURES:EXTENSIONS:UniqueDirectoryName
   #}}END:FEATURES:EXTENSIONS:UniqueDirectoryName
   ```

3. Add a section for each menu group that you added to the configuration `menu.xml` file as shown below:

   ```
   myMenuGroup=groupDisplayText
   myMenuItem=itemDisplayText
   ```

   where:

   - `myMenuGroup` is the menu group identifier specified in the `menu.xml` configuration file.
   - `myMenuItem` is the menu item identifier specified in the `menu.xml` configuration file.
   - *`groupDisplayText`* is the group label that Experience Portal displays in the EPM main menu.
   - *`itemDisplayText`* is the item label that Experience Portal displays in the EPM main menu.

   Note:

   Ensure that display text specified for the menu group and menu items in `feature.properties` match the display text specified for the same in `menu.properties` file.

4. Save and close the file.
5. Insert the contents of this file within the `#{{START:FEATURES:EXTENSIONS` and `#}}END:FEATURES:EXTENSIONS` tags, into the display features.properties file under the `TomcatHome/lib/messages` directory, where *TomcatHome* is the directory in which the Tomcat servlet engine software is installed. The default is `/opt/Tomcat/tomcat`.

Example

For example:

```
#{{START:FEATURES:EXTENSIONS
#{{START:FEATURES:EXTENSIONS:UniqueDirectoryName
myMenuGroup=My Menu Group
myUserItem=Users
myAdminItem=Administrators
myUserMgrItem=User Manager
#}}END:FEATURES:EXTENSIONS:UniqueDirectoryName
#}}END:FEATURES:EXTENSIONS
```

Add menu items to an existing menu group

To add a menu item to an existing menu group, complete the following procedures:

Step	Task	✔
1	Define a unique extensions directory as described in Defining a unique extensions directory on page 638.	
2	Define the new menu items in the configuration `menu.xml` file as described in Defining new menu items under an existing group on page 632.	
3	Define the labels that will be displayed for the menu items in the display `menu.properties` file as described in Defining a label for the new menu item on page 634.	
4	Set the access permissions by defining the user roles that can see the menu items in the `features.xml` file as described in Setting user access permissions for the new menu items on page 635.	
5	Define the labels that will be displayed on the role details web page for the features in the display `features.properties` file as described in Defining labels for features in the new menu item on page 637.	

Defining new menu items under an existing group

About this task

The configuration `menu.xml` file specifies the location of and properties for your new menu items.

Procedure

1. In an ASCII text editor, open the configuration `menu.xml` file in the *`TomcatHome`*`/lib/extensions/UniqueDirectoryName/config` directory, where *`TomcatHome`* is the directory in which the Tomcat servlet engine software is installed and `UniqueDirectoryName` is the directory defined as described in Defining a unique extensions directory on page 638. The default is `/opt/Tomcat/tomcat`.

2. Create the basic template for menu.xml by adding the following tags:

```
<?xml version="1.0" encoding="UTF-8"?>
<navigationmenu
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:noNamespaceSchemaLocation="menu.xsd">
</navigationmenu>
```

3. For each existing menu group for which a new menu item will be defined, add the <menu> and </menu> tags just before the </navigationmenu> tag.
4. Specify the following menu attributes:

Attributes	Example	Description
`type="group"`, where *type* defines the type of the menu.	To specify the type of the menu as `group`, specify `type="group"`	This attribute defines the type of the menu tag.
`tag="groupTag"`, where *groupTag* is the identifier the system uses to identify the group.	To assign the name specify, `tag="existingMenuGroup Identifier"`	The identifier of the menu group. This identifier must be unique across all menu groups and menu items in the configuration `menu.xml` file.

For Menu Group...	Set tag to...
User Management	tag=menuGroupUserManagement
Real-Time Monitoring	tag=menuGroupRealTimeMonitoring
System Maintenance	tag=menuGroupSystemMaintenance
System Management	tag=menuGroupSystemManagement
System Configuration	tag=menuGroupSystemConfiguration
Security	tag=menuGroupSecurity
Reports	tag=menuGroupReports

5. For each menu item you want to add, specify the <item> tag after the <menu> tag but before the corresponding </menu> tag and specify the following attributes:.

Property	Example	Description
`type="item"`, where type defines the type of the item.	To specify the type of the menu item as `item`, specify `type="item"`	This attribute defines the type of the item tag.
`render=[true|false]`, where `render` is either `true` or `false`.	To instruct the EPM to display the item in the menu group, specify `render=true`	If you set this property to `false`, the EPM does not display the menu group.

Table continues…

Property	Example	Description
`tag=itemTag`, where `itemTag` is the identifier the system uses to identify the item.	Specify `tag="newMenuItemIdentifier"`	The identifier of the menu item. This identifier must be unique across all menu groups and menu items in the configuration `menu.xml` file.
`action=displayURL`, where `displayURL` is the URL that you want the system to display when a user clicks this item.	To instruct the EPM to open admin.ops.page.html when the user clicks on the second item of the fifth menu group, specify `action="http://my.site.com/custom_pages/admin.ops.page.html"`	Determines what page Experience Portal displays when the user selects the menu item. **Important:** Experience Portal does not validate this URL
`newWindow="[true|false]"`, where `newWindow` is either `true` or `false`.	To instruct the EPM to open a new page when the user clicks on the menu item of the menu group, specify `newWindow=true`	If this option is set to `true`, Experience Portal opens the specified URL in a new browser window. If you do not specify this property, it defaults to false.

6. For each new <item> tag, specify a </item> tag to end the menu item definition.
7. Save and close the file.

Example

The Report menu group with the `menuItemMyCustomReport` item added could look like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<navigationmenu
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:noNamespaceSchemaLocation="menu.xsd">
<menu type="group" render="true" tag="menuGroupReports">
    <item type="item" render="true" tag="menuItemStandardReports"
         action="reports/standardReports.jsf?initializeBean=true">
    </item>
    <item type="item" render="true" tag="menuItemCustomReports"
         action="reports/customReports.jsf?initializeBean=true">
    </item>
    <item type="item" render="true" tag="menuItemScheduledReports"
         action="reports/scheduledReports.jsf?initializeBean=true">
     </item>
    <item type="item" render="true" tag="menuItemMyCustomReport"
        action="http://my.site.com/custom/custom.report.page.html" newWindow="true">
     </item>
</menu>
</navigationmenu>
```

Defining a label for the new menu item

About this task

To specify the labels that Experience Portal will display to the end user, edit the display `menu.properties` file.

Procedure

1. In an ASCII text editor, open the display `menu.properties` file in the *TomcatHome*`/lib/extensions/UniqueDirectoryName/messages` directory, where *TomcatHome* is the directory in which the Tomcat servlet engine software is installed and UniqueDirectoryName is the directory defined as described in Defining a unique extensions directory on page 638. The default is `/opt/Tomcat/tomcat`.
2. Add a line entry for each menu item you added to the configuration `menu.properties` file, as shown below:

   `myMenuItem=`*`itemDisplayText`*

   where:

   - `myMenuItem` is the menu item identifier specified in the `menu.xml` configuration file.
   - *`itemDisplayText`* is the text that the EPM displays in the main menu.
3. Save and close the file.

Example

For example, if you added menu items `menuItemMyStandardReport` and `menuItemMyCustomReport` to the Reports menu group in the configuration `menu.xml` file, you would specify:

```
menuItemMyStandardReport=My Standard Report
menuItemMyCustomReport=My Custom Report
```

Setting user access permissions for the new menu items

About this task

The `features.xml` file specifies which user roles have access to the new menu items.

Procedure

1. In an ASCII text editor, open the configuration `features.xml` file in the *TomcatHome*`/lib/extensions/UniqueDirectoryName/config` directory, where *TomcatHome* is the directory in which the Tomcat servlet engine software is installed and UniqueDirectoryName is the directory defined as described in Defining a unique extensions directory on page 638. The default is `/opt/Tomcat/tomcat`.
2. Create the basic template for the features.xml by adding the following tags:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <features
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xsi:noNamespaceSchemaLocation="features.xsd">
   </features>
   ```
3. For each menu group to be defined in configuration menu.xml, add the <category> and </category> tags just before the </features> tag.

Note:

For each new menu group defined in the `menu.xml` configuration file, you need to define the <category> and </category> tags in the `features.xml` file.

4. Specify a </feature> tag for each new menu item after the <category> and before the corresponding </category> tag.

Note:

For each new menu item defined in the `menu.xml` configuration file, you need to define a <feature> tag within the corresponding <category> tag in the `features.xml` file.

5. For each <feature> tag added, specify the following attributes:

Attributes	Example	Description
`name="itemTag"`, where *`itemTag`* is the identifier defined for the menu item in the `menu.xml` configuration file.	Specify `name="newMenuItemIdentifier"`	The identifier of the menu item defined in the configuration `menu.xml` file.
`allow="roles"`, where *`roles`* is a combination of any of the following roles separated by commas: • administration • maintenance • operations • usermanager • auditor	To define that this menu group is accessible only to administrator and user manager, specify `allow="administration,usermanager"`	This attribute defines the roles that have permission to view this menu group.

Note:

Make sure that any user role specified for a menu item is also specified for the entire group.

6. Make sure each of the new <feature> tags have a corresponding</feature> tag.
7. Save and close the file.

Example

For example, to specify that users with the Administration, Operations, and Reporting user roles can view the menu item `menuItemMyCustomreport` for the Reports menu group, add the following lines within the category which defines the menuGroupReports:

```
<?xml version="1.0" encoding="UTF-8"?>
<features
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
    xsi:noNamespaceSchemaLocation="features.xsd">
<category name="menuGroupReports">
<feature name="menuItemMyCustomReport"
     allow="administration,operations,maintenance,reporting">
</feature>
</category>
</features>
```

Defining labels for features in the new menu item

About this task

The display `feature.properties` file specifies the labels that the EPM displays to the end user on the Roles page.

Procedure

1. In an ASCII text editor, open the display `feature.properties` file in the *TomcatHome*`/lib/extensions/UniqueDirectoryName/messages` directory, where *TomcatHome* is the directory in which the Tomcat servlet engine software is installed and UniqueDirectoryName is the directory defined as described in Defining a unique extensions directory on page 638. The default is `/opt/Tomcat/tomcat`.
2. Create the basic template for the menu.xml by adding the following tags:

   ```
   #{{START:FEATURES:EXTENSIONS:UniqueDirectoryName
   #}}END:FEATURES:EXTENSIONS:UniqueDirectoryName
   ```

3. Add a section for each menu item that you added to the configuration `menu.xml` file, as shown below:

   `myMenuItem=`*`itemDisplayText`*

   where:

   - `myMenuItem` is the menu item identifier specified in the `menu.xml` configuration file.
   - *`itemDisplayText`* is the item label that Avaya Experience Portal displays in the EPM main menu.

   Note:

   Ensure that the display text specified for the menu group and menu items in `feature.properties` file match the display text specified for the same in `menu.properties` file.

4. Save and close the file.
5. Insert the contents of this file within the `#{{START:FEATURES:EXTENSIONS` and `#}}END:FEATURES:EXTENSIONS` tags, in the display features.properties file under `TomcatHome/lib/messages` directory, where *TomcatHome* is the directory in which the Tomcat servlet engine software is installed. The default is `/opt/Tomcat/tomcat`.

Example

For example:

```
#{{START:FEATURES:EXTENSIONS
#{{START:FEATURES:EXTENSIONS:UniqueDirectoryName
menuItemMyStandardReport=My Standard Report
menuItemMyCustomReport=My Custom Report
#}}END:FEATURES:EXTENSIONS:UniqueDirectoryName
#}}END:FEATURES:EXTENSIONS
```

Defining a unique extensions directory

About this task

Defining a unique extensions directory allows one to separate the menu and feature customizations from other menu and feature customizations.

Procedure

1. Create a unique extensions directory to identify the extension, in the `TomcatHome/lib/extensions` directory, where `TomcatHome` is the directory in which the Tomcat servlet engine software is installed. The default is /opt/Tomcat/tomcat.

   Note:

   The unique id must be in upper case and three characters long.

   'The unique ids already in use are EPE, POM, and ICR.

2. Create directories called `config` and `messages` under `TomcatHome/lib/extensions/UniqueDirectoryName` where `UniqueDirectoryName` is the folder created in the previous step.

Chapter 25: The Application Logging web service

The Application Logging web service for third-party speech applications

Avaya Experience Portal includes an Application Logging web service that lets you save application and call flow data information from third-party speech applications into the `vpappLog` table of the Experience Portal database. Experience Portal can then include information from these third-party applications when it generates the Application Detail report and Application Summary report.

The Application Logging web service conforms to all W3C standards and can be accessed through any web service client using the Avaya-provided Web Services Description Language (WSDL) file.

Best practices

Experience Portal supports Axis 2.0 Application Logging web service.

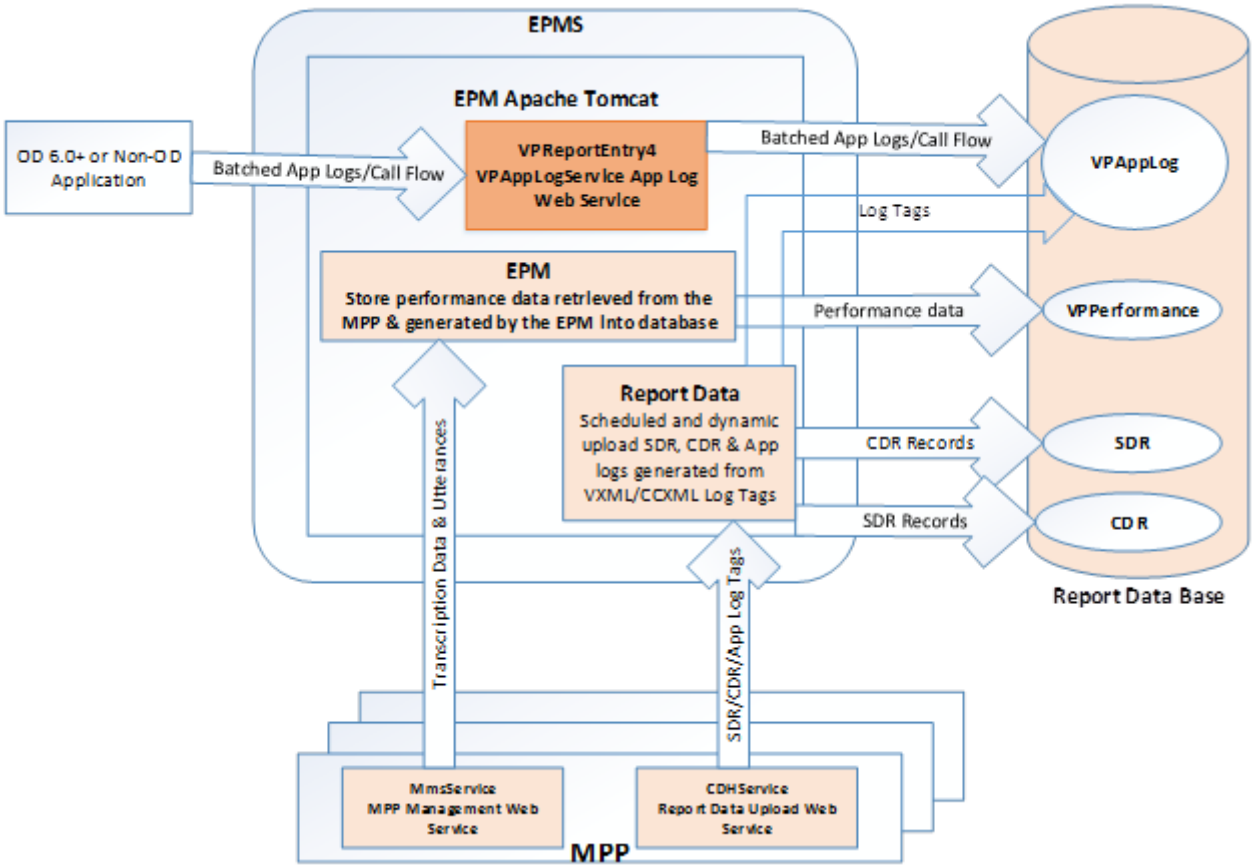
When using the Application Logging web service, keep in mind that:

- The Axis 2.0 Application Logging web service use Basic Authentication to authenticate web service client requests and only support HTTPS protocol.
- When the HTTPS protocol is used in the Web Service client, the Web Service client needs to handle to accept the certificate from the EPM server. No certificate needs to be installed on the Application Server. It is one-way SSL authentication.
- When calling the Axis 2.0 Application Logging web services, ensure to turn HTTP Chunking off.
- When you submit a request to the web service, you need to specify the user name and password which are specified in the Application Reporting section of the Web Service Authentication group on the EPM Settings page. If you need to change this user name or password, you must do it through the EPM. For details, see Configuring the Application Logging web service on page 641. For Axis 2.0 Application Logging web service requests, you can also use the Experience Portal web user name and password. The web user has to have the Web Services role with Application Reporting feature enabled.

- You must send all of the log entries for one or more session blocks at the same time. Do not send each log entry as it occurs or you may adversely affect Experience Portal system performance.
- You must use the logApplicationEventAlarm web service method with utmost caution. You should implement a throttling mechanism on the client side to limit flooding the EPM with the application events and alarms.
- You should have a proper queuing mechanism or sampling rate control method in place if you are sending a large number of log entries to the database. Otherwise this may adversely affect Experience Portal system performance.
- You should save all log entries in case the EPM is unavailable when the Application Logging web service is called. That way you can resend the log entries when the EPM becomes available.
- If your Experience Portal EPM software runs on a dedicated server machine, you should configure a auxiliary EPM server to handle Application Logging web service requests if the primary EPM server is unavailable.
- The Avaya Experience Portal Application Detail report and Application Summary report expect the report data to be in a particular format. For details about what Application Detail Records (ADRs) are stored in the `vpapplog` table, see Generating custom reports using third-party software in *Administering Avaya Experience Portal*.

Application Logging web service flow diagram

The following figure shows how speech applications interact with the Application Logging web service to add application messages to the Experience Portal database.



Configuring the Application Logging web service

About this task

To configure the Application Logging web service, you need to download the Avaya-provided WSDL file and build a custom web service client based on that file.

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** > **EPM Server**.
3. On the EPM Servers page, click **EPM Settings**.
4. On the EPM Settings page, go to the **Application Reporting** section in the **Web Service Authentication** group.
5. Enter the user name and password that must be included with all Application Logging web service requests for Digest Authentication.

This is the same user name and password that you should use when accessing the web service though the WSDL file.

6. Click **OK**.
7. For Axis 2.0 Application Logging web services: open the `https://<EPM-server>/axis2/services/VPAppLogService` page in a web browser.

   Where *<EPM-server>* is the domain name or IP address of the system on which the primary EPM software is installed.
8. When prompted, enter the user name and password specified in the **Application Reporting** section of the EPM Settings page.
9. Save the WSDL file and use it to build the web service client that accesses the Application Logging web service. This web service conforms to all current W3C standards.

Application Logging web service methods

The Application Logging web service includes the following methods:

- reportBatch method for application logging on page 643
- reportBatch method for call flow data on page 645
- logFailed method on page 642
- logApplicationEventAlarm method for application Logging / Alarming on page 648

logFailed method

The Application Logging web service `logFailed` method adds the event `PALOG00017` to the Experience Portal database.

Parameters

Parameter	Type	Description
lastVPMSDown	Long integer	The timestamp of the last time the EPM was down.

Return values

There are no return values from this method.

reportBatch method for application logging

The `reportBatch` method can be used to create application or call flow data log entries in the Experience Portal report database. In either case, the list of input parameters is the same. The only difference is the information you specify for each input parameter.

This topic discusses the information you should specify to create an application log entry. For information about creating a call flow data log entry, see reportBatch method for call flow data on page 645.

Parameters

Parameter	Type	Description
appServerAddress	string	The hostname or IP address of the application server.
applicationID	string	The name of the application. For example: `CollectTicketInfo` **Important:** The applicationID must match the name that was specified when the application was added to Avaya Experience Portal through the EPM. For an application that is assigned to a non-default zone, include the zone information using the format: `ZoneId:applicationName` You can view all application names on the Applications page. You can retrieve the zone Id information using the getZoneInfo method of the Management Interface web service.
level	string	The logging level. The options are: • `Fatal` • `Error` • `Warning` • `Info`
reason	string	The reason this log entry was made. For example: `Application ended successfully.` The reason for the first log entry in a session block should always be "–" (dash).
sessionID	string	The session ID for the session. This is a user-defined identifier that should be unique across sessions.

Table continues…

Parameter	Type	Description
timestamp	string	The current system time in milliseconds since January 1, 1970 00:00:00 UTC. The value of this parameter should contain a long number.
transactionName	string	The transaction name that this log entry is a part of. For example: `Hung Up` **Important:** Every transaction should start with a log entry setting the transaction name along with the activity type of `Start`. Once you start a transaction, all log entries should use the same transaction name up to and including the final log entry for that transaction.
type	string	The activity type for this log. The options are: • `Start` • `In Progress` • `End` • `Cancel`
userLog	string	The session label.
varName	string	A variable name, if one should be included with this log entry.
varValue	string	The value of the variable named in varName.
activityDuration	integer	The duration in seconds between the timestamp of the first log entry with the same transaction name and the activity type of `Start` and this log entry in a single session block. **Note:** This calculation should be based on one block of log entries that belong in one session.
moduleIdNodeId	string	The module ID and node ID in the format: `[Module Id]:Node Id`, where `Module Id` is only specified if it is *not* the same as the application name. For example, if the application name is `CollectTicketInfo` and it contains the `CollectTicketInfo` module with the node `StartTicket` and the `GetPayment` module with the node `StartPay`, you would specify them as: • `:StartTicket` • `GetPayment:StartPay`

Return values

The `reportBatch` method returns one of the following values:

- `success`
- `decryption failed - error occured decrypting the password`
- `Password incorrect`
- `Request is out of date`
- `Error storing data in database`
- `Error initializing database`
- `Error getting the EPID`

If the method fails, you can use the `logFailed` method to enter an event into the Experience Portal event log.

reportBatch method for call flow data

The `reportBatch` method can be used to create application or call flow data log entries in the Experience Portal report database. In either case, the list of input parameters is the same. The only difference is the information you specify for each input parameter.

This topic details the information you should specify to create a call flow data log entry. For information about creating an application log entry, see reportBatch method for application logging on page 643.

Parameters

Parameter	Type	Description
appServerAddress	string	The hostname or IP address of the application server.

Table continues…

Parameter	Type	Description
applicationID	string	The name of the application. For example: `CollectTicketInfo` **Important:** The applicationID must match the name that was specified when the application was added to Avaya Experience Portal through the EPM. For an application that is assigned to a non-default zone, include the zone information using the format: `ZoneId:applicationName` You can view all application names on the Applications page. You can retrieve the zone Id information using the getZoneInfo method of the Management Interface web service.
level	string	This should always be: `Info`
reason	string	The reason this log entry was made. When entering data in this field, you should keep in mind that: • The reason for the first log entry in a session block should always be "–" (dash). • If the activity type is `Node Entry` or `Application Exit`, this field must contain the moduleIdNodeId of the previous log entry of type `Node Entry`. This allows Experience Portal to track the source of the breadcrumb. • If the activity type is `Module Exit`, this field can contain whatever reason code you want to use.
sessionID	string	The session ID for the session. This is a user-defined identifier that should be unique across sessions.
Timestamp	string	The current system time in milliseconds since January 1, 1970 00:00:00 UTC. The value of this parameter should contain a long number.
transactionName	string	This should always be: `Framework`
type	string	The options are: • `Node Entry` • `Module Exit` • `Application Exit`
userLog	string	The session label.
varName	string	A variable name, if one should be included with this log entry.

Table continues…

Parameter	Type	Description
varValue	string	The value of the variable named in varName.
activityDuration	integer	The duration in seconds between the timestamp of the first log entry with the activity type of `Node Entry` or `Application Exit` and this log entry in a single session block. **Note:** This calculation should be based on one block of log entries that belong in one session.
moduleIdNodeId	string	The module and node identifiers. If the type of the last log entry in the session block is `Application Exit`, than this field should be "`--`" (dash dash). Otherwise, it should contain the module ID and node ID in the format: `[Module Id]:Node Id`, where `Module Id` is only specified if it is *not* the same as the application name. For example, if the application name is `CollectTicketInfo` and it contains the `CollectTicketInfo` module with the node `StartTicket` and the `GetPayment` module with the node `StartPay`, you would specify them as: • `:StartTicket` • `GetPayment:StartPay`

Return values

The `reportBatch` method returns one of the following values:

- `success`
- `decryption failed - error occured decrypting the password`
- `Password incorrect`
- `Request is out of date`
- `Error storing data in database`
- `Error initializing database`
- `Error getting the VPID`

If the method fails, you can use the `logFailed` method to enter an event into the Experience Portal event log.

logApplicationEventAlarm method for application Logging / Alarming

The logApplicationEventAlarm method can be used to issue the application events / alarms from the application to the EPM. The alarm events are sent via SNMP traps to the configured network management station but not through INADS.

This topic discusses the information you need to specify to create an application event entry.

Parameters

Parameter	Type	Description
appServerAddress	string	The hostname or IP address of the application server.
applicationID	string	The name of the application. For example: `CollectTicketInfo`
level	string	The logging level. The options are: • `Fatal` • `Error` • `Warning`
reason	string	The generated message defined by the application. Internationalization must be provided by the application. The maximum length is 100 characters. If the length is over the maximum, it will be truncated.
sessionID	string	The session ID for the session.
timestamp	string	The current system time in milliseconds since January 1, 1970 00:00:00 UTC. The value of this parameter should contain a long number.
transactionName	string	Not used.
type	string	Not used.
userLog	string	Not used.
varName	string	A variable name, if one should be included with this event entry. This is optional.
varValue	string	The value of the variable named in *varName*. This is optional.
activityDuration	integer	Not used.
moduleIdNodeId	string	Not used.

Return values

The logApplicationEventAlarm method returns one of the following values:

- `success`
- `decryption failed - error occured decrypting the password`
- `Password incorrect`

- `Request is out of date`
- `Error storing data in database`
- `Error initializing database`
- `Error getting the EPID`

The following table displays the log events and the associated messages to Alarm Maps:

Log Message	Message to Alarm Map	Log Level	Alarm Severity	Log Message Alarm Message
PAPP_00001	QAPP_00001	Warning	Minor	Application {0} reported an error from {1} at {2} with message: {3} {4} QAPP_00001: Application generated a Minor alarm
PAPP_00002	QAPP_00002	Error	Major	Application {0} reported an error from {1} at {2} with message: {3} {4} QAPP_00002: Application generated a Major alarm
PAPP_00003	QAPP_00003	Fatal	Critical	Application {0} reported an error from {1} at {2} with message: {3} {4} QAPP_00003: Application generated a Critical alarm

The parameter definitions for the log entries are:

- {0} – Name of the application defined on the application configuration web page *(applicationID)*
- {1} – Application server IP or host name *(appServerAddress)*, Session ID: *(sessionID)*
- {2} – Application server time of the log event *(timestamp)*
- {3} – The generated message defined by the application. Internationalization must be provided by the application *(reason)*
- {4} – Variable Name: *(varName)* Variable Value: *(varValue)*

Sample Application Logging web service WSDL file

The following is an example of the Application Logging web service WSDL file. The actual file is installed on the server that is running the EPM software. For details about accessing this file, see Configuring the Application Logging web service on page 641.

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions targetNamespace="urn:com.avaya.vp.report.EPReport4"
xmlns:apachesoap="http://xml.apache.org/xml-soap"
```

```
xmlns:impl="urn:com.avaya.vp.report.EPReport4"
xmlns:intf="urn:com.avaya.vp.report.EPReport4"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<!--WSDL created by Apache Axis version: 2.0
Built on Apr 22, 2006 (06:55:48 PDT)-->
<wsdl:types>
 <schema elementFormDefault="qualified"
  targetNamespace="urn:com.avaya.vp.report.EPReport4"
  xmlns="http://www.w3.org/2001/XMLSchema">
 <complexType name="EPReportEntry4">
   <sequence>
    <element name="appServerAddress" nillable="true" type="xsd:string"/>
    <element name="applicationID" nillable="true" type="xsd:string"/>
    <element name="level" nillable="true" type="xsd:string"/>
    <element name="reason" nillable="true" type="xsd:string"/>
    <element name="sessionID" nillable="true" type="xsd:string"/>
    <element name="timestamp" nillable="true" type="xsd:string"/>
    <element name="transactionName" nillable="true" type="xsd:string"/>
    <element name="type" nillable="true" type="xsd:string"/>
    <element name="userLog" nillable="true" type="xsd:string"/>
    <element name="varName" nillable="true" type="xsd:string"/>
    <element name="varValue" nillable="true" type="xsd:string"/>
    <element name="activityDuration" type="xsd:int"/>
    <element name="moduleIdNodeId" nillable="true" type="xsd:string"/>
   </sequence>
 </complexType>
  <element name="reportBatch">
   <complexType>
    <sequence>
     <element maxOccurs="unbounded" name="entries" type="impl:EPReportEntry4"/>
     </sequence>
   </complexType>
  </element>
 <element name="reportBatchResponse"
 </complexType>
  </element>
  <element name="reportBatchReturn" type="xsd:string"/>
  </sequence>
 </complexType>
  </element>
  <element name="logFailed">
   <complexType>
    <sequence>
     <element name="lastVpmsDown" type="xsd:long"/>
    </sequence>
   </complexType>
  </element>
  <element name="logFailedResponse">
    </complexType>
  </element>
  <element name="logApplicationAlarm">
  </complexType>
  <sequence>
  <element maxOccurs="unbounded" name="entries" type="impl:EPReportEntry4"/>
  <sequence>
  </complexType>
  </element>
  <element name="logApplicationAlarmResponse">
  </complexType>
  <sequence>
  <element name="logApplicationEventAlarmReturn" type="xsd:string"/>
  <sequence>
  <complexType/>
```

```
  </element>
 </schema>
</wsdl:types>
<wsdl:message name="reportBatchRequest">
 <wsdl:part element="impl:reportBatch" name="parameters"/>
</wsdl:message>
<wsdl:message name="logFailedRequest">
 <wsdl:part element="impl:logFailed" name="parameters"/>
</wsdl:message>
<wsdl:message name="logApplicationEventAlarmRequest">
<wsdl:part element="impl:logApplicationEventAlarm" name="parameters"/>
</wsdl:message>
<wsdl:message name="reportBatchResponse">
 <wsdl:part element="impl:reportBatchResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="logFailedResponse">
 <wsdl:part element="impl:logFailedResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="llogApplicationEventAlarmResponse">
<wsdl:part element="impl:logApplicationEventAlarmResponse" name="parameters"/>
</wsdl:message>
<wsdl:portType name="EPReport4">
 <wsdl:operation name="reportBatch">
  <wsdl:input message="impl:reportBatchRequest" name="reportBatchRequest"/>
  <wsdl:output message="impl:reportBatchResponse" name="reportBatchResponse"/>
 </wsdl:operation>
 <wsdl:operation name="logFailed">
  <wsdl:input message="impl:logFailedRequest" name="logFailedRequest"/>
  <wsdl:output message="impl:logFailedResponse" name="logFailedResponse"/>
</wsdl:operation>
 <wsdl:operation name="logApplicationEventAlarm">
  <wsdl:input message="impl:logApplicationEventAlarmRequest"
name="logApplicationEventAlarmRequest"/>
  <wsdl:output message="impl:logApplicationEventAlarmResponse"
name="logApplicationEventAlarmResponse"/>
 </wsdl:operation>
</wsdl:portType>
<wsdl:binding name="EPReport4SoapBinding" type="impl:EPReport4">
 <wsdlsoap:binding style="document"
  transport="http://schemas.xmlsoap.org/soap/http"/>
 <wsdl:operation name="reportBatch">
  <wsdlsoap:operation soapAction=""/>
  <wsdl:input name="reportBatchRequest">
   <wsdlsoap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="reportBatchResponse">
   <wsdlsoap:body use="literal"/>
  </wsdl:output>
 </wsdl:operation>
 <wsdl:operation name="logFailed">
  <wsdlsoap:operation soapAction=""/>
  <wsdl:input name="logFailedRequest">
   <wsdlsoap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="logFailedResponse">
   <wsdlsoap:body use="literal"/>
  </wsdl:output>
 </wsdl:operation>
 <wsdl:operation name="logApplicationEventAlarm">
  <wsdlsoap:operation soapAction=""/>
  <wsdl:input name="logApplicationEventAlarmRequest">
   <wsdlsoap:body use="literal"/>
  </wsdl:input>
<wsdl:output name="logApplicationEventAlarmResponse">
   <wsdlsoap:body use="literal"/>
```

```
  </wsdl:output>
 </wsdl:operation>
</wsdl:binding>
<wsdl:service name="EPReport4Service">
 <wsdl:port binding="impl:EPReport4SoapBinding" name="EPReport4">
  <wsdlsoap:address location="http://localhost:80/EPReport4"/>
 </wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

Chapter 26: The Application Interface web service

The Application Interface web service

Developers can use the Application Interface web service to:

- Start a CCXML or VoiceXML application that has been added to Avaya Experience Portal using the Add Application page.

  The web service automatically examines each MPP in the Experience Portal system and starts the session on the first available MPP that has the required outbound resources available.
- Send an event to a specific application session running on an MPP.
- Query the system for the total number of:
  - Used and unused outbound resources available
  - Unused SIP outbound resources
  - Unused H.323 outbound resources
- Send an SMS message or email message using one of the Avaya Experience Portal configured SMS or Email connections.
- Start an SMS or email application that has been added to Avaya Experience Portal using the Add Application page.

The Application Interface web service conforms to all W3C standards and can be accessed through any web service client using the Avaya-provided Web Services Description Language (WSDL) file.

Tip:

Sample files showing how you can communicate with the Application Interface web service using such methods as Java, JavaScript, and php are located in the `Support/Examples/Application Interface Web Service` directory on the Experience Portal installation DVD.

You can use the Application Interface test client to validate the Application Interface web service and the Experience Portal outcall, SMS, and Email functionality. Avaya supplies an installation script that automatically installs the Application Interface test client when Experience Portal is installed. For more information , see the *Configure and run the Application Interface test client*

section in the *Implementing Avaya Experience Portal on a single server* guide or the *Implementing Avaya Experience Portal on multiple servers* guide.

Best practices

When using the Application Interface web service, keep in mind that:

- The Axis 2.0 Application Interface web service uses Basic Authentication to authenticate web service client requests. When you submit a request to the web service, you need to include the user name and password that is configured as one of the Experience Portal users and that user must have the Web Services role checked.
- If non-ASCII characters are sent in the URL request to the web service they should be encoded as UTF-8 prior to sending the request.

  For example, an application name of ‘aña’ is encoded and sent as ‘a%C3%B1a’. Note that the non-ASCII character ‘ñ’ is sent as the UTF-8 value of ‘%C3%B1’.
- A non zero timeout value should be specified when using the `LaunchVXML` method. If no timeout value is passed, or if the value is 0, then a default value of 120 seconds will be used.
- For the methods `LaunchCCXML`, `LaunchVXML`, `LaunchSMS`, `LaunchEmail`, `SendSMS`, and `SendEmail`, parameters must be passed as name value pairs. For example, `parameter1=value`.

  Each name value pair is separated by semicolon. If a value of the specific parameter has multiple values, those values should be separated by comma (,). If the value contains a semicolon (;), you must escape it by using `\;`
- If you plan to use a single CCXML application to start multiple outgoing calls simultaneously, keep in mind that each application is handled by a single MPP, which means that each application is limited to the number of ports available on the MPP to which it is assigned. While the Application Interface web service tries to select the best MPP to handle the call, the application must have a way to verify the number of available ports so that it does not exceed the resources available on the MPP.

  If you want to make additional calls, you can either:

  - Start one additional instance of the CCXML call blast application for each additional MPP in the system.
  - Use the `QueryResources` method to check the available resources and start another instance of the CCXML call blast application as soon as enough resources are available.
- If your Experience Portal EPM software runs on a dedicated server machine, you should configure a auxiliary EPM server to handle Application Interface web service requests if the primary EPM server is unavailable.

Application Interface web service flow diagram

The following figure shows how an external application interacts with the Application Interface web service and how the Application Interface web service interacts with the rest of the Experience Portal system.

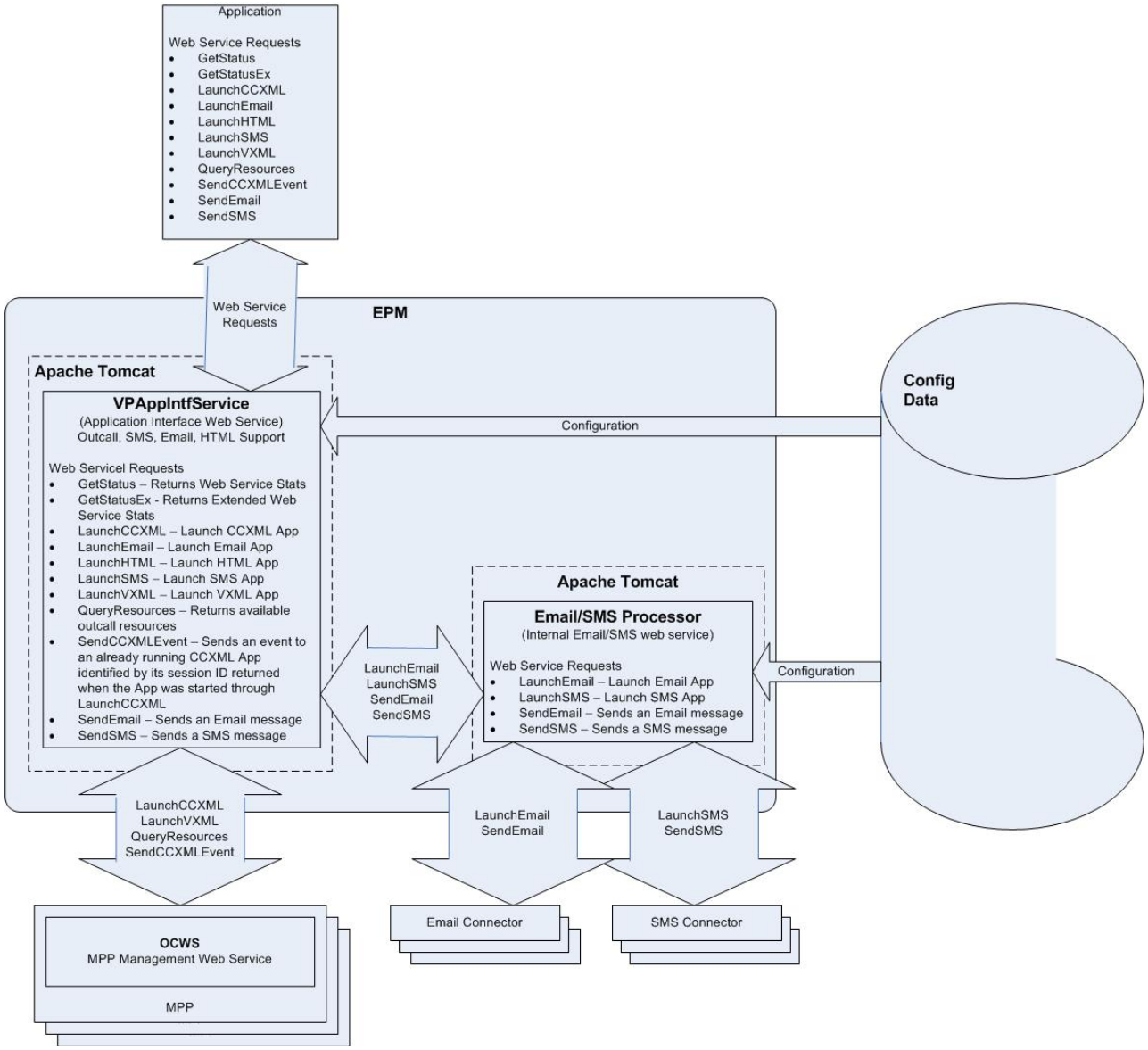


Figure 1: Application Interface Web service flow diagram

Configuring the Application Interface web service

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 **User Management** > **Users**.
3. Select a user that will be used when sending requests to the Web Service.
4. On the Change User page, click the **Web Services** role to enable the user to use web service.
5. Click **Save**.
6. Open the following page in a Web browser: `https://<EPM-server>/axis2/services/VPAppIntfService?wsdl`

   Where *<EPM-server>* is the domain name or IP address of the system where the primary EPM software is installed.

   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?wsdl`.
7. When prompted, enter the user name and password for the Experience Portal with the web services role checked.
8. Save the WSDL file and use it to build the web service client that accesses the Application Interface web service (axis 2.0). This web service conforms to all current W3C standards.

Application Interface web service methods

The Application Interface web service includes the following methods:

- SendSMS method on page 678

All methods can be called from any application that is running on the same network as theAvaya Experience Portal EPM server.

GetStatus method

This method returns the:

- Number of SIP requests processed since the Application Interface web service last started
- Number of telephony requests processed since the Application Interface web service last started
- Number of VoiceXML requests since the Application Interface web service last started
- Number of CCXML event requests since the Application Interface web service last started
- Number of Send CCXML requests sent since the Application Interface web service last started
- Maximum, minimum, and average number of MPP servers examined before a suitable MPP was found to run the requested application
- Date and time that the Application Interface web service was started
- Date and time on which the last request was made
- The version of the EPM software on the server running the Application Interface web service

Important:

The return values are described Return values on page 681.

Data Returned

Parameter	Type	Description
iSIPRequestsProcessed_returned	Integer	Total number of SIP requests processed since the Application Interface web service was started.
iTELRequestsProcessed_returned	Integer	Total number of H.323 or SIP telephony requests processed since the web service was started.
iVXMLRequestsProcessed_returned	Integer	Total number of VoiceXML requests processed since the web service was started.
iCCXMLRequestsProcessed_returned	Integer	Total number of CCXML requests processed since the web service was started.
iCCXMLEventsSent_returned	Integer	Total number of CCXML events sent since the web service was started.

Table continues…

Parameter	Type	Description
maxMPPHops_returned	Integer	Maximum number of MPPs that were examined before the web service found an MPP on which to run the requested application.
minMPPHops_returned	Integer	Minimum number of MPPs that were examined before the web service found an MPP on which to run the requested application.
avgMPPHops_returned	Integer	Average number of MPPs that were examined before the web service found an MPP on which to run the requested application.
lastRequestDateTime_returned	Date	Date and time on which the last request was made.
serviceStartedDateTime_returned	Date	Date and time on which the web service was last started.
vpmsSoftwareVersion_returned	String	The version of the EPM software running on the server.

GetStatusEx method

This method returns the:

- Number of SIP requests processed since the Application Interface web service last started
- Number of telephony requests processed since the Application Interface web service last started
- Number of VoiceXML requests since the Application Interface web service last started
- Number of CCXML requests since the Application Interface web service last started
- Number of Send CCXML event requests sent since the Application Interface web service last started
- Maximum, minimum, and average number of MPP servers examined before a suitable MPP was found to run the requested application
- Date and time that the Application Interface web service was started
- Date and time on which the last request was made
- The version of the EPM software on the server running the Application Interface web service
- Number of `LaunchEmail` requests since the Application Interface web service last started
- Number of `LaunchSMS` requests since the Application Interface web service last started
- Number of `SendEmail` requests since the Application Interface web service last started
- Number of `SendSMS` requests since the Application Interface web service last started

Important:

The return values are described Return values on page 681.

Data returned

Parameter	Type	Description
iSIPRequestsProcessed_returned	Integer	Total number of SIP requests processed since the Application Interface web service was started.
iTELRequestsProcessed_returned	Integer	Total number of H.323 or SIP telephony requests processed since the web service was started.
iVXMLRequestsProcessed_returned	Integer	Total number of VoiceXML requests processed since the web service was started.
iCCXMLRequestsProcessed_returned	Integer	Total number of CCXML requests processed since the web service was started.
iCCXMLEventsSent_returned	Integer	Total number of CCXML events sent since the web service was started.
maxMPPHops_returned	Integer	Maximum number of MPPs that were examined before the web service found an MPP on which to run the requested application.
minMPPHops_returned	Integer	Minimum number of MPPs that were examined before the web service found an MPP on which to run the requested application.
avgMPPHops_returned	Integer	Average number of MPPs that were examined before the web service found an MPP on which to run the requested application.
lastRequestDateTime_returned	Date	Date and time on which the last request was made.
serviceStartedDateTime_returned	Date	Date and time on which the web service was last started.
vpmsSoftwareVersion_returned	String	The version of the EPM software running on the server.
iLaunchAppRequestsProcessed_returned	Integer	Total number of `LaunchApp` requests processed since the Application Interface web service was started.
iLaunchEmailRequestsProcessed_returned	Integer	Total number of `LaunchEmail` requests processed since the Application Interface web service was started.
iLaunchSmsRequestsProcessed_returned	Integer	Total number of `LaunchSMS` requests processed since the Application Interface web service was started.
iSendAppRequestsProcessed_returned	Integer	Total number of `SendApp` requests processed since the Application Interface web service was started.
iSendEmailRequestsProcessed_returned	Integer	Total number of `SendEmail` requests processed since the Application Interface web service was started.
iSendSmsRequestsProcessed_returned	Integer	Total number of `SendSMS` requests processed since the Application Interface web service was started.

LaunchCCXML method

This method starts the specified CCXML application, and, if successful, returns the:

- Experience Portal session ID for the new session
- Total number of outbound resources available, both used and unused
- Total number of unused SIP outbound resources
- Total number of unused H.323 outbound resources

Important:

The CCXML application started *must* return the status of that start using a custom event as described in Returning the status of a LaunchCCXML request on page 663. For information on return values, see CCXML application status return values on page 662. The return values are described Return values on page 681.

Note:

If a CCXML application starts multiple VoiceXML applications, each of these applications can use a different speech server. Prior to Experience Portal 7.0, multiple applications used only one speech server. This feature comes into play if you have different languages loaded onto different speech servers.

When a CCXML application starts a VoiceXML dialog by name, the configured ASR or TTS is used. If the configured ASR or TTS changes, the current ASR or TTS resources are released and new resources are seized before the dialog starts.

For example, a CCXML application can start a dialog with English ASR or TTS. The application can determine that the caller prefers Spanish and so, the second dialog is opened with Spanish ASR or TTS.

Parameters

Parameter	Type	Description
toURI	String	Provides a hint to the Application Interface web service about what resources this CCXML application requires. The options are: • Blank (no input): Indicates that there are no requirements. • `tel`: Use this for an H.323 or SIP connection, or a mix of both. • `sip`: Use this for a standard SIP connection. • `sips`: Use this for a secure SIP connection.

Table continues…

Parameter	Type	Description
applicationName	String	Name of the CCXML application to run once the outbound call has connected. **Important:** The applicationName must match the name that was specified when the application was added to Avaya Experience Portal through the EPM. For an application that is assigned to a non-default zone, include the zone information using the format: `ZoneId:applicationName` You can view all application names on the Applications page. You can retrieve the zone Id information using the getZoneInfo method of the Management Interface web service.
applicationURL	String	Parameters that should be appended to URL specified for the application in the EPM. This allows you to invoke the application with different arguments as needed.
parameters	String	One or more name-value variable pairs that will be passed to the CCXML application when it is invoked. Each pair should be in the format `parametername=value`, and multiple pairs should be separated by a `;` (semi-colon). **Note:** When the web service passes the parameter to the application, it appends the namespace `session.values.avaya.ParameterMap`. Therefore, the variable should be referenced in your application as `session.values.avaya.ParameterMap.`*`parametername`*. For example, if you specify `UserCounter=0` in the web service, you would reference `session.values.avaya.ParameterMap.UserCounter` in your application.
uuiInfo	String	The Application Interface web service passes any information in this parameter to the platform telephony layer included in the outbound call.
launchTimeout	Integer	The maximum amount of time, in seconds, to wait for the CCXML application to be start before returning an error message.
zone	String	Zone name where request should be directed. This is the zone name. (Optional).

Data returned

Parameter	Type	Description
sessionID_returned	String	If the CCXML application connected successfully, the Application Interface web service sets this return value to the session ID Experience Portal assigned to the new CCXML session.
totalRes_returned	Integer	Total number of outbound resources available, both used and unused.
unusedSIP_returned	Integer	Total number of unused SIP outbound resources.
unusedH323_returned	Integer	Total number of unused H.323 outbound resources.

Note:

If zones are enabled, the returned resource information is the information for either the zone specified in the request, or for the default zone, if no zone was specified.

CCXML application status return values

Status	App Intf WS rc	Application
"success" `	0	
"networkdisconnect"	0	
"nearenddisconnect"	0	
"farenddisconnect"	0	
"calltransferred"	0	
"parse error"	0x22 (Invalid URL)	
"uri not found"	0x22 (Invalid URL)	
"fetch timeout"	0x13 (Failed)	LaunchCCXML only
"web server error"	0x13 (Failed)	LaunchCCXML only
"fetch error"	0x13 (Failed)	LaunchCCXML only
"unknown error"	0x13 (Failed) v	LaunchCCXML only
"noresource"	0x2 (No Resource)	
"busy"	0x10 (Busy)	
"networkbusy"	0x10 (Busy)	
"noanswer"	0x11 (No Answer)	
"noroute"	0x20 (Invalid URI)	LaunchVXML only
"unknown"	0x12 (Network Refusal)	LaunchVXML only
"internalerror"	0x12 (Network Refusal)	LaunchVXML only
"glare"	0x12 (Network Refusal)v	LaunchVXML only
"invalidstate"	0x12 (Network Refusal)	LaunchVXML only
"fax detected"	0x16 (Fax Detected)	

Note:

All return values generated by the LaunchVXML and LaunchCCXML may not have a mapping to the status that the CCXML application sends.

Returning the status of a LaunchCCXML request

About this task

If you invoke a CCXML application using the Application Interface web service `LaunchCCXML` method, the application started *must* return the status of that start using a custom event. This allows the CCXML application to determine whether the start was successful instead of relying on the limited information available to the Application Interface web service.

For example, if the CCXML application starts correctly but no one answers the outgoing call, the Application Interface web service still considers the call to be a success because the application started correctly. The CCXML application, on the other hand, may consider that call a failure because no one answered. In this case, the CCXML application would return a failure code to the Application Interface web service, and the Application Interface web service would return the failure code to Experience Portal.

Note:

For information on the status related return values that the CCXML application sends, see CCXML application status return values on page 662.

Procedure

1. Create a custom event handler in your application that sends the results back to the Application Interface web service.
2. In the custom event handler, create a variable called `status` that contains the status you want to return to the Application Interface web service.

   For example, if the call was not answered, you could assign `status` the value "no answer" using the `<var name="status" expr="no answer"/>` tag.
3. Send the response to the Application Interface web service using a `<send>` tag with the format: `<send name="avaya.launchresponse" targettype="avaya_platform" target="`*`session.id`*`" namelist="status"/>`, where *`session.id`* is the session identifier assigned to the session by Experience Portal.

CCXML session properties

session.values namespace properties

At the start of a CCXML session, the Application Interface web service places several properties in the `session.values.avaya` namespace properties.

Property	Description
telephony.native_audio_format	The audio encoding codec the MPP uses as the default for audio recording within the Avaya Voice Browser (AVB) when the speech application does not specify the format for recording caller inputs. The options are: • **audio/basic**: The AVB uses the mu-Law encoding format, which is used mostly in the United States and Japan. • **audio/x-alaw-basic**: The AVB uses the A-Law encoding format, which is used in most countries other than the United States and Japan.
fax_detect_enabled	For inbound calls, this property is set to the same value as the **Fax Detection Enable** parameter set for the application through the EPM web interface.
fax_detect_redirect_uri	For inbound calls, if fax detection is enabled, this property is set to the same value as the **Fax Phone Number** parameter set for the application through the EPM web interface.
ConnectTimeoutSecs	For outbound calls launched by the Application Interface web service, this is the maximum amount of time, in seconds, to wait for the CCXML application to be start before returning an error message.
UUI_Info	For outbound calls launched by the Application Interface web service, this property contains the information passed to the application in the uuiInfo parameter of the LaunchCCXML method.
Parameters	For outbound calls launched by the Application Interface web service, this property contains the name-value pairs passed to the application by the LaunchCCXML method.
ParameterMap	For outbound calls launched by the Application Interface web service, this object contains all of the parameters encoded in the session.values.avaya parameters field.

Additional properties

The CCXML browser also maintains current data in the connections, conferences and dialogs objects available within the session namespace. For details about these objects, see the W3C CCXML Version 1.0, W3C Working Draft dated 19 January 2007.

LaunchEmail method

This method starts the specified email type application and if successful, returns the Experience Portal session ID for the new session.

Note:

The launched applications is responsible for sending the email message using the information passed to the application.

Important:

For more details on the return values, see Return values on page 681.

Parameters

Parameter	Type	Description
to	String	Email address that is configured on the system and can be used by the application being launched.
from	String	Multiple values, using a comma (,) as a delimiter, that can be used by an application. For example: john@abc.com,sam@abc.com,bob@abc.com.
cc	String	Email CC. You can specify multiple values using a comma (,) as a delimiter. For example: john@abc.com,sam@abc.com,bob@abc.com. (Optional)
bcc	String	Email BCC. You can specify multiple values using a comma (,) as a delimiter. For example: john@abc.com,sam@abc.com,bob@abc.com. (Optional)
subject	String	The subject of the message. (Optional)
body	String	Body of the message. (Optional)
attachments	String	A list of attachment URLs, separated by a comma (,). (Optional)
headers	String	Contains name value in this format: name=value;name=value with a semicolon (;) as delimiter. Content-Type, Reply-To etc can be specified as headers. (optional)
applicationName	String	Name of the application to be launched. Contains zone information in the format zoneId:appName. **Important:** The applicationName must match the name that was specified when the application was added to Avaya Experience Portal through the EPM. For an application that is assigned to a non-default zone, include the zone information using the format: `ZoneId:applicationName` You can view all application names on the Applications page. You can retrieve the zone Id information using the getZoneInfo method of the Management Interface web service.

Table continues…

Parameter	Type	Description
appParameters	String	Parameters to be send to Orchestration Designer App. Contains name value in this format: name=value;name=; with ; as delimiter. (optional)
emailParameters	String	Parameters to be send to Orchestration Designer App. Contains name value in this format: name=value;name=; with ; as delimiter. See table below for parameters. (optional)
ucid	String	Unique customer ID. (Optional)
parentID	String	Caller's session ID. (Optional)
requestTimeout	Integer	Time to wait for the request to finish. (In seconds)

Data returned

Parameter	Type	Description
sessionID_returned	String	If the request completes successfully, this return value contains the session ID string

LaunchSMS method

This method starts the specified SMS type application and if successful, returns the Experience Portal session ID for the new session.

Note:

The launched applications is responsible for sending the SMS message using the information passed to the application.

Important:

The return values are described Return values on page 681.

Parameters

Parameter	Type	Description
to	String	Short code that is configured on the system and can be used by the application being launched.
from	String	Multiple values using a comma (,) as a delimiter, that can be used by an application. For example: 12345,23456,54321. (Mandatory)
message	String	Message to send. (Optional)

Table continues…

Parameter	Type	Description
applicationName	String	Name of the application to be launched. Contains zone information in the format: ZoneId:appName. **Important:** The applicationName must match the name that was specified when the application was added to Avaya Experience Portal through the EPM. For an application that is assigned to a non-default zone, include the zone information using the format: `ZoneId:applicationName` You can view all application names on the Applications page. You can retrieve the zone Id information using the getZoneInfo method of the Management Interface web service.
appParameters	String	Parameters to be sent to the Orchestration Designer app. Contains name value using semicolon (;) as delimiter, in the following format: name=value;name=;. (Optional)
smsParameters	String	Parameters to be sent to o SMSC. Contains name value using semicolon (;) as delimiter, in the following format: name=value;name=;. (Optional)
ucid	String	Unique caller ID. (Optional)
parentID	String	Caller's session ID. (Optional)
requestTimeout	Integer	Time to wait for the request to finish. (In seconds)

Data returned

Parameter	Type	Description
sessionID_returned	String	If the request completed successfully, this return value contains the session ID string.

LaunchHTML method

This method starts the specified HTML type application and if successful, returns the following:

- Experience Portal session ID for the new session
- The session ID created on the application server
- The application URI which the HTML application was launched

Important:

The return values are described in Return values on page 681.

Parameters

Parameter	Type	Description
applicationName	String	Name of the application to be launched. Contains zone information in the following format: ZoneId:appName. **Important:** The applicationName must match the name that was specified when the application was added to Avaya Experience Portal through the EPM. For an application that is assigned to a non-default zone, include the zone information using the format: `ZoneId:applicationName` You can view all application names on the Applications page. You can retrieve the zone Id information using the getZoneInfo method of the Management Interface web service.
appParameters	String	Parameters to be sent to the launched application. Contains name value using semicolon (;) as delimiter, in the following format: name=value;name=;. (Optional) If a value contains a semicolon (“;”) it needs to be escaped using backslash (“\”).
ucid	String	Unique caller ID. (Optional)
parentID	String	Caller’s session ID. (Optional)
requestTimeout	Integer	Time to wait for the request to finish. (In seconds) This value must be in the range 1-60 (inclusive).

Data returned

Parameter	Type	Description
sessionID_htlpApp	String	If the request completed successfully, this return value contains the Experience Portal session ID that was created when the application was launched.
sessionID_AppServer	String	If the request completed successfully, this return value contains the Session ID that was created on the application server.
applicationURL	String	If the request completed successfully, this return value contains the application URI against which the HTML application was launched.

LaunchVXML method

This method initiates an outbound call on an available MPP, then starts the specified VoiceXML application. If successful, it returns the:

- Experience Portal session ID for the new session
- Total number of outbound resources available, both used and unused
- Total number of unused SIP outbound resources
- Total number of unused H.323 outbound resources

The actual launch of the VoiceXML application is handled by the default CCXML page, which is also responsible for returning success or failure back to the Application Interface web service.

When the VoiceXML application is invoked, the first VoiceXML page is prepared. If this succeeds, the outbound call is placed by the system. If the call connects and the dialog starts without error, then the VoiceXML application returns a successful launch code. Otherwise, the application returns an appropriate error code.

Note:

If the initial VoiceXML page cannot be prepared for any reason, the Application Interface web service does not place the outbound call. Therefore a customer will never be bothered by an outbound call that cannot possibly start correctly.

For information about the status codes returned by the CCXML page, see Returning the status of a LaunchCCXML request on page 663.

Note:

If a CCXML application launches multiple VoiceXML applications, each of these applications can use a different speech server. Prior to Experience Portal 7.0, multiple applications used only one speech server. This feature comes into play if you have different languages loaded onto different speech servers.

When a CCXML application launches a VoiceXML dialog by name, the configured ASR or TTS is used. If the configured ASR or TTS changes, the current ASR or TTS resources are released and new resources are seized before the dialog starts.

For example, a CCXML application can launch a dialog with English ASR or TTS. The application can determine that the caller prefers Spanish and so, the second dialog is launched with Spanish ASR or TTS.

Important:

The return values are described Return values on page 681.

Parameters

Parameter	Type	Description
toURI	String	The number or destination to be contacted by the outbound application. This parameter can be prefixed with one of the following strings: • `tel`: Use this for an H.323 or SIP connection, or a mix of both. • `sip`: Use this for a standard SIP connection. • `sips`: Use this for a secure SIP connection.
fromURI	String	Calling address information to pass with the outbound call.
applicationName	String	Name of the VoiceXML application to run once the outbound call has connected. **Important:** The applicationName must match the name that was specified when the application was added to Avaya Experience Portal through the EPM. For an application that is assigned to a non-default zone, include the zone information using the format: `ZoneId:applicationName` You can view all application names on the Applications page. You can retrieve the zone Id information using the getZoneInfo method of the Management Interface web service.
applicationURL	String	Parameters that should be appended to URL specified for the application in the EPM. This allows you to invoke the application with different arguments as needed.

Table continues…

Parameter	Type	Description
parameters	String	One or more name-value variable pairs that will be passed to the VoiceXML application when it is invoked. Each pair should be in the format `parametername=value`, and multiple pairs should be separated by a `;` (semi-colon). **Note:** When the web service passes the parameter to the application, it appends the namespace `session.avaya.telephone`. Therefore, the variable should be referenced in your application as `session.avaya.telephone.`*`parametername`*. For example, if you specify `UserCounter=0` in the web service, you would reference `session.avaya.telephone.UserCounter` in your application. **Tip:** If you want to enable call classification for this call, see Call classification with the LaunchVXML method on page 672.
uuiInfo	String	The Application Interface web service passes any information in this parameter to the platform telephony layer included in the outbound call.
connectTimeoutSecs	Integer	The maximum amount of time, in seconds, to wait for the outbound call to be connected. Enter a value between 0 and 59. If this parameter is set to 0 (zero) or omitted, Experience Portal uses the default value of 120 seconds.
zone	String	This is the zone name where request should be directed. (Optional).

Data returned

Parameter	Type	Description
sessionID_returned	String	If the VoiceXML application connected successfully, the Application Interface web service sets this return value to the session ID Experience Portal assigned to the new CCXML session.
totalRes_returned	Integer	Total number of outbound resources available, both used and unused.
unusedSIP_returned	Integer	Total number of unused SIP outbound resources.
unusedH323_returned	Integer	Total number of unused H.323 outbound resources.

Note:

If zones are enabled, the resource information returned is the information for the zone specified in the request. If no zone is specified, the resource information returned is the information for the default zone.

Call classification with the LaunchVXML method

Call classification allows the VoiceXML application to return the appropriate status code based on whether a human, an answering machine, or a fax machine answers an outbound call.

Call classification parameters for the LaunchVXML method

The following call classification name-value pairs can be passed as parameters with the LaunchVXML method. For both parameters the default is `false`, which means that you must specify the name-value pair in order to enable the associated functionality.

Name-value pair	Description
`enable_call_classification=true`	This required parameter enables call classification.
`detect_greeting_end=true`	This optional parameter instructs the VoiceXML application to identify the end of a recorded greeting if an answering machine answers the outbound call.
`call_classification_recorded_msg_timeout = in mili secs (e.g. 30000 is 30 sec)`	This Optional parameter is to set wait timeout for “end of recorded greeting”, if an answering machine answers the outbound call. Default is 30 sec.
`call_classification_connectWhen = ( OnConnect or OnProgress)`	This optional parameter is to start the CPA engine (call classification) on either OnConnect or OnProgress. By default it is set to OnProgress. In case the engine is started before connect, early media will also be captured for call classification.
`call_classification_timeout=value`	Timeout for outbound call classification from engine. This optional parameter indicates how long the call classification function will run if it is unable to determine the classification. The value specified should be in milliseconds. If the value is not provided, the default timeout is 20 sec.

Call classifications

If you enable call classification, the VoiceXML application sends one of the following classifications to the application server using the query arguments on the URL:

Classification	Description
`live_voice`	If a human being answers the call, the application starts the previously-prepared VoiceXML dialog. **Note:** This is the default classification assigned to the VoiceXML session before the call is placed. If a human being does not answer the call, this classification must be changed.
`recorded_msg`	If the LaunchVXML method was invoked with `detect_greeting_end=false` or if the `detect_greeting_end` parameter was not specified and an answering machine answers the call, the application terminates the previously-prepared VoiceXML dialog and starts a new dialog by sending the classification `recorded_msg` to the application server.
`msg_end`	If the LaunchVXML method was invoked with `detect_greeting_end=true` and an answering machine answers the call, the application terminates the previously-prepared VoiceXML dialog and starts a new dialog by sending the classification `msg_end` to the application server.
`fax_answer_tone`	If a fax machine answers the call, the application terminates and returns the error code `fax detected (8206)` to the Application Interface web service.
`timeout`	If the VoiceXML application does not send a classification change message to the CCXML page within a given period of time, the CCXML applications assumes that a live person has answered the phone and it starts the previously-prepared VoiceXML dialog.
`*`	All other classifications result in the status code for `no answer ()` being returned the Application Interface web service.

VoiceXML session properties

At the start of a VoiceXML session, the Application Interface web service places several properties in the `session.connection`, `session.avaya.telephone`, and `session.telephone` namespaces.

session.connection namespace properties

Property	Description
`call_tag`	The unique identifier for the session assigned by the Media Server.
`ccxml.namelist.*`	If the CCXML application passes data to the VoiceXML dialog at the beginning of the session, this array variable contains a list of the variable names passed by the CCXML application.

Table continues…

Property	Description
ccxml.values.*	If the CCXML application passes data to the VoiceXML dialog at the beginning of the session, this array variable contains a list of the values for the variable names contained in ccxml.namelist.*.
local.uri	The Dialed Number Identification Service (DNIS) associated with the call that triggered the VoiceXML session.
protocol.name	The telephony protocol name. The options are: • h323 • sip
remote.uri	The Automatic Number Identification (ANI) associated with the call that triggered the VoiceXML session.

session.avaya namespace properties

Note:

For convenience, several of the session.avaya namespace properties are the same as the session.connection namespace properties.

Property	Description
telephone.ani	The Automatic Number Identification (ANI) associated with the call that triggered the VoiceXML session.
telephone.call_tag	The unique identifier for the session assigned by the Media Server.
telephone.called_extension	For calls using an H.323 connection, this is the telephony port servicing the VoiceXML session.
telephone.callid	The unique identifier for the call assigned by the Media Server.
telephone.channel	This property is reserved for future use.
telephone.dnis	The Dialed Number Identification Service (DNIS) associated with the call that triggered the VoiceXML session.
telephone.startPage	The full URL, including any query string parameters, used to fetch the first page of the VoiceXML session.
uui.mode	The User-to-User Interface (UUI) mode under which this application is operating. The options are: • shared • service provider
uui.shared[]	If uui.mode is shared, this property contains an array of the shared UUI data pieces in name-value format.

session.telephone namespace properties

Note:

For convenience, most of the session.telephone namespace properties are the same as the session.connection and session.avaya namespace properties.

Property	Description
ani	The Automatic Number Identification (ANI) associated with the call that triggered the VoiceXML session.
dnis	The Dialed Number Identification Service (DNIS) associated with the call that triggered the VoiceXML session.
call_tag	The unique identifier for the session assigned by the Media Server.
called_extension	For calls using an H.323 connection, this is the telephony port servicing the VoiceXML session.
callid	The unique identifier for the call assigned by the Media Server.
channel	This property is reserved for future use.
startPage	The full URL, including any query string parameters, used to fetch the first page of the VoiceXML session.
*	This property contains any parameters passed to the Application Interface web service through the LaunchVXML method.

QueryResources method

This method takes a snapshot of the current outbound usage across all MPPs in the Experience Portal system and returns:

- Total number of outbound resources available, both used and unused
- Total number of unused SIP outbound resources
- Total number of unused H.323 outbound resources

  If zones are enabled, the returned resource information is the information for all MPPs with the zone specified in the request, or for the default zone if no zone was specified.

You can use this method to determine the approximate availability of outbound resources before you use the LaunchCCXML or LaunchVXML method to start a new outbound session.

Keep in mind, however, that system usage is extremely dynamic. The QueryResources method only returns a snapshot of the current usage. It does not look for upcoming outbound calls or try to determine whether another LaunchCCXML or LaunchVXML command has just started and is about to claim one or more outbound resources.

In addition, this method reports the total number of outbound resources available across all MPPs in the Experience Portal system, or all MPPs in the specified zone, if zones are enabled. Each application only has access to the available ports on the MPP to which it is assigned. If your site has multiple MPPs, that means any single application will probably not have access to the total number of resources returned by this method. For more information on using applications that launch multiple outgoing calls, see Best practices on page 654.

Important:

The return values are described Return values on page 681.

Data Returned

Name	Type	Description
totalRes_returned	Integer	Total number of outbound resources available, both used and unused.
unusedSIP_returned	Integer	Total number of unused SIP outbound resources.
unusedH323_returned	Integer	Total number of unused H.323 outbound resources.

Note:

If zones are enabled, the resource information returned is the information for the zone specified in the request. If no zone is specified, the resource information returned is the information for the default zone.

SendCCXMLEvent method

This method instructs the MPP to dispatch a user-named event with an accompanying parameter string to the specified CCXML session.

Important:

The return values are described Return values on page 681.

Parameters

Name	Type	Description
sessionID	String	The session ID of an existing CCXML session. This parameter must match exactly the session ID assigned by Avaya Experience Portal when the session started.
eventName	String	The user-defined event that the MPP should send to the session.
parameters	String	Any user-defined parameters that the MPP should pass along with the event to the CCXML session.

SendEmail method

This method starts the specified email type application and if successful, returns the Experience Portal session ID for the new session.

Important:

The return values are described Return values on page 681.

Parameters

Parameter	Type	Description
from	String	Email address used to send the message
to	String	Target of the message. You can specify multiple values, using a comma (,) as a delimiter. For example: john@abc.com,sam@abc.com,bob@abc.com.
cc	String	Email CC. You can specify multiple values, using a comma (,) as a delimiter. For example: john@abc.com,sam@abc.com,bob@abc.com. (Optional)
bcc	String	Email BCC. You can specify multiple values, using a comma (,) as a delimiter. For example: john@abc.com,sam@abc.com,bob@abc.com. (Optional)
subject	String	The subject of the message. (Optional)
body	String	Body of the message. (Optional)
attachments	String	A list of attachment URLs, separated by a comma (,). (Optional)
headers	String	Contains name value in this format: name=value;name=value with a semicolon (;) as delimiter. Content-Type, Reply-To etc can be specified as headers. (optional)
applicationName	String	Name of the application to be launched. Contains zone info in the format zoneId:appName.
emailParameters	String	Parameters to be send to Orchestration Designer App. Contains name value in this format: name=value;name=; with ; as delimiter. See table below for parameters. (optional)
ucid	String	Unique customer ID. (Optional)
sessionID	String	Caller's session ID.

Table continues…

Parameter	Type	Description
requestTimeout	String	Time to wait for the request to finish. (In seconds)

Data returned

Parameter	Type	Description
messageID_returned	String	If the request completes successfully, this return value contains the session ID string

SendSMS method

This method sends an SMS message, and if successful, returns the Experience Portal message ID for the new session.

Important:

The return values are described Return values on page 681.

Parameters

Parameter	Type	Description
from	String	Short code used to send the message.
to	String	Target of the message. You can specify multiple values using a comma (,) as a delimiter. For example: 12345,23456,54321.
message	String	Message to send.
applicationName	String	name of the application to be launched. Contains zone information in the format: ZoneId:appName.
smsParameters	String	Parameters to be sent to o SMSC. Contains name value using semicolon (;) as delimiter, in the following format: name=value;name=;. (Optional)
ucid	String	Unique caller ID. (Optional)
sessionID	String	Caller’s session ID. (Optional)
requestTimeout	Integer	Time to wait for the request to finish. (In seconds)

Data returned

Parameter	Type	Description
sessionID_returned	String	If the request completed successfully, this return value contains the session ID.

Additional parameters in the LaunchEmail and SendEmail methods

Parameter	Description
CC	The CC email address. You can separate multiple email addresses by comma (,).
BCC	The BCC email address. You can separate multiple email addresses by comma (,).
ReplyTo	The ReplyTo address to be set in the email.
Attachment	The attachment list. You can separate multiple attachment files by comma (,).
RegisteredDelivery	Demanding a registered delivery for the request. Value should be one of the SMTP notification value: -1 (Notify Never), 1 (Notify Success), 2 (Notify Failure), 4 (Notify Delay)
Priority	Assigns a priority level, in the range of to >=1 and <=5, to the message. The "X-Priority" value in the email is set accordingly so that email importance is honored by the SMTP servers. 1 indicates high priority and 5 as low. If none specified, set as 0 – no priority marking for the email.
ContentType	Email content type: text/plain or text/html.
Charset	The charset of the email.
DisplayName	Display name to be used for the email from address.

Additional parameters in the LaunchSMS and SendSMS methods

Parameter	Description
RegisteredDelivery	Demanding a registered delivery for the request. Accepted values: 0 and 1. 1= Requires a receipt; 0 (default) = No delivery receipt.
DataCoding	Defines the encoding scheme of the short message user data. Default is 0 to use the SMSC default Alphabet. Refer to the SMPP specifications for details (Short Message Peer to Peer Protocol Specification v3.4; section: 5.2.19).
Priority	Designates a priority level to the message. 4 priority levels are supported (0 being lowest and 3 being highest). Default to 0. Refer to the SMPP specification document section 5.2.14 for more details.
ValidityPeriod	Sets the validity period for this message, so that SMSC can ignore the message if it can't deliver within this time. Default to 0 for SMSC default validity period. Refer to the SMPP specification document section 5.2.16 & 7.1.1.
ScheduleDelivery	Indicates that SMSC need to schedule the message for delivery at the time specified. Default to 0 for immediate delivery.
Encoding	Defines the character encoding scheme of the message user data. Default is to use ASCII. For the list of character encoding, refer: `http://docs.oracle.com/javase/1.3/docs/guide/intl/encoding.doc.html`
Language	The SMPP language indicator of the short message (CMT-136 standard). Refer to the SMPP specification for details: (Short Message Peer to Peer Protocol Specification v3.4; section: 5.3.2.19).
UserMessageReference	A custom reference id that can be submitted along with the message that could be used by the application to build context and further interpretation. Optional parameter; not all SMSC vendor required to support.

Return Values

The following table describes the return values that the application interface web service receives when the system process the web services request:

Return value		Attributes	Condition	Get Status	Get StatusEx	Launch CCXML	Launch Email	Launch SMS	Launch VXML	Query Resources	Send CCXML Event	Send Email	Send SMS	LaunchHTML
hex														
0x0	0	Success	The web service successfully completed the request.	X	X	X	X	X	X	X	X	X	X	X
0x1	1	Failure	The web service was unable to complete the request. Verify that the EPM and MPP servers are communicating properly and retry the request.	X	X	X	X	X	X	X	X	X	X	
0x2	2	No resource	No resources are available to process the request.			X	X	X	X			X	X	
0x3	3	No User Access	The user is not allowed to access the web service.			X	X	X	X		X	X	X	X
0x4	4	No App Access	The user is not allowed to access the specified application.			X	X	X	X			X	X	X
0x10	16	Busy	The destination named in the toURI parameter is busy and cannot be reached.						X					
0x11	17	No Answer	The destination named in the toURI parameter did not answer within the amount of time specified in the connectTimeoutSecs parameter.						X					
0x12	18	Network Refusal	The outbound call was rejected due to a network error.						X					
0x13	19	Failed	The application was not started due to a problem with the application server.			X								
0x14	20	Timeout	The operation did not get a response within the amount of time specified in the timeout parameter.			X	X	X	X			X	X	
0x15	21	No Response	The session ended and the VoiceXML/CCXML page did not return a response to Experience Portal. This can happen if the VoiceXML/CCXML page is not designed to send a response, or if the page has an error and exits before the code that sends the response executes.			X			X					
0x16	22	Fax Detected	The outbound number is associated with a fax machine.			X			X					
0x20	32	Invalid URI	The toURI parameter contains an invalid URI specification.			X			X					
0x21	33	Unknown Application	The applicationName parameter does not match one of the application names configured though the EPM. You can view all application names on the Applications page.			X	X	X	X			X	X	X
0x22	34	Invalid URL	The applicationURL parameter contains an invalid URL specification.			X			X					

Return value		Attributes	Condition	Get Status	Get StatusEx	Launch CCXML	Launch Email	Launch SMS	Launch VXML	Query Resources	Send CCXML Event	Send Email	Send SMS	LaunchHTML
0x23	35	Invalid Session ID	No current session ID matched the one specified in the sessionID parameter. Make sure that the session ID is correct and that the session is still running on the MPP.								X	X	X	
0x24	36	Invalid Connect Timeout	The Connect timeout in LaunchVXML request (connectTimeoutSecs) is too long. The value specified must be less than the MaxLaunchVXMLConnectTimeout parameter in the voiceportal.properties file on Experience Portal.						X					
0x25	37	Invalid Zone	Invalid Zone specified.			X	X	X	X	X		X	X	X
0x30	48	MPP Down	The MPP service is not running and cannot service the request.								X			
0x31	49	MPP Stopped	The MPP service is running, but the MPP is not currently processing calls.								X			
0x32	50	MPP WS Failure	The required out call web service is not running on any MPP in the system. Therefore the call cannot be connected. Messages from the Application Interface web service appear in the OCWSServer.log file on the MPP, which is accessible from the Media Server Service Menu Log Directories page.			X	X	X	X		X	X	X	
0x43	67	Invalid Timeout	Invalid timeout specified				X	X				X	X	X
0x44	68	Invalid To	Invalid data in the "to" field									X	X	
0x45	69	Invalid From	Invalid data in the "from" field				X						X	
0x46	70	Invalid Message	Invalid data in the message field										X	
0x47	71	Invalid Request Data	Invalid data in the request				X	X				X	X	X
0x57	87	Exception from HTMLLauncher	The HTML Launcher generated an exception											X
0x58	88	HTMLLauncher Failure	The HTML Launcher generated a failure											X
0x59	89	HTMLLauncher returned unknown application	The HTML Launcher could not locate the specified application											X
0x5A	90	HTMLLauncher returned unspecified error	The HTML Launcher returned an error that is unspecified.											X

Return value		Attributes	Condition	Get Status	Get StatusEx	Launch CCXML	Launch Email	Launch SMS	Launch VXML	Query Resources	Send CCXML Event	Send Email	Send SMS	LaunchHTML
0x5B	91	HTML Launcher returned Not Licensed	The HTML Launcher was unable to launch the application due to licensing.											X
0x102	258	Fatal Error	The web service is in an error state that requires a restart of the EPM service.	X	X	X	X	X	X	X	X	X	X	
0x103	259	Not Initialized	The web service is not initialized and unable to accept requests.	X	X	X	X	X	X	X	X	X	X	
0x104	260	Shutting Down	The web service is shutting down and no new requests are being accepted.	X	X	X	X	X	X	X	X	X	X	
0x201	513	Network Failed before Connection Completed	Represents that the network failed before the connection was completed.			X			X					
0x202	514	Near End Disconnect before Connection Completed	Represents that the caller disconnected the call before the called number was connected.			X			X					
0x203	515	Near End Disconnect before Connection Completed	Far End Disconnected before the connection was completed.			X			X					
0x204	516	Transferred before Connection Completed	Represents that the call is transferred before the connection was completed.			X			X					
0x205	517	Unknown Failure before Connection Completed	Represents that the call cannot be completed due to unknown reason.			X			X					
0x206	518	Call Disconnected before Application Started	Represents that the call is disconnected before the application was started.						X					

Sample Application Interface web service WSDL file

The following is an example of the Application Interface web service WSDL file. The actual file is installed on the server that is running the EPM software. For details about accessing this file, see Configuring the Application Interface web service on page 656.

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:ns1="http://org.apache.axis2/xsd"
xmlns:ns="http://xml.avaya.com/ws/VPAppIntf/VoicePortal"
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
xmlns:ax25="http://services.vp.avaya.com/xsd"
xmlns:http="http://schemas.xmlsoap.org/wsdl/http/" xmlns:ax21="http://rmi.java/xsd"
xmlns:ax22="http://io.java/xsd" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
targetNamespace="http://xml.avaya.com/ws/VPAppIntf/VoicePortal">
    <wsdl:types>
        <xs:schema xmlns:ax23="http://io.java/xsd" attributeFormDefault="qualified"
elementFormDefault="qualified" targetNamespace="http://rmi.java/xsd">
            <xs:import namespace="http://io.java/xsd"/>
            <xs:complexType name="RemoteException">
                <xs:complexContent>
                    <xs:extension base="ax23:IOException">
                        <xs:sequence>
                            <xs:element minOccurs="0" name="cause" nillable="true"
type="xs:anyType"/>
                            <xs:element minOccurs="0" name="message" nillable="true"
type="xs:string"/>
                        </xs:sequence>
                    </xs:extension>
                </xs:complexContent>
            </xs:complexType>
        </xs:schema>
        <xs:schema attributeFormDefault="qualified" elementFormDefault="qualified"
targetNamespace="http://services.vp.avaya.com/xsd">
```

```
            <xs:complexType name="SendCCXMLEventRequest">
                <xs:sequence>
                    <xs:element minOccurs="1" name="eventName" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="parameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="sessionID" nillable="false"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="SendCCXMLEventResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="retCode" type="xs:int"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="QueryResourcesRequest">
                <xs:sequence>
                    <xs:element minOccurs="0" name="queryResourcesRequestUnused"
type="xs:int"/>
                    <xs:element minOccurs="0" name="zone" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="QueryResourcesResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="totalRes_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="unusedH323_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="unusedSIP_returned" type="xs:int"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="LaunchVXMLRequest">
                <xs:sequence>
                    <xs:element minOccurs="1" name="applicationName" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="applicationURL" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="connectTimeoutSecs" type="xs:int"/>
                    <xs:element minOccurs="1" name="fromURI" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="parameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="toURI" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="uuiInfo" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="zone" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="LaunchVXMLResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="sessionID_returned"
nillable="false" type="xs:string"/>
                    <xs:element minOccurs="1" name="totalRes_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="unusedH323_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="unusedSIP_returned" type="xs:int"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="LaunchCCXMLRequest">
                <xs:sequence>
                    <xs:element minOccurs="1" name="applicationName" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="applicationURL" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="launchTimeout" type="xs:int"/>
```

```
                    <xs:element minOccurs="0" name="parameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="toURI" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="uuiInfo" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="zone" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="LaunchCCXMLResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="sessionID_returned"
nillable="false" type="xs:string"/>
                    <xs:element minOccurs="1" name="totalRes_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="unusedH323_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="unusedSIP_returned" type="xs:int"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="LaunchSMSRequest">
                <xs:sequence>
                    <xs:element minOccurs="0" name="appParameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="applicationName" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="from" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="message" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="parentID" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="requestTimeout" type="xs:int"/>
                    <xs:element minOccurs="0" name="smsParameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="to" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="ucid" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="LaunchSMSResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="sessionID_returned"
nillable="false" type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="SendSMSRequest">
                <xs:sequence>
                    <xs:element minOccurs="1" name="applicationName" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="1" name="from" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="1" name="message" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="1" name="requestTimeout" type="xs:int"/>
                    <xs:element minOccurs="1" name="sessionID" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="smsParameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="to" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="ucid" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
```

```
            <xs:complexType name="SendSMSResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="messageID_returned"
nillable="false" type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="LaunchEmailRequest">
                <xs:sequence>
                    <xs:element minOccurs="0" name="appParameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="applicationName" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="attachments" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="bcc" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="body" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="cc" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="emailParameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="from" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="headers" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="parentID" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="requestTimeout" type="xs:int"/>
                    <xs:element minOccurs="0" name="subject" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="to" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="ucid" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="LaunchEmailResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="sessionID_returned"
nillable="false" type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="SendEmailRequest">
                <xs:sequence>
                    <xs:element minOccurs="1" name="applicationName" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="attachments" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="bcc" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="body" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="cc" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="emailParameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="from" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="headers" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="requestTimeout" type="xs:int"/>
                    <xs:element minOccurs="1" name="sessionID" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="1" name="subject" nillable="false"
```

```
type="xs:string"/>
                    <xs:element minOccurs="1" name="to" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="ucid" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="SendEmailResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="messageID_returned"
nillable="false" type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
             <xs:complexType name="LaunchHtmlRequest">
                <xs:sequence>
                    <xs:element minOccurs="0" name="appParameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="applicationName" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="parentID" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="requestTimeout" type="xs:int"/>
                    <xs:element minOccurs="0" name="ucid" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="LaunchHtmlResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="applicationURL" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="1" name="sessionID_AppServer"
nillable="false" type="xs:string"/>
                    <xs:element minOccurs="1" name="sessionID_htmlApp" nillable="false"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="LaunchAppRequest">
                <xs:sequence>
                    <xs:element minOccurs="1" name="applicationName" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="1" name="from" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="1" name="genericAppType" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="parameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="0" name="parentID" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="requestTimeout" type="xs:int"/>
                    <xs:element minOccurs="1" name="to" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="ucid" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="LaunchAppResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="ID_returned" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="1" name="parameters" nillable="false"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="GetStatusExRequest">
                <xs:sequence>
```

```
                    <xs:element minOccurs="0" name="getStatusExRequestUnused"
type="xs:int"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="GetStatusExResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="avgMPPHops_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="iCCXMLEventsSent_returned"
type="xs:int"/>
                    <xs:element minOccurs="1" name="iCCXMLRequestsProcessed_returned"
type="xs:int"/>
                    <xs:element minOccurs="1"
name="iLaunchAppRequestsProcessed_returned" type="xs:int"/>
                    <xs:element minOccurs="1"
name="iLaunchEmailRequestsProcessed_returned" type="xs:int"/>
                    <xs:element minOccurs="1"
name="iLaunchSmsRequestsProcessed_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="iSIPRequestsProcessed_returned"
type="xs:int"/>
                    <xs:element minOccurs="1" name="iSendAppRequestsProcessed_returned"
type="xs:int"/>
                    <xs:element minOccurs="1"
name="iSendEmailRequestsProcessed_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="iSendSmsRequestsProcessed_returned"
type="xs:int"/>
                    <xs:element minOccurs="1" name="iTELRequestsProcessed_returned"
type="xs:int"/>
                    <xs:element minOccurs="1" name="iVXMLRequestsProcessed_returned"
type="xs:int"/>
                    <xs:element minOccurs="1" name="lastRequestDateTime_returned"
nillable="false" type="xs:dateTime"/>
                    <xs:element minOccurs="1" name="maxMPPHops_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="minMPPHops_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="serviceStartedDateTime_returned"
nillable="false" type="xs:dateTime"/>
                    <xs:element minOccurs="1" name="vpmsSoftwareVersion_returned"
nillable="false" type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="SendAppRequest">
                <xs:sequence>
                    <xs:element minOccurs="1" name="applicationName" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="1" name="from" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="1" name="genericAppType" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="parameters" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="requestTimeout" type="xs:int"/>
                    <xs:element minOccurs="0" name="sessionID" nillable="true"
type="xs:string"/>
                    <xs:element minOccurs="1" name="to" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="0" name="ucid" nillable="true"
type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="SendAppResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="ID_returned" nillable="false"
type="xs:string"/>
                    <xs:element minOccurs="1" name="parameters" nillable="false"
type="xs:string"/>
                </xs:sequence>
```

```
            </xs:complexType>
            <xs:complexType name="GetStatusRequest">
                <xs:sequence>
                    <xs:element minOccurs="0" name="getStatusRequestUnused"
type="xs:int"/>
                </xs:sequence>
            </xs:complexType>
            <xs:complexType name="GetStatusResponse">
                <xs:sequence>
                    <xs:element minOccurs="1" name="avgMPPHops_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="iCCXMLEventsSent_returned"
type="xs:int"/>
                    <xs:element minOccurs="1" name="iCCXMLRequestsProcessed_returned"
type="xs:int"/>
                    <xs:element minOccurs="1" name="iSIPRequestsProcessed_returned"
type="xs:int"/>
                    <xs:element minOccurs="1" name="iTELRequestsProcessed_returned"
type="xs:int"/>
                    <xs:element minOccurs="1" name="iVXMLRequestsProcessed_returned"
type="xs:int"/>
                    <xs:element minOccurs="1" name="lastRequestDateTime_returned"
nillable="false" type="xs:dateTime"/>
                    <xs:element minOccurs="1" name="maxMPPHops_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="minMPPHops_returned" type="xs:int"/>
                    <xs:element minOccurs="1" name="serviceStartedDateTime_returned"
nillable="false" type="xs:dateTime"/>
                    <xs:element minOccurs="1" name="vpmsSoftwareVersion_returned"
nillable="false" type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
        </xs:schema>
        <xs:schema attributeFormDefault="qualified" elementFormDefault="qualified"
targetNamespace="http://io.java/xsd">
            <xs:complexType name="IOException">
                <xs:sequence/>
            </xs:complexType>
        </xs:schema>
        <xs:schema xmlns:ax26="http://services.vp.avaya.com/xsd" xmlns:ax24="http://
rmi.java/xsd" attributeFormDefault="qualified" elementFormDefault="qualified"
targetNamespace="http://xml.avaya.com/ws/VPAppIntf/VoicePortal">
            <xs:import namespace="http://rmi.java/xsd"/>
            <xs:import namespace="http://services.vp.avaya.com/xsd"/>
            <xs:element name="VPAppIntfServiceRemoteException">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="RemoteException"
nillable="true" type="ax24:RemoteException"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="sendCCXMLEvent">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:SendCCXMLEventRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="sendCCXMLEventResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:SendCCXMLEventResponse"/>
                    </xs:sequence>
                </xs:complexType>
```

```
            </xs:element>
            <xs:element name="queryResources">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:QueryResourcesRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="queryResourcesResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:QueryResourcesResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="launchVXML">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:LaunchVXMLRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="launchVXMLResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:LaunchVXMLResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="launchCCXML">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:LaunchCCXMLRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="launchCCXMLResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:LaunchCCXMLResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="launchSMS">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:LaunchSMSRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="launchSMSResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:LaunchSMSResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
```

```
            <xs:element name="sendSMS">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:SendSMSRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="sendSMSResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:SendSMSResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="launchEmail">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:LaunchEmailRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="launchEmailResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:LaunchEmailResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="sendEmail">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:SendEmailRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="sendEmailResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:SendEmailResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
             <xs:element name="launchHtml">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:LaunchHtmlRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="launchHtmlResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:LaunchHtmlResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="launchApp">
```

```
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:LaunchAppRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="launchAppResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:LaunchAppResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="getStatusEx">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:GetStatusExRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="getStatusExResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:GetStatusExResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="sendApp">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:SendAppRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="sendAppResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:SendAppResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="getStatus">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="args0" nillable="true"
type="ax25:GetStatusRequest"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="getStatusResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="0" name="return" nillable="true"
type="ax25:GetStatusResponse"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="getConversation">
                <xs:complexType>
```

```
                    <xs:sequence>
                        <xs:element minOccurs="1" name="args0" nillable="false"
type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="getConversationResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="1" name="return" nillable="false"
type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="createConversation">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="1" name="args0" nillable="false"
type="xs:string"/>
                        <xs:element minOccurs="1" name="args1" nillable="false"
type="xs:string"/>
                        <xs:element minOccurs="1" name="args2" type="xs:long"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="deleteConversation">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="1" name="args0" nillable="false"
type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="updateConversation">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="1" name="args0" nillable="false"
type="xs:string"/>
                        <xs:element minOccurs="1" name="args1" nillable="false"
type="xs:string"/>
                        <xs:element minOccurs="1" name="args2" type="xs:long"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="getConversationByAlias">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="1" name="args0" nillable="false"
type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="getConversationByAliasResponse">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="1" name="return" nillable="false"
type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="addConversationAlias">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element minOccurs="1" name="args0" nillable="false"
type="xs:string"/>
```

```
                        <xs:element minOccurs="1" name="args1" nillable="false"
type="xs:string" maxOccurs="3"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:schema>
    </wsdl:types>
    <wsdl:message name="queryResourcesRequest">
        <wsdl:part name="parameters" element="ns:queryResources"/>
    </wsdl:message>
    <wsdl:message name="queryResourcesResponse">
        <wsdl:part name="parameters" element="ns:queryResourcesResponse"/>
    </wsdl:message>
    <wsdl:message name="VPAppIntfServiceRemoteException">
        <wsdl:part name="parameters" element="ns:VPAppIntfServiceRemoteException"/>
    </wsdl:message>
    <wsdl:message name="launchCCXMLRequest">
        <wsdl:part name="parameters" element="ns:launchCCXML"/>
    </wsdl:message>
    <wsdl:message name="launchCCXMLResponse">
        <wsdl:part name="parameters" element="ns:launchCCXMLResponse"/>
    </wsdl:message>
    <wsdl:message name="launchAppRequest">
        <wsdl:part name="parameters" element="ns:launchApp"/>
    </wsdl:message>
    <wsdl:message name="launchAppResponse">
        <wsdl:part name="parameters" element="ns:launchAppResponse"/>
    </wsdl:message>
    <wsdl:message name="launchEmailRequest">
        <wsdl:part name="parameters" element="ns:launchEmail"/>
    </wsdl:message>
    <wsdl:message name="launchEmailResponse">
        <wsdl:part name="parameters" element="ns:launchEmailResponse"/>
    </wsdl:message>
    <wsdl:message name="launchHtmlRequest">
        <wsdl:part name="parameters" element="ns:launchHtml"/>
    </wsdl:message>
    <wsdl:message name="launchHtmlResponse">
        <wsdl:part name="parameters" element="ns:launchHtmlResponse"/>
    </wsdl:message>
    <wsdl:message name="sendAppRequest">
        <wsdl:part name="parameters" element="ns:sendApp"/>
    </wsdl:message>
    <wsdl:message name="sendAppResponse">
        <wsdl:part name="parameters" element="ns:sendAppResponse"/>
    </wsdl:message>
    <wsdl:message name="sendEmailRequest">
        <wsdl:part name="parameters" element="ns:sendEmail"/>
    </wsdl:message>
    <wsdl:message name="sendEmailResponse">
        <wsdl:part name="parameters" element="ns:sendEmailResponse"/>
    </wsdl:message>
    <wsdl:message name="getStatusRequest">
        <wsdl:part name="parameters" element="ns:getStatus"/>
    </wsdl:message>
    <wsdl:message name="getStatusResponse">
        <wsdl:part name="parameters" element="ns:getStatusResponse"/>
    </wsdl:message>
    <wsdl:message name="sendCCXMLEventRequest">
        <wsdl:part name="parameters" element="ns:sendCCXMLEvent"/>
    </wsdl:message>
    <wsdl:message name="sendCCXMLEventResponse">
        <wsdl:part name="parameters" element="ns:sendCCXMLEventResponse"/>
    </wsdl:message>
    <wsdl:message name="getStatusExRequest">
```

```
        <wsdl:part name="parameters" element="ns:getStatusEx"/>
    </wsdl:message>
    <wsdl:message name="getStatusExResponse">
        <wsdl:part name="parameters" element="ns:getStatusExResponse"/>
    </wsdl:message>
    <wsdl:message name="launchSMSRequest">
        <wsdl:part name="parameters" element="ns:launchSMS"/>
    </wsdl:message>
    <wsdl:message name="launchSMSResponse">
        <wsdl:part name="parameters" element="ns:launchSMSResponse"/>
    </wsdl:message>
    <wsdl:message name="launchVXMLRequest">
        <wsdl:part name="parameters" element="ns:launchVXML"/>
    </wsdl:message>
    <wsdl:message name="launchVXMLResponse">
        <wsdl:part name="parameters" element="ns:launchVXMLResponse"/>
    </wsdl:message>
    <wsdl:message name="sendSMSRequest">
        <wsdl:part name="parameters" element="ns:sendSMS"/>
    </wsdl:message>
    <wsdl:message name="sendSMSResponse">
        <wsdl:part name="parameters" element="ns:sendSMSResponse"/>
    </wsdl:message>
    <wsdl:message name="getConversationResponse">
        <wsdl:part name="parameters" element="ns:getConversationResponse"/>
    </wsdl:message>
    <wsdl:message name="createConversationRequest">
        <wsdl:part name="parameters" element="ns:createConversation"/>
    </wsdl:message>
    <wsdl:message name="getConversationRequest">
        <wsdl:part name="parameters" element="ns:getConversation"/>
    </wsdl:message>
    <wsdl:message name="deleteConversationRequest">
        <wsdl:part name="parameters" element="ns:deleteConversation"/>
    </wsdl:message>
    <wsdl:message name="updateConversationRequest">
        <wsdl:part name="parameters" element="ns:updateConversation"/>
    </wsdl:message>
    <wsdl:message name="getConversationByAliasRequest">
        <wsdl:part name="parameters" element="ns:getConversationByAlias"/>
    </wsdl:message>
    <wsdl:message name="getConversationByAliasResponse">
        <wsdl:part name="parameters" element="ns:getConversationByAliasResponse"/>
    </wsdl:message>
    <wsdl:message name="addConversationAliasRequest">
        <wsdl:part name="parameters" element="ns:addConversationAlias"/>
    </wsdl:message>
    <wsdl:portType name="VPAppIntfServicePortType">
        <wsdl:operation name="queryResources">
            <wsdl:input message="ns:queryResourcesRequest"
wsaw:Action="urn:queryResources"/>
            <wsdl:output message="ns:queryResourcesResponse"
wsaw:Action="urn:queryResourcesResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:queryResourcesVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="launchCCXML">
            <wsdl:input message="ns:launchCCXMLRequest" wsaw:Action="urn:launchCCXML"/>
            <wsdl:output message="ns:launchCCXMLResponse"
wsaw:Action="urn:launchCCXMLResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:launchCCXMLVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
```

```
        <wsdl:operation name="launchApp">
            <wsdl:input message="ns:launchAppRequest" wsaw:Action="urn:launchApp"/>
            <wsdl:output message="ns:launchAppResponse"
wsaw:Action="urn:launchAppResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:launchAppVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="launchEmail">
            <wsdl:input message="ns:launchEmailRequest" wsaw:Action="urn:launchEmail"/>
            <wsdl:output message="ns:launchEmailResponse"
wsaw:Action="urn:launchEmailResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:launchEmailVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="launchHtml">
            <wsdl:input message="ns:launchHtmlRequest" wsaw:Action="urn:launchHtml"/>
            <wsdl:output message="ns:launchHtmlResponse"
wsaw:Action="urn:launchHtmlResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:launchHtmlVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="sendApp">
            <wsdl:input message="ns:sendAppRequest" wsaw:Action="urn:sendApp"/>
            <wsdl:output message="ns:sendAppResponse"
wsaw:Action="urn:sendAppResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:sendAppVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="sendEmail">
            <wsdl:input message="ns:sendEmailRequest" wsaw:Action="urn:sendEmail"/>
            <wsdl:output message="ns:sendEmailResponse"
wsaw:Action="urn:sendEmailResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:sendEmailVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="getStatus">
            <wsdl:input message="ns:getStatusRequest" wsaw:Action="urn:getStatus"/>
            <wsdl:output message="ns:getStatusResponse"
wsaw:Action="urn:getStatusResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:getStatusVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="sendCCXMLEvent">
            <wsdl:input message="ns:sendCCXMLEventRequest"
wsaw:Action="urn:sendCCXMLEvent"/>
            <wsdl:output message="ns:sendCCXMLEventResponse"
wsaw:Action="urn:sendCCXMLEventResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:sendCCXMLEventVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="getStatusEx">
            <wsdl:input message="ns:getStatusExRequest" wsaw:Action="urn:getStatusEx"/>
            <wsdl:output message="ns:getStatusExResponse"
wsaw:Action="urn:getStatusExResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:getStatusExVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
```

```
        <wsdl:operation name="launchSMS">
            <wsdl:input message="ns:launchSMSRequest" wsaw:Action="urn:launchSMS"/>
            <wsdl:output message="ns:launchSMSResponse"
wsaw:Action="urn:launchSMSResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:launchSMSVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="launchVXML">
            <wsdl:input message="ns:launchVXMLRequest" wsaw:Action="urn:launchVXML"/>
            <wsdl:output message="ns:launchVXMLResponse"
wsaw:Action="urn:launchVXMLResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:launchVXMLVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="sendSMS">
            <wsdl:input message="ns:sendSMSRequest" wsaw:Action="urn:sendSMS"/>
            <wsdl:output message="ns:sendSMSResponse"
wsaw:Action="urn:sendSMSResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:sendSMSVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="deleteConversation">
            <wsdl:input message="ns:deleteConversationRequest"
wsaw:Action="urn:deleteConversation"/>
            <wsdl:output message="ns:null"
wsaw:Action="urn:deleteConversationResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:deleteConversationVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="getConversation">
            <wsdl:input message="ns:getConversationRequest"
wsaw:Action="urn:getConversation"/>
            <wsdl:output message="ns:getConversationResponse"
wsaw:Action="urn:getConversationResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:getConversationVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="updateConversation">
            <wsdl:input message="ns:updateConversationRequest"
wsaw:Action="urn:updateConversation"/>
            <wsdl:output message="ns:null"
wsaw:Action="urn:updateConversationResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:updateConversationVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="createConversation">
            <wsdl:input message="ns:createConversationRequest"
wsaw:Action="urn:createConversation"/>
            <wsdl:output message="ns:null"
wsaw:Action="urn:createConversationResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:createConversationVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="getConversationByAlias">
            <wsdl:input message="ns:getConversationByAliasRequest"
wsaw:Action="urn:getConversationByAlias"/>
            <wsdl:output message="ns:getConversationByAliasResponse"
wsaw:Action="urn:getConversationByAliasResponse"/>
```

```
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:getConversationByAliasVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
        <wsdl:operation name="addConversationAlias">
            <wsdl:input message="ns:addConversationAliasRequest"
wsaw:Action="urn:addConversationAlias"/>
            <wsdl:output message="ns:null"
wsaw:Action="urn:addConversationAliasResponse"/>
            <wsdl:fault message="ns:VPAppIntfServiceRemoteException"
name="VPAppIntfServiceRemoteException"
wsaw:Action="urn:addConversationAliasVPAppIntfServiceRemoteException"/>
        </wsdl:operation>
    </wsdl:portType>
    <wsdl:binding name="VPAppIntfServiceSoap11Binding"
type="ns:VPAppIntfServicePortType">
        <soap:binding transport="http://schemas.xmlsoap.org/soap/http"
style="document"/>
        <wsdl:operation name="queryResources">
            <soap:operation soapAction="urn:queryResources" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="launchCCXML">
            <soap:operation soapAction="urn:launchCCXML" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="launchApp">
            <soap:operation soapAction="urn:launchApp" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="launchEmail">
            <soap:operation soapAction="urn:launchEmail" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
```

```
        </wsdl:operation>
        <wsdl:operation name="launchHtml">
            <soap:operation soapAction="urn:launchHtml" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="sendEmail">
            <soap:operation soapAction="urn:sendEmail" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="sendApp">
            <soap:operation soapAction="urn:sendApp" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="getStatus">
            <soap:operation soapAction="urn:getStatus" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="sendCCXMLEvent">
            <soap:operation soapAction="urn:sendCCXMLEvent" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="getStatusEx">
            <soap:operation soapAction="urn:getStatusEx" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
```

```
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="launchSMS">
            <soap:operation soapAction="urn:launchSMS" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="launchVXML">
            <soap:operation soapAction="urn:launchVXML" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="sendSMS">
            <soap:operation soapAction="urn:sendSMS" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="deleteConversation">
            <soap:operation soapAction="urn:deleteConversation" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="getConversation">
            <soap:operation soapAction="urn:getConversation" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
```

```
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="updateConversation">
            <soap:operation soapAction="urn:updateConversation" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="createConversation">
            <soap:operation soapAction="urn:createConversation" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="getConversationByAlias">
            <soap:operation soapAction="urn:getConversationByAlias" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="addConversationAlias">
            <soap:operation soapAction="urn:addConversationAlias" style="document"/>
            <wsdl:input>
                <soap:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
    </wsdl:binding>
    <wsdl:binding name="VPAppIntfServiceSoap12Binding"
type="ns:VPAppIntfServicePortType">
        <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"
style="document"/>
        <wsdl:operation name="queryResources">
            <soap12:operation soapAction="urn:queryResources" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
```

```
            <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
        </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="launchCCXML">
        <soap12:operation soapAction="urn:launchCCXML" style="document"/>
        <wsdl:input>
            <soap12:body use="literal"/>
        </wsdl:input>
        <wsdl:output>
            <soap12:body use="literal"/>
        </wsdl:output>
        <wsdl:fault name="VPAppIntfServiceRemoteException">
            <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
        </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="launchApp">
        <soap12:operation soapAction="urn:launchApp" style="document"/>
        <wsdl:input>
            <soap12:body use="literal"/>
        </wsdl:input>
        <wsdl:output>
            <soap12:body use="literal"/>
        </wsdl:output>
        <wsdl:fault name="VPAppIntfServiceRemoteException">
            <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
        </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="launchEmail">
        <soap12:operation soapAction="urn:launchEmail" style="document"/>
        <wsdl:input>
            <soap12:body use="literal"/>
        </wsdl:input>
        <wsdl:output>
            <soap12:body use="literal"/>
        </wsdl:output>
        <wsdl:fault name="VPAppIntfServiceRemoteException">
            <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
        </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="launchHtml">
        <soap12:operation soapAction="urn:launchHtml" style="document"/>
        <wsdl:input>
            <soap12:body use="literal"/>
        </wsdl:input>
        <wsdl:output>
            <soap12:body use="literal"/>
        </wsdl:output>
        <wsdl:fault name="VPAppIntfServiceRemoteException">
            <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
        </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="sendEmail">
        <soap12:operation soapAction="urn:sendEmail" style="document"/>
        <wsdl:input>
            <soap12:body use="literal"/>
        </wsdl:input>
        <wsdl:output>
            <soap12:body use="literal"/>
        </wsdl:output>
        <wsdl:fault name="VPAppIntfServiceRemoteException">
            <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
        </wsdl:fault>
    </wsdl:operation>
    <wsdl:operation name="sendApp">
        <soap12:operation soapAction="urn:sendApp" style="document"/>
```

```
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="getStatus">
            <soap12:operation soapAction="urn:getStatus" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="sendCCXMLEvent">
            <soap12:operation soapAction="urn:sendCCXMLEvent" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="getStatusEx">
            <soap12:operation soapAction="urn:getStatusEx" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="launchSMS">
            <soap12:operation soapAction="urn:launchSMS" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="launchVXML">
            <soap12:operation soapAction="urn:launchVXML" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
```

```
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="sendSMS">
            <soap12:operation soapAction="urn:sendSMS" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="deleteConversation">
            <soap12:operation soapAction="urn:deleteConversation" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="getConversation">
            <soap12:operation soapAction="urn:getConversation" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="updateConversation">
            <soap12:operation soapAction="urn:updateConversation" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="createConversation">
            <soap12:operation soapAction="urn:createConversation" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
```

```
        <wsdl:operation name="getConversationByAlias">
            <soap12:operation soapAction="urn:getConversationByAlias" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="addConversationAlias">
            <soap12:operation soapAction="urn:addConversationAlias" style="document"/>
            <wsdl:input>
                <soap12:body use="literal"/>
            </wsdl:input>
            <wsdl:output>
                <soap12:body use="literal"/>
            </wsdl:output>
            <wsdl:fault name="VPAppIntfServiceRemoteException">
                <soap12:fault use="literal" name="VPAppIntfServiceRemoteException"/>
            </wsdl:fault>
        </wsdl:operation>
    </wsdl:binding>
    <wsdl:binding name="VPAppIntfServiceHttpBinding" type="ns:VPAppIntfServicePortType">
        <http:binding verb="POST"/>
        <wsdl:operation name="queryResources">
            <http:operation location="queryResources"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="launchCCXML">
            <http:operation location="launchCCXML"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="launchApp">
            <http:operation location="launchApp"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="launchEmail">
            <http:operation location="launchEmail"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="launchHtml">
            <http:operation location="launchHtml"/>
```

```
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="sendEmail">
            <http:operation location="sendEmail"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="sendApp">
            <http:operation location="sendApp"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="getStatus">
            <http:operation location="getStatus"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="sendCCXMLEvent">
            <http:operation location="sendCCXMLEvent"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="getStatusEx">
            <http:operation location="getStatusEx"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="launchSMS">
            <http:operation location="launchSMS"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="launchVXML">
            <http:operation location="launchVXML"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
```

```
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="sendSMS">
            <http:operation location="sendSMS"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="deleteConversation">
            <http:operation location="deleteConversation"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="getConversation">
            <http:operation location="getConversation"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="updateConversation">
            <http:operation location="updateConversation"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="createConversation">
            <http:operation location="createConversation"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="getConversationByAlias">
            <http:operation location="getConversationByAlias"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="addConversationAlias">
            <http:operation location="addConversationAlias"/>
            <wsdl:input>
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:input>
            <wsdl:output>
```

```
                <mime:content type="application/xml" part="parameters"/>
            </wsdl:output>
        </wsdl:operation>
    </wsdl:binding>
    <wsdl:service name="VPAppIntfService">
        <wsdl:port name="VPAppIntfServiceHttpSoap11Endpoint"
binding="ns:VPAppIntfServiceSoap11Binding">
            <soap:address location="http://localhost:8080/axis2/services/
VPAppIntfService"/>
        </wsdl:port>
        <wsdl:port name="VPAppIntfServiceHttpSoap12Endpoint"
binding="ns:VPAppIntfServiceSoap12Binding">
            <soap12:address location="http://localhost:8080/axis2/services/
VPAppIntfService"/>
        </wsdl:port>
        <wsdl:port name="VPAppIntfServiceHttpEndpoint"
binding="ns:VPAppIntfServiceHttpBinding">
            <http:address location="http://localhost:8080/axis2/services/
VPAppIntfService"/>
        </wsdl:port>
    </wsdl:service>
</wsdl:definitions>
```

Chapter 27: Managing external messages

External messages overview

Experience Portal supports sending and receiving events from the CCXML application synchronously or asynchronously within a voice application as specified in the VXML 3.0 specification. When an external message arrives, it reflects in the application.

VoiceXML 3.0 interpreters receive events from external sources. In particular, VoiceXML 3.0 receives the life cycle events specified as part of the Multimodal Architecture and Interfaces (MMI) specification . These life cycle events allow the flow component of the Data Flow Presentation architecture to control the presentation layer by starting and stopping the processing of markup. By handling these events, the VoiceXML interpreter acts as a modality component in the multimodal architecture, while the flow component acts as an Interaction manager. As a result, you can extend VoiceXML 3.0 into multimodal applications.

External messages are reflected in the application in the *application.lastmessage$* variable.

Note:

Experience Portal cannot send or receive any other source, except the CCXML application, for processing the external event in the VXML browser.

The variable is an ECMAScript object with the following properties:

application.lastmessage$ properties	
contenttype	The media type of the external message. Vb currently support “string” only.
event	The event name, if any, or ECMAScript undefined if no event name was included in the external message.
content	The content of the message, if any, or ECMAScript undefined. The interpreter throws "error.badfetch" in one of the following scenarios: • An interpreter receives an external message with a payload in a data format that it does not understand. * The payload is not well formed as defined by the specification of that format. • The payload is not well formed as defined by the specification of that format.

If no external messages are received, *application.lastmessage$* is ECMAScript undefined. Only the last received message is available.

Since external messages can arrive at any time, they can be disruptive to a voice application. A voice application developer decides whether these messages are delivered to the application synchronously or asynchronously using the externalevents.enable property.

You can set the property to one of the following values:

externalevents.enable values	
true	External messages are delivered asynchronously as VoiceXML events.
false	External messages are delivered synchronously. This is the default.

Receiving an external message asynchronously

To receive an external message asynchronously, an application defines an "externalmessage" event handler. If the payload of an external message includes an event name, the name is appended to the name of the event that is thrown to the application separated by a dot, or example, "externalmessage.ready". This allows applications to handle external messages using different event handlers.

Asynchronous external messages are processed in the same manner that a disconnect event is handled in VXML2.

Events are dispatched to the application serially. Because the interpreter only reflects the data associated with a single external message at a time, the application handles the data associated with each external message after that message is delivered. If multiple events arrive, VB deals with them one at a time, until all events are processed, or when execution goes to an element where externalevents. enable turns to false, whichever happens first.

The following example demonstrates asynchronous receipt of an external message. The catch handler copies the reflected external message into an array at the application level.

```
<vxml version="2.1"
  xmlns="http://www.w3.org/2001/vxml">
  <property name="externalevents.enable" value="true"/>
  <var name="myMessages" expr="new Array()"/>

  <catch event="externalmessage">
    <var name="lm" expr="application.lastmessage$"/>
    <if cond="typeof lm.content == 'string'"/>
      <log>received <value expr="lm.content"/></log>
    <else/>
      <log>received unknown external message type
        <value expr="typeof lm.content"/>
      </log>
    </if>
    <script>
      myMessages.push({'content' : lm.content, 'ctype' : lm.contenttype});
    </script>
  </catch>

  <form>
  <field name="num" type="digits">
    <prompt>pick a number any number</prompt>
    <catch event="noinput nomatch">
      sorry. didn't get that.
      <reprompt/>
    </catch>
    <filled>
      you said <value expr="num"/>
      <clear/>
    </filled>
```

```
  </field>
  </form>
</vxml>
```

Receiving external message synchronously

When external message is delivered synchronously, an application developer decides whether the message is preserved or discarded by setting the externalevents.queue property. The property can be set to one of the following values:

externalevents.queue values	
true	External messages are queued and set to *application.lastmessage$*.
false	An external message that is not delivered as a VoiceXML event is discarded. This is the default value.

To receive an external message synchronously, set the externalevents.enable property to false and the externalevents.queue property to true, and use the <receive>element to pull messages off the queue. The <receive>element blocks waits until an external message is received or the timeout specified by the maxtime attribute is exceeded.

The <receive> element supports the following attributes:

The <receive> properties			
Name	**Description**	**Required**	**Default**
fetchaudio	See Section 6.1 of [VXML2]. This the defaults value to the fetchaudio property described in Section 6.3.5 of [VXML2].	No	N/A
fetchaudioexpr	An ECMAScript expression evaluating to the fetchaudio URI. If evaluation of the expression fails, the interpreter displays"error.semantic".	No	N/A
maxtime	A W3C time specifier indicating the maximum amount of time the interpreter waits to receive an external message. If the timeout is exceeded, the interpreter throws "error.badfetch." A value of "none" indicates the interpreter the blocks indefinitely.	No	0s
maxtimeexpr	An ECMAScript expression evaluating to the maxtime value. If evaluation of the expression fails, the interpreter throws "error.semantic".	No	0s

You can specify any one of fetchaudio and fetchaudioexpr. Otherwise, the system returns the `error.badfetch` error message.

You can specify any one of maxtime and maxtimeexpr . Otherwise, the system returns the `error.badfetch` error message.

When present, the attributes fetchaudioexpr and maxtimeexpr are evaluated when the <receive> command is ran.

The following example demonstrates synchronously received external message. In this example, the interpreter blocks for up to 15 seconds waiting for an external message to arrive. If no external message is received during that interval, the interpreter returns the `error.badfetch` error message. If a message is received, the interpreter proceeds by executing the <log >element.

```
<vxml version="2.1"
  xmlns="http://www.w3.org/2001/vxml">

  <property name="externalevents.queue" value="true"/>
  <form>
    <catch event="error.badfetch">
      <log>timed out waiting for external message</log>
    </catch>

    <block>
      Hold on ...
      <receive maxtime="15s"
        fetchaudio="http://www.example.com/audio/fetching.wav"/>
      <log>got <value expr="application.lastmessage$.content"/></log>
    </block>
  </form>
</vxml>
```

Sending messages from a voice application

To send a message from a VoiceXML application to a remote endpoint, use the <send> element.

The <send> element supports the following attributes:

The <send> attributes			
Name	**Description**	**Required**	**Default**
async	A boolean indicating whether to block until the final response to the transaction created by sending the external event is received, or a timeout.	No	true
asyncexpr	An ECMAScript expression evaluating the value of the async attribute. If evaluation of the expression fails, the interpreter displays "error.semantic".	No	N/A
body	A string representing the data to be sent in the body of the message.	No	N/A
bodyexpr	An ECMAScript expression evaluating the body of the message to be sent. If evaluation of the expression fails, the interpreter displays "error.semantic".	No	N/A

Table continues…

The <send> attributes			
Name	**Description**	**Required**	**Default**
contenttype	A string indicating the media type of the body being sent, if any. The set of content types might be limited by the underlying platform. If an unsupported media type is specified, the interpreter displays "error.badfetch.<protocol>.400." The interpreter is not required to inspect the data specified in the body to validate that it conforms to the specified media type.	No	text/plain
contenttypeexpr	An ECMAScript expression evaluating the media type of the body. If evaluation of the expression fails, the interpreter displays "error.semantic".	No	N/A
event	The name of the event to send. The value is a string which only includes alphanumeric characters and the "." (dot) character. The first character must be a letter. If the value is invalid, then an "error.badfetch" event is displayed.	No	N/A
eventexpr	An ECMAScript expression evaluating the name of the event to be sent. If evaluation of the expression fails, the interpreter displays "error.semantic".	No	N/A
fetchaudio	See Section 6.1 of [VXML2]. This is a default valueto the fetchaudio property described in Section 6.3.5 of [VXML2].	No	N/A
fetchaudioexpr	An ECMAScript expression evaluating the fetchaudio URI. If evaluation of the expression fails, the interpreter displays "error.semantic".	No	N/A

Table continues…

The <send> attributes			
Name	**Description**	**Required**	**Default**
namelist	A list of zero or more whitespace-separated variable names to send. By default, no variables are submitted. Values for these variables are evaluated when the <send> element is ran. Only declared variables can be referenced. Otherwise, error.semantic is displayed. Variables must be submitted to the server with the same qualification used in the namelist. When an ECMAScript variable is submitted to the server, its value must be converted first into a string before being sent. If the variable is an ECMAScript object, the mechanism by which it is submitted is platform specific. Instead of submitting an ECMAScript object directly, the application developer can explicitly submit the individual properties of the object. For example, date.month date.year.	No	N/A
target	The attribute that specifies the URI to which the event is sent. If the attribute is not specified, the event is sent to the component which started the VoiceXML session.	No	Invoking component
targetexpr	An ECMAScript expression evaluating the target URI. If evaluation of the expression fails, the interpreter displays "error.semantic".	No	N/A
timeout	See 6.13.2.1 sendtimeout. This defaults to the sendtimeout property.	No	N/A
timeoutexpr	An ECMAScript expression evaluating the timeout interval for a synchronous <send>. If evaluation of the expression fails, the interpreter displays "error.semantic"	No	N/A

You can specify any of the following items. Otherwise, the system returns the `error.badfetch` error message:

- async or asyncexpr
- event or eventexpr
- contenttype or contenttypeexpr
- fetchaudio or fetchaudioexpr
- target or targetexpr
- timeout or timeoutexpr

Additionally, only one of the following attributes must be specified. Otherwise the system returns the `error.badfetch` error message:

body, bodyexpr, or namelist.

For synchronous <send>, if time-out occurs, the interpreter returns the `error.badfetch` error message. If the interpreter encounters an error upon sending the external message, the system returns the `error.badfetch.<protocol>.<status_code>` output.

The following example demonstrates the use of <send> synchronously:

```
<vxml version="2.1"
  xmlns="http://www.w3.org/2001/vxml">

  <form>
  <field name="user_id" type="digits">
    <prompt>please type your five digit i d</prompt>
    <filled>
      <send async="false"
            bodyexpr="'<userinfo><id>' + user_id + '</id></userinfo>'"
            contenttype="text/xml" timeout=”5s”/>
      <goto next="mainmenu.vxml"/>
    </filled>
  </field>
  </form>
</vxml>
```

Upon executing an asynchronous <send>, the interpreter continues execution of the voice application immediately and disregards the disposition of the message that was sent.

The following example demonstrates the use of <send> asynchronously:

```
<vxml version="2.1"
  xmlns="http://www.w3.org/2001/vxml">

  <form>
    <var name="tasktarget" expr="'http://www.example.com/taskman.pl'"/>
    <var name="taskname" expr="'cc'"/>
    <var name="taskstate"/>
    <block>
      <assign name="taskstate" expr="'start'"/>
      <send async="true"
            targetexpr="tasktarget"
            namelist="taskname taskstate"/>
    </block>
    <field name="ccnum"/>
    <field name="expdate"/>
    <block>
      <assign name="taskstate" expr="'end'"/>
      <send async="true"
            targetexpr="tasktarget"
            namelist="taskname taskstate"/>
    </block>
  </form>
</vxml>
```

Chapter 28: The Management Interface web service

Overview

Administrators can use the Management Interface web service on the Primary EPM to configure and manage the Experience Portal system. This web service supports the following functionality:

Zones

- Retrieve zone names: For retrieving the names of the configured zones.
- Get zone information: For retrieving the information of an existing zone.

Applications

- Retrieve application names: For retrieving the names of the configured applications.
- Add application: For configuring a new application.
- Delete application: For deleting an existing application.
- Get application information: For retrieving the parameters of an existing application.
- Set application information: For updating the parameters of an existing application.

Configurable Application Variables

- Retrieve configurable application variables: For retrieving the CAVs of an existing application.
- Set configurable application variables: For updating the CAVs of an existing application.

Authentication and Authorization

The Management Interface web service is accessible by an authenticated user. An EPM user name and password is required to be able to invoke any of the web service methods.

The authorization is based on the role and features assigned to the EPM user invoking the web service. In order to be able to invoke a specific web service method, the EPM user account used must have permission to perform the same operation on the web page. For example, if an EPM user has a role which allows addition of an application over the web page, the user can add an application through the web service. Similarly if an EPM user has a role which does not allow deletion of an application over the web page, the user cannot delete the application through the web service as well.

Management web services WSDL

The WSDL of the Management web services is available on the Primary EPM. The URL for the Management Interface web service WSDL is:

`https://<EPM-server>/axis2/services/VPManagementService?wsdl`

Where, *<EPM-server>* is the domain name or IP address of the system where the primary EPM software is installed.

The Management Interface web service conforms to all W3C standards and can be accessed through any web service client using the Avaya-provided Web Services Description Language (WSDL) file.

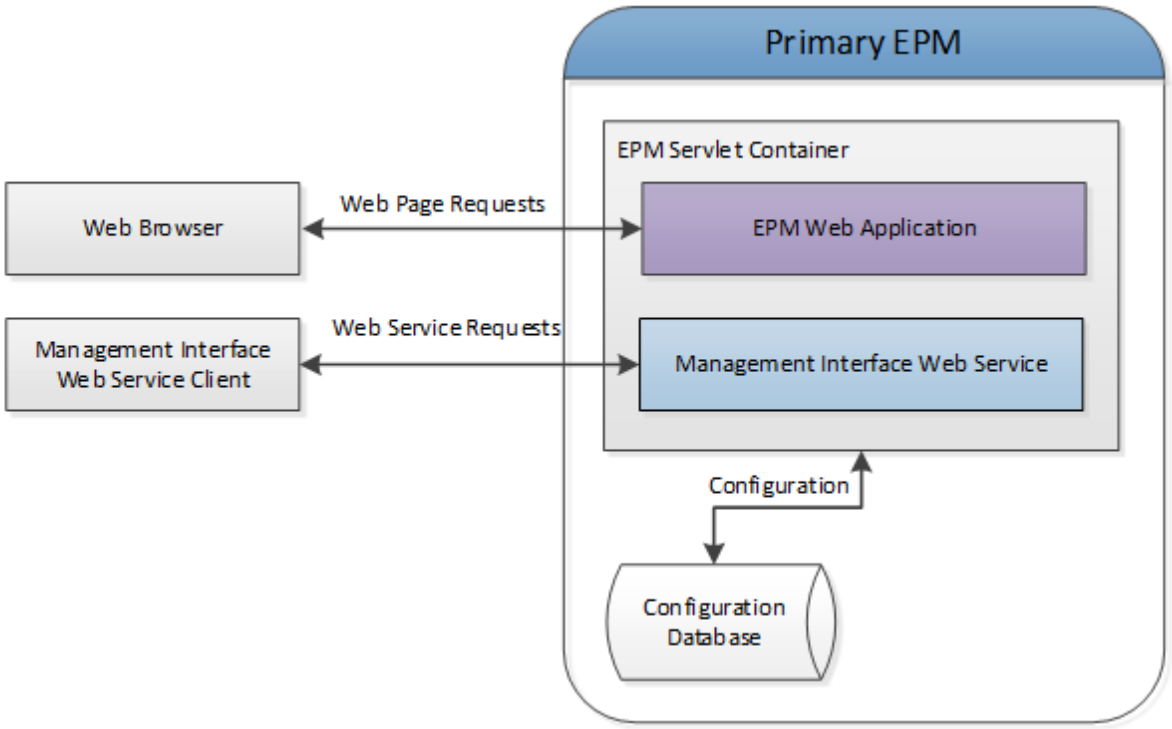
Best Practices

When using the Management Interface web service, keep the following in mind:

- The Management Interface web service is only available on the Primary EPM and only accessible over HTTPS. The web service clients need to accept the SSL certificate from the Primary EPM server.
- The Management Interface web service uses Basic Authentication to authenticate web service client requests. When you submit a request to the web service, you need to include the user name and password that is configured as one of the Experience Portal users and that user must have the role with the appropriate feature enabled. For example, if the user wants to add an application, then the role must have the feature for adding an application enabled. Similarly, if the user wants to delete an application, then the role must have the feature for deleting an application enabled. If the user wants to update an application, then the role must have the feature for updating an application enabled.
- If non-ASCII characters are sent in the URL request to the web service they should be encoded as UTF-8 prior to sending the request. For example, an application name of ‘aña’ is encoded and sent as ‘a%C3%B1a’. Note that the non-ASCII character ‘ñ’ is sent as the UTF-8 value of ‘%C3%B1’.
- If zones are configured on the system, the zone name should be specified. If the zone name is not specified, then the web service operation is performed against the default zone.
- Field names are case-sensitive.

Management Interface web service flow diagram

The following diagram shows how an external application interacts with the Management Interface web service and how the Management Interface web service interacts with the rest of the Experience Portal system.



Configuring Management Interface web service

Procedure

1. Log in to the EPM web interface using an account with the User Manager role.
2. From the EPM main menu, select **User Management** > **Users**.
3. Click the user name that will be used when sending requests to the web service.
4. On the Change User page, select the roles that have the appropriate features checked to enable the user to use web service methods.

   For example, if the user wants to invoke the *addApplicationInfo* web service method to add an application, then the role must have the *addApplication* feature enabled. Similarly, if the user wants to invoke the *deleteApplicationInfo* web service to delete an application, then the role must have the *deleteApplication* feature enabled and if the user wants to invoke the *setApplicationInfo* web service to update an application, then the role must have the *changeApplication* feature enabled.

5. Click **Save**.
6. Open the following page in a web browser:

   `https://<EPM-server>/axis2/services/VPManagementService?wsdl`

   <EPM-server> is the domain name or IP address of the system where the primary EPM software is installed.
7. When prompted, enter the user name and password for Experience Portal with the web services role checked.
8. Save the WSDL file and use it to build the web service client that accesses the Application Interface web service (axis 2.0). This web service conforms to all current W3C standards.

Management Interface web service method objects

The Management Interface web service methods use the following objects as parameters or as return values:

- Field
- FieldArray
- Status

Field

This object contains the field name, field type, and field value.

Object members	Notes
name	Name of the field. This entry is case sensitive.

Table continues…

Object members	Notes
dataType	Data type of the field. The supported data types are: • String • Integer • Boolean • Floatingpoint • Date • Time • Datetime • Password • File • List • Combo
value	Value of the field.

Field array

This object contains an array of fields. When retrieving the application information, each application parameter is returned as an array of fields where each field contains information for each parameter.

The use of the *Field* and *FieldArray* objects provides compatibility to the web services when new parameters are introduced in future. It also allows the web services to be backward compatible if and when existing parameters need to be dropped or changed.

Status

This object contains information about the status of the method invocation.

Object members	Notes
String statusCode	Success or Error
String statusMessage	Empty if the statusCode is Success Error message if the statusCode is Error

Management Interface web service methods

The Management Interface web service includes the following methods:

getZoneNames method

This topic describes the method for retrieving the names of the configured zones.

```
FieldArray getZoneNames()
```

Parameter

None

Data returned

Return Type	Notes
FieldArray	Arrays of fields where each field has the name of the zone.

getZoneInfo method

This section describes the method for retrieving the information of an existing zone.

```
FieldArray getZoneInfo(String name)
```

Parameters

Parameters	Notes	Required?
String name	Name of the zone	Y

Data returned

Return Type	Notes
FieldArray	Array of fields where each field contains the details of the zone.

getApplicationNames method

This section describes the method for retrieving the names of the configured applications.

```
FieldArray getApplicationNames(String zoneName)
```

Parameters

Parameters	Notes	Required?
String zoneName	Name of the zone configured on the system. If the zone name is not specified, then the names of the applications configured in the default zone are returned.	N

Data returned

Return Type	Notes
FieldArray	Arrays of fields where each field has the name of the application.

getApplicationInfo method

This section describes the method for retrieving the parameters of an existing application.

```
FieldArray getApplicationInfo(String name, String zoneName)
```

Parameters

Parameters	Notes	Required?
String name	Name of the application in the format application name for global applications or organization name/application name for organization applications.	Y
String zoneName	Name of the zone from which the application information is retrieved. If the zone name is not specified, then the information retrieved for the application configured in the default zone.	N

Data returned

Return Type	Notes
FieldArray	Array of fields where each field contains the details of the application field.

setApplicationInfo method

This section describes the method for updating the parameters of an existing application.

```
Status setApplicationInfo(String name, FieldArray fieldArray, String
zoneName)
```

Parameters

Parameters	Notes	Required?
String name	Name of the application in the format application name for global applications or organization name/application name for organization applications.	Y
FieldArray fieldArray	Array of fields where each field contains the details of the application field.	Y
String zoneName	Name of the zone in which the application is updated. If the zone name is not specified, then the application is updated in default zone.	N

Data returned

Return Type	Notes
Status	Status of the method invocation.

addApplicationInfo method

This section describes the method for configuring a new application.

```
Status addApplicationInfo(String name, FieldArray fieldArray, String zoneName)
```

Parameters

Parameters	Notes	Required?
String name	Name of the application in the format application name for global applications or organization name/application name for organization applications.	Y
FieldArray fieldArray	Array of fields where each field contains the details of the application field.	Y
String zoneName	Name of the zone to which the application is added. If the zone name is not specified, then the application is added to the default zone.	N

Data returned

Return Type	Notes
Status	Status of the method invocation.

deleteApplicationInfo method

This section describes the method for deleting an existing application.

```
void deleteApplicationInfo(String name, String zoneName)
```

Parameters

Parameters	Notes	Required?
String name	Name of the application in the format application name for global applications or organization name/application name for organization applications.	Y
String zoneName	Name of the zone from which the application is deleted. If the zone name is not specified, then the application is deleted from the default zone.	N

Data returned

None

Execution of the web service method without any exception implies that the deletion was successful.

getAppConfigurableVars method

This section describes the method for retrieving the configurable application variables of an existing application.

```
FieldArray getAppConfigurableVars(String name, String zoneName)
```

Parameters

Parameters	Notes	Required?
String name	Name of the application in the format application name for global applications or organization name/application name for organization applications.	Y
String zoneName	Name of the zone from which the application information is retrieved. If the zone name is not specified, then the information retrieved for the application configured in the default zone.	N

Data returned

Return Type	Notes
FieldArray	Array of fields where each field contains the details of the configurable application variable of the application.

setAppConfigurableVars method

This section describes the method for updating the configurable application variables of an existing application.

```
Status setAppConfigurableVars(String name, FieldArray fieldArray, String
zoneName)
```

Parameters

Parameters	Notes	Required?
String name	Name of the application in the format application name for global applications or organization name/application name for organization applications.	Y
FieldArray fieldArray	Array of fields where each field contains the details of the configurable application variable of the application.	Y
String zoneName	Name of the zone in which the application is updated. If the zone name is not specified, then the application is updated in default zone.	N

Data returned

Return Type	Notes
Status	Status of the method invocation.

Note:

To update the configurable application variable file using the web service method, you must first upload the file to the server using the FileUpload servlet interface and then use the web service method to update the variable. The value specified for the file variable is the name of the file uploaded using the FileUpload servlet interface.

Exception codes

The Management Interface web service methods throw *RemoteException* error codes for various error conditions and validation failures. The following table lists the exception error codes.

Value	Attributes	Condition
401	Unauthorized	Invalid user name and password.
1005	Required field	Required field is missing.
1010	Not in range	Specified value is not in the acceptable range.
1016	Duplicate name	Duplicate name is specified.
1018	Invalid parameter	Invalid parameter name specified.
1025	Invalid file	Invalid file name specified when updating configurable application variable of type file.
1026	Invalid file contents	File with invalid contents or an empty file was specified.
7001	Resource not found	Invalid application name specified.
7014	Invalid ASR	Invalid ASR name specified.
7015	Invalid TTS	Invalid TTS name specified.
7017	Missing language	No ASR with the specified language is available.

Table continues…

Value	Attributes	Condition
7018	Missing voice	No TTS with the specified voice is available.
7019	Invalid language format	Invalid language format, for example: English(USA) EN-US
7020	Invalid voice format	Invalid voice format, for example: English(USA) EN-US Andrew Male
7022	Invalid DNIS	Invalid DNIS format specified.
7024	URI Expression error	Called URI expression error.
7026	Invalid Prosody	Invalid prosody value specified.
7027	Invalid minimum	Value specified is below the minimum acceptable value.
7028	Invalid DTMF	Invalid DTMF value specified.
7029	Invalid TTS data	Invalid TTS data specified.
7030	Invalid ASR data	Invalid ASR data specified.
7032	Invalid VoiceXML handler	Invalid VoiceXML handler name specified.
7033	Invalid CCXML handler	Invalid CCXML handler name specified.
7034	ASR language required	ASR language must be specified.
7035	TTS voice required	TTS voice must be specified.
7038	Only one default	Only one default application can be configured.
7041	Invalid video screen format	Invalid video screen format specified.
7043	Invalid URL	Invalid URL specified
7044	Invalid prompt data	Invalid prompt data specified.
7045	URL username and or password missing	URL username and password must be specified.
7058	Pattern required	Pattern must be specified for the launch parameters.
7072	Enable Remote DTMF is not allowed.	If ASR is not configured, *Support Remote DTMF Processing* in Advanced group must be set to No.
7073	Algorithm required	Email Additional Launch Parameters: Algorithm is input required. <Email Additional Launch Parameters entry number>
7074	Launch parameters required	Launch parameters must be specified.
7075	Component required.	Email Additional Launch Parameters: Component is input required. <Email Additional Launch Parameters entry number>
7076	Algorithm not supports Component	Email Additional Launch Parameters: The Algorithm does not support the selected Component. <Email Additional Launch Parameters entry number>
7077	Notification URL required	Notification URL must be specified.
7078	Access not allowed	Access is not allowed. Please check the assigned roles.
7079	Notification URL2 required	Notification URL2 must be specified.
7080	Invalid zone name	Invalid zone name specified.

Table continues…

Value	Attributes	Condition
7081	Organization not in zone	Organization does not exist in the specified zone.
7082	Mime type change is not allowed	Changing of <*MIME type*> MimeType is not allowed.
7083	Extension and ExtensionAppType are required	Extension and ExtensionAppType are required.
7084	Invalid DNIS range	Stations need to be of same length.

FileUpload Serverlet Interface

The FileUpload Servlet Interface provides the ability to upload a file to the server. This interface uses the FileUpload method.

You can call the interface from any application that is running on the same network as the EPM server.

FileUpload Serverlet Interface URL

The URL for uploading file is:

`https://<EPM server>/axis2/FileUpload/AppVariable`

<*EPM server*> is the domain name or IP address of the system where the primary EPM software is installed.

FileUpload method

This section provides the details for uploading a file that can be used for setting the configurable application variable of type file. When you need to update the configurable application variable file from the Configurable Application Variables (CAV) web page, you must browse and select a file that is uploaded to the server and then the CAV is updated. To update the configurable application variable file from the web service, you need to first upload the file to the server using the FileUpload Servlet Interface and then use the web service method to update the file variable.

The FileUpload Servlet accepts a file that is uploaded using the HTTP Post method in which the content type is set to multi-part/form data and the file contents are uploaded as multi-part request entity. This interface saves the uploaded file on the server. Then you can use the setAppConfigurableVars method to update the file variable of an application. The name of the file uploaded is the name that you must provide when invoking the setAppConfigurableVars method for setting the file variable.

Status returned

This method returns HTTP status code for the invocation of the file upload URL. When the URL is invoked successfully, the method returns the standard HTTP status code 200.

Data returned

Apart from checking the HTTP status code, the client must also check the response string returned by the URL.

Response String	Notes
success	Implies the file upload was successful.
failure, error message	Implies the file upload was not successful. The failure text followed by the error message (delimited by a comma).

Management Interface web service client

A Management Interface web service client (VPManagementClient) is located in the `Support/WebServices/VPManagementClient` folder on the Experience Portal installation DVD or in the `$AVAYA_ HOME/Support/WebServices/VPManagementClient` folder on the Primary EPM. You can use this client for invoking any of the web services including uploading of the files.

The command **`./VPManagementClient.sh`** from this folder displays the information on how to use the client and the various web service methods supported. The command **`VPManagementClient.sh -help`** also includes examples for the various web service methods. The help also provides information on how to pass parameters when updating an application.

Management Interface web service client examples

This section provides some examples of how to invoke the `VPManagementClient.sh` script in the `Support/WebServices/VPManagementClient` folder. The following section provides a list of the examples, with the purposes, commands, and a description of the variables used in the commands.

Purpose and Command

Enter the following command to:

- Retrieve the application names for the default zone:

  `./VPManagementClient.sh <epm address> <username> <password> true getApplicationNames`

- Retrieve the application names for a specific zone:

  `./VPManagementClient.sh <epm address> <username> <password> true getApplicationNames <zone name>`

- Retrieve the application information for a specific application in the default zone:

  `./VPManagementClient.sh <epm address> <username> <password> true getApplicationInfo <appname>`

- Update the Launch Parameters of a VoiceXML application in the default zone:

  ```
  ./VPManagementClient.sh <epm address> <username> <password> true
  setApplicationInfo <appname>
  Name=DnisRanges[0].Range,,Type=String,,Value='1022-1033'
  ```

- Update the multiple parameters of an application in a specific zone:

  ```
  ./VPManagementClient.sh <epm address> <username> <password> true
  setApplicationInfo <appname> Name=Url,,Type=String,,Value=http://
  myappserver/myapp/Start
  \;\;Name=DnisRanges[0].Range,,Type=String,,Value='1022-1033'\;\;Name
  =DnisRanges[1].Range,,Type=String,,Value='1044-1055' <zonename>
  ```

- Retrieve the configurable application variables for a specific application in the default zone:

  ```
  ./VPManagementClient.sh <epm address> <username> <password> true
  getAppConfigurableVars <appname>
  ```

- Update the configurable application variable of type String for a specific application in the default zone:

  ```
  ./VPManagementClient.sh <epm address> <username> <password> true
  setAppConfigurableVars <appname>
  Name=<cavname>,,Type=String,,Value=newValue
  ```

- Upload a file that can be used for updating configurable application variable of type file:

  ```
  ./VPManagementClient.sh <epm address> <username> <password> true
  fileUpload AppVariable <filename with full path>
  ```

- Update the configurable application variable of type file for a specific application in a specific zone:

  ```
  ./VPManagementClient.sh <epm address> <username> <password> true
  setAppConfigurableVars <appname>
  Name=<cavname>,,Type=File,,Value=<filename> <zonename>
  ```

Variables

- *<epm address>*: The EPM host name or EPM IP address
- *<username>*: The EPM user name
- *<password>*: The password for the specified user name
- *<zone name>*: The name of the zone of the application, or the name of the zone for which the application names are to be retrieved.
- *<appname>*: The name of the application.
- *<cavname>*: The name of the configurable application variable.
- *<filename with full path>*: The filename with the fully qualified path.
- *<filename>*: The name of the file uploaded to the system.

Chapter 29: Resources

Documentation

The following table lists the documents related to Avaya Experience Portal. Download the documents from the Avaya Support web site at http://support.avaya.com.

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 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.	Administrators 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.	Administrators Sales engineers Implementation engineers Avaya Professional Services
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

Table continues…

Title	Description	Audience
Deploying Avaya Experience Portal in an Avaya Customer Experience Virtualized Environment	Provides procedures for deploying the Experience Portal virtual application in the Avaya Customer Experience Virtualized Environment. This document includes installation, configuration, initial administration, troubleshooting, and basic maintenance checklists and procedures.	Implementation engineers
Upgrading to Avaya Experience Portal 8.1	Describes how to upgrade your Avaya Experience Portal system to Avaya Experience Portal 8.1.	Implementation engineers
Troubleshooting Avaya Experience Portal	Provides general information about troubleshooting and resolving system problems. This document also provides detailed information and procedures for finding and resolving specific problems.	Administrators Implementation engineers Avaya Professional Services
Avaya Experience Portal Solutions Guide	Provides a high-level description of Avaya Experience Portal as well as topology diagrams, connectivity details, interoperability concept, product interactions, and failover best practices.	Sales engineers Implementation engineers Avaya Professional Services
Avaya Experience Portal Programmer's Reference	Provides information about designing speech applications for Avaya Experience Portal.	Application Developers
Deploying Avaya Experience Portal on Amazon Web Services	Provides procedures for deploying Avaya Experience Portal as *Software as a Solution* by using the Amazon Web Services Management console.	Administrators Implementation engineers Support Personnel Avaya Professional Services
Deploying Avaya Experience Portal on Google Cloud Platform	Provides procedures for deploying Avaya Experience Portal as *Software as a Solution* by using the Google Cloud Platform.	Administrators Avaya Professional Services Implementation engineers Support Personnel

Table continues…

Title	Description	Audience
Deploying Avaya Experience Portal on Microsoft Azure	Provides procedures for deploying Avaya Experience Portal as *Software as a Solution* by using the Microsoft Azure portal.	Administrators Implementation engineers Support Personnel Avaya Professional Services
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 Implementation engineers
Avaya Experience Portal Mobile Web Best Practices White Paper	Provides recommended strategies for deploying Avaya Orchestration Designer Mobile Web applications with Avaya Experience Portal, detailing configuration for security, scalability and high availability.	Avaya Professional Services Implementation engineers
Avaya Experience Portal Call Classifications White Paper	Provides information about the call classification feature in Avaya Experience Portal, detailing the configuration and tuning of the call progress engine.	Sales engineers 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

For some programs, the latest customer documentation 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 keywords.

  To filter by product, click **Filters** and select a product.

- Search for documents.

  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 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 the 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 in to the website. The available functionality depends on your role.

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and press **Enter** or click **>** to search for the course.

Course code	Course title
5C00020E	Knowledge Access: Avaya Experience Portal Administration

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.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z