Administering Voice Portal

January 2011

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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 Web sites referenced within this site or documentation(s) 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 this product. 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 Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER, AND 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 End User a license within the scope of the license types described below. 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 End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

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

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. 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.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

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 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 Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: User management

Users in Voice Portal

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

- Voice Portal Management System (VPMS) web interface, which enables users to perform administrative, configuration, and maintenance tasks.
- MPP Service Menu web interface, which helps administrators troubleshoot problems on a Media Processing Platform (MPP).

Both web interfaces require a unique user name and password created by a Voice Portal administrator. Avaya recommends that you create a limited number of accounts and ensure that the passwords they use are secure.

Roles-based access in Voice Portal

Voice Portal provides role-based access to the VPMS 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 VPMS pages for that particular feature. For example, if you have the View Only permission on the Users VPMS 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.

User roles

Voice Portal provides role based access to the VPMS 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 VPMS, such as managing MPPs, VoIP

Role	Description
	connections, and speech applications. The only things Administrators *cannot* do are managing user accounts and viewing the audit logs. Because users with the Administration role have such a wide range of access and privilege, Avaya recommends that you 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 Voice 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 Voice Portal system.
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 Voice Portal system.
User Manager	User accounts with User Manager access can add and change Voice 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 VPMS so that VPMS users no longer need to be defined locally on the VPMS. Users with just the User Manager role can only see the **User Management** section of the main VPMS menu.
Web Services	User accounts with Web Services access can use Application Interface Web Service to launch any application configured on the Voice Portal system. They can also use Application Logging Web Service to save application and breadcrumb information for any application.

Note:

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

Password administration

Passwords are keys to a Voice 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 Voice 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 be the same as its associated user name.
- Although you can determine the minimum password length, you should not use any fewer than eight characters.

After installation, when you use the VPMS to create additional user accounts, the minimal characteristics for passwords are enforced. However, administrators can customize the minimum password length. Avaya recommends that you set this value to at least eight characters.

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

Logging in to the Voice Portal web interface

The Voice Portal Management System (VPMS) web interface is the main interface to the Voice Portal system.

You must log in to the VPMS web interface on the primary VPMS server before you can perform any Voice Portal administrative tasks.

1. Open an Internet Explorer browser and enter the URL for your Voice Portal system.

   The default URL is: `https://VPMS-server/VoicePortal`, where *VPMS-server* is the hostname or IP address of the system where the primary VPMS software is installed.

   Note:

   Transport Layer Security (TLS) must be enabled in your IE browser. For more information, see the *Configuring browsers to use TLS security* topic in the *Planning for Voice Portal* guide.

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

   The user name must match an existing Voice Portal VPMS account name exactly, including case.

   If organization level access is enabled in the Voice Portal system and you are assigned to an organization, prefix your user name with the organization name and a forward slash character. For example, sales/john. For more information on

organization level access, see Organization level access in Voice Portal on page 89.

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

   The password must match the password assigned to the specified user name exactly, including case.
5. Click **Logon**.

   Important:

   If you are logging on to the Voice Portal system for the first time with a specific user name and password, you are forced to change the temporary password at first logon.

   If you are not logging on to the Voice Portal system for the first time, then if your user name and password:

   - Match an authorized Voice Portal user account, the VPMS displays the Voice Portal Management System Home page with **Voice Portal Management System Version *version_number*** and the **Legal Notice** display text box. What you see and can do from there depends on your user role.
   - Do not match an authorized Voice Portal user account, the VPMS displays an error message and returns you to the **User Name** prompt so that you can log in again.
6. If you are forced to change the password on the first log in, or your password expires or you want to change or reset the password, click the **Change Password** link, specify the **User Name**, **Old Password**, **New Password** and re-enter the new password in the **Verify Password** field.
7. Click **Submit**.

Changing your account password

Note:

You cannot reuse any of your last ten passwords.

1. In Internet Explorer, enter the URL for your Voice Portal system.

The URL is `https://<VPMS-server>/VoicePortal` where *<VPMS-server>* is the name of the system where the VPMS 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, enter your user name in the **User Name** field.
4. Enter your old password in the **Old Password** field.
5. Enter your new password in the **New Password** field.

   The password is case-sensitive and must have at least the number of characters defined in the **Minimum Password Length** field.
6. Reenter your new password in the **Verify Password** field.
7. To change your password, click **Submit**.

Setting global login parameters

1. Log in to the VPMS web interface using an account with the User Manager user role.
2. From the VPMS main menu, select **User Management** > **Login Options**.
3. On the Login Options page, set the global login parameters in the **User Login Options** group.
4. If you changed one or more parameters, click **Save**.

Unlocking a locked user account

If a user has attempted to log in several times unsuccessfully, that user might be locked out for a certain length of time based on the settings for the global login parameters **Failed Login Lockout Threshold** and **Failed Login Lockout Duration**. User Managers can unlock an account manually before the **Failed Login Lockout Duration** expires.

1. Log in to the VPMS web interface using an account with the User Manager user role.
2. From the VPMS main menu, select **User Management** > **Users**.
3. On the Users page, click the **Minimum Password Length** link in the **Locked** column for each user account you want to unlock.

Viewing existing user accounts

1. Log in to the VPMS web interface using an account with the Administration, Operations, Maintenance, or User Manager user role.
2. From the VPMS main menu, select **User Management** > **Users**.
   If you are not logged in with the User Manager user role, the VPMS displays the Users page in view only mode.

Adding user accounts

1. Log in to the VPMS web interface using an account with the User Manager user role.
2. From the VPMS main menu, select **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 VPMS account can also access the MPP Service Menu on each MPP server.

Changing user accounts

Note:
You cannot change the existing user name.

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

Deleting VPMS user accounts

You can delete all VPMS user accounts except for the user account that you used to log into the VPMS, and if the Avaya Services is maintaining this system, the init account that was created when the Avaya Service accounts were configured.

1. Log in to the VPMS web interface using an account with the User Manager user role.
2. From the VPMS main menu, select **User Management** > **Users**.
3. On the Users page:
   - Select the check box to the left of the account's **User Name** for each user account that you want to delete.
   - Click 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 into the VPMS, those users will continue to have access until their current sessions end. At that point, the users will be unable to log back into the VPMS.

   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 VPMS removes it from the table in this section, but it does *not* keep the user from logging back into the VPMS. In order to do that, you need to change the corporate directory account access rules defined in the **LDAP Settings** group on the Users page.

4. Click **Delete**.
   The VPMS deletes all selected VPMS user accounts *without* requesting confirmation.

Using a corporate directory to specify Voice Portal users

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

Prerequisites

Consult your corporate directory administrator to determine what LDAP settings you need to use to establish a connection to the corporate directory, and how your directory is structured so that you can enter the appropriate search filters and paths.

The first time a user in the directory logs into the VPMS, Voice Portal verifies what permissions that user should have based on his or her directory settings and creates a temporary account for that user with the appropriate user roles.

Important:
If an account with the same user name exists on both the VPMS and in the corporate directory, Voice Portal uses the permissions specified on the VPMS account regardless of the directory settings.

1. In your corporate directory, add an attribute to each record that specifies what Voice Portal permissions that user should have.
   This attribute can specify the exact roles or be a custom group map name whose permissions you set within Voice Portal.
2. Log in to the VPMS web interface using an account with the User Manager user role.
3. From the VPMS main menu, select **User Management** > **Users**.
4. On the Users page, enter the appropriate information in the fields in the **LDAP Settings** group.

5. Click **Save**.
6. Verify that the connection was properly established by logging into the VPMS using one of the user names associated with an authorized Voice Portal group in the corporate directory.

Users page field descriptions

Use this page to add, view, or change the existing Voice Portal Management System (VPMS) 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.
User Name	The unique identifier for this account. This name is case-sensitive and must be unique across all VPMS user accounts. **Note:** You cannot change a user name once it is created.
Enable	The options are: • **Yes**: The user account is active and can be used to log into the VPMS. • **No**: The user account is inactive and cannot be used to log into the VPMS.
Assigned Roles	The options are: • One or more of the Voice Portal user roles. This indicates a locally-defined VPMS user account. • **Remote User**. This indicates that the user has logged into the VPMS at least once using an authorized account from the corporate directory defined in the **LDAP Settings** group.
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.

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.
Enforce Password Longevity	The options are: • **Yes**: The Password Longevity option is enabled for this account. Password Longevity, configured in *VPMS* > *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. • **No**: The password for this account will not expire.
Add	Opens the Add User page.
Delete	Deletes the user accounts whose Selection check box has been checked. **Note:** If you delete a remote user account, the VPMS removes it from the table in this section, but it does *not* keep the user from logging back into the VPMS. In order to do that, you need to change the corporate directory account access rules defined in the **LDAP Settings** group.

Add User page field descriptions

Use this page to create a user account that can access the Voice Portal Management System (VPMS) web interface.

Field	Description
Organization	The organization associated with the user you want to add.

Field	Description
	Note: This field is displayed only if organization level access is enabled in the Voice 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 Voice Portal on page 89.
User Name	The unique identifier for this account. This name is case-sensitive and must be unique across all VPMS user accounts. Enter from 1 to 95 characters. The user name must not contain *:, /, or !* 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 Voice Portal on page 89. • Once you save the user, this name cannot be changed.
Enable	The options are: • **Yes**: The user account is active and can be used to log into the VPMS. • **No**: The user account is inactive and cannot be used to log into the VPMS.
Roles	Each user account can have one or more of the following roles: • **Administration** • **Auditor** • **Maintenance** • **Operations** • **Reporting** • **User Manager** • ***<Custom Role>***: The name defined while creating a custom role. You can assign one or more custom roles along with the system roles to a user account. **Note:** Additional roles may be available if you have installed managed application on Voice Portal. For more information on managed application based roles, see the documentation delivered with the managed application.
Password	The initial password for this account.

Field	Description
	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 role for an existing account but do not want to change the password, leave this field and **Verify Password** field blank. **Important:** The Voice Portal system forces the user to change the default password on first login.
Verify Password	The initial password again for verification purposes.
Enforce Password Longevity	Enables the Password Longevity option for this account. Password Longevity, configured in *VPMS* > *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

Change User page field descriptions

Use this page to change an existing user account for the Voice Portal Management System (VPMS) web interface.

Field	Description
User Name	The unique identifier for this account. This name is case-sensitive and must be unique across all VPMS 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 VPMS. • **No**: The user account is inactive and cannot be used to log into the VPMS.
Roles	Each user account can have one or more of the following roles: • **Administration** • **Auditor**

Field	Description
	• **Maintenance** • **Operations** • **Reporting** • **User Manager** • ***<Custom Role>***: The name defined while creating a custom role. You can assign one or more custom roles along with the system roles to a user account. **Note:** Additional roles may be available if you have installed managed application on Voice Portal. For more information on managed application based roles, see the documentation delivered with the managed application.
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 have at least the number of characters defined in the **Minimum Password Length** field. If you are changing the role for an existing account but do not want to change the password, leave this field and **Verify Password** field blank. **Important:** If you change the password, the Voice Portal system forces the user to change the password on login.
Verify Password	The password again for verification purposes.
Enforce Password Longevity	Enables the Password Longevity option for this account. Password Longevity, configured in **VPMS > 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

Login Options page field descriptions

Use this page to configure security options for all user accounts. You can also configure an LDAP connection between a corporate directory and the VPMS so that VPMS users no longer need to be defined locally on the VPMS.

This page contains the:

User Login Options group

Field	Description
Failed Login Lockout Threshold	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. To disable the account lockout feature, set this field to 0 (zero).
Failed Login Lockout Duration	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.
Failed Login Alarm Threshold	The number of attempts users get to successfully log in to the system before the system raises an alarm. The default is 3. This value is usually the same as the **Failed Login Lockout Threshold**. To disable these alarms, set this field to 0 (zero).
Inactivity Lockout Threshold	The number of days to wait until Voice Portal should consider the account inactive and lock it out of the system. **Note:** This field is only used for local user accounts. Any user accounts created through a corporate directory do not expire. Enter an integer between 0 and 365. The default is 0, which means that accounts are never locked out regardless of how much time passes between logins.

Field	Description
	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. **Note:** If the user account was created in Voice Portal 3.0.1.x, the inactivity counter is set during the upgrade to 5.1. If the 3.0.1.x account was: • Logged into at least once, the counter is set to the length of time that has passed since the account was last used. • Never logged into, the counter is set to 0 during the upgrade and it begins timing from that point forward.
Minimum Password Length	The minimum number of characters users must use in setting their passwords. The default is 8 characters. For security purposes, Avaya recommends setting this at 8 or higher.
Password Longevity	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. Enter an integer between 0 and 365, where 0 means that passwords never expire. The default is 60.
Password Expiration Warning	The maximum number of days before a user password expires when Voice Portal displays a message warning the user that they need to change their password. Enter an integer between 1 and 30. The default is 10. Once this time limit has been reached, Voice Portal will display the warning message every time the user logs in until they have changed their password. **Note:** This field is ignored if **Password Longevity** is set to 0.

LDAP Settings group

Use the fields in this group to establish a connection between Voice Portal and your corporate directory using Lightweight Directory Access Protocol (LDAP). You can control which accounts in the directory have access to Voice Portal based on their group membership. For more information, see Using a corporate directory to specify Voice Portal users on page 20.

If you need more information about what to enter in the fields in this section, consult your corporate directory administrator.

Note:
If these fields are not displayed, click the group heading to expand the group.

Field	Description
Enable	The options are: • **Yes**: The connection between Voice Portal and your corporate directory using LDAP is enabled. • **No**: The connection between Voice Portal and your corporate directory using LDAP is disabled. **Note:** Voice Portal verifies the LDAP settings when you click **Apply** only if the **Enable** field is set to **Yes**. The changes are saved but not verified if the **Enable** field is set to **No**.
Connection Settings section	
URL	The fully-qualified address of the LDAP server which includes the following: • IP address of the host • LDAP schema • Port name For example: `ldap://10.0.0.20:389 or ldap://ldapserver.company.com:389`.
User Name	A user name that is authorized to access the corporate directory through the LDAP server. The user name can be a Distinguished Name (DN) or a simple user name. Example of a DN: `uid=jbloggs,ou=people,dc=mycompany,dc=com`. Example of a simple user name: `jbloggs`. Enter a user name that is authorized to access the corporate directory through the LDAP server. **Note:** To use an anonymous connection, leave this field blank.
Password	The password for the specified user name. **Note:** To use an anonymous connection, leave this field blank.
User Entry Settings section	
User DN Pattern	A pattern specifying the Distinguished Name (DN) to use when verifying the user name and password with the LDAP server. Use this option if the DN of the user records in your corporate directory contains a component with a unique user ID for authentication.

Field	Description
	The pattern must contain the string `{0}`, which represents the user name to be validated. For example, `uid={0}, ou=people, dc=mycompany, dc=com`
Search Filter	The LDAP search filter to use when verifying the user name and password with the LDAP server. Use this option if the user records in your corporate directory contain an attribute with a unique user ID for authentication. The field must contain the string `{0}`, which represents the user name to be validated. For example, `(mail={0})`
Base DN	The DN where the **Search Filter** will be applied. For example, `OU=na, OU=Global Users, DC=global, DC=avaya, DC=com`
Search Subtree	If enabled, all subtrees of the base DN will be recursively searched.
Password Verification Settings section	
Bind	Select this option if you want to verify the user's password using a “simple” LDAP bind operation.
Attribute	Select this option if you want to verify the user's password by a direct comparison with a specific attribute in the user's record.
Role Assignment Settings section	
User Entry Attribute	The LDAP attribute Voice Portal should use to determine the group names assigned to the user. This should be an attribute of the user record matched by the **User DN Pattern** or **Search Filter** options. For example, `memberOf`
Group Search Filter	The LDAP search filter Voice Portal should use to match a user in a group record. The field must contain either: • `{0}` to indicate the user’s distinguished name • `{1}` to indicate the specific user ID For example, `(uniqueMember={0})`
Group Entry Attribute	The attribute of the group record that specifies the name of the group. For example, `cn`
Group Search Base DN	The DN where the **Group Search Filter** will be applied. For example, `OU=Global Distribution, DC=global, DC=avaya, DC=com`
Search Subtree	If enabled, all subtrees of the base DN will be recursively searched.

Field	Description
Group Map Name	The group name to associate with a given set of Voice Portal user roles. Use this option to map a group name from the LDAP directory to a set of Voice Portal user roles. This option is necessary when the group names specified in the LDAP directory do not match the role names used by Voice Portal. 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	Display 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 a previously-added group map name.

Roles page field descriptions

Use this page to view the existing Voice Portal Management System (VPMS) user roles.

You can also use this page to add a new custom role, and modify or delete 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 modify or delete the System or Organization roles.
Name	The unique identifier for the user role. **Note:** You cannot change a role name once it is created.
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. • **Custom**: The custom roles are the user defined roles. You can add a new custom role, and modify or delete an existing role. • **Organization**: The organization roles are system defined roles for the organization level access. For more information on organization level

Field or Button	Description
	access see *Organization level access in Voice Portal* in the *User management* chapter in the *Administering Voice Portal* guide.
Assigned To	List of users who are assigned to the corresponding role in the **Name** field.
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.
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. When you delete a custom role, VPMS removes the role from the role list only. The role may still appear in user profiles. For more information about deleting a user role completely, see *Deleting a custom user role* in the *User management* chapter in the *Administering Voice Portal* guide.

Add New Role page field descriptions

Use this page to create a new Voice Portal Management System (VPMS) user roles.

Field or Button	Description
Role 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.
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.

Field or Button	Description
Continue	Opens the Edit Role page. Use this page to modify the user role permissions.

Adding a new user role

Note:
You cannot create and add a new system user role.

1. Log in to the VPMS web interface using an account with the User Manager user role.
2. From the VPMS main menu, select **User Management** > **Roles**.
3. On the Roles page, click **Add**.
4. On the Add New Role page, enter a name for the custom role that you want to add. The role name must be 1 to 256 alphanumeric characters in length.

   Note:
   Once you save the role, the role name cannot be changed.
5. Select a role from the **Start with Role** list. The privileges assigned to the role that you select in this list are used as a base for creating a new user role.
6. Click **Continue**. The Edit Role page opens.

   (Optional) Click the required role to give or remove permissions.

   The status of user permissions is indicated as follows:

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

Changing a user role

Note:
You cannot change the existing user role name.

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

   Note:
   You cannot select the System roles for changing.
4. The Edit Role page is displayed with a hierarchical list of the features made available by the Voice Portal system.
5. 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.
6. Click **Save**.

Deleting a custom user role

Important:
You can delete the custom defined roles that are assigned to the users. On deleting such roles, the deleted roles will continue to display in the user account. However, the users will be unable to use the permissions for the deleted role. To delete these roles completely, clear the selection of the deleted roles from the user account. If required, you can assign users to other roles to manage their access to the Voice Portal system. When you create a role

with the same name as the deleted role, the user profile that still contains the original role name will be automatically assigned the new permissions.

1. Log in to the VPMS web interface using an account with the User Manager user role.
2. From the VPMS main menu, select **User Management** > **Roles**.
3. On the Roles page:
   - Select the check box for the custom user role that you want to delete.
   - Click the Selection check box in the header row of the table, which automatically selects all user roles.
4. Click **Delete**.
   The VPMS deletes all selected VPMS user roles without requesting confirmation.

Cannot access or view certain features in VPMS

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

This problem typically occurs because of the following reasons:

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

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

Related topics:

Proposed Solution on page 34

Proposed Solution

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

Chapter 2: System configuration

Licenses and ports

Voice Portal licenses

The Voice Portal Management System (VPMS) contacts an Avaya WebLM server on a regular basis to determine the number of licenses that are authorized for your system. For security reasons, Voice Portal requires that the license server be running WebLM version 4.4 or later, and that a valid Voice Portal Release 5.1 license be installed on the license server.

After the VPMS receives current information about authorized licenses, it allocates the available licenses among the Media Processing Platform (MPP) servers in the system. Voice Portal requires a license for:

Component	Description
Telephony ports	Each license authorizes you to use one port for telephony activities. A Voice Portal system supports up to 5,000 telephony ports. **Note:** To configure an authorized telephony port on the Voice 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 license for each call that requires ASR resources. The license will not become available again until the call completes.
Text-to-Speech (TTS) connections	Each license authorizes you to use one connection, or port, for speech synthesis activities. If you did not purchase any TTS licenses, you cannot configure TTS servers on your system. You need one TTS license while a call is using TTS resources. As soon as the call stops using TTS resources, the license becomes available to other calls.

Viewing your licenses

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **Security** > **Licensing**.
   The VPMS displays the Licensing page if you are authorized to change the license information, or the View Licensing page otherwise.

Setting the license reallocation time

When you stop or restart an MPP, the VPMS 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 Voice 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.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **MPP Servers**.
3. On the MPP Servers page, click the **MPP Settings** button.
4. On the MPP Settings page, go to the **Miscellaneous** group.
5. Enter the number of minutes to wait in the **License Re-allocation Wait Time** field.
   Enter a whole number from 0 to 1440. The default is 10.
6. Click **Save**.

Configuring the connection to the Avaya license server

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **Security** > **Licensing**.

3. Click **License Server Information** icon .
4. On the License Server Information page, enter the new URL in the **License Server URL** field.

   The URL must be in the format `https://WebLM-machine:port_num/WebLM/LicenseServer`, where *`Weblm-machine`* is the hostname or IP address of the WebLM server and *`:port_num`* is an optional parameter that consists of a colon followed by the port number for the WebLM server. If WebLM uses the default configuration, specify `:8443`. If no port number is specified, Voice Portal sets the default to `:443`.
5. Click **Verify** to ensure that the URL is correct.
6. If your system can connect to the Avaya license server, click **Apply** then click **OK** to confirm.
   Voice Portal immediately polls the Avaya WebLM server to retrieve the current license information and, if successful, updates the fields in the Licensing page.

Updating license information manually

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

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **Security** > **Licensing**.
3. Click **License Server Information** icon .
4. Click **Save** on the License Server URL page.
   Voice Portal polls the license server immediately even if no changes have been made on that page.

Viewing telephony port distribution

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

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **Real-Time Monitoring** > **Port Distribution**.
3. On the Port Distribution page, if you want to view more information about a particular port, click its number in the **Port** column.
   The VPMS 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 VPMS 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 166.
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.

State	Description
Trying	The MPP is trying to register with the port.

Licensing page field descriptions

Use this page to:

- View the number of licenses currently available on the Voice Portal system.
- View the URL that links Voice 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 Voice Portal.

Note:

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

Important:

Voice 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, Voice 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 41
- Licensed Products section on page 42

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 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.

Field	Description
	

Licensed Products section

Field or Button	Description
Voice Portal	
ASR Connections	The number of ASR licenses on your system. This setting is the maximum number of MRCP connections to ASR servers that can be active at any one time.
Announcement Ports	The number of announcement port licenses on your system.
Enhanced Call Classification	The number of enhanced call classification licenses on your system. If the value is a non-zero (positive) number, the enhanced call classification is enabled. If it is zero, the enhanced call classification feature is disabled.
SIP Signaling Connections	The number of SIP Signaling connections licenses on your system.
TTS Connections	The number of Text-to-Speech (TTS) licenses on your system. This setting is the maximum number of MRCP connections to TTS servers that can be active at any one time.
Telephony Ports	The number of Telephony Port licenses on your system.
Video Server Connections	The maximum number of video connections to the video servers on the MPP. If the value is a non-zero (positive) number, the video feature is enabled. If it is zero, the video feature is disabled.
Version	The version number of the license.
Expiration Date	The date when the licence expires.
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.
Voice Portal icon 	Opens the Voice Portal License Settings page for updating the license settings.

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_num`*`/WebLM/LicenseServer`, where *`Weblm-machine`* is the hostname or IP address of the WebLM server and `:`*`port_num`* is an optional parameter that consists of a colon followed by the port number for the WebLM server. If WebLM uses the default configuration, specify `:8443`. If no port number is specified, Voice Portal sets the default to `:443`. **Note:** Unless your site uses a dedicated WebLM server machine, the WebLM server is installed on the Voice Portal VPMS server.
Verify	Opens a new browser window and loads the License Administration page for the WebLM license server. If this page loads properly, then Voice Portal can connect to the license server.

Voice 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 Voice Portal system generates an event that the system does not have enough licenses.

Column or Button	Description
	Enter a value in the range 0 to 5000. • **Maximum**: Indicates the maximum number of licenses to be retrieved by VPMS for that feature. Enter a value in the range 0 to 5000.
SIP Signaling Connections	Specify the minimum and maximum number of licenses. • **Minimum**: Indicates the minimum number of licenses below which the Voice Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 5000. • **Maximum**: Indicates the maximum number of licenses to be retrieved by VPMS for that feature. Enter a value in the range 0 to 5000.
Telephony Ports	Specify the minimum and maximum number of licenses. • **Minimum**: Indicates the minimum number of licenses below which the Voice Portal system generates an event that the system does not have enough licenses. Enter a value in the range 0 to 5000. • **Maximum**: Indicates the maximum number of licenses to be retrieved by VPMS for that feature. Enter a value in the range 0 to 5000.

Port Distribution page field descriptions

Use this page for a real-time view of telephony port distribution across all Media Processing Platform (MPP) servers.

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
Port	The Voice Portal port number associated with the port.

Column	Description
	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 port's operational mode. 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.
State	The port's state. 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 VPMS 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.

Column	Description
	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 is a member of. Port groups are administered on the System Configuration pages.
Protocol	The port protocol.
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 a Voice Portal telephony port.

This window contains the:

- Details group on page 46
- Status group on page 47
- Allocation group on page 48

Details group

Field	Description
Port	The Voice Portal port number associated with the port.
Port Group	The name of the port group that the port is a member of.

Field	Description
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 port's state. 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 VPMS 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 Voice Portal by the switch.
Call Type	If the port is currently being used, displays the type of call that is currently using the port.

Field	Description
Mode	The port's operational mode. 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 Voice Portal

H.323 is an Internet standard set of protocols for the transmission of real-time audio, video, and data using packet-switching technology. Avaya Voice 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 Voice 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 Voice Portal system, the Communication Manager handles this function.

Important:

Avaya strongly recommends that you 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

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **System Configuration** > **VoIP Connections** and go to the H.323 tab.

   From this page, authorized users can also add, delete, or change connections.

Adding H.323 connections

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VoIP Connections** and go to the H.323 tab.

3. Click **Add**.
4. On the Add H.323 Connection page, enter the appropriate information and click **Save**.

Changing H.323 connections

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VoIP Connections** and go to the H.323 tab.
3. Click the name of the connection that you want to change.
4. On the Change H.323 Connection page, enter the appropriate information and click **Save**.

Defining maintenance stations for an H.323 connection

Maintenance stations allow you to isolate call activity to an MPP running in the Test operational mode.

Voice 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 you have MPPs in Test mode, each Test mode MPP is assigned one port and the extra ports are ignored
- More MPPs in Test mode than you have Test mode ports, Voice Portal randomly distributes the available ports to a subset of the MPPs in Test mode

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VoIP Connections** and go to the H.323 tab.
3. If you want to create a new connection:
   a. Click **Add**.
   b. On the Add H.323 Connection page, enter the required information in the General section.

4. If you want to add one or more maintenance stations to an existing connection, click the name of the connection to open the Change H.323 Connection page for that connection.
5. In the **New Stations** group:
   a. Enter the first maintenance station in the **Station From** field.
   b. If you want to enter a range of numbers, enter the last number in the range in the **To** field.
   c. Enter a password in the **Password** field.
   d. Select **Maintenance** in the **Station Type** list box.
   e. Click **Add**.
6. If you want to define another maintenance station or range of numbers, repeat step 5.
7. Click **Save**.

Deleting H.323 connections

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VoIP Connections** and go to the H.323 tab.
3. For each connection that you want to delete, select the check box to the left of the connection's name.

   Tip:
   To delete all connections, click 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 Voice Portal system.

This page contains the:

General section

Field	Description
Name	The unique identifier for this H.323 connection on the Voice 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 Voice 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 Voice 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 another H.323 gatekeeper to use in case the primary gatekeeper is unavailable. 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 Voice 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**: Voice 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 Voice Portal ports you have licensed. For more information on the number of available licenses, see Viewing your licenses on page 38.
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**: Voice Portal uses the password specified in the **Password** field for all stations in the specified range. • **Use sequential passwords**: Voice 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.
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 186.

Field or Button	Description
	Note: If you select **Maintenance**: • You must also specify a password in the **Password** field. • Voice 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 association between the selected entry in the display text box and the connection.

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
Name	The unique identifier for this H.323 connection on the Voice Portal system. **Note:** This field cannot be changed.

Field	Description
Enable	Whether this H.323 connection is available for use by the Voice 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 Voice 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 another H.323 gatekeeper to use in case the primary gatekeeper is unavailable. 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 Voice 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**: Voice 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.

Field or Button	Description
	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 Voice Portal ports you have licensed. For more information on the number of available licenses, see Viewing your licenses on page 38.
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**: Voice Portal uses the password specified in the **Password** field for all stations in the specified range. • **Use sequential passwords**: Voice 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.
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 186. **Note:** If you select **Maintenance**: • You must also specify a password in the **Password** field. • Voice 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 association between the selected entry in the display text box and the connection.

H.323 tab on the VoIP Connections page field descriptions

Use this tab to view, add, or change H.323 connections on the Voice 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.
Name	The unique identifier for this H.323 connection on the Voice 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 Voice 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 Voice Portal system.
Alternative Gatekeeper Address	The network address of another H.323 gatekeeper to use in case the primary gatekeeper is unavailable.
Gatekeeper Port	The port on the gatekeeper that Voice Portal uses for this connection.

Column or Button	Description
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**, Voice 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 Voice 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.

Important:

In Voice Portal, SIP requires Communication Manager with Avaya SIP Enablement Services (SES) enabled. For more information, see the *SIP requirements* topic in the *Planning for Voice Portal* guide.

Viewing existing SIP connections

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **System Configuration** > **VoIP Connections**.
3. Click the SIP tab.

From this page, users logged in with the Administration user role can also add, delete, or change connections.

Adding SIP connections

Prerequisites

Configure the Avaya Communications Manager with Avaya SIP Enablement Services (SES) enabled. For details, see the *Avaya Configuration Note 3911* on the Avaya online support Web site, http://support.avaya.com.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VoIP Connections** and go to the SIP tab.
3. Click **Add**.
4. On the Add SIP Connection page, enter the appropriate information and click **Save**.

Changing SIP connections

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VoIP Connections**.
3. Click the SIP tab.
4. Click the name of the connection that you want to change.
5. On the Change SIP Connection page, enter the appropriate information and click **Save**.

Deleting SIP connections

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VoIP Connections**.
3. Click the SIP tab.
4. For each connection that you want to delete, select the check box to the left of the connection name.

   Tip:
   To delete all connections, click the Selection check box in the header row of the table, which automatically selects all connections.
5. Click **Delete**.

Installing a certificate for TLS authentication

To use TLS authentication, you must install a root certificate on the VPMS server.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **Security** > **Certificates**.
3. Click the Root Certificates tab.
4. Specify the path to the certificate in the **Enter Security Certificate Path** field.
5. Enter the appropriate password in the **Password** field.
6. Click **Install**.

Add SIP Connection page field descriptions

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

Add SIP Connection page

This page contains the:

General section

Column	Description
Name	The unique identifier for this SIP connection on the Voice 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 Voice 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.
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.

Field	Description
	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.
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.

Field	Description
	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 pattern used when routing outbound calls to this trunk. * (asterisk) means that all calls will be 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.
Consultative Transfer	If a connection cannot be established, Consultative Transfer allows Voice Portal to regain control of the call. The following options determine the SIP messages used for a VXML Consultative Transfer: • **INVITE with REPLACES**: When Voice 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. Voice 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. Voice

Field	Description
	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 Voice Portal. The default option is **INVITE with REPLACES**.

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.
Call type radio buttons	The options are: • **All Calls can be either inbound or outbound**: This connection will accept 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, Voice 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**.

SRTP group

Field	Description
Enable	The options are: • **Yes**: This connection uses SRTP. • **No**: This connection does not use SRTP.

Field	Description
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.

Root Certificate tab on the Certificates page field descriptions

Use this tab to view the currently installed security certificate for Voice Portal to use for SIP TLS authentication or to install a new security certificate.

Field or Button	Description
Security Certificate	Displays the current security certificate. **Note:** Voice Portal automatically installs a default root security certificate.

Field or Button	Description
	For information on regenerating the root security certificate, see the *SIP: The root CA certificate will expire in {0} days* topic in the *Troubleshooting Voice Portal* guide.
Enter Security Certificate Path	The fully-qualified path to the security certificate you want to install. **Note:** The certificate must be formatted as a PKCS#12 file that stores both the root certificate and its key. The file must also be encrypted and require a password.
Browse	Click this button if you want to select the certificate file from the Choose file dialog.
Password	The password associated with the security certificate.
Install	Installs the new certificate.

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.

This page contains the:

General section

Column	Description
Name	The unique identifier for this SIP connection on the Voice Portal system. **Note:** This field cannot be changed.
Enable	Whether this SIP connection is available for use by the Voice 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.

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.
Remove	Removes the proxy server.

Field	Description
	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 pattern used when routing outbound calls to this trunk. * (asterisk) means that all calls will be 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.
Consultative Transfer	If a connection cannot be established, Consultative Transfer allows Voice Portal to regain control of the call.

Field	Description
	The following options determine the SIP messages used for a VXML Consultative Transfer: • **INVITE with REPLACES**: When Voice 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. Voice 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. Voice 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 Voice Portal. The default option is **INVITE with REPLACES**.

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.
Call type radio buttons	The options are: • **All Calls can be either inbound or outbound**: This connection will accept 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, Voice 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**.

Field	Description
	- **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**.

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.

Field	Description
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 Voice Portal system.

Note:
While you can configure multiple SIP connections, only one can be active at any one time.

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.
Name	The unique identifier for this SIP connection on the Voice 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 Voice 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.
Listener Port	The port used by the Listener.
SIP Domain	The pattern used when routing outbound calls to this trunk. * (asterisk) means that all calls will be routed to this trunk.

Column	Description
Maximum Simultaneous Calls	The maximum number of calls that this trunk can handle at one time.
Inbound Calls Allowed	The maximum number of simultaneous inbound calls allowed.
Outbound Calls Allowed	The maximum number of simultaneous outbound calls allowed.
Add	Opens the Add SIP Connection page. **Note:** While you can configure multiple SIP connections, only one can be active at any one time.
Delete	Deletes the SIP connections whose associated Selection check box is checked.

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
Supervised transfer (also	Operates like a blind transfer	Supported	Supported

Feature	H.323	H.323 with SA8874 feature	SIP
called consultative transfer)	**Note:** The only supported VoiceXML event for this transfer is `error.connection.noroute`.		
Bridge transfer (see also Bridge transfers in a mixed SIP/H.323 environment on page 75)	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
Consultative Transfer **Note:** If a connection cannot be established, the Consultative Transfer feature in Voice Portal allows the application to regain control of the call.	Supported	Supported	Supported
DTMF detection **Note:** Voice Portal supports only out-band DTMF detection.	Supported	Supported	Supported
Playing prompt files	Supported	Supported	Supported
Recording	Supported	Supported	Supported
Converse-on vectoring	Supported	Supported	Not supported

Feature	H.323	H.323 with SA8874 feature	SIP
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 User-to-User Interface (UUI) data passed in SIP headers on page 235.
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 Voice Portal. For more information, see Universal Call Identifier (UCID) values included in UUI data on page 236.	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 Voice Portal. For more information, see Universal Call Identifier (UCID) values included in UUI data on page 236.	Supports the capability to both send and receive UCID. For more information, see Universal Call Identifier (UCID) values included in UUI data on page 236.
Switch failover	An alternate gatekeeper address	An alternate gatekeeper address	No additional support is supplied by Voice Portal,

Feature	H.323	H.323 with SA8874 feature	SIP
	can be specified in the VPMS, and an alternate gatekeeper address list can come from Communication Manager	can be specified in the VPMS, and an alternate gatekeeper address list can come from Communication Manager	but the Avaya SIP Enablement Services (SES) hardware has failover support and MPPs can be configured as members of an adjunct in the SES
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 Voice Portal system, Voice 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, Voice Portal tries to get an outbound port from the same H.323 port group. If none are available, Voice Portal tries any H.323 port.

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

VoIP in Voice Portal

Voice 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 Voice 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 Voice Portal VoIP settings

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **System Configuration** > **MPP Servers**.
3. On the MPP Servers page, click the **VoIP Settings** button.
   If you are not logged in with the Administration user role, the VPMS displays the VoIP Settings page in view only mode.

Configuring the Voice Portal VoIP settings

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **MPP Servers**.
3. On the MPP Servers page, click the **VoIP Settings** button.
4. On the VoIP Settings page, enter the appropriate information and click **Save**.
5. If you have changed any VoIP settings, restart all MPPs as described in Restarting one or more MPP servers on page 184.

VoIP Settings page field descriptions

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

This page contains the:

- Port Ranges group on page 77
- RTCP Monitor Settings group on page 78
- VOIP Audio Formats group on page 78
- Audio Codecs group on page 79
- QoS Parameters group on page 80
- Out of Service Threshold group on page 81

Port Ranges group

The port range specifies source ports. The range must be large enough to allow for the necessary network connections, which vary based not just on configuration, but load as well.

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** fiel..d. The range must be within 1024 to 65535. The default range is 27000 to 34999. **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 31999. **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 32000 to 32999. The number of MRCP ports you need depends on the setting of the **New Connection per Session** option for the Voice 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.

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 35000 to 50000. **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 VPMS 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. If you want to use this option with a Nuance OSR server, see the *Configuring A-Law encoding for Nuance ASR servers* topic in the *Planning for Voice Portal* guide. 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.

Field	Description
	Note: The AVB ignores this setting if a recording format is specified in a given speech application.

Audio Codecs group

Field	Description
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 Voice Portal. The audio quality is reduced slightly when you enable this option. Voice 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**.
Discontinuous Transmission	The G.729B discontinuous transmission algorithm allows Voice 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.

Field	Description
	The options are: • **Yes**: Select **Yes** to enable this option. • **No**: Select **No** to disable this option. With this option Annexe B is not used. **Note:** The G.729 offers may still be accepted.
First Offered	The media codec that is offered first in the SIP SDP media list. The codecs are offered in the most preferred to the least preferred order, so that a far end media selects the first media codec that it can accept. **Note:** This field is enabled only if you have selected **Yes** in the G729 field. The options are: • **G729** • **G711**

QoS Parameters group

Quality of Service (QoS) is used in network routing to improve performance for certain data streams. 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:

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.

Field	Description
	The default for **VLAN** is 6 and the default for **Diffserv** is 46.
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%	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 Voice 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.

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 Voice 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. If the MPP remains in this state for three minutes, Voice Portal automatically attempts to restart the MPP. If the percentage of out-of-service ports is still above the fatal threshold after the restart, Voice Portal attempts to restart the MPP again. If the percentage of out-of-service ports is still above the fatal threshold after the second restart, Voice Portal attempts to restart the MPP a third time. If the percentage of out-of-service ports is still above the fatal threshold after the third restart, the MPP enters the Error state and must be manually restarted. If the MPP remains in this state for less than three minutes, the MPP will not issue another fatal alarm until the percentage of out of service ports is at or below the value set in the **Reset** field before it once again rises above the value in the **Trigger** field. 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 70 and the **Reset** default is 50.

Determining the installation history on a Voice Portal server

You can check the following data related to the installation history on a Voice Portal server:

- The current version installed on the server by using the `iaversion.php` command.
- All versions since Voice Portal 5.1 that have been installed on the server by using the `iahistory.php` command.
- All versions that have been installed in a particular directory or all directories on the server by using the `GetInstallHistory` and `GetInstallHistory -search_all` commands respectively.

Note:

The `GetInstallHistory` command is disabled in versions higher than Voice Portal 5.1.

Avaya recommends that you use the `iaversion.php` and `iahistory.php` commands for checking the installation history.

1. Log in to Linux on the Voice Portal server.

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

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

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

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

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

   Tip:

   This script is also available in the `Support/VP-Tools` directory of the Voice Portal installation DVD.

3. To search for the current installation that has been made in any subdirectory under `$AVAYA_HOME`, enter the bash `iaversion.php` command

4. To search for all installations since Voice Portal 5.1, made in any subdirectory under `$AVAYA_HOME`, enter the bash `iahistory.php` command.

5. To search for all installations that have been made in any subdirectory under `$AVAYA_HOME`, enter the `bash GetInstallHistory` command.

6. To search for pervious installations in all directories on the server, enter the `bash GetInstallHistory -search_all` command.

   Note:

   This search could take a significant amount of time depending on the number of directories on the server.

Configuring the PostgreSQL database user accounts

Prerequisites

If you have just installed the VPMS software and are still logged into the VPMS server, make sure that the environment variables are properly loaded as described in the *Reloading the Voice Portal environment variables* topic in the *Implementing Voice Portal on multiple servers* guide.

Voice Portal uses the following PostgreSQL user accounts:

Default account name	Description
postgres	The VPMS server uses this account to log in to the Voice Portal database to store and retrieve data, and to install new updates or patches. The database administrator can use this account to log into the local `VoicePortal` database and perform database administration tasks. You can set the password for this account, but you cannot add other accounts of this type, delete this account, or change the account name. **Important:** Contact your Avaya Services representative if you need to modify the local VoicePortal database as the database contains critical configuration information used to run the system.
report	This user account can only read those tables in the Voice Portal database that store report data. Speech application developers can use this account to login to the database to create custom reports using any SQL-enabled report generation tool. You can have any number of accounts of this type with any account names you want to use.
reportwriter	This user account can only change the data in the tables that store report data in the Voice Portal database on the auxiliary VPMS server. You can have any number of accounts of this type with any account names you want to use. **Important:** Contact your Avaya Services representative if you need to modify the tables that store report data in the local VoicePortal database.
vpcommon	This account allows the auxiliary VPMS server limited access the main Voice Portal database, and it is required if you plan to configure a auxiliary VPMS server.

Default account name	Description
	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.

The `SetDbpassword` script allows you to change all account passwords and add and delete all accounts except for postgres, which cannot be deleted.

Note:

This script replaces the `UpdateDbPassword` script that was included with Voice Portal 4.0 or 4.1.

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

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

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

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

2. Navigate to the `Support/VP-Tools/SetDbPassword` directory under the Voice Portal installation directory by entering the `cd $AVAYA_HOME/Support/VP-Tools/SetDbPassword` command.

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

   Tip:

   This script is also available in the `Support/VP-Tools/SetDbPassword` directory on the Voice Portal installation DVD.

3. Navigate to the `Support/VP-Tools/SetDbpassword` directory under the Voice Portal installation directory by entering the `cd $AVAYA_HOME/Support/VP-Tools/SetDbpassword/SetDbpassword.sh` command.

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

   Tip:

   This script is also available in the `Support/VP-Tools` directory of the Voice Portal installation DVD.

4. If you want to:

Options	Description
View a list of all Voice 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`* `-p` *`password`* command, where: • *`username`* is the name of the user account whose password you want to change • *`password`* is the new password you want to use for this account. For example, to set the postgres password to NewPostgres1, you would enter the `bash SetDbpassword.sh update -u postgres -p NewPostgres1` command. **Note:** If you change the password for the: • postgres account, Voice Portal stops and then restarts the VPMS service. • vpcommon account on the primary VPMS server, you must also change the password on the VPMS server as well.
Add a new report user with read only privileges	Enter the `bash SetDbpassword.sh add_report_r -u` *`username`* `-p` *`password`* command, where: • *`username`* is the PostgreSQL account name for the new report user • *`password`* is the password for this account. For example, to create a report account called RptReadOnly and set the password to ReportPW1, you would enter: `bash SetDbpassword.sh add_report_r -u RptReadOnly -p ReportPW1`
Add a new report user with read/write privileges on the VPMS server	Enter the `bash SetDbpassword.sh add_report_w -u` *`username`* `-p` *`password`* command, where: • *`username`* is the PostgreSQL account name for the new report user

Options	Description
Note: **You cannot add a report user with read/write privileges on the primary VPMS server.**	• *password* is the password for this account. For example, to create a report account called RptReadWrite and set the password to ReportPW2, you would enter: `bash SetDbpassword.sh add_report_r -u RptReadWrite -p ReportPW2`
Delete a report account from either VPMS server or delete the vpcommon account from the primary VPMS server	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`
Note: **You cannot delete the postgres user account.**	
Add the vpcommon user account on the primary VPMS server so that an VPMS server can access the database	Enter the `bash SetDbpassword.sh add_vpcommon -p` *password* command, where *password* is the password for this account. For example, to create the vpcommon account and set the password to CommonPW1, you would enter: `bash SetDbpassword.sh add_vpcommon -p CommonPW1`
Note: **You cannot add the vpcommon account to the VPMS server.**	
View the help for this command	Enter the `bash SetDbpassword.sh help` command.

Chapter 3: Organization level access

Organization level access in Voice Portal

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

Important:

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

For more information, see Configuring organization level access in Voice Portal on page 90.

In the following VPMS 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

For more information on the access allowed to organization level users, see Organization level roles on page 92.

Organizational level access is created in Voice 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 VPMS.

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.

Configuring organization level access in Voice Portal

To configure multi-tenancy in Voice Portal Management System (VPMS), you need to enable organization level access in Voice Portal.

Note:

By default, organization level access is disabled.

Related topics:

[Enabling organization level access in Voice Portal](#) on page 90
[Disabling organization level access in Voice Portal](#) on page 91

Enabling organization level access in Voice Portal

1. Log in to Linux on the Voice Portal primary VPMS server.

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

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

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

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

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

Tip:

This script is also available in the `Support/VP-Tools` directory of the Voice Portal installation DVD.

3. Enter the `EnableOrganizations` command to enable organization level access in Voice Portal.
4. Type `Y` and press `Enter` when prompted to restart the vpms service.

Result

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

Note:

Log into the VPMS web interface using an account with the User Manager user role.

For more information on creating organization level access in Voice Portal, see Organization level access in Voice Portal on page 89

Disabling organization level access in Voice Portal

Note:

By default, organization level access is disabled.

1. Log in to Linux on the Voice Portal primary VPMS server.

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

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

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
2. Navigate to the `Support/VP-Tools` directory by entering the `cd $AVAYA_HOME/Support/VP-Tools` command.

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

Tip:

This script is also available in the `Support/VP-Tools` directory of the Voice Portal installation DVD.

3. Enter the `EnableOrganizations --disable` command to disable organization level access in Voice Portal.
4. Type `Y` and press `Enter` when prompted to restart the vpms service.
   The **Organizations** page is disabled in **VPMS > User Management**.

Organization level roles

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

- Org User Manager
- Org Auditor
- Org Administration
- Org Reporting
- Org Web Services

Note:

Custom roles are not available for organization level users.

Organization level users can perform the following actions in these web pages based on their role:

Organization level Role	Web Page	Description
Org User Manager	*Users*	User accounts with Org User Manager access can add new users to their organization. They can change, delete, unlock, or reset password for existing users in their organization.

Organization level Role	Web Page	Description
Org Auditor	*Audit Log Viewer*	User accounts with Org Auditor access can view the audit log entries for the users in their organization.
Org Administration	*Applications*	User accounts with Org Administration access can view and edit the configurable application variables of the applications in their organization. **Note:** User accounts with Org Administration access cannot add, change or delete applications which belong to their organization.
Org Administration	*Active Calls*	User accounts with Org Administration access can view the active calls for their organization.
Org Administration and *Org Reporting*	*Standard Reports*	User accounts with Org Administration and Org Reporting access can run standard reports for their organization related data. **Note:** Organization level administrator cannot run the performance report.
Org Administration and *Org Reporting*	*Custom Reports.*	User accounts with Org Administration and Org Reporting access can run standard reports for their organization related data.
Org Administration and *Org Reporting*	*Scheduled Reports*	User accounts with Org Administration and Org Reporting access can add, change, delete, and view the scheduled reports output for their organization.
Org Web Services	This user role is related to the Application Interface and Application logging Web Service.	User accounts with Org Web Services access can use Application Interface Web Service to launch

Organization level Role	Web Page	Description
		applications that belong to their organizations. They can also use Application Logging Web Service to save application and breadcrumb information for any application.

Organizations page field descriptions

Use this page to add organizations to the Voice Portal Management system (VPMS). 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.
Organization Name	The name for the organization. **Note:** You cannot change the **Organization Name** after creating it.
Add	Opens the Add Organization page for defining a new organization.
Delete	Deletes the selected organization. You can select an organization using the check box next to the **Organization Name**.

Add Organization page field descriptions

Use this page to add organizations to the system.

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

Field or Button	Description
Organization Name	The name for the organization that you want to add. **Note:** You cannot change the **Organization Name** after creating it.
Save	Saves the newly added organization name.

Chapter 4: Server and database administration

VPMS server administration

Changing VPMS server settings

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

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VPMS Servers**.
3. On the VPMS Servers page, click **VPMS Settings**.
4. On the VPMS Settings page, enter the appropriate information and click **Save**.

Configuring an auxiliary VPMS server

The auxiliary VPMS server:

- Can assign outgoing calls made with the Application Interface web service to an available MPP server. Voice 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 VPMS server is in service.

Note:
When using the Application Logging web service, Dialog Designer 5.1 provides failover and load balancing between the primary and auxiliary VPMS 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 VPMS is down
- Does *not* include the VPMS web interface, therefore it cannot be used to administer the system or monitor the status of the MPP servers.

---

1. If the vpcommon PostgreSQL database user account was not created on the primary VPMS server during the VPMS software installation, or if you need to reset the password for that account:
   a. Log in to Linux on the Voice Portal primary VPMS server.

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

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

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

   b. Navigate to the `Support/VP-Tools/SetDbpassword` directory by entering the `cd $AVAYA_HOME/Support/VP-Tools/SetDbpassword/SetDbpassword.sh` command.

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

      Tip:

      This script is also available in the `Support/VP-Tools` directory of the Voice Portal installation DVD.

   c. Enter the `bash SetDbpassword.sh add_vpcommon -p` *`password`* command.

      Where Enter the `bash SetDbpassword.sh add_vpcommon -p` *`password`* command.

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

   When you get to the Database Login Check for Auxiliary VPMS 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 Voice Portal system:
   a. Log in to the VPMS web interface.

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

Otherwise, log in to the VPMS using an account with the Administration user role.

b. From the VPMS main menu, select **System Configuration** > **VPMS Servers**.

c. On the VPMS Servers page, click **Add**.

d. On the first Add VPMS Server page, enter the appropriate information and click **Continue**.

e. On the second Add VPMS Server page, enter the appropriate information.

If you logged in using the init account, make sure you enter the appropriate LDN number for the server in the **LDN** field. If you do not specify an LDN number, Voice Portal uses the default value (000)000-0000.

f. Click **OK**.

Changing the configuration information for a VPMS server

1. Log in to the VPMS web interface.

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

   Otherwise, log in to the VPMS using an account with the Administration user role.

2. From the VPMS main menu, select **System Configuration** > **VPMS Servers**.

3. On the VPMS Servers page, click the name of the VPMS server whose settings you want to change.

4. On the Change VPMS Server page, enter the appropriate information and click **Save**.

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

Relinking the primary and auxiliary VPMS servers

1. Log in to the VPMS web interface.

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

   Otherwise, log in to the VPMS using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VPMS Servers**.
3. On the VPMS Servers page, click the name of the auxiliary VPMS server.
4. On the Change VPMS Server page, enable the **Trust new certificate** check box in the **VPMS Certificate** section.

   If you logged in using the init account, make sure 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 VPMS server

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VPMS Servers**.
3. On the VPMS Servers page, click the Selection check box next to the name of the auxiliary VPMS server.
4. Click **Delete**.

Stopping the VPMS service

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

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

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

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

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

2. Stop the `vpms` service by entering the `/sbin/service vpms stop` command. You will see a series of messages as the command shuts down several VPMS components. When the command has successfully stopped all relevant components, it displays the message: `VPMS Shutdown Status: [ OK ].`

Next steps

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

Moving the Voice Portal software

Move the Voice Portal software to a different server machine

If required, you can move the Voice Portal software to a different server machine. In all cases, you should make every effort to 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 Voice Portal system configuration.

If you want to:

- Move the VPMS software to a new server in a system where the VPMS and MPP software runs on different servers, see Move the VPMS software to a different server machine on page 102.
- Move the MPP software to a new server in a system where the VPMS and MPP software runs on different servers, see Moving an MPP to a different dedicated server on page 104.
- Move the Voice Portal software in a system where the VPMS and the MPP run on the same server, see Move a single-server Voice Portal system to a different server on page 106.

Move the VPMS software to a different server machine

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

- Move the VPMS software in a system where the VPMS and the MPP software runs on the same server, see Move a single-server Voice Portal system to a different server on page 106.
- Move the auxiliary VPMS software, simply install the software on the new server as described in #unique_91.

Important:

Because these steps build on each other, you must complete them in the order given or you may encounter errors during the procedures.

Step	Description	✔
1	On the old VPMS server, back up the Voice Portal database as described in System Backup Overview on page 122.	
2	If possible, set up the new server so that it has the same IP address and hostname as the old VPMS server.	
3	On the new VPMS server, install the operating system and the VPMS server software as if this was a new installation. If at all possible, the new VPMS server should have the same hostname and IP address as the old VPMS server in order to minimize the number of manual changes you will need to make.	

Step	Description	✔
	Important: Make sure you: • Perform all software prerequisites, such as synchronizing the time between the new VPMS 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 VPMS server with an external time source, make sure you configure the new server to use that time source as well.	
4	On the new VPMS server, configure the backup and restore scripts as described in Verifying the backup server mount point on page 133. Make sure that you specify the same mount point and shared directory that you used on the old VPMS sever.	
5	Restore the Voice Portal database from the backup you made on the old VPMS server as described in Database Restore utility on page 133.	
6	If you could not use the same hostname and IP address for the new VPMS server, change the information in the Voice Portal database as described in Changing the hostname or IP address on a dedicated primary VPMS server on page 115.	
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 VPMS server as described in Reconnecting an existing MPP server with the VPMS server on page 103.	
8	If your WebLM server ran on the old VPMS server, install the Voice Portal license file on the new VPMS server as described in the *Installing the license file* topic in the *Implementing Voice Portal on multiple servers* guide. Otherwise, verify that the new VPMS server can contact the WebLM sever by selecting **Security** > **Licensing** from the VPMS main menu and clicking **Verify** on the Licensing page.	

Reconnecting an existing MPP server with the VPMS server

In a dedicated server environment, if the IP address or hostname of the VPMS server changes or if you reinstalled the VPMS software, you need to reconnect all MPP servers with the VPMS server.

1. Log in to Linux on the Voice Portal MPP server.

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

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

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

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

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

   Tip:

   This script is also available in the `Support/VP-Tools` directory of the Voice Portal installation DVD.

3. Associate this MPP server with the VPMS server by entering the `setup_vpms.php` *`myhost`* command, where *`myhost`* is the server name or IP address where the VPMS software is installed.
4. Follow the on-screen prompts to install the certificate, restart Apache, and configure Network Time Protocol (NTP).

Next steps

If necessary, relink the VPMS server with the MPP server as described in Reestablishing the link between the VPMS and an MPP on page 105.

Moving an MPP to a different dedicated server

Note:

This procedure applies to a Voice Portal system in which the MPP software runs on a dedicated server. If you need to move the MPP in a system where the VPMS and the MPP run on the same server, see Move a single-server Voice Portal system to a different server on page 106.

1. If you want to transfer the MPP log files:
   a. Log into the MPP Service Menu as described in Logging in to the MPP Service Menu on page 191.

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 Voice 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 Voice 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 110.

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 in to the VPMS web interface 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 169.

6. Reestablish the link between the VPMS and the MPP as described in Reestablishing the link between the VPMS and an MPP on page 105.

Reestablishing the link between the VPMS and an MPP

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

2. From the VPMS main menu, select **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. At the bottom of the page, click **Save**.
6. From the VPMS main menu, select **System Management** > **MPP Manager**.
7. On the MPP Manager page, look at the **Mode** column for this server. If it says **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 moments, click **Refresh** to verify that the **Mode** column now says **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. If desired, make sure that telephony ports were correctly allocated to the MPP server:
    a. From the VPMS main menu, select **Real-Time Monitoring** > **Port Distribution**.
    b. On the Port Distribution page, examine the **Current Allocation** column to find the ports allocated to this MPP.
    c. Look at the **Mode** and **State** columns to make sure the assigned ports are ready to receive calls.

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

This procedure applies to a Voice Portal system in which the VPMS software runs on the same server as the MPP software. If you need to move the VPMS or MPP software in a system where the VPMS and the MPP run on different servers, see Move the VPMS software to a different server machine on page 102 or Moving an MPP to a different dedicated server on page 104.

Important:

Because these steps build on each other, you must complete them in the order given or you may encounter errors during the procedures.

Step	Description
1	On the old Voice Portal server, back up the Voice Portal database. For more information, see System Backup Overview on page 122.

Step	Description
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 107.
3	If possible, set up the new server so that it has the same IP address and hostname as the old Voice Portal server.
4	On the new server, install the Voice Portal software. For more information, see *Installing the Voice Portal software* topic in the *Implementing Voice 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 Voice 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 Voice Portal on multiple servers* guide.
5	On the new Voice Portal server, configure the backup and restore scripts as described in Verifying the backup server mount point on page 133. Make sure that you specify the same mount point and shared directory that you used on the old sever.
6	Restore the Voice Portal database from the backup you made on the old VPMS server as described in Database Restore utility on page 133.
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 110.
8	If you could not use the same hostname and IP address for the new VPMS server, change the information in the Voice Portal database as described in Changing the hostname or IP address on a dedicated primary VPMS server on page 115.
9	Reestablish the link between the VPMS and the MPP as described in Reestablishing the link between the VPMS and an MPP on page 105.
10	If your WebLM server ran on the old VPMS server, install the Voice Portal license file on the new VPMS server as described in the Installing the license file topic in the *Implementing Voice Portal on multiple servers* guide. Otherwise, verify that the new VPMS server can contact the WebLM sever by selecting **Security** > **Licensing** from the VPMS main menu and clicking **Verify** on the Licensing page.

Packing MPP logs and transcriptions in a TAR file

You can use the Diagnostics in the MPP 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.

1. Log into the MPP Service Menu.
2. From the MPP Service Menu, select **Diagnostics**.
3. On the Diagnostics page, click **Pack Files**.
4. On the Pack Files Options page, select the files you want to pack. You can select any or all of the following:
   - Select all check box: Pack all available files.
   - **Logs**: Pack all the MPP log files.
   - **Transcriptions and utterances**: Pack all the transcriptions and utterances saved by the applications running on the MPP.
   - **Debug files**: Pack all the debug (trace) data recorded on the MPP.
5. Click **Pack**.
   Voice Portal creates a TAR file with the format *<hostname>*_*<date and time stamp>*_MPP.tar that contains all of the selected information. In addition, Voice Portal creates a TAR file for each MPP component with the format *<MPP component>*_*<hostname>*_*<date and time stamp>*_MPP.tar.

   Voice 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.

Note:
You can also pack the log files from the Diagnostics page in the MPP Service Menu.

1. Log in to Linux on the Voice Portal MPP server.

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

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

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

Note:

You can run this script as an avayagroup member, but if you run this script while logged in as `root` or sroot, it collects additional log files.

2. Navigate to the MPP `bin` directory by entering the `cd $AVAYA_MPP_HOME/bin` command.
3. Enter the `getmpplogs.sh` command with the desired options. You can select:

Option	Purpose
--web	To export a TAR file from the `$AVAYA_MPP_HOME/web/admin/AVPSupport` directory that can be accessed from the web browser. If this command option is not used, the TAR file can be found in the `$AVAYA_MPP_HOME/tmp/AVPSupport/` directory.
--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.

Option	Purpose
--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/web/admin/AVPSupport` 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

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 MPP Service Menu.

The `restorempplogs.sh` script:

- Stops the MPP service
- Restores the call data records
- Restores the installation logs
- Restores the process logs, if available
- Restores the transcriptions and utterances, if available
- Restarts the MPP service

1. If the MPP was started through the VPMS:
   a. Log in to the VPMS web interface using an account with the Administration or Operations user role.
   b. From the VPMS 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**.

2. Log in to Linux on the Voice Portal MPP server.

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

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

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

3. Restore the log files by entering the `bash restoreMPPlogs.sh <path/file.tar>` command, where *<path/file.tar>* is the fully qualified path and file name of the TAR file created by the **Pack** command or the `getMPPlogs.sh` script.

   If the script finds the TAR 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/transcription` 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 VPMS server and therefore will not be accessible to any reports created through the VPMS.

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.

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.

Pack Files Options page field descriptions

Use this page to combine one or more log files into a single compressed file that you can send to Avaya support if you are trying to troubleshoot a problem with the MPP.

Field or Button	Description
Select all check box	Pack all available files.
Logs	Pack all of the MPP log files.

Field or Button	Description
Transcriptions and utterances	Pack all of the transcriptions and utterances saved by the applications running on the MPP.
Debug files	Pack all the debug (trace) data recorded on the MPP.
Pack	When you click **Pack**, Voice Portal creates a TAR file with the format *<hostname>_<date and time stamp>*_MPP.tar that contains all of the selected information. In addition, Voice Portal creates a TAR file for each MPP component with the format *<MPP component>_<hostname>_<date and time stamp>*_MPP.tar.

Port Distribution page field descriptions

Use this page for a real-time view of telephony port distribution across all Media Processing Platform (MPP) servers.

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
Port	The Voice Portal port number associated with the port. 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 port's operational mode. 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.
State	The port's state.

Column	Description
	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 VPMS 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 is a member of. Port groups are administered on the System Configuration pages.
Protocol	The port protocol.
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*>.

Column	Description
	• 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 Voice Portal servers

If you need to change the IP address or hostname of any server running the Voice Portal software after that 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 Voice Portal database to match the new system configuration.

If you want to change the IP address or hostname of:

- The primary VPMS server in a dedicated server environment, see Changing the hostname or IP address on a dedicated primary VPMS server on page 115.
- The auxiliary VPMS server in a dedicated server environment, see #unique_106.
- An MPP server in a dedicated server environment, see Changing the hostname or IP address for a dedicated MPP server on page 117.
- The Voice Portal server running the VPMS and MPP software in a single server environment, see Changing the hostname or IP address for the Voice Portal single server system on page 120.

Changing the hostname or IP address on a dedicated primary VPMS server

If you need to change the IP address or hostname of a dedicated primary VPMS server after the VPMS software is installed, or if you need to move the primary VPMS software to a new

server that has a different IP address and hostname, you need to change the information stored in the Voice Portal database to match the new system configuration.

Note:

If you want to change the IP address or hostname for a single server Voice Portal system, follow the steps in Changing the hostname or IP address for the Voice Portal single server system on page 120. If you want to change the IP address or hostname for a auxiliary VPMS server, follow the steps in #unique_106.

1. Log in to Linux on the Voice Portal primary VPMS server.

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

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

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

2. Stop the `vpms` service by entering the `/sbin/service vpms stop` command. You will see a series of messages as the command shuts down several VPMS components. When the command has successfully stopped all relevant components, it displays the message: `VPMS Shutdown Status: [ OK ].`

3. If you want to change the hostname or IP address of the current server:

   a. If you are using Avaya Enterprise Linux, enter the `/opt/ecs/install/bin/netconfig` command and follow the prompts to set the new IP address or hostname.

   b. If you are using Red Hat Enterprise Linux Server Release 5.4, use the neat tool as described in your Red Hat documentation.

   c. 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.

   d. Reboot the VPMS server.

4. Navigate to the backup script directory by entering the `cd /opt/Avaya/VoicePortal/Support` command.

5. Enter the `bash do_UpdateHost` command to change the hostname in the database to the hostname of the current server.
   The script restarts the vpms service automatically. After all relevant components are started successfully, it displays the message: VPMS Start Status: [OK].

6. Enter the `setup_vpms` command to re-authorize the security certificate.

Next steps

Reconnect the existing MPP server with the VPMS server. For more information see, Reconnecting an existing MPP server with the VPMS server on page 103.

Changing the hostname or IP address for a dedicated MPP server

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 Voice Portal database to match the new system configuration.

Note:

If your Voice Portal system consists of a single server, follow the steps in Changing the hostname or IP address for the Voice Portal single server system on page 120.

1. Log in to Linux on the Voice Portal MPP server.

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

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

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

2. Stop the `mpp` service by entering the `service mpp stop` command.
3. If you want to change the hostname or IP address of the current server:
   a. If you are using Avaya Enterprise Linux, enter the `/usr/sbin/netconfig` command and follow the prompts to set the new IP address or hostname.
   b. If you are using Red Hat Enterprise Linux Server Release 5.4, use the neat tool as described in your Red Hat documentation.
   c. Log in to Linux on the Voice Portal primary VPMS server.

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

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

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

d. Open the `/etc/hosts` file on the primary VPMS server in an ASCII editor and change the IP address and hostname for the MPP to the values you specified with the configuration tool.

e. Reboot the primary VPMS server.

f. Reboot the MPP server.

4. Log in to the VPMS web interface.

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

   Otherwise, log in to the VPMS using an account with the Administration user role.

5. From the VPMS main menu, select **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, make sure 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 on the auxiliary VPMS server

If you need to change the IP address or hostname of the auxiliary VPMS server after the VPMS software has been installed, or if you need to move the auxiliary VPMS software to a new server that has a different IP address and hostname, you need to change the information stored in the Voice Portal database to match the new system configuration.

Note:

If you want to change the IP address or hostname for the primary VPMS server, follow the steps in Changing the hostname or IP address on a dedicated primary VPMS server on page 115.

1. Log in to Linux on the auxiliary VPMS server.

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

   • Log in to the local Linux console as sroot.

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

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

2. Stop the `vpms` service by entering the `/sbin/service vpms stop` command. You will see a series of messages as the command shuts down several VPMS components. When the command has successfully stopped all relevant components, it displays the message: `VPMS Shutdown Status: [ OK ].`
3. If you want to change the hostname or IP address of the current server:
   a. If you are using Avaya Enterprise Linux, enter the `/opt/ecs/install/bin/netconfig` command and follow the prompts to set the new IP address or hostname.
   b. If you are using Red Hat Enterprise Linux Server Release 5.4, use the neat tool as described in your Red Hat documentation.
   c. 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.
   d. Reboot the VPMS server.
4. Navigate to the backup script directory by entering the `cd /opt/Avaya/VoicePortal/Support` command.
5. Enter the `bash do_UpdateHost` command.

   The script prompts the following message:

   Selection of VPMS address update:

   (1) Primary VPMS (2) auxiliary VPMS (local)

   a. To enter a new IP address for the primary VPMS server
      - Select 1
      - Enter the new IP address for the primary VPMS server
      - Press Enter
   b. To update the hostname in the database to the hostname of the current (auxiliary VPMS) server
      - Select 2
      - Press Enter

   The script restarts the vpms service automatically. After all relevant components are started successfully, it displays the message: VPMS Start Status: [OK].

Note:

To update the IP address of the primary VPMS server as well as the auxiliary VPMS server, you need to run the `bash do_UpdateHost` command twice and repeat this step.

6. Enter the `setup_vpms` command to re-authorize the security certificate.
7. Update the link between the primary and auxiliary VPMS servers:
   a. Log in to the VPMS web interface.

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

      Otherwise, log in to the VPMS using an account with the Administration user role.

   b. From the VPMS main menu, select **System Configuration** > **VPMS Servers**.
   c. On the VPMS Servers page, click the name of the auxiliary VPMS server.
   d. On the Change VPMS Server page, update the information in the **Host Address** field.

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

   e. Click **OK**.

Next steps

Reconnect the existing MPP server with the VPMS server. For more information see, Reconnecting an existing MPP server with the VPMS server on page 103.

Changing the hostname or IP address for the Voice Portal single server system

If you need to change the IP address or hostname of the Voice Portal server after the VPMS and MPP software has been installed, or if you need to move the Voice Portal software to a new server that has a different IP address and hostname, you need to change the information stored in the Voice Portal database to match the new system configuration.

Note:

If your Voice Portal system consists of one or more dedicated servers, follow the steps in Changing the hostname or IP address on a dedicated primary VPMS server on page 115.

1. Log in to Linux on the Voice Portal server.

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

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

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

2. Stop the `vpms` service by entering the `/sbin/service vpms stop` command. You will see a series of messages as the command shuts down several VPMS components. When the command has successfully stopped all relevant components, it displays the message: `VPMS Shutdown Status: [ OK ]`.

3. Stop the `mpp` service by entering the `service mpp stop` command.

4. If you want to change the hostname or IP address of the current server:

   a. If you are using Avaya Enterprise Linux, enter the `/opt/ecs/install/bin/netconfig` command and follow the prompts to set the new IP address or hostname.

   b. If you are using Red Hat Enterprise Linux Server Release 5.4, use the neat tool as described in your Red Hat documentation.

   c. 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.

   d. Reboot the Voice Portal server.

5. Navigate to the backup script directory by entering the `cd /opt/Avaya/VoicePortal/Support` command.

6. Enter the `bash do_UpdateHost` command to change the hostname in the database to the hostname of the current server.
   The script restarts the vpms service automatically. After all relevant components are started successfully, it displays the message: VPMS Start Status: [OK].

7. Start the `mpp` service by entering the `service mpp start` command.

8. If the application server is co-resident with the Voice Portal single server system, verify and/or change the hostname or IP address referenced in the System Configuration > Applications page

   a. From the VPMS main menu, select **System Configuration > Applications**.

   b. Verify the hostname or IP address

Next steps

Reconnect the existing MPP server with the VPMS server. For more information see, Reconnecting an existing MPP server with the VPMS server on page 103.

Local database maintenance

System Backup

System Backup Overview

You can use the System Backup feature in the Voice Portal Management System (VPMS) to regularly back up the data in a local Voice Portal database and the associated properties files.

Note:
Before you can use the System Backup feature in VPMS, you must complete the tasks in Database backup prerequisites on page 123.

The System Backup web page in VPMS allows you to perform the following backup tasks:

- *Server configuration*—Configure the backup server and verify the backup server connectivity. For more information, see Backup Server page field descriptions on page 129.
- *Backup operation*—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 131.
- *Custom properties*—Backs up Voice Portal database, the associated default properties files, and the specified custom files. Using the enhanced backup, you can also backup user components along with the default properties. For more information, see User Components page field descriptions on page 132.
- *Multiple backup packages*—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 129.

  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. You can select any package that is available in the retained backup list and restore the critical data.

The System Backup copies the Voice Portal database and the property files from the VPMS 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.

Tip:

Avaya recommends that 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 VPMS.

✔	Description
	Make sure that there is enough disk space to store a copy of the database.
	Verify that the port mapper service is running on the Voice Portal server as described in Verifying the port mapper service status on page 123.
	Set up the Linux or Windows backup server. For details, see: • Setting up a Linux backup server on page 124 • Setting up a Windows backup server on page 125

Verifying the port mapper service status

Prior to performing a backup or restore, verify that the port mapper service is running.

1. Log in to Linux on the Voice Portal primary VPMS server.

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

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

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

2. Enter the `/sbin/service portmap status` command from the shell prompt.

3. If the service is stopped, enter the `/sbin/service portmap start` command.
4. After you start the service, wait for it to initialize and then check the status again to verify that it has started correctly.

Setting up a Linux backup server

Prerequisites

Make sure that you can run the X Windows System as described in your Red Hat Enterprise Linux documentation.

---

1. Log in to Linux on the backup server with the user account that Voice 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. For example:
   $>id backupuser uid=500(backupuser) gid=500(backupuser) groups=500(backupuser) context=user_u:system_r:unconfined_t
3. Create the directory for the backup. For example, if you want Voice Portal to store the backup in the `/home/voiceportal/backup` directory, enter the `mkdir /home/voiceportal/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 Voice Portal, using the following format:
   `<BackupDir> <VoicePortalAddress>(rw,sync,all_squash,anonuid=<UID>)` where
   - `<BackupDir>` is the name of the directory to be shared. For example, `/home/voiceportal/backup`.
   - `<VoicePortalAddress>` is the IP address of the Primary VPMS server that accesses the backup directory.
   - `<UID>` is the ID of the user account that Voice Portal uses when accessing the backup directory.
7. Save and close the file.
8. Enter the following commands to restart the portmap and NFS service:
   - #>service portmap restart
   - #>service nfs restart

Setting up a Windows backup server

You can set up shared directories between the main Voice Portal server and a Windows 2000 or Windows XP backup server.

Note:

You cannot connect to a Windows server unless you have Samba or some other connection utility. For details, see the Red Hat Web site, http://www.redhat.com.

1. Log into the Windows back up server using an Administrator account name and password.
2. If desired, add a new Windows user that will be authorized to access the Voice Portal database. For more information adding a new Windows user, see the Microsoft Windows documentation.

   The default user name is postgres. If you want to use a different user name, make sure you modify the **System Management** > **System Backup** web page in VPMS. For more information, see Backup Server page field descriptions on page 129.
3. Create the directory that you want to share with the Voice Portal server.
4. Right-click on the directory in Windows Explorer and select **Sharing and Security** to set the shared permissions.
5. In the <folder name> Properties dialog box, go to the **Sharing** tab.
6. Select **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 database 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 `BackupVPMSServer` and the Windows user name is `postgres`, you would enter `BackupVPMSServer\postgres`.
10. Click **OK** to return to the Permissions dialog box.
11. In the **Group or user names** list box, select the user you just added.
12. Enable the **Change** and **Read** check boxes in the **Allow** column for that user. The **Full Control** permission is optional.

13. Click **OK** to save your changes and return to the <folder name> Properties dialog box.
14. Click **OK**.

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

Field	Description
Server Type	Type of the backup server type. The options are: • PC Windows • RH Linux
Server Address	Network address of the backup server. The network address should be 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.
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
VP Database/ Properties	Voice Portal data that includes the Voice 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.  **Note:** The number of maximum packages to be saved is based on the configured **Number of Backup(s) to Retain** value. Each backup data is formed as a package. The package name follows the `pkg_timestamp` format, where the time stamp is in milliseconds.
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.

Button	Description
	Tip: Avaya recommends that you 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 131 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 128
- Backup Scheduler section on page 129
- Backup Components section on page 129
- Backup History section on page 129

Backup Server section

Field	Description
Server Type	Type of the backup server type. The options are: • PC Windows • RH Linux
Server Address	Network address of the backup server. The network address should be 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.
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
VP Database/ Properties	Voice Portal data that includes the Voice 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. **Note:** The number of maximum packages to be saved is based on the configured **Number of Backup(s) to Retain** value. Each backup data is formed as a package. The package name follows the `pkg_timestamp` format, where the time stamp is in milliseconds.
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 130
- Number of Backup(s) to Retain section on page 130
- State Commands on page 130

Backup Server section

Field	Description
Server Type	Type of the backup server. The options are: • PC Windows • RH Linux
Server Address	Network address of the backup server. The network address should be 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.
Backup Folder	Name of the folder where the backup data is stored. The backup folder name 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.
Username	The user name used to mount the backup server. This field is displayed only when the backup server type selected is **PC Windows**.
Password	The password used to connect and mount the backup server. This field is displayed only when the backup server type selected is **PC Windows**.
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.

Button	Description
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: • PC Windows • RH Linux
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**.
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.
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:

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.

Database Restore utility

Database Restore utility

You can use the Database Restore utility to restore your Voice Portal database from a backup created through the **System Backup** web page in VPMS.

To restore your Voice Portal database:

- Ensure the backup server mount point tis updated in the `do_MntDrv` script. For more information, see Verifying the backup server mount point on page 133.
- Use the do_RestoreData script for restoring data. For more information, see Restoring data backed up from System Backup on page 135.

Important:

If your primary Voice Portal server fails and cannot be recovered, you must first reinstall the VPMS software on a new server. Then you can restore your Voice Portal database using the Database Restore utility.

For details about the **System Backup** feature in VPMS, see System Backup Overview on page 122.

Verifying the backup server mount point

The Database Backup utility `do_MntDrv` script, used during the restore procedure, creates a shared directory at the mount point on the Voice 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 some 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** VPMS 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.

1. Log in to Linux on the Voice Portal primary VPMS server.

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

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

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` 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 [type] [host address] shared_dir [Windows_user]` where
   - `[type]` is either `linux` or `pc` based on the type of back up server you are using.
   - *`[host address]`* is the backup server name or IP 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.
   - *`[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`.
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** VPMS 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\VP_dbbackup` as the shared directory in the **System Backup>Backup Server** VPMS web page, verify the `do_MntDrv` script is as follows:

     ```
     bash MntDrive pc voiceportal-xp-backup VP_dbbackup
     postgres
     ```

     For example: `bash MntDrive pc 148.147.46.89 VP_bu postgres`.
5. Save and close the file if `do_MntDrv` is updated.

Restoring data backed up from System Backup

Prerequisites

The Voice Portal software version must be the same version that was used to create the backup.

Ensure that the server you want to restore has the same postgres account and password as the backed up server.

Verify the `do_MntDrv` script. For further information, see Verifying the backup server mount point on page 133.

You can choose the backup data package you want to restore during the restore process. The number of packages prompted for selection, depends on the configuration in **System Management** > **System Backup** page in VPMS.

For more information, see Backup Server page field descriptions on page 129.

1. Log in to Linux on the Voice Portal primary VPMS server.

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

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

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
2. Stop the vpms service by entering the `/sbin/service vpms stop` command.
3. Enter the `/sbin/service appserver stop` command to stop the application server.
4. Enter the `/sbin/service avpSNMPAgentSvc stop` command to stop the avpSNMPAgentSvc service.
5. Navigate to the backup directory located in $AVAYA_HOME by entering the cd `$AVAYA_HOME/Support/Database/DBbackup` command.
6. Enter the `do_MntDrv` command.
7. Restore the database by entering the `bash do_RestoreData` command.

   Note:
   The `do_RestoreData` command will first clean the database .

The list of existing backup packages saved in the backup server is displayed.

8. Select the package for Voice Portal data restore.
9. Press Enter to continue.
   The script completes the restore process.
10. Restart the `vpms` service by entering the `/sbin/service vpms start` command.
11. Restart the application server by entering the `/sbin/service appserver start` command.
12. Restart the `avpSNMPAgentSvc` service by entering the `/sbin/service avpSNMPAgentSvc start` command.
13. If the hostname or IP address of the any server running the VPMS or MPP software has changed since you created this database back up, see Hostname or IP address changes for Voice Portal servers on page 115.
14. Reconnect each MPP server with the VPMS server as described in Reconnecting an existing MPP server with the VPMS server on page 103.
15. Relink the VPMS server with the MPP server as described in Reestablishing the link between the VPMS and an MPP on page 105.
16. Reconnect the auxiliary VPMS server with the primary VPMS server as described in Relinking the primary and auxiliary VPMS servers on page 100.
17. If you are restoring your Voice 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 Voice Portal on multiple servers* or the *Implementing Voice Portal on single server* guide.
18. If you want to unmount the shared directory, enter the `bash UmntDrive` command.

Purging report data from a local Voice Portal database

The `PurgeReportDataLocalDB` script purges all report data from the `VoicePortal` database. This data includes all:

- Application Detail Records (ADRs) stored in the `vpapplog` table
- Call 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 VPMS until the VPMS has downloaded the current report data from the MPP servers.

1. Make sure that the VPMS is not currently downloading report data from the MPP servers.
   a. Log in to the VPMS web interface using an account with the Administration user role.
   b. From the MPP Service Menu, select **System Properties** > **Report Data**.
   c. Go to the display text box in the **Download Schedules** group and make sure that no downloads are scheduled for the current time.
2. Log in to Linux on the Voice Portal primary VPMS server.
   If you are an Avaya Services representative, and are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:
   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
3. Navigate to the `Support/VP-Tools` directory by entering the `cd $AVAYA_HOME/Support/VP-Tools` command.
   $AVAYA_HOME is the environment variable pointing to the name of the installation directory specified during the Voice Portal software installation. The default value is `/opt/Avaya/VoicePortal`.

   Tip:
   This script is also available in the `Support/VP-Tools` directory of the Voice Portal installation DVD.
4. Enter the `bash PurgeReportDataLocalDB` command.
   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.

External database configuration

Shared external database configuration for multiple Voice Portal systems

If you have multiple Voice Portal systems, you may want to set up a shared external database so that you can log into the VPMS 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 a Voice 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:

- Call 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 Voice Portal Database Backup utility to back up an external database.

External database requirements

The external database can be a new or existing database created in:

- Postgres 8.2.3
- Oracle 9.0 or higher
- Microsoft SQL Server 2008 SP1

If you use an existing database, Voice Portal appends its required tables to that database without altering any of the existing data.

The Voice 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 2005 and 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.

Creating the required tables in the external database

In order to create the tables that Voice Portal requires in the shared database, you need to run the scripts provided on the Voice Portal Installation DVD against an Oracle, Postgres, or Microsoft SQL Server database.

Prerequisites

Make sure the external database you want to use was created in Oracle 9.0+ or Postgres 8.2.3+ or Microsoft SQL Server 2008SP1+.

Note:
Voice Portal adds tables to the database without changing any existing data. Therefore Voice 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 Voice Portal server.

1. Insert the Voice 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/`.
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 Voice Portal must be assigned CREATE TABLE and CREATE SESSION privileges for the database.

For Microsoft SQL Server, the database user name for Voice Portal must be assigned SELECT, INSERT, UPDATE and DELETE privileges on all tables in the database.

Next steps

Connect your Voice Portal systems to the external database as described in Connecting a Voice Portal system to a shared external database on page 140

Connecting a Voice Portal system to a shared external database

Prerequisites

Make sure you have created the required tables in the external database as described in Creating the required tables in the external database on page 139.

Once you connect a Voice Portal system to an external database, the system copies all report data currently on all MPPs in that system into the external database. Users can then generate reports that include that data, but they cannot include any data that resides in the local Voice 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.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VPMS Servers** and click the **VPMS Settings** button.
3. On the VPMS Settings page, go to the **Report Database** group.
4. Select the **Remote** radio button.
5. Enter the path to the external database in the **URL** field.

   A common URL format for Oracle connections is: `jdbc:oracle:thin:@`*`OracleServerName`*`:1521:`*`DBName`*

   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`

6. Enter the name of the Java class that implements the JDBC API to the external database in the **JDBC Driver** field.

   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`.

7. Enter the user name and password for the external database in the **User Name** and **Password** fields.
8. Click **Apply** at the bottom of the page.

Result

If Voice Portal:

- Can connect to the new database, the system scheduler begins saving all report data currently on all MPPs in that system into the external database.
- Cannot connect to the database, it displays an error message on the page. Voice Portal cannot write to the external database until you fix the error.

Disconnecting a Voice Portal system from a shared external database

When you disconnect a Voice Portal system from a shared external database, the system scheduler begins saving all report data currently on all MPPs in that system into the local Voice 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, but 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.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VPMS Servers** and click the **VPMS Settings** button.

3. On the VPMS Settings page, go to the **Report Database** group.
4. Select the **Local** radio button.
5. Click **Apply** at the bottom of the page.

Result

Voice Portal records all data in the local Voice Portal database from this point forward.

It does not, however, 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 Voice Portal report data from an external database

The `PurgeReportDataExtDB` script purges the report data from the external database for any inactive Voice Portal system. This data includes all:

- Application Detail Records (ADRs) stored in the `vpapplog` table
- Call 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 MPP server associated with the Voice Portal system

1. Make sure that the Voice Portal system whose data you want to purge is inactive. To do so:
   a. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
   b. From the VPMS 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 a Voice Portal system from a shared external database on page 141
2. Log in to Linux on the Voice Portal primary VPMS server.
   If you are an Avaya Services representative, and are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:
   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

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

3. Navigate to the `Support/VP-Tools` directory by entering the `cd $AVAYA_HOME/Support/VP-Tools` command.

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

   Tip:

   This script is also available in the `Support/VP-Tools` directory of the Voice Portal installation DVD.

4. Enter the `bash PurgeReportDataExtDB` *`Ext_DB_URL JDBC_Driver Ext_DB_Username Ext_DB_Password VP_System_Name`* command, where:

   - *`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.
   - *`Ext_DB_Password`* is the password for the external database.
   - *`VP_System_Name`* is the name of an **Inactive** Voice Portal system.

   Note:

   The values specified for these parameters should match the values specified on the VPMS Settings page in the VPMS.

   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.

VPMS Servers page field descriptions

Use this page to configure the VPMS servers on this Voice Portal system.

Column	Description
Selection check box	Indicates which auxiliary VPMS servers you want to delete.

Column	Description
	Note: You cannot delete the primary VPMS server.
Name	The name of the VPMS server.
Type	The options are: • **Primary**: This is the primary VPMS server for this system. • **Auxiliary**: This is the backup VPMS server for this system.
Host Address	The hostname or IP address of the VPMS server.
Add	Opens the Add VPMS Server page so that you can specify the location of the auxiliary VPMS server, if one is configured for your system. **Note:** You can add one or more auxiliary VPMS servers to a Voice Portal system.
Delete	Deletes the selected auxiliary VPMS servers.
VPMS Settings	Opens the VPMS Settings page.
Email Servers	Opens the Email Servers page.
Report DB Settings	Opens the Report Database Settings page.
Syslog Settings	Opens the Syslog Settings page.

VPMS Settings page field descriptions

Use this page to set the options that affect both the primary VPMS server as well as the optional auxiliary VPMS server.

This page contains the:

- General section on page 145
- Resource Alerting Thresholds (%) group on page 145
- Web Service Authentication group on page 145

General section

Field	Description
Voice Portal Name	The name of this Voice Portal system. Voice Portal displays this name on the Summary tab of the System Monitor page.
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 Voice 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 VPMS 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 Voice Portal database is restored and the application server can write its logs to that database.
Commands to Retain in MPP Configuration History	The number of MPP configuration changes that Voice Portal should save in the database. This value determines the number of entries on the <MPP Name> Configuration History page.

Resource Alerting Thresholds (%) group

Field	Description
Disk	The low water threshold determines when the VPMS generates an event, warning you, that disk usage is getting high. The high water threshold determines when the VPMS 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.

Note:

If the system is configured to use the local postgres database, the Call Data Handler (CDH) scheduler stops downloading report data from MPPs when the disk space on the VPMS 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 *:* character. • 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	
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.

Avaya Services information

Avaya Services MPPmap.data file

If this Voice Portal system is being maintained by Avaya Services, several of the Voice Portal servers have a Listed Directory Number (LDN) entry in the Avaya Services database.

You associate each server on the Voice Portal system with the corresponding LDN entry using the `$AVAYA_VPMS_HOME/bin/data/MPPmap.data` file.

The `MPPmap.data` file should contain an entry for:

- Each dedicated MPP server in a system where the VPMS and MPP software resides on different servers.
- Each Automatic Speech Recognition (ASR) server.
- Each Text-to-Speech (TTS) server.
- The auxiliary VPMS server, if one is configured for this system.

If you want to:

- Add, delete, or change the IP address of an MPP, ASR, TTS, or auxiliary VPMS server in the Voice Portal system, you must also update its entry in the Avaya Services map file through the VPMS.
- View the contents of the map file or change an LDN entry in that file, you need to use the `MPPmap.sh` script.

Maintaining the server IP addresses in the MPPmap.data file

1. Log in to the VPMS using the init VPMS account created during the VPMS software installation.
2. If you want to add a new server to both the Voice Portal system and the `MPPmap.data` file and the server is:
   - An ASR server, follow the steps in Adding ASR servers on page 327.
   - An MPP server, follow the steps in Adding an MPP on page 168.
   - An ASR server, follow the steps in Adding TTS servers on page 341.
   - The auxiliary VPMS server, follow the steps in #unique_91.
3. If you want to add or change the IP address or LDN entry for an existing Voice Portal server in the `MPPmap.data` file and the server is:
   - An ASR server, follow the steps in Changing ASR servers on page 328.
   - An MPP server, follow the steps in Changing an MPP on page 169.
   - An ASR server, follow the steps in Changing TTS servers on page 342.
   - The primary or auxiliary VPMS server, follow the steps in Changing the configuration information for a VPMS server on page 99.

Using the MPPmap.sh script

You can use the `MPPmap.sh` script to view the current entries in the `MPPmap.data` file. You cannot change the IP address or LDN values for an existing server or add a new server to this file using the script. You must make those changes using the VPMS.

1. On the primary VPMS server, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
2. Navigate to the `bin` directory under the VPMS installation directory by entering the `cd $AVAYA_VPMS_HOME/bin` command.

   $AVAYA_VPMS_HOME is the environment variable pointing to the name of the installation directory specified during the VPMS software installation. If Linux does not recognize this environment variable, see *Reloading the Voice Portal environment variables* topic in the *Implementing Voice Portal on multiple servers* guide or *Implementing Voice Portal on a single server* guide.
3. If you want to view the contents of the current map file, enter the `bash MPPmap.sh -l` command.
4. If you want to view the online help for this script, enter the `bash MPPmap.sh -h` command.

Logging in to an MPP manually through the MPP map file

If you cannot start a secure shell (SSH) session on an MPP in the MPP map file using the connect2 tool, you can log into the MPP manually using the MPP map file.

Note:
This procedure is primarily used by the Avaya services representative.

1. On the primary VPMS server, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
2. Navigate to the `bin` directory under the VPMS installation directory by entering the `cd $AVAYA_VPMS_HOME/bin` command.

   $AVAYA_VPMS_HOME is the environment variable pointing to the name of the installation directory specified during the VPMS software installation. If Linux does not recognize this environment variable, see *Reloading the Voice Portal*

environment variables topic in the *Implementing Voice Portal on multiple servers* guide or *Implementing Voice Portal on a single server* guide.

3. Run the connection script by entering the `bash MPPssh.sh LDN_entry Username` command, where:
   - *LDN_entry* is the value stored in the Avaya Services database, including all formatting characters and quotation marks.

     Note:

     The LDN entry value must be in the format of a 10 digit telephone number including the formatting characters `(`, `)`, and `-`. This number must be enclosed in double quotes or a `\` (backslash) must precede the open and close parentheses.

     For example, to use the MPPssh.sh script that logs on to the LDN entry (000)555-1212 using the Linux username *"myusername"*, you can enter any of the following:

     ```
     -bash MPPssh.sh "(000)555-1212" myusername
     -bash MPPssh.sh \(000\)555-1212 myusername
     ```

   - *Username* is the initial user name to use when logging into the target system.

Viewing the AF ID for the Voice Portal system

The Avaya Service Account authentication file for each Voice Portal system is assigned a unique ID. After you install the file, you can view the ID using a script installed with Voice Portal.

Prerequisites

Install the Avaya Service Account authentication file as described in the *Configuring the Avaya Service accounts* topic in the *Implementing Voice Portal on multiple servers* guide or *Implementing Voice Portal on a single server* guide.

1. Log in to Linux on the Voice Portal server.

   If you are an Avaya Services representative, and are using Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:
   - Log in to the local Linux console as sroot.
   - Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

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

2. Enter the `afview` command.

Chapter 5: SNMP agents and traps

SNMP Agents and Traps

The Voice Portal Simple Network Management Protocol (SNMP) network includes agents, traps, and managers.

SNMP agents

You can configure Voice Portal to act as an *SNMP agent* so that a third party network management software can retrieve the Voice 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 Voice 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 some type of graphical user interface (GUI).

For Avaya Voice 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 Voice Portal SNMP agent and SNMP trap destinations if you are an administrator.

Configuring Voice Portal as an SNMP agent

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Properties** > **SNMP**.
3. On the On the SNMP page, click **SNMP Agent Settings**.
4. On the SNMP Agent Settings page, enter the appropriate information and click **Save**.
5. If you changed the port number, restart the SNMP Agent.

Viewing existing SNMP traps

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **System Properties** > **SNMP**.
   The VPMS displays the SNMP page. From this page, authorized users can add, change, or delete SNMP trap destinations.

Adding an SNMP trap

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Properties** > **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

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Properties** > **SNMP**.
3. On the SNMP page, click the SNMP manager IP address or hostname in the **IP Address/Hostname** column.
4. On the Change SNMP Trap Configuration page, enter the appropriate information and click **Save**.

Disabling SNMP traps

If you want a particular SNMP trap to stop sending SNMP notifications but you want to save the configuration information for future reference, you can disable the trap instead of deleting it.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Properties** > **SNMP**.
3. On the SNMP page, click the SNMP manager IP address or hostname in the **IP Address/Hostname** column.
4. On the Change SNMP Trap Configuration page, select **No** in the **Enabled** field.
5. Click **Save**.

Testing SNMP traps

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Properties** > **SNMP**.
3. On the SNMP page, click **Test**.
   Voice Portal sends a test message to each SNMP trap configured on the system.

Next steps

When you test your SNMP traps, Voice 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

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Properties** > **SNMP**.
3. On the SNMP page, click the Selection check box to the left of the destination name in the table for each SNMP trap destination that you want to delete.

   Tip:
   To delete all SNMP trap destinations, click the selection check box in the header row of the table. This automatically selects all rows in the SNMP traps table.
4. Click **Delete**.

Configuring IBM Tivoli or HP OpenView with Voice Portal

For details about configuring Voice Portal with IBM's *Tivoli* or HP's *OpenView*, see the configuration files on the Voice 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 Voice 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
Selection check box	Indicates which SNMP traps you want to delete.
IP Address/Hostname	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. Voice Portal opens the Change SNMP Trap Configuration page.
Enable	Whether this SNMP trap is active.
Device	The options are: • **SSG/SAL**: Voice Portal sends SNMP traps to an Avaya Services Security Gateway (SSG)/Secure Access Link (SAL). **Note:** Voice Portal sends only Initialization and Administration System (INADS) traps to the SSG. • **NMS**: Voice Portal sends SNMP traps to a customer-provided Network Management System (NMS). **Note:** The Voice 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 Voice Portal system uses to send SNMP traps.
Type	The options are: • **Trap**: Voice Portal sends notifications with the SNMP `trap` command. • **Inform**: Voice 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.

Column or Button	Description
Security Name	The character string the Voice 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.
Add	Opens the Add SNMP Trap Configuration page.
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 that lets you change how device notifications are sent.

SNMP Agent Settings page field descriptions

Use this page to view or configure the SNMP agent settings for this Voice Portal system.

This page contains the:

SNMP Version 1 group

Field	Description
Enable SNMP Version 1	To configure the Voice 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 Voice 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 Voice 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 Voice 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 Voice Portal SNMP agent to receive and respond to SNMP Version 3 messages, select this check box.

Field	Description
Security Name	If you enabled version 3 messages, enter an alphanumeric name for the Voice 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".
Authentication Password	Enter a character string to be used as the authentication password for SNMP Version 3 messages. This password must either be blank or contain at least 8 alphanumeric characters. If you leave it blank, then you must also leave the **Privacy Password** field blank as well.
Privacy Password	Enter a character string to be used as the privacy password for SNMP Version 3 messages. This password must either be blank or contain at least 8 alphanumeric characters.

Authorized for SNMP Access group

Field	Description
Allow All IP Addresses	Allows any SNMP manager access to the Voice Portal SNMP agent. This is the default.
Allow Only the Following	Allows up to five specified SNMP managers access to the Voice 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 Voice Portal SNMP agent communicates with SNMP managers using the default port number for UDP, which is 161.
Custom Port Number	Specifies that the Voice 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.
Device	The options are: • **SSG/SAL**: Voice Portal sends SNMP traps to an Avaya Services Security Gateway (SSG)/Secure Access Link (SAL). **Note:** Voice Portal sends only Initialization and Administration System (INADS) traps to the SSG. • **NMS**: Voice Portal sends SNMP traps to a customer-provided Network Management System (NMS). **Note:** The Voice 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**.
IP Address/ Hostname	The IP address or fully qualified domain name of the SNMP manager that receives the SNMP traps.
Port	The port number the Voice Portal system uses to send SNMP traps. The default is 162.
Notification Type	The options are: • **Trap**: Voice 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**: Voice 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.

Column	Description
	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**.
Security Name	The character string the Voice 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 alphanumeric 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.

Column	Description
	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 alphanumeric 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**: Voice Portal sends SNMP traps to an Avaya Services Security Gateway (SSG)/Secure Access Link (SAL). **Note:** Voice Portal sends only Initialization and Administration System (INADS) traps to the SSG. • **NMS**: Voice Portal sends SNMP traps to a customer-provided Network Management System (NMS). **Note:** The Voice 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**.
IP Address/ Hostname	The IP address or fully qualified domain name of the SNMP manager that receives the SNMP traps.
Port	The port number the Voice Portal system uses to send SNMP traps.

Column	Description
	The default is 162.
Notification Type	The options are: • **Trap**: Voice 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**: Voice 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**.
Security Name	The character string the Voice 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 alphanumeric 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.

Column	Description
	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 alphanumeric characters.

Chapter 6: Media Processing Platforms

Media Processing Platform server overview

A Media Processing Platform (MPP) server is a server machine running the Voice Portal MPP software.

The MPP software:

- Runs on Avaya Enterprise Linux or Red Hat Enterprise Linux 5.4.
- 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:
Voice 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 Voice Portal Management System (VPMS) web interface allows administrators to control any MPP server in the system.

Data storage

The Voice Portal system is designed so that all persistent data is stored on the primary VPMS server. For example, all configuration information is stored on the primary VPMS server and downloaded to the MPP when required.

Any persistent data created on the MPP server is uploaded to the VPMS either on-demand or through scheduled jobs. For example:

- The VPMS regularly polls the MPP server's status.
- Event and alarm data is delivered to the VPMS on demand.
- Report data, including Call Detail Records (CDRs) and Session Detail Records (SDRs), are delivered to the VPMS 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

Setting the global grace period and trace level parameters

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **MPP Servers**.
3. On the MPP Servers page, click **MPP Settings**.
4. On the MPP Settings page, go to the **Miscellaneous** group.
   a. In the **Operational Grace Period** field, enter the number of minutes Voice Portal waits for calls to complete before it terminates any remaining active calls and begins stopping, rebooting, or halting an MPP.

      Enter a whole number of minutes between 0 and 999 in this field.

Important:

Ensure that the grace period is long enough for the MPP to complete any existing calls before it stops, reboots, or halts.

b. In the **Event Level Threshold to Send to VPMS** drop-down list, select the lowest level of events to be included in the performance tracing log that is sent to the VPMS.

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.

5. If the **Categories and Trace Levels** section is collapsed, click the section header to view the complete table of options and select the performance trace level you want to use as the default for each component. You can select **Off**, **Fine**, **Finer**, or **Finest**.

Important:

Performance tracing is a valuable troubleshooting tool, but it can adversely impact Voice Portal system performance if you set all categories to **Finest** on a busy production system. If you need to troubleshoot a particular area, Avaya recommends that you 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

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. To view the:
   - Current status of all MPP servers and get detailed information about any alarms they have generated, select **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.
   - MPP configuration, select **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, Voice 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

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **Real-Time Monitoring** > **System Monitor** and go to the appropriate <System name> Details tab.
3. In the **Server Name** column, click the name of the MPP whose details you want to view.
4. On the <MPP name> Details page, if you want to view the configuration history of the MPP, click the **History** link next the **Configuration** group at the top of the second column.

   Note:
   If you are logged in with the Administration user role, you can access the MPP Service Menu for the MPP by clicking the **Service Menu** link in the **Miscellaneous** group at the bottom of the second column.

Adding an MPP

1. Log in to the VPMS web interface.

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

   Otherwise, log in to the VPMS using an account with the Administration user role.
2. From the VPMS main menu, select **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, make sure you enter the appropriate LDN number for the server in the **LDN** field. If you do not specify an LDN number, Voice Portal uses the default value (000)000-0000.

   Note:
   Make sure you verify the security certificate displayed in the click the **MPP Certificate** section and then check the **Trust new certificate** check box. You cannot save the MPP unless this check box has been selected.

Changing an MPP

You can change all MPP options except the name of the MPP.

1. Log in to the VPMS web interface.

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

   Otherwise, log in to the VPMS using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **MPP Servers**.
3. On the MPP Servers page, click the name of the MPP you want to reconfigure in the **Name** column.
4. On the Change MPP Server page, enter the appropriate information and click **Save**.

   If you logged in using the init account, make sure 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 Voice 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 Voice 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. To avoid dropped calls, 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 Voice 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 Voice 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, Voice 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 Voice 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, Voice 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.

If desired, you can add up to 30 MPP servers to a single Voice Portal system, and that system can handle up to 5,000 telephony ports. You can also link several Voice Portal systems together through an external database. When the systems are combined, they can handle a maximum of 10,000 telephony ports.

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 VPMS, 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 VPMS.
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 has no 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 VPMS.

Related topics:

[Changing the operational mode of an MPP](#) on page 171

Changing the operational mode of an MPP

1. Log in to the VPMS web interface using an account with the Administration or Operations user role.
2. From the VPMS main menu, select **System Management** > **MPP Manager**.
3. On the MPP Manager page, use the Selection check box in the MPP server table to select which MPP you want to change.
4. Click the desired operational state button in the **Mode Commands** group. You can select:
   - **Offline** if the MPP server is currently in Online or Test mode.
   - **Test** if the MPP server is currently in Offline mode.

• **Online** if the MPP server is currently in Offline mode.

5. When you have finished setting the operational mode, click **Refresh** to ensure the mode is now what you expect.

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. To check them, see the *Viewing telephony port distribution* topic in the *Administering Voice Portal* guide. • 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, Voice Portal automatically restarts the MPP in an attempt to fix the problem. If the problem persists after the restart, Voice 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.
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. Voice 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.

State	Description
	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. Voice 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 VPMS 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. Voice Portal will restart the MPP automatically if the MPP: • Stopped unexpectedly and the **Auto Restart** option is selected for that MPP. In this case, Voice Portal restarts the MPP immediately. • Has a specified restart schedule. In this case, Voice 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. Voice Portal stops the corresponding server machine after all calls in progress are completed or the grace period ends, whichever comes first.

Related topics:

Checking the operational state for one or more MPPs on page 174
Changing the operational state for one or more MPPs on page 175

Checking the operational state for one or more MPPs

1. Log in to the VPMS web interface using an account with the Administration or Operations user role.
2. From the VPMS main menu, select **System Management** > **MPP Manager**.
3. On the MPP Manager page, look at the **State** column for the MPPs whose state you want to check.

   The options are:

   - **Booting**: The MPP is in the process of restarting and is not yet ready to take new calls.
   - **Degraded**: The MPP is running but it is not functioning at full capacity.
   - **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.
   - **Halting**:The MPP is responding to heartbeats but is not taking new calls.
   - **Never Used**:The MPP has never successfully responded to a heartbeat request.
   - **Not Responding**:The MPP is not responding to heartbeat requests and it has not received a **`Restart`** or **`Halt`** command.
   - **Rebooting**:The MPP is responding to heartbeats but is not taking new calls.
   - **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 VPMS 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.

- **Stopping**:The MPP is responding to heartbeats but is not taking new calls.

Changing the operational state for one or more MPPs

1. Log in to the VPMS web interface using an account with the Administration or Operations user role.
2. From the VPMS main menu, select **System Management** > **MPP Manager**.
3. On the MPP Manager page, use the Selection check box in the MPP server table to select which MPP servers you want to change.
4. If you selected multiple servers and you plan to either restart or reboot them, in the **Restart/Reboot Options** group, select either **One server at a time** or **All selected servers at the same time**.
5. Click the desired operational state button in the **State Commands** group and confirm your selection when prompted. You can select:
   - **Start**
   - **Stop**
   - **Restart**
   - **Reboot**
   - **Halt**
   - **Cancel**
6. When you have finished setting the operational state, click **Refresh** to ensure that the state is now what you expect.

Tip:

You can also verify the state change by selecting **Real-Time Monitoring** > **System Monitor** from the VPMS main menu and going to the <System name> Details tab. The information on this page refreshes automatically if you leave the browser window open.

Software Upgrade

Software Upgrade overview

The Software Upgrade page in Voice Portal allows you to upgrade the software version of the MPPs running on your Voice 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 VP, make sure you:

- Execute the **`/opt/Avaya/InstallAgent/bin/DownloadPK.bash`** *<VPMS_Hostname, or VPMS IP address>* command on the MPPs to authorize the software upgrades through VPMS. For more information see the *Authorizing the VPMS to upgrade the MPP* section in the *Implementing Voice Portal on multiple servers* guide.
- Set 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 Voice Portal system.

This page contains the:

- Software Upgrade server table on page 176
- Upgrade Commands group on page 179

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.

Field	Version Description
	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 available in the `$AVAYA_IA_HOME/download` directory. • An MPP is already being upgraded. • The MPP version is not Voice Portal 5.0 or higher. • The MPP is on the same server as the primary VPMS. If you select all MPPs, the upgrade process skips MPPs which meet any of the conditions mentioned above.
Server Name	The name of the MPP.
Mode	The MPP operational mode. 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 VPMS 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.
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

Field	Version Description
	• **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.
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 typically displayed when the VPMS server reboots while the MPP is being upgraded. The upgrade of this MPP continues while the VPMS 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.

Field	Version Description
	• **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.

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 are available for selection which have the .iso image set in the directory `$AVAYA_IA_HOME/download (default = /opt/Avaya/InstallAgent/download)`. • Ensure that each .iso has a corresponding .sig in the `$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

Prerequisites

Execute the **`/opt/Avaya/InstallAgent/bin/DownloadPK.bash`** <*VPMS_Hostname, or VPMS IP address*> command on the MPPs to authorize the software upgrades through VPMS.

For more information, see the *Authorizing the VPMS to upgrade the MPP* section in the *Implementing Voice Portal on multiple servers* guide.

1. Log in to the VPMS web interface.

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

   Otherwise, log in to the VPMS using an account with the Administration user role.
2. From the VPMS main menu, select **System Management** > **Software Upgrade**.
3. Click the Selection check box in the first column header of the MPP server table to select all MPP servers.

   Note:

   The upgrade process skips an MPP if:

   - The user does not have the permission to upgrade an MPP.
   - There is no .iso image available in the `$AVAYA_IA_HOME/download` directory.
   - An MPP is already being upgraded.
   - The MPP version is not Voice Portal 5.0 or higher.
   - The MPP is on the same server as the primary VPMS.
4. Select the required upgrade version in the **New Version** field.

   Note:

   Only those versions are available for selection which have the .iso image set in the directory $AVAYA_IA_HOME/download (default = /opt/Avaya/InstallAgent/download).
5. Click **Upgrade** in the **State Commands** group and confirm your selection when prompted.

   Voice Portal upgrades the MPP servers. 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 current one completes.

6. After a few minutes, click **Refresh** and verify that, for all MPP servers, the:
   - **Mode** is **Online**.
   - **State** is **Running**.
   - **Config** is **OK**.
7. Check that the version numbers are correctly allocated to the MPP servers by verifying the **Current Version** column.

Upgrading an MPP server

1. Log in to the VPMS web interface.

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

   Otherwise, log in to the VPMS using an account with the Administration user role.
2. From the VPMS main menu, select **System Management** > **Software Upgrade**.
3. Click the Selection check box next to 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 available in the `$AVAYA_IA_HOME/download` directory.
   - An MPP is already being upgraded.
   - The MPP version is not Voice Portal 5.0 or higher.
   - The MPP is on the same server as the primary VPMS.
4. Select the required upgrade version in the **New Version** field.

   Note:

   Only those versions are available for selection which have the .iso image set in the directory $AVAYA_IA_HOME/download (default = /opt/Avaya/InstallAgent/download).

5. Click **Upgrade** in the **State Commands** group and confirm your selection when prompted.
   Voice 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

1. From the VPMS main menu, select **System Management** > **MPP Manager**.
2. On the MPP Manager page, make sure that the **Mode** column says **Online** for all servers. If any are shown as **Offline**:
   a. Click the Selection check box next to each 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 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.
   Voice Portal starts the MPP servers. This process can take several minutes depending on how many servers there are in your system.
5. After a few minutes, click **Refresh** and verify that, for all MPP servers, the:
   - **Mode** is **Online**.
   - **State** is **Running**.

- **Config** is **OK**.

6. If desired, make sure that all licensed telephony ports were correctly allocated to the MPP servers:
   a. From the VPMS main menu, select **Real-Time Monitoring** > **Port Distribution**.
   b. On the Port Distribution page, examine the **Mode** and **State** columns.

Starting an MPP server

1. From the VPMS main menu, select **System Management** > **MPP Manager**.
2. On the MPP Manager page, make sure that the **Mode** column says **Online** for the server you want to start. If the mode is **Offline**:
   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 that the:
   - **Mode** is **Online**.
   - **State** is **Running**.
   - **Config** is **OK**.
6. If desired, make sure that all licensed telephony ports were correctly allocated to the MPP server:
   a. From the VPMS main menu, select **Real-Time Monitoring** > **Port Distribution**.
   b. On the Port Distribution page, examine the **Mode** and **State** columns.

Restarting one or more MPP servers

1. Log in to the VPMS web interface using an account with the Administration or Operations user role.
2. From the VPMS 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 MPP servers you want to restart.

   Tip:

   To restart all MPP servers, click the Selection check box in the header row of the MPP server table.
4. If you selected multiple servers, in the **Restart/Reboot Options** group, select either **One server at a time** or **All selected servers at the same time**.
5. Click **Restart** in the **State Commands** group.
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

1. Log in to the VPMS web interface using an account with the Administration or Operations user role.
2. From the VPMS main menu, select **System Management** > **MPP Manager**.
3. On the MPP Manager page, if you want to:
   - Change the action Voice Portal takes if an MPP stops unexpectedly, click the pencil icon in the **Auto Restart** column and enter the appropriate information in the Auto Restart <MPP Name> page.
   - Schedule a one time restart during the current day, click the pencil icon under **Restart Today** in the**Restart Schedule** column and enter the appropriate information in the Restart <MPP Name> Today page.

- Specify that the MPP should be automatically restarted on a regular basis, click the pencil icon under **Recurring** in the **Restart Schedule** column and enter the appropriate information in the Restart Schedule for <MPP Name> page.

4. When you have specified the required information, click **Save** to return to the MPP Manager page.

Viewing MPP configuration history

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **Real-Time Monitoring** > **System Monitor**.
3. On the <System name> Details tab of the System Monitor page, 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.
5. On the <MPP Name> Configuration History page, if you want to view or save an XML document detailing a specific configuration change, click the link in the **Configuration** column for that change and follow the prompts.

   Note:
   The number of configuration changes displayed depends on the setting for the **Commands to Retain in MPP Configuration History** field on the VPMS Settings page.

6. If you want to view or save an XML document showing the complete current configuration for the MPP, click **Export** in the top right corner of the page and follow the prompts.

Configuring Voice Portal to use the Test operational mode

You can test any MPP in the Voice 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.

Prerequisites

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 50.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS 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 Voice Portal on page 230, 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 Voice Portal on page 231, making sure that you specify the maintenance stations in the **Application Launch** group on the Change Application page.

Related topics:

Using the Test operational mode on page 186

Using the Test operational mode

The Test operational mode allows you to send a test call to one or more MPPs in the Voice Portal system.

Prerequisites

Configure one or more H.323 connections to use the Test operational mode as described in Configuring Voice Portal to use the Test operational mode on page 186.

---

1. Log in to the VPMS web interface using an account with the Administration or Operations user role.
2. From the VPMS 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 **Online**.
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.

   Voice 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, Voice Portal assigns one Test mode port to each MPP.
   - Greater than the number of defined maintenance stations, Voice 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 39.
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 Voice 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 VPMS and an MPP

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **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. At the bottom of the page, click **Save**.
6. From the VPMS main menu, select **System Management** > **MPP Manager**.
7. On the MPP Manager page, look at the **Mode** column for this server. If it says **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 moments, click **Refresh** to verify that the **Mode** column now says **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. If desired, make sure that telephony ports were correctly allocated to the MPP server:
    a. From the VPMS main menu, select **Real-Time Monitoring** > **Port Distribution**.
    b. On the Port Distribution page, examine the **Current Allocation** column to find the ports allocated to this MPP.
    c. Look at the **Mode** and **State** columns to make sure the assigned ports are ready to receive calls.

Deleting MPP servers

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **MPP Servers**.
3. On the MPP Servers page, for each MPP that you want to delete, click the Selection check box to the left of the MPP name in the MPP server table.

   Tip:
   To delete all MPPs, click the Selection check box in the header row of the MPP server table.
4. Click **Delete**.
   Voice 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 has been removed.

MPP Service Menu

The MPP 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 VPMS as a user with the Administration user role to access the MPP 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.
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 Voice 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.

Name	Description
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 VPMS user accounts that have the Administration user role and are therefore authorized to access the MPP Service Menu.

Related topics:

Logging in to the MPP Service Menu on page 191
Using the MPP Service Menu with a proxy server on page 192

Logging in to the MPP Service Menu

If you are logged in to the VPMS with the Administration user role, you can also log in to the MPP Service Menu for a specific MPP.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **Real-Time Monitoring** > **System Monitor**.
3. Go to the <System name> Details tab on the System Monitor page, where <System Name> matches the name of the Voice Portal system that contains the MPP whose MPP 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, click **Service Menu** in the **Miscellaneous** group at the bottom of the second column.
   If the VPMS does not automatically open the MPP Service Menu, there may be a problem with the proxy server settings. For details, see Using the MPP Service Menu with a proxy server on page 192.

Using the MPP Service Menu with a proxy server

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 MPP Service Menu from the appropriate <MPP name> Details page.

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 MPP 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 VPMS main menu, select **System Configuration** > **MPP Servers**.
5. When you are done, click **OK** three times to close the Proxy Settings dialog, the LAN Settings dialog, and the Internet Options dialog.

Next steps

Log into the MPP Service Menu as described in Logging in to the MPP Service Menu on page 191.

Moving the MPP logs to a different location

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.

1. If necessary, install the target drive or create the target partition as described in your operating system documentation.

   Important:

   Do *not* create the new directory on this drive or partition, as the script will fail if 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 Voice Portal log directory, you can improve security by setting its properties in the `/etc/fstab` file to `rw,nosuid,noexec,auto,nouser,async,noatime,nodev`. For more information about these options, see http://www.faqs.org/docs/securing/chap5sec45.html.

3. Log in to the VPMS web interface using an account with the Administration or Operations user role.
4. Stop the MPP whose logs you want to move:
   a. From the VPMS main menu, select **System Configuration** > **MPP Servers**.
   b. On the MPP Servers page, click the Selection check box next to the name of the MPP you want to stop.
   c. Click **Stop** in the **State Commands** group
   d. Confirm the action when requested.
   e. Wait until the operational state becomes Stopped. To check this, click **Refresh** and look at the **State** field.

      Note:

      The operational state changes when the last active call completes or the grace period expires, whichever comes first.

5. Log in to Linux on the Voice Portal MPP server.

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

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

   Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` 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 VPMS main menu, select **System Configuration** > **MPP Servers**.
   b. On the MPP Servers page, click the Selection check box next to the name of the MPP you want to start.
   c. Click **Start** 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 Voice Portal system.

Add MPP Server page (page 1 of 2)

Field	Description
Name	The unique identifier for the MPP server on the Voice Portal system. This name is used only in the VPMS 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 VPMS 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 Voice 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 Voice Portal for verification. Voice 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, Voice Portal prompts you to correct the **Host Address** field entry and try again. When the SSL certificate downloads successfully, Voice Portal displays the second Add MPP Server page.

Add MPP Server page (page 2 of 2)

This page contains the:

General section

Field	Description
Name	The name you entered on the first Add MPP page. **Note:** This field cannot be changed.
Host Address	The network address, or location, of the computer on which the MPP server resides. The VPMS 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 Voice 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, Voice 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. 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.

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 Voice 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 MPP server capacity on page 169.
Restart Automatically	The options are: • **Yes**: If the MPP stops unexpectedly, Voice 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 **`Stop`** or **`Halt`** command. For details about issuing a **`Stop`** or **`Halt`** command, see Changing the operational state for one or more MPPs on page 175
Listed Directory Number (LDN)	This field is only shown when you are logged into the VPMS using the Avaya Services init account created when the Avaya Service accounts were configured. If you are logged into the VPMS 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, Voice 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 Voice Portal system performance if you set all categories to **Finest** on a busy production system. If you need to troubleshoot a particular area, Avaya recommends that you 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 VPMS. 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**.

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 VPMS 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**.
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 VPMS. 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**.
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

Field or Radio Button	Description
	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**.
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**.

Auto Restart <MPP Name> page field descriptions

Field	Description
Auto Restart	Determines whether Voice Portal automatically restarts an MPP if it stops unexpectedly. If this check box is: • Selected, Voice 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 **`Stop`** or **`Halt`** command. For details about issuing a **`Stop`** or **`Halt`** command, see Changing the operational state for one or more MPPs on page 175

Change MPP Server page field descriptions

Use this page to change an existing Media Processing Platform (MPP).

This page contains the:

- General section on page 200
- MPP Certificate section on page 202
- Categories and Trace Levels section on page 202

General section

Field	Description
Name	The unique identifier for the MPP server on the Voice 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 VPMS 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 Voice Portal system and the machine must already have the MPP software installed on it.

Field	Description
	You cannot use any of the following hostnames: `127.0.0.1`, `localhost`, or `localhost.local.domain`.
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.
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 Voice 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 MPP server capacity on page 169.
Restart Automatically	The options are: • **Yes**: If the MPP stops unexpectedly, Voice 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 **`Stop`** or **`Halt`** command. For details about issuing a **`Stop`** or **`Halt`** command, see Changing the operational state for one or more MPPs on page 175
Listed Directory Number (LDN)	This field is only shown when you are logged into the VPMS using: • The Avaya Services init account created when the Avaya Service accounts were configured.

Field	Description
	In this case, you can enter a value in this field. • Any other VPMS 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 VPMS 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, Voice 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 Voice Portal system performance if you set all categories to **Finest** on a busy production system. If you need to troubleshoot a particular area, Avaya recommends that you 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.

Field or Radio Button	Description
	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 VPMS. 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**.
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 VPMS and commands from SessionManager **Note:** SMIL parsing is done in SessionManager and low level video commands are sent to this component.

Field or Radio Button	Description
	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**.
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 VPMS. 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**.
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.

Field or Radio Button	Description
	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**.
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> Configuration History page field descriptions

Use this page to view information about the history of configuration changes for *<MPP Name>*.

Column	Description
Time	The date and time the MPP configuration change occurred.
Command	A summary of the MPP configuration change.

Column	Description
Configuration	Click the link to open or save an XML file with detailed information about MPP configuration changes.

<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 <VPMS Name>/<MPP Name> Details page if the VPMS and MPP server are installed on the same machine.

This page contains the:

General Information group

Field	Description
Server Name	The unique name for this MPP.
Unique ID	The ID number used for this MPP in the database. Voice Portal selects this number from the range given in the **MPP Numeric ID Range** field on the MPP Settings page.
Host Address	The hostname or IP address of the MPP.
Version	The version number of the MPP software.
Last Successful Poll	The last date and time that the VPMS polled the MPP successfully.

Operational Information group

Field	Description
Restart Today	The options are: • **Yes at *time***: Voice Portal will stop and restart the MPP at the time shown • **No**: There is no restart scheduled for today
Restart Schedule	The options are: • **None:** There is no restart schedule for this MPP • The restart schedule

Operational State group

Field or Button	Description
Current State	The operational state of the MPP. The options are: • **Booting**: The MPP is in the process of restarting and is not yet ready to take new calls. • **Degraded**: The MPP is running but it is not functioning at full capacity. • **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. • **Halting**:The MPP is responding to heartbeats but is not taking new calls. • **Never Used**:The MPP has never successfully responded to a heartbeat request. • **Not Responding**:The MPP is not responding to heartbeat requests and it has not received a **`Restart`** or **`Halt`** command. • **Rebooting**:The MPP is responding to heartbeats but is not taking new calls. • **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 VPMS 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.

Field or Button	Description
	• **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. • **Stopping**:The MPP is responding to heartbeats but is not taking new calls.
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 MPP is available to handle normal call traffic. • **Offline**: The MPP is unavailable to handle any calls and is not being polled by the VPMS 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.
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 MPP 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 Voice Portal system.

This page contains the:

- MPP server table on page 210
- State Commands group on page 211
- Restart/Reboot Options group on page 213
- Mode Commands group on page 213

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.
Server Name	The name of the MPP.
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 VPMS 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 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

Field	Description
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
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 166.

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 Voice Portal system experiences a brief disruption in service while it reallocates the licensed ports. Avaya recommends that you only 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. Voice Portal will only restart the MPP if: • You issue an explicit **`Start`** command • The MPP has a specified restart schedule

Button	Description
	Note: For more information, see Setting the global grace period and trace level parameters on page 166.
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 VPMS 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 VPMS web interface. **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 VPMS 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, Voice Portal automatically starts the MPP. • You can manually restart the MPP using the **Start** button on this page.

Button	Description
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, Voice 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 selected servers at the same time**.

Mode 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
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 186.
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 Voice Portal system.

Tip:

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

Field	Description
Selection check box	Indicates which MPP servers you want to delete.

Field	Description
Name	The unique identifier for the MPP server on the Voice Portal system.
Host Address	The network address, or location, of the computer on which the MPP server resides. The VPMS uses this address to communicate with the MPP server.
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 Voice 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.
Event Handlers	Opens the Event Handlers page so you can change the global event handlers and prompts for all MPP servers.

Field	Description
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 Voice Portal system.

This page contains the:

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 50. • **Low Water**: Enter a whole number from 0 to 100. The default is 40.
Disk	The low water threshold determines when the MPP generates an event warning you that disk usage is getting high. The high water threshold

Field	Description
	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 ($AVAYA_MPP_HOME/logs/process/MediaMgr/EndPointMgr): 2x • Media Manager ($AVAYA_MPP_HOME/logs/process/MediaMgr/MediaManager): 2x • Session Manager ($AVAYA_MPP_HOME/logs/process/SessMgr/*): 2x
Number of Logs to Retain	The maximum number of log files the system can retain, including the current one. Once this number of log files exists, the system deletes the oldest log file before starting a new one. Enter a whole number from 1 to 5. The default is 2. **Note:** Due to the volume of trace messages from the following components, the number of log files retained by the system are set higher than the number you specify in this field. The actual size is as follows: • Endpoint Manager ($AVAYA_MPP_HOME/logs/process/MediaMgr/EndPointMgr): 2x • 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.
Maximum Transcriptions per Day	The maximum number of transcriptions that the MPP should record in any given day. The default is 6000.

Record Handling on MPP group

Field	Description
Session Data	Whether an MPP keeps detailed records about the sessions that it handles. Voice 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 0 to 999. The default is 14.
Call Data Record	Whether an MPP keeps detailed records about the calls that it handles. Voice Portal uses this data to create the Call Detail report andCall 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 0 to 999. The default is 14.
Application	Whether an MPP keeps the CCXML and VoiceXML Log tag data from the application sessions transacted on that server. If desired, Voice 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 0 to 999. The default is 14.

Miscellaneous group

Field	Description
License Re-allocation Wait Time	The number of minutes the system waits before reallocating the licenses from an MPP that is out of service to other MPPs in the system. Enter a whole number from 0 to 1440. The default is 10.

Field	Description
Operational Grace Period	The number of minutes Voice Portal waits for calls to complete before it terminates any remaining active calls and begins stopping, rebooting, or halting an MPP. Enter a whole number of minutes between 0 and 999 in this field. **Important:** Ensure that the grace period is long enough for the MPP to complete any existing calls before it stops, reboots, or halts.
Event Level Threshold to Send to VPMS	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 VPMS. 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.
MPP Numeric ID Range	Voice Portal assigns a numeric ID for each MPP in the Voice Portal system from the number range given in this field. This numeric ID identifies the MPP in the Voice Portal database and becomes part of the Universal Call Identifier (UCID) associated with every call processed on that MPP. **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 are creating Universal Call Identifier (UCID) values that conflict with the default Voice Portal values. If you do change the value, make sure that you specify a large enough range to cover all MPP servers in your Voice Portal system.

Categories and Trace Levels section

Performance tracing is a valuable troubleshooting tool, but it can adversely impact Voice Portal system performance if you set all categories to **Finest** on a busy production system. If you need to troubleshoot a particular area, Avaya recommends that you 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 VPMS. 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**.
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 VPMS 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.

Field or Radio Button	Description
	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**.
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 VPMS. 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**.
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**.

Field or Radio Button	Description
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**.
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 VPMS restarts the MPP and clears this check box. The VPMS 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 Voice Portal to periodically stop and then restart the MPP.

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`.
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, Voice 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, Voice 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 Voice 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 VPMS and each MPP in the Voice Portal system named in <*System Name*>. The information on this page refreshes automatically if you leave the browser window open.

Note:

If the VPMS server needs to be restarted, Voice Portal displays the message "VPMS needs to be restarted." in red text just above the system status table.

Column	Description
Server Name	The options are: • The name of the VPMS server. Click this name to view the <VPMS Name> Details page. • The name of an MPP running on the system. Click this name to view the <MPP name> Details page. • *<VPMS Name>/<MPP Name>*, if an MPP resides on the same server as the VPMS. Click this name to view the <MPP name> Details page.
Type	The options are: • **VPMS**: The Voice Portal Management System • **MPP**: A Media Processing Platform • **VP**: This is the overall Voice Portal system summary
Mode	The operational mode of the MPP. 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 VPMS 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. The options are: • **Booting**: The MPP is in the process of restarting and is not yet ready to take new calls. • **Degraded**: The MPP is running but it is not functioning at full capacity. • **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. • **Halting**:The MPP is responding to heartbeats but is not taking new calls. • **Never Used**:The MPP has never successfully responded to a heartbeat request. • **Not Responding**:The MPP is not responding to heartbeat requests and it has not received a **`Restart`** or **`Halt`** command.

Column	Description
	• **Rebooting**:The MPP is responding to heartbeats but is not taking new calls. • **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 VPMS 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. • **Stopping**:The MPP is responding to heartbeats but is not taking new calls.  **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 configuration state of the MPP. 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.

Column	Description
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.
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.
Calls Today	The number of calls handled during the current day.
Alarms	The alarm status indicators for the VPMS, each MPP, and the overall Voice 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 tab on the System Monitor page field descriptions

Use this tab for a consolidated view of the health and status of the Voice Portal system. The information on this page refreshes automatically if you leave the browser window open.

Note:

If the VPMS server needs to be restarted, Voice Portal displays the message "VPMS needs to be restarted." in red text just above the system status table.

Column	Description
System Name	The name of the Voice Portal system, as specified in the **Voice Portal Name** field on the VPMS Settings page. If your installation consists of multiple Voice 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 **VP**. • The name of the another Voice Portal system in the shared external database. The **Type** will always be **Remote VP**. Click the system name to log into the VPMS web interface for the remote system. • **Summary**. The call capacity and active call counts across all Voice Portal systems displayed on this page.
Type	If your installation consists of a single Voice Portal system, the type will always be **VP**. If you hover the mouse over this field, the VPMS displays a tooltip showing whether the associated server is a primary or auxiliary VPMS server. If your installation consists of multiple Voice Portal systems that share a common external database, this column contains: • **VP**: This type indicates that you are currently logged into the VPMS for this system. Any system commands you issue will affect this VPMS and any MPP servers assigned to this system. The <System name> Details tab for this system shows the assigned MPP servers. • **Remote VP**: This type indicates that this is an active Voice Portal system, but it is *not* the system you are currently logged into. To affect the VPMS or MPP servers assigned to a remote system, you must first log into that system by clicking the remote system name in the **System Name** column
State	Displays the operational state of the Voice Portal system. The options are: • **Active**: This Voice Portal system is updating its information in the database on a regular basis. • **Inactive**: A remote Voice Portal system of **TypeRemote VP** is no longer updating information in the shared database. Click the system name to log into the VPMS on that system and troubleshoot the problem locally. • **Stale**: It has been over an hour since this Voice 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 Voice Portal systems is too great. For more information, see the *Time Synchronization between external database and VPMS servers* topic in the *Troubleshooting Voice Portal* guide.

Column	Description
	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 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. 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	This field displays: • **In**: The number of active incoming calls in the system • **Out**: The number of active outgoing calls in the system
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 **VP**, 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 VP**, you must first log into the remote system by clicking the name in the **System Name** column.

Chapter 7: Speech applications in Voice Portal

Speech applications in Voice Portal

Speech applications are the “directors” of Voice 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.

Voice 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.

Viewing speech applications added to the Voice Portal system

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **System Configuration** > **Applications**.

The VPMS displays the Applications page, which lists all of the speech applications added to Voice Portal. The options displayed on this page depend on your user role.

Adding a speech application to Voice Portal

Prerequisites

Make sure that the:

- Required speech servers have been added to the Voice Portal system. For more information, see Speech servers in Voice Portal on page 323.
- Speech application has been deployed to the application server. For more information, see the *Deploying a speech application* topic in the *Planning for Voice Portal* guide.

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

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, Voice Portal uses the first application listed on the Applications page to handle an incoming call from that URI. If you want Voice 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	sip:+1-212-555-xxxx

Application name	Specified Called URI value
1212_specific	sip:+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 Voice Portal will always run `all_555` and never run `1212_specific`.

Related topics:

Changing speech application priority on page 231

Changing speech application priority

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **Applications**.
3. On the Applications page, click the **Change Launch Order** link above the right-most column of the table.
4. In the Application Launch Order window, click the name of the application whose priority you want to change, then click:
   - The up arrow to the right of the list box to move the application up in priority.
   - The down arrow to the right of the list box to move the application down in priority.
5. Click **Save**.

Changing speech application settings through Voice Portal

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **Applications**.

3. On the Applications page, click the application name in the **Name** column.
4. On the Change Application page, enter the appropriate information and click **Save**.

Specifying the default application for inbound calls

You can specify a default application for Voice Portal to use when the system receives a call from a telephone number that is not associated with any other application.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **Applications**.
3. On the Applications page, if you want 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.
   - Designate an existing application as the default, click the application name in the **Name** column. The VPMS displays the Change Application page.
4. On the Add Application or Change Application page, go to the **Application Launch** group.
5. Select the **Inbound Default** radio button in the **Type** field.
6. Click **Save** at the bottom of the page.

Accessing VoiceXML and CCXML Log tag data through Voice Portal

If you include VoiceXML or CCXML Log tags in an application and you want to view that information in the Voice Portal application reports, you need to make sure that the data is being collected on the MPP and downloaded to the Voice Portal database.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. To specify that the MPP servers should collect and store Log tag data:
   a. From the VPMS main menu, select **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 **Application** option in the **Record Handling on MPP** group.
   d. Click **Apply**.
3. To download the Log tag data to the Voice Portal database:
   a. From the VPMS main menu, select **System Properties** > **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 Voice Portal database:
   a. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
   b. From the VPMS 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

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **Reports** > **Session Detail**.
3. On the Session Detail page, the **more >>** link to display the rest of the optional filters.
4. Enter any 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. When you are finished, click **OK**.
   The VPMS displays the Session Detail Report page.
6. Locate the particular session for which you want to view the transcription data and click the **View Session Details** icon at the end of the appropriate row.
   Voice Portal displays the Session Details page, which shows the both session and transcription data grouped by information category.
7. If you want to view the transcription information in XML format, click the **Export** link in the **Session Transcription** group.

Deleting speech applications from Voice Portal

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **Applications**.
3. On the Applications page, for each application that you want to delete, select the check box to the left of the application name in the applications table.

Tip:

To delete all applications, click the Selection check box in the header row of the table, which automatically selects all rows in the applications table.

4. Click **Delete**.
5. If desired, remove the application from the Application server as well.

SIP application support

User-to-User Interface (UUI) data passed in SIP headers

When you add an application to Voice Portal using the VPMS 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: Voice 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: Voice 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"`

Related topics:

[Universal Call Identifier (UCID) values included in UUI data](#) on page 236
[Voice Portal application parameters affecting the UUI data](#) on page 237

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 Voice Portal MPP server or it can be passed to Voice 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, Voice 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 Voice Portal.

A UCID consists of 20 decimal digits in three groups. Before the UCID is added to the UUI data, Voice 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 Voice 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.

Voice Portal application parameters affecting the UUI data

When you add an application to Voice Portal using the VPMS 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 Voice 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 Voice Portal treats the UUI data.

Parameter	Description
	The options are: • **Service Provider**: Voice 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**: Voice 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 235.
Transport UCID in Shared Mode	If **Operation Mode** is set to **Shared UUI** and **Generate UCID** is set to **Yes**, this field determines whether Voice Portal encodes a Voice 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 Voice 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 Voice 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 Voice Portal by the application, Voice 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. Voice 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.
<sip>.from.displayname <sip>.from.uri <sip>.tag	From	The initiator of the request.
<sip>.historyinfo[array].displayname	History-Info	This field is typically used to inform proxies and User Agent Clients and Servers involved in

Session Variable	SIP Header	Notes
<sip>.historyinfo[array].user <sip>.historyinfo[array].host <sip>.historyinfo[array].optheader		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 Voice 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.
<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.

Session Variable	SIP Header	Notes
<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 Voice 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 Voice 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 Voice Portal receives an INVITE with the following unknown headers:

```
new_header: "helloworld"
another_new_header: "howareyou"
```

Voice 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>.passerted.displayname <sip_prop>.passerted.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 VPMS, Voice 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

To create a custom header, store a name and value pair in the`session.connection.protocol.sip.unknownhdr` session variable array.

Example

To create a custom with a value of `new_header: "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].name =
"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, Voice 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:

Voice Portal supports SIP UPDATE method only if the Allow header indicates support.

Related topics:

Sample SIP UPDATE Method on page 245

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
```

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.

Voice 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.

If you want to use call classification in your applications, make sure you design the application so that it takes such mistakes into account.

Call classification analysis results

When Voice 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
`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.

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.
`recorded_msg`	Outbound calls only	An answering machine was detected and a recorded message has just started. This classification will always be followed by either a `msg_end` or `timeout` classification.
`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.
`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.

Value of `event$.info.callprogress`	Applies to	Description
		For example, for outbound calls the color ring tone will be 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.

When you add an application to Voice Portal using the VPMS 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

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 the *Call classification with the LaunchVXML method* topic in the *Administering Voice Portal* guide.

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 analysis results on page 246.

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>
```

Voice 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. Awell-designed speech application includes exception handlers that deal with these messages and help the application recover so that it can continue processing the call.

Voice 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, Voice Portal uses one of the event handlers installed on the MPP server.

The event handler Voice Portal uses depends on the state of the speech application. If an application:

- Was successfully started and there is a call in progress, Voice Portal uses the event handler associated with that application when it was added to the Voice Portal system.
- Could not be started, Voice 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, Voice 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 Voice Portal reacts to a problem, you can add your own event handlers and prompts and then designate which ones Voice Portal should use as the default.

For example, you may 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 Voice 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.

Related topics:

Adding application event handlers and prompts on page 250
Setting the default application event handlers on page 252

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.

Prerequisites

Make sure you test all event handlers thoroughly before you add them to the system.

Important:

Voice 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 Voice Portal tries to use the event handler to process a call.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **MPP Servers** and click **Event Handlers**.
3. To add a VoiceXML event handler:
   a. Go to the VXML 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, Voice 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. 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, Voice 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. 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, Voice 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

You can define a default CCXML and VoiceXML event handler, along with a default event handler prompt, for Voice Portal to use if an application encounters a problem and no specific event handler has been associated with that application.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **MPP 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.

Setting Avaya Voice Browser options

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **MPP Servers**.

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

AVB-specific VoiceXML events

The Avaya Voice Browser may issue any of the following Voice 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.

AVB event name	Description
`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.

Using a secure connection between the MPP and the application server

You can require that the MPP running a particular application uses a secure connection to the application server.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **Applications**.
3. For each application that you want to use a secure connection, verify that the URL in the **URL** column starts with `https`.

   If it does not, click the application name to open the Change Application page and specify a URL that begins with `https`.
4. From the VPMS main menu, select **Security** > **Certificates** and go to the Application Certificates tab.
5. Verify that a security certificate exists for each application server that Voice Portal can trust.

   Important:

   If Voice 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. If necessary, click **Add** to install a security certificate using the Add Application Certificate page.

7. From the VPMS main menu, select **System Configuration** > **MPP Servers** and click **AVB Settings**.
8. On the AVB Settings page, make sure that **SSL Verify** is set to **Yes**.

Add Application page field descriptions

Use this page to add a new speech application to the system.

This page contains the:

General settings section

Field	Description
Organization	The name of the organization associated with the application you want to add. **Note:** This field is displayed only if organization level access is enabled in the Voice 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 Voice Portal on page 89.
Name	The name used to identify this application on the Voice Portal system. **Note:** • If you select an organization in the field above, the selected organization and forward slash character are automatically prefixed to the application name. If you do not select the organization name, this indicates that the application does not belong to any organization. For more information on organization level applications see Organization level access in Voice Portal on page 89. • Once you save the application, this name cannot be changed. If you are using a Nuance server, this name must be between 1 and 30 characters.

Field	Description
Enable	Whether this application is available for use by the Voice Portal system. The default is **Yes**, which means the application is available.
Type	The type of Multipurpose Internet Mail Extensions (MIME) encoding used by this application. The options are: • **VoiceXML**: If selected, Voice Portal displays the **VoiceXML URL** field. • **CCXML**: If selected, Voice Portal displays the **CCXML URL** field. • **CCXML/VoiceXML**: If selected, Voice Portal displays both the **VoiceXML URL** and the **CCXML URL** fields. **Note:** Additional type options may be available if you have installed managed application on Voice Portal. For more information on managed application type, see the documentation delivered with the managed application.

URL group

Field	Description
Type	The options are: • **Single**: The only application server that handles the calls. • **Fail Over**: Allows you to add two URLs to handle a fail over: - URL 1: The primary application that handles the calls - URL 2: The application that handles the calls upon the failure of the primary application. • **Load Balance**: Allows you to add two URLs for load balancing purpose. The URLs are also used for failover. For instance, if URL 2 fails, URL1 handles all calls.
CCXML URL	The HTTP path to the root document of the Call Control eXtensible Markup Language (CCXML) speech application.

Field	Description
	The URL must be in the format `[http:|https:]//domain.name/subdirectory/startDocument` where • `[http:|https:]` indicates whether the URI uses normal or secure HTTP protocol. **Note:** You must specify a URL that begins with `https:` if you want Voice Portal to use a secure connection between the MPP and the application server. • *`domain.name`* is the fully qualified domain name or the IP address of the server on which the application resides. You can use a relative path for your domain name, but Avaya recommends that you use the fully qualified domain name. • *`subdirectory`* is an optional subdirectory or series of subdirectories on the application server. • *`startDocument`* is the first page that the CCXML-compliant speech application should load. The extension on this document will typically be `ccxml`, `htm`, `html`, `jsp`, or `xml`. For example, `vpmenu.html` or `vpmenu.jsp?gtype=vxml-srgs-avaya-ibm`. **Note:** Voice Portal uses the Oktopous™ ccXML Interpreter.
VoiceXML URL	The HTTP path to the root document of the VoiceXML speech application. The URL must be in the format `[http:|https:]//domain.name/subdirectory/startDocument` where • `[http:|https:]` indicates whether the URI uses normal or secure HTTP protocol. **Note:** You must specify a URL that begins with `https:` if you want Voice Portal to use

Field	Description
	a secure connection between the MPP and the application server. • *domain.name* is the fully qualified domain name or the IP address of the server on which the application resides. You can use a relative path for your domain name, but Avaya recommends that you use the fully qualified domain name. • *subdirectory* is an optional subdirectory or series of subdirectories on the application server. • *startDocument* is the first page that the VoiceXML-compliant speech application should load. The extension on this document will typically be `htm`, `html`, `jsp`, `vxml`, or `xml`. For example, `vpmenu.html` or `vpmenu.jsp?gtype=vxml-srgs-avaya-ibm`.
Verify	Instructs Voice Portal to open the associated root document in a new browser window. If the document cannot be found, the new browser window displays a `file not found` error. **Note:** **Verify** is not displayed if the URL(s) contains a secure HTTP protocol (https:), and the **Mutual Certificate Authentication** field is set to **Yes**.
Mutual Certificate Authentication	Enables mutual certificate authentication between the MPP and the application. **Important:** Do not enable this option if your application uses external grammars stored on the application server. The speech servers do not support mutual certificate authentication and therefore will not fetch the grammar from the application server. If you select this option ensure that: • The application server is configured to support mutual configuration and the MPP

Field	Description
	certificate is installed on the application server. • The application certificate is installed on the MPP. Voice Portal allows you to add and view the application certificate from the **Security>Certificates>Trusted Certificates** page in VPMS. • The URLs use secure HTTP protocol (https).
Basic Authentication	Enables user name and password authentication between the MPP and the application. Ensure that the application server is configured to support basic configuration. **Important:** Do not enable this option if your application uses external grammars stored on the application server and uses a Nuance speech server, as Nuance does not support basic authentication. If you select the **Basic Authentication** option, Voice Portal displays: • **User name** field: The name used to authenticate the MPP and the application. **Note:** The user name must not contain the *:* character. • **Password** field: The password used to authenticate the MPP and the application. **Note:** You can select both **Mutual Certificate Authentication** and **Basic Authentication** options.

Speech Servers group

Field	Description
ASR	If this application uses Automatic Speech Recognition (ASR) resources, this field lets you select the ASR engine type that will be used.

Field	Description
	The options are: • **No ASR**: This application does not use ASR resources. • The engine type associated with the ASR server to use for this application. The available engine types depend on the ASR servers on the Voice Portal system. If you select an engine type, Voice Portal displays the **Languages** field.
Languages	If an ASR engine is selected, this field displays the languages configured for the ASR servers of that engine type on the Voice Portal system. Select one or more languages for this application. Your selections must match exactly the ASR language defined in the speech application. Use `Ctrl+Click` and `Shift+Click` to make more than one selection from this list. The first selected language becomes the default for this 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 are configured for any single ASR server, Voice Portal sends a `No ASR Resource` exception to the application. What happens then depends on the event handler that the application uses.
TTS	If this application uses Text-to-Speech (TTS) resources, this field lets you select the TTS engine type that will be used. The options are: • **No TTS**: This application does not use TTS resources • The engine type associated with the TTS server to use for this application. The available options depend on the TTS servers on the Voice Portal system. If you select an engine type, Voice Portal displays the **Voices** field.
Voices	If a TTS engine is selected, this field displays the voices configured for the TTS servers of that engine type on the Voice Portal system. Select one or more default voices for this application. Your selections must match exactly the TTS voice defined in the speech application. Use `Ctrl+Click` and `Shift+Click` to make more than one selection from this list. The first selected voice becomes the default for this 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, Voice Portal sends a `No TTS Resource` exception to the application. What happens then depends on the event handler that the application uses.

Application Launch group

Note:

Voice Portal uses the information you enter in this group to make a master list of all telephone numbers and Universal Resource Indicators (URIs) that are mapped to specific applications. It then takes the number or URI dialed by the caller as input and determines which speech application is assigned to handle that number.

If you do not map any phone numbers or URIs to an application, then that application automatically handles any calls that come from numbers or URIs that are not otherwise mapped. However, you can only have one such application on the system. If you attempt to configure a second application without a DNIS or URI, the system generates an error.

Field or Button	Description
Type	The options are: • **Inbound**: This application handles inbound calls from a URI or one or more specified telephone numbers. • **Inbound Default**: This application handles all inbound calls made to a number that is not associated with any other application. • **Outbound**: This application handles outbound calls.
Number type radio buttons	The options are: • **Number**: Instructs Voice Portal to associate the application with a single telephone number. • **Number Range**: Instructs Voice Portal to associate the application with a sequential range of telephone numbers. • **URI**: Instructs Voice Portal to associate the application with a single URI.
Called Number	The definition of this field depends on the selected number type. If the number type is: • **Number**: This field is the telephone number you want to associate with this application. • **Number Range**: This field is the lowest telephone number in the range you want to associate with this application. • **URI**: This field is not available. You can enter from 1 to 15 digits. Do not include spaces or special characters such as (,), or -.
To	If you selected the number type **Number Range**, this field is the highest telephone number in the range you want to associate with the application. If you selected any other number type, this field is not available.
Called URI	If you selected the number type **URI**, this is the URI you want to associate with the application.

Field or Button	Description
	You can use any valid regular expression wildcards such as: • `?` to represent a single character • `*` to represent multiple characters If you selected any other number type, this field is not available.
Add	Associates the number, range of numbers, or URI with the application. After you click **Add**, the specified number, range of numbers, or URI appears in the display text box.
Display text box	Displays all the DNIS numbers and URIs that are mapped to this speech application. 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 association between the selected entries in the display text box and the application.

Speech Parameters group

When determining what value to use for each of the following settings, Voice Portal looks at the following sources:

- The speech application itself. If the parameter is defined in the application, Voice Portal uses that value.
- The values entered on this page. If the parameter is not defined in the application but is defined on this page, Voice Portal uses the value defined here.
- The values entered on the AVB Settings page.
- The default values defined for the Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) server by the server manufacturer. To determine the default settings for your ASR server, consult your server documentation.

Note:

If these fields are not displayed, click the group heading to expand the group.

Field	Description
ASR section	
Confidence Threshold	The confidence level below which the ASR engine will reject the input from the caller. Enter a number from `0.0` to `1.0`. 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`.

Field	Description
	Note: If you are using Dialog Designer, see the **Confidence** field description in your Dialog Designer documentation.
Sensitivity Level	How loud an utterance must be for the ASR engine to start speech recognition. Enter a number from `0.0` to `1.0`. 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. **Note:** If you are using Dialog Designer, refer to the *Nodes and Palette Options* chapter in the *DD Developer's Guide* for more information on the **Sensitivity** field description.
Speed vs. Accuracy	The balance between speed of recognition and accuracy of recognition. Enter a number from 0.0 to 1.0. 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. This value is mapped to whatever scale the ASR engine uses to compute the balance between speed and accuracy of recognition. **Note:** If you are using Dialog Designer, see the **Speed vs. Accuracy** field description in your Dialog Designer documentation.
N Best List Length	The maximum number of recognition results that the ASR engine can return. • For Nuance and IBM WVS, enter a number from 1 to 100. • For Loquendo, enter a number from 1 to 10. **Note:** If you are using Dialog Designer, see the **N-Best** input form field description in your Dialog Designer documentation.

Field	Description
No Input Timeout	The number of milliseconds the system waits for a caller to respond after the prompt is finished playing and before the system throws a No Input event. For Nuance, Loquendo and IBM WVS, enter an integer value in the range 0 to 65535. **Note:** If you are using Dialog Designer, see the **Timeout** field on the Prompt main tab in your Dialog Designer documentation.
Recognition Timeout	The number of milliseconds the system allows the caller to continue speaking before the system ends the recognition attempt and throws a `maxspeechtimeout` event. For Nuance, Loquendo and IBM WVS, enter an integer value in the range 0 to 65535. **Note:** This field corresponds to the **Maximum Speech** field in your VoiceXML application. For more information, see your Dialog Designer documentation.
Speech Complete Timeout	The number of milliseconds of silence required following user speech before the speech recognizer either accepts it and returns a result or reject it and returns a No Match event. Enter an integer in this field. • For Nuance and IBM WVS, enter a value in the range 0 to 65535. • For Loquendo, enter a value in the range 300 to 10000. This value is used when the recognizer currently has a complete match of an active grammar, and specifies how long it should wait for more input declaring a match. By contrast, the incomplete timeout is used when the speech is an incomplete match to an active grammar. **Tip:** Take care when setting this property. If you set the number too high, it can slow down system response time, even for successful recognitions. If you set the number too low, it can lead to an utterance being cut off prematurely. Reasonable values for this property are usually in the range of 5000 to 15000 milliseconds.
Speech Incomplete Timeout	The number of milliseconds of silence following user speech after which a recognizer finalizes a result. Enter an integer in this field. • For Nuance and IBM WVS, enter a value in the range 0 to 65535. • For Loquendo, enter a value in the range 300 to 10000. The incomplete timeout applies when the speech prior to the silence is an incomplete match of all active grammars. In this case, once the timeout is triggered, the speech recognizer rejects the partial result and returns a No Match event.

Field	Description
	Tip: Take care when setting this property. If you set the number too high, it can slow down system response time, even for successful recognitions. If you set the number too low, it can lead to an utterance being cut off prematurely. This property is usually set lower than the **Speech Complete Timeout** but high enough to allow for callers to pause mid-utterance. **Note:** If you are using Dialog Designer, see the **Timeout Incomplete** field description in your Dialog Designer documentation.
Maximum Grammar Cache Age	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. When determining whether an utterance is stale or not, the application adds this time together with the value specified in the **Maximum Grammar Staleness** field and compares that to the age of the utterance plus the value in the **Minimum Grammar Freshness Time** field. The maximum grammar cache age plus the maximum grammar staleness time must be greater than or equal to the age of the utterance plus the minimum grammar freshness time. For example, if the: • Maximum grammar cache age is 60 • Maximum grammar staleness is 20 • Current utterance has been cached for 45 seconds. • Minimum grammar freshness time is 30 Then the application will accept the utterance from the MPP because the expression 60 + 20 > 45 + 30 evaluates as True. **Note:** For the purposes of this calculation, if the maximum grammar staleness field is blank, that is the same as setting it to infinity. In that case, the application will always accept the cached utterance from the MPP because the maximum grammar cache age plus infinity will always be greater than the utterance age plus the minimum grammar freshness time.
Minimum Grammar Freshness Time	The minimum length of time beyond an utterance's current age for which the utterance must remain fresh to be accepted by the application. Enter a whole number of seconds in this field. f The application adds this value to the current age of the utterance and compares the result to the value in the **Maximum Grammar Cache Age** field plus the value in the **Maximum Grammar Staleness** field, as described above.

Field	Description
Maximum Grammar Staleness	The maximum amount of time beyond the normal expiration time of an utterance that the application server will accept. Enter a whole number of seconds in this field, or leave it blank to instruct the application to always use a cached response of any age. The application adds this value to the value in the **Maximum Grammar Cache Age** field and compares it to the current age of the utterance plus the value in the **Minimum Grammar Freshness Time** field, as described in the **Maximum Grammar Cache Age** field.
Vendor Parameters	Any vendor-specific or platform-specific parameters that the ASR server requires to function correctly with this speech application. **Note:** Contact your speech server provider for details on vendor parameters. These parameters must be in the general form*parameter=value*. You can include as many parameters as you want. Use semi-colons (`;`) to separate multiple entries. For example, you might need to specify:`ep.ThresholdSnr=12;Rec.PPR=1`
TTS section	
Prosody Volume	The default value for the loudness of the synthesized speech output. Specify one of the following values from the drop-down list or enter a value in the text field. • `<NONE>` • `default` • `silent` • `x-soft` • `soft` • `medium` • `loud` • `x-loud` **Note:** The text field is enabled only when you select None in the drop-down list. The text field is not displayed if you select Loquendo in the **TTS** field. Enter a number from 0 to 100, where zero (0) represents no audible output and 100 represents full volume **Note:** Avaya recommends setting the **Prosody Volume** to 50 to ensure that:

Field	Description
	• The TTS resource is properly initialized for the request. • All prompts from different speech server with different default volume settings, that include prerecord prompts, are played at the same volume.
Prosody Rate	Voice Portal uses this value to fine tune the default TTS speaking rate relative to the server default. Specify one of the following values from the drop-down list or enter a value in the text field. • `<NONE>` • `default` • `x-slow` • `slow` • `medium` • `fast` • `x-fast` **Note:** The text field is enabled only when you select None in the drop-down list. The text field is not displayed if you select Loquendo in the **TTS** field. For IBM WVS servers, enter a number from 70 to 1297. **Note:** The prosody rate for IBM WVS is based on the speaking rate in words per minute (wpm). For Nuance and Loquendo servers, enter a number from 0 to 100.
Vendor Parameters	Any vendor-specific or platform-specific parameters that the TTS server requires to function correctly with this speech application. **Note:** Contact your speech server provider for details on vendor parameters. These parameters must be in the general form *`parameter=value`*. You can include as many parameters as you want. Use semi-colons (`;`) to separate multiple entries. For example, to specify that a Nuance RealSpeak server should use the custom dictionary called `mydictionary.dct` on a Linux RealSpeak server, you would enter:`ssftrs_dict_enable=file:///opt/ttsdict/mydictionary.dct`. For more information, see Adding custom dictionaries for Nuance RealSpeak on page 343.

Reporting Parameters group

Note:
If these fields are not displayed, click the group heading to expand the group.

Field	Description
Application Logging section	
Minimum Level	Determines what messages will be sent by this application through the Application Logging web service. You can view this information in the Application Summary or Application Detail report. The options are: • **None**: Voice Portal ignores all application messages. If this option is selected, this application will not appear in any application reports. • **Fatal**: Voice Portal saves fatal level messages. • **Error**: Voice Portal saves fatal and error level messages. • **Warning**: Voice Portal saves fatal, error, and warning level messages. • **Info**: Voice Portal saves all messages sent by this application.
Call Flow Data Sample Rate	The percentage of times that this application will generate breadcrumb data when it runs. For example, if this field is set to 25%, then the application will generate breadcrumbs once out of every four times it runs. You can use this field to cut down on application logging if your Voice Portal system is running under a heavy load.
Transcription section	
Transcription Enabled	The options are: • **Yes**: Voice Portal creates a transcription log for each call handled by the application. If you select this option, the rest of the fields in this group become available. • **No**: Voice Portal does not save any transcription or performance data.
Transcription Sample Rate	The percentage of times that this application will generate a transcription log when it runs. For example, if this field is set to 25%, then the application will generate a transcription log once out of every four times it runs. You can use this field to reduce application logging if your Voice Portal system is running under a heavy load. **Note:** The total number of transcriptions per day per MPP is set in the **Maximum Transcriptions per Day** on the MPP Settings page.
Performance Trace	The options are: • **Yes**: Voice Portal creates a performance trace log for each call handled by the application that has an associated transcription log.

Field	Description
	Note: This information can be viewed on the Session Details page, which is accessible from the Session Detail Report page. • **No**: Voice Portal does not save performance trace data.
DTMF Data	Determines the information Voice Portal saves in the application's transcription log when a Dual-tone multi-frequency (DTMF) event occurs. The options are: • **Discard**: Voice Portal saves only the DTMF event. • **Save**: Voice Portal saves the DTMF event and its associated data.
Prompt Data	Determines the information Voice Portal saves in the application's transcription log when a prompt event occurs. The options are: • **Discard**: Voice Portal saves only the prompt event. • **Save**: Voice Portal saves the prompt event and its associated data.
TTS Data	Determines the information Voice Portal saves in the application's transcription log when a Text-to-Speech (TTS) event occurs. The options are: • **Discard**: Voice Portal saves only the TTS event. • **Save**: Voice Portal saves the TTS event and the first few characters of the TTS data.
Speech Data	Determines the information Voice Portal saves in the application's transcription log when a speech event occurs. The options are: • **Discard**: Voice Portal saves only the speech event with no result. • **Text Only**: Voice Portal saves the speech event with the result in text format. • **Text and Speech**: Voice Portal saves the speech event along with a link to the URL that contains the associated WAV file. The system stores each recording as a separate audio file on the MPP. Therefore, if you select this option for a very active application, you could end up with a large number of WAV files in a single directory. This could lead to performance issues over time.

Advanced Parameters group

Note:
If these fields are not displayed, click the group heading to expand the group.

Field	Description
Support Remote DTMF Processing	Whether the ASR server or the MPP server performs Dual-tone multi-frequency (DTMF) processing. The options are: • **Yes**: The ASR server performs DTMF processing. • **No**: The MPP server performs DTMF processing.
DTMF Type Ahead Enabled	Whether the application supports DTMF type ahead. DTMF type ahead feature allows a user to provide DTMF input when the prompt is being presented and thereby skip the prompt. The options are: • **Yes**: The application supports DTMF type ahead. • **No**: The application does not support DTMF type ahead. **Note:** This field is enabled only when the **Support Remote DTMF Processing** field is set to **No**.
Converse-On	Whether the application is invoked by an Avaya Call Center system using the **converse-on** vector command. The **converse-on** vector command makes it possible for the Call Center vector program to call and access a speech application on the Voice Portal system. When it does so, the vector program on the Call Center server makes it possible to send data in the form of DTMF tones. This option tells Voice Portal to listen for these DTMF tones before starting the VoiceXML application. **Note:** At run time, the MPP writes the DTMF digit data to the session variable `session.telephone.converse_on_data`. VoiceXML applications can access this data from that variable. In the case of Dialog Designer applications, the system writes this data to the `vpconverseondata` field of the `session` variable. For more information, see the Dialog Designer documentation.
Network Media Service	Whether this application uses the “voice dialog” Network Media Service for passing the application starting URI as part of the SIP invitation. **Note:** For more information, see RFC 4240 at http://www.rfc-archive.org/getrfc.php?rfc=4240.
Dialog URL Pattern	A regular expression used to verify the starting URI form the SIP invitation. This is a security parameter used to verity the URI is “trusted.” If it is blank, then any URI will be accepted.
VoiceXML Event Handler	The VoiceXML event handler to use for this application.

Field	Description
	The options are: • **<Default>**: This application uses the default VoiceXML error handler defined for the Voice Portal system. • An error handler name: This application uses a specific error handler instead of the system default. This drop-down lists all VoiceXML error handlers that have been uploaded through the Add VoiceXML Event Handler page.
CCXML Event Handler	The CCXML event handler to use for this application. The options are: • **<Default>**: This application uses the default CCXML error handler defined for the Voice Portal system. • An error handler name: This application uses a specific error handler instead of the system default. This drop-down lists all CCXML error handlers that have been uploaded through the Add CCXML Event Handler page.
Generate UCID	The Universal Call Identifier (UCID) is an Avaya-proprietary call identifier used to help correlate call records between different systems. *Inbound Calls:* If the Avaya Communication Manager (CM) passes a UCID to Voice Portal, Voice Portal always uses that UCID regardless of the setting in this field. If, however, CM does not pass a UCID, the Voice Portal MPP server can generate one for the call. The options are: • **Yes**: If the CM does not pass a UCID to Voice Portal, the MPP server generates a UCID. • **No**: The MPP does not generate a UCID. *Transfers & Outbound Calls:* The options are: • **Yes**: For blind and supervised transfers using the `<redirect>` CCXML tag, the MPP uses the same UCID as the call being transferred. For Bridge and Outcalls , MPP will generate a new 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 Voice Portal treats the UUI data. The options are: • **Service Provider**: Voice Portal passes the UUI data as a single block to the application without making any attempt to interpret data.

Field	Description
	If you select this option, the application must handle the UUI data on its own. • **Shared UUI**: Voice 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 235.
Transport UCID in Shared Mode	If **Operation Mode** is set to **Shared UUI** and **Generate UCID** is set to **Yes**, this field determines whether Voice Portal encodes a Voice 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 Voice 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 Voice 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 Voice Portal by the application, Voice 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. Enter an integer between 0 and 2,048, where 0 indicates that Voice Portal should not check the length of the UUI data. The default is 128.
Fax Detection Enabled	Whether this application should detect whether the inbound number is a fax machine. 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.
Video Enabled	Whether to enables or disables the support for the video server. The options are: • **Yes**: Enables the video server for a particular application. • **No**: Disables the video server for a particular application.
Video Screen Format	Select the video screen format. The options are:

Field	Description
	• **CIF**: Common Intermediate Format. The screen resolution for CIF is 352x288 pixels. • **QCIF**: Quarter CIF. The screen resolution for QCIF is 176x144 pixels. • **SQCIF**: Sub-Quarter CIF. The screen resolution for SQCIF is 128x96 pixels.
Video Minimum Picture Interval	Video Minimum Picture Interval (MPI) is the time interval used to define the frame rate. MPI uses the CIF, QCIF, and SQCIF formats. Enter a value in the range 1 to 32. The default is 2. For CIF, QCIF and SQCIF, if the value is zero, the screen format is disabled otherwise the frame rate is defined by (29.97/MPI). For example: for value 1 = 30 FPS, for 2 = 15 FPS, and so on.

Application Detail (Filters) page field descriptions

Use this page to create an Application Detail report.

This page contains the:

Select a Source Report group

Note:

- This group is available only when you are generating a custom report.
- On selecting a source report, the filters on the Add Custom Report (Filters) page is refreshed to correspond to the selected source report.
- You cannot change the source report once you save a custom report.

Field	Description
Standard Reports	Select one of the available standard reports as a base for generating the custom report.
Custom Reports	Select one of the available custom reports as a base for generating the custom report.
Organization	Select an organization associated with the custom report you want to generate. If you do not select an organization, this indicates that the user does not belong to any organization.

Field	Description
	Note: This field is displayed only if organization level access is enabled in the Voice 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 Voice Portal* in the *User management* chapter in the *Administering Voice Portal* guide. 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.
Report Name	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.

Date and Time group

Button	Description
Predefined Values	The options are: • **All Dates and Times** • **Today** • **Yesterday** • **This Week** • **Last Week** • **This Month** • **Last Month**
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: • In the beginning of the **Start Date/Time** field, enter the start date using the format `dd-mmm-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

Button	Description
	format and the same timezone as the VPMS. For example, you could enter `03-Mar-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 `dd-mmm-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 VPMS. For example, you could enter `10-Mar-2007 16:26:10`. The default for this field is the day prior to the current date at time 23:59:59.

Note:

The amount of data available for this report depends on the setting for call data records records in the **Application Retention Period** field in the **Report Database Record Data** group 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 it is set to 7, you can only check for the previous week.

Optional Filters group

In any text field:

- All searches are case insensitive unless otherwise noted.
- You can replace one or more characters with a wildcard. To replace one character, use `_` (underscore). To replace any number of characters, use a `%` (percent sign).

  For example, `car_` matches “Cart” or “cars”, while `Car%` matches “Cart”, “cars”, “Cart Rentals”, “Car Rentals”, “CARPET”, and so on.
- To specify multiple keywords, any one of which will result in a match, use the `,` (comma) search operator to separate the keywords. For example, to find all calls that came from either 111-555-1212 or 222-555-1214, you would enter `tel:1115551212,tel:2225551214` in the **Originating #** field.
- To specify that a keyword should NOT appear in record, use the `~` (tilde) search operator in front of the keyword. For example, to find all calls that did NOT come from 111-555-1212, you would enter `~tel:1115551212` in the **Originating #** field.
- To specify that multiple keywords must all appear in a record for it to be a match, use the `+` (plus sign) search operator in front of the keyword.
- You can combine wildcards and search operators. For example, if you want to eliminate all calls that originated from numbers in the 408 and 303 area codes, you would enter `~tel:303%+~tel:408%` in the **Originating #** field.

Field or Link	Description
Reset	Restores the default filter settings and displayed column settings.

Field or Link	Description
	The default columns are: • **Start Time** • **Level** • **Application** • **Activity** • **Type** • **Message** **Note:** When you click this link, Voice Portal restores the defaults for all filters, even those that are not displayed if the section is collapsed.
Voice Portal	If your installation has multiple Voice Portal systems that use a shared database, this field lists all of the available systems. The options are: • **All systems** • A specific Voice Portal system. If you select this option, only the call sessions handled by the MPPs assigned to this system will be shown in the report.
Application	The application name. The options are: • **All applications**. This is the default. • A specific application name. **Note:** This filter only works for applications compiled with Dialog Designer 4.0 or later.
more >>	Displays the rest of the optional report filters. **Note:** The rest of the fields in this group do not display until you click this link.
Show Column	Each filter has an associated check box under this header. To show a particular piece of information in its own column in the report, select its associated **Show Column** check box. To hide that piece of information, clear the associated check box.
Level	The severity level of the application message. The options are: • **Fatal** • **Error**

Field or Link	Description
	• **Warning** • **Info** All the levels are selected by default.
Node ID	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`.
Session ID	The session ID assigned by the MPP. **Note:** This field is case-sensitive.
Session Label/UCID	The session label assigned to the application in Dialog Designer or the Universal Call Identifier (UCID) assigned when the application was added to Voice Portal through the VPMS.
Activity Name	The name of the activity associated with the application.
Activity Type	The options are: • **Start** • **In Progress** • **End** • **Cancel** • **VoiceXML Log Tag** • **CCXML Log Tag** • **Node Entry** • **Module Exit** • **Application Exit** • **All Types** All the activity types are selected by default.
Activity Duration	Each application message has a `Duration`, `ActivityName`, and `LogType` field. The `Duration` field contains the number of seconds that have elapsed since an application message with the same `ActivityName` and a `LogType` of `Start` was received.

Field or Link	Description
	Note: The duration is measured in full seconds. If the duration is less than one full second, it is represented as a 0 (zero) in this report. Select a duration from the drop-down list and then, if necessary, enter a time in seconds. The options are: • **All Durations** • **Less Than** `<specified number of seconds>` • **Equal To** `<specified number of seconds>` • **Greater Than** `<specified number of seconds>` For example, if you want to view all instances when the activity named `Call_Survey` lasted for more than five minutes, you would enter `Call_Survey` in the **Activity Name** field, select **Greater Than** from the **Activity Duration** drop-down list, then enter `300` in the **seconds** field. The default is **All Durations**.
Activity Message	All or part of the activity message that you want to use as a filter. You can specify an explicit string or use the % wildcard character. For example, to see all logged events whose entire activity message is “transaction completed”, enter `transaction completed` in this field.
Variable Name	The name of a variable defined in the application.
Variable Value	The value of the variable named in **Variable Name**.
Filters from Custom Report	Limits the sessions in this report to those found in the selected custom report. **Note:** Applies all filters specified in another custom report, except the **Date and Time** filter. This option helps you to use filters across different custom report types. For example, if you have a custom Application Detail report that shows when blue cars are rented, you can view a Call Summary report that contains only calls on which blue cars were rented. Select a custom report from the drop-down list which includes all available custom reports.
Sort By	Sorts the report by the selected column. Select the column by which you want to sort the report, from the list of sortable columns. Select the option to sort the report by **Ascending** or **Descending** order. **Note:** The default is **Date and Time** and **Descending**.

Field or Link	Description
<< less	Collapses the **Optional Filters** group.

Application Detail Report page field descriptions

Use this page to view, print, or export an Application report.

This page contains the:

Summary section

This section always includes the field **Total Records**, which displays the total number of records that match the specified filter criteria. In addition, this section includes a field for each filter you specified on the Application Detail page.

For example, if you selected anything other than **All Dates and Times** in the **Date and Time** group, the summary section includes an entry for **Time Period**.

Application detail table

This page contains a table with one or more of the following columns, depending on the **Show Column** selections you made on the Application Detail page.

Tip:

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

Column	Description
Start Time	The date and time that the application started.
Level	The severity level of the application message. The options are: • **Fatal** • **Error** • **Warning** • **Info**
Voice Portal	The name of the Voice Portal system to which the associated MPP server is assigned.
Application	The application name.

Column	Description
Node ID	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.
Session ID	The session ID assigned by the MPP.
Session Label/UCID	The session label assigned to the application in Dialog Designer or the Universal Call Identifier (UCID) assigned when the application was added to Voice Portal through the VPMS. If no session label or UCID was assigned, then this field displays a **-** (hyphen).
Activity	The name of the activity associated with the application.
Type	The type associated with the activity. The options are: • **Start** • **In Progress** • **End** • **Cancel** • **VoiceXML Log Tag** • **CCXML Log Tag** • **Node Entry** • **Module Exit** • **Application Exit** • **All Types** **Note:** If the width of the activity type exceeds the width of this column, then the activity type appears as **...**. Hover the mouse over the **...** to view a tool tip with the complete type name.
Duration	Each application message has a `Duration`, `ActivityName`, and `LogType` field. The `Duration` field contains the number of seconds that have elapsed since an application message with the same `ActivityName` and a `LogType` of `Start` was received.
Message	The message associated with the application. To view the details of the message, click the message text. The VPMS opens the Message Details page.
Variable Name	The name of a variable defined in the application.
Variable Value	The value of the variable named in **Variable Name**.

Column	Description
	To filter the report by a particular line item, click this icon at the end of the row. Voice Portal discards all other active filters and creates an Application report displaying all messages that match the corresponding application name and session ID.

Application Summary (Filters) page field descriptions

Use this page to create an Application Summary report.

This page contains the:

- Select a Source Report group on page 273
- Date and Time group on page 282
- Optional Filters group on page 283
- Report Type group on page 286

Select a Source Report group

Note:

- This group is available only when you are generating a custom report.
- On selecting a source report, the filters on the Add Custom Report (Filters) page is refreshed to correspond to the selected source report.
- You cannot change the source report once you save a custom report.

Field	Description
Standard Reports	Select one of the available standard reports as a base for generating the custom report.
Custom Reports	Select one of the available custom reports as a base for generating the custom report.
Organization	Select an organization associated with the custom report you want to generate. 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 Voice 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 Voice Portal* in the *User management* chapter in the *Administering Voice Portal* guide.

Field	Description
	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.
Report Name	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.

Date and Time group

Button	Description
Predefined Values	The options are: • **All Dates and Times** • **Today** • **Yesterday** • **This Week** • **Last Week** • **This Month** • **Last Month**
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: • In the beginning of the **Start Date/Time** field, enter the start date using the format `dd-mmm-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 VPMS. For example, you could enter `03-Mar-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 `dd-mmm-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

Button	Description
	format and the same timezone as the VPMS. For example, you could enter `10-Mar-2007 16:26:10`. The default for this field is the day prior to the current date at time 23:59:59.

Note:

The amount of data available for this report depends on the setting for call data records records in the **Application Retention Period** field in the **Report Database Record Data** group 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 it is set to 7, you can only check for the previous week.

Optional Filters group

In any text field:

- All searches are case insensitive unless otherwise noted.
- You can replace one or more characters with a wildcard. To replace one character, use `_` (underscore). To replace any number of characters, use a `%` (percent sign).

  For example, `car_` matches “Cart” or “cars”, while `Car%` matches “Cart”, “cars”, “Cart Rentals”, “Car Rentals”, “CARPET”, and so on.
- To specify multiple keywords, any one of which will result in a match, use the `,` (comma) search operator to separate the keywords. For example, to find all calls that came from either 111-555-1212 or 222-555-1214, you would enter `tel:1115551212,tel:2225551214` in the **Originating #** field.
- To specify that a keyword should NOT appear in record, use the `~` (tilde) search operator in front of the keyword. For example, to find all calls that did NOT come from 111-555-1212, you would enter `~tel:1115551212` in the **Originating #** field.
- To specify that multiple keywords must all appear in a record for it to be a match, use the `+` (plus sign) search operator in front of the keyword.
- You can combine wildcards and search operators. For example, if you want to eliminate all calls that originated from numbers in the 408 and 303 area codes, you would enter `~tel:303%+~tel:408%` in the **Originating #** field.

Field or Link	Description
Reset	Restores the default filter settings and displayed column settings. **Note:** When you click this link, Voice Portal restores the defaults for all filters, even those that are not displayed if the section is collapsed.
Voice Portal	If your installation has multiple Voice Portal systems that use a shared database, this field lists all of the available systems.

Field or Link	Description
	The options are: • **All systems** • A specific Voice Portal system. If you select this option, only the call sessions handled by the MPPs assigned to this system will be shown in the report.
Application	The options are: • **All applications**. This is the default. • A specific application name. **Note:** This filter only works for applications compiled with Dialog Designer 4.0 or later.
more >>	Displays the rest of the optional report filters. **Note:** The rest of the fields in this group do not display until you click this link.
Level	The severity level of the application message. The options are: • **Fatal** • **Error** • **Warning** • **Info** All the levels are selected by default.
Node ID	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`.
Session ID	The session ID assigned by the MPP. **Note:** This field is case-sensitive.
Session Label/UCID	The session label assigned to the application in Dialog Designer or the Universal Call Identifier (UCID) assigned when the application was added to Voice Portal through the VPMS.
Activity Name	The name of the activity associated with the application.

Field or Link	Description
	Note: To exclude the system generated call flow data from the Application Summary report, set the **Activity Name** filter to `~Framework`.
Activity Type	The options are: • **Start** • **In Progress** • **End** • **Cancel** • **VoiceXML Log Tag** • **CCXML Log Tag** • **Node Entry** • **Module Exit** • **Application Exit** • **All Types** All the activity types are selected by default.
Activity Duration	Each application message has a `Duration`, `ActivityName`, and `LogType` field. The `Duration` field contains the number of seconds that have elapsed since an application message with the same `ActivityName` and a `LogType` of `Start` was received. **Note:** The duration is measured in full seconds. If the duration is less than one full second, it is represented as a 0 (zero) in this report. Select a duration from the drop-down list and then, if necessary, enter a time in seconds. The options are: • **All Durations** • **Less Than** `<specified number of seconds>` • **Equal To** `<specified number of seconds>` • **Greater Than** `<specified number of seconds>` For example, if you want to view all instances when the activity named `Call_Survey` lasted for more than five minutes, you would enter `Call_Survey` in the **Activity Name** field, select **Greater Than** from the **Activity Duration** drop-down list, then enter `300` in the **seconds** field. The default is **All Durations**.
Activity Message	All or part of the activity message that you want to use as a filter. You can specify an explicit string or use the % wildcard character.

Field or Link	Description
	For example, to see all logged events whose entire activity message is “transaction completed”, enter `transaction completed` in this field.
Variable Name	The name of a variable defined in the application.
Variable Value	The value of the variable named in **Variable Name**.
Filters from Custom Report	Limits the sessions in this report to those found in the selected custom report. **Note:** Applies all filters specified in another custom report, except the **Date and Time** filter. This option helps you to use filters across different custom report types. For example, if you have a custom Application Detail report that shows when blue cars are rented, you can view a Call Summary report that contains only calls on which blue cars were rented. Select a custom report from the drop-down list which includes all available custom reports.
<< less	Collapses the **Optional Filters** group.

Report Type group

The report type or types you want to summarize by.

The options are:

- **Activity Level** displays he **Summary By Activity Level** table
- **Activity Message** displays the **Summary By Activity Message** table
- **Activity Name** displays the **Summary By Activity Name** table
- **Activity Type** displays the **Summary By Activity Type** table
- **Call Flow** displays the **Summary By Call Flow** table
- **Variable Name** displays the **Summary By Variable Name and Value** table

Application Summary Report page field descriptions

Use the **Application Summary Report** page to view, print, or export an Application Summary report.

This page contains one or more of the following sections, depending on what report types you selected on the Application Summary page:

Summary section

Field	Description
Total Calls	The total number of calls that match the specified filter criteria.
Total Records	The total number of records that match the specified filter criteria. Each call can have any number of records associated with it, depending on what happened during the course of the call and what report types you selected to view in this report.

In addition, this section includes a field for each filter you specified on the Application Summary page.

For example, if you selected anything other than **All Dates and Times** in the **Date and Time** group, the summary section includes an entry for **Time Period**.

Summary By Activity Level table

Field	Description
Activity Level	The activity level. The options are: • **Fatal** • **Error** • **Warning** • **Info**
Call Count	The number of calls during which the given activity level was logged at least once.
Total Count	The total number of times that the given activity level was logged during all calls that match the specified criteria.

Summary By Activity Message table

Field or Link	Description
Single occurrences link	This link, located across from the table name is a toggle. If it says: • **Include Single Occurrences**, then the table only shows those messages that occur more than once. Click the link to show all messages, including the ones that occur only once. • **Exclude Single Occurrences**, then the table shows all messages, regardless of how many times they occur. Click the link to exclude those messages that only occur once.
Activity Message	The text of the activity message.
Call Count	The number of calls during which the given activity message was logged at least once.
Total Count	The total number of times that the given activity message was logged during all calls that match the specified criteria.

Summary By Activity Name table

Field	Description
Activity Name	The name of the activity.
Duration	Displays: • **Minimum**: The shortest time the activity lasted. • **Maximum**: The longest time the activity lasted. • **Average**: The average time the activity lasted.
Call Count	The number of calls during which the given activity was logged at least once.
Total Count	The total number of times that the given activity was logged during all calls that match the specified criteria.

Summary By Activity Type table

Field	Description
Activity Type	The options are: • **Start** • **In Progress** • **End** • **Cancel**

Field	Description
	• **VoiceXML Log Tag** • **CCXML Log Tag** • **Node Entry** • **Module Exit** • **Application Exit** • **All Types**
Call Count	The number of calls during which the given activity type was logged at least once.
Total Count	The total number of times that the given activity type was logged during all calls that match the specified criteria.

Summary By Call Flow table

For each Dialog Designer application, the system automatically logs the caller's selection at every menu, thereby recording each caller's path through the application. Voice Portal groups the paths together by **Source Node**, or starting menu choice, and presents them in this summary report.

Field	Description
Application	The name of the application.
Source Node	The name of the specific node within the application that the caller was on just before they reached the **Destination Node**. This is generally a menu choice in the application.
Destination Node	The name of the node that the caller went to from the associated **Source Node**.
Duration	Displays: • **Minimum**: The shortest time the call flow lasted. • **Maximum**: The longest time the call flow lasted. • **Average**: The average time the call flow lasted.
Total Count	The total number of calls that used this call flow.
Call Flow Graph	Opens a separate window that displays the call flow visualization. To view the call flow visualization graph, you must have Graphviz installed on Voice Portal. For information on how to install Graphviz, see the Graphing software not installed topic in the Troubleshooting Voice Portal guide. **Note:** To print large graphs, use the scaling options provided by your printer. You can typically access these options by clicking **Preferences** or **Properties** on the **Print** dialog box.

Summary By Variable Name and Value table

Field or Link	Description
Single occurrences link	This link, located across from the table name, is a toggle. If it says: • **Include Single Occurrences**, then the table only shows those variables that occur more than once. Click the link to show all variables, including the ones that occur only once. • **Exclude Single Occurrences**, then the table shows all variables, regardless of how many times they occur. Click the link to exclude those variables that only occur once.
Variable Name	The name of the variable used by the application.
Variable Value	The value of the specified variable.
Call Count	The number of calls during which the given variable was logged at least once.
Total Count	The total number of times that the given variable was logged during all calls that match the specified criteria.

Applications page field descriptions

Use this page to:

- View information about the speech applications currently deployed on the Voice Portal system
- Add new applications to the system
- Change the settings for an existing application
- Change the order in which the applications are launched when a call comes in
- View and configure the configurable application variables of a Dialog Designer, VXML, and CCXML/VXML application.

Note:

You cannot configure the configurable application variables for a pure CCXML application.

Column or Link	Description
Change Launch Order	Opens the Application Launch Order window that lets you specify the application priority. **Note:** Voice Portal only takes application priority into account if you have specified two or more applications whose assigned inbound numbers overlap due to the use of wildcards. When a call comes in that could be handled by one or more applications, Voice Portal launches the application that appears first on this page.
Selection check box	Indicates which applications you want to delete.
Organization	The name of the organization associated with the application you want to add. **Note:** This field is displayed only if organization level access is enabled in the Voice 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 Voice Portal on page 89.
Name	The names of all speech applications administered on the system. **Note:** • If you select an organization in the field above, the selected organization and forward slash character are automatically prefixed to the application name. If you do not select the organization name, this indicates that the application does not belong to any organization. For more information on organization level applications see Organization level access in Voice Portal on page 89. • Once you save the application, this name cannot be changed. Click the name to open the Change Application page.
Enable	Whether this application is available for use by the Voice Portal system.
Type	The options are: • **VoiceXML**. • **CCXML**. • **CCXML/VoiceXML**. **Note:** Additional type options may be available if you have installed managed application on Voice Portal. For more information on managed application type, see the documentation delivered with the managed application.
URL	The Universal Resource Indicator (URI), or full HTTP path, to the root document of the application.

Column or Link	Description
Launch	The options are: • The inbound URI or one or more telephone numbers that are assigned to this application. If the assigned numbers for two or more applications overlap, Voice Portal launches the application that appears first on this page. • **Inbound Default**: This application handles all inbound calls made to a number that is not associated with any other application. • **Outbound**: This application handles outbound calls.
ASR	If this application uses Automatic Speech Recognition (ASR) resources, this field shows the ASR engine type that will be used. Otherwise it displays **No ASR**.
Languages	The languages that can be used by this application for ASR activities.
TTS	If this application uses Text-to-Speech (TTS) resources, this field shows the TTS engine type that will be used. Otherwise it displays **No TTS**.
Voices	The languages and voices that can be used by this application for TTS activities.
Configurable Application Variables	Opens a page that displays the configurable application variable defined in the application. You can use this page to change these configurable application variables.
Add	Opens the Add Application page.
Delete	Deletes the applications whose associated Selection check box is checked.

Browser Settings page field descriptions

Use this page to configure the Browser settings that affect all MPPs in the Voice Portal system.

This page contains the:

- VoiceXML Properties group on page 293
- VoiceXML Browser Properties group on page 295
- CCXML Browser Properties group on page 296

Note:
Click the group heading to expand or collapse the group.

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 Voice Portal.

Field	Description
Reset to Default	Restores the default settings for all fields.
Language	The default application language. The available choices depend on the ASR application languages installed on your Voice 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.
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.

Field	Description
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.
Maximum Cache Age section	
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 Voice 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. For details, see Add Application page field descriptions on page 255.
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.

Field	Description
	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, used to interrupt infinite loops from (possibly malicious) scripts. Enter a value in the range 0 to 999999. The default is 100000 .
Cache section	
Total Size	The maximum size for the AVB cache. Once this size is reached, Voice 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.
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 1 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

Field	Description
	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.
SSL Verify	The options are: • **Yes**: If an application is configured to use https and this option is set to Yes, Voice 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**: Voice 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

Field	Description
	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.

Change Application page field descriptions

Use this page to change an existing speech application.

This page contains the:

General settings section

Field	Description
Name	The name used to identify this application on the Voice Portal system. If you are using a Nuance server, this name must be between 1 and 30 characters. **Note:** This field cannot be changed.
Enable	Whether this application is available for use by the Voice Portal system. The default is **Yes**, which means the application is available.
Type	The type of Multipurpose Internet Mail Extensions (MIME) encoding used by this application.

Field	Description
	The options are: • **VoiceXML**: If selected, Voice Portal displays the **VoiceXML URL** field. • **CCXML**: If selected, Voice Portal displays the **CCXML URL** field. • **CCXML/VoiceXML**: If selected, Voice Portal displays both the **VoiceXML URL** and the **CCXML URL** fields. **Note:** Additional type options may be available if you have installed managed application on Voice Portal. For more information on managed application type, see the documentation delivered with the managed application.

URL group

Field	Description
Type	The options are: • **Single**: The only application server that handles the calls. • **Fail Over**: Allows you to add two URLs to handle a fail over: - URL 1: The primary application that handles the calls - URL 2: The application that handles the calls upon the failure of the primary application. • **Load Balance**: Allows you to add two URLs for load balancing purpose. The URLs are also used for failover. For instance, if URL 2 fails, URL1 handles all calls.
CCXML URL	The HTTP path to the root document of the Call Control eXtensible Markup Language (CCXML) speech application. The URL must be in the format `[http:|https:]//`*`domain.name/subdirectory/startDocument`* where • `[http:|https:]` indicates whether the URI uses normal or secure HTTP protocol. **Note:** You must specify a URL that begins with `https:` if you want Voice Portal to use

Field	Description
	a secure connection between the MPP and the application server. • *domain.name* is the fully qualified domain name or the IP address of the server on which the application resides. You can use a relative path for your domain name, but Avaya recommends that you use the fully qualified domain name. • *subdirectory* is an optional subdirectory or series of subdirectories on the application server. • *startDocument* is the first page that the CCXML-compliant speech application should load. The extension on this document will typically be `ccxml`, `htm`, `html`, `jsp`, or `xml`. For example, `vpmenu.html` or `vpmenu.jsp?gtype=vxml-srgs-avaya-ibm`. **Note:** Voice Portal uses the Oktopous™ ccXML Interpreter.
VoiceXML URL	The HTTP path to the root document of the VoiceXML speech application. The URL must be in the format `[http:|https:]//`*domain.name*`/`*subdirectory*`/`*startDocument* where • `[http:|https:]` indicates whether the URI uses normal or secure HTTP protocol. **Note:** You must specify a URL that begins with `https:` if you want Voice Portal to use a secure connection between the MPP and the application server. • *domain.name* is the fully qualified domain name or the IP address of the server on which the application resides. You can use a relative path for your domain name, but Avaya recommends that you use the fully qualified domain name.

Field	Description
	• *subdirectory* is an optional subdirectory or series of subdirectories on the application server. • *startDocument* is the first page that the VoiceXML-compliant speech application should load. The extension on this document will typically be `htm`, `html`, `jsp`, `vxml`, or `xml`. For example, `vpmenu.html` or `vpmenu.jsp?gtype=vxml-srgs-avaya-ibm`.
Verify	Instructs Voice Portal to open the associated root document in a new browser window. If the document cannot be found, the new browser window displays a `file not found` error. **Note:** **Verify** is not displayed if the URL(s) contains a secure HTTP protocol (https:), and the **Mutual Certificate Authentication** field is set to **Yes**.
Mutual Certificate Authentication	Enables mutual certificate authentication between the MPP and the application. **Important:** Do not enable this option if your application uses external grammars stored on the application server. The speech servers do not support mutual certificate authentication and therefore will not fetch the grammar from the application server. If you select this option ensure that: • The application server is configured to support mutual configuration and the MPP certificate is installed on the application server. • The application certificate is installed on the MPP. Voice Portal allows you to add and view the application certificate from the **Security>Certificates>Trusted Certificates** page in VPMS. • The URLs use secure HTTP protocol (https).

Field	Description
Basic Authentication	Enables user name and password authentication between the MPP and the application. Ensure that the application server is configured to support basic configuration. **Important:** Do not enable this option if your application uses external grammars stored on the application server and uses a Nuance speech server, as Nuance does not support basic authentication. If you select the **Basic Authentication** option, Voice Portal displays: • **User name** field: The name used to authenticate the MPP and the application. **Note:** The user name must not contain the *:* character. • **Password** field: The password used to authenticate the MPP and the application. **Note:** You can select both **Mutual Certificate Authentication** and **Basic Authentication** options.

Speech Servers group

Field	Description
ASR	If this application uses Automatic Speech Recognition (ASR) resources, this field lets you select the ASR engine type that will be used. The options are: • **No ASR**: This application does not use ASR resources. • The engine type associated with the ASR server to use for this application. The available engine types depend on the ASR servers on the Voice Portal system. If you select an engine type, Voice Portal displays the **Languages** field.
Languages	If an ASR engine is selected, this field displays the languages configured for the ASR servers of that engine type on the Voice Portal system. Select one or more languages for this application. Your selections must match exactly the ASR language defined in the speech application.

Field	Description
	Use `Ctrl+Click` and `Shift+Click` to make more than one selection from this list. The first selected language becomes the default for this 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 are configured for any single ASR server, Voice Portal sends a `No ASR Resource` exception to the application. What happens then depends on the event handler that the application uses.
TTS	If this application uses Text-to-Speech (TTS) resources, this field lets you select the TTS engine type that will be used. The options are: • **No TTS**: This application does not use TTS resources • The engine type associated with the TTS server to use for this application. The available options depend on the TTS servers on the Voice Portal system. If you select an engine type, Voice Portal displays the **Voices** field.
Voices	If a TTS engine is selected, this field displays the voices configured for the TTS servers of that engine type on the Voice Portal system. Select one or more default voices for this application. Your selections must match exactly the TTS voice defined in the speech application. Use `Ctrl+Click` and `Shift+Click` to make more than one selection from this list. The first selected voice becomes the default for this 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, Voice Portal sends a `No TTS Resource` exception to the application. What happens then depends on the event handler that the application uses.

Application Launch group

Note:

Voice Portal uses the information you enter in this group to make a master list of all telephone numbers and Universal Resource Indicators (URIs) that are mapped to specific applications. It then takes the number or URI dialed by the caller as input and determines which speech application is assigned to handle that number.

If you do not map any phone numbers or URIs to an application, then that application automatically handles any calls that come from numbers or URIs that are not otherwise mapped. However, you can only have one such application on the system. If you attempt to configure a second application without a DNIS or URI, the system generates an error.

Field or Button	Description
Type	The options are: • **Inbound**: This application handles inbound calls from a URI or one or more specified telephone numbers. • **Inbound Default**: This application handles all inbound calls made to a number that is not associated with any other application. • **Outbound**: This application handles outbound calls.
Number type radio buttons	The options are: • **Number**: Instructs Voice Portal to associate the application with a single telephone number. • **Number Range**: Instructs Voice Portal to associate the application with a sequential range of telephone numbers. • **URI**: Instructs Voice Portal to associate the application with a single URI.
Called Number	The definition of this field depends on the selected number type. If the number type is: • **Number**: This field is the telephone number you want to associate with this application. • **Number Range**: This field is the lowest telephone number in the range you want to associate with this application. • **URI**: This field is not available. You can enter from 1 to 15 digits. Do not include spaces or special characters such as (,), or -.
To	If you selected the number type **Number Range**, this field is the highest telephone number in the range you want to associate with the application. If you selected any other number type, this field is not available.
Called URI	If you selected the number type **URI**, this is the URI you want to associate with the application. You can use any valid regular expression wildcards such as: • `?` to represent a single character • `*` to represent multiple characters If you selected any other number type, this field is not available.
Add	Associates the number, range of numbers, or URI with the application. After you click **Add**, the specified number, range of numbers, or URI appears in the display text box.
Display text box	Displays all the DNIS numbers and URIs that are mapped to this speech application. Select an individual entry in this list by clicking on it, or use `Ctrl+Click` and `Shift+Click` to select multiple entries.

Field or Button	Description
Remove	Removes the association between the selected entries in the display text box and the application.

Speech Parameters group

When determining what value to use for each of the following settings, Voice Portal looks at the following sources:

- The speech application itself. If the parameter is defined in the application, Voice Portal uses that value.
- The values entered on this page. If the parameter is not defined in the application but is defined on this page, Voice Portal uses the value defined here.
- The values entered on the AVB Settings page.
- The default values defined for the Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) server by the server manufacturer. To determine the default settings for your ASR server, consult your server documentation.

Note:

If these fields are not displayed, click the group heading to expand the group.

Field	Description
ASR section	
Confidence Threshold	The confidence level below which the ASR engine will reject the input from the caller. Enter a number from `0.0` to `1.0`. 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`. **Note:** If you are using Dialog Designer, see the **Confidence** field description in your Dialog Designer documentation.
Sensitivity Level	How loud an utterance must be for the ASR engine to start speech recognition. Enter a number from `0.0` to `1.0`. 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. **Note:** If you are using Dialog Designer, refer to the *Nodes and Palette Options* chapter in the *DD Developer's Guide* for more information on the **Sensitivity** field description.

Field	Description
Speed vs. Accuracy	The balance between speed of recognition and accuracy of recognition. Enter a number from 0.0 to 1.0. 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. This value is mapped to whatever scale the ASR engine uses to compute the balance between speed and accuracy of recognition. **Note:** If you are using Dialog Designer, see the **Speed vs. Accuracy** field description in your Dialog Designer documentation.
N Best List Length	The maximum number of recognition results that the ASR engine can return. • For Nuance and IBM WVS, enter a number from 1 to 100. • For Loquendo, enter a number from 1 to 10. **Note:** If you are using Dialog Designer, see the **N-Best** input form field description in your Dialog Designer documentation.
No Input Timeout	The number of milliseconds the system waits for a caller to respond after the prompt is finished playing and before the system throws a No Input event. For Nuance, Loquendo and IBM WVS, enter an integer value in the range 0 to 65535. **Note:** If you are using Dialog Designer, see the **Timeout** field on the Prompt main tab in your Dialog Designer documentation.
Recognition Timeout	The number of milliseconds the system allows the caller to continue speaking before the system ends the recognition attempt and throws a `maxspeechtimeout` event. For Nuance, Loquendo and IBM WVS, enter an integer value in the range 0 to 65535.

Field	Description
	Note: This field corresponds to the **Maximum Speech** field in your VoiceXML application. For more information, see your Dialog Designer documentation.
Speech Complete Timeout	The number of milliseconds of silence required following user speech before the speech recognizer either accepts it and returns a result or reject it and returns a No Match event. Enter an integer in this field. • For Nuance and IBM WVS, enter a value in the range 0 to 65535. • For Loquendo, enter a value in the range 300 to 10000. This value is used when the recognizer currently has a complete match of an active grammar, and specifies how long it should wait for more input declaring a match. By contrast, the incomplete timeout is used when the speech is an incomplete match to an active grammar. **Tip:** Take care when setting this property. If you set the number too high, it can slow down system response time, even for successful recognitions. If you set the number too low, it can lead to an utterance being cut off prematurely. Reasonable values for this property are usually in the range of 5000 to 15000 milliseconds.
Speech Incomplete Timeout	The number of milliseconds of silence following user speech after which a recognizer finalizes a result. Enter an integer in this field. • For Nuance and IBM WVS, enter a value in the range 0 to 65535. • For Loquendo, enter a value in the range 300 to 10000. The incomplete timeout applies when the speech prior to the silence is an incomplete match of all active grammars. In this case, once the timeout is triggered, the speech recognizer rejects the partial result and returns a No Match event. **Tip:** Take care when setting this property. If you set the number too high, it can slow down system response time, even for successful recognitions. If you set the number too low, it can lead to an utterance being cut off prematurely. This property is usually set lower than the **Speech Complete Timeout** but high enough to allow for callers to pause mid-utterance. **Note:** If you are using Dialog Designer, see the **Timeout Incomplete** field description in your Dialog Designer documentation.
Maximum Grammar Cache Age	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.

Field	Description
	Enter a whole number of seconds in this field. When determining whether an utterance is stale or not, the application adds this time together with the value specified in the **Maximum Grammar Staleness** field and compares that to the age of the utterance plus the value in the **Minimum Grammar Freshness Time** field. The maximum grammar cache age plus the maximum grammar staleness time must be greater than or equal to the age of the utterance plus the minimum grammar freshness time. For example, if the: • Maximum grammar cache age is 60 • Maximum grammar staleness is 20 • Current utterance has been cached for 45 seconds. • Minimum grammar freshness time is 30 Then the application will accept the utterance from the MPP because the expression 60 + 20 > 45 + 30 evaluates as True. **Note:** For the purposes of this calculation, if the maximum grammar staleness field is blank, that is the same as setting it to infinity. In that case, the application will always accept the cached utterance from the MPP because the maximum grammar cache age plus infinity will always be greater than the utterance age plus the minimum grammar freshness time.
Minimum Grammar Freshness Time	The minimum length of time beyond an utterance's current age for which the utterance must remain fresh to be accepted by the application. Enter a whole number of seconds in this field. The application adds this value to the current age of the utterance and compares the result to the value in the **Maximum Grammar Cache Age** field plus the value in the **Maximum Grammar Staleness** field, as described above.
Maximum Grammar Staleness	The maximum amount of time beyond the normal expiration time of an utterance that the application server will accept. Enter a whole number of seconds in this field, or leave it blank to instruct the application to always use a cached response of any age. The application adds this value to the value in the **Maximum Grammar Cache Age** field and compares it to the current age of the utterance plus the value in the **Minimum Grammar Freshness Time** field, as described in the **Maximum Grammar Cache Age** field.
Vendor Parameters	Any vendor-specific or platform-specific parameters that the ASR server requires to function correctly with this speech application. **Note:** Contact your speech server provider for details on vendor parameters.

Field	Description
	These parameters must be in the general form*parameter=value*. You can include as many parameters as you want. Use semi-colons (`;`) to separate multiple entries. For example, you might need to specify:`ep.ThresholdSnr=12;Rec.PPR=1`
TTS section	
Prosody Volume	The default value for the loudness of the synthesized speech output. Specify one of the following values from the drop-down list or enter a value in the text field. • `<NONE>` • `default` • `silent` • `x-soft` • `soft` • `medium` • `loud` • `x-loud` **Note:** The text field is enabled only when you select None in the drop-down list. The text field is not displayed if you select Loquendo in the **TTS** field. Enter a number from 0 to 100, where zero (0) represents no audible output and 100 represents full volume **Note:** Avaya recommends setting the **Prosody Volume** to 50 to ensure that: • The TTS resource is properly initialized for the request. • All prompts from different speech server with different default volume settings, that include prerecord prompts, are played at the same volume.
Prosody Rate	Voice Portal uses this value to fine tune the default TTS speaking rate relative to the server default. Specify one of the following values from the drop-down list or enter a value in the text field. • `<NONE>` • `default` • `x-slow` • `slow`

Field	Description
	• medium • fast • x-fast **Note:** The text field is enabled only when you select None in the drop-down list. The text field is not displayed if you select Loquendo in the **TTS** field. For IBM WVS servers, enter a number from 70 to 1297. **Note:** The prosody rate for IBM WVS is based on the speaking rate in words per minute (wpm). For Nuance and Loquendo servers, enter a number from 0 to 100.
Vendor Parameters	Any vendor-specific or platform-specific parameters that the TTS server requires to function correctly with this speech application. **Note:** Contact your speech server provider for details on vendor parameters. These parameters must be in the general form *parameter=value*. You can include as many parameters as you want. Use semi-colons (`;`) to separate multiple entries. For example, to specify that a Nuance RealSpeak server should use the custom dictionary called `mydictionary.dct` on a Linux RealSpeak server, you would enter:`ssftrs_dict_enable=file:///opt/ttsdict/mydictionary.dct`. For more information, see Adding custom dictionaries for Nuance RealSpeak on page 343.

Reporting Parameters group

Note:
If these fields are not displayed, click the group heading to expand the group.

Field	Description
Application Logging section	
Minimum Level	Determines what messages will be sent by this application through the Application Logging web service. You can view this information in the Application Summary or Application Detail report. The options are: • **None**: Voice Portal ignores all application messages. If this option is selected, this application will not appear in any application reports. • **Fatal**: Voice Portal saves fatal level messages. • **Error**: Voice Portal saves fatal and error level messages.

Field	Description
	• **Warning**: Voice Portal saves fatal, error, and warning level messages. • **Info**: Voice Portal saves all messages sent by this application.
Call Flow Data Sample Rate	The percentage of times that this application will generate breadcrumb data when it runs. For example, if this field is set to 25%, then the application will generate breadcrumbs once out of every four times it runs. You can use this field to cut down on application logging if your Voice Portal system is running under a heavy load.
Transcription section	
Transcription Enabled	The options are: • **Yes**: Voice Portal creates a transcription log for each call handled by the application. If you select this option, the rest of the fields in this group become available. • **No**: Voice Portal does not save any transcription or performance data.
Transcription Sample Rate	The percentage of times that this application will generate a transcription log when it runs. For example, if this field is set to 25%, then the application will generate a transcription log once out of every four times it runs. You can use this field to reduce application logging if your Voice Portal system is running under a heavy load. **Note:** The total number of transcriptions per day per MPP is set in the **Maximum Transcriptions per Day** on the MPP Settings page.
Performance Trace	The options are: • **Yes**: Voice Portal creates a performance trace log for each call handled by the application that has an associated transcription log. **Note:** This information can be viewed on the Session Details page, which is accessible from the Session Detail Report page. • **No**: Voice Portal does not save performance trace data.
DTMF Data	Determines the information Voice Portal saves in the application's transcription log when a Dual-tone multi-frequency (DTMF) event occurs. The options are: • **Discard**: Voice Portal saves only the DTMF event. • **Save**: Voice Portal saves the DTMF event and its associated data.
Prompt Data	Determines the information Voice Portal saves in the application's transcription log when a prompt event occurs.

Field	Description
	The options are: • **Discard**: Voice Portal saves only the prompt event. • **Save**: Voice Portal saves the prompt event and its associated data.
TTS Data	Determines the information Voice Portal saves in the application's transcription log when a Text-to-Speech (TTS) event occurs. The options are: • **Discard**: Voice Portal saves only the TTS event. • **Save**: Voice Portal saves the TTS event and the first few characters of the TTS data.
Speech Data	Determines the information Voice Portal saves in the application's transcription log when a speech event occurs. The options are: • **Discard**: Voice Portal saves only the speech event with no result. • **Text Only**: Voice Portal saves the speech event with the result in text format. • **Text and Speech**: Voice Portal saves the speech event along with a link to the URL that contains the associated WAV file. The system stores each recording as a separate audio file on the MPP. Therefore, if you select this option for a very active application, you could end up with a large number of WAV files in a single directory. This could lead to performance issues over time.

Advanced Parameters group

Note:

If these fields are not displayed, click the group heading to expand the group.

Field	Description
Support Remote DTMF Processing	Whether the ASR server or the MPP server performs Dual-tone multi-frequency (DTMF) processing. The options are: • **Yes**: The ASR server performs DTMF processing. • **No**: The MPP server performs DTMF processing.
DTMF Type Ahead Enabled	Whether the application supports DTMF type ahead. DTMF type ahead feature allows a user to provide DTMF input when the prompt is being presented and thereby skip the prompt. The options are: • **Yes**: The application supports DTMF type ahead. • **No**: The application does not support DTMF type ahead.

Field	Description
	Note: This field is enabled only when the **Support Remote DTMF Processing** field is set to **No**.
Converse-On	Whether the application is invoked by an Avaya Call Center system using the **converse-on** vector command. The **converse-on** vector command makes it possible for the Call Center vector program to call and access a speech application on the Voice Portal system. When it does so, the vector program on the Call Center server makes it possible to send data in the form of DTMF tones. This option tells Voice Portal to listen for these DTMF tones before starting the VoiceXML application. **Note:** At run time, the MPP writes the DTMF digit data to the session variable `session.telephone.converse_on_data`. VoiceXML applications can access this data from that variable. In the case of Dialog Designer applications, the system writes this data to the `vpconverseondata` field of the `session` variable. For more information, see the Dialog Designer documentation.
Network Media Service	Whether this application uses the “voice dialog” Network Media Service for passing the application starting URI as part of the SIP invitation. **Note:** For more information, see RFC 4240 at http://www.rfc-archive.org/getrfc.php?rfc=4240.
Dialog URL Pattern	A regular expression used to verify the starting URI form the SIP invitation. This is a security parameter used to verity the URI is “trusted.” If it is blank, then any URI will be accepted.
VoiceXML Event Handler	The VoiceXML event handler to use for this application. The options are: • **<Default>**: This application uses the default VoiceXML error handler defined for the Voice Portal system. • An error handler name: This application uses a specific error handler instead of the system default. This drop-down lists all VoiceXML error handlers that have been uploaded through the Add VoiceXML Event Handler page.
CCXML Event Handler	The CCXML event handler to use for this application. The options are: • **<Default>**: This application uses the default CCXML error handler defined for the Voice Portal system. • An error handler name: This application uses a specific error handler instead of the system default. This drop-down lists all CCXML error

Field	Description
	handlers that have been uploaded through the Add CCXML Event Handler page.
Generate UCID	The Universal Call Identifier (UCID) is an Avaya-proprietary call identifier used to help correlate call records between different systems. *Inbound Calls:* If the Avaya Communication Manager (CM) passes a UCID to Voice Portal, Voice Portal always uses that UCID regardless of the setting in this field. If, however, CM does not pass a UCID, the Voice Portal MPP server can generate one for the call. The options are: • **Yes**:If the CM does not pass a UCID to Voice Portal, the MPP server generates a UCID. • **No**: The MPP does not generate a UCID. *Transfers & Outbound calls:* The options are: • **Yes**: For blind and supervised transfers using the `<redirect>` CCXML tag, the MPP uses the same UCID as the call being transferred. For Bridge and Outcalls , MPP will generate a new 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 Voice Portal treats the UUI data. The options are: • **Service Provider**: Voice 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**: Voice 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 235.
Transport UCID in Shared Mode	If **Operation Mode** is set to **Shared UUI** and **Generate UCID** is set to **Yes**, this field determines whether Voice Portal encodes a Voice 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 Voice Portal by the application.

Field	Description
Maximum UUI Length	The maximum length of the UUI data that can be passed in the SIP header. If this length is exceeded and Voice 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 Voice Portal by the application, Voice 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. Enter an integer between 0 and 2,048, where 0 indicates that Voice Portal should not check the length of the UUI data. The default is 128.
Fax Detection Enabled	Whether this application should detect whether the inbound number is a fax machine. 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.
Video Enabled	Whether to enables or disables the support for the video server. The options are: • **Yes**: Enables the video server for a particular application. • **No**: Disables the video server for a particular application.
Video Screen Format	Select the video screen format. The options are: • **CIF**: Common Intermediate Format. The screen resolution for CIF is 352x288 pixels. • **QCIF**: Quarter CIF. The screen resolution for QCIF is 176x144 pixels. • **SQCIF**: Sub-Quarter CIF. The screen resolution for SQCIF is 128x96 pixels.
Video Minimum Picture Interval	Video Minimum Picture Interval (MPI) is the time interval used to define the frame rate. MPI uses the CIF, QCIF, and SQCIF formats. Enter a value in the range 1 to 32. The default is 2. For CIF, QCIF and SQCIF, if the value is zero, the screen format is disabled otherwise the frame rate is defined by (29.97/MPI). For example: for value 1 = 30 FPS, for 2 = 15 FPS, and so on.

CCXML tab on the Event Handlers page field descriptions

Use this tab to configure the CCXML event handlers available to all MPPs on the Voice Portal system.

Column or Button	Description
Selection check box	Indicates the CCXML event handlers you want to delete. There is no section check box next to: • Any Avaya-supplied error handlers, as these error handlers cannot be deleted. • The default error handler, even if it is customer-installed. If you want to delete it, specify a new default and then check the Selection check box associated with the old customer-installed default handler.
File Name	The name of the event handler file.
Upload Time	The options are: • **<System>**: This event handler was installed with Voice Portal. • The date and time at which the file was uploaded.
Default	The options are: • **Current Default**: This is the default event handler. Voice Portal uses this event handler for any application that does not have a specific event handler associated with it. • **<Make Default>** link: This is not the current default handler. Click this link to make this the default event handler.
Export	Opens the contents of the error handler in a browser window or saves it to your local machine.
Add	Opens the Add CCXML Event Handler page.
Delete	Deletes the selected event handlers.

Prompts tab on the Event Handlers page field descriptions

Use this tab to configure the event handler prompts available to all MPPs on the Voice Portal system.

Column or Button	Description
Selection check box	Indicates the event handler prompts you want to delete. There is no section check box next to: • Any Avaya-supplied error handler prompts, as these prompts cannot be deleted. • The default error handler prompt, even if it is customer-installed. If you want to delete it, specify a new default and then check the Selection check box associated with the old customer-installed default event handler prompt.
File Name	The name of the event handler prompt file.
Upload Time	The options are: • **<System>**: This event handler prompt was installed with Voice Portal. • The date and time at which the prompt file was uploaded.
Export	Opens the contents of the error handler in the default player or saves it to your local machine.
Add	Opens the Add Event Handler Prompt page.
Delete	Deletes the selected event handler prompts.

VoiceXML tab on the Event Handlers page field descriptions

Use this tab to configure the VoiceXML event handlers available to all MPPs on the Voice Portal system.

Column or Button	Description
Selection check box	Indicates the VoiceXML event handlers you want to delete. There is no section check box next to: • Any Avaya-supplied error handlers, as these error handlers cannot be deleted. • The default error handler, even if it is customer-installed. If you want to delete it, specify a new default and then check the Selection check box associated with the old customer-installed default handler.
File Name	The name of the event handler file.

Column or Button	Description
Upload Time	The options are: • **<System>**: This event handler was installed with Voice Portal. • The date and time at which the file was uploaded.
Default	The options are: • **Current Default**: This is the default event handler. Voice Portal uses this event handler for any application that does not have a specific event handler associated with it. • **<Make Default>** link: This is not the current default handler. Click this link to make this the default event handler.
Export	Opens the contents of the error handler in a browser window or saves it to your local machine.
Add	Opens the Add VoiceXML Event Handler page.
Delete	Deletes the selected event handlers.

MPP Servers page field descriptions

Use this page to view, add, change, and delete the Media Processing Platform (MPP) servers currently administered on the Voice Portal system.

Tip:

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

Field	Description
Selection check box	Indicates which MPP servers you want to delete.
Name	The unique identifier for the MPP server on the Voice Portal system.
Host Address	The network address, or location, of the computer on which the MPP server resides. The VPMS uses this address to communicate with the MPP server.
Network Address (VoIP)	The IP address the telephony servers must use to communicate with the MPP.

Field	Description
	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 Voice 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.
Event Handlers	Opens the Event Handlers page so you can change the global event handlers and prompts 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.

Report Data Configuration page field descriptions

Use this page to configure download settings for Session Detail Record (SDR), Call Detail Record (CDR), and Application Detail Record (ADR) data.

This page contains the:

General section

This section determines what records Voice Portal downloads from the MPP servers to the Voice Portal database. Voice Portal uses this data to create the call, session, application, and performance reports.

If you have:

- A single Voice Portal system, this database resides on the VPMS server.
- Multiple Voice Portal systems that share an external database, this database resides in a centralized location determined by your site's configuration.

Field	Description
Download Session Detail Records	The options are: • **Yes**: Voice Portal downloads the Session Detail Records (SDRs). • **No**: The SDRs are not downloaded to the VPMS. If necessary, you can view this data in the MPP logs through the Log Directories page on the MPP Service Menu. This information is the required in order to create the Session Summary report and Session Detail report.
Download VoiceXML Log Tags	The options are: • **Yes**: Voice Portal downloads the Voice eXtensible Markup Language (VoiceXML) Log tag data. • **No**: The Log tag data is not downloaded to the VPMS and will not appear in the application reports. This information is required to view VoiceXML Log tag messages in the Application Summary report and Application Detail report.

Field	Description
Download CCXML Log Tags	The options are: • **Yes**: Voice Portal downloads the Call Control eXtensible Markup Language (CCXML) Log tag data. • **No**: The Log tag data is not downloaded to the VPMS and will not appear in the application reports. This information is required to view CCXML Log Tag messages in the Application Summary report and Application Detail report.

Report Database Record Data group

Field	Description
Purge Records	The options are: • **Yes**: Voice Portal automatically purges the data from the database when the specified retention time has passed. • **No**: The data remains in the Voice Portal database until it is manually deleted. **Note:** **Yes** is recommended for most Voice Portal configurations. Use **No** *only* if there is a database administrator who is responsible for maintaining the Voice Portal database and making sure that old records are deleted in a timely fashion.
Call/ Session Retention Period	The number of days the VPMS retains call and session data records. The system purges any data that is older than this setting. Voice Portal uses this data to create the call activity reports. Enter a whole number from 0 to 9999. The default is 30. **Note:** This field is available only if **Purge Records** is set to **Yes**.
Application Retention Period	The number of days the VPMS retains application data records. The system purges any data that is older than this setting. Voice Portal uses this data to create the application reports. Enter a whole number from 0 to 9999. The default is 15. **Note:** This field is available only if **Purge Records** is set to **Yes**.
Performance Retention Period	The number of days the VPMS retains performance data records. The system purges any data that is older than this setting. Voice Portal uses this data to create the Performance report. Enter a whole number from 0 to 9999. The default is 30. **Note:** This field is available only if **Purge Records** is set to **Yes**.

Field	Description
Performance Report Aggregation Period	The number of minutes for the system to use as the periodic interval to collect, average, and store performance data records for the Performance report. Enter a whole number from 0 to 999. The default is 5.
Managed Application Retention Period	The number of days the VPMS retains managed application data records. The system purges any data that is older than this setting. **Note:** This field is displayed only if a managed application is installed on Voice Portal. Voice Portal uses this data to create the managed application reports. Enter a whole number from 0 to 9999. The default is 15. **Note:** This field is available only if **Purge Records** is set to **Yes**.

Scheduled Reports group

Field	Description
Output Folder Size	Maximum data storage capacity allocated for the output folder. The default is 5 GB. Setting the output folder size helps in controlling the use of disk space.
Output Retention (days)	The number of days the VPMS retains the report output files from the scheduled reports. The default for hourly report is 7 days, for Daily and one time reports is 30 days, weekly reports is 90 days and for monthly report the default is 365 days. The system purges any report output that is older than these setting.
Sender Email Address	The e-mail addresses used when sending the report notifications. By default this field is blank. If you do not specify the **Sender Email Address**, the system uses the To e-mail address specified for the e-mail notification while scheduling the report. **Note:** The e-mail address can contain only the alphanumeric characters (a-z, A-Z and 0-9) and the following special characters: ., _, %, +, -, @. For example, service@avaya.com, Tech.Support@avaya.com, tech_support@avaya.com, Support_01@avaya.com.

Download Schedules group

Field or Button	Description
Periodic Download	If this field is set to **Yes**, Voice Portal automatically downloads report data from the MPP servers at regular intervals.

Field or Button	Description
	The interval is specified in the **Download Interval** field. You should only select this option if your network can handle the bandwidth required to download the report data while the system is at full capacity.
Download Interval	If **Periodic Download** is **Yes**, the number of minutes that should elapse between downloads.
On-demand Download	If this option is set to **Yes**, Voice Portal downloads the latest data from the MPP servers whenever a user generates a report through the VPMS.
New Schedule	To create a new download schedule, select the check boxes for the appropriate days of the week on which this download should run.
Start Time	To create a new download schedule, enter the time that the download should start running using a 24-hour clock in the format `hh:mm`. For example, to set the download time to midnight, enter `00:00`. To set the download time to 11:59 p.m., enter `23:59`.
Add	Saves the new schedule.
Download Schedules	The current download schedules. You can select individual entries in this list by clicking on them.
Remove	Removes the selected schedules in the **Download Schedules** display text box.

Application Launch Order window field descriptions

Use this window to change the priority of the applications on the Voice Portal system.

Voice Portal only takes application priority into account if you have specified two or more applications whose assigned inbound numbers overlap due to the use of wildcards. When a call comes in that could be handled by one or more applications, Voice Portal launches the application that appears first on this page.

Field or Button	Description
Application Launch Order	This list box displays all applications on the Voice Portal system. Click on any application to select it.
Up Arrow icon	Moves the selected application up one position.
Down Arrow icon	Moves the selected application down one position.

Chapter 8: Speech servers in Voice Portal

Speech servers in Voice Portal

The Voice Portal system integrates with two types of third-party speech servers:

- Automatic Speech Recognition (ASR) technology enables an interactive voice response (IVR) system to collect verbal responses from callers.
- Text-to-Speech (TTS) technology enables an IVR system to render text content into synthesized speech output according to algorithms within the TTS software.

Voice Portal supports up to 5,000 telephony ports that can be distributed among any number of ASR and TTS servers. All ASR servers must come from the same vendor, and all TTS servers must come from the same vendor. You can, however, have ASR servers from one vendor and TTS servers from a different vendor.

Supported ASR speech servers

Required versions

Speech Server	Minimum Version Required	Also Required
IBM WebSphere Voice Server	R5.1.3	Fix Pack 3
Nuance Recognizer	9.0.3	Nuance Speech Server (NSS) version 5.0.3 **Note:** Avaya recommends that you use NSS version 5.0.4 or later.
Nuance OpenSpeech Recognizer (OSR)	3.0.13	SpeechWorks MediaServer (SWMS) component version 3.1.14 or 3.1.15 **Note:** SWMS version 4.0 is not supported.
Loquendo	7.6.0	Loquendo Speech Suite (LSS)

Speech Server	Minimum Version Required	Also Required
		7.0.4 – for Linux 7.0.13 – for Windows

MRCP support

Speech Server	MRCP V1 Support	MRCP V2 Support
IBM WebSphere Voice Server	MRCP V1	NA
Nuance Recognizer	MRCP V1	MRCP V2/TCP, and MRCP V2/TLS
Nuance OpenSpeech Recognizer (OSR)	MRCP V1	NA
Loquendo	MRCP V1	MRCP V2/TCP **Note:** MRCP V2/TLS is not supported.

SRGS support

Speech Server	SRGS support	SRGS format support with SISR tag
IBM WebSphere Voice Server	Yes	NA
Nuance Recognizer	Yes	Yes
Nuance OpenSpeech Recognizer (OSR)	Yes	NA
Loquendo	Yes	Yes

NLSML and EMMA recognition result support

Speech Server	NLSML recognition result support	EMMA recognition result support
IBM WebSphere Voice Server	NA	NA
Nuance Recognizer	Yes	Yes
Nuance OpenSpeech Recognizer (OSR)	NA	NA
Loquendo	Yes	Partially supported

Supported TTS speech servers

Speech Server	Minimum Version Required	Also Required	MRCP V1 and MRCP V2 Support
IBM WebSphere Voice Server	R5.1.3	Fix Pack 3	Only MRCP V1
Nuance RealSpeak	4.5	Nuance Speech Server version 5.0.3	MRCP V1, MRCP V2/TCP, and MRCP V2/TLS
Nuance RealSpeak	4.0.12	Nuance patch for RealSpeak SpeechWorks MediaServer (SWMS) component version 3.1.14 or 3.1.15 **Note:** SWMS version 4.0 is not supported.	Only MRCP V1
Loquendo	7.4.2	Loquendo Speech Suite (LSS) 7.0.4 – for Linux 7.0.13 – for Windows	MRCP V1 and MRCP V2/ TCP **Note:** MRCP V2/TLS is not supported.

Recommended releases for the speech servers

Speech Server	MRCP V1	MRCP V2
IBM	WebSphere Voice Server (WVS) R5.1.3 + Fix Pack 3	Not available
Nuance	ASR: OpenSpeech Recognizer (OSR) 3.0.15 or later TTS: RealSpeak 4.0.12 with Patch 1 SWMS: 3.1.15	Not available
Nuance – Quantum	ASR: Recognizer 9.0.4 or later TTS: RealSpeak 4.5 with SP1 Speech Server (NSS): 5.0.4 or later	ASR: Recognizer 9.0.4 or later TTS: RealSpeak 4.5 with Patch 1 and 2 Speech Server (NSS): 5.0.4 or later
Loquendo	TTS: Engine 7.5.2 and SDK 7.4.0 ASR: Engine 7.6.1 and SDK 7.6.0	TTS: Engine 7.5.2 and SDK 7.4.0 ASR: Engine 7.6.1 and SDK 7.6.0

Speech Server	MRCP V1	MRCP V2
	LSS: 7.0.13 for Windows, 7.0.4 for RH Linux	LSS: 7.0.13 for Windows, 7.0.4 for RH Linux

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. Voice Portal allows you to configure multiple MRCP options for each speech server depending upon which protocols are supported by the speech vendor.

For example, Voice Portal enables you to configure the following MRCP protocols for the Nuance speech server in a Voice 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 Open Speech Recognizer (OSR) to use MRCPV1 and a Nuance Recognizer server to use MRCPv2 w/ TLS, the MPP software uses the Nuance OSR MRCPv1 server for the first call, the Nuance Recognizer MRCPv2 w/ TLS for the second call, and so on.

Important:

- Although VPMS allows you to configure various MRCP options for different types of speech servers, you need to contact your speech server vendor for information on the MRCP options supported by each speech server. For example, Nuance Recognizer server supports all options (MRCPv1, MRCPv2+TCP, and MRCPv2+TLS) but OSR server only supports the MRCPv1 option.
- To configure TLS on any ASR or TTS speech server, you must restart the MPP server to reauthorize the certificates.

ASR servers in Voice Portal

ASR servers in Voice Portal

Automatic Speech Recognition (ASR) technology enables an Interactive Voice Response (IVR) system to collect verbal responses from callers. The IVR system can then recognize, or

interpret, them according to algorithms within the ASR software. Voice Portal integrates with third-party ASR servers to provide this capability in speech applications.

When the Voice Portal Media Processing Platform (MPP) software receives a call, the MPP starts the associated speech application that controls the call flow. If the speech application uses ASR resources, the MPP also starts a session with an ASR server that is configured to use *all* of 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 are configured for any single ASR server, Voice Portal sends a `No ASR Resource` exception to the application. What happens then depends on the event handler that the application uses.

As the call progresses, the MPP directs any requests for speech recognition 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 will not become available again until the call completes.

Viewing existing ASR servers

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **System Configuration** > **Speech Servers**.
3. Click the ASR tab.

   The options displayed on this page depend on your user role.

Adding ASR servers

1. Log in to the VPMS web interface.

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

Otherwise, log in to the VPMS using an account with the Administration user role.

2. From the VPMS main menu, select **System Configuration** > **Speech Servers**.
3. On the ASR tab of the Speech Servers page, click **Add**.
4. On the Add ASR Server page, enter the appropriate information and click **Save**.

   If you logged in using the init account, make sure you enter the appropriate LDN number for the server in the **LDN** field. If you do not specify an LDN number, Voice Portal uses the default value (000)000-0000.

Changing ASR servers

1. Log in to the VPMS web interface.

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

   Otherwise, log in to the VPMS using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **Speech Servers**.
3. On the ASR tab, click that server name in the **Name** column.
4. On the Change ASR Server page, enter the appropriate information and click **Save**.

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

Deleting ASR servers

Prerequisites

Important:

All ASR enabled applications on the Voice Portal system have associated ASR languages. Before you delete a server, look at the **Languages** column and make sure that all the languages 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 need to assign

that language to another ASR server or change any applications that use the old language.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **Speech Servers**.
3. Click the ASR tab on the Speech Servers page.
4. For each ASR server that you want to delete, click the Selection check box to the left of the server name in the table.

   Tip:
   To delete all servers, click the Selection check box in the header row of the table. This automatically selects all rows in the table.
5. Click **Delete**.

   If the server is currently in use, Voice Portal deletes it as soon as it finishes processing any active calls.

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 Voice Portal system, add a new ASR server, or change an existing server, and add or delete different languages and language codes.

Tip:
To sort the servers 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 ASR servers you want to delete.
Name	The unique identifier for this ASR server on the Voice Portal system. To change the parameters for an ASR server, click the name of the server in the table. Voice Portal opens the Change ASR Server page.
Enable	Whether this ASR server is available for use by the Voice Portal system.
Network Address	The network address, or location, of the ASR server.
Engine Type	The type of ASR software engine the server uses.

Column or Button	Description
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 Nuance, IBM, or Loquendo licenses on the TTS server that will be used by the Voice Portal system. Voice Portal uses this information to determine the total number of ASR resources available to the MPPs in the Voice 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.
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 Voice 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 Voice Portal system. This page contains the:

- General Section on page 330
- MRCP Section on page 332
- SRTP Section on page 334
- Configured SRTP List group on page 334

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
Name	The unique identifier for this ASR server on the Voice Portal system.

Field	Description
	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 Voice Portal system. The default is **Yes**, which means the server is available.
Engine Type	The type of ASR software engine the server uses. The options are: • **IBM WVS** • **Loquendo** • **Nuance** The selection of an engine type in this field affects what the VPMS 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.
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 VPMS 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 IBM WebSphere, the default is port 554 • 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 IBM, Loquendo, or Nuance licenses on the TTS server that will be used by the Voice Portal system. Voice Portal uses this information to determine the total number of ASR resources available to the MPPs in the Voice Portal system.

Field	Description
New Connection per Session	Whether Voice Portal opens a new connection for each call session. If you are using: • IBM WVS, the default is **Yes** • Loquendo, the default is **No** • Nuance, the default is **No** **Important:** Avaya strongly recommends that you 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. This list is prepopulated with the list of the languages that were available for the designated ASR engine type when Voice Portal was released. It is maintained in a special file on the Voice 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 VPMS 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, Voice Portal sends a `No ASR Resource` exception to the application. What happens then depends on the event handler that the application uses.
Listed Directory Number (LDN)	This field is only shown when you are logged into the VPMS using the Avaya Services init account created when the Avaya Service accounts were configured. If you are logged into the VPMS 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, Voice 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. Voice 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 Voice Portal system waits between heartbeat messages. Enter an integer in this field. The default is 15.

Field	Description
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** The default is MRCP V1. **Note:** MRCPv2 option is shown only when you select Nuance or Loquendo in the **Engine Type** field.
RTSP URL	The URL of the Real-Time Streaming Protocol (RTSP) server. The RTSP server is the network remote control for the Voice 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, Voice Portal will overwrite your changes when you enter a new network address or change the engine type.
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 the TLS certificate is installed on the VPMS server. From the VPMS main menu, select **Security > Certificates >**

Field	Description
	Trusted Certificates to view any currently installed certificates if one is available, or to install a new certificate. • Select **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.
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.

This page contains the:

- General Section on page 335
- MRCP Section on page 337
- SRTP Section on page 339
- Configured SRTP List group on page 340

General Section

Field	Description
Name	The unique identifier for this ASR server on the Voice 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 Voice Portal system. The default is **Yes**, which means the server is available.
Engine Type	The type of ASR software engine the server uses. The options are: • **IBM WVS** • **Loquendo** • **Nuance** The selection of an engine type in this field affects what the VPMS displays as the defaults in the **Base Port**, **New Connection per Session**, **Languages** and **RTSP URL** fields.

Field	Description
	Note: Once you save the ASR server, this type cannot be changed.
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 VPMS 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 IBM WebSphere, the default is port 554 • 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 Nuance, IBM, or Loquendo licenses on the TTS server that will be used by the Voice Portal system. Voice Portal uses this information to determine the total number of ASR resources available to the MPPs in the Voice Portal system.
New Connection per Session	Whether Voice Portal opens a new connection for each call session. If you are using: • IBM WVS, the default is **Yes** • Loquendo, the default is **No** • Nuance, the default is **No** **Important:** Avaya strongly recommends that you 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. This list is prepopulated with the list of the languages that were available for the designated ASR engine type when Voice Portal was released. It is

Field	Description
	maintained in a special file on the Voice 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 VPMS 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, Voice Portal sends a `No ASR Resource` exception to the application. What happens then depends on the event handler that the application uses.
Listed Directory Number (LDN)	This field is only shown when you are logged into the VPMS using the Avaya Services init account created when the Avaya Service accounts were configured. If you are logged into the VPMS 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, Voice 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. Voice 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 Voice 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** The default is MRCP V1.

Field	Description
	Note: MRCPv2 option is shown only when you select Nuance or Loquendo in the **Engine Type** field.
RTSP URL	The URL of the Real-Time Streaming Protocol (RTSP) server. The RTSP server is the network remote control for the Voice 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, Voice Portal will overwrite your changes when you enter a new network address or change the engine type.
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 the TLS certificate is installed on the VPMS server. From the VPMS main menu, select **Security > Certificates > Speech Server Certificates** to view any currently installed certificates if one

Field	Description
	is available, or to install a new certificate. • Select **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.
RTP Authentication Enabled	The options are:

Field	Description
	• **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 Voice Portal

TTS servers in Voice Portal

Text-to-Speech (TTS) technology makes it possible for an Interactive Voice Response (IVR) system to render text content into synthesized speech output, according to algorithms within the TTS software. Voice Portal integrates with third-party TTS servers to provide this capability in speech applications.

When the Voice Portal Media Processing Platform (MPP) software receives a call, the MPP starts the associated speech application that controls the call flow. If the speech application uses TTS resources, the MPP also starts a session with a TTS server that is configured to use *all* of the language/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, Voice

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, the 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 while a call is using TTS resources. As soon as the call stops using TTS resources, the license becomes available to other calls.

Viewing existing TTS servers

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **System Configuration** > **Speech Servers**.
3. Click the TTS tab.

   The options displayed on this page depend on your user role.

Adding TTS servers

1. Log in to the VPMS web interface.

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

   Otherwise, log in to the VPMS using an account with the Administration user role.
2. From the VPMS 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, make sure you enter the appropriate LDN number for the server in the **LDN** field. If you do not specify an LDN number, Voice Portal uses the default value (000)000-0000.

Changing TTS servers

1. Log in to the VPMS web interface.

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

   Otherwise, log in to the VPMS using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **Speech Servers**.
3. On the TTS tab on the Speech Servers page, click that server name in the **Name** column.
4. On the Change TTS Server page, enter the appropriate information and click **Save**.

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

Deleting TTS servers

Prerequisites

Important:
All TTS enabled applications on the Voice Portal system have associated TTS languages/ voices. Before you delete a server, look at the **Voices** column and make sure that all the languages/ voices 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/voice, you need to assign that language/voice to another TTS server or change any applications that use the old language/voice.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **Speech Servers**.
3. Go to the TTS tab on the Speech Servers page.
4. For each TTS server that you want to delete, click the Selection check box to the left of the server name in the table.

Tip:

To delete all servers, click the Selection check box in the header row of the table. This automatically selects all rows in the table.

5. Click **Delete**.
   If the server is currently in use, Voice Portal deletes it as soon as it finishes processing any active calls.

Custom RealSpeak TTS dictionaries

Adding custom dictionaries for Nuance RealSpeak

If desired, any application that uses the Nuance RealSpeak server can use a custom dictionary. You can create as many custom dictionaries as you need, but each application can only use one of those dictionaries.

1. Create the custom dictionaries, as described in the Nuance RealSpeak documentation. For ease of maintenance, Avaya recommends that you use the text-based dictionary type (DCT or TDC files) rather than the binary dictionary (BDC or DCB files), but you can use either type with Voice Portal.
2. If the user dictionary will be accessed from the application server through HTTP, you need to map the dictionary extensions you are using to the appropriate MIME type:
   a. On each Nuance RealSpeak HTTP server, open the `mime.types` file.
      The default file location on Linux is in the `/etc/` directory and the default location on Windows is in the `C:\Program Files\Apache Group\Apache\conf` directory.
   b. Add the following lines to this file to associate text and binary dictionaries with the proper file extensions:
      ```
      application/edct-text-dictionary dct tdc
      application/edct-bin-dictionary dcb bdc
      ```
   c. Save and close the file.
   d. Upload the custom dictionaries as described in the Nuance RealSpeak documentation.

Next steps

Associate the dictionary with the application.

Related topics:

[Associating a custom dictionary with an application through Voice Portal](#) on page 344
[Associating a custom dictionary with an application using the lexicon tag](#) on page 344

Associating a custom dictionary with an application through Voice Portal

1. Follow the steps described in [Adding a speech application to Voice Portal](#) on page 230 or [Changing speech application settings through Voice Portal](#) on page 231.
2. When you get to the **TTS** section in the **Speech Parameters** group, go to the **TTS** field and:
   - If your RealSpeak server is on Linux, add the `ssftrs_dict_enable=file:///opt/ttsdict/<dictionary name>.<extension>` parameter.
   - If your RealSpeak server is on Windows, add the `ssftrs_dict_enable=file://<drive>/<full path>/<dictionary name>.<extension>` parameter.
3. When you are finished adding or changing your application, click **Save**.

Example

On Windows, if your dictionary was stored in a file called `C:/custom/ttsdict/my_dictionary.dct`, you would specify `ssftrs_dict_enable=file://C:/custom/ttsdict/my_dictionary.dct`.

Associating a custom dictionary with an application using the lexicon tag

Avaya Dialog 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.

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 RealSpeak

The following shows a sample text-base dictionary for US English:

```
[Header]
Language = ENU
[SubHeader]
Content=EDCT_CONTENT_ORTHOGRAPHIC
Representation=EDCT_REPR_WSZ_STRING
[Data]
DLL     Dynamic Link Library
Inc     Incorporated
Info    Information
Tel     Telephone
[SubHeader]
Content = EDCT_CONTENT_BROAD_NARROWS
Representation = EDCT_REPR_SZZ_STRING
[Data]
addr    // '@.dR+Es
avaya   // @'va&Ij$.
```

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#

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#

Phonetic Symbols	Orthographic Example	Phonetic Example
m	(m)an	#'m@n#
n	(n)ut	#'n^t#
nK	ri(ng)	#'R+lnK#
.	syllable break	
	'primary stress	
'2	secondary stress	
\	"sentence accent	
#	silence (pause)	
_	word delimiter	
*.	end of declarative	
*	comma	
*!	end of exclamation	
*?	end of question	
*;	semicolon	
*:	colon	

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 Voice Portal system, add a new TTS server, or change an existing server, and add or delete different voices and voice codes.

Tip:

To sort the servers 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 servers you want to delete.
Name	The unique identifier for this TTS server on the Voice Portal system. To change the parameters for a TTS server, click the name of the server in the table. Voice Portal opens the Change TTS Server page.
Enable	Whether this TTS server is available for use by the Voice Portal system.

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.
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 Nuance, IBM, or Loquendo licenses on the TTS server that will be used by the Voice Portal system. Voice Portal uses this information to determine the total number of TTS resources available to the MPPs in the 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.
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 Voice 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 toVoice Portal system.

This page contains the:

- General Section on page 349
- MRCP Section on page 350
- SRTP Section on page 352
- Configured SRTP List group on page 353

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
Name	The unique identifier for this TTS server on the Voice 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 Voice 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: • **IBM WVS** • **Loquendo** • **Nuance** The selection of an engine type in this field affects what the VPMS 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.
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 VPMS 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 IBM WebSphere, the default is port 554 • 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	The total number of Nuance, IBM, or Loquendo licenses on the TTS server that will be used by the Voice Portal system.

Field	Description
Licensed TTS Resources	Voice Portal uses this information to determine the total number of TTS resources available to the MPPs in the system.
New Connection per Session	Whether Voice Portal establishes a new connection on the TTS server for each call session. If you are using: • IBM WVS, set this to **Yes** • Loquendo, set this to **No** • Nuance, set this to **No**
Voices	Displays all the voices that TTS servers can use on this system. The selected voices are the ones that this TTS server is configured to use. Select an individual entry in this list by clicking on it, or use `Ctrl+Click` and `Shift+Click` to select multiple entries. This list is prepopulated with the list of the voices that were available for the designated TTS engine type when Voice Portal was released. It is maintained in a special file on the Voice 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 VPMS 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, Voice Portal sends a `No TTS Resource` exception to the application. What happens then depends on the event handler that the application uses.
Listed Directory Number (LDN)	This field is only shown when you are logged into the VPMS using the Avaya Services init account created when the Avaya Service accounts were configured. If you are logged into the VPMS 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, Voice 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. Voice 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 Voice Portal system waits between the heartbeat messages.

Field	Description
	Enter an integer in this field. The default is 15.
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** The default is MRCP V1. **Note:** MRCPv2 option is shown only when you select Nuance or Loquendo in the **Engine Type** field.
RTSP URL	The URL of the Real-Time Streaming Protocol (RTSP) server. The RTSP server is the network remote control for the Voice 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.
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 the TLS certificate is installed on the VPMS server. From the VPMS main menu, select **Security > Certificates >Trusted Certificates** to view any currently installed certificates if one is available, or to install a new certificate. • Select **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

Field	Description
	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.

This page contains the:

General Section

Field	Description
Name	The unique identifier for this TTS server on the Voice 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 Voice 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: • **IBM WVS** • **Loquendo** • **Nuance**

Field	Description
	The selection of an engine type in this field affects what the VPMS 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.
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 VPMS 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 IBM WebSphere, the default is port 554 • 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 Nuance, IBM, or Loquendo licenses on the TTS server that will be used by the Voice Portal system. Voice Portal uses this information to determine the total number of TTS resources available to the MPPs in the system.
New Connection per Session	Whether Voice Portal establishes a new connection on the TTS server for each call session. If you are using: • IBM WVS, set this to **Yes** • Loquendo, set this to **No** • Nuance, set this to **No** **Important:** Avaya strongly recommends that you use the above settings for this parameter.
Voices	Displays all the voices that TTS servers can use on this system. The selected voices are the ones that this TTS server is configured to use.

Field	Description
	Select an individual entry in this list by clicking on it, or use `Ctrl+Click` and `Shift+Click` to select multiple entries. This list is prepopulated with the list of the voices that were available for the designated TTS engine type when Voice Portal was released. It is maintained in a special file on the Voice 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 VPMS 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, Voice Portal sends a `No TTS Resource` exception to the application. What happens then depends on the event handler that the application uses.
Listed Directory Number (LDN)	This field is only shown when you are logged into the VPMS using the Avaya Services init account created when the Avaya Service accounts were configured. If you are logged into the VPMS 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, Voice 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, Voice 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 Voice Portal system waits between the heartbeat messages. Enter an integer in this field. The default is 15.
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).

Field	Description
	The options are: • **MRCP V1** • **MRCP V2** The default is MRCP V1. **Note:** MRCPv2 option is shown only when you select Nuance or Loquendo in the **Engine Type** field.
RTSP URL	The URL of the Real-Time Streaming Protocol (RTSP) server. The RTSP server is the network remote control for the Voice 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.
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 the TLS certificate is installed on the VPMS server. From the VPMS main menu, select **Security > Certificates > Speech Server Certificates** to view any currently installed certificates if one is available, or to install a new certificate. • Select **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 –

Field	Description
	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.
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 9: Application Server Manager

Application Server Manager in Voice Portal

The Application Server web page in the Voice Portal Management System (VPMS) allows you to start and stop the application server co-resident with the primary VPMS.

You can also use this page to navigate to the Tomcat Manager web interface which allows users to deploy, undeploy, start and stop applications on the application server.

To access the Tomcat Manager web interface from VPMS, you need a Tomcat user name which is created during the Tomcat application installation.

Important:

The Application Server page is displayed only when Voice Portal is installed on a single server and has a Tomcat application server installed on it. For details, see the Optional: Installing a Tomcat application server topic in the *Implementing Voice Portal on a single server* guide.

Application Server page field descriptions

Use this page to start and stop the application server co-resident with the primary Voice Portal Management System (VPMS). You can also use this page to navigate to the Tomcat Manager web page which allows users to deploy, undeploy, start and stop applications on the application server.

Important:

The Application Server page is displayed only when Voice Portal is installed on a single server and has a Tomcat application server installed on it. For details, see the *Optional: Installing a Tomcat application server* topic in the *Implementing Voice Portal on a single server* guide.

This page contains the:

Application Server table

Field	Description
Selection check box	Indicates the application servers in the Voice 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. Voice Portal displays the Tomcat Manager web page in a separate window. **Note:** The link to the Tomcat Manager web page is enabled only when the application server state is **Running**.
State	The operational state of the application server.

State Commands group

Note:
These buttons are greyed out until 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

1. From the VPMS main menu, select **System Management** > **Application Server**.
2. Click the Selection check box next to the application server you want to start.

3. Click **Start** in the **State Commands** group 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 Voice Portal

The Voice Portal Management System (VPMS) web interface allows you to navigate to the *Tomcat Web Application Manager* page which allows users to deploy, remove, start and stop applications on the application server.

The login account for accessing the Tomcat Manager web interface is different from your VPMS user name. For more information see

1. Log into the VPMS web interface.
2. From the VPMS main menu, select **System Management** > **Application Server**.
3. Click the host address of the server.
   Opens a new browser window and displays the login dialog box for the Tomcat Manager web interface.
4. On the **Tomcat Manager** login page, enter your Tomcat user name in the **User Name** field.

   The user name must match an existing Tomcat account name exactly, including case.
5. In the **Password** field, enter your login password.

   The password must match the password assigned to the specified user name exactly, including case.
6. Click **OK**.
   If your user name and password:
   - Match an authorized Tomcat user account, the Tomcat Web Application Manager page is displayed in a new browser window.
   - Do not match an authorized Tomcat user account, the login dialog box is displayed again.

Chapter 10: Managed Applications in Voice Portal

Managed applications in Voice Portal overview

Managed applications are special classes of applications which derive the licensing, administration framework, manageability and accessibility from the Voice Portal management system (VPMS).

Voice Portal is the single point of management for managed applications.

For example, Avaya Proactive Outreach Manager is a managed application which runs on Voice Portal. Avaya Proactive Outreach Manager uses the Voice 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.

Voice Portal provides the following capabilities for managed applications:

- Acquire and maintain licenses on page 364
- Add managed application to VPMS on page 364
- Role-based access on page 365
- Multi-tenancy on page 365
- Logging and Alarming on page 366
- Reports related to managed applications on page 366

Managed applications related menus, web pages and associated online help are installed and integrated into the VPMS by the managed application installer.

Acquire and maintain licenses

The managed application installer adds the licensing information to the licensing tables in the Voice Portal database. Voice Portal retrieves this information from the database and acquires the licenses for the managed applications from the license server.

Voice Portal also handles the license expiry and grace period for the managed application licenses. Voice 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. The licensed values allowed during the grace period are specified by the managed application during installation.
- License server is no longer available or accessible from the VPMS.
- Managed application license has expired.

Note:
Voice Portal generates appropriate alarms for these conditions.

Voice Portal generates an alarm, seven days prior to the managed application license expiry.

Once a grace period is initiated, VPMS generates an alarm every day till the issue is resolved or the grace period expires.

Managed applications periodically retrieve the license information from the VPMS 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 managed application are still available in VPMS but they do not function.

You can view and configure the license details of the managed application from the Licensing web page in VPMS.

For more information, see the documentation delivered with the managed application.

Add managed application to VPMS

The managed application installer adds additional pages and fields to the VPMS. 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 VPMS pages, or new pages with new fields.

A managed application may also add an additional application type during installation. This application type will be available in the **VPMS>Add Application** page as an option in the **Type** field.

For more information about the pages and fields related to managed application, see the documentation delivered with the managed application.

Note:
You must log in to the VPMS web interface on the primary VPMS 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 VPMS.

Voice 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 VPMS.

You can create new users and assign them managed application based roles as well as Voice Portal based roles.

For more information on roles and features related to managed application, see the documentation delivered with the managed application.

Note:
The VPMS administrator role can access managed application features when the managed application is installed on Voice Portal.

Multi-tenancy

The multi-tenancy feature in Voice Portal allows the configuration data and reports maintained by the Voice Portal Management System (VPMS) 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 Voice Portal on page 89.

For more information on multi tenancy feature related to managed applications, see the documentation delivered with the managed application.

Logging and Alarming

Voice 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 in the **Audit Log Viewer** VPMS web page along with the VPMS audit log categories and can be used for filtering the audit logs.
- Event log categories. These categories are available in the **Log Viewer** VPMS web page along with the VPMS event log categories and can be used for filtering the event logs.
- Alarm categories. These categories are available in the **Alarm Manager** VPMS web page along with the VPMS 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** VPMS web page.

For more information, see the documentation delivered with the managed application.

Reports related to managed applications

The managed application installer adds additional standard reports to Voice Portal. These additional standard reports are available in the **Standard Reports** VPMS 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 11: Integrated Voice and Video Response

The Integrated Voice and Video Response (IVVR) is an extension to the voice support capabilities of the Voice Portal system. It combines the standard Voice Portal audio processing with video streaming between two endpoints.

IVVR uses the 3G video enabled devices and SIP-based video phones to deliver the multi-modal communication capabilities to the end users. IVVR supports video streaming in addition to static and dynamic menu creation and audio prompting.

You can use following VoiceXML tags when designing a video enabled application:

- `<media>`: This tag enables you to specify 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:

The video 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 applications. You must set the license value to a non-zero number to enable the video server and to zero to disables it.

Tip:

For more information on video settings, licenses, supported codecs and formats, and troubleshooting tips, see the *Avaya Voice Portal 5.1 IVVR White Paper* available in the Print section of the Voice Portal documentation library.For more information on video settings, licenses, supported codecs and formats, and troubleshooting tips, see the Avaya Voice Portal 5.1 IVVR White Paper.

Chapter 12: Voice Portal system events

Viewing Voice Portal system status

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **Real-Time Monitoring** > **System Monitor**.
3. On the System Monitor page, if you want to:
   - View the overall status for all Voice Portal systems in the network, go to the Summary tab.
   - View the status for the VPMS and all MPPs in the local Voice Portal system, go to the <System name> Details tab.
   - View detailed information for an MPP, go to the <System name> Details tab and click the name of the MPP in the **Server Name** column.
   - 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. If desired, check the resources being used by all current applications in the system by selecting **Real-Time Monitoring** > **Active Calls** from the VPMS main menu.

Related topics:

[<System name> Details tab on the System Monitor page field descriptions](#) on page 222
[Summary tab on the System Monitor page field descriptions](#) on page 225

Summary tab on the System Monitor page field descriptions

Use this tab for a consolidated view of the health and status of the Voice Portal system. The information on this page refreshes automatically if you leave the browser window open.

Note:

If the VPMS server needs to be restarted, Voice Portal displays the message "VPMS needs to be restarted." in red text just above the system status table.

Column	Description
System Name	The name of the Voice Portal system, as specified in the **Voice Portal Name** field on the VPMS Settings page. If your installation consists of multiple Voice 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 **VP**. • The name of the another Voice Portal system in the shared external database. The **Type** will always be **Remote VP**. Click the system name to log into the VPMS web interface for the remote system. • **Summary**. The call capacity and active call counts across all Voice Portal systems displayed on this page.
Type	If your installation consists of a single Voice Portal system, the type will always be **VP**. If you hover the mouse over this field, the VPMS displays a tooltip showing whether the associated server is a primary or auxiliary VPMS server. If your installation consists of multiple Voice Portal systems that share a common external database, this column contains: • **VP**: This type indicates that you are currently logged into the VPMS for this system. Any system commands you issue will affect this VPMS and any MPP servers assigned to this system. The <System name> Details tab for this system shows the assigned MPP servers. • **Remote VP**: This type indicates that this is an active Voice Portal system, but it is *not* the system you are currently logged into. To affect the VPMS or MPP servers assigned to a remote system, you must first log into that system by clicking the remote system name in the **System Name** column
State	Displays the operational state of the Voice Portal system. The options are: • **Active**: This Voice Portal system is updating its information in the database on a regular basis. • **Inactive**: A remote Voice Portal system of **TypeRemote VP** is no longer updating information in the shared database. Click the system name to log into the VPMS on that system and troubleshoot the problem locally. • **Stale**: It has been over an hour since this Voice Portal system has updated its summary information in the database. Create an Alarm report to view the error messages generated by the system.

Column	Description
	Note: If you are using an external database, the time difference between your Voice Portal systems is too great. For more information, see the *Time Synchronization between external database and VPMS servers* topic in the *Troubleshooting Voice 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 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. 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	This field displays: • **In**: The number of active incoming calls in the system • **Out**: The number of active outgoing calls in the system
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 **VP**, 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 VP**, 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 VPMS and each MPP in the Voice Portal system named in <*System Name*>. The information on this page refreshes automatically if you leave the browser window open.

Note:
If the VPMS server needs to be restarted, Voice Portal displays the message "VPMS needs to be restarted." in red text just above the system status table.

Column	Description
Server Name	The options are: • The name of the VPMS server. Click this name to view the <VPMS Name> Details page. • The name of an MPP running on the system. Click this name to view the <MPP name> Details page. • *<VPMS Name>/<MPP Name>*, if an MPP resides on the same server as the VPMS. Click this name to view the <MPP name> Details page.
Type	The options are: • **VPMS**: The Voice Portal Management System • **MPP**: A Media Processing Platform • **VP**: This is the overall Voice Portal system summary
Mode	The operational mode of the MPP. 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 VPMS 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.

Column	Description
	The options are: • **Booting**: The MPP is in the process of restarting and is not yet ready to take new calls. • **Degraded**: The MPP is running but it is not functioning at full capacity. • **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. • **Halting**:The MPP is responding to heartbeats but is not taking new calls. • **Never Used**:The MPP has never successfully responded to a heartbeat request. • **Not Responding**:The MPP is not responding to heartbeat requests and it has not received a **`Restart`** or **`Halt`** command. • **Rebooting**:The MPP is responding to heartbeats but is not taking new calls. • **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 VPMS 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. • **Stopping**:The MPP is responding to heartbeats but is not taking new calls. **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 configuration state of the MPP.

Column	Description
	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.
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.
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.
Calls Today	The number of calls handled during the current day.
Alarms	The alarm status indicators for the VPMS, each MPP, and the overall Voice 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.

Events and alarms

Events and alarms

The Voice Portal Management System (VPMS) or Media Processing Platform (MPP) software generates an *event* when it encounters a:

- Minor problem
- Change to the system
- Change to system resources

If a specific event is repeated several times in succession, or if the VPMS 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
- Are assigned a severity so that you can quickly find the critical issues

In addition, alarms have a status that you can change to indicated that the issue described in the alarm message has been dealt with.

You cannot control the events and alarms generated by the VPMS or an MPP, but you can control:

- When Voice Portal notifies you about high CPU, RAM, and disk space usage
- How long the system stores event and retired alarm records

Related topics:

Event and alarm categories on page 375
Event severities on page 377
Alarm severities on page 378

Event and alarm categories

Every event and alarm falls into one, and only one, of the following categories:

Category	Description
Administration	Messages related to administration activities on the Voice Portal Management System (VPMS).
Application Interface WS	Messages related to the Application Interface web service. This web service runs on the VPMS server and allows customer applications to initiate outbound calls.
Application Logger	Messages related to the Voice Portal application logger. The application logger is a web service running on Voice Portal which allows Dialog Designer applications to log messages to the VPMS.
ASR	Messages related to Automatic Speech Recognition (ASR).
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.
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 VPMS.
Licensing	Messages related to port licensing.
Listener	Messages related to the Alarm Codes Destinations types (Listeners) where the alarm notification is delivered.
Media Manager	Messages related to audio and video Real-time Transport Protocol (RTP) connections.
MMS	Messages related to the MPP Management Service (MMS), which stores configuration information and controls the initialization and operation of an MPP.
MPP Manager	Messages related to the MPP management subsystem, which provides the means to start and stop call processing.
MPP System Manager	Messages related to the MPP System Manager process, which manages and monitors MPP processes, configuration, licensing, and system resources.
MRCP	Messages related to Media Resource Control Protocol (MRCP), which is an open standard for speech interfaces.
Reporting	Messages related to the collection of report data and the generation of reports.
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.
Telephony	Messages related to the H.323 connections and Voice over IP (VoIP) telephony interfaces.
TTS	Messages related to Text-to-Speech (TTS).

Category	Description
Upgrade Manager	Messages related to software upgrades for MPPs running on the VPMS.
VP Backup	Messages related to the VP Backup subsystem, which provides the means to perform on-demand or scheduled backup operation.
VP Management WS	Messages related to the Voice Portal Management web service. This web service runs on the VPMS server and allows you to configure and manage a VPMS.
VP Trace	Messages related to the VP trace reports. It provides the means to collect trace data from VPMS or specific MPP.
Voice Browser	Messages related to the Voice Extensible Markup Language (VoiceXML) browser, which interprets and processes VoiceXML applications. VoiceXML application features synthesized speech, recognition of spoken and DTMF key input, telephony, mixed initiative conversations, and recording and presentation of a variety of media formats including digitized audio, and digitized video.
VP SNMP Trap	Messages related to VP SNMP Traps and SNMP Agent.

Note:

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

Related topics:

Events and alarms on page 375

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.

Related topics:

Events and alarms on page 375

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.

Related topics:

Events and alarms on page 375

Alarm statuses

Status	Description
Unacknowledged	When an event or alarm is issued, Voice Portal sets its status to Unacknowledged to indicate that it is new. Voice Portal does not automatically delete Unacknowledged alarms.
Acknowledged	You can set the event or alarm status to Acknowledged to indicate that you have seen the information but might want to refer back to it at a later point. Voice Portal does not automatically delete Acknowledged alarms.
Retired	You can set the event or alarm status to Retired to indicate that you no longer need to refer to that alarm. Voice Portal automatically deletes Retired alarms from the database depending on the alarm retention periods specified on 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 Voice Portal, you can specify a high water and low water setting for CPU, memory, and disk usage. When a resource exceeds its:

- **High Water** setting for the first time, the system generates an alarm. Voice Portal will 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** 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 VPMS, you can view low water events by generating an event report. Otherwise, you need to look in the System Manager process log, which is accessible from the Log Directories page on the MPP Service Menu.

For information on setting:

- The level of events that are sent to the VPMS, see Setting the resource thresholds for events and alarms on page 379.
- Which events are available in an event report, see Setting the global grace period and trace level parameters on page 166.

Related topics:

Setting the resource thresholds for events and alarms on page 379

Setting the resource thresholds for events and alarms

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **MPP Servers**.
3. On the MPP Servers page, click the **MPP Settings** button.
4. On the MPP Settings page, go to the **Resource Alerting Thresholds** group at the top of the page.
5. In the **CPU**: **High Water** field, 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 has been generated, another alarm will 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.
6. In the **CPU**: **Low Water** field, 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 has been generated, another event will not occur until the CPU percentage rises above the low water setting and then falls below it again. The default is 60.

7. In the **Memory**: **High Water** field, 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.

8. In the **Memory**: **Low Water** field, 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.

9. In the **Disk**: **High Water** field, 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.

10. In the **Disk**: **Low Water** field, 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

The Voice Portal viewer setting parameters determine whether event, Retired alarm, and audit log records are automatically deleted from the database when the specified retention period expires.

Note:
Voice Portal only purges Retired alarms. Unacknowledged and Acknowledged alarms are never automatically removed from the database.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **Alarm/Log Options**.
3. On the Alarm/Log Options page, enter the appropriate information and click **Save**.

Creating an event report

The Event report is affected by some fields on the Alarm/Log Options page.

- The**Logs** group fields determine whether old events are automatically deleted from the database, and, if so, how long those 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 Voice Portal displays the report, because it sets how many pages Voice Portal generates before it displays the first page.

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **System Maintenance** > **Log Viewer**.
3. On the Log Viewer page, enter the filter criteria that you want to use and click **OK**.
   The VPMS displays the Log Report page. Because generating this report can take a long time if the Voice Portal database contains a large number of event records, the Log Report only displays the first 10,000 entries that match the specified criteria.

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

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 it is set to 7, you can only check for the previous week.

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **System Maintenance** > **Alarm Manager**.
3. On the Alarm Manager page, enter the filter criteria that you want to use and click **OK**.

The VPMS displays the Alarm Report page.

4. To view the associated event details for an alarm, click the link in the **Event Code** column.
   The VPMS displays the Log Report for Event page.

Viewing alarms by alarm category

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **Real-Time Monitoring** > **System Monitor**.
3. Go to the <System name> Details tab on the System Monitor page.
   The **Alarms** column displays one of the following alarm status indicators for the VPMS, each MPP, and the overall Voice 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
4. To view the alarms in each alarm category for a particular server or the overall Voice Portal system, click any red or yellow alarm indicator at the end of the appropriate row.
5. On the Alarm Monitor page, to view an alarm report for a given category, click any red or yellow alarm indicator in the **Status** column.
   The VPMS 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 VPMS displays the Log Report for Event page.

Changing the status of an alarm

1. Log in to the VPMS web interface using an account with the Administration or Operations user role.
2. From the VPMS main menu, select **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, if you want to change the status of specific alarms, select them using the check boxes at the beginning of the appropriate alarm rows.
5. In the **Change Alarm Status** group at the bottom of the page, select:
   - **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. Select the status you want to assign to the alarms from the **New Status** drop-down list. You can select:
   - **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

1. Log in to the VPMS web interface using an account with the Administration or Operations user role.
2. From the VPMS main menu, select **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, click **ACK** or **RETIRED** in the **Alarm Status** column. The VPMS 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
Server Names	The name of the system for which you want to view alarms. The options are: • **All systems** • The VPMS • 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 systems**.
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**

Field	Description
	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: • In the beginning of the **Start Date/Time** field, enter the start date using the format `dd-mmm-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 VPMS. For example, you could enter `03-Mar-2007 16:26:10`.

Button	Description
	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 `dd-mmm-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 VPMS. For example, you could enter `10-Mar-2007 16:26:10`. The default for this field is the day prior to the current date at time 23:59:59.

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 it 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 375.
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.

Administration	Messages related to administration activities on the Voice Portal Management System (VPMS).

Application Interface WS	Messages related to the Application Interface web service. This web service runs on the VPMS server and allows customer applications to initiate outbound calls.

Application Logger	Messages related to the Voice Portal application logger. The application logger is a web service running on Voice Portal which allows Dialog Designer applications to log messages to the VPMS.

ASR	Messages related to Automatic Speech Recognition (ASR).
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.
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 VPMS.
Licensing	Messages related to port licensing.
Listener	Messages related to the Alarm Codes Destinations types (Listeners) where the alarm notification is delivered.
Media Manager	Messages related to audio and video Real-time Transport Protocol (RTP) connections.
MMS	Messages related to the MPP Management Service (MMS), which stores configuration information and controls the initialization and operation of an MPP.
MPP Manager	Messages related to the MPP management subsystem, which provides the means to start and stop call processing.
MPP System Manager	Messages related to the MPP System Manager process, which manages and monitors MPP processes, configuration, licensing, and system resources.
MRCP	Messages related to Media Resource Control Protocol (MRCP), which is an open standard for speech interfaces.
Reporting	Messages related to the collection of report data and the generation of reports.
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.
Telephony	Messages related to the H.323 connections and Voice over IP (VoIP) telephony interfaces.
TTS	Messages related to Text-to-Speech (TTS).
Upgrade Manager	Messages related to software upgrades for MPPs running on the VPMS.
VP Backup	Messages related to the VP Backup subsystem, which provides the means to perform on-demand or scheduled backup operation.

VP Management WS	Messages related to the Voice Portal Management web service. This web service runs on the VPMS server and allows you to configure and manage a VPMS.
VP Trace	Messages related to the VP trace reports. It provides the means to collect trace data from VPMS or specific MPP.

Note:

Additional categories may be available if you have installed managed application on Voice 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 388
- Change Alarm Status group on page 389

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.
Server Name	The options are: • The name of the primary or auxiliary VPMS server • The name of the MPP that generated the event
Category	Indicates which Voice Portal component generated the alarm.

Field	Description
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. Voice 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 VPMS interface. Using the trace viewer, you can generate trace reports for the traces that are retrieved from MPPs or the primary VPMS, more effectively and securely. With similar interface as the log viewer and alarm manager for filtering and reports, trace viewer provides better debugging capabilities on the Voice Portal system.

Trace Viewer feature has the following enhancements:

- Separate tab to configure the filters and retrieve trace records for MPP traces.
- Separate tab to configure the filters and retrieve trace records for VPMS traces.
- Ready to use details of trace information of specific components or processes that occurred in a selected MPP or VPMS 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 the Trace Viewer feature by clicking **Trace viewer** link under the **System Maintenance** on the left pane.

Important:

You must have the same version of VPMS and MPP installed to use the trace viewer feature.

If any of the incompatible MPPs are connected to VPMS, 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.

VPMS Traces tab on Trace Viewer page field descriptions

Use this page to configure the filters and retrieve trace records for primary VPMS traces.

This page contains the:

- General section on page 390
- Date and Time section on page 392

General section

Field	Description
Server Names	The primary VPMS.
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”.

Field	Description
	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: • **Application Interface WS** • **Application Logger** • **Listener** • **SNMP Agent** • **SUM Upgrade WS** • **VP Backup** • **VP Management WS** • **VPMS** The default is **Application Interface WS**. For details about the components, see Event and alarm categories on page 375.
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 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 it 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: • In the beginning of the **Start Date/Time** field, enter the start date using the format `dd-mmm-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 VPMS. For example, you could enter `03-Mar-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 `dd-mmm-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 VPMS. For example, you could enter `10-Mar-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	Indicates which Voice Portal component generated the log record.
Trace Level	Indicates 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 the detailed trace information of system server on the Voice Portal system.

VPMS Trace Report page field descriptions

Use this page to view, print, or export the formatted trace reports for the traces that are retrieved from the primary VPMS, 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 VPMS from which the traces are retrieved.
Category	Indicates which Voice Portal component generated the log record.
Trace Level	Indicates 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 the detailed trace information of system server on the Voice Portal system.

Log Report page field descriptions

Use this page to view, print, or export a log report, or to view exception information for an event.

Field	Description
Timestamp	The date and time that the event message was generated.

Field	Description
Server Name	The options are: • **VPMS**. • The name of the MPP that generated the event. If you are logged in as an authorized user, you can open the MPP Service Menu home page by clicking on the MPP system name in this column. **Note:** If you sort the report by this field, the VPMS actually sorts by the name of the server in the Voice Portal database, not the name displayed in this field. Therefore the sort results may be different than what you expect.
Category	Indicates which Voice Portal component generated the event. For more information, see Event and alarm categories on page 375.
Event Severity	Indicates how severe the problems surrounding the event were. For more information, see Event severities on page 377.
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 exception information is available for the event, a link labeled **More** appears in this column that you can click to display the exception information.

Log Viewer page field descriptions

Use this page to create an event report.

This page contains the:

- General information section on page 394
- Date and Time group on page 395
- Categories and Severities group on page 396

General information section

Field	Description
Server Names	Select the name of the system for which you want to view events. The options are: • **All systems** • The VPMS

Field	Description
	• 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 systems**.
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**
Last	Limits the report to a given number of days or hours.

Button	Description
	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: • In the beginning of the **Start Date/Time** field, enter the start date using the format `dd-mmm-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 VPMS. For example, you could enter `03-Mar-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 `dd-mmm-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 VPMS. For example, you could enter `10-Mar-2007 16:26:10`. The default for this field is the day prior to the current date at time 23:59:59.

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 it 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 375.
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.

MPP Servers page field descriptions

Use this page to view, add, change, and delete the Media Processing Platform (MPP) servers currently administered on the Voice Portal system.

Tip:

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

Field	Description
Selection check box	Indicates which MPP servers you want to delete.
Name	The unique identifier for the MPP server on the Voice Portal system.
Host Address	The network address, or location, of the computer on which the MPP server resides. The VPMS uses this address to communicate with the MPP server.
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.

Field	Description
	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 Voice 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.
Event Handlers	Opens the Event Handlers page so you can change the global event handlers and prompts 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 Voice Portal system.

This page contains the:

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 50. • **Low Water**: Enter a whole number from 0 to 100. The default is 40.
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.

Field	Description
	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 ($AVAYA_MPP_HOME/logs/process/MediaMgr/EndPointMgr): 2x • Media Manager ($AVAYA_MPP_HOME/logs/process/MediaMgr/MediaManager): 2x • Session Manager ($AVAYA_MPP_HOME/logs/process/SessMgr/*): 2x
Number of Logs to Retain	The maximum number of log files the system can retain, including the current one. Once this number of log files exists, the system deletes the oldest log file before starting a new one. Enter a whole number from 1 to 5. The default is 2. **Note:** Due to the volume of trace messages from the following components, the number of log files retained by the system are set higher than the number you specify in this field. The actual size is as follows: • Endpoint Manager ($AVAYA_MPP_HOME/logs/process/MediaMgr/EndPointMgr): 2x • 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.
Maximum Transcriptions per Day	The maximum number of transcriptions that the MPP should record in any given day. The default is 6000.

Record Handling on MPP group

Field	Description
Session Data	Whether an MPP keeps detailed records about the sessions that it handles. Voice 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 0 to 999. The default is 14.
Call Data Record	Whether an MPP keeps detailed records about the calls that it handles. Voice Portal uses this data to create the Call Detail report andCall 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 0 to 999. The default is 14.
Application	Whether an MPP keeps the CCXML and VoiceXML Log tag data from the application sessions transacted on that server. If desired, Voice 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 0 to 999. The default is 14.

Miscellaneous group

Field	Description
License Re-allocation Wait Time	The number of minutes the system waits before reallocating the licenses from an MPP that is out of service to other MPPs in the system. Enter a whole number from 0 to 1440. The default is 10.
Operational Grace Period	The number of minutes Voice Portal waits for calls to complete before it terminates any remaining active calls and begins stopping, rebooting, or halting an MPP. Enter a whole number of minutes between 0 and 999 in this field. **Important:** Ensure that the grace period is long enough for the MPP to complete any existing calls before it stops, reboots, or halts.
Event Level Threshold to Send to VPMS	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 VPMS.

Field	Description
	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.
MPP Numeric ID Range	Voice Portal assigns a numeric ID for each MPP in the Voice Portal system from the number range given in this field. This numeric ID identifies the MPP in the Voice Portal database and becomes part of the Universal Call Identifier (UCID) associated with every call processed on that MPP. **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 are creating Universal Call Identifier (UCID) values that conflict with the default Voice Portal values. If you do change the value, make sure that you specify a large enough range to cover all MPP servers in your Voice Portal system.

Categories and Trace Levels section

Performance tracing is a valuable troubleshooting tool, but it can adversely impact Voice Portal system performance if you set all categories to **Finest** on a busy production system. If you need to troubleshoot a particular area, Avaya recommends that you 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**.

Field or Radio Button	Description
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 VPMS. 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**.
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 VPMS 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**.
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.

Field or Radio Button	Description
	The Trace Logger uploads the MPP traces requested by the trace client that runs on VPMS. 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**.
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**.

Field or Radio Button	Description
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**.
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**.

<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 VPMS and each MPP in the Voice Portal system named in <*System Name*>. The information on this page refreshes automatically if you leave the browser window open.

Note:

If the VPMS server needs to be restarted, Voice Portal displays the message "VPMS needs to be restarted." in red text just above the system status table.

Column	Description
Server Name	The options are: • The name of the VPMS server. Click this name to view the <VPMS Name> Details page. • The name of an MPP running on the system. Click this name to view the <MPP name> Details page. • <*VPMS Name*>/<*MPP Name*>, if an MPP resides on the same server as the VPMS. Click this name to view the <MPP name> Details page.
Type	The options are: • **VPMS**: The Voice Portal Management System • **MPP**: A Media Processing Platform • **VP**: This is the overall Voice Portal system summary
Mode	The operational mode of the MPP.

Column	Description
	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 VPMS 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. The options are: • **Booting**: The MPP is in the process of restarting and is not yet ready to take new calls. • **Degraded**: The MPP is running but it is not functioning at full capacity. • **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. • **Halting**:The MPP is responding to heartbeats but is not taking new calls. • **Never Used**:The MPP has never successfully responded to a heartbeat request. • **Not Responding**:The MPP is not responding to heartbeat requests and it has not received a **`Restart`** or **`Halt`** command. • **Rebooting**:The MPP is responding to heartbeats but is not taking new calls. • **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 VPMS 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.

Column	Description
	• **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. • **Stopping**:The MPP is responding to heartbeats but is not taking new calls. **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 configuration state of the MPP. 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.
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.
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.
Calls Today	The number of calls handled during the current day.

Column	Description
Alarms	The alarm status indicators for the VPMS, each MPP, and the overall Voice 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.

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 Voice Portal generates before it displays the first page of the report to the user.

This page contains the:

- Alarms group on page 408
- Logs group on page 409
- Audit Logs group on page 409
- Alarms/Logs/Audit Logs/Traces Report Size group on page 410

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**: Voice Portal deletes Retired alarms once the retention period is exceeded. • **No**: Voice Portal leaves the Retired alarms in the database indefinitely. The default is **Yes**. **Note:** Voice 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**: Voice Portal deletes event log records once the retention period is exceeded. • **No**: Voice 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**: Voice Portal deletes event log records once the retention period is exceeded. • **No**: Voice 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 Voice 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, Voice 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**, Voice 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 410
- Alarm status change table on page 411

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.

Field	Description
Server Name	The options are: • The name of the primary or auxiliary VPMS server • The name of the MPP 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

The Audit Log report shows all action performed by all users logged into the VPMS. It does *not* show any system configuration or backup activities performed by running Voice Portal scripts or making other changes outside the VPMS 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.

1. Log in to the VPMS web interface using an account with the Auditor user role.
2. From the VPMS main menu, select **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 VPMS displays the Audit Log Report page.

Related topics:

Audit Log Viewer page field descriptions on page 412
Audit Log Report page field descriptions on page 415

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
Sort By	The options are: • **Time: newest first** • **Time: oldest first** • **Category**
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.
Category	The options are: • **All Categories** • **Alarm** • **Applications** • **ASR** • **Audit** • **AVB**

Field	Description
	• **CCXML** • **EmailServer** • **H323** • **Licensing** • **Log** • **MPP** • **Organization** • **Prompts** • **Report** • **Role** • **Security** • **SIP** • **SNMP** • **SpeechServer** • **Trace** • **TTS** • **Users** • **Video Settings** • **VoIP** • **VP AppServer** • **VoiceXML** • **VPMS** • **VPSettings** **Note:** Additional categories may be available if you have installed managed application on Voice Portal. For more information on managed application based categories, see the documentation delivered with the managed application.
Action	The options are: • **All Actions** • **Add** • **Change** • **Delete** • **Login**

Field	Description
	• **JNDI Login** • **Logoff** • **Start** • **Stop** • **Restart** • **Sequential Restart** • **Reboot** • **Sequential Reboot** • **Halt** • **Cancel** • **Offline** • **Test** • **Online** • **View** • **Failed Login** • **Backup** • **Upgrade** • **Deploy** • **Undeploy** • **Install** • **Uninstall** • **Change Password**

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.

Button	Description
	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: • In the beginning of the **Start Date/Time** field, enter the start date using the format `dd-mmm-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 VPMS. For example, you could enter `03-Mar-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 `dd-mmm-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 VPMS. For example, you could enter `10-Mar-2007 16:26:10`. The default for this field is the day prior to the current date at time 23:59:59.

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 it 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 log entry was made.
User	The user name that was logged in to the VPMS when the change was made.
Category	The options are: • **Alarm** • **Applications**

Column	Description
	• **ASR** • **Audit** • **AVB** • **CCXML** • **EmailServer** • **H323** • **Licensing** • **Log** • **MPP** • **Organization** • **Prompts** • **Report** • **Role** • **Security** • **SIP** • **SNMP** • **SpeechServer** • **Trace** • **TTS** • **Users** • **Video Settings** • **VoIP** • **VP AppServer** • **VoiceXML** • **VPMS** • **VPSettings** **Note:** Additional categories may be available if you have installed managed application on Voice Portal. For more information on managed application based categories, see the documentation delivered with the managed application.
Action	The options are: • **Add** • **Change**

Column	Description
	• **Delete** • **Login** • **JNDI Login** • **Logoff** • **Start** • **Stop** • **Restart** • **Sequential Restart** • **Reboot** • **Sequential Reboot** • **Halt** • **Cancel** • **Offline** • **Test** • **Online** • **View** • **Failed Login** • **Backup** • **Upgrade** • **Deploy** • **Undeploy** • **Install** • **Uninstall** • **Change Password**
Component	The affected component, if any.
Property	The property that was effected.
From	If applicable, what the value was before the change was made.
To	If applicable, the value after the change was made.

Chapter 13: Reports

Configuring report data settings

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **MPP Servers**.
3. On the MPP Servers page, click **MPP Settings**.
4. On the MPP Settings page, fill in the desired retention period and maximum number of transcriptions per day in the **Transcription** group.
5. In the **Record Handling on MPP** group:
   a. For each type of data you want each MPP to collect, verify that the **Enable** check box next to the field for that data type is selected.
   b. Enter the number of days the data should be kept on the MPP in the associated **Retention Period** field.

   The data types are:

   - **Session Data**: Voice Portal uses this data to create the Session Detail and Session Summary reports.
   - **Call Data Record**: Voice Portal uses this data to create the Call Detail and Call Summary reports.
   - **Application**: If desired, Voice Portal can download the Log tag data and display it in the Application Detail report and Application Summary report.
6. When you have set these options, click **Save**.
7. From the VPMS main menu, select **System Properties** > **Report Data**.
8. On the Report Data Configuration page, enter the appropriate information and click **Save**.
9. To create application reports for any speech applications running on the Voice Portal system, set the reporting options for each application:
   a. From the VPMS main menu, select **System Configuration** > **Applications**.

b. On the Applications page, click on 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 the appropriate information.

d. Click **Save**.

e. Repeat this step for each application for which you want to create reports.

Printing reports

1. To print the report, click the **Print** icon at the top of the report page.
2. As you follow the prompts, make sure that:
   - The page orientation is Landscape and not Portrait, or some columns of the report may not print
   - If you want the printout to contain the same shading in the columns and rows as the online report, the browser option to print background colors is selected

Exporting reports

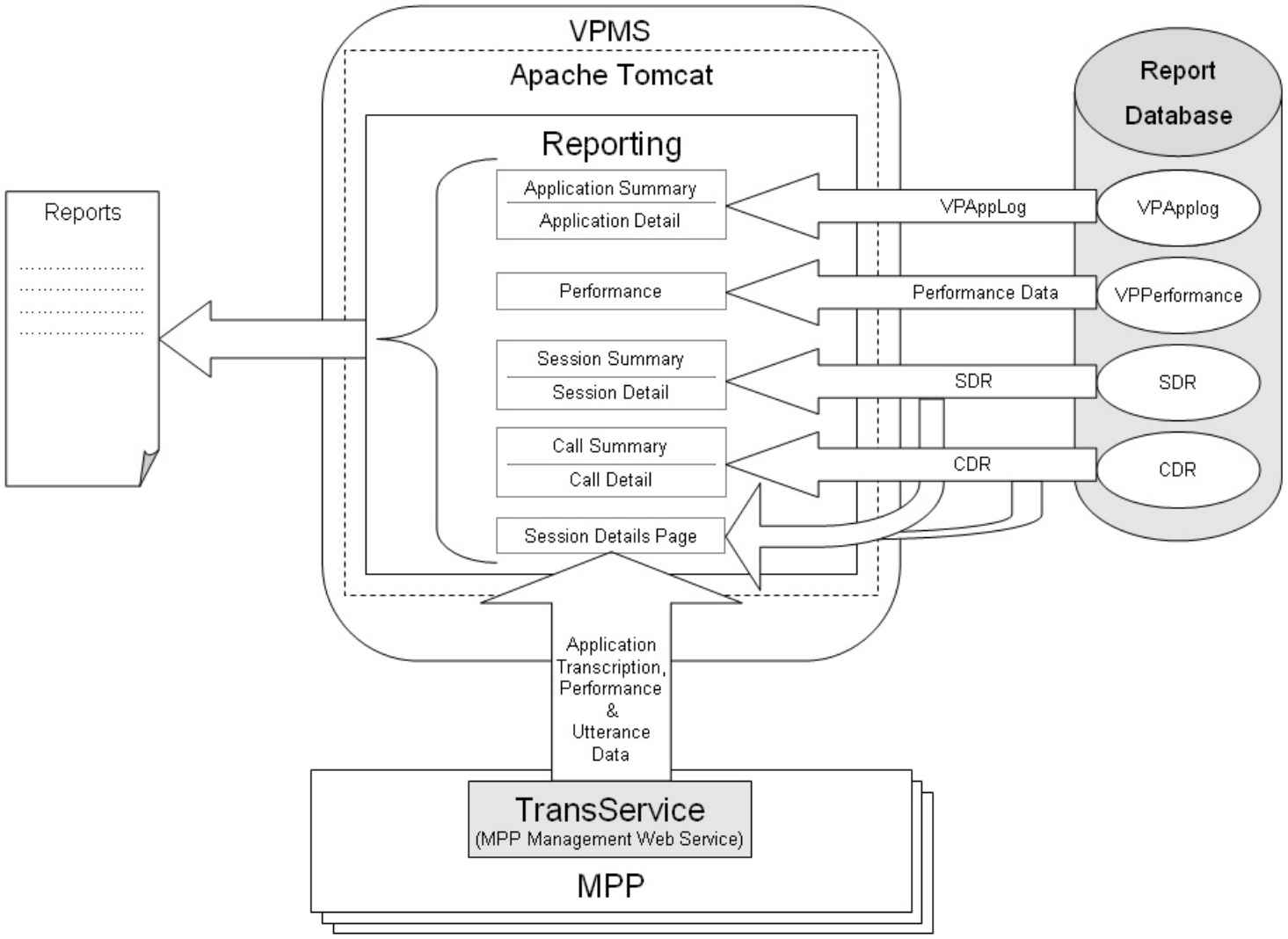
To export the data from the report, click the **Export** icon at the top of the report page, select the export option, and follow the prompts. Voice Portal has two export options:

- Export as XLS format
- Export as PDF format

Voice Portal creates a spreadsheet (XLS) 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 VPMS generates reports.



Application activity reports

The application activity reports show:

- Activity relating to and messages generated by the Dialog Designer applications added to the Voice Portal system
- Voice eXtensible Markup Language (VoiceXML) and Call Control eXtensible Markup Language (CCXML) Log Tag messages from all speech applications added to the Voice Portal system, if the Log Tag messages are stored on, and downloaded from, the MPP

The available activity reports are the Application Summary report and the Application Detail report. The amount of data available for these reports depend on:

- The length of time since the application finished processing. The VPMS downloads Application Detail Records (ADRs) within five minutes after an application finishes. If a particular 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** field 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 it is set to 7, you can only check for the previous week.
- The settings for the report parameters specified for each individual application in the **Reporting Parameters** group on the Change Application page.

Related topics:

Creating an Application Summary report on page 422
Creating an Application Detail report on page 423

Creating an Application Summary report

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **Reports** > **Standard**.
3. On the Standard Reports page, click **Application Summary** link under the **Report Name** column.
4. Optionally, click  next to Application Summary link to generate the report with the default selections of filters.
5. 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.

6. Click **OK**.
   The VPMS displays the Application Summary Report page.

Creating an Application Detail report

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS 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 VPMS 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

Call activity reports

The following reports track call activity in the Voice Portal system:

Call Summary report : Provides summary information about all calls handled by the specified MPPs and applications for the specified time period.

Call 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 **Call 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 it is set to 7, you can only check for the previous week.

Creating a Call Detail report

The Call Detail report provides detailed information about all calls handled by the specified MPPs and applications for the specified time period.

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select .**Reports** > **Standard**.
3. On the Standard Reports page, click **Call Detail** link under the **Report Name** column.
4. Optionally, click  next to **Call Detail** link to generate the report with the default selections of filters.
5. On the Call Detail 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 Call Detail Report page, if you want to:
   - View the messages generated by one of the Dialog Designer applications listed in the table, click the appropriate name in the **Application** column. The VPMS 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 at the end of the appropriate row. The VPMS displays the Session Details page.

Creating a Call Summary report

The Call Summary report provides summary information about all calls based on the specified filtering options.

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **Reports** > **Standard**.
3. On the Standard Reports page, click **Call Summary** link under the **Report Name** column.
4. Optionally, click next to **Call Summary** link to generate the report with the default selections of filters.
5. On the Call 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 VPMS displays the Call Summary Report page.

Creating a Session Detail report

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.

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS 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 with 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 VPMS displays the Session Detail Report page.
7. If you want to view more information about a particular session, click the **View Session Details** icon at the end of the appropriate row.
   Voice Portal displays the Session Details page.

Creating a Session Summary report

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.

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS 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 VPMS displays the Session Summary Report page.

Viewing application transcription data

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS main menu, select **Reports** > **Session Detail**.
3. On the Session Detail page, the **more >>** link to display the rest of the optional filters.
4. Enter any 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. When you are finished, click **OK**.
   The VPMS displays the Session Detail Report page.
6. Locate the particular session for which you want to view the transcription data and click the **View Session Details** icon at the end of the appropriate row.
   Voice Portal displays the Session Details page, which shows the both session and transcription data grouped by information category.
7. If you want to view the transcription information in XML format, click the **Export** link in the **Session Transcription** group.

Creating a Performance report

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 it is set to 7, you can only check for the previous week.

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS 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 VPMS 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 Voice Portal

The Avaya Voice 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 429
- Scheduled Reports on page 429
- Data Export reports on page 429

Custom Reports

With the custom reporting feature you can use any standard Voice 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 e-mail attachment, or access it through the secure links in the e-mail notification, RSS feeds or by logging into the Voice Portal Management System (VPMS). 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 Voice 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 VPMS, that is, the MPPs that are in another Voice 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

1. Log into the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS 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 VPMS 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 Voice Portal system and stored in the PostgreSQL `VoicePortal` database. Most of the data is protected by the system for security reasons, but you can use the database report user account created during VPMS 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 431.
- Call Detail Records (CDRs) stored in the `cdr` table. For more information, see Custom Call Detail report on page 433.
- Session Detail Records (SDRs) stored in the `sdr` table. For more information, see Custom Session Detail report on page 436.

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.

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	Application generated value used to group report or log entries. For example, "Buy Ticket" or "Rent Car".
ApplicationID	VARCHAR	*<Application Name>*:*<Servlet Name>* where entry was logged.

Column	Data Type	Description
AppServerAddress	VARCHAR	Hostname or IP address of the application server where the application was initially invoked.
LogLevel	VARCHAR	Application specified level of log entry "Info", "Warning", "Error", "Fatal".
LogTimestamp	TIMESTAMP	Date and time the log entry was generated in the time zone of the VPMS.
LogType	VARCHAR	Type of log (generated by application). Some possible values are: • Call flow data points, such as `Node Entry`, `Module Exit`, and `Application Exit`. • `Cancel`: Canceling of an activity. • `Cancel All`: Cancel all started activities in session. • `CCXML Log tag`: A message generated a CCXML Log tag in the application. • `End`: End of an activity. • `In Progress`: General log entry. • `Start`: Beginning of an activity. • `VoiceXML Log tag`: A message generated a VoiceXML Log tag in the application.
Message	VARCHAR	Application-defined, free-format text.
ModuleIDNodeID	VARCHAR	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.
SessionID	VARCHAR	Session ID generated by the MPP.
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	A unique identifier set by the application designer.

Column	Data Type	Description
		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	A user-defined Dialog Designer application variable associated with this log entry by the application designer.
VarValue	VARCHAR	Value of variable defined in the column VarName when the log entry was made.
VPID	INTEGER	The ID number of the Voice Portal system that handled the call. If there is only one Voice Portal system at your installation, this field will always be 1.

Custom Call Detail report

You can create a custom Call Detail report using the data stored in the `cdr` table of the PostgreSQL `VoicePortal` database.

Column	Data Type	Description
ApplicationName	VARCHAR	Application name as configured in VPMS.
Areacode	INTEGER	The area code from which calls were received.
AudioCodec	VARCHAR	Audio codec used in the call.
CallID	VARCHAR	Unique call identifier assigned by the MPP.
CallStartDate	INTEGER	Date the call started in YYYYMMDD format.
CallStartTime	INTEGER	Time of day that the call started in 24 hour format (HHMMSS) for GMT timezone.
CallTimestamp	TIMESTAMP	Date and time the call started in GMT time zone.
CallType	INTEGER	Type of call: • 0: Inbound call. • 1: Outbound call.
ConnectLatency	INTEGER	The amount of time before the call was answered, in milliseconds.

Column	Data Type	Description
DestinationNumber	VARCHAR	DNIS - Pilot number of the application.
Duration	INTEGER	Total length of the call, in seconds.
EndDetails	VARCHAR	Extra information as to why the call ended. For example: • SIT: Special Information tone (disconnected number). • Complete: SessionTerminated.
EndType	INTEGER	How the call completed: • 1: 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
FirstPromptLatency	INTEGER	The amount of time after the call connected and before the first prompt was played, in milliseconds.
MPP	VARCHAR	The name of the MPP name that handled this session. This name is configured in the VPMS.
OriginatingNumber	VARCHAR	ANI - The caller's number.
PortID	INTEGER	The switch station for H.323 or the index number on a SIP trunk.
ReasonCode	VARCHAR	Reason code from a transferred call. This can be: • 1: No Resource • 2: Busy • 3: No Answer • 4: Network Busy • 5: No Route • 6: Network Disconnect • 7: Unknown

Column	Data Type	Description
		• 8: Near End Disconnect • 9: Far End Disconnect • 10: Transferred • 11: Internal Error
RecordID	INTEGER	CDR entry count by day.
RedirectedNumber	VARCHAR	The number of the extension that the call is transferred from when calls are transferred to Voice 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.
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	The session ID generated by the MPP that handled the call.
SwitchOrProxy	VARCHAR	Name of the switch or proxy used during the call.
TelIEncryption	VARCHAR	This can be: • The type of telephony encryption used. • N/A if there was no encryption.
TelMediaEncryption	VARCHAR	The media encryption used during the call, if any.

Column	Data Type	Description
TellProtocol	VARCHAR	Telephony protocol use. This can be: • H.323 • SIP • SIPS
UCID	VARCHAR	The Universal Call ID.
VideoCodec	VARCHAR	Video codec used in the call.
VideoFrameRate	INTEGER	Video frame rate used in the call in Frame Per Second (FPS).
VideoBitRate	VARCHAR	Video bit rate used in the call.
VideoScreenSize	VARCHAR	Video screen resolution delivered on the call.
VPID	INTEGER	The ID number of the Voice Portal system that handled the call. If there is only one Voice Portal system at your installation, the value of this field will always be 1.

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.

Column	Data Type	Description
ApplicationName	VARCHAR	Application name as configured in VPMS.
AppServer	VARCHAR	Initial URL as configured in the VPMS that triggered the application.
ASRPercent	INTEGER	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 that page multiplied, as shown in the UttCntWPage column. The formula is: `(UttCntRecWPage/UttCntWPage)*100`
ASRServer	VARCHAR	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.

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 achieved while recognizing utterances.
DialogID	VARCHAR	The unique global identifier given to every dialog belonging to the session.
Duration	INTEGER	The total length of the session, in seconds. **Note:** The duration of a session includes call timeouts and other overhead operations that are not included in any particular call. Therefore, the duration of a session may be greater than the sum of the call durations that took place during that session.
HasPerformanceTrace	INTEGER	This can be: • 0: No performance tracing was done for this call. • 1: A performance trace log is available.
HasTranscription	INTEGER	This can be: • 0: No transcription available. • 1: A call transcription is available.
LatAnswer	INTEGER	Time until first prompt was played.
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.
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	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.

Column	Data Type	Description
		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	The name of the MPP name that handled this session. This name is configured in the VPMS.
MRCPSessionIDASR	VARCHAR	MRCP Session ID for ASR.
MRCPSessionIDTTS	VARCHAR	MRCP Session ID for TTS.
PageReqCacheHits	INTEGER	Number of VoiceXML page cache hits.
PageReqTotal	INTEGER	Number of VoiceXML page requests.
ParentID	VARCHAR	This can be: • root if this is the parent record. • the Session ID of the parent record if this is a child record.
RecordID	INTEGER	SDR entry count by day.
RecordType	INTEGER	This can be: • 0: VXML record • 1: Dialog record • 2: CCXML record
SessionID	VARCHAR	Session ID generated by MPP.
SessionTimestamp	TIMESTAMP	Date and time the session started in GMT time zone.
Slot	INTEGER	MPP slot number that handled the call. This is related to the MPP session log generated.

Column	Data Type	Description
Source	VARCHAR	This can be: • Inbound: The session was initiated by a telephone call coming into the Voice Portal system. • LaunchCCXML: The session was initiated by a CCXML application using the outcall webservice. • LaunchVoiceXML: The session was initiated by a VoiceXML application using the outcall webservice.
StartDate	INTEGER	Date the call started in YYYYMMDD format.
StartPageName	VARCHAR	URL of initial page loaded when call started.
StartTime	INTEGER	Time of day that the call started in 24 hour format (HHMMSS) for GMT timezone.
Switch	VARCHAR	Name of the Switch as configured by the VPMS.
TerminationPageName	VARCHAR	The final VoiceXML page displayed at the end of the call. To view the full URL for this page, use the Session Details page.
TerminationReason	VARCHAR	A value determined by the application. The Dialog Designer application developer determines the value for this database field by setting the exitReason field of the session variable. If the application does not pass a value, this field defaults to `Application exited`.
TerminationInfo1	VARCHAR	Optional information regarding the termination of the session. The Dialog Designer application developer determines the value for this database field by setting the exitInfo1 field of the session variable.
TerminationInfo2	VARCHAR	Optional information regarding the termination of the session. The Dialog Designer application developer determines the value for this database field by setting the exitInfo2 field of the session variable.
TimeTillAnswer	INTEGER	Time until call was answered in milliseconds.
TTSServer	VARCHAR	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.

Column	Data Type	Description
UttCntWPage	INTEGER	Number of utterances received on the page with the worst recognition.
UttWPageName	VARCHAR	URL of the page that had the worst recognition percentages.
VPID	INTEGER	The ID number of the Voice Portal system that handled the call. If there is only one Voice Portal system at your installation, this field will always be 1.

Generating Custom reports using VPMS

Custom Reports using VPMS

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 Voice 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 VPMS

The custom report provides summary information about all the filtering options specified in the source report that you used for generating the report.

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS 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 Voice 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 Voice Portal on page 89.

   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 VPMS displays the report.
10. Optionally, click **Save** to save the filter settings without generating the report.

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 e-mail attachment, or access it through the secure links in the e-mail notification, RSS feeds or by logging into the Voice Portal Management System (VPMS). 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

1. Log in to the VPMS web interface using an account with the Administration, Operations, or Maintenance user role.
2. From the VPMS 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 VPMS displays the scheduled report entry on the Scheduled Reports page.

SQL queries for the VPMS reports

When the VPMS generates a report, it sends one or more SQL queries to the Voice Portal database and displays the result as a VPMS page. This topic shows the:

Note:

For all reports, user-entered dates and times are converted from the local VPMS 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

Call 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;
```

Call 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 14: VPMS main menu customizations

VPMS main menu customizations

Voice Portal offers those users who need additional functionality in the Voice Portal Management System (VPMS) main menu the ability to modify and customize the VPMS main menu by changing the associated configuration files.

The VPMS main menu consists of menu groups and menu items associated with each group.

Examples of the menu groups in the VPMS 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 VPMS main menu.

Related topics:

[Add a new menu group and items](#) on page 448
[Add menu items to an existing menu group](#) on page 456

The VPMS main menu configuration files

Note:
You must define the groups and items in all four `configuration` files before they will display properly in the VPMS 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 VPMS 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 VPMS 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`.

Related topics:

Add a new menu group and items on page 448
Add menu items to an existing menu group on page 456

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 462.	
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 449.	
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 451.	
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 452.	

Step	Task	✔
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 454.	

Related topics:

VPMS main menu customizations on page 447
The VPMS main menu configuration files on page 447

Defining a new menu group and its items

The configuration `menu.xml` file specifies the location of and properties for your new menu group and the menu items.

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 462. 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.

Attributes	Example	Description
`render=[true|false]`, where `render` is either `true` or `false`.	To instruct the VPMS to display the menu group, specify `render=true`	If you set this property to `false`, the VPMS 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 VPMS to display the item in the menu group, specify `render=true`	If you set this property to `false`, the VPMS does not display the menu group.
`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 VPMS 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/`	Determines what page Voice Portal displays when the user selects the menu item. **Important:** Voice Portal does not validate this URL

Attributes	Example	Description
	custom_pages/admin.ops.page.html"	
newWindow="*[true|false]"*, where newWindow is either true or false.	To instruct the VPMS 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, Voice 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

The display menu.properties file specifies the labels that the VPMS displays to the end user.

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 462. 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 Voice Portal displays in the VPMS main menu.
- *`itemDisplayText`* is the item label that Voice Portal displays in the VPMS 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

The `features.xml` file specifies which user roles have access to a menu group and each item in the group.

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 as described in Defining a unique extensions directory on page 462. 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.
`allow="roles"`, where *roles* is a combination of any of the following roles separated by commas: • administration • maintenance • operations • usermanager	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.

Attributes	Example	Description
• auditor		

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

The display `feature.properties` file specifies the labels that the VPMS displays to the end user on the Roles page.

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 462. 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 Voice Portal displays in the VPMS main menu.
   - *`itemDisplayText`* is the item label that Voice Portal displays in the VPMS 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 462.	
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 456.	
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 459.	
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 459.	
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 461.	

Related topics:

VPMS main menu customizations on page 447
The VPMS main menu configuration files on page 447

Defining new menu items under an existing group

The configuration `menu.xml` file specifies the location of and properties for your new menu items.

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 462. 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="existingMenuGroupIdentifier"`	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 VPMS to display the item in the menu group, specify `render=true`	If you set this property to `false`, the VPMS does not display the menu group.

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 VPMS 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 Voice Portal displays when the user selects the menu item. **Important:** Voice Portal does not validate this URL
`newWindow="[true|false]"`, where `newWindow` is either `true` or `false`.	To instruct the VPMS 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`, Voice 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

To specify the labels that Voice Portal will display to the end user, edit the display `menu.properties` file.

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 462. 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 VPMS 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

The `features.xml` file specifies which user roles have access to the new menu items.

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 462. 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

The display `feature.properties` file specifies the labels that the VPMS displays to the end user on the Roles page.

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 462. 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 Voice Portal displays in the VPMS 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

Defining a unique extensions directory allows one to separate the menu and feature customizations from other menu and feature customizations.

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 VPE, 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 15: The Application Logging web service

The Application Logging web service for third-party speech applications

Voice Portal includes an Application Logging web service that lets you save application and breadcrumb information from third-party speech applications into the `VPAppLog` table of the Voice Portal database. Voice 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

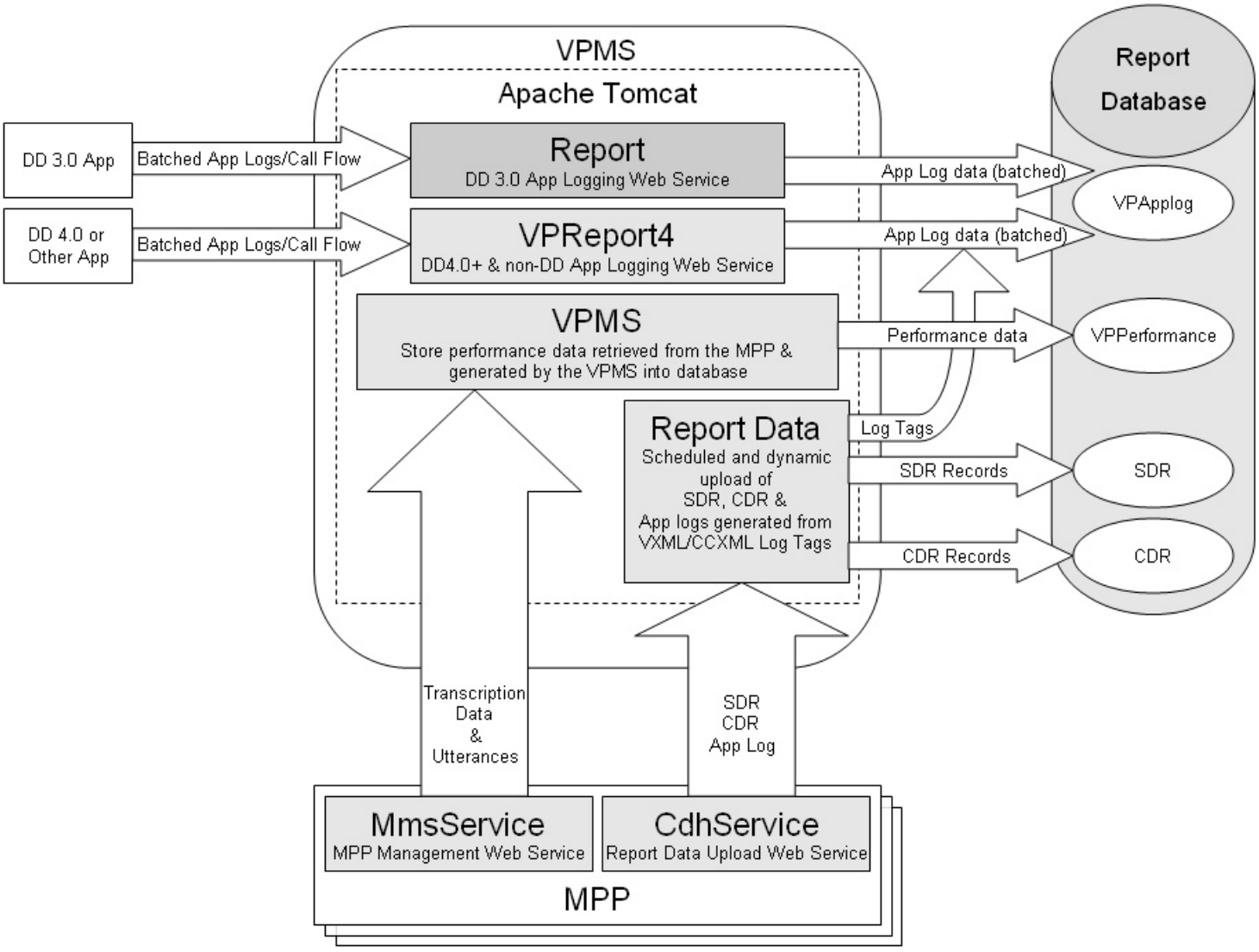
When using the Application Logging web service, keep in mind that:

- The Application Logging web service uses Digest Authentication to authenticate web service client requests. When you submit a request to the web service, you need to specify the user name and password specified in the **Application Reporting** section of the **Web Service Authentication** group on the VPMS Settings page. If you need to change this user name or password, you must do it through the VPMS. For details, see Configuring the Application Logging web service on page 467.
- Avaya strongly recommends that you 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 Voice Portal system performance.
- Avaya strongly recommends that you use the logApplicationEventAlarm web service method with utmost caution. You should implement a throttling mechanism on the client side in order to avoid flooding the VPMS 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 Voice Portal system performance.
- You should save all log entries in case the VPMS is unavailable when the Application Logging web service is called. That way you can resend the log entries when the VPMS becomes available.
- If your Voice Portal VPMS software runs on a dedicated server machine, you should configure a auxiliary VPMS server to handle Application Logging web service requests if the primary VPMS server is unavailable.
- The Voice 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 Custom application activity reports on page 431.

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 Voice Portal database.



Configuring the Application Logging web service

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.

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VPMS Servers**.

3. On the VPMS Servers page, click **VPMS Settings**.
4. On the VPMS 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. Open the following page in a web browser: `http://VPMS-server/axis/services/VPReport4?wsdl`

   Where *VPMS-server* is the domain name or IP address of the system where the primary VPMS software is installed.
8. When prompted, enter the user name and password specified in the **Application Reporting** section of the VPMS 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 469
- reportBatch method for breadcrumb logging on page 471
- logFailed method on page 468
- logApplicationEventAlarm method for application Logging / Alarming on page 473

logFailed method

The Application Logging web service `logFailed` method adds the event `PALOG00017` to the Voice Portal database.

Parameters

Parameter	Type	Description
lastVPMSDown	Long integer	The timestamp of the last time the VPMS 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 breadcrumb log entries in the Voice 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 breadcrumb log entry, see reportBatch method for breadcrumb logging on page 471.

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` • `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.

Parameter	Type	Description
timestamp	string	The timestamp of the log and the format that it is stated in. For example: `2007-04-30 11:23:34:21 yyyy-mm-dd hh:mm:ss.ms`
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 VPID`

If the method fails, you can use the `logFailed` method to enter an event into the Voice Portal event log.

reportBatch method for breadcrumb logging

The `reportBatch` method can be used to create application or breadcrumb log entries in the Voice 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 an breadcrumb log entry. For information about creating an application log entry, see reportBatch method for application logging on page 469.

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	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

Parameter	Type	Description
		allows Voice 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 timestamp of the log and the format that it is stated in. For example: `2007-04-30 11:23:34:21 yyyy-mm-dd hh:mm:ss.ms`
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.
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

Parameter	Type	Description
		`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 Voice 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 VPMS. 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.

Parameter	Type	Description
		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 timestamp of the log and the format that it is stated in. For example: `2007-04-30 11:23:34:21 yyyy-mm-dd hh:mm:ss.ms`
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 VPID`

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 VPMS software. For details about accessing this file, see Configuring the Application Logging web service on page 467.

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions targetNamespace="urn:com.avaya.vp.report.VPReport4"
xmlns:apachesoap="http://xml.apache.org/xml-soap"
xmlns:impl="urn:com.avaya.vp.report.VPReport4"
xmlns:intf="urn:com.avaya.vp.report.VPReport4"
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: 1.4
Built on Apr 22, 2006 (06:55:48 PDT)-->
<wsdl:types>
 <schema elementFormDefault="qualified"
  targetNamespace="urn:com.avaya.vp.report.VPReport4"
  xmlns="http://www.w3.org/2001/XMLSchema">
 <complexType name="VPReportEntry4">
   <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:VPReportEntry4"/>
     </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:VPReportEntry4"/>
 <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="VPReport4">
 <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="VPReport4SoapBinding" type="impl:VPReport4">
 <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="VPReport4Service">
 <wsdl:port binding="impl:VPReport4SoapBinding" name="VPReport4">
  <wsdlsoap:address location="http://localhost:80/VPReport4"/>
 </wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

Chapter 16: 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 Voice Portal using the Add Application page.

  The web service automatically examines each MPP in the Voice 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

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 Voice Portal installation DVD.

You can use the Outcall test application to validate the Application Interface web service and the Voice Portal outcall functionality. Avaya supplies an installation script that automatically installs the Outcall test application when Voice Portal is installed. For more information , see the *Configure and run the Outcall test application* section in the *Implementing Voice Portal on a single server* guide or the *Implementing Voice Portal on multiple servers* guide.

Best practices

When using the Application Interface web service, keep in mind that:

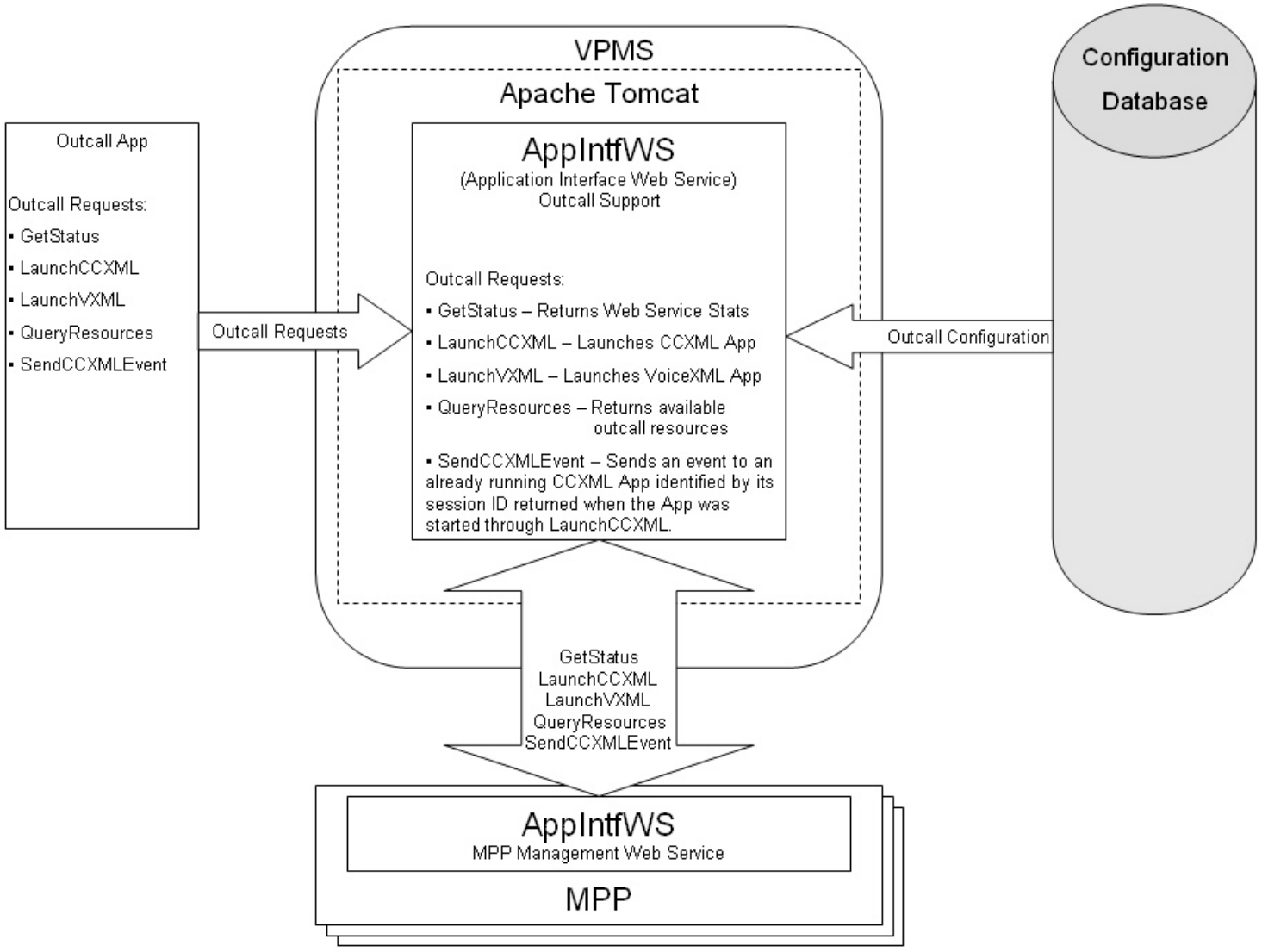
- The Application Interface web service uses Digest Authentication to authenticate web service client requests. When you submit a request to the web service, you need to include the user name and password specified in the **Outcall** section of the **Web Service Authentication** group on the VPMS Settings page. If you need to change this user name or password, you must do it through the VPMS. For details, see Configuring the Application Interface web service on page 481.
- 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 both the `LaunchCCXML` and the `LaunchVXML` method, parameters must be passed as name value pairs. For example, `parameter1=value`.
- If you plan to use a single CCXML application to launch 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 some 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:

  - Launch 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 launch another instance of the CCXML call blast application as soon as enough resources are available.
- If your Voice Portal VPMS software runs on a dedicated server machine, you should configure a auxiliary VPMS server to handle Application Interface web service requests if the primary VPMS server is unavailable.

Application Interface web service flow diagram

The following figure shows how the Voice Portal report data interacts with the Application Interface web service.



Configuring the Application Interface web service

1. Log in to the VPMS web interface using an account with the Administration user role.
2. From the VPMS main menu, select **System Configuration** > **VPMS Servers**.
3. On the VPMS Servers page, click **VPMS Settings**.

4. On the VPMS Settings page, go to the **Outcall** section in the **Web Service Authentication** group.
5. Enter the user name and password that must be included with all Application Interface 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. Open the following page in a web browser: `http://VPMS-server/axis/services/AppIntfWS?wsdl`

   Where *VPMS-server* is the domain name or IP address of the system where the primary VPMS software is installed.
8. When prompted, enter the user name and password specified in the **Outcall** section of the VPMS Settings page.
9. Save the WSDL file and use it to build the web service client that accesses the Application Interface web service. This web service conforms to all current W3C standards.

Application Interface web service methods

The Application Interface web service includes the following methods:

- GetStatus method on page 483
- LaunchCCXML method on page 484
- LaunchVXML method on page 490
- QueryResources method on page 497
- SendCCXMLEvent method on page 498

All methods can be called from any application that is running on the same network as theVoice Portal VPMS 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 requests since the Application Interface web service last started
- Number of 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 VPMS software on the server running the Application Interface web service

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.

Parameter	Type	Description
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 VPMS software running on the server.

Return values

Value	Attributes	Condition
0x0	Success	The web service successfully retrieved the status information.
0x1	Failure	The web service was unable to retrieve the status information. Verify that the VPMS and MPP servers are communicating properly and retry the request.

LaunchCCXML method

This method starts the specified CCXML application, and, if successful, returns the:

- Voice 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 being launched *must* return the status of that launch using a custom event as described in Returning the status of a LaunchCCXML request on page 488. For information on return values, see CCXML application Status return values on page 487.

Parameters

Parameter	Type	Description
toURI	String	Provides a hint to the Application Interface web service about what resources this CCXML application requires.

Parameter	Type	Description
		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.
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 Voice Portal through the VPMS. You can view all application names on the Applications page.
applicationURL	String	Parameters that should be appended to URL specified for the application in the VPMS. 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.
uuInfo	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.

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 Voice 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.

Return values

All return values except for "Success" indicate that this method has failed.

Value	Attributes	Condition
0x0	Success	The web service successfully started the CCXML application.
0x1	Failure	The Application Interface web service was unable to launch the CCXML application.
0x13	Failed	The application was not started due to a problem with the application server.
0x14	Timeout	The CCXML application did not begin within the amount of time specified in the launchTimeout parameter.
0x15	No Response	The session ended and the CCXML page did not return a response toVoice Portal. This can happen if the 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.
0x16	Fax Detected	The outbound number is associated with a fax machine.
0x20	Invalid URI	The toURI parameter contains an invalid URI specification.
0x21	Unknown Application	The applicationName parameter does not match one of the application names configured though the VPMS. You can view all application names on the Applications page.
0x22	Invalid URL	The applicationURL parameter contains an invalid URL specification.
0x32	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 MPP Service Menu Log Directories page.

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.

Related topics:

[Returning the status of a LaunchCCXML request](#) on page 488
[CCXML session properties](#) on page 488

Returning the status of a LaunchCCXML request

If you invoke a CCXML application using the Application Interface web service `LaunchCCXML` method, the application being launched *must* return the status of that launch using a custom event. This allows the CCXML application to determine whether the launch was successful instead of relying on the limited information available to the Application Interface web service.

For example, if the CCXML application launches correctly but no one answers the outgoing call, the Application Interface web service still considers the call to be a success because the application launched 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 Voice Portal.

Note:

For information on the status related return values that the CCXML application sends, see CCXML application Status return values on page 487.

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 Voice 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 VPMS 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 VPMS 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 uuInfo 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.

LaunchVXML method

This method initiates an outbound call on an available MPP, then starts the specified VoiceXML application. If successful, it returns the:

- Voice 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 488.

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.

Parameter	Type	Description
		Important: The applicationName must match the name that was specified when the application was added to Voice Portal through the VPMS. You can view all application names on the Applications page.
applicationURL	String	Parameters that should be appended to URL specified for the application in the VPMS. 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 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 493.
	String	Optional. If this parameter is set to `true`, then
uuInfo	String	The Application Interface web service passes any information in this parameter to the platform telephony layer included in the outbound call.
connectTimeout Secs	Integer	The maximum amount of time, in seconds, to wait for the outbound call to be connected. Enter a value between 0 and 2,147,483. If this parameter is set to 0 (zero) or omitted, Voice Portal uses the default value of 120 seconds.

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 Voice 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.

Return values

All return values except for "Success" indicate that this method has failed.

Value	Attributes	Condition
0x0	Success	The web service successfully connected the outbound call.
0x1	Failure	The Application Interface web service was unable to launch the VoiceXML application.
0x2	No resource	No outbound ports are available.
0x10	Busy	The destination named in the toURI parameter is busy and cannot be reached.
0x11	No Answer	The destination named in the toURI parameter did not answer within the amount of time specified in the connectTimeoutSecs parameter.
0x12	Network Refusal	The outbound call was rejected due to a network error.
0x15	No Response	The session ended and the VoiceXML page did not return a response toVoice Portal. This can happen if the VoiceXML 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.
0x16	Fax Detected	The outbound number is associated with a fax machine.
0x20	Invalid URI	Either or both of the toURI and fromURI parameters contain an invalid URI specification.
0x21	Unknown Application	The applicationName parameter does not match one of the application names configured though the VPMS. You can view all valid application names on the Applications page.

Value	Attributes	Condition
0x22	Invalid URL	The applicationURL parameter contains an invalid URL specification.
0x32	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 MPP Service Menu Log Directories page.

Related topics:

[Call classification with the LaunchVXML method](#) on page 493
[VoiceXML session properties](#) on page 495

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 milisecs (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 = 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.

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 MPP.
`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.
`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 MPP.
`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 MPP.

Property	Description
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 MPP.
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 MPP.
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 Voice 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

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 Voice Portal system. 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 480.

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.

Return values

Value	Attributes	Condition
0x0	Success	The web service successfully retrieved the resource information.
0x1	Failure	The web service was unable to retrieve the resource information. Verify that the VPMS and MPP servers are communicating properly and retry the request.

SendCCXMLEvent method

This method instructs the MPP to dispatch a user-named event with an accompanying parameter string to the specified CCXML session.

Parameters

Name	Type	Description
sessionID	String	The session ID of an existing CCXML session. This parameter must match exactly the session ID assigned by Voice 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.

Return values

All return values except for "Success" indicate that this method has failed.

Value	Attributes	Condition
0x0	Success	The specified event was successfully posted to the CCXML session.
0x1	Failure	Application Interface web service was unable to send the event to the CCXML session.
0x23	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.
0x30	MPP Down	The MPP service is not running and cannot service the request.
0x31	MPP Stopped	The MPP service is running, but the MPP is not currently processing calls.
0x32	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 MPP Service Menu Log Directories page.

Sample Application Interface web service WSDL file

The following is an example of theApplication Interface web service WSDL file. The actual file is installed on the server that is running the VPMS software. For details about accessing this file, see Configuring the Application Interface web service on page 481.

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
xmlns:impl="http://services.vp.avaya.com" xmlns:intf="http://services.vp.avaya.com"
xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/" xmlns:soap="http://
schemas.xmlsoap.org/wsdl/soap/"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:xsd="http://www.w3.org/2001/
XMLSchema"
name="AppIntfWS" targetNamespace="http://services.vp.avaya.com">
<wsdl:types>
 <xsd:schema xmlns="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" targetNamespace="http://services.vp.avaya.com">
  <xsd:element name="GetStatusRequest">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="GetStatusRequestUnused"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="GetStatusResponse">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="iSIPRequestsProcessed_returned"
type="int"/>
     <xsd:element name="iTELRequestsProcessed_returned"
type="int"/>
     <xsd:element name="iVXMLRequestsProcessed_returned"
type="int"/>
     <xsd:element name="iCCXMLRequestsProcessed_returned"
type="int"/>
     <xsd:element name="iCCXMLEventsSent_returned"
type="int"/>
     <xsd:element name="maxMPPHops_returned"
type="int"/>
     <xsd:element name="minMPPHops_returned"
type="int"/>
     <xsd:element name="avgMPPHops_returned"
type="int"/>
     <xsd:element name="serviceStartedDateTime_returned"
type="dateTime"/>
     <xsd:element name="lastRequestDateTime_returned"
type="dateTime"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="LaunchVXMLRequest">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="toURI"
type="string"/>
     <xsd:element name="fromURI"
type="string"/>
     <xsd:element name="applicationName"
```

```
type="string"/>
     <xsd:element name="applicationURL"
type="string"/>
     <xsd:element name="parameters"
type="string"/>
     <xsd:element name="uuiInfo"
type="string"/>
     <xsd:element name="connectTimeoutSecs"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="LaunchVXMLResponse">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="sessionID_returned"
type="string"/>
     <xsd:element name="totalRes_returned"
type="int"/>
     <xsd:element name="unusedSIP_returned"
type="int"/>
     <xsd:element name="unusedH323_returned"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="LaunchCCXMLRequest">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="toURI"
type="string"/>
     <xsd:element name="applicationName"
type="string"/>
     <xsd:element name="applicationURL"
type="string"/>
     <xsd:element name="parameters"
type="string"/>
     <xsd:element name="uuiInfo"
type="string"/>
     <xsd:element name="launchTimeout"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="LaunchCCXMLResponse">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="sessionID_returned"
type="string"/>
     <xsd:element name="totalRes_returned"
type="int"/>
     <xsd:element name="unusedSIP_returned"
type="int"/>
     <xsd:element name="unusedH323_returned"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="LaunchVXMLRequest">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="toURI"
type="string"/>
     <xsd:element name="fromURI"
type="string"/>
```

```
     <xsd:element name="applicationName"
type="string"/>
     <xsd:element name="applicationURL"
type="string"/>
     <xsd:element name="parameters"
type="string"/>
     <xsd:element name="uuiInfo"
type="string"/>
     <xsd:element name="connectTimeoutSecs"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="LaunchVXMLResponse">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="sessionID_returned"
type="string"/>
     <xsd:element name="totalRes_returned"
type="int"/>
     <xsd:element name="unusedSIP_returned"
type="int"/>
     <xsd:element name="unusedH323_returned"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="LaunchCCXMLRequest">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="toURI"
type="string"/>
     <xsd:element name="applicationName"
type="string"/>
     <xsd:element name="applicationURL"
type="string"/>
     <xsd:element name="parameters"
type="string"/>
     <xsd:element name="uuiInfo"
type="string"/>
     <xsd:element name="launchTimeout"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="LaunchCCXMLResponse">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="sessionID_returned"
type="string"/>
     <xsd:element name="totalRes_returned"
type="int"/>
     <xsd:element name="unusedSIP_returned"
type="int"/>
     <xsd:element name="unusedH323_returned"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="SendCCXMLEventRequest">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="sessionID"
type="string"/>
     <xsd:element name="eventName"
```

```
type="string"/>
     <xsd:element name="parameters"
type="string"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="SendCCXMLEventResponse">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="retCode"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="QueryResourcesRequest">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="queryResourcesRequestUnused"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
  <xsd:element name="QueryResourcesResponse">
   <xsd:complexType>
    <xsd:sequence>
     <xsd:element name="totalRes_returned"
type="int"/>
     <xsd:element name="unusedSIP_returned"
type="int"/>
     <xsd:element name="unusedH323_returned"
type="int"/>
    </xsd:sequence>
   </xsd:complexType>
  </xsd:element>
        <xsd:complexType name="GetStatusFault">
 <xsd:sequence>
  <xsd:element name="returnCode"
type="int"/>
  <xsd:element name="description"
type="xsd:string"/>
 </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name="LaunchCCXMLFault">
 <xsd:sequence>
  <xsd:element name="returnCode"
type="int"/>
  <xsd:element name="description"
type="xsd:string"/>
 </xsd:sequence>
        </xsd:complexType>
 <xsd:complexType name="QueryResourcesFault">
 <xsd:sequence>
  <xsd:element name="returnCode"
type="int"/>
  <xsd:element name="description"
type="xsd:string"/>
 </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name="SendCCXMLEventFault">
 <xsd:sequence>
  <xsd:element name="returnCode"
type="int"/>
  <xsd:element name="description"
type="xsd:string"/>
 </xsd:sequence>
```

```
        </xsd:complexType>
        <xsd:complexType name="LaunchVXMLFault">
 <xsd:sequence>
  <xsd:element name="returnCode"
type="int"/>
  <xsd:element name="description"
type="xsd:string"/>
 </xsd:sequence>
        </xsd:complexType>
 </xsd:schema>
</wsdl:types>
<wsdl:message name="GetStatusRequest">
 <wsdl:part element="impl:GetStatusRequest" name="parameters"/>
</wsdl:message>
<wsdl:message name="GetStatusResponse">
 <wsdl:part element="impl:GetStatusResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="LaunchVXMLRequest">
 <wsdl:part element="impl:LaunchVXMLRequest" name="parameters"/>
</wsdl:message>
<wsdl:message name="LaunchVXMLResponse">
 <wsdl:part element="impl:LaunchVXMLResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="LaunchCCXMLRequest">
 <wsdl:part element="impl:LaunchCCXMLRequest" name="parameters"/>
</wsdl:message>
<wsdl:message name="LaunchCCXMLResponse">
 <wsdl:part element="impl:LaunchCCXMLResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="SendCCXMLEventRequest">
 <wsdl:part element="impl:SendCCXMLEventRequest"
name="parameters"/>
</wsdl:message>
<wsdl:message name="SendCCXMLEventResponse">
 <wsdl:part element="impl:SendCCXMLEventResponse"
name="parameters"/>
</wsdl:message>
<wsdl:message name="QueryResourcesRequest">
 <wsdl:part element="impl:QueryResourcesRequest"
name="parameters"/>
</wsdl:message>
<wsdl:message name="QueryResourcesResponse">
 <wsdl:part element="impl:QueryResourcesResponse"
name="parameters"/>
</wsdl:message>
    <wsdl:message name="GetStatusFault">
 <wsdl:part name="GetStatusFault" type="impl:GetStatusFault">
 </wsdl:part>
    </wsdl:message>
    <wsdl:message name="LaunchCCXMLFault">
 <wsdl:part name="LaunchCCXMLFault" type="impl:LaunchCCXMLFault">
 </wsdl:part>
    </wsdl:message>
    <wsdl:message name="LaunchVXMLFault">
 <wsdl:part name="LaunchVXMLFault" type="impl:LaunchVXMLFault">
 </wsdl:part>
    </wsdl:message>
    <wsdl:message name="QueryResourcesFault">
 <wsdl:part name="QueryResourcesFault" type="impl:QueryResourcesFault">
 </wsdl:part>
    </wsdl:message>
    <wsdl:message name="SendCCXMLEventFault">
 <wsdl:part name="SendCCXMLEventFault" type="impl:SendCCXMLEventFault">
 </wsdl:part>
    </wsdl:message>
```

```
    <wsdl:portType name="AppIntfWS">
 <wsdl:operation name="GetStatus">
  <wsdl:input message="impl:GetStatusRequest"
name="GetStatusRequest"/>
  <wsdl:output message="impl:GetStatusResponse"
name="GetStatusResponse"/>
  <wsdl:fault message="impl:GetStatusFault"
name="Fault">
  </wsdl:fault>
 </wsdl:operation>
 <wsdl:operation name="LaunchVXML">
  <wsdl:input message="impl:LaunchVXMLRequest"
name="LaunchVXMLRequest"/>
  <wsdl:output message="impl:LaunchVXMLResponse"
name="LaunchVXMLResponse"/>
  <wsdl:fault message="impl:LaunchVXMLFault"
name="Fault"/>
 </wsdl:operation>
 <wsdl:operation name="LaunchCCXML">
  <wsdl:input message="impl:LaunchCCXMLRequest"
name="LaunchCCXMLRequest"/>
  <wsdl:output message="impl:LaunchCCXMLResponse"
name="LaunchCCXMLResponse"/>
  <wsdl:fault message="impl:LaunchCCXMLFault"
name="Fault"/>
 </wsdl:operation>
 <wsdl:operation name="SendCCXMLEvent">
  <wsdl:input message="impl:SendCCXMLEventRequest"
name="SendCCXMLEventRequest"/>
  <wsdl:output message="impl:SendCCXMLEventResponse"
name="SendCCXMLEventResponse"/>
  <wsdl:fault message="impl:SendCCXMLEventFault"
name="Fault"/>
 </wsdl:operation>
 <wsdl:operation name="QueryResources">
  <wsdl:input message="impl:QueryResourcesRequest"
name="QueryResourcesRequest"/>
  <wsdl:output message="impl:QueryResourcesResponse"
name="QueryResourcesResponse"/>
  <wsdl:fault message="impl:QueryResourcesFault"
name="Fault"/>
 </wsdl:operation>
</wsdl:portType>
<wsdl:binding name="AppIntfWSSOAP" type="impl:AppIntfWS">
 <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
 <wsdl:operation name="GetStatus">
  <soap:operation soapAction=" " style="document"/>
  <wsdl:input name="GetStatusRequest">
   <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="GetStatusResponse">
   <soap:body use="literal"/>
  </wsdl:output>
  <wsdl:fault name="Fault">
   <soap:fault name="Fault" use="literal"/>
  </wsdl:fault>
 </wsdl:operation>
 <wsdl:operation name="LaunchVXML">
  <soap:operation soapAction=" " style="document"/>
  <wsdl:input name="LaunchVXMLRequest">
   <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="LaunchVXMLResponse">
   <soap:body use="literal"/>
  </wsdl:output>
```

```
  <wsdl:fault name="Fault">
   <soap:fault name="Fault" use="literal"/>
  </wsdl:fault>
 </wsdl:operation>
 <wsdl:operation name="LaunchCCXML">
  <soap:operation soapAction=" " style="document"/>
  <wsdl:input name="LaunchCCXMLRequest">
   <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="LaunchCCXMLResponse">
   <soap:body use="literal"/>
  </wsdl:output>
  <wsdl:fault name="Fault">
   <soap:fault name="Fault" use="literal"/>
  </wsdl:fault>
 </wsdl:operation>
 <wsdl:operation name="SendCCXMLEvent">
  <soap:operation soapAction=" " style="document"/>
  <wsdl:input name="SendCCXMLEventRequest">
   <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="SendCCXMLEventResponse">
   <soap:body use="literal"/>
  </wsdl:output>
  <wsdl:fault name="Fault">
   <soap:fault name="Fault" use="literal"/>
  </wsdl:fault>
 </wsdl:operation>
 <wsdl:operation name="QueryResources">
  <soap:operation soapAction=" " style="document"/>
  <wsdl:input name="QueryResourcesRequest">
   <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="QueryResourcesResponse">
   <soap:body use="literal"/>
  </wsdl:output>
  <wsdl:fault name="Fault">
   <soap:fault name="Fault" use="literal"/>
  </wsdl:fault>
 </wsdl:operation>
</wsdl:binding>
<wsdl:service name="AppIntfWS">
 <wsdl:port binding="impl:AppIntfWSSOAP" name="AppIntfWS">
  <soap:address location="http://localhost:80/axis/services/AppIntfWS"/>
 </wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W