System Configuration

System Tab Options

Table 1: System Tab Options

System tab options	Use To
Control Center	View the status of the Cisco Unified Customer Voice Portal environment in a network control center. View the status and statistics by Device Type or Device Pools, logical groups of devices in the Cisco Unified Customer Voice Portal solution. Initiate Start, Shutdown, or Graceful Shutdown actions on devices in the control center.
Device Pool	Create, modify, and delete device pool names and descriptions for logical groups of devices (for example, all devices located in a geographical region). For details, see Device Pool and Add or Remove Device From Device Pool.
Import System Configuration	Import a previously-saved Operations Console Server configuration file and apply it to the current system. For details, see Import System Configuration, on page 2.

System tab options	Use To
Export System Configuration	Save and export all configuration information for the Operations Console Server to a single file on your local computer. You can later use this file to restore an Operations Console Server during disaster recovery. For details on this option, see Export System Configuration, on page 3.
Location	Add, edit, synchronize, and delete Unified CM location information.
SIP Server Groups	Configure server groups for SIP and view Call Server deployment status. For details, see Location Configuration, on page 4.
Web Services	Configure Diagnostic Portal servlet credentials. For details, see Deploy Web Services, on page 19.
Dialed Number Pattern	Configure the Dialed Number Patterns for a destination. You can define the dialed numbers for the Error Tone, Ring Tone, and other destinations. For details, see Add and Deploy Dialed Number Pattern, on page 16.
IOS Configuration	**IOS Template Management** - Add, Delete, Edit, Copy, and View an IOS template configuration pushed to an IOS gateway. The template contains the IOS commands required for use in a Unified CVP deployment. **IOS Template Deployment** - Deploy a gateway configuration template to an IOS gateway. The template provisions the gateway and substitutes any variables in the template with the source devices that are chosen when it is deployed. For details, see IOS Configuration, on page 19.
Courtesy Callback	For details, see Configure Courtesy Callback, on page 29.

Related Topics

Import System Configuration

For disaster recovery, import the saved Operations Console configuration to your computer. To back up and restore Operations Console configuration, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*.

Note
- Operations Console supports the import of system-level configuration data.

- Operations Console cannot export the sip.properties file. To export the sip.properties file, manually copy the sip.properties file along with the CVP Operations Console configuration.

- When you import a database which was exported from an older version, the imported database is automatically upgraded to the latest version, as indicated in the confirmation message

Procedure

Step 1 Stop the **Cisco CVP WebServicesManager** Windows Service by performing the following steps:

a) Select **Start** > **All Programs** > **Control Panel Programs** > **Administrative Tools** > **Services**.

Step 2 Select **System** > **Import System Configuration**.

Step 3 Enter the file name in the **Enter Configuration File** text box or click **Browse to** to search for the file to import.

Step 4 Select **Import**.

Step 5 Perform Step 1(a).

Step 6 Perform the following steps:

a) Select **Cisco CVP OPSConsoleServer**, and click **Restart**.

b) Select **Cisco CVP WebServicesManager**, and click **Restart**.

Step 7 Log in to the Operations Console.

What to do next

If 12.5(1) or an earlier version of CVP configuration (exported) is imported on 12.6(x) Operations Console (OAMP), you need to run the command **mgr-init.bat -oamp** from the command prompt from CVP's bin folder:

1. Stop Cisco Unified CVP Operations Console and Cisco CVP WebServicesManager.

2. Go to the CVP bin folder.

3. Run the `mgr-init.bat -oamp` command from the command prompt.

4. Restart Cisco Unified CVP Operations Console and Cisco CVP WebServicesManager.

Export System Configuration

For back up, save and export the Operations Console configuration to a single file on your computer. This file can later be used to configure another Operations Console Server without having to individually reconfigure each module. For details, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*. You can export the database on a regular basis and also when you make major configuration changes to a device.

Note
- All Operations Console configuration data is exported, except for any files you have uploaded, includingapplication scripts. The Operations Console supports the export of system-level configuration data.

- Import and export operations do not back up or restore the CVP configuration of the VoiceBrowser or the SIP.properties files. If the backup and record of the Unified CVP configuration is required, manually back up the SIP.properties file and the result of the VoiceBrowser **sall** command along with the export of system configuration through the Operations Console.

Procedure

Step 1	Select **System** > **Export System Configuration**.
Step 2	On the **Export System Configuration** page, click **Export**.
Step 3	In the **Save As** dialog box, select a location to save the file.

Note You may save the configuration multiple times. Choose a naming convention that helps you identify the configuration, for example, include the current date and time in the file name.

Location Configuration

Configure a location to route calls locally to the agent available in the branch office instead of routing calls to centralized or non-geographical numbers. Use the location configuration feature to select a Unified Communication Manager (CM) Server and extract the Unified CM location information (location provider). After an administrator initiates the synchronization, the system retrieves the location information for all available Unified CM servers which have been identified as sources for location information.

After you enable synchronization for a Unified CM server, information can be retrieved from any of the Unified CM servers that have been identified as sources for location information.

Note All Unified CM servers enabled for synchronization are used during the synchronization task. If you do not want a particular Unified CM to be used when the synchronization task is performed, then disable synchronization for that Unified CM.

The following table lists the location configuration settings:

Table 2: Location Configuration Settings

Property	Description	Default	Value	Restart Required
General				
Insert Site Identifier	Select one of the following options to identify the site information: • **Insert site identifier between the Network VRU label and the correlation ID** • **Insert site identifier at the beginning of the Network VRU label** • **Do not insert site identifier**	**Insert site identifier between the Network VRU label and the correlation ID**	Not applicable	No
Location				
Location Name (required)	This is a user defined field.	Not applicable	a-z, A-Z, 0-9, -_ Max length 128 characters	No
Site ID (required)	The Site ID is a unique user-defined field.	Null	0-9, # Max length 128 characters	No
Location ID (required)	The Location ID is a unique user-defined field.	Null	a-z, A-Z, 0-9 Max length 128 characters	No
Unified CM IP Address This field is not available for manually-configured locations.	Ensure to check the Enable Synchronization check box in the Unified CM Server Configuration screen's **General** tab to select Unified CM as a Unified CM location information provider. If a Unified CM server is removed from the Operations Console configuration, if the Unified CM server is unreachable, or if the synchronization check box is deselected, all locations stored in the Operations Console are automatically marked as invalid.	Not applicable	Not applicable	No

Property	Description	Default	Value	Restart Required
Associated Gateway	You can select Gateways from the Available list to deploy location information. You can configure multiple Gateways per location. An instance of a Gateway can only be assigned to one location. When a Gateway is associated with a location, the Gateway configuration window displays the location as a read-only field.	Not applicable	Not applicable	No

Property	Description	Default	Value	Restart Required
Status	The status indicates if the location information is valid or invalid: • **Invalid:** The location is invalid if any of the following scenarios apply: • The location was previously synchronized with a Unified CM server. Later, you delete this location from the Unified CM server. When you perform the next synchronization with the Unified CM server, this location becomes invalid. • The Unified CM server's Enable Synchronization check box remains unchecked. You can select and remove "Invalid" locations at any time. If a unified CM is deselected from the synchronization list after synchronizing with that Unified CM server, then all the locations synchronized from this Unified CM server become invalid. • If a Unified CM server is not reachable when the next synchronization occurs, then all the locations associated with that Unified CM become invalid. • **Valid:** The location is valid if any of the following scenarios apply: • the Enable Synchronization check box is checked • the location is exists in a Unified CM server configuration, the last synchronization was successful with the Unified CM, and if that Unified CM is still selected.	Not applicable	Valid or Invalid	No
Call Server Deployment				
Associate Call Servers	Select call servers from the Available list to deploy location information. One or more call servers can be selected and designated as Selected/Available.	Configuration is deployed to all selected call servers	Not applicable	No

Prerequisites for Location Configuration

• Configure the device type as a gateway.

Note If a location is associated with more than one Gateway, the system displays multiple rows of the same location information for each associated device.

• If the device location ID information is configured on the Location configuration page, ensure that it is displayed as a read-only field.

• Ensure that any configurable fields remain blank if they are not configured by a user.

Deploy Location Information

By default, location information is deployed to all associated Call Servers. However, you can choose to deploy location information to one or more Call Servers.

Procedure

Step 1 Select **System** > **Location** and make the enter or modify the location configuration field values.

Step 2 Click **Save & Deploy** to save the location information and initiate a deployment request to the selected Call Servers. Or, click **Save** to save the settings three components to the database: the location information, information in the General tab, and the associated Call Servers and deploy the location information later.

Caution The Deployment Status screen displays a warning message if you have:

• Saved only the configuration details and have not deployed them.

• Edited or deleted an existing configuration and have not deployed the changes.

• Changed the call server association.

Add Location

You can manually add location information for locations that do not exist in the Unified CM database.

Procedure

Step 1 Log in to the Operations Console and select **System** > **Location**.

Step 2 On the **Location** tab, select **Add New**.

The Location Configuration window appears.

Step 3 Enter the Location, Site ID, Location ID, and the Unified CM IP Address as applicable to your configuration.

Step 4 (Optional) Select the required Gateway by moving it to the **Selected** column.

Step 5 Click **Save**.

SIP Server Group Configuration

A SIP Server Group consists of one or more destination addresses (endpoints) and is identified by a Server Group domain name. This domain name is also known as the SRV cluster name, or Fully Qualified Domain Name (FQDN). Server Groups contain Server Group Elements.

In Unified CVP, you can add server groups at the system level to perform SIP dynamic routing.

Add SIP Server Groups

Procedure

Step 1 Log in to the Operations Console and select **System** > **SIP Server Groups**.

The SIP Server Groups window appears.

Step 2 Select **Add New**.

Step 3 Click the following tabs and enter or modify the default values of fields, if required:

a) **General**. See General Settings, on page 10.
b) **Heartbeat Properties**. See Heartbeat Properties Settings, on page 10.
c) **Call Server Deployment**. See Deploy Call Server, on page 14.

Step 4 (Optional) To remove an element from the group, select it and click **Remove**. To replace a selected element with a new element, edit the SIP Server Group Elements properties, select an existing element, and then click **Replace**

Step 5 Click **Save & Deploy**.

Note Click **Save** to save the changes on the Operations Console and configure the SIP Server group later.

Related Topics

General Settings

Table 3: SIP Server Group General Settings

Column	Description
Name	The name of the SIP Server Group. Nested under the SIP Server Group are the SIP Server Group Elements.
	Click the expand/collapse (+/-) icon to expand and collapse the elements within the group. Additionally, you can click **Collapse all** and **Expand all** to collapse/expand all the elements within the server groups listed on the page.
Number of Elements	The number of elements contained in the group.
Port	Port number of the element in the server group.
Priority	Priority of the element in relation to the other elements in the server group. Specifies whether the server is a primary or backup server. Primary servers are specified as 1.
Weight	Weight of the element in relation to the other elements in the server group. Specifies the frequency with which requests are sent to servers in that priority group.

Heartbeat Properties Settings

These properties enable Heartbeat communication between the SIP Server Group and the elements of the SIP Server Group. In case of element not responding to Heartbeat messages, the element is marked as unavailable; on receiving a successful response, it is marked as available again.

Table 4: SIP Server Group Heartbeat Properties Settings

Property	Description	Default	Value
Use Heartbeats to Endpoints	Select to enable the heartbeat mechanism. Heartbeat properties are editable only when this option is enabled. **Note** Endpoints that are not in a Server Group can not use the heartbeat mechanism.	Disabled (unchecked)	Enabled or Disabled **Note** Enable Heartbeat for high-availability and quick recovery of element in case of a failover.

Property	Description	Default	Value
Number of failed Heartbeats for unreachable status	The number of failed heartbeats before marking the destination as unreachable.	1	1 through 5
Heartbeat Timeout (ms)	The amount of time, in milliseconds, before timing out the heartbeat.	500 milliseconds	100 through 3000
Up Endpoint Heartbeat Interval (ms)	The ping interval for heart beating an endpoint (status) that is up.	5000 milliseconds	5000 through 3600000
Down Endpoint Heartbeat Interval (ms)	The ping interval for heart beating an endpoint (status) that is down.	5000 milliseconds	5000 through 3600000
Heartbeat Local Listen Port	The heartbeat local socket listen port. Responses to heartbeats are sent to this port on CVP by endpoints.	5067	0 through 65000
Heartbeat SIP Method	The heartbeat SIP method. **Note** PING is an alternate method; however, some SIP endpoints do not recognize PING and will not respond at all.	OPTIONS **Note** If SIP Server Group has secure SIP port configured, OPTIONS messages are sent on non-secure 5060 port.	OPTIONS or PING

Property	Description	Default	Value
Heartbeat Transport Type	During transportation, Server Group heartbeats are performed with a UDP or TCP socket connection. If the Operations Console encounters unreachable or overloaded callbacks invoked in the Server Group, that element is marked as being down for both UDP and TCP transports. When the element is up again, it is routable for both UDP and TCP. **Note**　TLS transport is not supported.	UDP	UDP or TCP
Overloaded Response Codes	The response codes are used to mark an element as *overloaded* when received. If more than one code is present, it is presented as a comma delimited list. An OPTIONS message is sent to an element and if it receives any of those response codes, then this element is marked as overloaded.	503,480,600	1 through 128 characters. Accepts numbers 0 through 9 and commas (,).

Property	Description	Default	Value
Options Override Host	The contact header hostname to be used for a heartbeat request (SIP OPTIONS). The given value is added to the name of the contact header of a heartbeat message. Thus, a response to a heartbeat would contain gateway trunk utilization information.	cvp.cisco.com	Valid hostname, limited to 128 characters.

Server Group Heartbeat Settings

The Server Group heartbeat default setting tracks the ping interval between any two pings; it is not the interval between pings to the same endpoint. The Server Group does not ping at a specific interval and ping all elements because this approach would introduce a fluctuation on CPU usage. Also, it takes more resources when the system has to ping many endpoints. For example, to ping 3 elements across all groups at 30-second intervals, you have to set the ping interval at 10 seconds.

It is less deterministic for reactive mode because elements that are currently down can fluctuate, so the ping interval fluctuates with it.

Note
- **Heartbeat Behavior Settings for Server Groups.** To turn off pinging when the element is up, set the **Up Endpoint Heartbeat Interval** to zero (reactive pinging). To turn off pinging when the element is down, set the **Down Endpoint Heartbeat Interval** to zero (proactive pinging). To ping when the element is either up or down, set the heartbeat intervals to greater than zero (adaptive pinging).
- **Heartbeat Response Handling.** Any endpoint that CVP may route calls to should respond to OPTIONS with some response, either a 200 OK or some other response. Any response to a heartbeat indicates the other side is alive and reachable. A 200 OK is usually returned, but CUSP Server may return a 483 Too Many Hops response, because the max-forwards header is set to zero in an OPTIONS message. Sometimes the endpoints may not allow OPTIONS or PING, and may return 405 Method Not Allowed.

By default, Server Group heartbeats are monitored using a UDP socket connection. The transport type can be changed to TCP from the Operations Console Server Groups window.

Whenever an element has an unreachable or overloaded status, that element is marked as down completely, that is for both UDP and TCP transports. When the element is up again, transports are routed for both UDP and TCP.

Duplicate Server Group Elements is not monitored because the primary element is already monitored.

Note See the *Configuration Guide for Cisco Unified Customer Voice Portal* for typical configurations for the Server Group feature, available at http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_ and_configuration_guides_list.html

Deploy Call Server

Procedure

Step 1 Log in to the Operations Console and select **System** > **SIP Server Groups**.

The SIP Server Groups Configuration window appears.

Step 2 Click the **Call Server Deployment** tab.

Step 3 From the **Associate Unified CVP Call Servers** screen, in the **Available** list box, select one or multiple Call Servers and click the **Add** arrow.

The added Call Servers appear in the **Selected** list box.

Note • Add and deploy at least one Call Server before you configure a SIP Server group. A warning message is displayed if you try to add a SIP Server group without deploying a Call Server. For details on how to configure a Call Server, see Configure Call Server.

• The Deployment Status screen displays a warning message In the following cases:

• If you have only saved the SIP server details and have not deployed them.

• If you have edited or deleted an existing configuration and have not deployed the changes.

• If you changed the call server association.

• Only one deployment process can run at a time. If one process is already running, you cannot initiate another process and receive an error message.

• A message displays to indicate the successful start of deployment process. The Operations Console saves the Call Server configuration to the Operations Console database and returns to display the new configuration in the list page.

Step 4 Click **Save & Deploy**.

Note   Click **Save** to save the changes on the Operations Console and deploy a Call Server for the SIP
           Server group later.

Related Topics
    Configure Call Server

Dialed Number Pattern Configuration

A dial plan essentially describes the number and pattern of digits that a user dials to reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of the number of digits dialed are all part of a dial plan. For example, the North American Public Switched Telephone Network (PSTN) uses a 10-digit dial plan that includes a 3-digit area code and a 7-digit telephone number. Most PBXs support variable length dial plans that use 3 to 11 digits. Dial plans must comply with the telephone networks to which they connect. A Dialed Number (DN) pattern is dial plan configured on one or multiple Call Servers and provides details on the call flow of dialed digits.

Dial plans on Cisco routers are manually defined using dial peers. Dial peers are similar to static routes; they define where calls originate and terminate and what path the calls take through the network. Attributes within the dial peer determine which dialed digits the router collects and forwards to telephony devices. For more information on Dial plans, see https://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/vcf_bk.pdf.

Use the **System** menu to configure a DN pattern. Select the **Display Pattern Type** to display the configured SN patterns in a tree-hierarchy view. The Display Pattern Type list box includes the following options:

- Display All (default)

- Local Static Route

- Send Calls to Originator

- RNA Timeout for Outbound Calls

- Custom Ringtone

- Post Call Survey for Incoming Calls

After you select a view, a table containing the Dialed Number Patterns for the respective, selected type appear. The current view for the dialed number system-level configuration list page is maintained until the user session expires, either by timeout or by signing out from the Operations Console or until the dialed number pattern view type selection changes.

Each dialed number pattern appears as a row. Each dialed number pattern column type can be sorted alphabetically in ascending or descending order. The Dialed Number list is in hierarchical format that lets you collapse or expand individual entries. One or more root hierarchical rows can be selected using the check boxes. All table entries are expanded by default or after certain operations, such as sorting, filtering, and pagination.

The column types are as follows:

Dialed Number Pattern - The actual dialed number pattern.

Description - The dialed number pattern description.

You may also use the filtering function to filter for specific Dialed Number Patterns. Only the Dialed Number Pattern itself is filterable by the standard constraint criteria (that is, begins with, contains, ends with, is exactly, is empty). The Dialed Number Pattern list also has sortable columns.

Add and Deploy Dialed Number Pattern

Procedure

Step 1	Log in to the Operations Console and select **System** > **Dialed Number Pattern**.
Step 2	Click **Add New**.
Step 3	Enter or modify the Dialed Number pattern configuration settings, as listed in the following table:

Table 5: Dialed Number Pattern Configuration Settings

Property	Description	Default	Value
General Configuration			
Dialed Number Pattern	The actual Dialed Number Pattern.	None	Must be unique Maximum length of 24 characters Can contain alphanumeric characters, wildcard characters such as exclamation point (!) or asterisk (*), single digit matches such as the letter "X" or period (.) Small letter "x" cannot be used as a wildcard. Can end with an optional greater than (>) wildcard character
Description	Information about the Dialed Number Pattern.	None	Maximum length of 1024 characters

Property	Description	Default	Value
Enable Local Static Route	Enable local static routes on this Dialed Number Pattern. If Local Static Routes are enabled: • **Route to Device -** Select the device from the drop-down list which contains a list of configured, supported devices. Once a selection is made, the IP Address/Hostname/Server Group Name field is automatically updated with the IP Address of the selected device. • **Route to SIP Server Group -** Select the device from the drop-down list which contains a list of configured, support devices. Once a selection is made, the IP Address/Hostname/Server Group Name field is automatically updated with the IP Address of the selected device. • **IP Address/Hostname/Server Group Name -** If you have not selected a **Route to Device** or **Route to SIP Server Group**, enter the IP address, hostname, or the server group name of the route.	Disabled	Maximum length of 128 characters Must be a valid IP address, hostname, or fully qualified domain name
Enable Send Calls to Originator	Enables calls to be sent to originator.	Disabled	n/a
Enable RNA Timeout for Outbound Calls	Enables Ring No Answer (RNA) timer for outbound calls. • **Timeout -** Enter the timeout value in seconds.	Disabled none	n/a Valid integer in the inclusive range from 5 to 60
Enable Custom Ringtone	Enables customized ring tone. • **Ringtone media filename -** Enter the name of the file that contains the ringtone.	Disabled none	Maximum length of 256 characters Cannot contain whitespace characters

Property	Description	Default	Value
Enable Post Call Survey for Incoming Calls	Enables post call survey for incoming calls. • **Survey Dialed Number Pattern -** Enter the survey dialed number pattern.	Disabled none	n/a Maximum length of 24 characters Can contain alphanumeric characters, wildcard characters such as exclamation point (!) or asterisk (*), single digit matches such as period (.) or X (not x), and can end with an optional greater than (>) wildcard character.

Step 4   Click **Save**.

The **Dialed Number Pattern** page appears.

Step 5   To deploy the Dialed Number Pattern configuration to all the Call Servers, click **Deploy**.

Note   Click **Deployment Status** to view the status of DN pattern deployment.

Web Services Configuration

Unified CVP offers a Web Services-based framework to deliver a common user experience across all Cisco Unified Communications applications for features, such as setting up preferences, directories, and communication logs, setting serviceability parameters, and collecting, analyzing, and reporting on information necessary to manage and troubleshoot the Cisco Unified Communications solution. This centralized framework enables consistency between Cisco Unified Communications applications and ensures a unified view of common serviceability operations.

The Web Services application handles API queries from external clients for CVP diagnostic information.

The Operations Console interfaces with the Web Services application in following two ways:

• **Web Services User Management:** The Operation Console administrator can configure new Web Services users (users with the Web Services user role type). The Operations Console administrator can also manually push any configured Web Services users using the procedure identified in Deploy Web Services, on page 19.

When you make Web Services user information changes and when you successfully deploy a device, all Web Services users are automatically pushed to the deployed Unified CVP devices listed below:

    • CVP Call Server

    • CVP Reporting Server

    • CVP VXML Server

    • Unified CVP VXML Server (standalone)

    • CVP Remote Operations device

External clients may connect to the Web Services application and authenticate themselves with these credentials.

- **List Application Servers:** The Operations Console currently stores configuration details for all devices in the database. The Operations Console writes this information to a device file which the Web Services application uses to reply to queries from external clients.

Related Topics

Deploy Web Services

Before you begin

Install Remote Operations on the third-party device.

Procedure

Step 1	Log in to the Operations Console and select **System** > **Web Services**.
Step 2	Click the **Remote Operations Deployment** tab and perform the following steps:
	a) Enter the IP Address and Hostname.
	b) (Optional) Enter the description of the third-party device.
	c) Click **Add** to add the device to the list of devices associated with the Unified CVP deployment Web services.
Step 3	Click **Save & Deploy** to save and deploy the configuration to the impacted devices in the Operations Console database.

IOS Configuration

Configure IOS gateways using templates through Operations Console. Templates are text files that contain the IOS commands required for use in a Unified CVP deployment. You can edit the templates locally and then upload it to the Operation Console. You can deploy the configuration defined in the template to a gateway right from the Operations Console. You can also rollback the configuration on the gateway to the point immediately before the template was deployed.

Note There is only one level of rollback. If you deploy a template (Template A) and then deploy another template (Template B), you can only roll back to Template A.

IOS Configuration consists of:

- Template Management. See

- Template Deployment. See .

You can use the default templates or create custom templates.

The templates contain variables that are placeholders for configuration data. The variables can reference data that is in the Operations Console database as well as reference data that is outside of the Operations Console database, if it is accessible to the Operations Console (such as some portions of the Unified ICM database). The variables are replaced with the actual values of the data when the template is sent to the IOS Gateway.

Templates are located in the following directories on the Operations Console server:

- **Default Templates** - %CVP_HOME%\OpsConsoleServer\IOSTemplates\default

- **Custom Templates** - %CVP_HOME%\OpsConsoleServer\IOSTemplates\custom

Related Topics

IOS Template Format

The IOS template must have a specific format to be accepted by the Operations Console:

- The first line of the template must be a comment that exactly matches the following format:

! Customer Voice Portal 9.0(1) IOS Template

- The second should be a configure terminal command, such as:

conf t

With the exception of variables, all of the commands use standard IOS syntax. The variables that can be used are listed in the following table:

Table 6: IOS Template Format

Component	Variables
CVP Call Server	• `%CVP.Device.CallServer.General.IP Address%` • `%CVP.Device.CallServer.ICM.Maximum Length of DNIS%` • `%CVP.Device.CallServer.ICM.New Call Trunk Group ID%` • `%CVP.Device.CallServer.ICM.Pre-routed Call Trunk Group ID%` • `%CVP.Device.CallServer.SIP.Outbound SRV Domain Name/Server Group Domain Name (FQDN)%` • `%CVP.Device.CallServer.SIP.Outbound Proxy Port%` • `%CVP.Device.CallServer.SIP.Port number for Incoming SIP Requests%` • `%CVP.Device.CallServer.SIP.DN on the Gateway to play the ringtone%` • `%CVP.Device.CallServer.SIP.DN on the Gateway to play the error tone%` • `%CVP.Device.CallServer.SIP.Generic Type Descriptor (GTD) Parameter Forwarding%` • `%CVP.Device.CallServer.SIP.PrependDigits - Number of Digits to Strip and Prepend%` • `%CVP.Device.CallServer.SIP.UDP Retransmission Count%` • `%CVP.Device.CallServer.IVR.Media Server Retry Attempts%` • `%CVP.Device.CallServer.IVR.IVR Service Timeout%` • `%CVP.Device.CallServer.IVR.Call Timeout%` • `%CVP.Device.CallServer.IVR.Media Server Timeout%` • `%CVP.Device.CallServer.IVR.ASR/TTS Server Retry Attempts%` • `%CVP.Device.CallServer.IVR.IVR Service Retry Attempts%`
CVP Reporting Server	`%CVP.Device.ReportingServer.General.IP Address%`
Unified CVP VXML Server	`%CVP.Device.VXMLServer.General.IP Address%`
Gateway	• `%CVP.Device.Gateway.Target.IP Address%` • `%CVP.Device.Gateway.Target.Trunk Group ID%` • `%CVP.Device.Gateway.Target.Location ID%`
SIP Proxy Server	`%CVP.Device.SIPProxyServer.General.IP Address%`
Speech Server	`%CVP.Device.Speech Server.General.IP Address%`

Component	Variables
Unified Communications Manager	`%CVP.Device.Unified CM.General.IP Address%`
Media Server	`%CVP.Device.Media Server.General.IP Address%`

IOS Template Management

Manage IOS templates by adding, deleting, editing, copying, and viewing details about templates.

Add New Template

Procedure

Step 1 Select **System** > **IOS Configuration** > **IOS Template Management**.

Step 2 From the toolbar, select **Add New**.

The IOS Template Configuration page opens.

Step 3 Click **Browse** to browse to a template file on your local computer. Provide a name for the template and an optional description. Click **Save** to upload the template file to the Operations Console.

Note The file you select to upload must be of a valid file format or the upload fails. See the IOS Template Format, on page 20 section for details on the format required and the variables that you can use in your template.

A message is displayed confirming successful upload if the file is valid.

Delete Template

Note You cannot delete default templates. Only custom templates can be deleted.

Procedure

Step 1 Select **System** > **IOS Configuration** > **IOS Template Management**.

The IOS Template Management page opens.

Step 2 Select the check boxes next to the templates you want to delete.

Step 3 From the toolbar, select **Delete**.

A confirmation appears. Select **OK** to proceed and delete any custom templates selected.

Edit Templates

You can change the description of any template and edit the body of custom templates from within the browser. However, you cannot edit the body of default templates.

Procedure

Step 1	Select **System** > **IOS Configuration** > **IOS Template Management**.
	The IOS Template Management window opens.
Step 2	Select the check box next to the template you want to edit.
Step 3	From the toolbar, select **Edit**.
	The IOS Template Configuration page appears.
Step 4	(Optional) Edit the description field.
Step 5	If this is a custom template, then you can check the **Enable template modification** check box to allow for editing of the template body. See IOS Template Format, on page 20 for details about template syntax. You can cancel any unsaved changes you made to the body by clicking **Undo Template Body Changes**.
Step 6	Click **Save**.

Related Topics

IOS Template Format, on page 20

Copy Templates

You can copy templates to create a new template to which you can make modifications. It is not possible to edit the body of a default template. However, you can copy a default template and then edit the body of the copy.

Procedure

Step 1	Select **System** > **IOS Configuration** > **IOS Template Management**.
	The IOS Template Management window opens.
Step 2	Select the check box next to the template that you want to copy
Step 3	From the toolbar, select **Copy**.
Step 4	Edit the name and description for the copy.
Step 5	(Optional) Check the **Enable template modification** check box and make changes to the copy. You can also make changes later. See Edit Templates, on page 23.
Step 6	Select **Save**.

Related Topics

Edit Templates, on page 23

IOS Template Deployment

Use the IOS Template Deployment page to deploy a gateway configuration template to a gateway. The template provisions the gateway and substitutes any variables in the template with source devices that you choose when you deploy.

From this page, you can:

- Preview the body of the template (and validate the template) and deploy to a gateway.

- Check the status of the template deployment.

- Rollback the configuration sent to a gateway to its previous state.

Related Topics

IOS Template Format, on page 20

Preview and Deploy Template

To preview (validate) and deploy a template:

Procedure

Step 1 Log in to the Operations Console and select **System** > **IOS Configuration** > **IOS Template Deployment**.

Step 2 In the **Select Template** panel, select the template that you want to deploy.

Step 3 In the **Associate Source Device(s)** panel, select the devices to be replaced with device variables in the template.

Step 4 In the **Associated Gateways** panel, deselect any of the gateways that will not receive the template deployment. By default, all gateways are selected.

Step 5 Click **Preview and Deploy** to validate and preview the template to the selected gateways with the selected settings.

After clicking **Preview and Deploy**, the script is validated. If there is an error in the script, or if there is a variable in the script for which a device is required with no device selected from the **Associate Source Device(s)** panel, then errors are listed on the IOS Template Preview Page. Clicking **Deploy** at this point does not deploy the template, and the status page shows a failure due to an invalid template.

Once the preview screen appears, you can perform one of three actions:

- If the template is valid or invalid, click **Enable template modification** and edit the template on this screen. Click **Verify** to verify your changes as valid, or click **Undo All Changes** to revert the template to the way it was before you began editing.

- If the template is valid, click **Deploy** to deploy the template to the selected gateways,

- If the template is valid, click **Save and Deploy** to save the template and deploy the template to the selected gateways. If this is an existing custom template, then any changes you made are saved to this custom template. If this is a default template, then the template is copied to a new custom template and saved.

Check Deployment Status

To check the status of a template deployment:

Procedure

Step 1   Log in to the Operations Console and select **System** > **IOS Configuration** > **IOS Template Deployment**.

Step 2   From the toolbar, select **Deployment Status**.

The IOS Template Deployment - Deployment Status window opens.

The status page lists information about the attempted deployment. Click the status message for any deployment for additional details.

Roll Back Deployment

Note   There is only one level of rollback. If you deploy a template (Template A) and then deploy another template (Template B), you can only roll back to Template A.

Procedure

Step 1   Log in to the Operations Console and select **System** > **IOS Configuration** > **IOS Template Deployment**.

Step 2   From the toolbar, click **Deployment Status**.

The IOS Template Deployment - Deployment Status window opens.

Step 3   Check the check box next to the deployment you want to rollback and click **Rollback**.

- A confirmation dialog opens. Read the warning message and click **OK** to continue the rollback.

- A status message is displayed stating that the rollback is in progress. Refresh the status page by clicking **Refresh** to see the status of the rollback.

IOS Gateway Configuration

With CiscoIOS Gateways, dial peers are used to match phone numbers, and the destination can be a SIP Proxy Server, DNS SRV, or IP address. The following example shows a CiscoIOS Gateway configuration to send calls to a SIP Proxy Server using the SIP Proxy's IP address.

```
sip-ua
 sip-server ipv4:10.4.1.100:5060

dial-peer voice 1000 voip
 session target sip-server
 ...
```

The **sip-server** command on the dial peer tells the CiscoIOS Gateway to use the globally defined SIP Server that is configured under the **sip-ua** settings. In order to configure multiple SIP Proxies for redundancy, you can change the IP address to a DNS SRV record, as shown in the following example. The DNS SRV record allows a single DNS name to be mapped to multiple Reporting Servers.

```
sip-ua
 sip-server dns:cvp.cisco.com

dial-peer voice 1000 voip
 session target sip-server
 ...
```

Alternatively, you can configure multiple dial peers to point directly at multiple SIP Proxy Servers, as shown in the following example. This configuration allows you to specify IP addresses instead of relying on DNS.

```
dial-peer voice 1000 voip
 session target ipv4:10.4.1.100
 preference 1
 ...
dial-peer voice 1000 voip
 session target ipv4:10.4.1.101
 preference 1
 ...
```

In the preceding examples, the calls are sent to the SIP Proxy Server for dial plan resolution and call routing. If there are multiple Unified CVP Call Servers, the SIP Proxy Server would be configured with multiple routes for load balancing and redundancy. It is possible for CiscoIOS Gateways to provide load balancing and redundancy without a SIP Proxy Server. The following example shows a CiscoIOS Gateway configuration with multiple dial peers so that the calls are load balanced across three Unified CVP Call Servers.

```
dial-peer voice 1001 voip
 session target ipv4:10.4.33.131
 preference 1
 ...
dial-peer voice 1002 voip
 session target ipv4:10.4.33.132
 preference 1
 ...
dial-peer voice 1003 voip
 session target ipv4:10.4.33.133
 preference 1
 ...
```

DNS SRV records allow an administrator to configure redundancy and load balancing with finer granularity than with DNS round-robin redundancy and load balancing. A DNS SRV record allows you to define which hosts should be used for a particular service (the service in this case is SIP), and it allows you to define the load balancing characteristics among those hosts. In the following example, the redundancy provided by the three dial peers configured above is replaced with a single dial peer using a DNS SRV record. Note that a DNS server is required in order to do the DNS lookups.

```
ip name-server 10.4.33.200
 dial-peer voice 1000 voip
 session target dns:cvp.cisco.com
```

With CiscoIOS Gateways, it is possible to define DNS SRV records statically, similar to static host records. This capability allows you to simplify the dial peer configuration while also providing DNS SRV load balancing and redundancy. The disadvantage of this method is that if the SRV record needs to be changed, it must be changed on each gateway instead of on a centralized DNS Server. The following example shows the configuration of static SRV records for SIP services handled by cvp.cisco.com, and the SIP SRV records for cvp.cisco.com are configured to load balance across three servers:

```
        ip host cvp4cc2.cisco.com 10.4.33.132
        ip host cvp4cc3.cisco.com 10.4.33.133
        ip host cvp4cc1.cisco.com 10.4.33.131
```

(SRV records for SIP/TCP)

```
        ip host _sip._tcp.cvp.cisco.com srv 1 50 5060 cvp4cc3.cisco.com
        ip host _sip._tcp.cvp.cisco.com srv 1 50 5060 cvp4cc2.cisco.com
        ip host _sip._tcp.cvp.cisco.com srv 1 50 5060 cvp4cc1.cisco.com
```

(SRV records for SIP/UDP)

```
        ip host _sip._udp.cvp.cisco.com srv 1 50 5060 cvp4cc3.cisco.com
        ip host _sip._udp.cvp.cisco.com srv 1 50 5060 cvp4cc2.cisco.com
        ip host _sip._udp.cvp.cisco.com srv 1 50 5060 cvp4cc1.cisco.com
```

Courtesy Callback

The Courtesy Callback (CCB) feature, available in Unified CVP, reduces the time callers have to wait on hold/in queue. The feature allows the system to offer callers who meet certain criteria. For example, callers with the possibility of being in queue for more than X minutes, the option to be called back by the system when the wait time would be considerably shorter.

If the caller decides to be called back by the system, then they leave their name and phone number. When the system determines that an agent is available (or are available soon), then a call is placed back to the caller. The caller must answer the call and indicate that they are the caller. The caller is connected to the agent after a short wait.

Use this page to identify the required Unified CVP Reporting Server for which Courtesy Callback data is stored and deploy them to the selected Unified CVP Call Servers. The configured values for Courtesy Callback are stored as cached attributes.

Configure the Courtesy Callback feature on the following servers/gateways:

- Ingress Gateway (IOS configuration)
- VXML Gateway (IOS configuration)
- Reporting Server (through the Unified CVP Operations Console)
- Media Server (upload of Courtesy Callback media files)
- Unified CVP VXML Server (upload of Call Studio Scripts)
- Unified ICM (through the ICM script)

Note Ensure that the registry is modified to use the CVP keystore. CCB uses CVP keystore instead of Java keystore in 12.0(1) and higher releases.

Callback Criteria

In your callback script, you can establish criteria for offering a caller a courtesy callback. Examples of callback criteria include:

• Number of minutes a customer is expected to wait in queue that exceeds a maximum number of minutes (based on your average call handling time per customer)

Note The included example scripts use this method for determining callback eligibility.

• Assigned status of a customer (for example, a callback can be given on the basis of status of a customer).

• The service a customer has requested (sales calls, or system upgrades, for example, may be established as callback criteria).

Note
• CCB does not support the use of SRTP.

• ANI provides a caller extension/number which is required for CCB. If ANI is null or anonymous, CCB cannot be offered to the callers.

Modifiable Example Scripts and Sample Audio Files

The courtesy callback feature is implemented using Unified CCE scripts. Modifiable example scripts are provided. These scripts determine whether or not to offer the caller a callback, depending on the callback criteria. Sample audio files are also provided.

The example scripts and audio files are located on the CVP installation media in the `\CVP\Downloads and Samples\` folder.

Following files are provided:

• `CourtesyCallback.ICMS`, the ICM script, in the `ICMDownloads` subfolder.

• `CourtesyCallbackStudioScripts.zip`, a collection of Call Studio scripts, in the `helloStudio` Samples subfolder.

Following example scripts are provided:

• BillingQueue: Plays queue music to callers. Can be customized.

• Callback Engine: Keeps the VoIP leg of the call alive when the caller elects to receive the callback (and hangs up) and when the caller actually receives the callback. Cannot be customized or modified.

• CallbackEntry: Initial IVR when caller enters the system and is presented with opportunity for a callback. Can be customized.

• **CallbackQueue:** Handles the keepalive mechanism for the call when callers are in queue and listening to the music played by BillingQueue. Do **not** modify this script.

• CallbackWait: Handles IVR portion of call when caller is called back. Can be customized.

• `CCBAudioFiles.zip`, in the `CCBDownloads` subfolder, contains sample audio files that accompany the sample studio scripts.

Courtesy Callback Configuration

Configure Courtesy Callback

Procedure

Step 1   Log in to the Operations Console and select **System** > **Courtesy Callback**.

Step 2   Select the required Unified CVP Reporting Server, if configured, from the drop-down list.

> **Note**   If you leave the selection blank, no Reporting Server is associated with the Courtesy Callback deployment.

Step 3   (Optional) Check the **Enable secure communication with the Courtesy Callback database** check box to secure the communication between the Call Server and Reporting Server used for Courtesy Callback.

Step 4   In the **Dialed Number Configuration** section:

The Dialed Number Configuration of Courtesy Callback allows you to restrict the dialed numbers that callers can enter when they are requesting a callback. For example, it can stop a malicious caller from having Courtesy Callback dial **911**. The following table lists the configuration options for the **Dialed Number Configuration**:

Table 7: Configuration Options for Dialed Number Configuration

Field	Description	Default
Allow Unmatched Dialed Numbers	This checkbox controls whether or not dialed numbers that do not exist in the **Allowed Dialed Numbers** field can be used for a callback. By default, this is unchecked. If no dialed numbers are present in the **Allowed Dialed Numbers** list box, then **Courtesy Callback does not allow any callbacks**.	Unchecked - Callbacks can only be sent to dialed numbers listed in the **Allowed Dialed Numbers** list.
Allowed Dialed Numbers	The list of allowed dialed numbers to which callbacks can be sent. You can use dialed number patterns; for example, `978>` allows callbacks to all phone numbers in the area code *978*. To Add/Remove Dialed Numbers: • To Add a number to the list of allowed dialed numbers - Enter the dialed number pattern in the **Dialed Number (DN):** field and click **Add**. • To remove a number from the list - Highlight the number and click **Remove**.	Empty - If **Allow Unmatched Dialed Numbers** is *not* checked, and this list remained empty, then no callbacks can be made.

Field	Description	Default
Denied Dialed Numbers	The list of denied dialed numbers to which callbacks are never sent. You can use dialed number patterns; for example, 555> allows callbacks to all phone numbers in the area code 555. To Add/Remove Dialed Numbers: • To Add a number to the list of denied dialed numbers - Enter the dialed number pattern in the **Dialed Number (DN):** field and click **Add**. • To remove a number from the list - Highlight the number and click **Remove**. Denied numbers takes precedence over allowed numbers. • Wildcarded DN patterns can contain "." and "X" in any position to match a single wildcard character. **Note** Small letter "x" cannot be used as a wildcard. • Any of the wildcard characters in the set ">*!T" match multiple characters but can only be used as trailing values because they always match all remaining characters in the string. • The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match. • When the number of characters are matched equally by wildcarded patterns in both the Allowed Dialed Numbers and Denied Dialed Numbers lists, precedence is given to the one in the Denied Dialed Numbers list.	The Denied Dialed Numbers window is prepopulated if your local language is "en-us"(United States, English). Be sure to add any additional numbers you want to deny.
Maximum Number of Calls Per Calling Number	The default value is 0, which is equivalent to an unlimited number of callbacks offered per calling number. The maximum value is 1000. This setting allows you to limit the number of calls, from the same calling number that are eligible to receive a callback when there are outstanding callbacks already waiting for the same number. If this field is set to a positive number (X), then the courtesy callback "Validate" element only allows X callbacks per calling number to go through the "preemptive" exit state at any time. If there are already X callbacks offered for a calling number, new calls go through the "none" exit state of the "Validate" element. In addition, if no calling number is available for a call, the call always goes through the "none" exit state of the "Validate" element.	0

Step 5 Click the **Call Server Deployment** tab to view a list of available call servers and to select a Unified CVP Call Server to associate with Courtesy Callback.

Step 6 Click **Save & Deploy**.

Note	Click **Save** to save the configuration to the Operations Console database and configure Courtesy Callback later.

Configure Ingress Gateway for Courtesy Callback

The ingress gateway where the call arrives is the gateway that processes the pre-emptive callback for the call, if the caller elects to receive a callback.

Note	A sip-profile configuration is needed on ISR for the courtesy callback feature, only when deploying an IOS-XE version affected by CSCts00930. For more information on the defect, access the Bug Search Tool at https://sso.cisco.com/autho/forms/CDClogin.html.

For more information about sip-profile configuration, see *Design Guide for Cisco Unified Customer Voice Portal,* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-implementation-design-guides-list.html.

Procedure

Step 1 Login to the CVP OAMP Operations Console (from the CVP OAMP VM), using this syntax:

```
https://<server_ip>:9443/oamp.
```

Step 2 Copy survivability.tcl from the Operations Console to the flash memory of the gateway. Using the Operations Console, perform the following:

a) Select: **Bulk Administration** > **File Transfer** > **Scripts and Media**.
b) In Device Association, for **Select Device Type** select: **Gateway**.
c) Select all the Ingress gateways.
d) From the default gateway files, highlight: **survivability.tcl**.
e) Click **Transfer**.

Step 3 Log into the ingress gateway.

Step 4 Configure Call Survivability. See Call Survivability for details.

Step 5 To add services to the gateway, ensure that the enabled-config application mode is turned on. Type these commands at the gateway console:

```
GW81#en
GW81#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
GW81(config)#application
GW81(config-app)#
```

Step 6 Add the following to the survivability service:

```
param ccb id:<host name or ip of this gateway>;loc:<location name>;trunks:<number of callback
trunks>
```

Where the definitions of the preceding fields are:

- *id*: A unique identifier for this gateway and is logged to the database to show which gateway processed the original callback request.

- *loc*: An arbitrary location name specifying the location of this gateway.

- *trunks*: The number of DS0's reserved for callbacks on this gateway. Limit the number of T1/E1 trunks to enable the system to limit the resources allowed for callbacks.

The Courtesy Callback(CCB) *trunks* param configuration on the ingress gateway should be calculated based on CCB call parameters by including the *average CCB call duration* and the *fixed throttling period,* to ensure effective utilization of trunks between CCB and non-CCB calls.

The trunk value is given by the equation: Number of DS0 channels * (Throttling period/Average call duration)

Example

To dedicate a maximum of 10 DS0 channels for CCB calls, if you consider the following:

- The concurrent CCB calls at any given point is 10.

- The average CCB call duration is 900 seconds which includes the callback registration, callback offered, and talk time of called back user.

- The fixed throttling period is 1800 seconds.

Then, the trunk value will be 10 * (1800/900) = 20

The following example shows a basic configuration:

```
service cvp-survivability flash:survivability.tcl
param ccb id:10.86.132.177;loc:doclab;trunks:1
!
```

If you are updating the survivability service, or if this is the first time you created the survivability service, remember to load the application using the command:

```
call application voice load cvp-survivability
```

Step 7   Create the incoming dial peer, or verify that the survivability service is being used on your incoming dial peer. For example:

```
dial-peer voice 978555 pots
service cvp-survivability
incoming called-number 9785551234
direct-inward-dial
!
```

Note: We support both POTS and VoIP dial peers that point to a service provider.

Step 8   Create outgoing dial peers for the callbacks. These are the dial peers that place the actual call back out to the PSTN. For example:

```
dial-peer voice 978554 pots
destination-pattern 978554....
no digit-strip
port 0/0/1:23
!
```

Step 9   Use the following configuration to ensure that SIP is set up to forward SIP INFO messaging:

```
voice service voip
signaling forward unconditional
```

Note   The default value for the estimated wait time (EWT) for Courtesy Callback is 90 minutes (5400 seconds). This can be configured up to four hours (14400 seconds). This is applicable for both static route and dynamic route configurations. For more information, see Configure Courtesy Callback up to Four Hours, on page 45.

Related Topics

Call Survivability

Configure VXML Gateway for Courtesy Callback

Procedure

Step 1   Copy **cvp_ccb_vxml.tcl** from the Operations Console to the flash memory of the gateway. Using the Operations Console:

a) Select **Bulk Administration** > **File Transfer** > **Scripts and Media**.

b) On the **General** tab, select a device association by selecting **Gateway** from the **Select Device Type**drop-down box.**Gateway**.

c) From the default gateway files, highlight **cvp_ccb_vxml.tcl**.

d) Click **Transfer**.

Step 2   To add services to the gateway, ensure that the enabled-config application mode is turned on. Type the following commands at the gateway console:

```
GW81#en
GW81#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
GW81(config)#application
GW81(config-app)#
```

Step 3   Add the cvp_cc service to the configuration:

```
service cvp_cc flash:cvp_ccb_vxml.tcl
```

The service does not require any parameters.

Load the application with the command:

```
call application voice load cvp_cc
```

Note   The media-activity detection feature should be turned off in the VXML Gateway to successfully callback the caller. With media-activity enabled on the VXML Gateway, the `cvp_cc` service disconnects the waiting callback calls after 'ip rtcp report interval' * 1000 milliseconds interval. This configuration becomes important in a co-located Ingress/VXML setup where media inactivity timers are always enabled. In such scenarios, the 'ip rtcp report interval' has to be increased to support the maximum allowable waiting for a callback call as defined by the solution requirements.

Step 4   On the VoIP dial-peer that defines the VRU leg from Unified ICM, verify that the codec can be used for recording. The following example shows that g711ulaw can be used for recording in Courtesy Callback:

```
dial-peer voice 123 voip
service bootstrap
incoming called-number 123T
dtmf-relay rtp-nte
codec g711ulaw
no vad
!
```

In other words, this example shows the g711ulaw codec set on the 123 voip dial-peer. Note that the codec must be specified explicitly. A codec class cannot be used because recording will not work.

Step 5   Use the following configuration to ensure that SIP is setup to forward SIP INFO messaging:

```
voice service voip
signaling forward unconditional
```

Step 6   VXML 2.0 is required to play the beep to prompt the caller to record their name in the BillingQueue example script. Add the following text to the configuration so the VXML Server uses VXML 2.0:

```
vxml version 2.0
```

Note   Whenever vxml version 2.0 is enabled on the gateway,vxml audioerror is off by default. When an audio file cannot be played, error.badfetch will not generate an audio error event. To have the gateway generate an error.badfetch event when a file cannot be played, enable vxml audioerror in your gateway configuration. The following example uses config terminal mode to add both commands:

```
config t
vxml version 2.0
vxml audioerror
exit
```

Configure Reporting Server for Courtesy Callback

Before you begin

Install and configure a Reporting Server.

Note   To install Reporting Server, see *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*. To configure Reporting Server, see Reporting Server Configuration chapter.

Note   The *RPT.DynamicEwtCalculationEnabled* variable is configured in the Unified CVP Reporting Server properties at `c:\cisco\cvp\conf`. This variable decides whether the dynamic calculation for estimated waiting time (EWT) is enabled or not. The variable is set to *false* by default. You may change the configuration, if needed:

- *RPT.DynamicEwtCalculationEnabled = true* – Unified ICM decides the EWT based on the average call handling time and the number of agents available. Unified CVP recalculates the EWT based on the dynamics of the contact center's incoming call rate and leaving rate.

- *RPT.DynamicEwtCalculationEnabled = false* – Unified ICM provides a static EWT, for example 15 minutes, and the Unified CVP uses this static EWT for calling back the caller. Unified CVP doesn't use the agent availability to alter the EWT.

Procedure

Step 1   On the Operations Console page, select **System** > **Courtesy Callback**.

On the **General** tab, you can:

- Select the Reporting Server for Courtesy Callback.

- Enable secure communication with the Courtesy Callback database.

- Configure allowed and disallowed dialed numbers.

Step 2   On the Courtesy Callback Configuration page, select the **Unified CVP Reporting Server** drop-down list, and select the Reporting Server to use for storing Courtesy Callback data.

Note   If you leave the selection blank, no Reporting Server is associated with the Courtesy Callback deployment.

Step 3   (Optional) Enable secure communication with the callback reporting database. Check the **Enable secure communication with the Courtesy Callback database** check box.

Step 4   Configure allowed and denied dialed numbers. These are the numbers that the system *should* and *should not* call when it is making a courtesy callback to a caller. Also, configure the Maximum Number of Calls Per Calling Number.

Use the following table to configure these fields:

Initially, there are **no** allowed dialed numbers for the Courtesy Callback feature. which means:

- **Allow Unmatched Dialed Numbers** is deselected.

- And, the **Allowed Dialed Numbers window** is empty.

This initial configuration is intentional; you must specifically enable the dialed numbers allowed for your deployment.

If you wish to allow **all** dialed numbers *except* those that are specifically listed in the Denied Dialed Numbers box, check **Allow Unmatched Dialed Numbers** .

Otherwise, add specific allowed number to the Allowed Dialed Numbers box. Refer to the Operations Console online help for detailson how to add specific allowed numbers, and for allowed valid dialed number shortcut patterns.

> **Note** The Denied Dialed Numbers window is prepopulated if your local language is "en-us" (United States, English). Be sure to add any additional numbers you want to deny.

- Wildcarded DN patterns can contain "." and "X" in any position to match a single wildcard character.

- Any of the wildcard characters in the set ">*!T" will match multiple characters but can only be used for trailing values because they will always match all remaining characters in the string.

- The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match.

- When the number of characters are matched equally by wildcarded patterns in both the Allowed Dialed Numbers and Denied Dialed Numbers lists, precedence is given to the one in the Denied Dialed Numbers list.

Step 5 Adjust the "Maximum Number of Calls per Calling Number" to the desired number. By default, this is set to 0 and no limit is imposed.

This setting allows you to limit the number of calls, from the same calling number, that are eligible to receive a callback. If this field is set to a positive number (X), then the courtesy callback "Validate" element only allows X callbacks per calling number to go through the "preemptive" exit state at any time. If there are already X callbacks offered for a calling number, new calls go through the "none" exit state of the "Validate" element. In addition, if no calling number is available for a call, the call always goes through the "none" exit state of the "Validate" element."

Step 6 Click the **Call Server Deployment** tab and move the Call Server you want to use for courtesy callbacks from the **Available** box to the **Selected** box, as shown in the following screen shot :

Step 7 Click **Save & Deploy** to deploy the new Reporting Server configuration immediately.

If you click **Save**, the configuration is saved and is deployed after the Reporting Server restarts.

> **Note** If you are updating the courtesy callback configuration (for example, changing to a different Reporting Server), perform deployment during a scheduled maintenance period. Otherwise, restarting the Reporting Server could cause the cancellation of currently scheduled courtesy callbacks.

Configure Media Server for Courtesy Callback

Several Courtesy-Callback-specific media files are included with the sample scripts for Courtesy Callback. During the Operations Console installation , the media files are placed in the following directory:

```
%CVP_HOME%\OPSConsoleServer\CCBDownloads\CCBAudioFiles.zip
```

After CVP installation, the media files are located on the Operations Console in *%CVP_Home%*\OPSConsoleServer\. A typical value for *%CVP_Home%* is C:\Cisco\CVP.

CCBAudioFiles.zip has callback-specific application media files in `C:\inetpub\wwwroot\en-us\app` and the media files for *Say it Smart* in `C:\inetpub\wwwroot\en-us\sys`.

Unzip the special audio files copy to a Media Server.

Note   If you selected the Media File installation option, during the Unified CVP installation, the audio files are unzipped and copied to `C:\inetpub\wwwroot\en-us\app` on the installation server.

Note   CCBAudioFiles.zip also contains media files for Say It Smart. During installation, these files are copied to `C:\inetpub\wwwroot\en-us\sys`. Copy these files to your media server, if you do not have them there already.

Note   The sample scripts are set up to use the default location of `http://<server>:<port>/en-us/app` for the audio files. Later in this configuration process, change the <server> and <port> parameters in the default location of the audio files in the example scripts to be your media server IP address and port number.

Configure Call Studio Scripts for Courtesy Callback

The Courtesy Callback feature is controlled by a combination of Call Studio scripts and ICM scripts. See the *Configuration Guide for Cisco Unified Customer Voice Portal* for details of the script logic.

Note   This example follows the BillingQueue example application.

Procedure

Step 1   Extract the example Call Studio Courtesy Callback scripts contained in CourtesyCallbackStudioScripts.zip to a folder on the computer that has Call Studio installed.

You can access the .zip file from the following two locations:

- From the Unified CVP install media in \CVP\Downloads and Samples\Studio Samples\CourtesyCallbackStudioScripts.

- From the Operations Console server in %CVP_HOME%\OPSConsoleServer\StudioDownloads.

Step 2   Each folder contains a Call Studio project having the same name as the folder. The five individual projects comprise the Courtesy Callback feature.

Do not modify the following scripts.

- CallbackEngine: Keeps the VoIP leg of the call alive when the caller elects to receive the callback (and hangs up) and when the caller actually receives the callback.

- CallbackQueue: Handles the keepalive mechanism for the call when callers are in queue and listening to the music played by BillingQueue.

Modify the following scripts to suit your business needs:

- BillingQueue: Determines the queue music played to callers.

- CallbackEntry: Modify the initial IVR treatment a caller receives when entering the system and is presented with an opportunity for a callback.

- CallbackWait: Modify the IVR treatment a caller receives when they respond to the callback.

Note   Do not change the CCB application names.

Step 3   Start Call Studio by selecting **Start** > **Programs** > **Cisco** > **Cisco Unified Call Studio**.

Step 4   In Call Studio, select **File** > **Import**.

Step 5   In the **Import** dialog box, expand the Call Studio folder and select **Existing Call Studio Project Into Workspace** .

Step 6   Click **Next**.

Step 7   In the **Import Call Studio Project From File System** dialog, browse to the location where you extracted the call studio projects. For each of the folders that are unzipped, select the folder (for example BillingQueue), and click **Finish**.

The project is imported into Call Studio. Repeat this action for each of the five folders.

When you have imported the five folders, you should see five projects in the **Navigator** window in the upper left corner.

Step 8   Update the Default Audio Path URI field in Call Studio to contain the IP address and port value for your Media Server.

For each of the Call Studio projects previously unzipped, complete the following steps:

a)   Select the project in the Navigator window of Call Studio.

b)   Click **Project** > **Properties** > **Call Studio** > **Audio Settings**.

c)   On the Audio Settings window, modify the Default Audio Path URI field by supplying your server IP address and port number for the *<Server>* and *<Port>* placeholders.

d)   Click **Apply**, and then click **OK**.

Step 9   (Optional) Billing Queue Project: Change the music played to the caller while on hold.

You can also create multiple instances of this project if you want to have different hold music for different clients, for example, BillingQueue with music for people waiting for billing, and SalesQueue with music for people waiting for sales. You also need to point to the proper version (BillingQueue or SalesQueue) in the ICM script. In the ICM script, the parameter queueapp=BillingQueue would also have a counterpart, queueapp=SalesQueue.

The CallbackEntry Project (in the following step) contains a node called SetQueueDefaults. This node contains the value Keepalive Interval which must be greater than the length of the queue music you use.

Step 10   Callback Entry Project: If desired, in the CallbackEntry project, modify the caller interaction settings in the SetQueueDefaults node.

This step defines values for the default queue. You can insert multiple SetQueueDefaults elements here for each queue name, if it is necessary to customize configuration values for a particular queue. If you do not have a SetQueueDefaults element for a given queue, the configuration values in the default queue are used.

Note   You can define a Callback_Set_Queue_Defaults node with **Queue Name** parameter set to default. Configuration defined in this default node will be picked whenever a queue type is encountered for which there are no explicitly defined values.

a) In the Call Studio Navigator panel, open the CallBackEntry project and double click **app.callflow** to show the application elements in the script window.

b) Open the Start of Call page of the script using the tab at the bottom of the script display window.

c) Select the SetQueueDefaults node.

d) In the **Element Configuration panel**, select the Setting tab and modify the following default settings as desired:

For the SetQueueDefaults element, the caller interaction values in the Start of Call and the Wants Callback elements, may be edited. For more information on the caller interaction values, see the Settings table in Chapter 10, Callback_Set_Queue_Defaults, in the *Element Specifications for Cisco Unified CVP VXML Server and Cisco Unified Call Studio* guide.

Step 11   Perform the following steps.

a. Set the path for the storage of recorded caller names.

b. Select app.callflow.

c. In the CallbackEntry project, on the Wants Callback page, highlight the Record Name node and click the **Settings** tab in the Element Configuration window of Call Studio.

d. In the Path setting, change the path to the location where you want to store the recorded names of the callers.

By default, Call Studio saves the path string in your VXML Server audio folder. If you are using the default path, you can create a new folder called Recordings in the `%CVP_HOME%\VXMLServer\Tomcat\webapps\CVP\audio\` folder on the VXML Server. If you are using IIS as your Media Server, create a new folder called Recordings in `C:\Inetpub\wwwroot\en-us\app` and set that as the path for recordings.

Step 12   Set the name of the Record name file.

From the CallbackEntry project on the Wants Callback page, highlight the **Add Callback to DB** node and select the **Settings** tab in the Element Configuration window of Call Studio.

Change the **Recorded name file** setting to match the location of the recording folder you created.

This setting references the URL of the recordings folder, whereas the Path setting references the file system path.

The AddCallback element setting in the CallbackEntry project is configured to do automatic recorded file deletions. If automatic recorded file deletion is not desired, then remove the value of the Recorded name path setting in the AddCallback element. This removal action assumes that you will be doing the deletion or management of the recorded file yourself.

Step 13   In the CallbackEntry project on the Callback_Set_Queue_Defaults node, be sure the keepalive value (in seconds) is greater than the length of the queue music being played. The default is 120 seconds.

Step 14   Save the **CallbackEntry** project.

Step 15   CallbackWait Project: Modifying values in the CallbackWait application.

In this application, you can change the IVR interaction that the caller receives at the time of the actual callback. The caller interaction elements in **CallbackWait** > **AskIfCallerReady (page)** may be modified. Save the project after you modify it. The WaitLoop retry count can also be modified from the default of six retries in the Check Retry element. This will allow a larger window of time to pass before the call is dropped from the application. It is used in a failure scenario when the CallbackServlet on the reporting server cannot be reached.

For instance, in a reboot or a service restart, this allows more time for the reporting server to reload the entry from the database when it is initializing. If the reporting server is not online within the retry window, then the entry will not be called back.

Step 16 Validate each of the five projects associated with the Courtesy Callback feature by right-clicking each Courtesy Callback project in the Navigator window and selecting **Validate**.

Step 17 Validate each of the five projects associated with the Courtesy Callback feature and deploy them to your VXML Server.

a) Right-click each Courtesy Callback project in the Navigator window and select **Validate**.

b) Right click each of the projects and click **Deploy**, then click **Finish**.

Step 18 Using windows explorer, navigate to `%CVP_HOME%\VXMLServer\applications`.

Step 19 For each of the five Courtesy Callback applications, open the project's admin folder in `%CVP_Home%\VXMLServer\applications`, and double-click **deployApp.bat** to deploy the application to the VXML Server.

Step 20 Verify that all the applications are running by going into `%CVP_HOME%\VXMLServer\admin` and double-clicking **status.bat**. All five applications should be listed under Application Name, and the status for each one should be Running.

> **Note** As an alternative to following steps 16-19 above, to deploy a VXML application to the VXML Server, you can also use the Bulk Administration VXML Applications feature. This way, you can deploy all the applications into a single archive, and then deploy them from OAMP in one click. This process is simpler and saves time. Bulk Administration deploys the application to the VXML Server, runs update-all-apps batch file, and then runs deploy-all-new-apps batch file.

CCE Script for Courtesy Callback

This section describes of the scripts used for the courtesy callback feature. There are nine numbered blocks or sets of blocks as identified below.
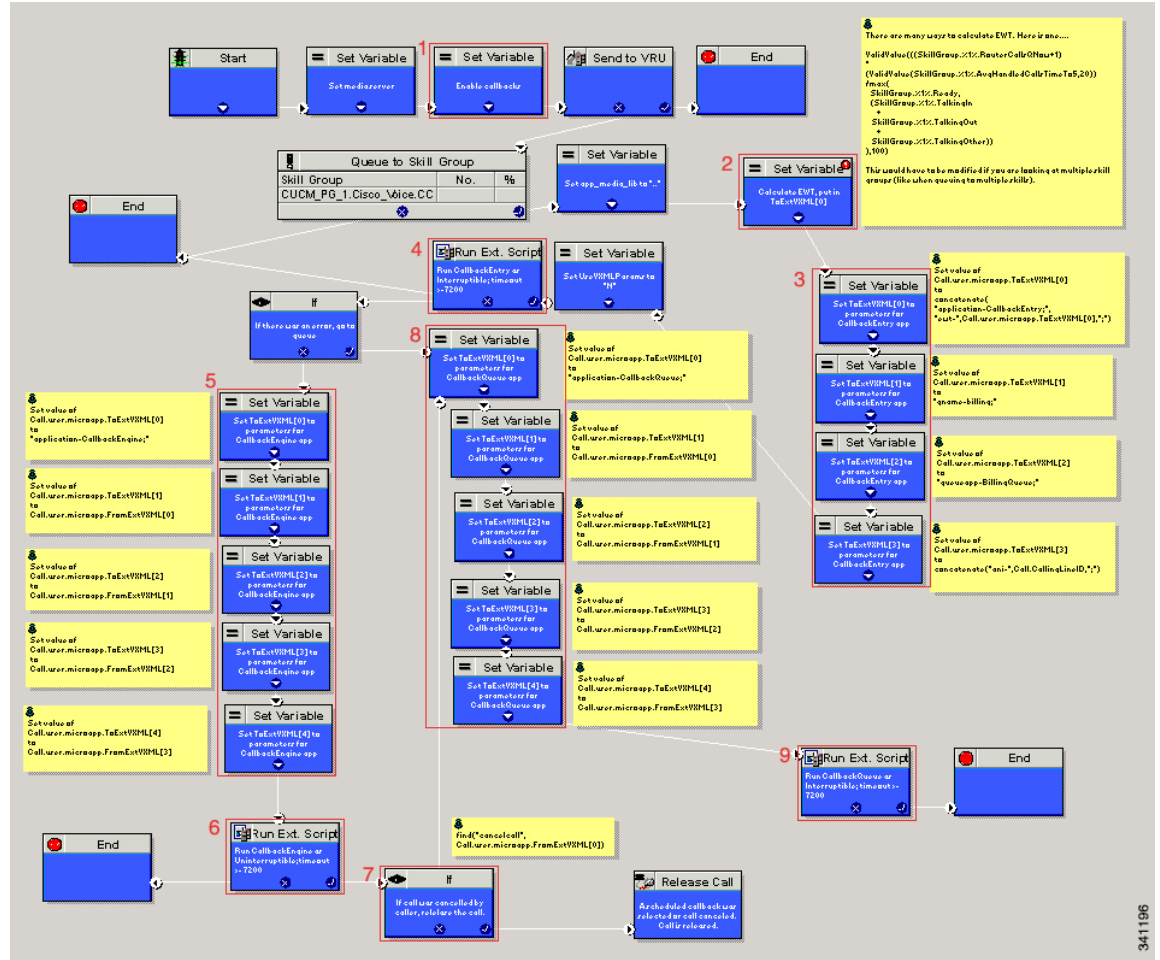
> **Note** In the following example, the yellow comment blocks describe the value being set and the location where the value is being sent.

Figure 1: Setting Value for Courtesy Callback

The numbered blocks in the above figure as described as follows:

- Block 1: Enable callback or shut it off.

- Block 2: Compute average wait time. Once the caller is *in queue*, calculate the Estimated Wait Time (EWT) for that queue and place the value in ToExtVXML[0].

  If there is poor statistical sampling because of sparse queues and the wait time cannot be calculated in the VXML Server, use the ICM-calculated estimated wait time.

  One method of calculating EWT (the method used in this example) is:

```
ValidValue(((SkillGroup.%1%.RouterCallsQNow+1)
*
(ValidValue(SkillGroup.%1%.AvgHandledCallsTimeTo5,20))

/max(
SkillGroup.%1%.Ready,
(SkillGroup.%1%.TalkingIn
+
SkillGroup.%1%.TalkingOut
+
SkillGroup.%1%.TalkingOther))
```

```
),100)
```

Modify this method if you are looking at multiple skill groups (when queuing to multiple skills).

• Block 3: Set up parameters to be passed.

• Block 4: Run this block and prompt the caller. If the caller does not accept the offer for a callback, keep the caller in the queue and provide queue music.

• Block 5: Set up variables. Call flow returns to this block if the caller elects to receive a callback. Otherwise, the call remains queuing in the queuing application (BillingQueue in this example) on the VXML Server.

• Block 6: Run external to Callback engine to keep the call alive. If the agent becomes available and there is no caller, then agent can't interrupt (do not want an agent to pick up and have no one there).

• Block 7: Has the caller rejected the callback call? If no, then go to block 8.

• Block 8: Set up variables.

• Block 9: Put caller briefly into queue (after caller accepts the actual callback call)

Overview of CCE Script Configuration for Courtesy Callback

The CCE script elements needed to enable Courtesy Callback are on the CVP Installation CD in *CVP\Downloads and Samples\ICM Downloads*. The script sample found there (CourtesyCallback) contains the necessary sample elements for the courtesy callback feature. However you must merge this script into your existing CCE scripts.

As a starting point and to run a simple test, import the script into the CCE script editor, validate it with the CCE script editor validation tool to locate nodes that need extra configuration (such as for Network VRU scripts and expanded call variables), and then modify the script according to your existing CCE environment.

1. Locate each queue point in every CCE script. For example: Queue To Skill Group, Queue to Enterprise Skill Group, Queue to Scheduled Target or Queue to Agent.

2. Categorize each queue point according to the pool of resources that it is queuing for. Each unique pool of resources will ultimately require a queue in VXML Server if Courtesy Callback is going to be offered for that resource pool. For example, using the following example, QueueToSkill X and QueueToSkill Z are queuing for the exact same resource pool (despite the different queuing order). Queue to Skill Y, however, is queuing to a different pool because it includes Skill Group D.

   • QueueToSkillGroup X is queuing for Skill Group A, B, C in that order.

   • QueueToSkillGroup Y is queuing for Skill Group A, C and D in that order.

   • QueueToSkillGroup Z is queuing for Skill Group C, B, A in that order.

3. Assign a unique name to each unique resource pool. In the above example, we can use names ABC and ACD as example names.

4. For each resource pool, decide whether callbacks will be allowed in that resource pool. If yes, then every occurrence of that resource pool in all ICM scripts must be set up to use VXML Server for queuing. This is to ensure that the Courtesy Callback mechanism in the VXML Server gets a full, accurate picture of each resource pool's queue.

5. For any queue point where Courtesy Callback will be offered, modify all CCE scripts that contain this queue point according to the guidelines in the following CCE script examples.

Configure CCE Script for Courtesy Callback

Many of the configuration items below relate to the numbered blocks in the diagram and provide understanding for CCE Script for Courtesy Callback. See CCE Script for Courtesy Callback, on page 40 for details. Steps that refer to specific blocks are noted at the beginning of the each step.

To configure CCE to use the sample Courtesy Callback CCE script, perform the following steps:

Procedure

Step 1 Copy the CCE example script, **CourtesyCallback.ICMS** to the CCE Admin Workstation.

The example CCE script is available in the following locations:

- On the CVP install media in `\CVP\Downloads and Samples\`.

- From the Operations Console in **%CVP_HOME%\OPSConsoleServer\ICMDownloads**

Step 2 Map the route and skill group to the route and skill group available for courtesy callback.
   a) In Script Editor, select **File** > **Import Script...**.
   b) In the script location dialog, select the **CourtesyCallback.ICMS** script and click **Open**.
   c) In the Import Script - Manual Object Mapping window, map the route and skill group to the route and skill group available for courtesy callback (identified previously).

Step 3 Once the script is open in Script Editor, open the **Set media server** node and specify the URL for your VXML Server.

For example: **http://10.86.132.139:7000/CVP**

Step 4 **Refer to Block #1:** A new ECC variable is used when determining if a caller is in queue and can be offered a callback. Define the **user.CourtesyCallbackEnabled** ECC variable for courtesy callback.
   a)
   b) On the CCE Admin Workstation, in the ICM Configuration Manager, use the Expanded Call Variable List tool.
   c) Create **user.CourtesyCallbackEnabled**.
   d) Set **Maximum Length** to 1.
   e) Check **Enabled**.
   f) Check **Persistent**.

This step assumes you have already created the standard ECC variables required for any Unified CVP installation. See Define Unified CVP ECC Variables.

Step 5 **Block #2:** If you wish to use a different estimated wait time (EWT), modify the calculation in block #2; you will need to do this if you use a different method for calculating EWT or if you are queuing to multiple skill groups.

Step 6 **Block #3:** Set up the parameters that will be passed to CallbackEntry (VXML application).

Note	This step assumes you have already configured the CCE and expanded call variables not related to Courtesy Callback.

Variable values specific to Courtesy callback include:

ToExtVXML[0] = concatenate("application=CallbackEntry",";ewt=",Call.user.microapp.ToExtVXML[0])

ToExtVXML[1] = "qname=billing";

ToExtVXML[2] = "queueapp=BillingQueue;"

ToExtVXML[3] = concatenate("ani=",Call.CallingLineID,";");

Definitions related to these variables are:

- CallbackEntry is the name of the VXML Server application that will be run.

- ewt is calculated in **Block #2** .

- qname is the name of the VXML Server queue into which the call will be placed. There must be a unique qname for each unique resource pool queue.

- queueapp is the name of the VXML Server queuing application that will be run for this queue.

- ani is the caller's calling Line Identifier.

Step 7   Create Network VRU Scripts.

Using the ICM Configuration Manager, Network VRU Script List tool, create the following Network VRU Scripts:

Block #4: Interruptible Script (agent can interrupt the caller on hold):

- Name: **VXML_Server_Interruptible**

- Network VRU: Select your Type 10 CVP VRU

- VRU Script Name: **GS,Server,V,interrupt**

- Timeout: **9000 seconds**

- Interruptible: **Checked**

Block #6:   Noninteruptible Script (agent cannot interrupt because no caller is available):

- Name: **VXML_Server_Noninterruptible**

- Network VRU: Select your Type 10 CVP VRU

- VRU Script Name: **GS,Server,V,nointerrupt**

- Timeout: **9000 seconds** (must be greater than the maximum possible call life in Unified CVP)

- Interruptible: **Not Checked**

Step 8   Verify that the **user.microapp.ToExtVXML ECC** variable is Enabled,Persistent, with at least 60 (chars) for the maximum length setting, set up as an array with a maximum array size of 5 elements.

Check **Array** and then a subfield for **Maximum array size** appears.

Step 9 Verify that the **user.microapp.FromExtVXML** variable is Enabled, Persistent, with at least 60 (chars) for the maximum length setting, set up as an array with a maximum array size of 4 elements.

Check **Array** and then a subfield for **Maximum array size** appears.

Step 10 Verify that you have at least one available route and skill group to map to the route and skill group in the example script.

Step 11 Save the script, then associate the call type and schedule the script.

Note For an example of scheduling the script refer to *Getting Started with Cisco Unified Customer Voice Portal* , the *Create a Call Type Manager Entity Routing Script and Call Schedule* topic.

Related Topics

Define Unified CVP ECC Variables

Configure Courtesy Callback up to Four Hours

The default value for the estimated wait time (EWT) for Courtesy Callback is 90 minutes (5400 seconds). This can be configured up to four hours (14400 seconds). This is applicable for both static route and dynamic route configurations. To configure EWT for Courtesy Callback for more than two hours, you need to change CVP, ICM, and Gateway configurations.

These configurations work with Cisco Virtualized Voice Browser (VVB).

Procedure

Step 1 To configure **CVP**, perform the following steps:
a) Go to **C:\Cisco\CVP\conf** folder.
b) Edit the *ivr.properties* file:

Set the following parameters to the desired value:

- **IVR.LastAccessTimeout=** <value between 5400 and 14400>

- **IVR.VBCallTimeout=** <value between 5400 and 14400>

c) Restart Call Server and VXML service from the Call Server.

Step 2 To configure **ICM**, perform the following steps:
a) Open **ICM Configuration Manager**.
b) Go to **Configuration Manage**, and then open **Network VRU Script List**.

Set the **Timeout Attributes**: **VXML_Server_Interruptible** and **VXML_Server_Noninterruptible** to the desired value.

c) Go to **Configuration Manage**, and then open **Media Routing Domain List**.

Set the **Max time in queue** attribute to the desired value.

d) Go to **regedit Router** > **CurrentVersion** > **Configuration** > **Queuing**.

Set the **MaxTimeInQueue** attribute to to the desired value.

    e)   Restart the **VRU PG** in **ICM**.

Step 3   To configure **Ingress Gateway**, run the following commands from the command prompt:

```
router# configure terminal
router(config)# sip-ua
router(config)#voice service voip
router(conf-voi-serv)#sip
router(conf-serv-sip)#session refresh
```