



## Interactive Voice Gateway (IVG) Cisco UCCE Configuration Guide Version 3.3-3.4

This page was not added to the PDF due to the following tag(s): article:topic-guide

## Required IVG Cisco UCCE Configuration

### Cisco Configuration

This discussion provides an overview of the initial configuration of Cisco components (using the Cisco Configuration Manager):

1. Create a network voice response unit (VRU). Required settings are:
  - Set VRU Type to **Type 8**.
2. Create a VRU peripheral gateway (PG). Required settings are:
  - When configuring a logical controller, set Client Type to **VRU**.
  - When configuring a peripheral, set Client Type to **VRU**.
  - When configuring a peripheral, set Call Control Map to **/ASSUME\_ANSWERED**.
  - When configuring a peripheral, select **Enable Post Routing**.
  - When configuring a routing client, set Client Type to **VRU**.
3. Create trunks and a trunk group (trunk groups, trunks, etc.) to be associated with a service. Required settings are:
  - When configuring a trunk group, set Trunk Count to **Use Trunk Data**.
  - When configuring a range of trunks, click **Multiple...**
  - When configuring a range of trunks, set First Trunk Number and Last Trunk Number to appropriate numbers. The current recommendation is to set this value equal to the number of available Callback inbound licenses.
  - When configuring a range of trunks, set Trunk Type to **Tie Line**.
4. Create a service. Required settings are:
  - When configuring a route, set Name to service name.
  - Add a peripheral target.
  - When configuring a label, set Routing Client Label to DNIS value and Label Type to **Normal**.
5. Enable a message (using Network VRU script lists) to be sent to Holly to notify that speech treatment is required. Required settings are:
  - Set VRU Script Name to **GS,V** for inbound scripts and Timeout to 180 seconds (recommended).
  - Select **Interruptible** to allow customer key selections.
6. Assign scripts (using call type lists) to the appropriate call types for appropriate dialed numbers:
7. Connect call types (using dialed number/script selector lists) to dialed numbers. Required setting are:
  - When configuring dialed numbers, set Routing Client to **Initial Routing Client**.
  - When configuring dialed numbers, set Media Routing Domain attribute to *cisco\_voice*.
  - When configuring dialed number mappings, set Calling Line ID and Call-Enter Digits to **All**.
8. Configure CM application gateways to connect to Queue Manager. Required settings are:

- When configuring gateway attributes, set Name to **VHT\_Gateway** (recommended), Type to **Gateway**, Preferred Side to **Side A**, Encryption to **None**, Fault Tolerance to **None** and Connection (**Duplex**, **Simplex** if non-duplex ICM system).
  - When configuring Connection Side A, set Address using format *IP\_address\_of\_QM\_server:port\_number*.
  - When configuring Connection Side A, select **In Service**.
  - When configuring Connection Side A timeouts, set Request to **10000**, Abandon to **15000**, Late to **10000**, and enable **Override Default**.
  - When configuring Connection Side A sessions, set Retry Timeout to **5000** and select **Override Default**. This value can be increased to avoid the need of resetting connection to the gateway and Queue Manager.
  - When configuring Connection Side A sessions, set Errors to **50** and select **Override Default**. This value can be increased to avoid the need of resetting connection to the gateway and Queue Manager.
  - Repeat Steps for Connection Side B.
9. Create translation routes to route calls:
- Inbound:
    - When configuring translation routes, set Type to **DNIS**.
    - When configuring a route, set Service Name to previously defined service name (from Step 4).
    - Add a peripheral target.
    - When configuring a label, set Routing Client to peripheral gateway name, Label to DNIS number and Label Type to **Normal**.
    - Create a sufficient number of translation routes to be able to allocate the appropriate number of routes to the TranslationRoutetoVRU blocks within inbound and outbound Cisco scripts.
    - Use the following Cisco-recommended formula to determine the appropriate number routes to allocate to **inbound** scripts.  
$$\text{maximum\_sustained\_inbound\_call\_rate\_per\_second} \times 20 = \text{appropriate\_number\_of\_routes}$$
Use the following
  - Outbound (Cisco Queuing Only)
    - Use the following Cisco-recommended formula to determine the appropriate number routes to allocate to **outbound** scripts.  
$$\text{maximum\_number\_of\_outbound\_call\_rate\_per\_second} \times 20 = \text{appropriate\_number\_of\_routes}$$

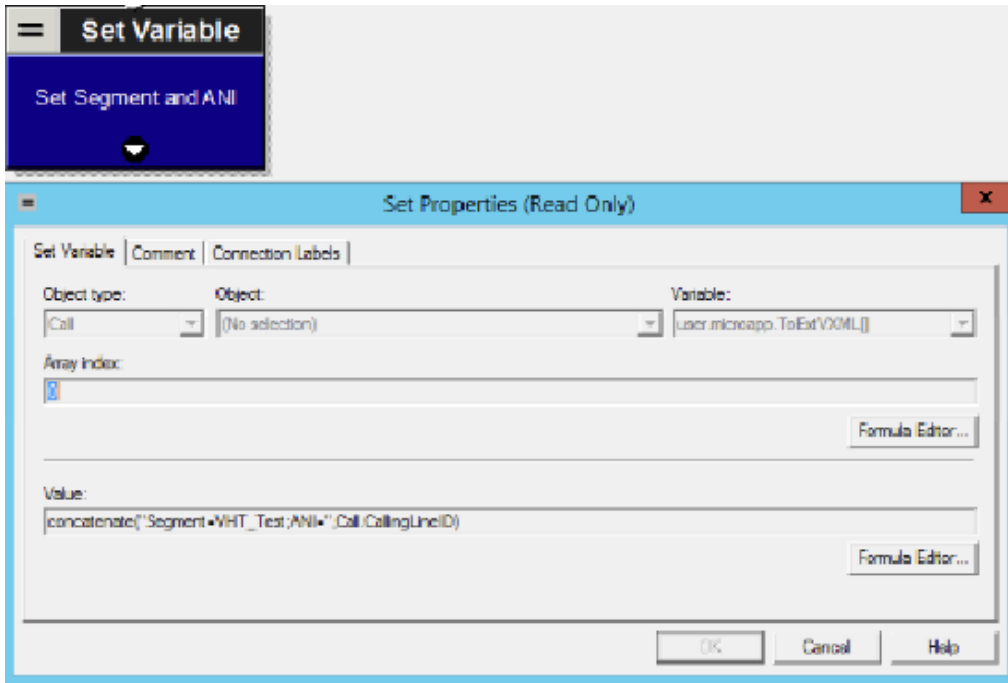
## Cisco ICM Scripting

The following logic is required for all call types that are considered for Callback treatment. Insert this logic prior to call queuing for inbound calls. Create a new script containing the necessary queuing logic (for ACD or CVP queuing). Use a script editor (Cisco Script Editor, Cisco ICM Internet Script Editor, etc.) to implement the following configuration.

### Inbound Call Logic (Performed Prior to Reaching IVG)

1. Set Segment and ANI in ECC Variable:
  - Used for calls that arrive in IVG. IVG uses the configured Segment value as the Segment for the Call. The

configured ANI value is the ANI announced to callers in IVG when using ANI detection.

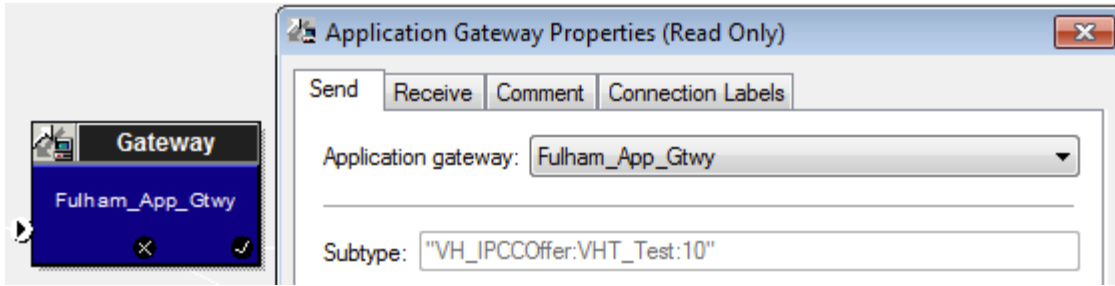


## 2. IPCC Offer Application Gateway:

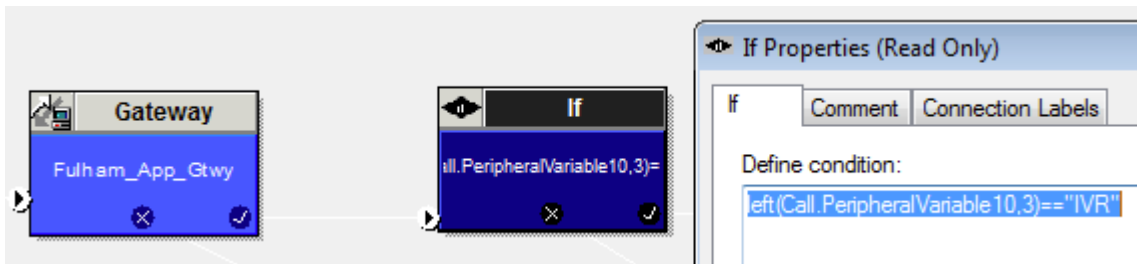
- Used for all call types. Presents Callback with a routing decision to inform ICM whether calls should route to IVG or Queue.
- The segment, found in bold below, is always found after VH\_IPCCOffer colong (:.) up to the next colon (:).  
**VH\_IPCCOffer:VHT\_Segment:10**  
 The number after the last colon (10 in this case) is the PVar that Callback should place the routing decision.
- Callback should place the routing decision.
- Send tab - Select CallingLineID, Dialed Number String, all PVars, and expanded call context variables (ECC Vars).
- Receive tab - Select PVar reserved for Virtual Hold use.

### Note:

Callback requires one PVar for use only for the life of a call.



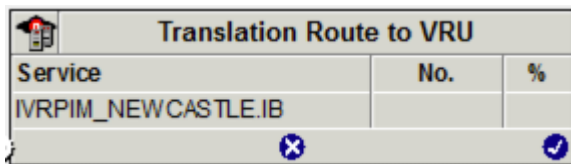
3. If Block for call routing based on Routing Decision on IPCC Offer AppGW response.
  - Segment calls intended for IVG vs calls going to Queue.
    - IVR = Send calls to IVG
    - QUE = Send calls to Queue
  - String is populated in PVar selected in AppGW. Read the first three characters (left values).



## Establishing Calls in IVG

1. Translation Routes to IVG:
  - Build translation routes to IVG systems.
  - Number of translation routes to build.
    - Number of inbound Callback licenses

### Single IVG Callback Solution



	Service	Consider If	Select Min Value Of	Route	Translation Route
1	IVRPIM_NEWCASTL	Peripheral.IVRPIM_NE	1=1	IVRPIM_NEWCASTL	NEWCASTLE_Tran

### Multiple IVG Callback Solution

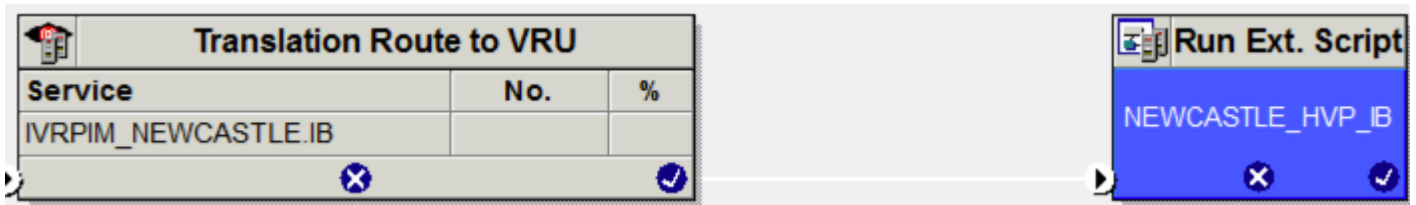
ICM balances the load between IVG solutions. Check for PIM is recommended for the Consider IF value.

Translation Route to VRU			
Service	No.	%	%
IVRPIM_HVP08.IB			▶
IVRPIM_HVP09.IB			▶
✕			

	Service	Consider If	Select Min Value Of	Route	Translation Route
1	IVRPIM_HVP08.IB	Peripheral.IVRPIM_HVP	1=1	IVRPIM_HVP08.IB	HVP08_TransRoute
2	IVRPIM_HVP09.IB	Peripheral.IVRPIM_HVP	1=1	IVRPIM_HVP09.IB	HVP09_TransRoute

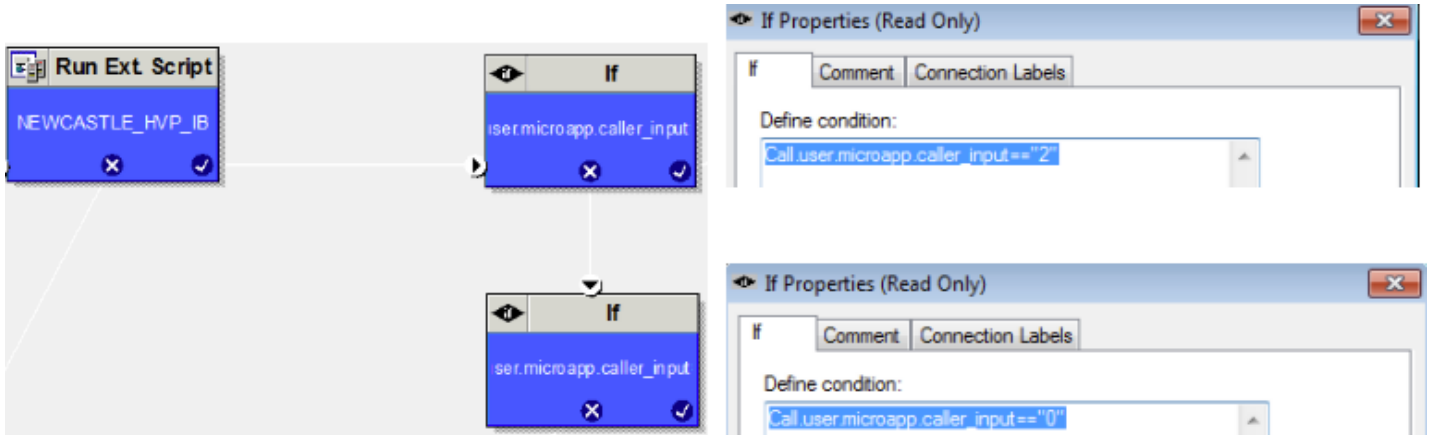
2. Run External Script:

- Used to deliver variables to VIS for new calls on the IVG Inbound VXML application.
- External Script Name GS.IVG.V <- Standard name but not used by IVG. Required value to be set by ICM.



3. If blocks for caller input:

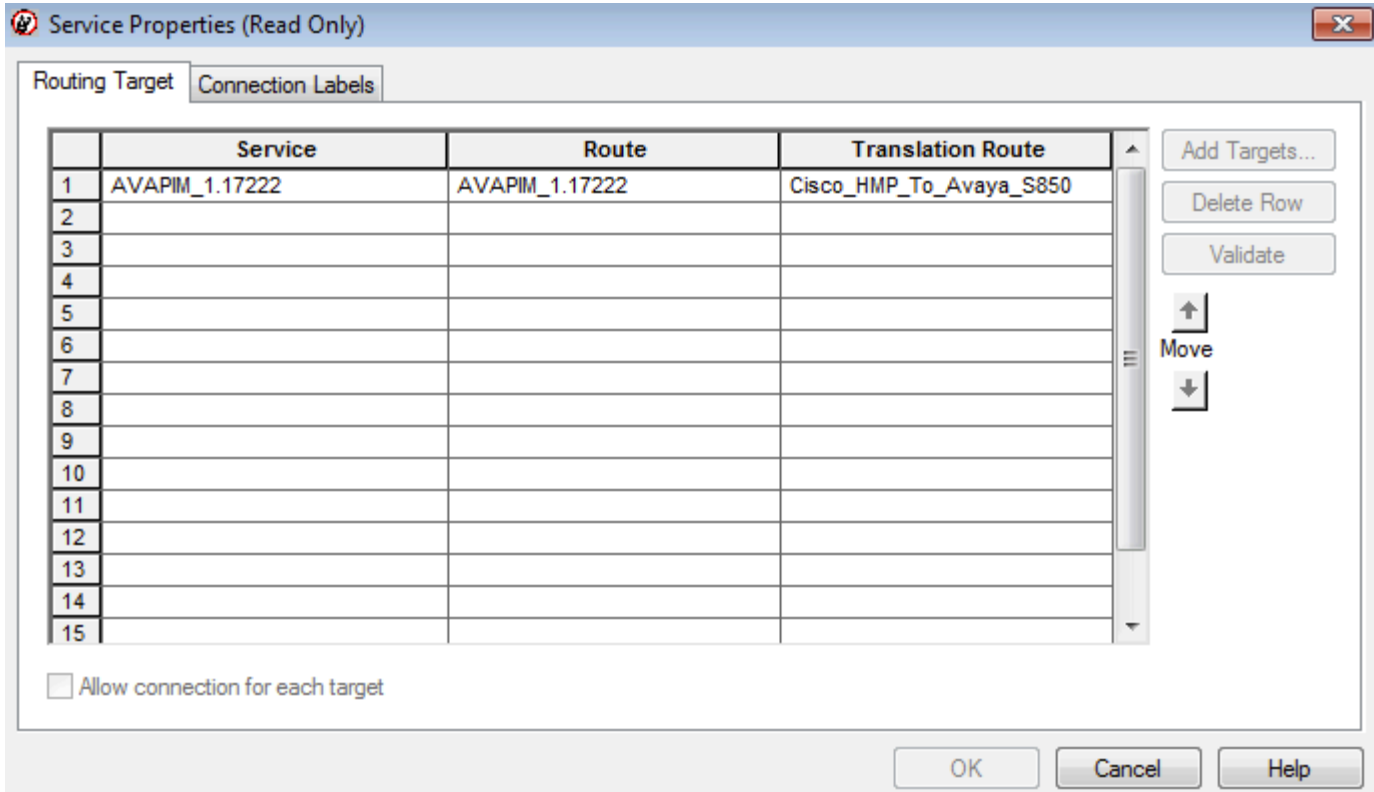
- 0 = Abandon in IVG - Disconnect.
- 1 = Choose hold/force hold - Medium priority queue.
- 2 = CBDC - Top priority queue.



## Queuing Logic

1. ACD queuing:
  - Service block needed after IF blocks to target a service to get the call back to the ACD.

Service		
Service	No.	%
AVAPIM_1.17222		



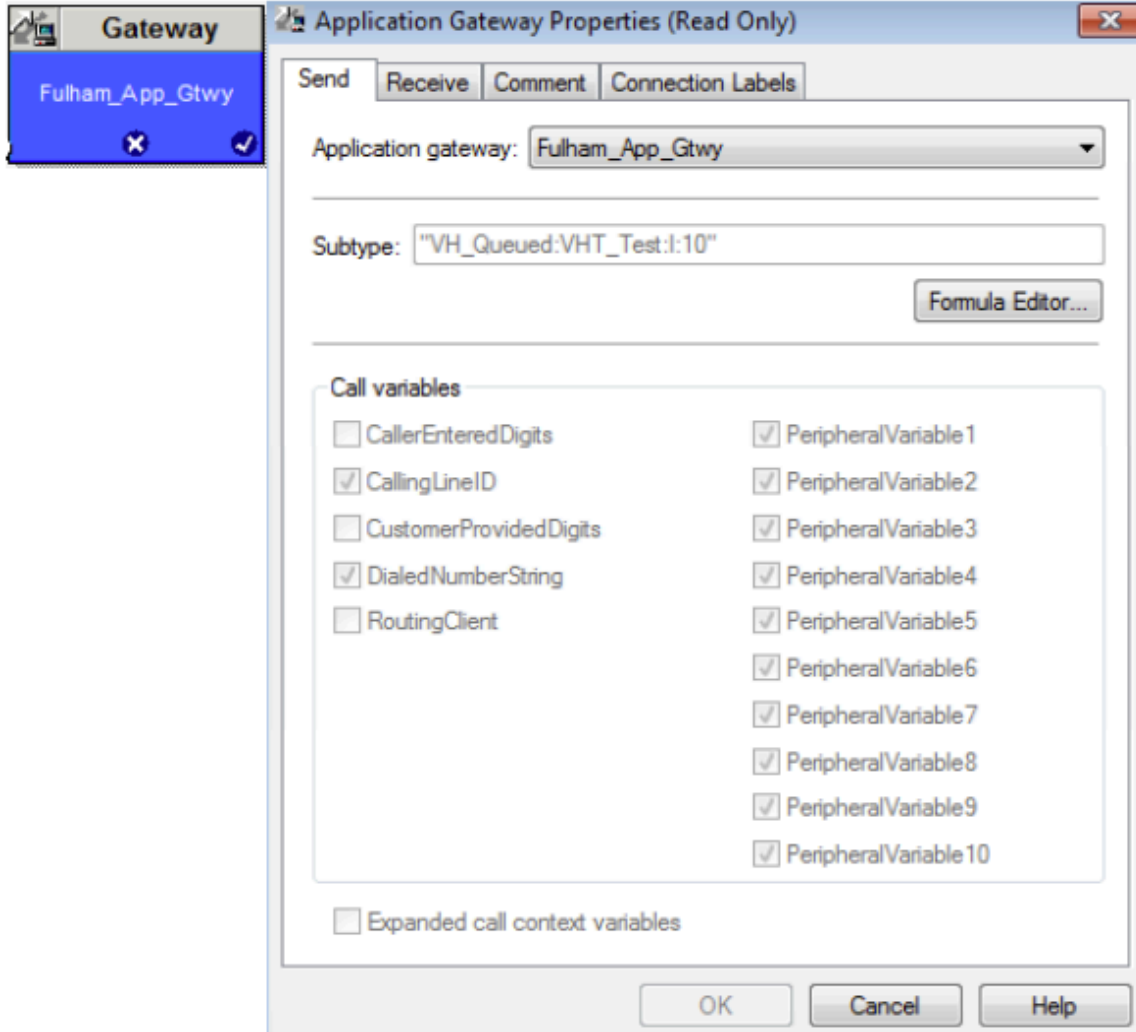
2. CVP queuing:

- Requires two Application Gateway blocks.

**VH\_Queued**

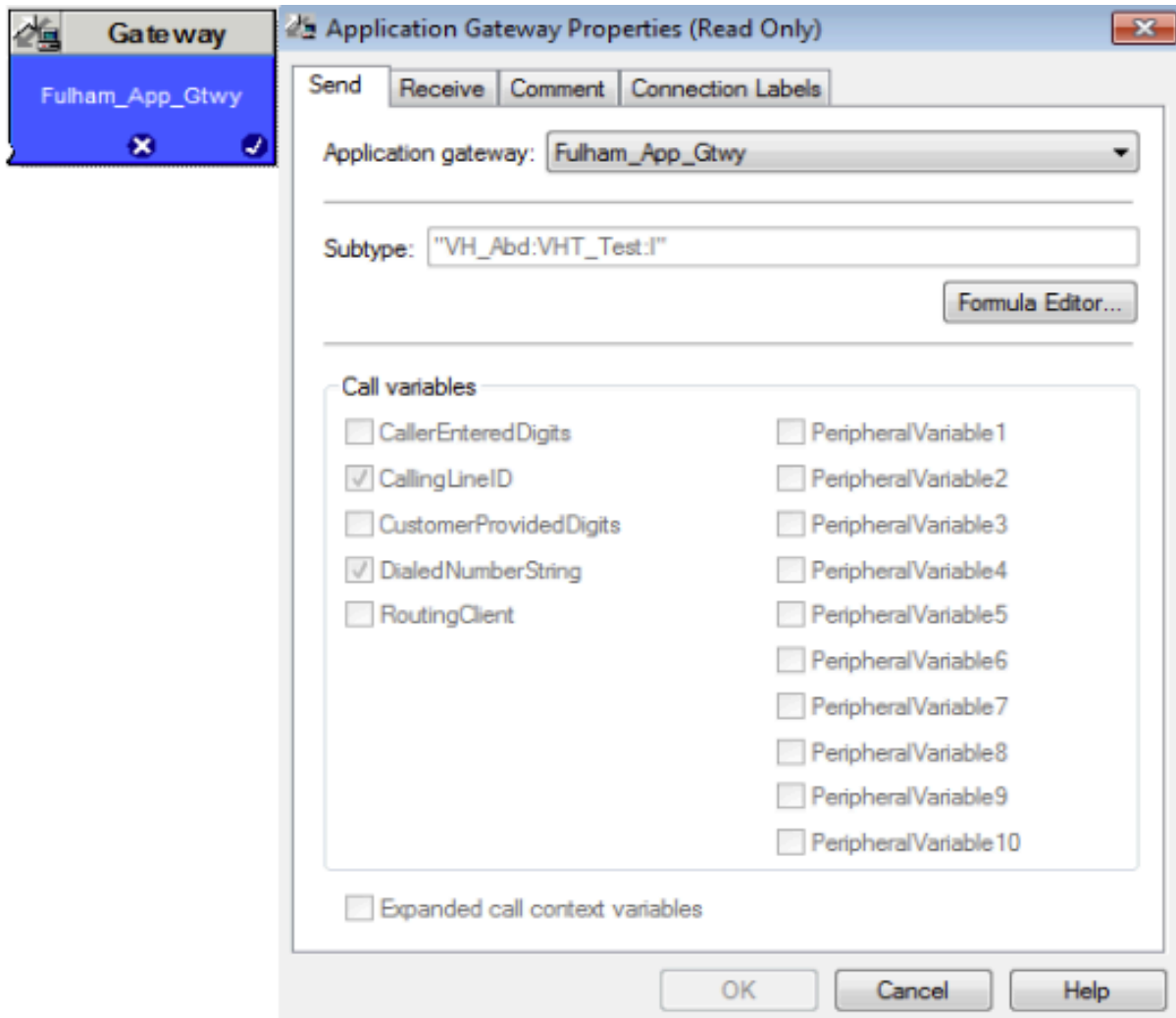
- Used by Callback to successfully mark a call as arriving in Queue.
- Should send a :I for inbound and :O for outbound (callbacks) at the end of the Application Gateway string.
- Send tab - Select CallingLineID and Dialed Number String.
- Receive tab - Select nothing.





## VH\_Abd

- Used by Callback to help mark calls as abandoned.
- Should send a **:I** for inbound and **:O** for outbound (Callbacks) at the end of the Application Gateway string.
- Send tab - Select CallingLineID and Dialed Number String.
- Receive tab - Select nothing.

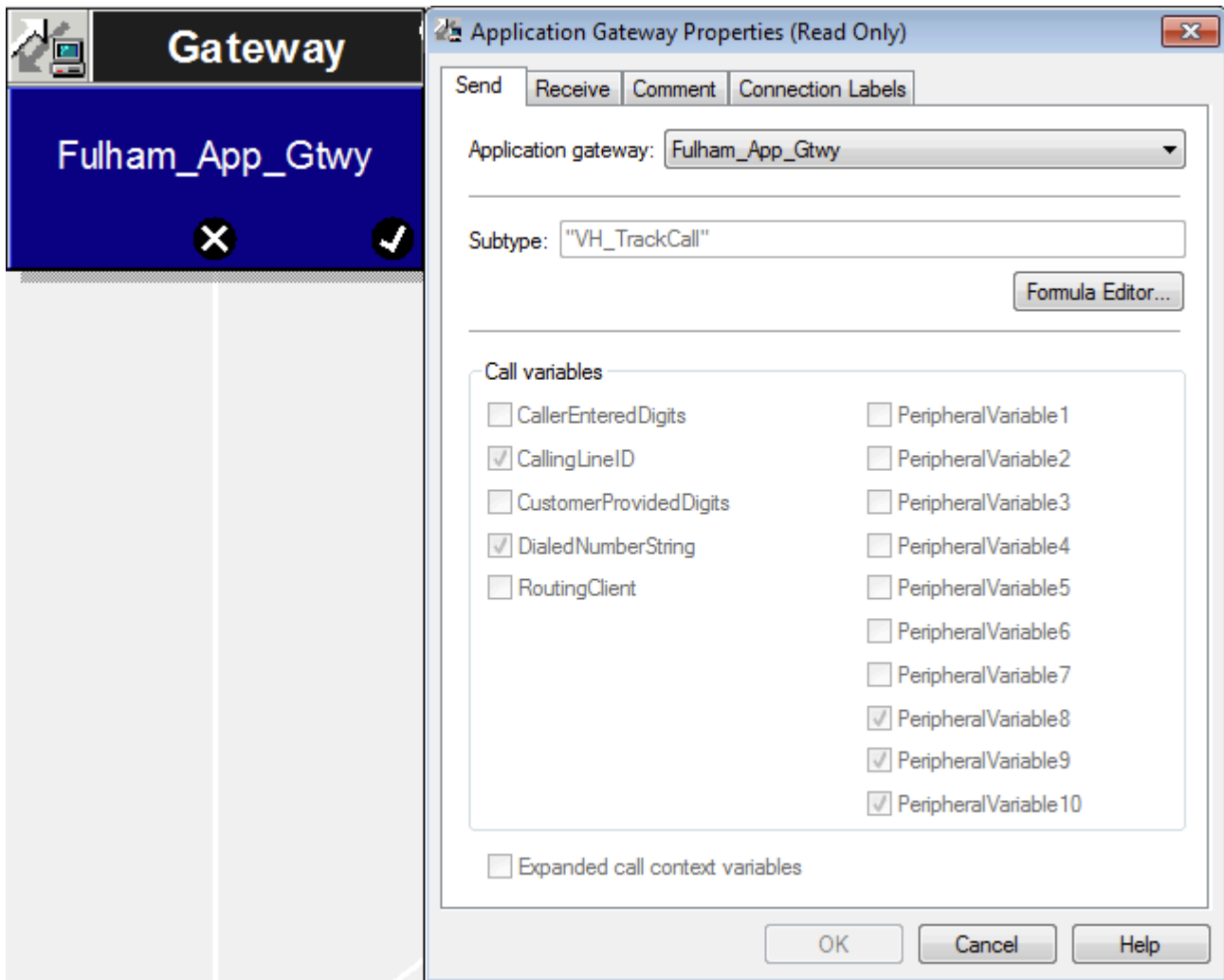


- After VH\_Queued, a timer is started.
- Timer stops when call is answered.
- If timer expires due to Callback not receiving the VH\_Abd event prior to the call being answered, the call is marked as abandoned.



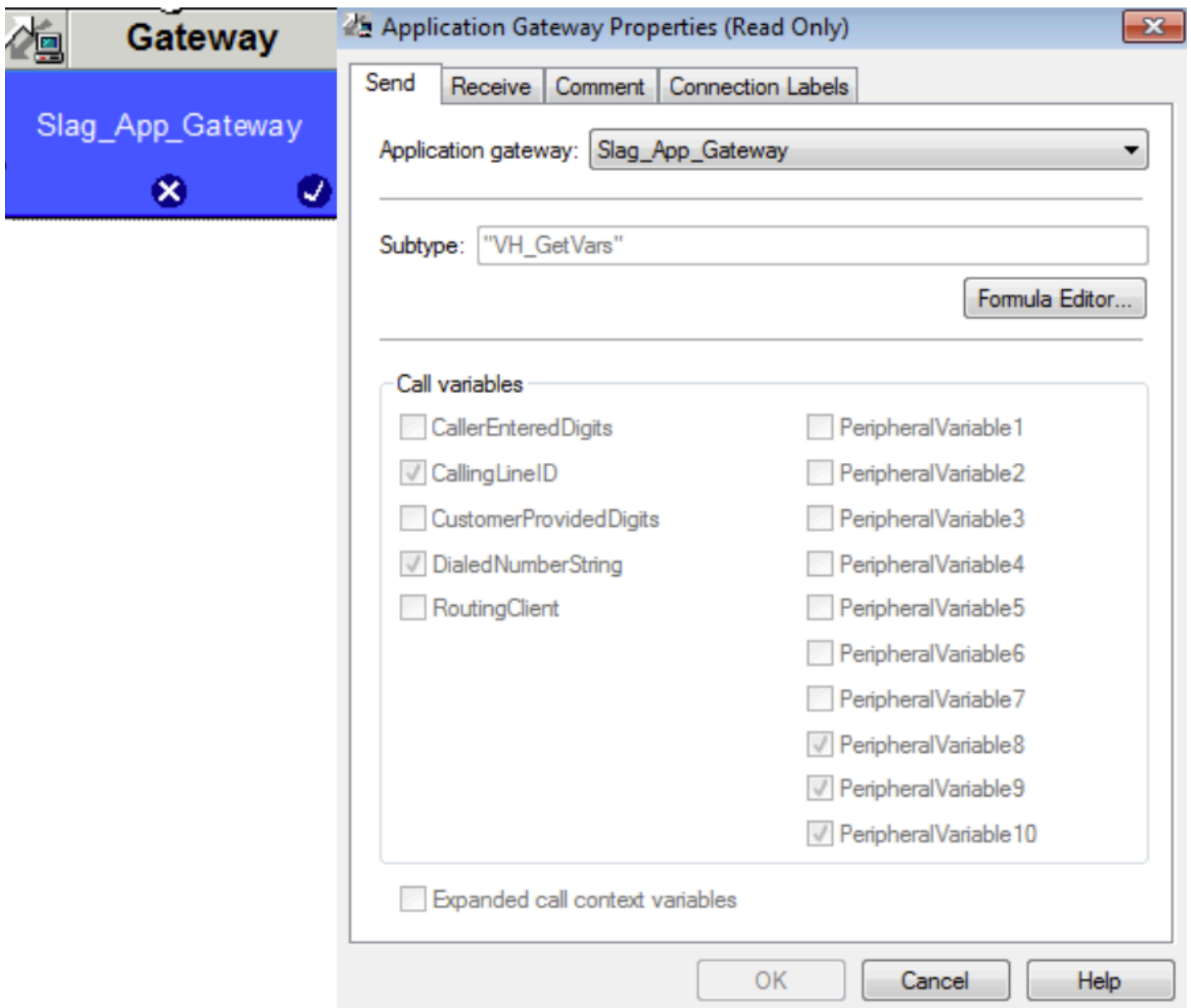
## Outbound Call Logic

1. Translation Route to VRU for CVP queuing:
  - The first blocks in the script callbacks to Translation Route calls to (CVP).
2. Track Call AppGW block:
  - This block is required for CVP and ACD queuing.
  - The first block for callbacks ready to queue to an agent should be an Application Gateway block that sends VH\_TrackCall.
  - This allows Callback's Queue Manager application to successfully track calls for queuing and answered or abandoned events.
  - Should contain the following settings:
    - Send tab - CallingLineID, Dialed Number String, PV (reserved for Callback use).
    - Receive tab - Select nothing.



### 3. Get Vars AppGW block:

- This block is required for ACD queuing only.
- The last block for callbacks ready to queue to an agent should be an Application Gateway block that sends VH\_GetVars.
- This allows user data to be reattached to the call from the inbound call leg.
- Should contain the following settings:
  - Send tab - CallingLineID, Dialed Number String, PV reserved for Callback use.
  - Receive tab - All PVars selected and expanded call context variables (ECC Vars).





## Callback Configuration

Within the Callback database, ensure Callback Queue ID and Callback Transfer Device for each queue are identical and set to the DNIS value used by the outbound script.



## Log in to IVG Management System

### Overview

The IVG management system provides centralized configuration and administration of all Holly Voice Platforms installed in the IVG system. There are six management features which require specific attention in IVG systems:

- Workers
- Service Provider
- Affiliates
- Applications
- Cisco Parameter Adjustment
- Trunk Groups Adjustment

The first step in using the IVG management system is logging in to the User Interface (UI).

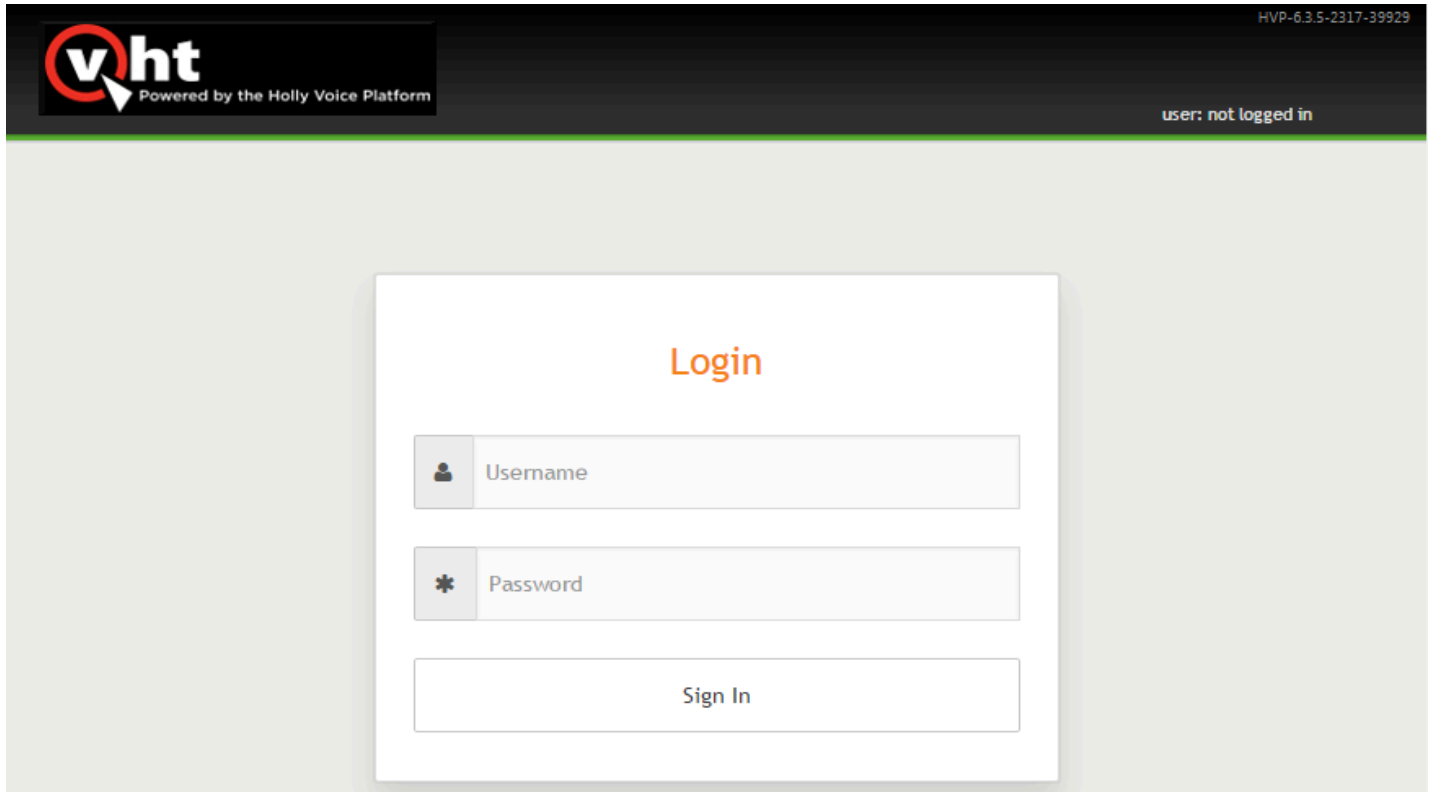
### Log In and Out

To start the IVG management system from the server containing the IVG:

1. Open a web browser.
2. Enter **http://server\_address:2020**.
3. Enter a username and password and click **Login**.

**Note:**

The username and password for the initial default user is **administrator** and **holly12**. It is highly recommended to change the default password after the first login using the **System Users** option within the **Administration** menu within the management system.



To exit the managementsystem:

1. Select **Logout** in the IVG management system window.



## Activating IVG Workers

Use the **Workers** option of the **Configuration** menu within the IVG management system to verify the required IVG Workers (listed in the following table) are Started and Running as part of the installation process. If necessary, use the following procedure to start IVG workers.

**Note:**

You must log into the IVG management system before these procedures can be utilized.

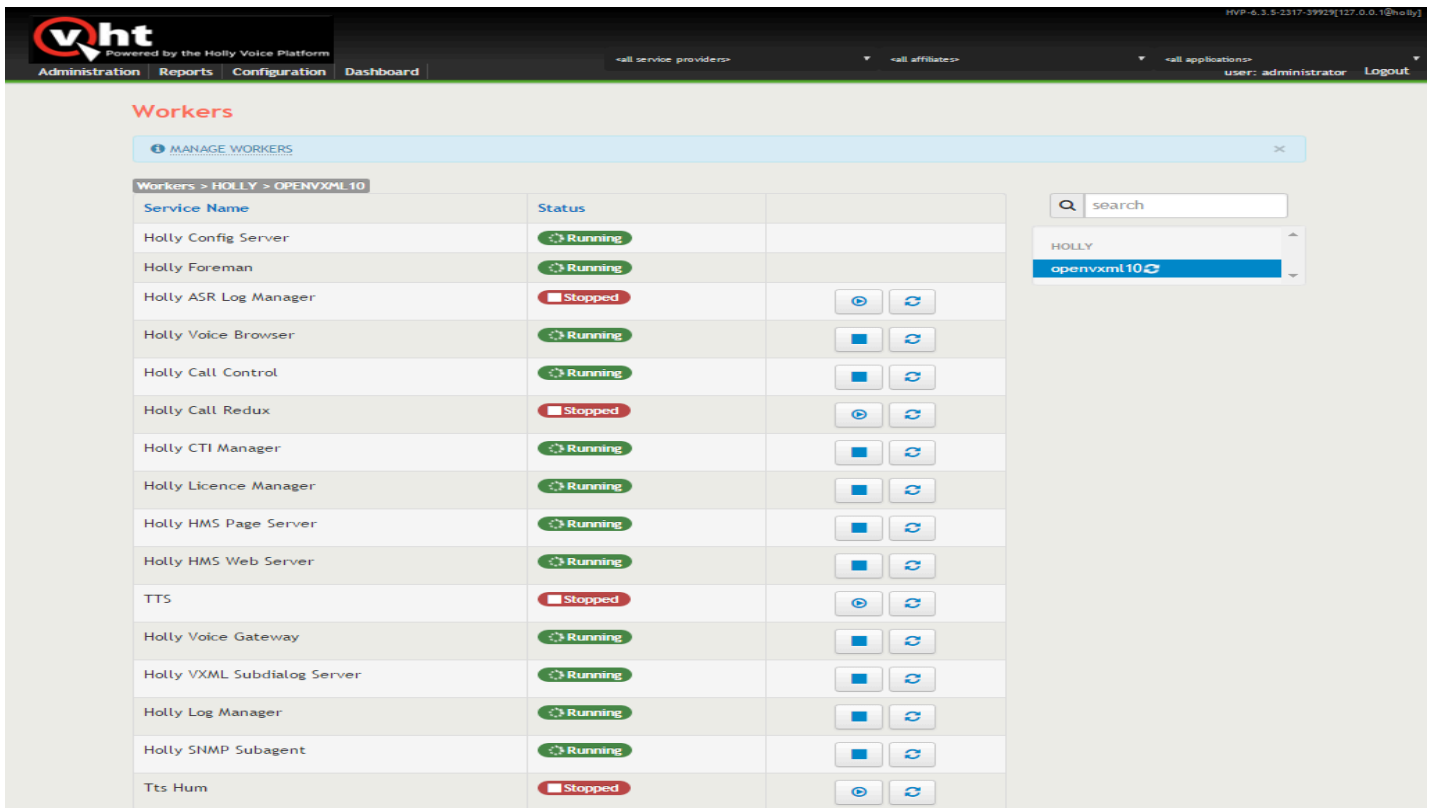
Worker Name	Process Name	Description
Holly Config Server	configserver	Required by all workers to access configuration information and ensure the parameter information is accurate throughout the IVGmanagementsystem.
Holly Foreman	foreman	Required to monitor and restart workers.
Holly Voice Browser	browser	Required for calls using an IVR.
Holly Call Control	callcontrol	Required when using CCXML.
Holly CTI Manager	ctimgr	Required to manage telephony to ICM connections.
Holly License Manager	hlm	Required for incoming calls. Used to limit the number of calls on a server to prevent oversubscribing. Also returns the configuration and URL for the application.
Holly HMS Page Server	hmspageserver	Required for IVG management system access.
Holly HMS Web Server	hmsweb	
Holly Voice Gateway	hvg	Required for calls using an IVR.
Holly VXML Subdialog Server	hvss	Required by license manager to access IVG license information.



Worker Name	Process Name	Description
Holly Log Manager	logmgr	Required for writing diagnostic log information.
Holly SNMP Subagent	subagent	Required for SNMP integration and alarm consolidation in ~/log/alarms.log file.

To select and activate the required IVG workers:

1. Select **Configuration > Workers** within the IVG management system.
2. Select the IVG server on the right side of the window.



1. Click the start icon (right arrow) for the IVG worker to be started.
2. Verify the status of the worker changes to Running.
3. Repeat Steps 3 and 4 for the remaining IVG workers that need started.

It is also possible to check the IVG installer log (installer\_ *mmdyy*.txt file) to verify the workers have been started. Refer to one of the following topics for an example installer log:



- [Single IVG](#)
- [Multiple IVG and Local PostgreSQL](#)
- [Multiple IVG and Standalone PostgreSQL](#)
- [High Availability Virtual Hold with Multiple IVG and Standalone PostgreSQL](#)



## Voice platform provisioning

### Overview

This topic describes how to provision the voice platform by adding the following components:

- [Service Provider](#)
- [Affiliate](#)
- [Applications](#)

**Note:**

You must log into the IVG management system before these procedures can be utilized.

### Adding the Service Provider

Use the **Service Providers** option of the **Administration** menu within the IVG management system to define (or edit) the VHT service provider for this IVG.

**Note:**

Only one Service Provider needs to be added since IVG employs the HVP centralized management feature.

To create or edit the VHT service provider, complete the following minimum configuration:

1. Select **Administration > Service Providers** within the IVG management system.

The screenshot shows the 'Service Provider Editor' interface. At the top, there is a navigation bar with 'Administration', 'Reports', 'Configuration', and 'Dashboard'. The main content area is divided into several sections:

- Select Service Provider:** Contains dropdown menus for 'Service Provider' (set to VHT), 'Domain Name' (VHT), and 'Domain Description' (VHT).
- Service Provider Contact Details:** Includes input fields for 'Name', 'Email', 'Phone', and 'Address'.
- Licence Port Allocation:** Features input fields for 'Max Available Ports' and 'Warn Ports', both set to 999.
- Alarm Recipients:** Includes a dropdown for 'Alarm Type' (set to email) and an 'Address' input field. It also has 'Add', 'Replace', and 'Delete' buttons.
- Application Parameters:** Includes 'Key' and 'Value' input fields, and a 'Preset Parameters' dropdown set to 'Set Application Type To CCXML'. It has 'Set', 'Replace', and 'Delete' buttons.
- Service Provider Numbers:** Includes a 'DNIS Numbers' input field with the value '69300 - 69399 outbound - outbound' and 'Add', 'Replace', and 'Delete' buttons.

2. Complete the **Select Service Provider** and **Licenses Port Allocation** areas. Fields are defined as follows:

Field	Description
Select Service Provider	
Service Provider	Unique name of previously created service providers. Select a provider here when editing an existing provider. Leave this field set to <b>&lt;new service provider&gt;</b> when creating a new provider.
Domain Name	Enter the desired service provider name when creating a new service provider. ( <b>VHT_ServiceProvider</b> is recommended).
Domain Description	Enter the desired service provider name when creating a new service provider. Copy the name from the Domain Name field if necessary.



Field	Description
License Port Allocation	
Max Available Ports	<p>Maximum number of ports available to affiliates attached to this service provider. A warning (if configured in <b>Alarm Recipients</b> area) is sent when this value is exceeded. This value is defaulted to 999.</p> <p><b>Note:</b> Set this value greater than the total number of Virtual Hold licensed ports (sum of VoiceLicenses, NonVoiceLicenses, VoiceBurstingLicenses, and NonVoiceBurstingLicenses).</p>
Warn Ports	<p>Number of allocated ports used (by the affiliates attached to this service provider) at which a warning is generated. A warning (if configured in <b>Alarm Recipients</b> area) gives advance notice of approaching the port allocation limit. This value is defaulted to 999.</p> <p><b>Note:</b> Set this value greater than the total number of Virtual Hold licensed ports (sum of VoiceLicenses, NonVoiceLicenses, VoiceBurstingLicenses, and NonVoiceBurstingLicenses).</p>

3. Click **Save Service Provider**.
4. Complete the Service Provider **Numbers Available** area. Available values are as follows:

Value	Description
Range of numbers	Range of DNIS number available to this service provider.
<b>outbound</b>	Required value.
<b>outreach</b>	Specify when Outreach application is used.

**Notes:**

- Ensure the DNIS numbers and values for this service provider are configured in Outbound Contact Client (OCC).
- DNIS numbers and values are case-sensitive and can be alphanumeric.

5. Click **Add**.
6. Click **Save Service Provider**.

**Notes:**

1. Associated affiliates must be deleted before a service provider can be deleted.
2. Deleting a service provider deletes the associated service provider groups and users.
3. Deleting a service provider removes all connections to associated archived log records.

## Adding the Affiliate

Use the **Affiliates** option of the **Administration** menu to create (or edit) the VHT affiliate and associate it to the VHT service provider.

**Note:**

Only one Affiliate needs to be add since IVG employs the HVP centralized management feature.

To create or edit the VHT affiliate, complete the following minimum configuration:

1. Select **Administration > Affiliates** within the IVG management system.



The screenshot shows the VHT Affiliate Editor interface. At the top, there is a navigation bar with 'Administration', 'Reports', 'Configuration', and 'Dashboard'. The main content area is titled 'Affiliate Editor' and contains several sections:

- Select Affiliate:** Includes dropdown menus for 'Service Provider' (VHT-ServiceProvider), 'Affiliate' (VHT-Affiliate), and 'Domain Name' (VHT-Affiliate). There is also a text field for 'Domain Description'.
- Affiliate Contact Details:** Includes text input fields for 'Name', 'Email', 'Phone', and 'Address'.
- Licence Port Allocation:** Includes input fields for 'Max Available Ports' (400) and 'Warn Ports' (300), with a note '(Available 400)'.
- Alarm Recipients:** Includes a dropdown for 'Alarm Type' (email) and a text field for 'Address'. There are buttons for 'Add', 'Replace', and 'Delete'.
- Application Parameters:** Includes a table with 'Key' and 'Value' columns. A 'Preset Parameters' dropdown is set to 'Set Application Type To CCXML'. There are buttons for 'Set', 'Replace', and 'Delete'.
- Affiliate Numbers:** Includes a 'Numbers Available' section with a 'DNIS Numbers' input field. A list of numbers is shown: '48241 - 48241', '48249 - 48249', 'outbound - outbound', and 'outreach - outreach'. There are buttons for 'Add', 'Replace', and 'Delete'.

2. Complete the **Select Affiliate** and **Licenses Port Allocation** areas. Fields are defined as follows:

Field	Description
Select Affiliate	
Service Provider	Select the service provider to which affiliate is associated ( <b>VHT_ServiceProvider</b> is recommended).
Affiliate	Unique name of previously created affiliates. Select an affiliate here when editing an existing affiliate. Leave this field set to <b>&lt;new affiliate&gt;</b> when creating a new affiliate.
Domain Name	Enter the desired affiliate name when creating a new affiliate ( <b>VHT_Affiliate</b> is recommended).



Field	Description
Domain Description	Enter the desired affiliate name when creating a new affiliate. Copy the name from the Domain Name field if necessary.
License Port Allocation	
Max Available Ports	Maximum number of ports available to this affiliate. A warning (if configured in <b>Alarm Recipients</b> area) is sent when this value is exceeded. Set this value to <b>0</b> indicating that a license from the parent object is used.
Warn Ports	Number of allocated ports used (by the applications attached to this affiliate) at which a warning is generated. A warning (if configured in <b>Alarm Recipients</b> area) gives advance notice of approaching port allocation limit. Set this value to <b>0</b> indicating that a license from the parent object is used.

3. Click **Save Affiliate**.
4. Complete the Affiliates **Numbers Available** area. Available values are as follows:

Value	Description
Range of numbers	Range of DNIS number available to this affiliate.
<b>outbound</b>	Required value.
<b>outreach</b>	Optional, use when Outreach application is utilized.

**Notes:**

- Ensure the DNIS numbers and values for this affiliate are configured in Outbound Contact Client (OCC).
- DNIS numbers and values are case-sensitive and can be alphanumeric.
- Ensure DNIS numbers represent a unique subset of the range of numbers available to the associated service provider (**VHT\_ServiceProvider** is recommended).

5. Click **Add**.
6. Click **Save Affiliate**.

**Notes:**

1. Associated applications must be deleted before an affiliate can be deleted.



2. Deleting an affiliate deletes the associated affiliate groups and users.
3. Deleting an affiliate removes all connections to associated archived log records.

## Add VHT Applications

Use the **Applications** option of the **Administration** menu to provision the following VHT voice applications and associate them to the appropriate affiliate:

- Inbound (e.g. **VHT\_Inbound**) - Required for Callback integrations.
- Outbound (e.g. **VHT\_Outbound**) - Required for Callback integrations.
- Outreach (e.g. **VHT\_Outreach**) - Optional, provision as required
- Prompt Recorder (e.g. **VHT\_PromptRecorder**) - Optional, provision as required.

### Notes:

- These applications only need to be added once because IVG employs the HVP centralized management feature.
- Outreach applications are optional and should only be configured if purchased.

## Inbound Application

To create or edit the inbound application for call treatment, complete the following minimum configuration:

1. Select **Administration > Applications** within the IVG management system.

2. Complete the **Select Application**, **URLs**, **Licenses Port Allocation**, and **Application Parameters** areas. Fields are defined as follows:

Field	Description
Select Application	
Service Provider	Select the service provider to which this application is associated ( <b>VHT_ServiceProvider</b> is recommended).
Affiliate	Select the affiliate to which this application is associated ( <b>VHT_Affiliate</b> is recommended).



Field	Description
Application	Unique name of previously created applications. Select an application here when editing an existing application. Leave the field set to <b>&lt;new application&gt;</b> when creating a new application.
Name	Enter the desired application name when creating a new application ( <b>VHT_Inbound</b> is recommended).
Description	Enter the desired description for the application.
URLs	
URL	URL where this application can be found. Always specify a fetch time out when inserting a URL.
Fetch Time Out	Time allotted to fetch this URL. Recommended value is <b>5</b> seconds. Click <b>Add</b> after entering the Fetch Time Out.
URLs	<p>Listing of URLs where this application is published. URLs are utilized in the order presented. An example URL is <code>http://localhost:8080/VIS/PlatformSupport_HVPCisco/Begin?Tenant=VHT&amp;MODE=HVP</code>.</p> <ol style="list-style-type: none"><li>1. Use <b>Move Up</b> and <b>Move Down</b> to ensure URLs are listed in desired order.</li><li>2. Limit number of URLs inserted because fetch time outs are cumulative.</li><li>3. Ensure last URL listed is local to browser so that access is assured.</li></ol>
License Port Allocation	
Max Available Ports	Maximum number of ports available to this application. A warning (configured in <b>Alarm Recipients</b> area) is sent when this value is exceeded. Set this value to <b>0</b> indicating that a license from the parent object is used.
Warn Ports	Number of allocated ports used (by this application) at which a warning is generated. Warning is configured in <b>Alarm Recipients</b> area and gives advance notice of approaching the port allocation limit. Set this value to <b>0</b> indicating that a license from the parent object is used.
License Life	Amount of time the License Manager holds on to a license before it assumes the license is no longer in use.
Application Parameters	
Key	Name of key used by this application.



Field	Description
Value	Value of key used by this application. Complete Key and Value fields and click <b>Set</b> to enter parameters.

At a minimum, the following parameters are required for the inbound IVR:  
**failure\_destination** = *location* where *location* is the IP address to which calls are transferred when VIS fails to execute and inbound call treatment is not delivered. Required format is **sip:DN\_number@IP\_address** (sip:55202@10.10.0.217 for example).  
**type** = **application/voicexml+xml**

3. Click **Save Application**.
4. Complete the Application **Numbers Available** area. Available values are as follows:

Value	Description
Range of numbers	Range of DNIS number available to this application. Example setting for this value is 48231 - 48239.

**Notes:**

- Ensure the DNIS numbers and values for this application are configured in Outbound Contact Client (OCC).
- DNIS numbers and values are case-sensitive and can be alphanumeric.
- Ensure DNIS numbers represent a unique subset of the range of numbers available to the associated affiliate (**VHT\_Affiliate** is recommended).

5. Click **Add**.
6. Click **Save Application**.

## Outbound Application

To create or edit the outbound applications for call treatment, complete the following minimum configuration:

1. Select **Administration > Applications** within the IVG management system.
2. Complete the **Select Application**, **URLs**, **Licenses Port Allocation**, and **Application Parameters** areas. Fields are defined as follows:

Field	Description
Select Application	



Field	Description
Service Provider	Select the service provider to which this application is associated ( <b>VHT_ServiceProvider</b> is recommended).
Affiliate	Select the affiliate to which this application is associated ( <b>VHT_Affiliate</b> is recommended).
Application	Unique name of previously created applications. Select an application here when editing an existing application. Leave the field set to <b>&lt;new application&gt;</b> when creating a new application.
Name	Enter the desired application name when creating a new application ( <b>VHT_Outbound</b> is recommended).
Description	Enter the desired description for the application.
URLs	
URL	URL where this application can be found. Always specify a fetch time out when inserting a URL.
Fetch Time Out	Time allotted to fetch this URL. Recommended value is <b>5</b> seconds. Click <b>Add</b> after entering the Fetch Time Out.
URLs	<p>Listing of URLs where this application is published. URLs are utilized in the order presented. An example URL is <code>http://localhost:8080/VIS/PlatformSupport_HVPCisco/Outbound?MODE=HVP</code>.</p> <ol style="list-style-type: none"><li>1. Use <b>Move Up</b> and <b>Move Down</b> to ensure URLs are listed in desired order.</li><li>2. Limit number of URLs inserted because fetch time outs are cumulative.</li><li>3. Ensure last URL listed is local to browser so that access is assured.</li></ol>
License Port Allocation	
Max Available Ports	Maximum number of ports available to this application. A warning (if configured in <b>Alarm Recipients</b> area) is sent when this value is exceeded. Set this value to <b>0</b> indicating that a license from the parent object is used.
Warn Ports	Number of allocated ports used (by this application) at which a warning is generated. A Warning (if configured in <b>Alarm Recipients</b> area) gives advance notice of approaching the port allocation limit. Set this value to <b>0</b> indicating that a license from the parent object is used.
License Life	Amount of time the License Manager holds on to a license before it assumes the license is no longer in use.
Application Parameters	



Field	Description
Key	Name of key used by this application.
Value	Value of key used by this application. Complete Key and Value fields and click <b>Set</b> to enter parameters.
At a minimum, the following parameters are required for the outbound IVR: <b>type = application/voicexml+xml</b>	

- Click **Save Application**.
- Complete the Application **Numbers Available** area. Available values are as follows:

Value	Description
Range of numbers	Range of DNIS number available to this application. Example setting for this value is 48240 - 48249.
<b>outbound</b>	Required value.

**Notes:**

- Ensure the DNIS numbers and values for this application are configured in Outbound Contact Client (OCC).
- DNIS numbers and values are case-sensitive and can be alphanumeric.
- Ensure DNIS numbers represent a unique subset of the range of numbers available to the associated affiliate (**VHT\_Affiliate** is recommended).

- Click **Add**.
- Click **Save Application**.

## Outreach Application

To create or edit the Outreach application for call treatment, complete the following minimum configuration:

- Select **Administration > Applications** within the IVG management system.
- Complete the **Select Application**, **URLs**, **Licenses Port Allocation**, and **Application Parameters** areas. Fields are defined as follows:

Field	Description
Select Application	



Field	Description
Service Provider	Select the service provider to which this application is associated ( <b>VHT_ServiceProvider</b> is recommended).
Affiliate	Select the affiliate to which this application is associated. Set this value to ( <b>VHT_Affiliate</b> is recommended).
Application	Unique name of previously created application. Select an application here when editing an existing application. Leave the field set to <b>&lt;new application&gt;</b> when creating a new application ( <b>VHT_Outreach</b> is recommended).
Name	Enter the desired application name when creating a new application ( <b>VHT_Outreach</b> is recommended).
Description	Enter the desired description for the application.
URLs	
URL	URL where this application can be found. Always specify a fetch time out when inserting a URL.
Fetch Time Out	Time allotted to fetch this URL. Recommended value is <b>5</b> seconds.
URLs	<p>Listing of URLs where this application is published. URLs are utilized in the order presented. An example URL is <code>http://localhost:8080/VIS/PlatformSupport_HVPCisco/Begin?Tenant=VHT&amp;MODE=HVP</code>.</p> <ol style="list-style-type: none"><li>1. Use <b>Move Up</b> and <b>Move Down</b> to ensure URLs are listed in desired order.</li><li>2. Limit number of URLs inserted because fetch time outs are cumulative.</li><li>3. Ensure last URL listed is local to browser so that access is assured.</li></ol>
License Port Allocation	
Max Available Ports	Maximum number of ports available to this application. A warning (if configured in <b>Alarm Recipients</b> area) is sent when this value is exceeded. Set this value to <b>0</b> indicating that a license from the parent object is used.
Warn Ports	Number of allocated ports used (by this application) at which a warning is generated. A warning (if configured in <b>Alarm Recipients</b> area) gives advance notice of approaching the port allocation limit. Set this value to <b>0</b> indicating that a license from the parent object is used.
Application Parameters	



Field	Description
Key	Name of key used by this application.
Value	Value of key used by this application. Complete Key and Value fields and click <b>Set</b> to enter parameters.
At a minimum, the following parameters are required for Outreach: <b>type = application/voicexml+xml</b>	

3. Click **Save Application**.
4. Complete the Application **Numbers Available** area. Available values are as follows:

Value	Description
Range of numbers	Range of DNIS number available to this application. Example setting for this value is 48250 - 48259.
<b>outreach</b>	Required value.

**Notes:**

- Ensure the DNIS numbers and values for this application are configured in Outbound Contact Client (OCC).
- DNIS numbers and values are case-sensitive and can be alphanumeric.
- Ensure DNIS numbers represent a unique subset of the range of numbers available to the associated affiliate (**VHT\_Affiliate** is recommended).

5. Click **Add**.
6. Click **Save Application**.

## Prompt Recorder Application

To create or edit the prompt recorder application for custom voice prompt usage, complete the following minimum configuration:

1. Select **Administration > Applications** within the IVG management system.
2. Complete the **Select Application, URLs, Licenses Port Allocation, and Application Parameters** areas. Fields are defined as follows:





Field	Description
Select Application	
Service Provider	Select the service provider to which this application is associated ( <b>VHT_ServiceProvider</b> is recommended).
Affiliate	Select the affiliate to which this application is associated ( <b>VHT_Affiliate</b> is recommended).
Application	Unique name of previously created applications. Select an application here when editing an existing application. Leave the field set to <b>&lt;new application&gt;</b> when creating a new application.
Name	Enter the desired application name when creating a new application ( <b>VHT_PromptRecorder</b> is recommended).
Description	Enter the desired description for the application.
URLs	
URL	URL where this application can be found. Always specify a fetch time out when inserting a URL.
Fetch Time Out	Time allotted to fetch this URL. Recommended value is <b>5</b> seconds. Click <b>Add</b> after entering the Fetch Time Out.
URLs	<p>Listing of URLs where this application is published. URLs are utilized in the order presented. An example URL list is <code>http://localhost:8080/PRec/Begin?Tenant=VHT&amp;MODE=HVP</code> for HVP systems, <code>http://localhost:8080/PRec/Begin?Ten...HT&amp;MODE=AVPSIP</code> for AVP systems, <code>http://localhost:8080/PRec/Begin?Tenant=VHT&amp;MODE=GVP</code> for GVP systems, and <code>http://localhost:8080/PRec/Begin?Tenant=VHT&amp;MODE=CVP</code> for CVP systems.</p> <ol style="list-style-type: none"><li>1. Use <b>Move Up</b> and <b>Move Down</b> to ensure URLs are listed in desired order.</li><li>2. Limit number of URLs inserted because fetch time outs are cumulative.</li><li>3. Ensure last URL listed is local to browser so that access is assured.</li></ol>
License Port Allocation	
Max Available Ports	Maximum number of ports available to this application. A warning (if configured in <b>Alarm Recipients</b> area) is sent when this value is exceeded. Set this value to <b>0</b> indicating that a license from the parent object is used.
Warn Ports	Number of allocated ports used (by this application) at which a warning is generated. A Warning (if configured in <b>Alarm Recipients</b> area) gives advance notice of approaching the port allocation limit. Set this value to <b>0</b> indicating that a license from the parent object is used.



Field	Description
License Life	Amount of time the License Manager holds on to a license before it assumes the license is no longer in use.
Application Parameters	
Key	Name of key used by this application.
Value	Value of key used by this application. Complete Key and Value fields and click <b>Set</b> to enter parameters.
At a minimum, the following parameters are required for prompt recorder usage: <b>type = application/voicexml+xml</b>	

3. Click **Save Application**.
4. Complete the Application **Numbers Available** area. Available values are as follows:

Value	Description
Range of numbers	Range of DNIS number available to this application. Example setting for this value is 48270 - 48279.

**Notes:**

- Ensure the DNIS numbers and values for this application are configured in Outbound Contact Client (OCC).
- DNIS numbers and values are case-sensitive and can be alphanumeric.
- Ensure DNIS numbers represent a unique subset of the range of numbers available to the associated affiliate (**VHT\_Affiliate** is recommended).

5. Click **Add**.
6. Click **Save Application**.

## Voice Platform Configuration

### Overview

This topic describes how to configure the voice platform for Cisco operation and changes in trunk group information.

### Cisco Parameter Adjustment

After completing installation and configuration of the IVG application, performance of a text call may reveal that the inbound call/port is not being released when the outbound call/port connects.

It may be necessary to change the `referwaitfortify` parameter within the `hvp_params_cisco.cfg` file from **0** (default value of don't wait) to **1** (wait) to eliminate this problem. After making this change, perform another test call to verify proper call treatment.

### Trunk Groups Adjustment

**Note:**

You must log into the IVG management system before this procedure can be utilized.

Use the following procedure to change the trunk group name, port count, or gateway name set during the installation process (within the `hvp_params_cisco.cfg` file) on all host servers. Changes to this parameter require a restart of the CTI Manager component before taking effect.

1. Select **Configuration > Holly CTI Manager** within the IVG management system.
2. Select the appropriate **Component** and **Pool** parameters.
3. Select the **Pool Holly** tab.
4. Enter the appropriate trunkgroups parameter using the following format `trunkgroup=portcount:gatewayname`  
Where:  
`trunkname` = Peripheral number of the Network Trunk Group in Cisco.  
`portcount` = New maximum number of ports.  
`gatewayname` - The name of the gateway (always use default value of **gateway1**).  
For example, 100=30:gateway1
5. Click **Modify** for this parameter.



## Enabling SSL/TLS ciphers and options

### Overview

Enable SSL/TLS in IVG through the voice platform UI.

---

#### For multiple IVG deployments:

Enable SSL/TLS parameters at the Pool level. This enables these parameters for all voice platforms in the designated pool.

---

### Enabling SSL/TLS in the voice platform

1. Navigate to **Configuration > Holly Configuration**.
2. Select **OpenSSL** from the **Component** dropdown.
3. Select the **Pool**.
  - **TIP:** The default pool name is **holly**.
4. In **sslciphers**, enter the list of SSL ciphers for openssl.
  - For example: **"HIGH:DES:MD5:AES256-SHA256"**
5. In **ssloptions**, enter the SSL options to use from the following:
  - no\_sslv2
  - no\_sslv3
  - no\_tlsv1
  - no\_tlsv1\_1
  - no\_tlsv1\_2

#### Important:

Escape the separator (,) when listing multiple **ssloptions** using a forward slash (\). For example:

```
no_sslv2\, no_sslv3\, no_tlsv1\, no_tlsv1_1\, no_tlsv1_2
```

6. Restart IVG for the changes to take effect.



## Generating the self-signed certificates

The IVG installer process generates the self-signed certificates for each IVG instance, and stores them in the **/export/home/holly/etc** directory.

The certificate and key file names are referenced in the values for **httpscertificatefilename** and **httpsprivatekeyfilename**.

## Verifying available ciphers

Ciphers available for a voice platform can be checked by using the following Linux shell command:

```
openssl ciphers -V
```

For available cipher options:

Learn more about available cipher options at <https://www.openssl.org/docs/apps/ciphers.html>.

[return to top](#)



## IVG Performance Configuration

### Overview

This topic details default performance enhancements and how these enhancements can be customized to improve IVG system performance.

### Performance Configuration

The following sections detail requirements and performance configuration items (both automatically and manually set) and how to configure them. This content is divided into the following topics:

- [Server Components](#)
- [Virtual Machine \(Hypervisor\)](#)
- [Operating System](#)
- [Voice Platform](#)

### Server Components

The following sections identify the Virtual Hold recommendations for common server components.

#### CPUs

Virtual Hold recommends the use of at least two, quad core high clock speed (2.95 MHz or faster) processors.

#### Network Interfaces

Virtual Hold recommends the use of 1 GB Network Interface Cards (NICs).

#### Disk Space

Virtual Hold recommends thick provisioned hard disks of 60 GB or larger.

### Virtual Machine (Hypervisor)

IVG software has been tested using the following virtualized environment:

- VMWARE ESXi (version 5.5 or higher), 64-bit compatible.



## Operating System

The following sections detail Virtual Hold requirements and recommendations (both automatically and manually set) for the operating system and how to set them.

### Version

Virtual Hold requires CentOS 6.8 and RHEL 6.8 (both 64-bit only).

### /tmp as tmpfs

As the voice platform writes optional call recordings and caches data temporarily to the /tmp/holly directory, a negative performance impact is seen if /tmp is left at its default Red Hat configuration as a normal disk-based file system location. The installer in Version 3.1.0 or later automatically mounts the /tmp as a tmpfs file system with a memory size of 4GB. To configure this setting post installation, use the following command in **/etc/fstab**:

```
tmpfs /tmp tmpfs defaults size=memory_size 0 0
```

where:

*memory\_size* = As a general rule, set this value to 50% of the RAM memory available to the system.

Repeat this procedure on all servers containing an IVG.

### Realtime Option [Automatic Configuration]

This option places the processes responsible for handling RTP audio into a higher priority real time process class. Audio is a realtime environment and quality suffers if packets are delayed or jittered. Raising the priority of these processes minimizes the chances of these delays occurring. To enable Realtime feature at the operating system level:

1. Have a root user create a 99-realtime.conf file in the ...etc\security\limits.d directory.
2. Ensure this file contains the following lines:

```
@realtime - rtprio 99
@realtime - memlock unlimited
Eg.
```

3. Have the root user create a group named **realtime** and add the holly user to it using the following commands.

```
groupadd realtime
usermod -a -G realtime holly
```

4. Restart this server.
5. Repeat this procedure on all servers containing an IVG.

## Voice Platform

The following sections detail voice platform requirements and recommendations (both automatically and manually set) and how to configure them.

### Version

IVG installs Version 6.3 of the voice platform.

### HMS Settings

Use the **Holly Configuration** option of the **Configuration** menu to create (or edit) performance enhancements to this IVG.

**Note:**

This configuration only needs to be made once because the parameters are being configured at the pool level. Such changes apply to all voice platforms installed as a member of the pool.

To edit the voice platform performance related configuration:

1. Select **Configuration > Holly Configuration** within the IVG management system.
2. Configure the **Component** and **Pool** parameters as follows:

Field	Description
Component	Component to be configured. Set this value to <b>Audio Provider - SIP</b> .
Pool	Pool or group of IVG servers ( <b>holly</b> for example).

3. Configure the **distributercount** parameter to **2** (default value is **4**). [Manual Configuration]

**Note:**

The amount of processes used by the **realtime** parameter (refer to Step 5) is determined by the **distributercount** parameter. The **distributercount** parameter is the number of SIP threads available to distribute and mix the audio and RTP channels. Set the **distributercount** parameter to the number of physical CPU cores, not including hyperthreads, allocated to a VM. The distributors are responsible for handling RTP audio. As an example, for a four vCPU VM that contains four CPU threads and two CPU cores, set **distributercount** to 2.

4. Click **Add** or **Modify** for this parameter.





- 5. Ensure the **realtime** parameter is set to **1** (default value). [Automatic Configuration]
- 6. If necessary, click **Add** or **Modify** for this parameter.
- 7. Ensure the **tonedetect** parameter is set to **0** (disabled - the default value). [Automatic Configuration]

**Note:**

This option is used when DTMF is delivered to the voice platform in-band as a tone in the audio stream. Enabling the **tonedetect** option causes usage of extra processing for every call so it recommended to disable this option. Reset the value or click **Delete** to return this option to the default value.

- 8. If necessary, click **Add** or **Modify** for this parameter.
- 9. Configure the **Component** and **Pool** parameters as follows:

Field	Description
Component	Component to be configured. Set this value to <b>Holly Globals</b> .
Pool	Pool or group of IVG servers ( <b>holly</b> for example).

- 10. Ensure the **CC** parameter is set to **1** (default value). [Automatic Configuration]
- 11. If necessary, click **Add** or **Modify** for this parameter.
- 12. Configure the **Component** and **Pool** parameters as follows:

Field	Description
Component	Component to be configured. Set this value to <b>Holly Voice Browser</b> .
Pool	Pool or group of IVG servers ( <b>holly</b> for example).

- 13. Configure the **callevts** parameter to contain the minimum required number of call events generating log entries because (none by default) the platform logs a large amount of events to the database. This excessive logging of call events should be avoided in production systems as it consumes processing resources. At a minimum, the **fetch** event should be removed. At a maximum, all events can be removed. The complete list of available call events is: [Automatic Configuration]

- asr\_session
- log\_element
- recognition\_start
- recognition\_end
- record\_start
- record\_end
- transfer\_start



```

transfer_end
disconnect
fetch
error_critical
error_severe
error_warning
note
exit
placecall_start
placecall_end
sip_session
grammar_activation

```

14. Configure the **jsruntimesizekb** parameter to **40960**. This setting should improve performance in high call volume systems using JavaScript. [Manual Configuration]
15. Click **Add** or **Modify** for this parameter.
16. Configure the **Component** and **Pool** parameters as follows:

Field	Description
Component	Component to be configured. Set this value to <b>Holly Call Control</b> .
Pool	Pool or group of IVG servers ( <b>holly</b> for example).

17. Ensure the **dthreads** parameter is set to **1** (default value). [Manual Configuration]

**Note:**

This option handles outbound CCXML calls at VHT. If jitter (incomplete voice prompts, intermittent call response, etc.) is present during high load call, it may be necessary to increment this value. However, be aware that a setting of **4** in a system using four vCPUs was tested and caused other problems. A setting of **2** would be suggested. In some cases, the **distributercount** (Audio Provider - SIP) and **dthreads** (Holly Call Control) options interacted. For example, a four vCPU system handling a large load of concurrent inbound and outbound calls may require setting both of them to **1** so they do not unnecessarily impact Tomcat processing.

18. Click **Add** or **Modify** for this parameter.
19. Configure the **Component** and **Pool** parameters as follows:

Field	Description
Component	Component to be configured. Set this value to <b>Holly Log Manager</b> .



Field	Description
Pool	Pool or group of IVG servers ( <b>holly</b> for example).

- 20. Ensure the **disklogging** parameter is set to **1** (default value). [Automatic Configuration]
- 21. If necessary, click **Add** or **Modify** for this parameter.
- 22. Select **Configuration > Holly Essentials** within the IVG management system.
- 23. Configure the **Component** and **Pool** parameters as follows:

Field	Description
Pool	Pool or group of IVG servers ( <b>holly</b> for example).

- 24. Select the **Trace Level** tab.
- 25. Ensure all parameters are set to **2: Status Messages**. [Automatic Configuration]
- 26. If necessary, click **Add** or **Modify** for this parameter.

### Adjusting Resource Levels

The following Call Control and Browser resource levels should be configured to a value greater than the total number of Callback licensed ports on each IVG. This ensures there are always more resources available than needed for the available licenses. It is These levels are currently set to a high value by default through use of the hvp\_param.cfg file by the IVG installer.

Holly Configuration > Call Control:

- maxcreateccxmlsessions (default value = 999)
- maxexternalsessions (default value = 999)
- maxnewcallsessions (default value = 999)
- maxsessions (default value = 999)

Holly Essentials (Telephony):

- Number of Ports per Server (default value = 400)
- Maximum Concurrent Inbound Calls per Server (default value = 400)
- Maximum Concurrent Outbound Calls per Server (default value = 400)



These values are based on the baseline system used for IVG performance testing. Adjustment of these values is expected to achieve the best performance. Refer to the appropriate Interactive Voice Gateway (IVG) Technical Overview for baseline system specifications.

To set these resource levels for this IVG, use the **Configuration > Holly Configuration** menu within HMS.

[Return to top.](#)

## Configuring log purging

### Overview

The data purging values for `logtokeep`, `logtodelete`, and `datatodelete` are automatically configured during IVG installation in the `install_ivg.cfg` file, and log to `/export/home/<holly user>/log/logmgr`. These values may be adjusted post-installation by manually modifying the values.

**Note:**

Virtual Hold recommends keeping log data only as long as it is needed. If reports for a specific time period are required, Virtual Hold also recommends that these reports be run, exported to CSV files, and the supporting data purged or moved to a data warehouse.

### Update logtokeep and logtodelete

The values for `logtokeep` and `logtodelete` establish a range of how many days PostgreSQL database log records are kept.

- `logtokeep` - This value determines the maximum number of days PostgreSQL database log records are kept.
- `logtodelete` - PostgreSQL database log records up to this value (in days) are deleted.

For example, if the value for `logtokeep` is 10 and the value for `logtodelete` is 30, then the PostgreSQL database logs that fall between 11 - 30 days old will be deleted.

To update the values for `logtokeep` or `logtodelete`:

1. Edit the `/var/spool/cron/postgres` file as a root user using a Linux text editor:
2. Locate the following line:

```
00 3 * /bin/sh /export/home/postgres/9/logmgr_expire.sh holly holly holly12 10 30 postgres >> /dev/null 2>&1
```

3. The fields for `logtokeep` and `logtodelete` are expressed as integers with the default values 10 and 30, respectively. Modify the fields with the required values.

Field		Description	Default Value
logmgr_expire	logtokeep	Maximum number of days postgresQL database log records are kept. This is the value set during installation in the install_ivg.cfg file.	10
	logtodelete	PostgreSQL database log records up to this value (in days) are deleted. This value is set during installation in the install_ivg.cfg file.	30

4. Save the file.
5. Restart the Cron service for these changes to take effect.

## Update datatodelete

The value for datatodelete determines how long (in days) to keep data files inside the call data directory folder structure. Data files older than the datatodelete value are deleted.

To update the values for datatodelete:

1. Edit the `/var/spool/cron/holly` file as a root user using a Linux text editor:

```
/var/spool/cron/holly
```

2. Locate the following line:

```
00 4 * * * /bin/sh /export/home/holly/bin/datalog_expire.sh 10 >> /dev/null 2>$
```

3. The value following `datalog_expire.sh` is the integer value for the number of days of data to keep and is set to 10 by default. Update this value with the maximum age (in days) of data to keep.
4. Save the file.
5. Restart the Cron service for these changes to take effect.

## Name File Sharing

### Overview

**Important:**

These instructions apply to IVG 3.1.0 or higher.

A CentOS or RHEL machine can be configured as a network drive to share name files at a common location across other CentOS or RHEL machines in a Network File System (NFS). The machine being shared is referred to as a **Server**, and the machines that share the folder are referred to as a **Client**.

Use the following steps to configure the Server that will share its folder with the Clients.

### Configure the Server

1. Install a NFS to share across all Linux machines that will share the same folder by installing the following package:

```
yum install nfs-utils nfs-utils-lib
```

2. Execute the following commands to start the services and make them restart when the machine reboots:

```
chkconfig rpcbind on  
chkconfig nfs on
```

3. Execute the following commands to make the services restart when the machine reboots:

```
service rpcbind start  
service nfs start
```

4. Designate the directory or folder to share with the other machines by adding an entry to the `\etc\exports` file such as the following sample:

```
/usr/local/namefiles 10.10.0.42(rw,sync,no_root_squash,no_subtree_check)
```

- `\usr\local\namefiles` – Indicates the name of the folder to be shared
- `10.10.0.42` – Indicates the IP address to share the folder with
- `rw` - Indicates read and write access to the folder form the given IP address.

**Note:**

Replacing the IP address with an asterisk (\*) allows access to the designated folder by any host.

5. Run the following command to enable the folder:

```
exportfs -a
```

## Configure the Client

Use the following instructions to configure the Client that will share the Server's folder.

1. Run the following command to install the necessary packages:

```
yum install nfs-utils nfs-utils-lib
```

2. Mount the NFS folder on the Server to a folder in the Client by running the following command:

```
mount ServerIPAddress:NameFilesFolderPath
```

- a. For example, if the Server IP address is 10.10.0.30 and the namefiles folder path is `usr\local\tomcat7\webapps\ROOT\namefiles`, the command would be:

```
mount IPAddress:/var/lib/namefiles /usr/local/tomcat7/webapps/ROOT/namefiles
```

- IPAddress - The IP address

4. Ensure the mount occurs on every server reboot by adding an entry to the `etc/fstab` file by running the following command:

```
:NameFilesFolderPath nfs auto,noatime,nolock,bg,nfsvers=3,intr,tcp,actimeo=1800 0 0
```

5. Run the following command on server reboot to mount fstab:

```
mount -a
```

6. Repeat Steps 1-4 for each Client that will share the Server's folder.

## Example

A deployment has three IVG instances with tomcat installed:

- IVG01
- IVG02
- IVG03



Another machine does not have IVG installed:

- SERVER1

Given the preceding information, file sharing can be enabled in two scenarios:

- Configure IVG01 as a Server and IVG02 and IVG03 as Clients
  1. Perform Steps 1-2 from the [Configuring the Server](#) steps above to install the NFS and start the services.
  2. Since HVP01 has tomcat, use the following command to designate the folder to share with the Clients:

```
/usr/local/tomcat7/webapps/ROOT/namefiles  
10.10.0.42(rw,sync,no_root_squash,no_subtree_check)
```

3. Enable the folder by running the command:

```
exportfs -a
```

4. Configure IVG02 and IVG03 as Clients by executing Steps 1-5 from the [Configuring the Client](#) steps.
- Configure SERVER1 as a Server and IVG01, IVG02, and IVG03 as Clients.
    1. Perform Steps 1-2 from the [Configuring the Server](#) steps above to install the NFS and start the services.
    2. Since SERVER1 does not have tomcat, any folder can be selected as the NFS shared folder. For example, **var/lib/namefiles**. Use the following command to designate the folder to share with the Clients:

```
/var/lib/namefiles 10.10.0.42(rw,sync,no_root_squash,no_subtree_check)
```

3. Enable the folder by running the command:

```
exportfs -a
```

4. Configure IVG01, IVG02, and IVG03 as Clients by executing Steps 1-5 from [Configuring the Client](#).

**Important:**

In either scenario, if the NFS machine is down, then the clients cannot access the name file share.

## Configuring SMTP Server and Sentinel Email for IVG

### Overview

The Interactive Voice Gateway (IVG) management system has the ability to generate alarms when workers are stopped, started, or down. These alarms are sent over an SMTP server, which acts as a relay host to send the alerts.

The Sentinel, a process which monitors the Foreman and Configuration Manager, can also generate alerts should one of the monitored applications stop or fail.

The SMTP server and Sentinel email are configured during IVG Installation, but can also be configured post-installation by using the following steps.

### Configuring SMTP Server

**Important:**

If the values for **smtpserver**, **smtpuser**, and **smtppwd** were configured during IVG Installation, executing the manual configuration will override the values written by the installer.

To configure the SMTP server:

1. Configure postfix smtp secure password file by running the following echo command:

```
>echo "smtpserver smtpuser:smtppwd" > /etc/postfix/sasl_passwd
```

Example:

```
| >echo "196.10.10.1 installer@mobi.com:testing" > /etc/postfix/sasl_passwd
```

2. Verify the contents of the **/etc/postfix/sasl\_passwd** file.
3. Configure the relay host using the following echo command:

```
>postconf -e 'relayhost = 'relayhostIPaddress ='
```

Example:

```
| >postconf -e 'relayhost = '196.10.10.1'
```

4. Verify action by running the following command:

```
>postconf -n |grep '^relayhost ='
```

5. Verify the output is similar to:

```
| Relayhost=196.10.10.1
```

6. Enable SMTP secure authentication using the following echo command:

```
>postconf -e 'smtp_sasl_auth_enable = yes'
```

7. Verify action by running the following echo command:

```
>postconf -n |grep '^smtp_sasl_auth_enable ='
```

8. Verify output of the echo command is similar to:

```
| smtp_sasl_auth_enable = yes
```

9. Set a secure SMTP password file for postfix using the following echo command:

```
>postconf -e 'smtp_sasl_password_maps = hash:/etc/postfix/sasl/password'
```

10. Verify action by running the following echo command:

```
>postconf -n |grep '^smtp_sasl_password_maps='
```

11. Verify the output of the echo command is similar to:

```
| smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
```

12. Allow the postfix to use plain text authentication using the following echo command:

```
>postconf -e 'smtp_sasl_security_options='
```

13. Verify action by running the following echo command:

```
>postconf -n |grep '^smtp_sasl_security_options ='
```

14. Verify the output of the echo command is similar to:

```
| smtp_sasl_security_options =
```

**Important:**

The configuration parameter **smtp\_sasl\_security\_options** should not be set.

15. Secure the password file using the following echo commands:

```
>chown root:root /etc/postfix/sasl_password
```



```
>chmod 600 /etc/postfix/sasl_pswd
```

16. Hash the password file to generate the password database file using the following echo command:

```
>postmap /etc/postfix/sasl_pswd
```

17. Verify action by verifying the `/etc/postfix/sasl_pswd.db` file is generated.  
18. Restart postfix and check its status by running the following echo commands:

```
>/etc/init.d/postfix restart
```

```
>/etc/init.d/postfix status
```

19. Log in using the Holly user and restart the subagent by running the following echo commands:

```
>su - holly
```

```
>fm start subagent
```

20. Verify the subagent status by running the following echo command:

```
>fm status
```

**Note:**

It is recommended to wait a minute prior to running the `>fm status` command.

20. Verify the status reads **OK**.  
21. Send a test email by running the following echo command:

```
>echo "this is a test email." | mail -s "send mail config testing." smtpuser
```

**Important:**

The value for `smtpuser` should be the email address configured in Step 1.

22. Verify the email was sent to the `smtpuser` email address.  
23. Check `/var/log/maillog` and verify the email was sent using the configured smtp. The log should resemble the following:

```
Nov 29 04:21:19 installhvp02 postfix/pickup[21520]: 797DE22070D: uid=5431 from=<holly>  
Nov 29 04:21:19 installhvp02 postfix/cleanup[15570]: 797DE22070D: message-id=<20161129092119.  
797DE22070D@installhvp02.qalab.local>  
Nov 29 04:21:19 installhvp02 postfix/qmgr[8332]: 797DE22070D: from=<holly@installhvp02.qalab.local>,  
size=469, nrcpt=1 (queue active)  
Nov 29 04:21:19 installhvp02 postfix/smtp[15593]: 797DE22070D: to=<developer@developer.com>, relay=196.  
10.10.1[196.10.10.1]:25, delay=0.11, delays=0.04/0.06/0.01/0.01, dsn=2.0.0, status=sent (250 Queued (0.000
```

```
seconds))
```

```
Nov 29 04:21:19 installhvp02 postfix/qmgr[8332]: 797DE22070D: removed
```

**Notes:**

- The value for **to** should be the **smtpuser** email address.
- The value for **relay** should be the value for **smtpserver**.
- The value for **status** should be **sent**.

After configuring the SMTP server, user, and password, alarms can be configured in the management system by navigating to **Configuration > Holly Alarms**.

## Configuring Sentinel Email

After configuring the SMTP server, a recipient must be configured to receive the email alerts. To configure an email recipient:

1. Navigate to **/export/home/holly/bin/sentinel**
2. Locate the **MAILTO** line.
3. Add the recipient email address.
4. Save the file.
5. Run the following command to restart Sentinel:

```
sentinelctl start
```

## Configuring Sentinel Polling Period

The Sentinel polls the status of the Foreman and Configuration Manager every five minutes in a 60 minute period. Update the polling frequency by:

1. Navigate to **/var/spool/cron/holly**
2. Locate the **bin/sentinel** line. The default values indicate a polling frequency of every five minutes within a 60 minute period:

```
0,5,10,15,20,25,30,35,40,45,50,55 * * * * bin/sentinel
```

3. Update the integer string with the desired polling frequency for a 60 minute period. The following example represents a polling interval of every 15 minutes:

```
0,15,30,45 * * * * bin/sentinel
```

4. Save the file.
5. Restart the Cron service by executing the following commands:



- **/sbin/service crond stop**
- **/sbin/service crond start**

## VIS Configuration for IVG

### Overview

This topic details purpose and locations of a variety of IVG-related items such as:

- [VIS Toolkit.properties file](#)
- [VIS .war file](#)
- [VIS voice files](#)
- [VIS log files](#)
- [Holly log files](#)
- [IVG External Media Files](#)
- [VIS to Platform Toolkit \(PTK\) Configuration](#)

### VIS Toolkit.properties File

The toolkit.properties file for VIS contains various information such as the properties used to configure the VIS published to the local Tomcat server. This file is located in the ...\\etc\\VirtualHold directory and can be replaced using normal file copy procedures. No restart is required.

### VIS.war File

The VIS.war file contains the default VIS application. This file and the VIS voice files are required to successfully install VIS. The VIS.war file is located in the ...\\usr\\local\\Tomcat7\\webapps directory. To replace this file:

1. Back up the current Apache Software Foundation directory.
2. Stop the Apache Tomcat service.
3. Navigate to the \\Tomcat\\webapps directory and delete the unpacked .war file as well as the zipped .war file.
4. Navigate to the \\Tomcat\\work\\Catalina\\localhost directory (this is the cache directory) and delete the unpacked .war file
5. Paste the new .war file (ensuring it has the same name as the previous .war file) into the Tomcat7\\webapps directory.
6. Start the Tomcat service. This automatically expands out the .war file into the appropriate directories.
7. Verify that the new .war file was pulled to the cache in Tomcat\\work\\Catalina\\localhost.

## VIS Voice Files

The VIS voice files contain the default set of voice prompts (.wav files) for supported languages. These files and the VIS.war file are required to successfully install VIS. These voice files are located in the ...\\usr\\local\\Tomcat7\\webapps\\Voices directory.

To replace the Voices directory:

1. Back up the current Voices directory.
2. Stop the Apache Tomcat service.
3. Navigate to the \\Tomcat\\webapps directory and delete the Voices directory as well as any existing zipped voice files.
4. Paste the new Voices directory into the Tomcat7\\webapps directory.
5. Start the Tomcat service.

To replace individual voice files:

1. Back up the current Voices directory.
2. Stop the Apache Tomcat service.
3. Navigate to the \\Tomcat\\webapps\\Voices directory and delete the individual voice file to be replaced.
4. Paste the new voice file into the Tomcat7\\webapps\\Voices directory.
5. Start the Tomcat service.

## VIS Log Files

The VIS log files record the messages generated by the VIS application and are located in the ...\\usr\\local\\Tomcat7\\logs directory.

## Holly Log Files

The Holly log files record the messages generated by the Holly system and are located in the ...\\export\\home\\holly\\logs directory.

## IVG External Media Files

A client's collection of voice files can reside on a media server separate from the VXML Interaction Server (VIS) in systems using Interactive Voice Gateways (IVGs). The external voice project can be edited independently outside of Eclipse and then deployed to the server without building a new VXML project or .war file. This allows for quicker deployment and easier customization of the voice files.



The standard procedures for using external voice files are described in the Customizing External Media Files topic within the [VXML Interaction Server Installation Guide](#) or [VXML Interaction Server Configuration Guide](#). One difference in systems using IVGs is that voice files are located in the `.../usr/local/tomcat7/webapps/voices` directory within the IVG directory structure. Other than this difference, VIS and the accompanying external voice files are utilized in the standard manner.

## VIS to Platform Toolkit (PTK) Configuration

To configure VIS with PTK from the `toolkit.properties` file:

1. Locate the PTK `toolkit.properties` file (`...etc/Virtual Hold/toolkit.properties`) located on the VXML Interaction Server (VIS).
2. Edit the following line of code in the `toolkit.properties` file:  
**`com.virtualhold.toolkit.baseurl+http://location/VHTPlatformWS-v5/`**  
Where:  
*location* - IP address of the server containing the PTK application (the management instance server IP address).
3. Verify the following lines of code are automatically set as shown to enhance Answering Machine Detection (AMD) performance:  
**`com.virtualhold.toolkit.hvp.amd.url=/vht-ivg/amdRecord.jsp`**  
**`com.virtualhold.toolkit.hvp.amd.finalsilence=1s`**  
**`com.virtualhold.toolkit.hvp.amd.asengine=dtmf`**  
**`com.virtualhold.toolkit.hvp.amd.sensitivity=0.4`**  
**`com.virtualhold.toolkit.hvp.amd.maxspeech=20s`**  
**`com.virtualhold.toolkit.hvp.amd.maxinitialsilence=3s`**  
**`com.virtualhold.toolkit.hvp.amd.lifethreshold=4.0`**
4. Verify the following lines of code are set to the following defaults to support the Holly CTI Manager interface:  
**`com.virtualhold.toolkit.holly.ctiurl=https://localhost:8443/holly/update`**  
**`com.virtualhold.toolkit.holly.serviceid=1`**  
**`com.virtualhold.toolkit.holly.callvariablenumber=10`**
5. Save the `toolkit.properties` file. These changes will take effect immediately
6. Repeat Steps 1 through 5 on each VIS/IVG server.