



Interactive Voice Gateway (IVG) Avaya Configuration Guide Version 3.2.0

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

Required Inbound IVG Avaya Configuration

The Avaya components used with the Interactive Voice Gateway (IVG) application must be configured correctly for inbound calls to be handled by IVG. The following procedures use the Avaya Site Administration (other comparable terminal emulators can be used if necessary) and System Manager applications to configure the Avaya components. Once configured, vectors must be programmed in Avaya Communication Manager to load the required VDNs. Refer to [Building Avaya Vectors for IVGs](#) for more information.

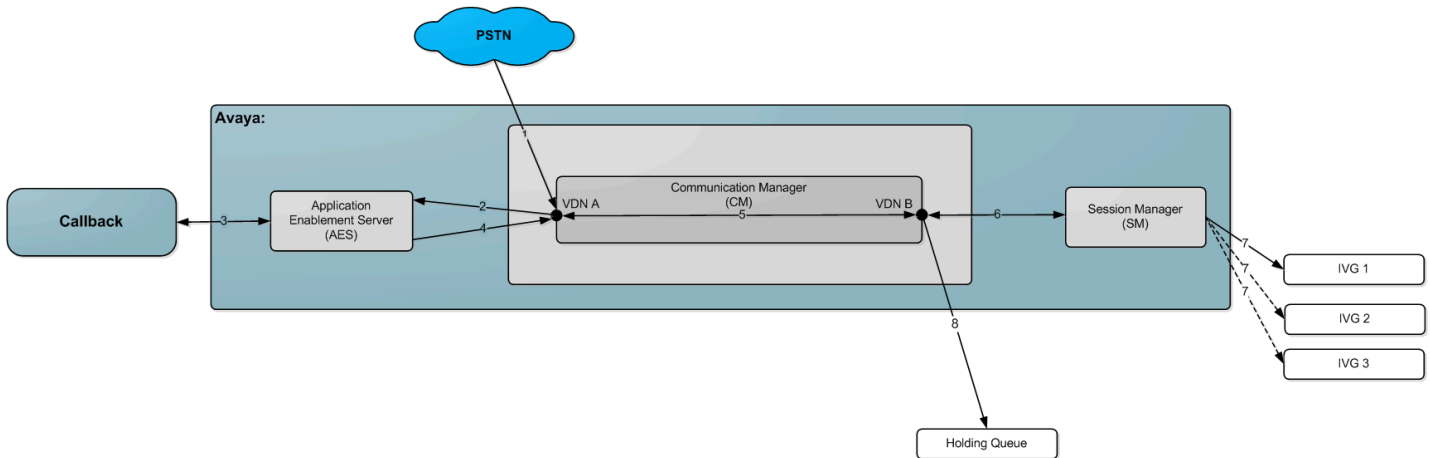
Multiple IVG Load Balancing and Failover

In Avaya integrations using multiple IVGs, it is possible to leverage Avaya and IVG mechanisms to support the following functions:

- Load balancing
- High availability
- Failover

Callflow

The following diagram details how inbound calls are handled in multiple IVG integrations.



Calls progress through this integration as follows:

1. Inbound calls arrive at the PSTN (telephone system) and are routed to VDN A, the inbound vector directory number. TDM protocol is used.
2. An adjunct route directs the calls to AES (Avaya enablement server). Proprietary Avaya protocol is used.



3. AES directs the calls to Callback where the appropriate treatment is determined. In this case, calls are routed back to VDN A, VDN B, Session Manager and on to the IVGs. Proprietary Virtual Hold protocol is used.
4. Callback attaches routing information to the calls and directs them back to VDN A (Communications Manager). Proprietary Avaya protocol is used.
5. Communication Manager reads the routing information and directs the calls to VDN B. Proprietary Avaya protocol is used.
6. Communication Manager directs the calls to Session Manager. SIP protocol is used.
7. Session Manager load balances the calls (using a proprietary Avaya algorithm) across the available IVGs. SIP protocol is used.
8. If the IVGs do not receive the load balanced calls for any reason (failure of all IVGs, incorrect DNIS configuration, etc.), Communication Manager routes the calls to a holding queue. Proprietary Avaya protocol is used.

Avaya Configuration

Use the following tools to configure Avaya components to function correctly with and support IVG implementations:

- [Avaya Site Administrator](#) - Creates dialing plans (including component parts) and configures trunk groups.
- [Avaya System Manager](#) - Creates SIP entities, entity links, and configures routing policies and dial patterns.

Avaya Site Administrator

From the Avaya Site Administrator, perform the following:

1. Create a dialing plan that is set to handle the appropriate dialed strings with each string set to a call type of **UDP**.
2. Configure the matching patterns for this dialing plan to use **Automatic Alternative Routing**.
3. Configure the dialed strings for the matching patterns to use the appropriate route pattern and a call type of **aar**. Output of the Avaya Site Administrator should contain results similar to the following excerpts:

Dialplan and AAR

```
display dialplan analysis                               Page 1 of 12
              DIAL PLAN ANALYSIS TABLE
              Location: all      Percent Full: 3
Dialed Total Call  Dialed Total Call  Dialed Total Call
String Length Type  String Length Type  String Length Type
1      5 ext 9      1 fac
2      2 fac *      3 fac
3      5 ext #      3 fac
400    7 udp
41     2 fac
45     5 ext
480    5 udp
4804   5 udp
487    5 udp
```



```

488    5  udp
489    5  ext
5      5  ext
6      5  ext
7      3  dac
8      6  ext

```

display uniform-dialplan 1 Page 1 of 2

UNIFORM DIAL PLAN TABLE

Percent Full: 0

Matching Pattern	Len	Del	Insert Digits	Node Net Conv Num
48	5	0	aar	n
480	5	0	aar	n

display aar analysis 4 Page 1 of 2

AAR DIGIT ANALYSIS TABLE

Location: all Percent Full: 1

Dialed String	Total Min	Route Max	Call Pattern	Node Type	ANI Num	Reqd
4	7	7	999	aar	n	
400xxxx	7	7	6	aar	n	
4801x	5	5	3	aar	n	
4802x	5	5	3	aar	n	
4803x	5	5	5	aar	n	
4804x	5	5	5	aar	n	
4805x	5	5	5	aar	n	
4806x	5	5	5	aar	n	
4807x	5	5	5	aar	n	
487xx	5	5	1	aar	n	
488xx	5	5	1	aar	y	
5	7	7	999	aar	n	
53xxx	5	5	1	aar	n	
54xxx	5	5	1	aar	n	
6	7	7	999	aar	n	

display trunk-group 5 Page 2 of 22

Group Type: sip

TRUNK PARAMETERS

Unicode Name: auto

Redirect On OPTIM Failure: 5000

SCCAN? n

Digital Loss Group: 18

Preferred Minimum Session Refresh Interval(sec): 600

Disconnect Supervision - In? y Out? y

XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n



display trunk-group 5 Page 3 of 22

TRUNK FEATURES

ACA Assignment? n Measured: none
Maintenance Tests? y

Numbering Format: private
UI Treatment: shared
Maximum Size of UI Contents: 128
Replace Restricted Numbers? n
Replace Unavailable Numbers? n

Modify Tandem Calling Number: no
Send UCID? y
Show ANSWERED BY on Display? y
DSN Term? n

display trunk-group 5 Page 4 of 22

SHARED UI FEATURE PRIORITIES

ASAI: 1

Universal Call ID (UCID): 2

MULTI SITE ROUTING (MSR)

In-VDN Time: 3
VDN Name: 4
Collected Digits: 5
Other LAI Information: 6
Held Call UCID: 7

display trunk-group 5 Page 5 of 22

PROTOCOL VARIATIONS

Mark Users as Phone? n
Prepend '+' to Calling Number? n
Send Transferring Party Information? n
Network Call Redirection? y
Send Diversion Header? n
Support Request History? y
Telephone Event Payload Type:

Convert 180 to 183 for Early Media? n
Always Use re-INVITE for Display Updates? n
Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
Enable Q-SIP? n

display trunk-group 5 Page 6 of 22



TRUNK GROUP

Administered Members (min/max): 1/24

GROUP MEMBER ASSIGNMENTS Total Administered Members: 24

Port	Name
1: T00019	IVG to
2: T00020	IVG to
3: T00021	IVG to
4: T00022	IVG to
5: T00023	IVG to
6: T00024	IVG to
7: T00025	IVG to
8: T00026	IVG to
9: T00027	IVG to
10: T00028	IVG to
11: T00054	IVG to
12: T00055	IVG to
13: T00056	IVG to
14: T00057	IVG to
15: T00058	IVG to

display trunk-group 5

Page 7 of 22

TRUNK GROUP

Administered Members (min/max): 1/24

GROUP MEMBER ASSIGNMENTS Total Administered Members: 24

Port	Name
16: T00059	IVG to
17: T00060	IVG to
18: T00061	IVG to
19: T00062	IVG to
20: T00063	IVG to
21: T00064	IVG to
22: T00065	IVG to
23: T00066	IVG to
24: T00067	IVG to
25:	

display route-pattern 5

Page 1 of 3

Pattern Number: 5 Pattern Name: IVG to SM

SCCAN? n Secure SIP? n

Grp No	FRL Mrk	NPA Lmt	Pfx List	Hop Del	Toll Digits	No. Inserted	DCS/ IXC	Intw
1: 5	0							n user
2:								n user
3:								n user
4:								n user
5:								n user



```

6:                                     n user
   BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR
   0 1 2 M 4 W Request Dgts Format
                               Subaddress
1: y y y y n n rest lev0-pvt none
2: y y y y n n rest none
3: y y y y n n rest none
4: y y y y n n rest none
5: y y y y n n rest none
6: y y y y n n rest none

```

4. Configure the route pattern to link to a trunk group.
5. Configure the trunk group to be of the type **SIP** (routes calls from the Avaya Communication Manager to the System Manager). Output of the Avaya Site Administrator should contain results similar to the following excerpts:

Trunk Group and Signalling Group

```

display trunk-group 5                               Page 1 of 22
                TRUNK GROUP
Group Number: 5      Group Type: sip      CDR Reports: y
Group Name: IVG to SM      COR: 1      TN: 1      TAC: 726
Direction: two-way      Outgoing Display? n
Dial Access? n          Night Service:
Queue Length: 0
Service Type: tie      Auth Code? n
                        Member Assignment Method: auto
                        Signaling Group: 5
                        Number of Members: 24

display signaling-group 5
                SIGNALING GROUP
Group Number: 5      Group Type: sip
IMS Enabled? n      Transport Method: tls
Q-SIP? n
IP Video? n          Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM

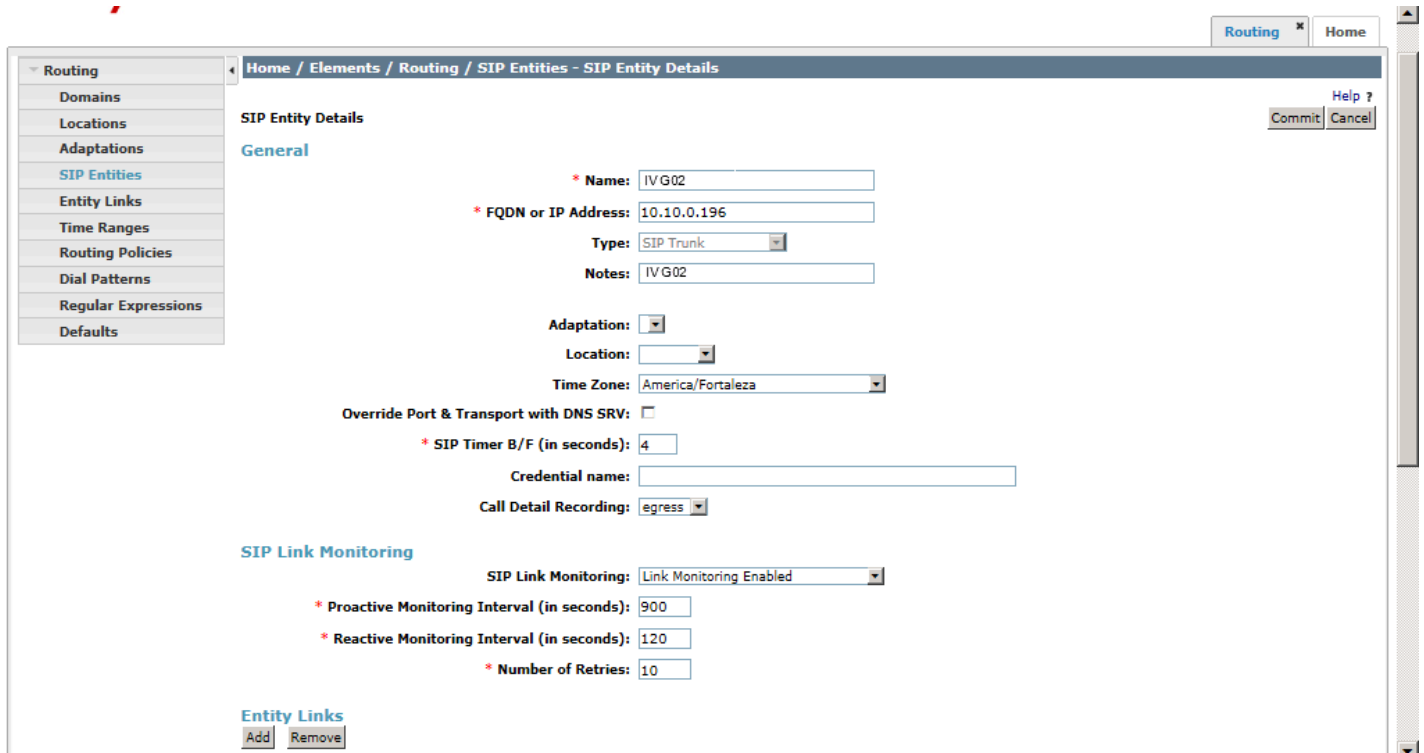
Near-end Node Name: CLAN01A04      Far-end Node Name: S8800SM
Near-end Listen Port: 5061      Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Secondary Node Name:
Far-end Domain:
Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate      RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload      Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3      IP Audio Hairpinning? n
Enable Layer 3 Test? y      Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n      Alternate Route Timer(sec): 6

```

Avaya System Manager

From the Avaya System Manager, perform the following:

1. For each IVG in the network routing plan, create a SIP entity and set the type to **SIP Trunk** and SIP Link Monitoring to **Link Monitoring Enabled**.



The screenshot shows the Avaya System Manager interface for configuring a SIP Entity. The breadcrumb trail is: Home / Elements / Routing / SIP Entities - SIP Entity Details. The left-hand navigation menu includes: Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and is divided into sections: 'General' and 'SIP Link Monitoring'. In the 'General' section, the following fields are visible: Name (IVG02), FQDN or IP Address (10.10.0.196), Type (SIP Trunk), Notes (IVG02), Adaptation (dropdown), Location (dropdown), Time Zone (America/Fortaleza), Override Port & Transport with DNS SRV (checkbox), SIP Timer B/F (in seconds) (4), Credential name (text field), and Call Detail Recording (egress). In the 'SIP Link Monitoring' section, the following fields are visible: SIP Link Monitoring (Link Monitoring Enabled), Proactive Monitoring Interval (in seconds) (900), Reactive Monitoring Interval (in seconds) (120), and Number of Retries (10). At the bottom of the page, there is an 'Entity Links' section with 'Add' and 'Remove' buttons. The top right corner of the window has 'Routing' and 'Home' tabs, and 'Commit' and 'Cancel' buttons.

2. For each IVG in the network routing plan, create an Entity Link that uses the UDP protocol.

Entity Links

17 Items Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
<input type="checkbox"/> Acme	S8800SM	UDP	5060	Acme	5060	Trusted	
<input type="checkbox"/> Asterisk	S8800SM	TCP	5060	Asterisk	5060	Trusted	
<input type="checkbox"/> CiscoGW	S8800SM	UDP	5060	CiscoGW	5060	Trusted	
<input type="checkbox"/> CONSTELLATION 2 SM	S8800SM	TLS	5061	CONSTELLATION	5061	Trusted	
<input type="checkbox"/> CUCM	S8800SM	TLS	5061	CUCM	5061	Trusted	
<input type="checkbox"/> CYARA02	S8800SM	TCP	5060	CYARA02	5060	Trusted	
<input type="checkbox"/> MIDWAY	S8800SM	UDP	5060	MIDWAY	5070	Trusted	
<input type="checkbox"/> IVG	S8800SM	UDP	5060	IVG	5060	Trusted	
<input type="checkbox"/> IVG02	S8800SM	UDP	5060	IVG02	5060	Trusted	
<input type="checkbox"/> IVG03	S8800SM	UDP	5060	IVG03	5060	Trusted	
<input type="checkbox"/> IVG04	S8800SM	UDP	5060	IVG04	5060	Trusted	
<input type="checkbox"/> IVG05	S8800SM	UDP	5060	IVG05	5060	Trusted	
<input type="checkbox"/> Paraguay	S8800SM	TLS	5061	Paraguay	5061	Trusted	
<input type="checkbox"/> Quasar 2 SM	S8800SM	UDP	5060	Quasar	5060	Trusted	
<input type="checkbox"/> S8800CM TCP	S8800SM	TCP	5060	S8800CM	5060	Trusted	

Select : All, None < Previous Page 1 of 2 Next >

3. Configure the IVG destination in the routing policy to the IVG SIP entity.

Routing Policy Details

General

* Name:

Disabled:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
IVG02	10.10.0.196	SIP Trunk	IVG02

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/> 0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

1 Item Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>						

- Configure the required dial patterns, with the Originating Location and Routing Policy Names, for those created for IVG usage.

The screenshot shows the 'Dial Patterns' configuration page in the Avaya system. The page title is 'Home / Elements / Routing / Dial Patterns - Dial Patterns'. On the left is a sidebar with a tree view containing: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns (highlighted), Regular Expressions, and Defaults. The main content area has a 'Dial Patterns' section with buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below this is a table with 21 items. The table has columns: Pattern, Min, Max, Emergency Call, SIP Domain, and Notes. At the bottom of the table, there is a 'Select' dropdown set to 'All, None' and a pagination control showing 'Page 1 of 2'.

Pattern	Min	Max	Emergency Call	SIP Domain	Notes
<input type="checkbox"/> 2015xx	6	6	<input type="checkbox"/>	qaleb.local	OB to Hammer G5 using CiscoGW
<input type="checkbox"/> 4006xxxx	7	7	<input type="checkbox"/>	qaleb.local	Route to Cisco GW
<input type="checkbox"/> 45xxxx	5	5	<input type="checkbox"/>	-ALL-	SIP to VDN on S8800CM
<input type="checkbox"/> 4801x	5	5	<input type="checkbox"/>	qaleb.local	Quasar Route Point
<input type="checkbox"/> 4802x	5	5	<input type="checkbox"/>	qaleb.local	Midway Route Points
<input type="checkbox"/> 4803	5	5	<input type="checkbox"/>	qaleb.local	SIP to IVG
<input type="checkbox"/> 4804	5	5	<input type="checkbox"/>	qaleb.local	SIP to IVG02
<input type="checkbox"/> 4805	5	5	<input type="checkbox"/>	qaleb.local	SIP to IVG03
<input type="checkbox"/> 4806	5	5	<input type="checkbox"/>	qaleb.local	SIP to IVG04
<input type="checkbox"/> 4807	5	5	<input type="checkbox"/>	qaleb.local	SIP to IVG05
<input type="checkbox"/> 488xx	5	5	<input type="checkbox"/>	qaleb.local	SIP to EPMS
<input type="checkbox"/> 52xxxx	5	5	<input type="checkbox"/>	qaleb.local	Asterisk Connection
<input type="checkbox"/> 5300x	5	5	<input type="checkbox"/>	qaleb.local	SIP Station to SIP Station within the S8800
<input type="checkbox"/> 54xxxx	5	5	<input type="checkbox"/>	qaleb.local	Station to Station within the S8800
<input type="checkbox"/> 55xxxx	5	5	<input type="checkbox"/>	-ALL-	SIP to VDN on S8800CM



Routing x Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details Help ?
Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ¹ ▲	Originating Location Notes	Routing Policy Name	Rank ² ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	VHT Lab		IVG02	0	<input checked="" type="checkbox"/>	IVG02	

Select : All, None

Denied Originating Locations

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------



Building Avaya Vectors for IVGs (Samples)

You must build vectors for your VDNs in Avaya Communication Manager. Vectors provide routing instructions for the VDNs. This integration requires four VDNs, because calls below threshold are routed directly from the Entry VDN to the Holding VDN. Calls above threshold are routed from the Entry VDN to the Routing VDN for IVR treatment and then sent to the Holding VDN, a skill, or through an Interactive Voice Gateway (IVG) to the Callback VDN. The four are:

- [Entry](#)
- [Routing](#)
- [Holding](#)
- [Callback](#)

Entry

VDN

```

VECTOR DIRECTORY NUMBER

      Extension: 55190
      Name*: VHT IVG Entry
      Destination: Vector Number      90
      Attendant Vectoring? n
      Meet-me Conferencing? n
      Allow VDN Override? y
      COR: 1
      TN*: 1
      Measured: none

      VDN of Origin Annc. Extension*:
      1st Skill*:
      2nd Skill*:
      3rd Skill*:

```

* Follows VDN Override Rules

VECTOR DIRECTORY NUMBER

AUDIX Name:



Return Destination*:
 VDN Timed ACW Interval*: After Xfer or Held Call Drops*? n
 BSR Application*:
 BSR Available Agent Strategy*: 1st-found Used for BSR Polling? n
 BSR Tie Strategy*: system

Observe on Agent Answer? n

Send VDN as Called Ringing Name Over QSIG? n

Display VDN for Route-To DAC*? n
 VDN Override for ASAI Messages*: no

BSR Local Treatment*? n

Reporting for PC or POM Calls? n
 Pass Prefixed CPN to VDN/Vector*? system

* Follows VDN Override Rules

VECTOR DIRECTORY NUMBER

VDN VARIABLES*

Var	Description	Assignment
V1		
V2		
V3		
V4		
V5		
V6		
V7		
V8		
V9		

VDN Time-Zone Offset*: + 00:00
 Daylight Saving Rule*: system

Use VDN Time Zone For Holiday Vectoring*? n
 Apply Ringback for Auto Answer calls*? y

* Follows VDN Override Rules

Vector

CALL VECTOR

Number: 90 Name: VHT IVG Ent
 Multimedia? n Attendant Vectoring? n Meet-me Conf? n Lock? n



```
Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y 3.0 Enhanced? y
01 wait-time 0 secs hearing ringback
02 set A = digits ADD 12345
03 adjunct routing link 5
04 wait-time 5 secs hearing ringback
05 route-to number 55202 with cov n if unconditionally
06 disconnect after announcement none
07 stop
08
09
10
11
12
```

Note:

It is recommended that adjunct be set to **routing link 1** for TSAPI integrations and **routing link 5** for CVLAN integrations.

Routing

If the number of concurrent calls reaches the limit configured in the IVG management system for inboundmaxcalls (default value = 40), all the excessive calls are rejected by the IVG, so Avaya Communication Manager can route those calls to Holding Queue VDN . This is handled via Routing VDN and instructions to handle this scenario are provided in the following sample Routing [Vector](#).

VDN

VECTOR DIRECTORY NUMBER

```
Extension: 55200
Name*: VHT IVG Rte to 48050
Destination: Vector Number 5200
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? y
COR: 1
TN*: 1
Measured: none
```

VDN of Origin Annc. Extension*:



1st Skill*:
2nd Skill*:
3rd Skill*:

* Follows VDN Override Rules

VECTOR DIRECTORY NUMBER

AUDIX Name:
Return Destination*:
VDN Timed ACW Interval*: After Xfer or Held Call Drops*? n
BSR Application*:
BSR Available Agent Strategy*: 1st-found Used for BSR Polling? n
BSR Tie Strategy*: system

Observe on Agent Answer? n

Send VDN as Called Ringing Name Over QSIG? n

Display VDN for Route-To DAC*? n
VDN Override for ASAI Messages*: no

BSR Local Treatment*? n

Reporting for PC or POM Calls? n
Pass Prefixed CPN to VDN/Vector*? system

* Follows VDN Override Rules

VECTOR DIRECTORY NUMBER

VDN VARIABLES*

Var	Description	Assignment
V1		
V2		
V3		
V4		
V5		
V6		
V7		
V8		
V9		

VDN Time-Zone Offset*: + 00:00
Daylight Saving Rule*: system

Use VDN Time Zone For Holiday Vectoring*? n
Apply Ringback for Auto Answer calls*? y



* Follows VDN Override Rules

Vector

CALL VECTOR

Number: 5200 Name: VHT IVG 48050
 Multimedia? n Attendant Vectoring? n Meet-me Conf? n Lock? n
 Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
 Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
 Variables? y 3.0 Enhanced? y
 01 wait-time 0 secs hearing ringback
 02 route-to number 48050 with cov n if unconditionally
 03 wait-time 5 secs hearing ringback
 04 route-to number 55202 with cov n if unconditionally
 05 disconnect after announcement none
 06 stop
 07
 08
 09
 10
 11
 12

Holding

VDN

VECTOR DIRECTORY NUMBER

Extension: 55202
 Name*: VHT IVG Hold
 Destination: Vector Number 82
 Attendant Vectoring? n
 Meet-me Conferencing? n
 Allow VDN Override? n
 COR: 1
 TN*: 1
 Measured: internal
 Acceptable Service Level (sec): 20
 VDN of Origin Annc. Extension*:
 1st Skill*:
 2nd Skill*:



3rd Skill*:

* Follows VDN Override Rules

VECTOR DIRECTORY NUMBER

AUDIX Name:

Return Destination*:

VDN Timed ACW Interval*: After Xfer or Held Call Drops*? n

BSR Application*:

BSR Available Agent Strategy*: 1st-found Used for BSR Polling? n

BSR Tie Strategy*: system

Observe on Agent Answer? n

Send VDN as Called Ringing Name Over QSIG? n

Display VDN for Route-To DAC*? n

VDN Override for ASAI Messages*: no

BSR Local Treatment*? n

Reporting for PC or POM Calls? n

Pass Prefixed CPN to VDN/Vector*? system

* Follows VDN Override Rules

VECTOR DIRECTORY NUMBER

VDN VARIABLES*

Var	Description	Assignment
V1		
V2		
V3		
V4		
V5		
V6		
V7		
V8		
V9		

VDN Time-Zone Offset*: + 00:00

Daylight Saving Rule*: system

Use VDN Time Zone For Holiday Vectoring*? n

Apply Ringback for Auto Answer calls*? y

* Follows VDN Override Rules



Vector

CALL VECTOR

Number: 82 Name: VHT IVG Hold
Multimedia? n Attendant Vectoring? n Meet-me Conf? n Lock? n
Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y 3.0 Enhanced? y
01 wait-time 0 secs hearing ringback
02 queue-to skill 5 pri m
03 wait-time 30 secs hearing ringback
04 goto step 3 if unconditionally
05 disconnect after announcement none
06 stop
07
08
09
10
11
12

Callback

VDN

VECTOR DIRECTORY NUMBER

Extension: 55203
Name*: VHT IVG CB
Destination: Vector Number 83
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none

VDN of Origin Annc. Extension*:
1st Skill*:
2nd Skill*:
3rd Skill*:

* Follows VDN Override Rules

VECTOR DIRECTORY NUMBER

AUDIX Name:

Return Destination*:

VDN Timed ACW Interval*: After Xfer or Held Call Drops*? n

BSR Application*:

BSR Available Agent Strategy*: 1st-found Used for BSR Polling? n

BSR Tie Strategy*: system

Observe on Agent Answer? n

Send VDN as Called Ringing Name Over QSIG? n

Display VDN for Route-To DAC*? n

VDN Override for ASAI Messages*: no

BSR Local Treatment*? n

Reporting for PC or POM Calls? n

Pass Prefixed CPN to VDN/Vector*? system

* Follows VDN Override Rules

VECTOR DIRECTORY NUMBER

VDN VARIABLES*

Var	Description	Assignment
-----	-------------	------------

V1

V2

V3

V4

V5

V6

V7

V8

V9

VDN Time-Zone Offset*: + 00:00

Daylight Saving Rule*: system

Use VDN Time Zone For Holiday Vectoring*? n

Apply Ringback for Auto Answer calls*? y

* Follows VDN Override Rules



Vector

CALL VECTOR

Number: 83 Name: VHT IVG CB
Multimedia? n Attendant Vectoring? n Meet-me Conf? n Lock? n
Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y 3.0 Enhanced? y
01 wait-time 0 secs hearing ringback
02 queue-to skill 5 pri h
03 wait-time 30 secs hearing ringback
04 goto step 3 if unconditionally
05 disconnect after announcement none
06 stop
07
08
09
10
11
12



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 four management features which require specific attention in IVG systems:

- Workers
- Service Provider
- Affiliates
- Applications

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

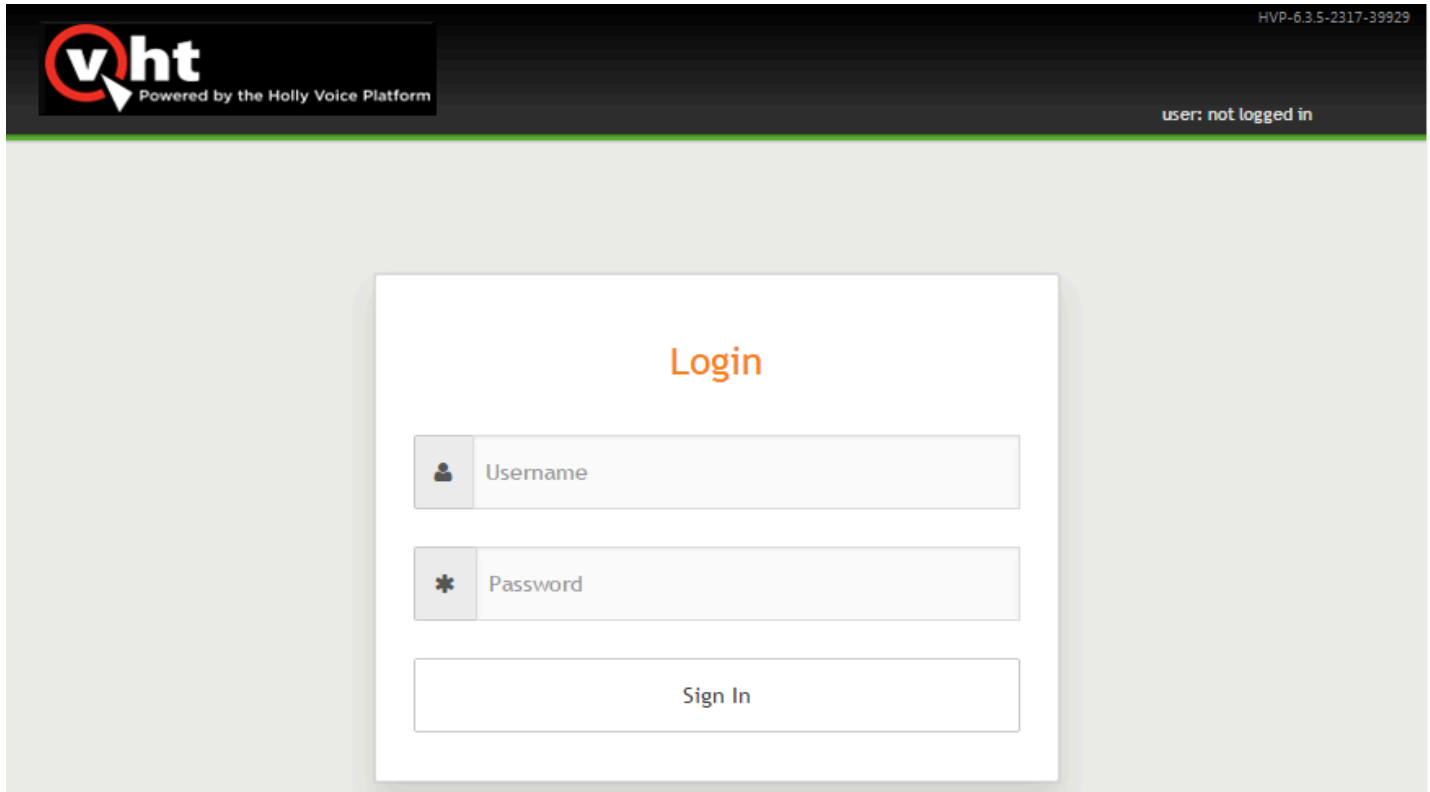
Log In and Out

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:

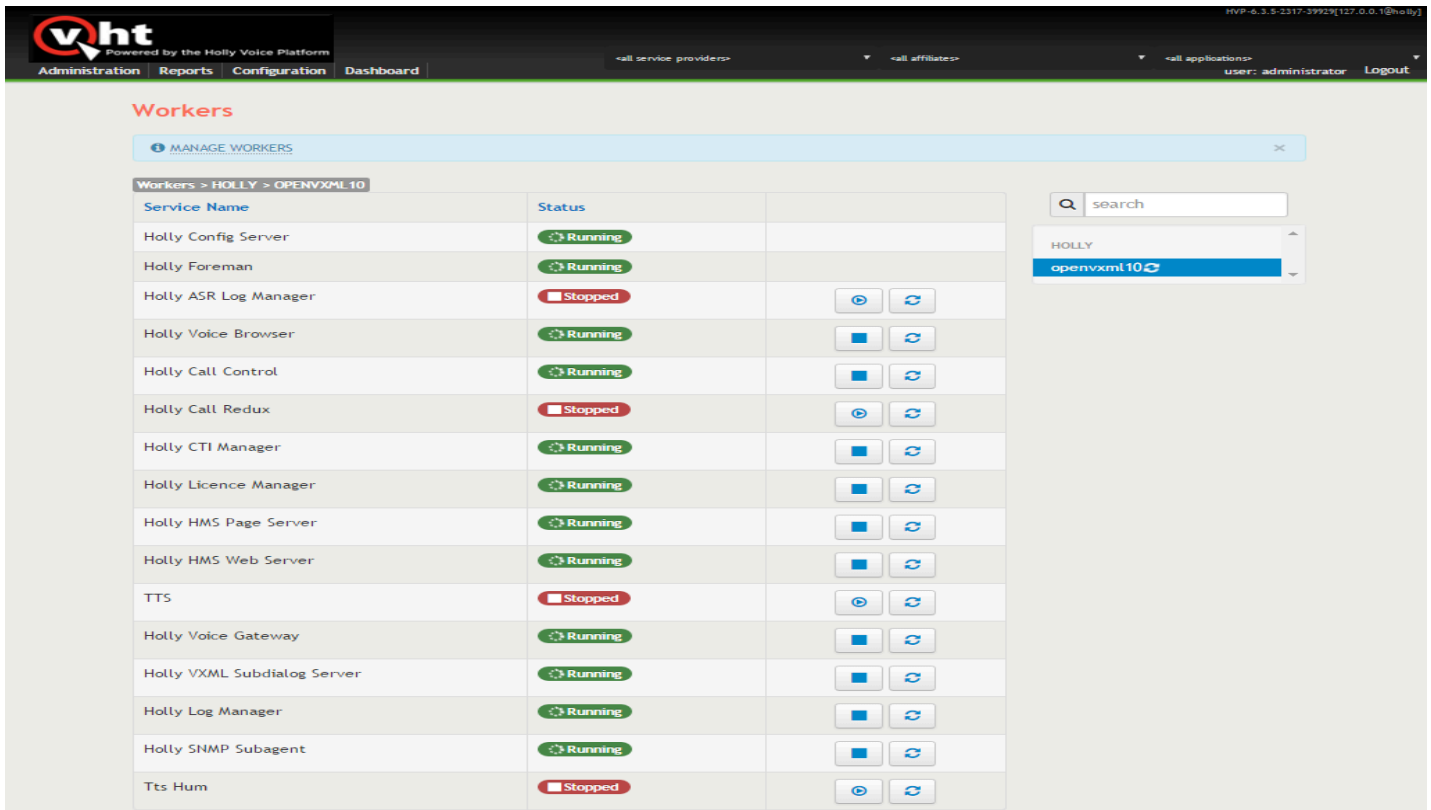
You must log into the IVG management system before these procedures can be utilized.

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 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.
Holly Log Manager	logmgr	Required for writing diagnostic log information.

Worker Name	Process Name	Description
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.



The screenshot displays the 'Workers' management page in the VHT interface. The page title is 'Workers' and it includes a 'MANAGE WORKERS' button. Below the title, there is a breadcrumb trail: 'Workers > HOLLY > OPENVXML10'. A table lists various workers with their status and control icons. The 'Holly SNMP Subagent' worker is highlighted in the table. On the right side, there is a search bar and a dropdown menu showing 'openvxml10' selected.

Service Name	Status	Control Icons
Holly Config Server	Running	[Start] [Refresh]
Holly Foreman	Running	[Start] [Refresh]
Holly ASR Log Manager	Stopped	[Start] [Refresh]
Holly Voice Browser	Running	[Start] [Refresh]
Holly Call Control	Running	[Start] [Refresh]
Holly Call Redux	Stopped	[Start] [Refresh]
Holly CTI Manager	Running	[Start] [Refresh]
Holly Licence Manager	Running	[Start] [Refresh]
Holly HMS Page Server	Running	[Start] [Refresh]
Holly HMS Web Server	Running	[Start] [Refresh]
TTS	Stopped	[Start] [Refresh]
Holly Voice Gateway	Running	[Start] [Refresh]
Holly VXML Subdialog Server	Running	[Start] [Refresh]
Holly Log Manager	Running	[Start] [Refresh]
Holly SNMP Subagent	Running	[Start] [Refresh]
Tts Hum	Stopped	[Start] [Refresh]

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 a dropdown for 'Service Provider' (set to VHT), and text boxes for 'Domain Name' and 'Domain Description' (both set to VHT).
- Service Provider Contact Details:** Contains text boxes for 'Name', 'Email', 'Phone', and 'Address'.
- Licence Port Allocation:** Contains text boxes for 'Max Available Ports' and 'Warn Ports', both set to 999.
- Alarm Recipients:** Contains a dropdown for 'Alarm Type' (set to email), an 'Address' text box, and a list area with 'Add', 'Replace', and 'Delete' buttons.
- Application Parameters:** Contains 'Key' and 'Value' text boxes, a list area with 'Set', 'Replace', and 'Delete' buttons, and a 'Preset Parameters' dropdown (set to 'Set Application Type To CCXML') with a 'Set' button.
- Service Provider Numbers:** Contains a 'DNIS Numbers' text box with '69300 - 69399' and 'outbound - outbound', and a list area with '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 <new service provider> when creating a new provider.
Domain Name	Enter the desired service provider name when creating a new service provider. (VHT_ServiceProvider 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 Alarm Recipients area) is sent when this value is exceeded. This value is defaulted to 999.</p> <p>Note: 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 Alarm Recipients area) gives advance notice of approaching the port allocation limit. This value is defaulted to 999.</p> <p>Note: 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. Ensure the DNIS numbers represent the range of numbers available to this service provider.

Note:

DNIS numbers are case-sensitive and can be alphanumeric.

5. Click **Add**.

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 added 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:** A form with dropdown menus for 'Service Provider' (VHT-ServiceProvider), 'Affiliate' (VHT-Affiliate), 'Domain Name' (VHT-Affiliate), and 'Domain Description' (VHT-Affiliate). Buttons for 'Edit Service Provider...' and 'Edit Applications...' are visible.
- Affiliate Contact Details:** Input fields for 'Name', 'Email', 'Phone', and 'Address'.
- Licence Port Allocation:** Input fields for 'Max Available Ports' (400) and 'Warn Ports' (300), with '(Available 400)' shown next to the Max Available Ports field.
- Alarm Recipients:** A table with 'Alarm Type' (email) and 'Address' columns, and buttons for 'Add', 'Replace', and 'Delete'.
- Application Parameters:** A table with 'Key' and 'Value' columns, and buttons for 'Set', 'Replace', and 'Delete'. A 'Preset Parameters' dropdown is set to 'Set Application Type To CCXML'.
- Affiliate Numbers:** A table with 'DNIS Numbers' and buttons for 'Add', 'Replace', and 'Delete'. The table contains entries like '48241 - 48241', '48249 - 48249', 'outbound - outbound', and 'outreach - outreach'.

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 (VHT_ServiceProvider is recommended).
Affiliate	Unique name of previously created affiliates. Select an affiliate here when editing an existing affiliate. Leave this field set to <new affiliate> when creating a new affiliate.
Domain Name	Enter the desired affiliate name when creating a new affiliate (VHT_Affiliate is recommended).
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 Alarm Recipients area) is sent when this value is exceeded. Set this value to 0 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 Alarm Recipients area) gives advance notice of approaching port allocation limit. Set this value to 0 indicating that a license from the parent object is used.

3. Click **Save Affiliate**.
4. Complete the Affiliates **Numbers Available** area. Ensure the DNIS numbers represent a unique subset of the range of numbers available to the associated Service Provider.

Note:

DNIS numbers are case-sensitive and can be alphanumeric .

5. Click **Add**.

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.
- Agent Priority (e.g. **VHT_AgentPriority**) - Optional, provision as required.
- 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.

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

- Select Application:** Includes dropdown menus for 'Service Provider' (VHT-ServiceProvider), 'Affiliate' (VHT-Affiliate), and 'Application' (VHT_Inbound). It also has text input fields for 'Name' (VHT_Inbound) and 'Description' (VHT_Inbound), and a 'Licence Exception URL' field.
- URLs:** Features a 'URL' input field, a 'Fetch Time Out' dropdown set to 'sec', and a list of 'URLs' containing 'http://localhost:8080/VIS/PlatformSupport_HVP/Begin?Tenant=VHT&MODE=HVPAvaya'. Buttons for 'Add', 'Replace', 'Delete', 'Move Up', and 'Move Down' are present.
- Licence Port Allocation:** Shows 'Max Available Ports' (0), 'Warn Ports' (0), and 'Licence Life' (0s). A note indicates '(Available 400)'.
- Alarm Recipients:** Includes an 'Alarm Type' dropdown (email) and an 'Address' input field. Buttons for 'Add', 'Replace', and 'Delete' are available.
- Application Parameters:** Contains 'Key' and 'Value' input fields. The 'Value' field contains 'ap.comhnrstodlg = 1', 'failure_destination = sip:56452@10.10.0.217', and 'type = application/voicexml+xml'. A 'Preset Parameters' dropdown is set to 'Set Application Type To CCXML'. Buttons for 'Set', 'Replace', and 'Delete' are provided.
- Application Numbers:** Features a 'DNIS Numbers' input field with a list containing '48241 - 48241' and '48249 - 48249'. Buttons for 'Add', 'Replace', and 'Delete' are present.

At the bottom of the interface, there are buttons for 'Delete the Application', 'Revert', and 'Save Application'.

- 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 (VHT_ServiceProvider is recommended).
Affiliate	Select the affiliate to which this application is associated (VHT_Affiliate 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 <new application> when creating a new application.
Name	Enter the desired application name when creating a new application (VHT_Inbound is recommended).
Description	Enter the desired description of 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 5 seconds. Click Add 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_HVP/Begin?Tenant=VHT&MODE=HVP</code>Avaya.</p> <ol style="list-style-type: none">1. Use Move Up and Move Down to ensure URLs are listed in desired order.2. Limit number of URLs inserted because fetch time outs are cumulative.3. Ensure last URL listed is local to browser so that access is assured.
License Port Allocation	
Max Available Ports	Maximum number of ports available to this application. A warning (configured in Alarm Recipients area) is sent when this value is exceeded. Set this value to 0 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 Alarm Recipients area and gives advance notice of approaching the port allocation limit. Set this value to 0 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 Set to enter parameters.
<p>At a minimum, the following parameters are required for the inbound IVR:</p> <p>ap.connhdrstodlg = 1</p> <p>failure_destination = location where <i>location</i> 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).</p> <p>type = application/voicexml+xml</p>	

3. Click **Save Application**.
4. Complete the Application **Numbers Available** area. Ensure the DNIS numbers represent a unique subset of the range of numbers available to the associated affiliate (**VHT_Affiliate** is recommended). An example setting for this area is 48231 - 48239.

Note:

DNIS numbers are case-sensitive and can be alphanumeric.

5. Click **Add**.

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	
Service Provider	Select the service provider to which this application is associated (VHT_ServiceProvider is recommended).
Affiliate	Select the affiliate to which this application is associated (VHT_Affiliate is recommended).
Application	Unique name of previously created applications. Select an application here when editing an existing application. Leave the field set to <new application> when creating a new application.



Field	Description
Name	Enter the desired application name when creating a new application (VHT_Outbound is recommended).
Description	Enter the desired description of 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 5 seconds. Click Add after entering the Fetch Time Out.
URLs	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_HVP/Outbound?MODE=HVP</code> Avaya. <ol style="list-style-type: none">1. Use Move Up and Move Down to ensure URLs are listed in desired order.2. Limit number of URLs inserted because fetch time outs are cumulative.3. Ensure last URL listed is local to browser so that access is assured.
License Port Allocation	
Max Available Ports	Maximum number of ports available to this application. A warning (if configured in Alarm Recipients area) is sent when this value is exceeded. Set this value to 0 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 Alarm Recipients area) gives advance notice of approaching the port allocation limit. Set this value to 0 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.
Value	Value of key used by this application. Complete Key and Value fields and click Set to enter parameters.
At a minimum, the following parameters are required for the outbound IVR: type = application/voicexml+xml	

3. Click **Save Application**.
4. Complete the Application **Numbers Available** area. Ensure the DNIS numbers represent a unique subset of the range of numbers available to the associated affiliate (**VHT_Affiliate** for example). An example setting for this area is outbound - outbound.

Note:

DNIS numbers are case-sensitive and can be alphanumeric.

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

Agent Priority Application

To create or edit the Agent Priority 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 (VHT_ServiceProvider is recommended).
Affiliate	Select the affiliate to which this application is associated. Set this value to (VHT_Affiliate is recommended).
Application	Unique name of previously created application. Select an application here when editing an existing application. Leave the field set to <new application> when creating a new application (VHT_AgentPriority is recommended).
Name	Enter the desired application name when creating a new application (VHT_AgentPriority is recommended).
Description	Enter the desired description of the application.
URLs	
URL	URL where this application can be found. Always specify a fetch time out when inserting a URL.

Field	Description
Fetch Time Out	Time allotted to fetch this URL. Recommended value is 5 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/AgentPriority</code>.</p> <ol style="list-style-type: none"> 1. Use Move Up and Move Down to ensure URLs are listed in desired order. 2. Limit number of URLs inserted because fetch time outs are cumulative. 3. Ensure last URL listed is local to browser so that access is assured.
License Port Allocation	
Max Available Ports	<p>Maximum number of ports available to this application. A warning (if configured in Alarm Recipients area) is sent when this value is exceeded.</p> <p>Set this value to 0 indicating that a license from the parent object is used.</p>
Warn Ports	<p>Number of allocated ports used (by this application) at which a warning is generated. A warning (if configured in Alarm Recipients area) gives advance notice of approaching the port allocation limit.</p> <p>Set this value to 0 indicating that a license from the parent object is used.</p>
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 Set to enter parameters.
<p>At a minimum, the following parameters are required for Agent Priority IVR:</p> <p>type = application/voicexml+xml</p>	

3. Click **Save Application**.
4. Complete the Application **Numbers Available** area. Ensure the DNIS numbers represent a unique subset of the range of numbers available to the associated affiliate (**VHT_Affiliate** is recommended). An example setting for this area is `agntpriority - agntpriority`.

Note:

DNIS numbers are case-sensitive and can be alphanumeric.

5. Click **Add**.

Outreach Application

To create or edit the Outreach 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 (VHT_ServiceProvider is recommended).
Affiliate	Select the affiliate to which this application is associated. Set this value to (VHT_Affiliate is recommended).
Application	Unique name of previously created application. Select an application here when editing an existing application. Leave the field set to <new application> when creating a new application (VHT_Outreach is recommended).
Name	Enter the desired application name when creating a new application (VHT_Outreach is recommended).
Description	Enter the desired description of 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 5 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_HVP/Outreach?MODE=HVP</code>Avaya.</p> <ol style="list-style-type: none"> 1. Use Move Up and Move Down to ensure URLs are listed in desired order. 2. Limit number of URLs inserted because fetch time outs are cumulative. 3. Ensure last URL listed is local to browser so that access is assured.
License Port Allocation	

Field	Description
Max Available Ports	Maximum number of ports available to this application. A warning (if configured in Alarm Recipients area) is sent when this value is exceeded. Set this value to 0 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 Alarm Recipients area) gives advance notice of approaching the port allocation limit. Set this value to 0 indicating that a license from the parent object is used.
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 Set to enter parameters.
At a minimum, the following parameters are required for Outreach: type = application/voicexml+xml	

3. Click **Save Application**.
4. Complete the Application **Numbers Available** area. Ensure the DNIS numbers represent a unique subset of the range of numbers available to the associated affiliate (**VHT_Affiliate** is recommended). An example setting for this area is outreach - outreach.

Note:

DNIS numbers are case-sensitive and can be alphanumeric.

5. Click **Add**.

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 (VHT_ServiceProvider is recommended).
Affiliate	Select the affiliate to which this application is associated (VHT_Affiliate is recommended).
Application	Unique name of previously created applications. Select an application here when editing an existing application. Leave the field set to <new application> when creating a new application.
Name	Enter the desired application name when creating a new application (VHT_PromptRecorder 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 5 seconds. Click Add 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&MODE=HVP</code> for HVP systems, <code>http://localhost:8080/PRec/Begin?Ten...HT&MODE=AVPSIP</code> for AVP systems, <code>http://localhost:8080/PRec/Begin?Tenant=VHT&MODE=GVP</code> for GVP systems, and <code>http://localhost:8080/PRec/Begin?Tenant=VHT&MODE=CVP</code> for CVP systems.</p> <ol style="list-style-type: none">1. Use Move Up and Move Down to ensure URLs are listed in desired order.2. Limit number of URLs inserted because fetch time outs are cumulative.3. Ensure last URL listed is local to browser so that access is assured.
License Port Allocation	
Max Available Ports	Maximum number of ports available to this application. A warning (if configured in Alarm Recipients area) is sent when this value is exceeded. Set this value to 0 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 Alarm Recipients area) gives advance notice of approaching the port allocation limit. Set this value to 0 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 Set to enter parameters.
At a minimum, the following parameters are required for prompt recorder usage: type = application/voicexml+xml	

3. Click **Save Application**.
4. Complete the Application **Numbers Available** area. Ensure the DNIS numbers represent a unique subset of the range of numbers available to the associated affiliate (**VHT_Affiliate** for example). An example setting for this area is promptrecorder - promptrecorder.

Note:

DNIS numbers are case-sensitive and can be alphanumeric.

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

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 Audio Provider - SIP .
Pool	Pool or group of IVG servers (holly 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 Holly Globals .
Pool	Pool or group of IVG servers (holly 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 Holly Voice Browser .
Pool	Pool or group of IVG servers (holly for example).

10. 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
```

11. Configure the **jsruntimesizekb** parameter to **40960**. This setting should improve performance in high call volume systems using JavaScript. [Manual Configuration]
12. Click **Add** or **Modify** for this parameter.
13. 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** and **dthreads** 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.

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

Field	Description
Component	Component to be configured. Set this value to Holly Log Manager .
Pool	Pool or group of IVG servers (holly for example).

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

Field	Description
Pool	Pool or group of IVG servers (holly for example).

14. Select the **Trace Level** tab.
15. Ensure all parameters are set to **2: Status Messages**. [Automatic Configuration]
16. 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 [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 Data 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.

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
<code>logmgr_expire</code>	<code>logtokeep</code> Maximum number of days postgresSQL database log records are kept. This is the value set during installation in the <code>install_ivg.cfg</code> file.	10

Field		Description	Default Value
	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 folder structure. Data files older than the

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. 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_psswd
```

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

```
>postmap /etc/postfix/sasl_psswd
```

17. Verify action by verifying the `/etc/postfix/sasl_psswd.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. Save the toolkit.properties file. These changes will take effect immediately
5. Repeat Steps 1 - 4 on each VIS/IVG server.