



## **Genesys Voice Platform 7.6**

# Reference Manual

**The information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Telecommunications Laboratories, Inc.**

Copyright © 2006–2011 Genesys Telecommunications Laboratories, Inc. All rights reserved.

## About Genesys

Alcatel-Lucent's Genesys solutions feature leading software that manages customer interactions over phone, Web, and mobile devices. The Genesys software suite handles customer conversations across multiple channels and resources—self-service, assisted-service, and proactive outreach—fulfilling customer requests and optimizing customer care goals while efficiently using resources. Genesys software directs more than 100 million customer interactions every day for 4000 companies and government agencies in 80 countries. These companies and agencies leverage their entire organization, from the contact center to the back office, while dynamically engaging their customers. Go to [www.genesyslab.com](http://www.genesyslab.com) for more information.

Each product has its own documentation for online viewing at the Genesys Technical Support website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

## Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc., cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

## Your Responsibility for Your System's Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

## Trademarks

Genesys, the Genesys logo, and T-Server are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other trademarks and trade names referred to in this document are the property of other companies. The Crystal monospace font is used by permission of Software Renovation Corporation, [www.SoftwareRenovation.com](http://www.SoftwareRenovation.com).

## Technical Support from VARs

If you have purchased support from a value-added reseller (VAR), please contact the VAR for technical support.

## Technical Support from Genesys

If you have purchased support directly from Genesys, please contact Genesys Technical Support at the following regional numbers:

Region	Telephone	E-Mail
North and Latin America	+888-369-5555 (toll-free) +506-674-6767	<a href="mailto:support@genesyslab.com">support@genesyslab.com</a>
Europe, Middle East, and Africa	+44-(0)-127-645-7002	<a href="mailto:support@genesyslab.co.uk">support@genesyslab.co.uk</a>
Asia Pacific	+61-7-3368-6868	<a href="mailto:support@genesyslab.com.au">support@genesyslab.com.au</a>
Japan	+81-3-6361-8950	<a href="mailto:support@genesyslab.co.jp">support@genesyslab.co.jp</a>

Prior to contacting technical support, please refer to the [Genesys Technical Support Guide](#) for complete contact information and procedures.

## Ordering and Licensing Information

Complete information on ordering and licensing Genesys products can be found in the [Genesys Licensing Guide](#).

## Released by

Genesys Telecommunications Laboratories, Inc. [www.genesyslab.com](http://www.genesyslab.com)

**Document Version:** 76gvp\_ref\_07-2011\_v7.6.402.00



# Table of Contents

Preface	15
Intended Audience	15
Chapter Summaries	16
Document Conventions	18
Related Resources	20
Making Comments on This Document	21
Document Change History	21
Release 7.6.4	21
 Part 1	 <b>GVP GUIs and Tools</b>
 Chapter 1	 <b>Element Management Provisioning System</b>
EMPS GUI Overview	25
Navigation Tree	27
Information Panel	28
Main Frame	28
Top Menu	30
Resellers	32
Creating a Reseller	32
Modifying a Reseller	33
Deleting a Reseller	34
Customers	34
Creating a Customer	34
Provisioning a Customer	36
Modifying a Customer	45
Deleting a Customer	45
Deprovisioning Customers	46
Regenerating a Customer	46
IVR Profiles	47
Creating an IVR Profile	47
Provisioning an IVR Profile	49
Modifying an IVR Profile	67
Copying IVR Profile Attributes	67
Deprovisioning IVR Profiles	69

Deleting an IVR Profile .....	69
Regenerating an IVR Profile .....	70
Shortcuts.....	70
Servers .....	71
Editing Server Information .....	71
Copying Nodes .....	72
Deleting Nodes from a Server .....	72
Adding and Deleting Attributes .....	72
Adding a New Cache Server to the EMPS .....	73
Notifying a Server .....	74
Opening the NetMgt GUI .....	75
Importing the Server Instance CSV .....	75
Custom Data.....	76
Enabling the Custom Data Feature .....	76
Adding TTS Vendors.....	76
Adding ASR Vendors .....	77
Disabling the Custom Data Feature.....	77
Tasks .....	77
Creating a New Task.....	77
Modifying a Task .....	81
Removing a Task .....	81
Viewing Task Status.....	81
Server Groups .....	81
Creating Server Groups.....	82
Editing Server Groups .....	82
Removing Server Groups .....	82
Copying Server Groups .....	83
DID Groups.....	83
Creating DID Groups .....	83
Reports .....	84
RCA Reports.....	84
Servers Reports.....	85
DIDs Reports .....	85
Find.....	85
Users .....	85
Options .....	89
Diagnostics .....	90
Viewing Diagnostics.....	90
Recovery from OpenLDAP Data Corruption.....	91
 Chapter 2	
<b>Bulk Provisioning Tool .....</b>	<b>93</b>
Overview.....	93
Accessing the BPT .....	94

	Bulk Operations .....	95
	Swap IVR URLs .....	95
	Create New Applications .....	97
	Regenerate DID Groups .....	98
	Progress Bar and Log Window .....	99
	Canceling a Bulk Task .....	100
	Log and Audit Files .....	101
	BPT Configuration .....	102
	CSV Mapping .....	102
Chapter 3	<b>Bulk DID Operations Tool .....</b>	<b>109</b>
	Overview .....	109
	The BDOT .....	110
	BDOT Error Checking .....	112
Chapter 4	<b>Login Server .....</b>	<b>115</b>
	Login Server .....	115
	Passwords .....	115
	Accessing the Login Server .....	116
	Login Server Administration .....	117
	User Administration .....	119
	Service Administration .....	123
	Advanced Options .....	125
	Call Status Monitor .....	131
	Automatic Speech Recognition Log Server .....	133
	Reporter .....	133
	Reporter GUI .....	133
	Customizing the Interface .....	138
	Logo .....	138
	Fonts and Colors .....	138
Chapter 5	<b>Network Monitor .....</b>	<b>139</b>
	Overview .....	139
	Accessing the Network Monitor Interface .....	140
	Server Status Summary Report .....	140
	Category Codes .....	141
	Server Status Reasons .....	142
	Component Summary Report .....	143
	Servers Listing Report .....	143
	Server Details .....	144

## Chapter 6

<b>Element Management System.....</b>	<b>145</b>
Overview.....	146
Top Frame.....	146
Left Frame .....	146
Main Frame.....	147
Display Settings .....	147
System Information Menu.....	148
Processes .....	148
Page Collector .....	149
Scheduler.....	150
Management Information Base.....	152
Log.....	153
Bandwidth Manager.....	155
Bandwidth Manager Summary .....	155
Customer Summary .....	156
Customer Orders .....	158
Cisco Queue Adapter .....	159
Cisco Queue Adapter Call Summary .....	159
Connection Status .....	160
Cisco Queue Adapter Application Summary .....	161
Element Management Provisioning System .....	165
Events Collector .....	165
Events Collector Work-in-Progress.....	166
Event Collector Statistics .....	166
Event Collector Configuration Test Results .....	167
EventC Manager Activity History .....	168
Analyze a Call.....	169
EventC Manager Advanced Options .....	170
H.323 Session Manager .....	171
H.323 Session Manager Summary.....	171
H.323 Session Manager Active Calls .....	173
Configuration .....	175
IP Communication Server.....	176
IPCS Call Summary.....	176
Routes .....	178
Call Flow Assistant .....	179
IVR Server Client.....	181
IVR Server Client Call Summary .....	181
Connection Status .....	182
IVR Server Client Application Summary .....	183
MRP SMP Integrator .....	186
Agent Summary .....	187
OBN Manager.....	189

	OBN Manager Summary Page .....	189
	Policy Manager .....	191
	Policy Manager Summary .....	191
	Policy Manager Application Summary .....	192
	Resource Manager .....	196
	Resource Manager Summary .....	196
	Resource Manager Configuration .....	197
	Media Gateway Properties .....	198
	IPCS/PopGateway Properties .....	199
	SIP Session Manager .....	200
	SIP Session Manager Summary .....	200
	SIP Session Manager Active Calls .....	201
	SIP Session Manager Configuration .....	203
	Text-to-Speech .....	204
	TTS Requests Summary .....	204
	Active Requests .....	205
	Statistics .....	206
	Pending Requests .....	209
	Voice Communication Server .....	210
	Call Summary .....	210
	Call Volume .....	211
	PopGateway .....	212
	Call Flow Assistant .....	217
Chapter 7	<b>Portal .....</b>	<b>221</b>
	Overview .....	221
	Accessing the Portal Interface .....	222
Chapter 8	<b>CTI Simulator for GVP: DE .....</b>	<b>225</b>
	Introduction .....	225
	CTI Simulator User Interface .....	225
	Clear Window .....	226
	Define UserData .....	226
	Command Window .....	228
	Drop-down List of Actions .....	229
	Action Parameter Display .....	233
	Sample Call .....	234
	Setting Up the Sample Voice Application .....	234
	Sample Voice Application Code .....	235
	Placing a Sample Call with Pingtel .....	237

<b>Part 2</b>	<b>Features and Configurations .....</b>	<b>245</b>
<b>Chapter 9</b>	<b>Voice Communication Server.....</b>	<b>247</b>
	Configuring Outbound Dial Number Format .....	247
	Configuring Overlap Receive on ISDN .....	248
	Enabling Overlap Receive .....	248
	Setting the T.302 Timer for ISDN Protocols .....	249
	Configuring Enhanced CPA.....	249
	Qualification Parameters .....	250
<b>Chapter 10</b>	<b>IP Communication Server.....</b>	<b>253</b>
	Supported SIP Features .....	253
	Early Media.....	254
	Gateway Model Outbound Calls .....	254
	Gateway Model Inbound Calls .....	254
	Media Support .....	254
	HMP Support .....	254
	Convedia Support .....	256
	NativeRTP Support .....	257
	MRF Support .....	259
	Resource Manager .....	260
	Media Server Configuration.....	261
	G.729 Support .....	262
	Host Media Processing .....	262
	LConvedia.....	263
	Outbound Call Setup .....	264
	MRF .....	264
	Outbound Call Resolution .....	264
	SIP INFO .....	265
	SIP INFO Message Details .....	266
	VoiceXML Extension .....	266
	SIP Re-INVITE .....	267
	SDP Updates of IP Address and/or Port.....	267
	Call Hold Support.....	270
	Taking Call off Hold .....	272
	Re-INVITE Received When Bridging .....	273
	SDP Updates When DTMF or Audio Codec Changes .....	273
	Convedia.....	273
	MRP .....	273
	Adding New Media Streams .....	273
	Re-INVITE Requests Before a Final Response to Initial INVITE.....	273
	Propagation of SIP Header Values.....	274



	P-Asserted-Identity .....	274
	Call-ID .....	274
	Implementation Details .....	274
	Session Timers .....	274
	DTMF Rendering .....	276
	RTP Tone Detection .....	277
	Generating Tone Packets .....	277
	Detecting Tone Packets .....	277
Chapter 11	<b>H.323 Session Manager .....</b>	<b>279</b>
	Detecting DTMF .....	279
	Gatekeeper.....	280
	Codec .....	280
	Bridge and Transfer .....	281
	Numbering Type and Plan .....	282
	Fast Start and Tunneling .....	282
	Configuring Media Gateway .....	283
Chapter 12	<b>IVR Server Client .....</b>	<b>285</b>
	IVR Server Client Heartbeat .....	285
	Configuring GVP .....	285
	Success and Failure Scenarios .....	286
	Flow Control .....	288
	Universal Connection ID .....	289
Chapter 13	<b>Outbound Notification Manager .....</b>	<b>291</b>
	Overview.....	291
	OBN Manager Implementation Example .....	292
	OBN Manager Components and Workflow .....	292
	OBN Manager Components .....	292
	OBN Manager Interfaces.....	294
	Error Codes Returned by OBN Manager.....	298
	Provisioning Voice Applications.....	299
	Integrating with Outbound Contact Server .....	299
	User Data from OCS.....	302
	User Data to OCS .....	302
	Framework Port .....	302
	VoiceXML Application .....	303

Chapter 14	<b>MRCP Server Hunt List .....</b>	<b>307</b>
	Overview.....	307
	Out-of-Service Designation .....	307
	Heartbeat.....	308
	Load Balancing.....	308
	First Attempt .....	308
	Second Attempt .....	308
	Traps.....	310
Chapter 15	<b>Media Server Hunt List.....</b>	<b>311</b>
	Overview.....	311
	Out-of-Service Designation .....	311
	Heartbeat.....	311
	High Availability .....	312
	First Attempt .....	312
	Second Attempt .....	312
Chapter 16	<b>Network Announcement .....</b>	<b>315</b>
	Overview.....	315
	Requirements .....	315
	SIP Functions .....	316
	Overview .....	316
	Formal Syntax for Dialog Service .....	316
	Call Manager Requirements .....	317
	IPCS Requirements .....	317
	EMPS Requirements .....	317
Chapter 17	<b>Transactional Recording .....</b>	<b>319</b>
	Configuring the VCS.....	319
	Using a Dialogic JCT Board.....	319
	Using a Dialogic DMV-A/DMV-B Board .....	321
Chapter 18	<b>Multiple PopGateways and MCUs.....</b>	<b>323</b>
	Overview.....	323
	Configuring Multiple PopGateway Processes .....	324
	Configuring Multiple Mcu Processes for IPCS.....	326
	Symmetric RTP Ports .....	327

Chapter 19	<b>Proxy Support.....</b>	<b>329</b>
	Overview.....	329
	Configuring Page Collector.....	330
Chapter 20	<b>SIP Registration with Avaya SIP Server .....</b>	<b>333</b>
	Overview.....	333
	SIP Registration.....	334
	Configuring IPCS.....	337
	Requirements and Functionality .....	339
	Configuring Trusted Hosts on the Avaya Switch.....	339
Part 3	<b>GVP Transfers .....</b>	<b>341</b>
Chapter 21	<b>Transfers .....</b>	<b>343</b>
	VCS Transfers .....	343
	IPCS Transfers .....	346
	SIP REFER.....	347
	SIP REFER with Replaces .....	347
	Bridge Transfer .....	351
Chapter 22	<b>Explicit Call Transfer .....</b>	<b>353</b>
	Overview.....	353
	Directory Assistance for ECT .....	353
	Redirecting Number .....	354
	Presentation and Screening Indicators.....	354
	Configuring VCS .....	355
Chapter 23	<b>AT&amp;T Out-of-Band Transfer Connect .....</b>	<b>357</b>
	Overview.....	357
	Courtesy Transfer with Data .....	359
	Consult and Transfer with Data .....	359
	Conference and Transfer with Data .....	359
	User-to-User Data Forwarding Information Tags .....	359
	Provisioning Voice Applications.....	360
	Voice Applications .....	360
	Results Returned to Voice Application .....	361
	Example Voice Applications .....	362

Chapter 24	<b>Empty Capability Set-Based Semi-Blind Transfer.....</b>	<b>365</b>
	Overview.....	365
	Configuring H.323 Session Manager.....	366
	Requirements and Functionality .....	366
	Cisco Call Manager Requirements and Functionality .....	367
Chapter 25	<b>Empty Capability Set-Based Customized Consultation Transfer ..</b>	<b>369</b>
	Overview.....	369
	Configuring H.323 Session Manager.....	370
	Requirements and Functionality .....	371
	HSM Supported Codecs .....	371
Part 4	<b>Appendixes .....</b>	<b>373</b>
Appendix A	<b>Call Data Records.....</b>	<b>375</b>
	Events File.....	375
	Collector Database .....	377
	raw_events .....	377
	call_events.....	378
	call_exceptions .....	379
	eventc_manager .....	381
	eventc_stats.....	381
	load_balancer .....	382
	state_transitions.....	383
	Peaks Database .....	383
	etrackforpeak .....	383
	current peak.....	384
	eventc_stats.....	387
	peak_control .....	388
	Reporter Database .....	390
	callrecords .....	390
	hr_call_status.....	391
	ts_hr_call_status.....	392
	report_tables.....	393
	peaks tables.....	395
	download_request .....	399
	RepDWH Database .....	400
	call_phases .....	401
	billcallrecords .....	402
	Scenarios.....	403
	EventC and Reporter Data Cleanup.....	405

	Billing Data Files .....	406
	Resetting Peaks for EventC .....	406
	Resetting Peaks .....	406
	After Resetting Peaks .....	406
Appendix B	<b>Default Settings .....</b>	<b>409</b>
	Changing VCS/IPCS to Another EventC .....	409
Appendix C	<b>Call Control Adapter .....</b>	<b>411</b>
	Overview .....	411
	CFA to CCA Requests .....	411
	CCA to CFA Requests .....	412
	CCA Messages .....	412
	NEW_CALL_REQ .....	412
	UPDATE_CALL_STATUS_REQ .....	413
	INITIATE_TRANSFER_REQ .....	414
	PING_REQ .....	414
	Error Handling .....	415
	Summary of Message Flows .....	415
Appendix D	<b>Integration with Genesys Framework .....</b>	<b>417</b>
	Integration .....	417
	Configuring Objects .....	418
	Modifying the IVR Server .....	418
	With an IVR-Behind-the-Switch Configuration .....	419
	Ports .....	419
	With an IVR-In-Front-of-the-Switch Configuration .....	421
	Activating Routing .....	421
	Solution Control Interface .....	422
	Integration Features .....	426
	Call Flow Types .....	426
	Route Request .....	426
	Treatments .....	427
	Launching of Routing Strategy on URS .....	427
	Call Transfer .....	427
	Whisper .....	427
	Detecting Operator Hang Up .....	427
	Sending Caller-Entered Data .....	428
	Load Balancing Between IVR Servers .....	428
	Invoking IVR Application Based on User Data from the IVR Server .....	428

	Treating Missing DNIS .....	428
	Log Server Integration .....	428
	Feature Comparison .....	428
Appendix E	<b>Reporting GVP in Framework.....</b>	<b>431</b>
	Activating Reporting .....	431
	With an IVR-Behind-the-Switch Configuration .....	432
	With an IVR-In-Front-of-the-Switch Configuration .....	433
Appendix F	<b>System Prompts .....</b>	<b>435</b>
	Overview.....	435
	Creating ALaw System Prompts.....	435
	Installing ALaw System Prompts .....	436
Appendix G	<b>Scaling EventC .....</b>	<b>439</b>
	EventC Subsystem Components.....	439
	Deployment Considerations .....	440
	Deployment Scenarios.....	441
	Database Considerations .....	442
	Hardware Recommendations .....	442
	Database Sizing and Configuration .....	443
	Installing EventC on Multiple Boxes .....	444
Appendix H	<b>IP Call Manager High Availability.....</b>	<b>447</b>
	Call Manager—SIP.....	447
	Components .....	447
	Call Manager—H.323 .....	448
	Components .....	448
	Deployment Methods.....	449
	Single IPCM.....	449
	Dual IPCMs with Redundancy .....	450
	Recommended Deployment .....	452
	High Availability Using Microsoft Cluster Service .....	453
	Deployment Architecture .....	453
	Windows Clustering—Quorum Options .....	454
	Configuring IPCM .....	457
	Configuring MSCS for Use with IPCM .....	460
Index	.....	<b>465</b>



## Preface

Welcome to the *Genesys Voice Platform 7.6 Reference Manual*. This guide provides operating and provisioning instructions for the Genesys Voice Platform.

This document is valid only for the 7.6 release(s) of this product.

---

Note: For versions of this document created for other releases of this product, please visit the Genesys Technical Support website, or request the Documentation Library DVD, which you can order by e-mail from Genesys Order Management at [orderman@genesyslab.com](mailto:orderman@genesyslab.com).

---

This preface provides an overview of this document, identifies the primary audience, introduces document conventions, and lists related reference information:

- [Intended Audience, page 15](#)
- [Chapter Summaries, page 16](#)
- [Document Conventions, page 18](#)
- [Related Resources, page 20](#)
- [Making Comments on This Document, page 21](#)

0""Fqewo gpv'Ej cpi g'J kxqt{.'r ci g"43

Genesys Voice Platform is a robust, carrier-grade voice processing platform that unifies voice and web technologies. The solution includes management tools to operate a multi-customer, multi-application (IVR profile), multi-media network, and includes scalable components for call processing, speech processing, and system administration.

---

## Intended Audience

This document, primarily intended for system administrators, assumes that you have a basic understanding of:

- Computer-telephony integration (CTI) concepts, processes, terminology, and applications.
- Network design and operation.
- Your own network configurations.

You should also be familiar with Genesys Framework architecture and functions.

---

## Chapter Summaries

In addition to this opening chapter, this guide contains these chapters and appendixes:

- Chapter 1, “Element Management Provisioning System,” on [page 25](#), provides information about provisioning resellers, customers, and IVR profiles through the Element Management Provisioning System (EMPS).
- Chapter 2, “Bulk Provisioning Tool,” on [page 93](#), describes how to use the Bulk Provisioning Tool.
- Chapter 3, “Bulk DID Operations Tool,” on [page 109](#), describes how to use the Bulk DID Operations Tool.
- Chapter 4, “Login Server,” on [page 115](#), introduces the Login Server. It describes how to use the Login Server Administration module to create new services, assign user roles, and so on. It also describes the Web-based services that are accessed through the Login Server.
- Chapter 5, “Network Monitor,” on [page 139](#), introduces the Network Monitor, which provides single-point monitoring of servers that run GVP components and services.
- Chapter 6, “Element Management System,” on [page 145](#), introduces the Element Management System (EMS) graphical user interface (GUI) and provides an overview of EMS GUI functionality.
- Chapter 7, “Portal,” on [page 221](#), describes the GVP Portal, which is a website that provides links to all of the GVP web-based user interfaces that are available within a GVP installation.
- Chapter 8, “CTI Simulator for GVP: DE,” on [page 225](#), describes how to use the CTI Simulator that is provided with GVP: DE.
- Chapter 9, “Voice Communication Server,” on [page 247](#), provides additional configuration options for the Voice Communication Server.
- Chapter 10, “IP Communication Server,” on [page 253](#), provides additional configuration options for the IP Communication Server.
- Chapter 11, “H.323 Session Manager,” on [page 279](#), provides additional information about configuring H.323.
- Chapter 12, “IVR Server Client,” on [page 285](#), provides information about the IVR Server Client Heartbeat feature, the Flow Control message, and the Universal Connection ID.
- Chapter 13, “Outbound Notification Manager,” on [page 291](#), describes the Outbound Notification Manager, its components, and its workflow.
- Chapter 14, “MRCP Server Hunt List,” on [page 307](#), provides information about the MRCP Server Hunt List feature.



- Chapter 15, “Media Server Hunt List,” on [page 311](#), provides information about the Media Server Hunt List feature.
- Chapter 16, “Network Announcement,” on [page 315](#), describes how to configure the Network Announcement option with GVP.
- Chapter 17, “Transactional Recording,” on [page 319](#), describes how to configure the Transactional Recording option with the VCS.
- Chapter 18, “Multiple PopGateways and MCUs,” on [page 323](#), describes how to configure the IPCS to support multiple PopGateway and MCU processes.
- Chapter 19, “Proxy Support,” on [page 329](#), describes the HTTP Proxy feature, and how to configure Genesys Voice Platform (GVP) to support this feature.
- Chapter 20, “SIP Registration with Avaya SIP Server,” on [page 333](#), describes how to implement SIP Registration with the Avaya SIP Server.
- Chapter 21, “Transfers,” on [page 343](#), provides a list of the transfers that GVP supports.
- Chapter 22, “Explicit Call Transfer,” on [page 353](#), describes how to configure Explicit Call Transfer with the Voice Communication Server (VCS).
- Chapter 23, “AT&T Out-of-Band Transfer Connect,” on [page 357](#), provides information about the AT&T Out-of-Band Transfer Connect feature.
- Chapter 24, “Empty Capability Set-Based Semi-Blind Transfer,” on [page 365](#), describes how to configure the Blind Call Transfer using Empty Capability Set with GVP.
- Chapter 25, “Empty Capability Set-Based Customized Consultation Transfer,” on [page 369](#), describes how to configure the Custom Consultation Call Transfer using Empty Capability Set with GVP.
- Appendix A, “Call Data Records,” on [page 375](#), provides information about the call data records generated by the EventC and processing components. This appendix also provides recommendations on data cleanup.
- Appendix B, “Default Settings,” on [page 409](#), provides information about how to change the default settings.
- Appendix C, “Call Control Adapter,” on [page 411](#), provides information about the functions and messages of the Call Control Adapter.
- Appendix D, “Integration with Genesys Framework,” on [page 417](#), describes GVP integration with Genesys Framework.
- Appendix E, “Reporting GVP in Framework,” on [page 431](#), describes how to configure and use Genesys reporting functions.
- Appendix F, “System Prompts,” on [page 435](#), describes how to create and install ALaw system prompts.

- Appendix G, “Scaling EventC,” on [page 439](#), describes the components of the EventC subsystem, and how to scale EventC up to three boxes.
- Appendix H, “IP Call Manager High Availability,” on [page 447](#), describes high availability for IP Call Manager.

---

## Document Conventions

This document uses certain stylistic and typographical conventions—introduced here—that serve as shorthands for particular kinds of information.

### Document Version Number

A version number appears at the bottom of the inside front cover of this document. Version numbers change as new information is added to this document. Here is a sample version number:

fr\_ref\_02-2008\_v7.6.001.00

You will need this number when you are talking with Genesys Technical Support about this product.

### Type Styles

#### Italic

In this document, italic is used for emphasis, for documents’ titles, for definitions of (or first references to) unfamiliar terms, and for mathematical variables.

- Examples:**
- Please consult the *Genesys Migration Guide* for more information.
  - *A customary and usual practice* is one that is widely accepted and used within a particular industry or profession.
  - Do *not* use this value for this option.
  - The formula,  $x + 1 = 7$  where  $x$  stands for . . .

#### Monospace Font

A monospace font, which looks like teletype or typewriter text, is used for all programming identifiers and GUI elements.

This convention includes the *names* of directories, files, folders, configuration objects, paths, scripts, dialog boxes, options, fields, text and list boxes, operational modes, all buttons (including radio buttons), check boxes, commands, tabs, CTI events, and error messages; the values of options; logical arguments and command syntax; and code samples.

- Examples:**
- Select the Show variables on screen check box.

- Click the `Summation` button.
- In the `Properties` dialog box, enter the value for the host server in your environment.
- In the `Operand` text box, enter your formula.
- Click `OK` to exit the `Properties` dialog box.
- The following table presents the complete set of error messages T-Server® distributes in `EventError` events.
- If you select `true` for the `inbound-bsns-calls` option, all established inbound calls on a local agent are considered business calls.

Monospace is also used for any text that users must manually enter during a configuration or installation procedure, or on a command line:

**Example:** • Enter `exit` on the command line.

## Screen Captures Used in This Document

Screen captures from the product GUI (graphical user interface), as used in this document, may sometimes contain a minor spelling, capitalization, or grammatical error. The text accompanying and explaining the screen captures corrects such errors *except* when such a correction would prevent you from installing, configuring, or successfully using the product. For example, if the name of an option contains a usage error, the name would be presented exactly as it appears in the product GUI; the error would not be corrected in any accompanying text.

## Square Brackets

Square brackets indicate that a particular parameter or value is optional within a logical argument, a command, or some programming syntax. That is, the parameter's or value's presence is not required to resolve the argument, command, or block of code. The user decides whether to include this optional information. Here is a sample:

```
smcp_server -host [/flags]
```

## Angle Brackets

Angle brackets indicate a placeholder for a value that the user must specify. This might be a DN or port number specific to your enterprise. Here is a sample:

```
smcp_server -host <confighost>
```

---

## Related Resources

Consult these additional resources as necessary:

- *Genesys Voice Platform 7.6 Deployment Guide*, which provides detailed installation and configuration instructions for GVP and associated third-party software.
- *Genesys Voice Platform 7.6 Troubleshooting Guide*, which provides trap and basic troubleshooting information for GVP.
- *Genesys Voice Platform 7.6 VoiceXML 2.1 Reference Manual*, which provides information about developing Voice Extensible Markup Language (VoiceXML) 2.1 applications on GVP. It presents VoiceXML 2.1 concepts and provides examples that focus on the GVP implementation of VoiceXML.
- *Voice Extensible Markup Language (VoiceXML) Version 2.1, W3C Candidate Recommendation 13 June 2005*. The World Wide Web Consortium (W3C) publishes a technical report as a *Candidate Recommendation* to indicate that the document is believed to be stable, and to encourage its implementation by the developer community.
- *Genesys Voice Platform 7.6 Studio Deployment Guide*, which provides installation instructions for Genesys Studio.
- *Studio Help*, which provides online information about Genesys Studio, a GUI for the development of applications based on the VoiceXML.
- *Genesys Voice Platform 7.6 Voice Application Reporter Deployment and Reference Manual*, which provides installation instructions for the Voice Application Reporter. It also describes its interface and how to use it.
- *Genesys Voice Platform 7.6 Voice Application Reporter SDK Developer's Guide*, which provides examples on how to develop VoiceXML applications that interface with the Voice Application Reporter (VAR) database and generate application reports.
- *Genesys 7.6 Proactive Contact Solution Guide*, which consolidates information about the Genesys Proactive Contact solution. The Genesys Proactive Contact solution integrates Outbound Contact with GVP, and provides the ability to proactively initiate and handle outbound campaign calls using GVP.
- *Genesys Technical Support Troubleshooting Guide*, which includes information about the GVP log files.
- *Genesys Technical Publications Glossary*, which ships on the Genesys Documentation Library DVD and which provides a comprehensive list of the Genesys and CTI terminology and acronyms used in this document.

- *Genesys Migration Guide*, also on the Genesys Documentation Library DVD, which provides a documented migration strategy from Genesys product releases 5.1 and later to all Genesys 7.x releases. Contact Genesys Technical Support for additional information.
- The Release Notes and Product Advisories for this product, which are available on the Genesys Technical Support website at <http://genesyslab.com/support>.

Information on supported hardware and third-party software is available on the Genesys Technical Support website in the following documents:

- *Genesys Supported Operating Environment Reference Manual*
- *Genesys Supported Media Interfaces*
- *Genesys Hardware Sizing Guide*

Genesys product documentation is available on the:

- Genesys Technical Support website at <http://genesyslab.com/support>.
- Genesys Documentation Library DVD, which you can order by e-mail from Genesys Order Management at [orderman@genesyslab.com](mailto:orderman@genesyslab.com).

---

## Making Comments on This Document

If you especially like or dislike anything about this document, please feel free to e-mail your comments to [Techpubs.webadmin@genesyslab.com](mailto:Techpubs.webadmin@genesyslab.com).

You can comment on what you regard as specific errors or omissions, and on the accuracy, organization, subject matter, or completeness of this document. Please limit your comments to the information in this document only and to the way in which the information is presented. Speak to Genesys Technical Support if you have suggestions about the product itself.

When you send us comments, you grant Genesys a nonexclusive right to use or distribute your comments in any way it believes appropriate, without incurring any obligation to you.

---

## Document Change History

This section lists topics that are new or that have changed significantly since the first release of this document.

### Release 7.6.4

- *Appendix D, Integration with Genesys Framework*:
  - Table 122 on [page 429](#), has been changed to update the Behind the Switch feature for IVR Server when configured for Load Balancing.





Part

# 1

## GVP GUIs and Tools

Part One of this manual describes the GUIs and tools that are available with Genesys Voice Platform (GVP):

- Chapter 1, “Element Management Provisioning System,” on [page 25](#)
- Chapter 2, “Bulk Provisioning Tool,” on [page 93](#)
- Chapter 3, “Bulk DID Operations Tool,” on [page 109](#)
- Chapter 4, “Login Server,” on [page 115](#)
- Chapter 5, “Network Monitor,” on [page 139](#)
- Chapter 6, “Element Management System,” on [page 145](#)
- Chapter 7, “Portal,” on [page 221](#)
- Chapter 8, “CTI Simulator for GVP: DE,” on [page 225](#)







## Chapter

# 1

# Element Management Provisioning System

This chapter introduces the Element Management Provisioning System (EMPS) graphical user interface (GUI) and describes how to use it. This chapter has these sections:

- [EMPS GUI Overview, page 25](#)
- [Resellers, page 32](#)
- [Customers, page 34](#)
- [IVR Profiles, page 47](#)
- [Servers, page 71](#)
- [Custom Data, page 76](#)
- [Tasks, page 77](#)
- [Server Groups, page 81](#)
- [DID Groups, page 83](#)
- [Reports, page 84](#)
- [Users, page 85](#)
- [Options, page 89](#)
- [Diagnostics, page 90](#)
- [Recovery from OpenLDAP Data Corruption, page 91](#)

---

## EMPS GUI Overview

The EMPS uses a Lightweight Directory Access Protocol (LDAP) directory to store information. Before you can log in to the EMPS, you must have an account in the directory with sufficient permissions to make changes to the data. By default, you can use the `Admin` account, which has the required permissions.

To access the EMPS:

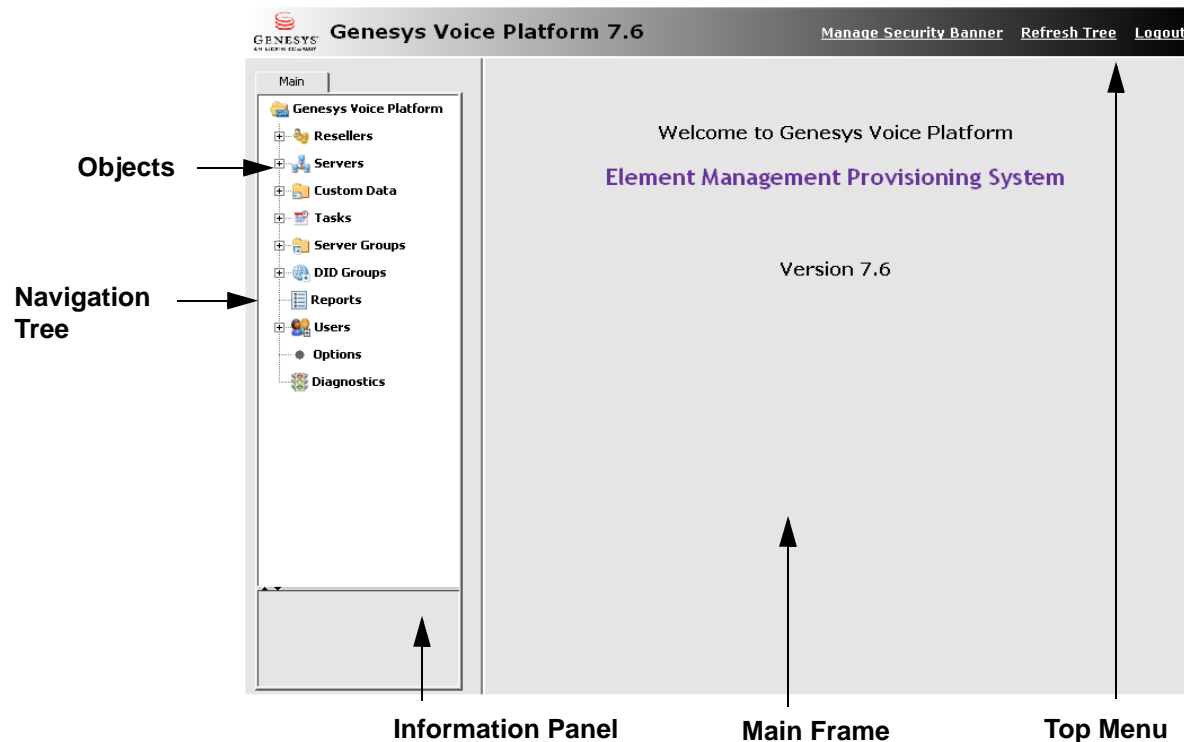
1. Open a web browser.
2. You have three different options for accessing the EMPS. You can use whichever option you prefer:
  - **Access through the Genesys Voice Platform (GVP) Portal**—Enter `http://<FQDN of EMPS Machine>:9810/gvpportal` in the address bar. The Portal GUI opens. Click the link under Provisioning, which opens the EMPS login page.
  - **Direct access**—If the EMPS is installed on the local computer, enter `http://localhost:9810/spm`. If the EMPS is installed on another computer, enter `http://<EMPS Computer>:9810/spm`. The EMPS login page opens.
  - **Access through the Element Management System (EMS) GUI**—Enter the URL `http://<EMPS Computer>:9810`. The EMS GUI opens. Click EMPS in the left pane. The login page for the EMPS opens. You can log in using the Admin account.

---

Note: If you access the EMPS GUI from the EMS GUI, and the EMPS and Directory server are located on different servers, a message similar to the following appears: URL does not work. EMPS might not be running on the Directory Server machine(s): <Directory Server machine name>.

---

3. On the EMPS login page, enter your user name and password. The EMPS uses LDAP user accounts. The default account is:
  - Username: Admin
  - Password: password
4. Click Login. The EMPS Welcome page opens (see Figure 1 on [page 27](#)).



**Figure 1: EMPS Welcome Page**

The EMPS GUI has a navigation tree, an information panel, a main frame, and a top menu.

## Navigation Tree

The navigation tree displays GVP objects in a hierarchy that reflects the relationships between these objects.

To expand an object in the navigation tree and view its children, click the plus (+) sign beside the object or double-click on the object. Note that an object with a plus sign might not always have child objects. To collapse the object and hide the children, click the minus (-) sign. By default, the navigation tree is collapsed. The circle character represents a leaf object (no children) and clicking it does not change the tree.

**Clicking an Object** Right-clicking an object opens a shortcut menu. Single-clicking certain objects displays a set of links in the main frame. Double-clicking an object opens the details of the object in edit mode.

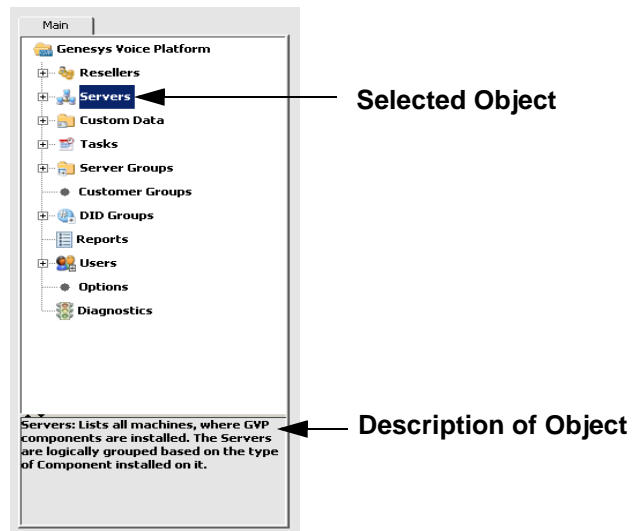
**Navigation Tree Appearance** The navigation tree appears differently, depending on your setup—that is, whether the single-tenancy option or the multi-tenancy option is enabled. In multi-tenancy, the navigation tree displays resellers, its customers, and the IVR profiles associated with those customers. In single-tenancy, the reseller is GVPowner, and the customer is Admin.

Each object will be discussed in detail in this manual:

- Resellers
- Customers (appear under the Resellers object)
- IVR Profiles (appear under the Resellers > Customers object)
- Servers
- Custom Data
- Tasks
- Server Groups
- DID Groups
- Reports
- Users
- Options
- Diagnostics

## Information Panel

When you select an object, the information panel displays a general description of it (for example, see [Figure 2](#)).



**Figure 2: Example Information Panel**

## Main Frame

The main frame displays the relevant EMPS page when you select (right-click, single-click, or double-click) an item from the navigation tree.

Figure 3 on [page 29](#) shows an example of the links that the main frame displays after single-clicking an object.

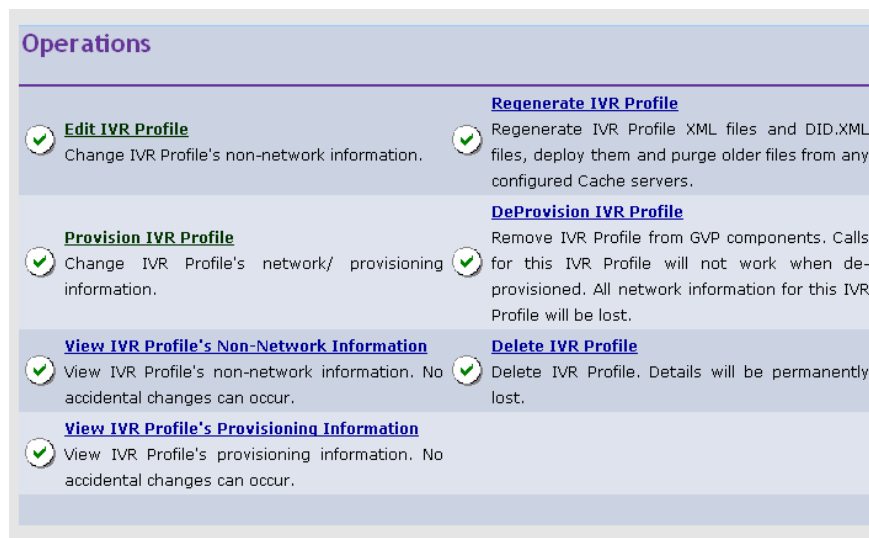


Figure 3: Example Main Frame Display of Links

Figure 4 shows an example property page displayed in the main frame.

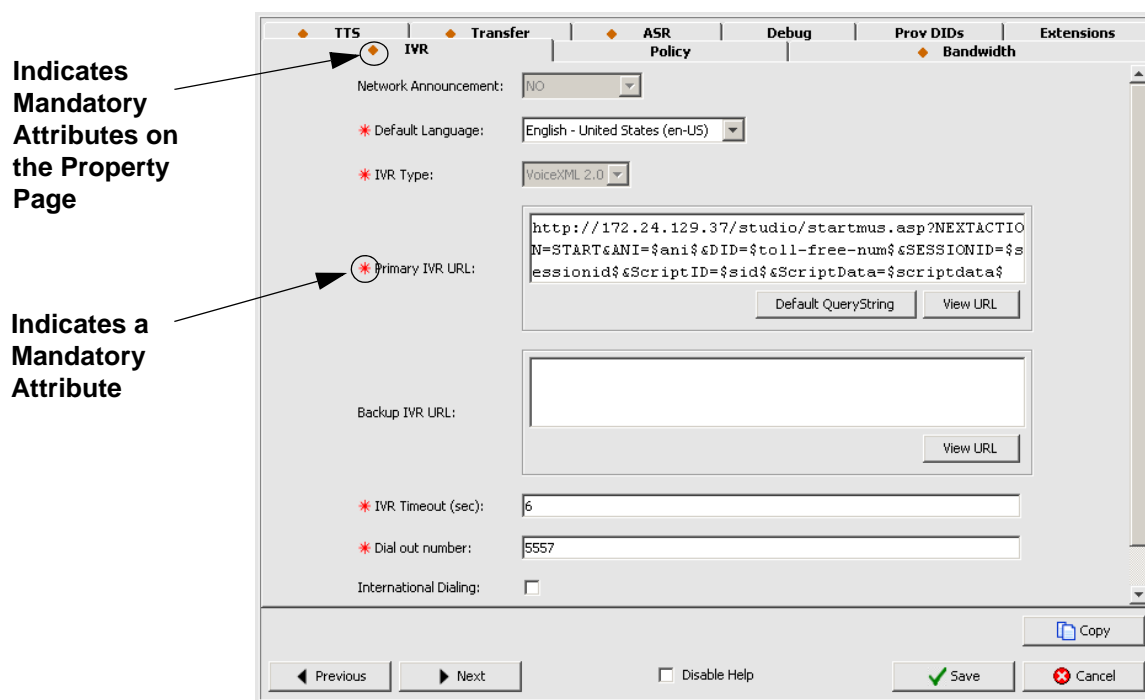


Figure 4: Example Property Page

## Mandatory Attributes

The tab header of each property page displays an orange diamond when there are mandatory attributes on the page. On the property page itself, a red star next to a field indicates that the field is required.

If a mandatory field is not completed, the EMPS will not allow you to navigate to the next page or click the Save button.

## Saving Changes

You can save changes in the EMPS by clicking Save on the property page.

The Next button saves changes temporarily. The changes are only saved permanently when you click Save.

The Previous and Next button navigate between tabs.

---

**Note:** The EMPS GUI registers navigation from the Previous, Next, Save, and Cancel buttons in the GUI. Do not use the browser's Back and Forward buttons.

---

## Help

To display or remove the context-sensitive Help, clear or select the Disable Help check box, which is located at the bottom of the property pages. When this check box is cleared, Help is enabled as a cookie on the client side, and is read each time the screens are re-opened. The lifetime of this cookie is seven days.

## View Mode

All objects, except the Servers object, have a View mode with which you can view settings for the object. You cannot change settings in this mode. Opening a page in View mode disables the Save button.

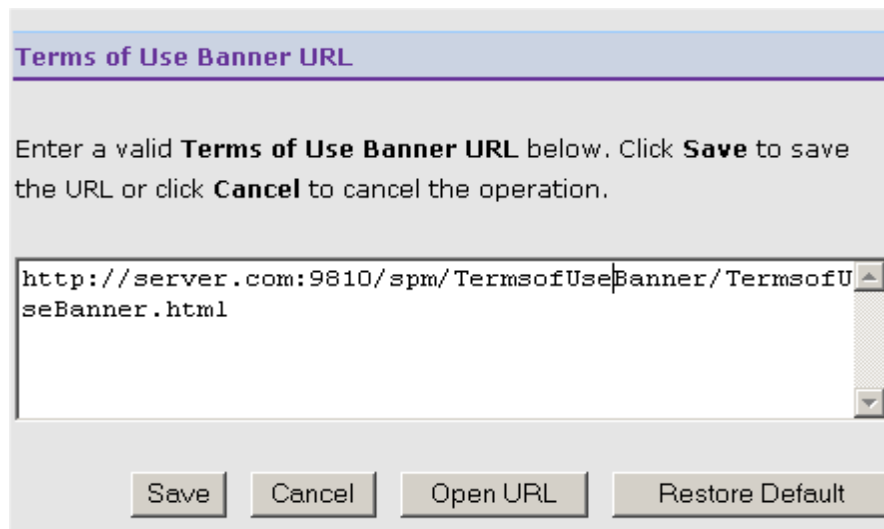
## View URL Button

The View URL button appears in many of the property pages in the EMPS GUI, typically next to a text input field. When clicked, the View URL button opens the URL that is currently in the text input box in a new browser window. If the URL is invalid, an error is displayed. If the URL is valid, the response that is received from the web server that processes the URL is displayed.

## Top Menu

The EMPS top menu provides links to perform the following actions:

- **Manage Terms of Use Banner**—Enables you to enter any security URL in order to display proprietary or informational pages. Click on this link to launch the Terms of Use Banner URL configuration window (see [Figure 5](#)).



The image shows a configuration window titled "Terms of Use Banner URL". It contains a text area with the URL "http://server.com:9810/spm/TermsofUseBanner/TermsofUseBanner.html". Below the text area are four buttons: "Save", "Cancel", "Open URL", and "Restore Default".

**Figure 5: Terms of Use Banner URL Configuration Window**

Enter a valid Terms of Use Banner URL, and click Save.

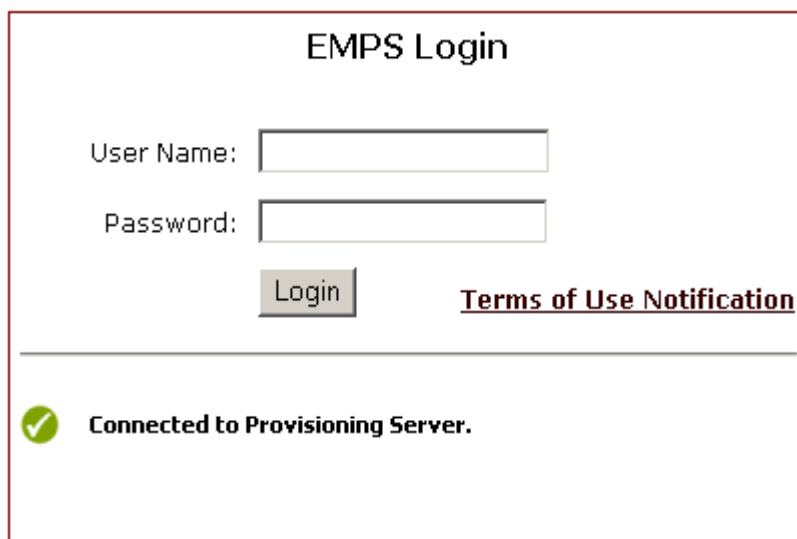
---

Note: EMPS does not validate the URL for accuracy.

---

- Click Open URL to open the Terms of Use Banner URL.
- Click Restore Default to revert back to the default Terms of Use Banner URL configuration.

You can also open the Terms of Use Banner URL by clicking Terms of Use Notification on the EMPS Login screen (see [Figure 6](#)).



The image shows the EMPS Login screen. It has a title "EMPS Login". Below the title are two input fields: "User Name:" and "Password:". Below the "Password:" field is a "Login" button. To the right of the "Login" button is a link labeled "Terms of Use Notification". Below a horizontal line, there is a green checkmark icon followed by the text "Connected to Provisioning Server."

**Figure 6: EMPS Login Screen with Terms of Use Notification Link.**

- **Refresh Tree**—Enables you to view the most recent data. Once you have added, modified, or deleted a reseller, customer, IVR profile, server, or group, you can refresh the information in the navigation tree in the left frame of the GUI by clicking **Refresh Tree**. In most cases, the tree is refreshed automatically.
- **Logout**—Enables you to log out of the EMPS. Automatic logout occurs after a period of inactivity (the system default is 20 minutes).

---

## Resellers

A *reseller* is an organization that acts as a channel to get customers to the Network Service Provider (NSP). Typically, the NSP is also the reseller, but it may have other resellers as well. *Customers* are accounts that are owned by the reseller, and *IVR profiles* are owned by the customer. This three-part hierarchy is implemented within the GVP components.

When the **Reseller** object is expanded, it displays a list of the provisioned and nonprovisioned customers for the reseller, and a list of provisioned and nonprovisioned IVR profiles for each customer.

In single-tenant mode, the default reseller is **GVPOwner**, and its default customer is **Admin**. An EMPS configured for single-tenant mode can only have one reseller, and the **Add New Reseller** shortcut menu is disabled. An EMPS configured for multi-tenant mode can have more than one reseller. In single-tenant mode, you can create IVR profiles under the default customer.

## Creating a Reseller

This section applies to multi-tenant mode only.

1. On the EMPS navigation tree, select the **Reseller** object, and then right-click it. Select **Add New Reseller**. The **Main** property page opens (see [Figure 7](#)).

The Reseller ID is a unique identifier for the reseller, and it is generated automatically.



The screenshot shows a web-based form titled "Main" for managing reseller properties. The form contains several input fields and checkboxes. The "Reseller ID" field is pre-filled with "822200691437". The "Start Date" field is pre-filled with "07/22/2006". The "GMT Offset" field is a dropdown menu set to "GMT-7 (Mountain Time)". The "Offset (mins.) for daylight saving" field is pre-filled with "60". The "Active" checkbox is checked. The "Reseller Is Parent NSP" checkbox is unchecked. The "Reseller Name" and "Reseller Display Name" fields are empty. The "Comments" field is a large text area. At the bottom, there are "Previous" and "Next" buttons, a "Disable Help" checkbox, and "Save" and "Cancel" buttons.

**Figure 7: Reseller Main Property Page**

2. Enter the name of the reseller in the Reseller Name field.

---

**Note:** The Reseller Display Name field defaults to the name you entered in the Reseller Name field. If required, you can change this name, which appears throughout the reseller's IVR profiles. However, once you save the Reseller Name, you cannot modify it. You can only modify the Reseller Display Name.

---

3. Enter the date, in MM/DD/YYYY format, in the Start Date field.
4. The Reseller Is Parent NSP check box determines whether the reseller is the parent NSP. If some other reseller is already the parent NSP, this check box is disabled, and the parent NSP reseller name is displayed beside the check box.
5. To provision the reseller immediately, select the Active check box. If you do not do this, GVP does not recognize the reseller as provisioned, even though the reseller information is stored in the EMPS.
6. Select the reseller's time zone from the GMT Offset drop-down list.
7. Enter a value in minutes for the offset (mins.) for daylight saving the field. For example, -20 or +20.
8. Enter any additional comments in the Comments field.
9. Click Save.

## Modifying a Reseller

1. On the EMPS navigation tree, expand the Reseller object.

2. Select the reseller that you want to modify, and then do one of the following:
  - Right-click it and select `Edit` from the shortcut menu.
  - Single-click it and click `Edit Reseller Information` from the main frame.
  - Double-click it.

The `Main Reseller` dialog box opens.

3. Make the required changes, and then click `Save`. This modifies the reseller and if your changes affect database entries, those are updated.

## Deleting a Reseller

This section applies to multi-tenant mode only.

1. On the EMPS navigation tree, expand the `Reseller` object.
2. Select the reseller that you want to delete, and then do one of the following:
  - Right-click it and select `Delete` from the shortcut menu.
  - Single-click it and click `Delete Reseller` from the main frame.
3. Click `Yes` when prompted `Deleting this reseller will delete all the children under this reseller. Do you want to continue?` This deletes the reseller.

---

**Note:** You cannot delete a reseller that has customers. Deleting a reseller removes all of the information associated with the reseller from the Directory server.

---

---

## Customers

This section provides information about customers. Once you have provisioned a reseller, you can create and provision its customers.

In single-tenant mode, the default customer is `Admin`. You can create IVR profiles only under this default customer.

## Creating a Customer

This section applies to multi-tenant mode only.

1. On the EMPS navigation tree, expand the `Reseller` object.
2. Select the reseller to which the customer will belong, and then you can either:
  - Right-click it and select `Add New Customer` from the shortcut menu.
  - Single-click it and click `Create New Customer` from the main frame.

The Create New Customer property page opens in the main frame (see Figure 8 on [page 35](#)).

EMPS automatically generates the Customer ID, which uniquely identifies the customer.

The screenshot shows a software window titled "Main" and "Contact". The "Main" tab is selected. The form contains the following fields and controls:

- Customer ID:** A text field containing the value "914065158".
- Customer Name:** An empty text field.
- Customer Display Name:** An empty text field.
- Active:** A checkbox that is checked.
- NSP Customer:** A text field containing the value "Another Reseller [GVPOwner] is parent NSP".
- Comments:** A large empty text area.

At the bottom of the window, there is a horizontal bar with several buttons: "Previous", "Next", "Disable Help", "Save", and "Cancel".

**Figure 8: Customer Information Property Page**

3. Enter the name of the customer in the Customer Name field. For reporting purposes, the customer name must be unique across all resellers, not just the parent reseller.

---

**Note:** The Customer Display Name field defaults to the name you entered in the Customer Name field. If required, you can change this name, which appears throughout the customer's IVR profiles. However, once you save the customer information, you cannot modify the Customer Name. You can only modify the Customer Display Name.

---

4. Select the Active check box to activate the customer. If you do not do this, the information is not currently active. However, EMPS preserves the information about the customer for later reinstatement or persistence of the call event.
5. Enter any additional information or comments in the Comments field.

6. Click **Next**, which opens the **Contact Information** page. The fields on this page are optional.
7. Enter a customer contact name in the **Contact** field.
8. Enter the billing address and information in the remaining fields.
9. Click **Save** to save the information. The EMPS adds the new customer to the database and the navigation tree is automatically refreshed to display the new customer.

---

**Note:** If the newly added entry does not appear in the navigation tree, click **Refresh Tree** on the top menu, which refreshes the entire tree and shows the newly added node.

---

## Provisioning a Customer

1. On the EMPS navigation tree, expand the **Reseller** object, and then expand the reseller to which the customer belongs.
2. Do one of the following:
  - Right-click the customer that you want to provision. From the shortcut menu, select **Provision**.
  - Single-click the customer that you want to provision. From the main frame, click **Provision Customer**.

The customer provisioning property pages open, starting with the **Policy** property page (see [Figure 9](#)).

Policy | GenesysCTI | Reporting | CiscoCTI

\* Level 1 Ports: 1000

\* Rule1: DayOfWeek=,StartTime=,EndTime=,RuleCallType Edit

\* Level 2 Ports: 1000

\* Level 3 Ports: 1001

\* Billable Ports: 1000

\* Primary PM Machine: qa3-h5.qa.telera.com

\* Primary PM URL: http://qa3-h5.qa.telera.com:9810/webnotify.asp?notifyprocess=\$reseller-name\$\_\$customer-name\$ PMDashboardURL=\$dashboardurl\$&Dashboard\_Trace=\$DB\_TRACE\$ View URL

Secondary PM Machine: qa1-h6.qa.telera.com

Secondary PM URL: http://qa1-h6.qa.telera.com:9810/webnotify.asp?notifyprocess=\$reseller-name\$\_\$customer-name\$ PMDashboardURL=\$dashboardurl\$&Dashboard\_Trace=\$DB\_TRACE\$ View URL

Previous Next Disable Help Save Cancel

**Figure 9: Customer Provision—Policy Property Page**

The customer provisioning property pages are made up of each GVP component that you must provision.

You must complete four steps to provision a customer. Once you have completed the Policy property page, click Next to open the next property page. When you have completed that page, click Next to open the next property page in the sequence, and so on. Continue this process until you have provisioned all of the components.

---

**Note:** When provisioning a customer for the first time, you must navigate through each provisioning property page.

If the GVP component was not installed, the property page will not be displayed. You must have installed the component in order for these property pages to display.

---

## Step 1—Policy

This property page provisions the Policy Manager.

1. Enter the number of ports assigned to the customer in the **Level 1 Ports** field. The Level 1 Ports are the initial ports that a customer purchases for which they will be billed at normal rates.

---

Note: Rule 1 appears by default. Under normal circumstances do not modify this rule.

---

2. Enter the number of ports assigned to the customer in the **Level 2 Ports** field. Level 2 Ports are used when all of the Level 1 Ports are exhausted. For these ports, the customer will be billed at a different rate.

Level 2 Ports = Level 1 Ports + Level 2 bursting

For example, if the customer has 1000 ports at Level 1 and they want 100 more ports in the next level, set Level 2 ports at 1100. Therefore, if the customer IVR profile receives 1100 simultaneous calls, 1000 ports are billed at normal rates, and 100 ports are billed at the Level 2 rate.

3. Enter the number of ports assigned to the customer in the **Level 3 Ports** field. The Level 3 Ports are the next level of bursting to be billed at a higher rate than Level 2.

For example, if the customer wants 100 ports in Level 3, then set the **Level 3 Ports** field to 1200 (1000 + 100 + 100).

4. Enter the number of billable ports assigned to the customer in the **Billable Ports** field. Billable ports are used by some customers where the number of ports to be billed is different from the number of ports provisioned (Port Levels 1, 2, and 3). This information is transferred to EventC and stored as part of the CDR records.

---

Note: The **Billable Ports** field is available only if EventC is installed.

---

5. Select a PM machine from the **Primary PM Machine** drop-down list. If the list is empty, then no PM machines have been installed.

The primary URL PM machine appears by default.

To launch the URL, click **View URL**.

6. Select a secondary PM machine (if there is one) from the **Secondary PM Machine** drop-down list.

The secondary URL PM machine appears by default.

To launch the URL, click **View URL**.

- Click Next. If configuring in Single Tenancy mode, the following GenesysCTI property page appears (see Figure 10). If configuring in Multi Tenancy mode, see Figure 11 on page 42 and the steps that follow to configure the GenesysCTI tab for Multi Tenancy. This property page provisions the IVR Server Client.

## Step 2—GenesysCTI

**GenesysCTI**

IVR Svr Client Active: ☒

Local ISvr Client for IPCS/VCS: ☐

**IVR Svr Clients and IServers selection**

**IVR Server Clients List**

- dev-luna.us.int.genesyslab.com
- dev-tuna.us.int.genesyslab.com
- naveenka.us.int.genesyslab.com

**IVR Servers List**

- IServer\_Sample
- IServer\_Sample1
- IServer\_Sample2
- IServer\_Sample3

Update

IVR Server Clients List	IVR Servers List	IVR Server Client URL
dev-luna.us.int.genesyslab.com	IServer_Sample,IServer_Sample1,...	http://dev-luna.us.int.genesyslab...
naveenka.us.int.genesyslab.com	IServer_Sample2,IServer_Sample3	http://naveenka.us.int.genesysla...

\* IVR Server Mode: Network

Called Number: UseTFN

Fetch Script ID from URS: ☐

Script ID Key Name:

Script ID Fetch Timeout:

Previous Next ☒ Disable Help Save Cancel

**Figure 10: Customer Provision—GenesysCTI Property Page for Single Tenant**

- Select the IVR Server Client Active check box to assign an Active status to the IVR Server Client.

**Note:** You cannot configure the other fields on this page unless the IVR Server Client is active.

2. Select `Local ISrv Client` for IPCS/VCS to allow each IPCS/VCS to connect to its own IVR Server Client. For each IPCS and VCS, make sure that the `I-Server Client URL` parameter under the `CFA` node is set to `http://localhost/WebNotify.asp?NotifyProcess=GVPOwner_Admin_GQA`.
3. In the `IVR Server Clients List` listbox, select an IVR Server Client that you wish to configure as the Primary.
4. In the `IVR Servers List` listbox, select one or multiple IVR Servers that you wish to associate with the selected IVR Server Client.
5. Click `Update`. The selected IVR Server Client and IVR Servers pair will be added to the list as the first entry.

Continue with the following steps to configure the Secondary IVR Server Client for the default customer:

6. In the `IVR Server Clients List` listbox, select an IVR Server Client that you wish to configure as the Secondary.
7. In the `IVR Servers List` listbox, select one or multiple IVR Servers that you wish to associate with the selected IVR Server Client.
8. Click `Update`. The selected IVR Server Client / IVR Servers pair will be added to the list as the second entry.

---

Note: If configured in In-Front or Network mode, the first entry in the list will be used as the Primary IVR Server Client, and the second entry in the list will be used as the Backup IVR Server Client. These entries are ignored if configured in Behind-the-switch mode. Any other subsequent entries are also ignored.

---

9. Select the IVR Server mode from the drop-down list. The modes available are:
  - **Network**—You can use toll-free number (TFN) or DNIS in Network mode. By default, the IVR Server Client uses TFN as the RouteDN. Any RouteDN value specified in the `QUEUE_CALL` tag is ignored. The `CalledNum` field of the `NewCall` message contains the TFN. The IVR Server uses the TFN as the RouteDN.  
In this mode, ports are not defined in Configuration Manager, and therefore, there is no real-time reporting in CCPulse on specific port usage.
  - **In-front**—The IVR Server Client sends the port number on which it received the call to the IVR Server. You must configure the IVR ports as type `Extension` in the Configuration Manager. Configure the ports on the Configuration Manager as specified below.

---

Note: GVP supports CTI transfer in the in-front mode.

---



In this mode, the Call Flow Assistant (CFA) process on each Voice Communication Server (VCS)/IP Communication Server (IPCS) server generates a unique Host ID from the server's IP Address. If the IP address of the server is 12.23.231.99, the HostID will be in the form 012023231099. The IVR Server Client process then appends the port number to the HostID to form a unique IVR port ID (012023231099n where *n* is the port number on which the call arrived on that particular VCS/IPCS server). So if a VCS/IPCS has, for example, 23 ports, on the Configuration Manager you need to configure ports 0120232310991, 0120232310992...01202323109923 as type Extension.

Also in this mode, the IVR Server Client sends the RouteRequest message with the value for RoutedDN set to the value passed in the QUEUE\_CALL tag.

- **Behind-the-Switch**—The IVR Server Client sends the port number on which it received the call to the IVR Server. In this mode, the port numbers are not pre-pended with the IP address of the GVP server, as they are in the In-front mode. In this mode, the DNIS for the call is fetched through the IVR Server. The GVP IVR ports must be configured in Configuration Manager.

---

Note: Behind-the-Switch mode is available for GVP Windows only.

---

**10.** Select the Called Number value from the drop-down list. The values available are:

- **UseTFN**—If you select this value, the CalledNum field of the NewCall message contains the TFN.
- **UseDNIS**—If you select this value, the CalledNum field of the NewCall message contains the DNIS.

---

Note: The Called Number field is disabled if you selected Behind-the-Switch for the IVR Server mode.

---

**Figure 11: Customer Provision—GenesysCTI Property Page for Single Tenant**

1. Select the IVR Server Client Active check box to assign an Active status to the IVR Server Client.

---

Note: You cannot configure the other fields on this page unless the IVR Server Client is active.

---

2. Select the Primary IVR Server Client machine from the drop-down list. If the list is empty, no IVR Server Client machines have been installed. The Primary IVR Server Client URL appears by default.  
To launch the URL, click View URL.
3. Select the Secondary IVR Server Client machine (if there is one) from the drop-down list. The Secondary IVR Server Client URL appears by default.  
To launch the URL, click View URL.
4. Add or remove the desired IVR Servers from the Customer IServers list.

---

Note: The IVR Servers must have been previously added in order for the IVR Servers to appear in this list. If no IVR Servers are listed, refer to the *Genesys Voice Platform 7.6 Deployment Guide* for instructions on how to add the IVR Servers.

---

5. Go to [Steps 9](#) and [10](#) of configuring the GenesysCTI tab for Single Tenancy mode.
6. Select the Fetch Script ID from URS check box if you want GVP to fetch the script ID from the Universal Routing Server (URS). This field is enabled for Behind-the-Switch mode only.

When you select this check box, the Script ID Key Name and Script ID Fetch Timeout fields automatically populate with default values.

Script ID Key Name—Specifies the key name that is configured in Framework, and that will be used in the UdataGet message by the IVR Server Client. The default Script ID key name is `scriptname`.

Script ID Fetch Timeout—Specifies, in milliseconds, how long GVP waits for a response on the `scriptname` fetch file from the IVR Server before it times out. The minimum value is 500 msec, the maximum value is 5000 msec, and the default value is 5000 msec.

7. Click Next, which opens the Reporting property page (see [Figure 12](#)). This property page provisions the Reporter.

### Step 3—Reporting

The screenshot shows the 'Reporting' tab of a configuration window. The 'GMT Offset' is set to 'GMT-11 (Samoa)'. The 'Access through VPN only' checkbox is unchecked. The 'Offset (mins.) for daylight saving' is set to '60'. Navigation buttons 'Previous' and 'Next' are visible, along with 'Disable Help', 'Save', and 'Cancel'.

**Figure 12: Customer Provision—Reporter Property Page**

1. Select the customer's time zone from the GMT Offset drop-down list.
2. To restrict the customer so that it can access the service through the virtual private network (VPN) only, select the Access Through VPN Only check box.

3. Enter a value in minutes for the `Offset (mins.) daylight saving` field. For example, `-20` or `+20`. The default value is `+60`.
4. Click **Next**, which opens the `CiscoCTI` property page (see [Figure 13](#)). This property page provisions the Cisco Queue Adapter.

## Step 4—CiscoCTI

The screenshot shows the 'CiscoCTI' tab selected in a multi-tabbed interface. The 'CQA Active' checkbox is checked. Below it, there are two sections for 'Primary CQA machine' and 'Secondary CQA machine', each with a dropdown menu and a corresponding 'View URL' button. Further down are text input fields for 'CQA Port Number', 'Primary PG Addresses', 'Backup PG Addresses', 'TFN mapping Call Variable', and 'CQA ECC Variable Names'. The bottom of the window features navigation buttons: 'Previous', 'Next', 'Disable Help' (with a checkbox), 'Save' (with a green checkmark), and 'Cancel' (with a red X).

**Figure 13: Customer Provision—CiscoCTI Property Page**

The Cisco Queue Adapter (CQA) is an optional feature. If you are not using the CQA, you can click **Save**, which provisions the customer and updates the database.

1. Select the `CQA Active` check box to assign an `Active` status to the CQA.

---

**Note:** You cannot configure the other fields on this page unless the CQA is active.

---

2. Select the Primary CQA machine from the drop-down list. If the list is empty, then no CQA machines have been installed. The Primary CQA URL appears by default. To launch the URL, click **View URL**.

3. Select the Secondary CQA machine (if there is one) from the drop-down list. The Secondary CQA URL appears by default. To launch the URL, click **View URL**.
4. Enter the CQA port number in the **CQA Port Number** field. The CQA port value is the TCP port number in the CQA machine to which Cisco VRUPG makes the TCP/IP connection.
5. Enter an IP address in the **Primary PG (Peripheral Gateway) Addresses** field. This field refers to PGs used with the primary queue adapter, and can have up to two PG IP addresses, separated by a comma.
6. Enter an IP address in the **Backup PG (Peripheral Gateway) Addresses** field. This field refers to PGs used with the backup queue adapter, and can have up to two PG IP addresses, separated by a comma.
7. Enter a call variable number in the **TFN (Toll-Free Number) Mapping Call Variable** field. This call variable maps to the toll-free number that the customer has called. Valid values are 0–10. A value of 0 disables this field. These ten (1-10) variables can be passed in the call variable.
8. Enter variable names in the **CQA ECC (Expanded Call Context) Variable Names** field.

---

**Note:** In addition to the basic call variables, you can use the ECC variables to pass data to the Cisco ICM. You must obtain the names of these variables from the Cisco ICM script developer.

---

9. Click **Save**, which provisions the customer and updates the database.

## Modifying a Customer

1. On the EMPS navigation tree, expand the **Reseller** object, and then expand the reseller to which the customer belongs.
2. Select the customer that you want to modify, and then do one of the following:
  - Right-click it and select **Edit** from the shortcut menu.
  - Single-click it and click **Edit Customer** from the main frame.
  - Double-click it.
3. Make any necessary changes to the customer property pages.
4. When you are finished, click **Save** to save any changes and updates to the database.

## Deleting a Customer

1. On the EMPS navigation tree, expand the **Reseller** object, and then expand the reseller to which the customer belongs.

2. Select the customer that you want to delete, and then do one of the following:
  - Right-click it and select **Delete** from the shortcut menu.
  - Single-click it and click **Delete Customer** from the main frame.
3. Click **Yes** when prompted **Deleting this customer will delete all the children under this customer. Do you want to continue?** This deletes the customer from the system, and it also deletes the customer record from the Directory server.

If this customer has any IVR profiles or if this customer is provisioned, the EMPS will not delete the customer.

## Deprovisioning Customers

Before deprovisioning a customer, you must first deprovision all IVR profiles from the customer, and then delete all IVR profiles from the customer.

To deprovision a customer:

1. On the EMPS navigation tree, expand the **Reseller** object, and then expand the reseller to which the customer belongs.
2. Do one of the following:
  - Right-click the customer that you want to deprovision. From the shortcut menu, select **Deprovision**.
  - Single-click the customer that you want to deprovision. From the main frame, click **Deprovision Customer**.

This removes the customer from the EMS components. Calls for a deprovisioned customer are not completed, and the deprovisioned customer loses all network information.

---

**Note:** During deprovisioning, if there are ports allocated to the IVR Profile, a message is sent to Policy Manager stating this and requesting that these ports be deleted.

---

## Regenerating a Customer

1. On the EMPS navigation tree, expand the **Reseller** object, and then the reseller.
2. Select the customer that you want to regenerate, and then do one of the following:
  - From the main frame, click **Regenerate Customer**.
  - Right-click the customer, and from the shortcut menu, select **Regenerate**.

A message box appears with the text: Regenerate this customer [Customer]?

3. Click Yes. EMPS regenerates and redeploys the IVR Profiles and the DID XML files.

---

Note: Customer provisioning does not regenerate IVR profiles. You must regenerate IVR Profiles separately. For more information, see “Regenerating an IVR Profile” on [page 70](#).

---

---

## IVR Profiles

For multi-tenancy, you can create and provision IVR profiles after you have created and provisioned the reseller and customers.

For single-tenancy, resellers and customers do not apply.

### Creating an IVR Profile

1. On the EMPS navigation tree, expand the Reseller object, and then expand the reseller to which the customer belongs.
2. Select the customer to which you want to add an IVR profile, and then do one of the following:
  - Right-click it. From the shortcut menu, select Add New IVR Profile.
  - Single-click it. From the main frame, click Create New IVR Profile.

The Create New IVR Profile property page opens (see Figure 14 on [page 48](#)).

The Application ID is automatically generated and uniquely identifies the IVR profile.

**Main**

\* Application ID: 329112810

\* Application Name:

\* Application Display Name:

\* Application Type: Inbound

Network Announcement: ☐

\* Toll Free Number:

\* Start of Service Date: 03/29/2007

\* Application Creation Date: 03/29/2007

\* Reporting description: Testing

Application active in network: ☒

Description:

Responsible Organization: - No Selection -

Previous Responsible Organization: - No Selection -

Previous Next Disable Help Save Cancel

**Figure 14: IVR Profile Main Page**

3. Enter the name of the IVR profile in the `Application Name` field.  
The `Application Display Name` field defaults to the name you enter in the `Application Name` field. If required, you can change this name, which appears throughout the IVR Profile.
4. Select the application type from the drop-down list. The choices are:
  - Inbound
  - Outbound
5. To designate this IVR Profile as a Network Announcement IVR profile, select the `Network Announcement` check box.
6. Enter a number in the `Toll Free Number` field. Inbound IVR profiles require this number, and it is usually the toll free number used to access the IVR Profile. This number is optional for Outbound IVR profiles.
7. Enter the service start date in the `Start of Service` field. The date must be in the format `mm/dd/yyyy`. Do not use any spaces in front of or after the date format.
8. Enter the date on which you created the IVR profile in the `Application Creation Date` field. The date must be in the format `mm/dd/yyyy`. Do not use any spaces in front of or after the date format.



---

**Note:** The next two fields, `Reporting Description` and `Application Active in Network` are strictly for reporting purposes only. They do not control the application's actual behavior and they do not get modified automatically based on the application's real status. You update these fields so that you can view the corresponding status in EMPS reports.

---

9. Select the reporting status from the `Reporting Description` drop-down list.
10. To activate the IVR profile, select the `Application Active in Network` check box. If you do not do this, the IVR profile is not active. However, the information about the IVR profile is stored for later use.
11. Enter any notes or comments in the `Description` field.
12. Select the organization responsible for this IVR profile from the `Responsible Organization` drop-down list.
13. Select the organization that was previously responsible for this IVR profile from the `Previous Responsible Organization` drop-down list.
14. Enter any notes or comments in the `Comments` field.
15. Click **Save**. This creates the new IVR profile. The navigation tree is automatically refreshed and displays the new IVR profile.

## Provisioning an IVR Profile

1. On the EMPS navigation tree, expand the `Reseller` object, the reseller, and then the customer.
2. Select the IVR profile that you want to provision, and then do one of the following:
  - Right-click it. From the shortcut menu, select `Provision`.
  - Single-click it. From the main frame, click `Provision IVR Profile`.

The IVR profile provisioning property pages open, starting with the IVR property page (see Figure 15 on [page 50](#)).

**Figure 15: Provision IVR Profile—IVR Property Page**

The amount of steps it takes to provision an IVR profile will vary slightly, depending on which GVP components were installed. If a GVP component was not installed, its property page will not be displayed. At the most, there would be 11 steps to provision an IVR profile.

Once you have completed the IVR property page, click Next to open the next component page. When that page is complete, click Next to open the next component page in the sequence, and so on. Continue this process until you have provisioned all of the components.

---

**Note:** When provisioning an IVR profile for the first time, you must navigate through every page.

---

## Step 1—Provision IVR

1. The **Network Announcement** field, which is read-only, displays whether (YES or NO) this is a Network Announcement IVR profile. This option was selected when you first created this IVR profile (see “Creating an IVR Profile” on [page 47](#)).
2. Select the default language from the drop-down list. If you are selecting a default language other than U.S. English, you must install the desired language pack before provisioning the IVR profile.

3. Enter the Primary IVR URL. You can click `Default Querystring` to obtain the full query string. To launch the URL, click `View URL`.

---

Note: The `Default Querystring` is required. Make sure that the IVR URL starts with `http://` and that the URL contains the fully qualified path to the first page of the IVR profile.

If this is a Network Announcement IVR profile, you cannot enter a Primary IVR URL.

---

4. Enter the Backup IVR URL. You can click `Default Querystring` to obtain the full query string. To launch the URL, click `View URL`.

---

Note: Make sure that the IVR URL starts with `http://` and that the URL contains the fully qualified path to the first page of the IVR profile.

If this is a Network Announcement IVR profile, you can enter a Backup IVR URL along with a query string.

---

5. Enter the number of seconds allowed in the `IVR Timeout (sec)` field. This value is the amount of time that the VCS/IPCS waits for a response from the primary web IVR profile server before trying to contact the backup web IVR profile server.

6. Enter the phone number to be dialed in the `Dial out number` field. The dial out number is the number called if an error occurs with the IVR profile.

The Dial Out Number that you set for the IVR profile must *not* be equal to the DID that is configured for that IVR profile. You must configure a separate DID for the Dial Out Number. This restriction is applicable when Call Manager is deployed.

If a call comes in to GVP and the `DID.xml` fails, the error number configured in the application provisioning is used to dial out.

If the `DID.xml` is fetched successfully, and errors occur during the transition to IVR application pages, an attempt is made to fetch the `<num>.xml` (the `DID.xml` used in case of failures) configured in the Call Flow Assistant (CFA) in IP Communication Server (IPCS)/Voice Communication Server (VCS). If, after multiple attempts, GVP fails to fetch that URL, the error number configured in the application provisioning is used to dial out..

7. For international dialing, the value depends on the carrier that is providing the trunk. Check with your carrier for the network value.

---

Note: This field is only required for the VCS.

---

8. Enter the number of seconds allowed in the `CPA (Call Progress Analysis) Timeout` field.

- Click **Next**, which opens the **Policy** property page (see Figure 16 on page 52). This property page provisions the Policy Manager.

## Step 2—Provision Policy

The screenshot shows the 'Provision IVR Profile—Policy Property Page'. The top navigation bar includes tabs for TTS, IVR, Transfer, ASR Policy, Debug, Prov DIDs, and Extensions. The 'IVR' tab is active. The main content area has a 'Maximum Ports' input field containing '10' and a 'Generate Rule' button. Below this is the 'Application Rule1' field, which contains a default rule string: 'DayOfWeek=,StartTime=,EndTime=,RuleCallType='. An 'Edit' button is next to this field. At the bottom of the window, there are navigation buttons: 'Previous' and 'Next', a 'Disable Help' checkbox, and 'Save' and 'Cancel' buttons.

**Figure 16: Provision IVR Profile—Policy Property Page**

- Enter the maximum number of ports allowed for the IVR profile, and click **Generate Rule**. This provides a default rule in the **Application Rule1** field. Under normal circumstances, do not modify this rule.

**Note:** If you do not specify the number of ports for the IVR profile, GVP assumes that the IVR profile ports are to be the same as the provisioned ports for the customer. Additionally, the maximum number of ports for the IVR profile should not be greater than the maximum of Level 3 ports. Provide a value if you wish to restrict the number of calls for this IVR profile.

- Click **Next**, which opens the **Bandwidth** property page (see Figure 17 on page 53). This property page provisions the Bandwidth Manager (BWM).

## Step 3—Provision Bandwidth

The screenshot shows a web-based configuration interface for an IVR profile. The top navigation bar includes tabs for TTS, IVR, Transfer, ASR Policy, Debug, Prov DIDs, and Extensions. The 'Prov DIDs' tab is selected, and within it, the 'Bandwidth' sub-tab is active. The main content area is mostly empty, with two required fields marked by red asterisks: 'BWM Machine:' and 'BWM URL:'. The 'BWM Machine' field is a dropdown menu currently showing 'select BWM machine'. The 'BWM URL' field is a text input box containing the URL 'http://che111.adcc.alcatel.be:9810/WebNotify.asp?NotifyProcess=bwm1&Action='. At the bottom of the window, there is a row of controls: 'Previous' and 'Next' buttons, a 'Disable Help' checkbox, a green 'Save' button, and a red 'Cancel' button. A 'Copy' button is also visible on the right side of the main area.

**Figure 17: Provision IVR Profile—Bandwidth Property Page**

1. Select a BWM machine from the drop-down list.  
Once you select the BWM machine, the BWM URL field automatically populates with the URL. Under normal circumstances, do not change this URL.
2. Click Next, which opens the Provision TTS property page (see Figure 18 on [page 54](#)). This property page provisions the Text-to-Speech (TTS).

## Step 4—Provision TTS

The screenshot shows the 'Provision IVR Profile—TTS Property Page' with the following configuration:

- TTS Enabled:** ☒
- \* TTS Vendor:** MRCP
- \* TTS Timeout (sec):** 134
- \* TTS Gender:** MALE
- \* TTS Output Format:** Mu-law

Navigation and action buttons at the bottom include: Previous, Next, ☐ Disable Help, Save, and Cancel.

**Figure 18: Provision IVR Profile—TTS Property Page**

1. Select the TTS Enabled check box to enable text-to-speech.

---

**Note:** You must select this check box in order to configure the remaining fields on this page.

---

2. Select a TTS vendor from the drop-down list. To add a TTS vendor to this list, see “Custom Data” on [page 76](#).
3. Enter a timeout value, in seconds, in the TTS Timeout (sec) field. This field indicates the amount of time, in seconds, that the platform waits for the TTS server to respond to a request. If the TTS server does not respond in the allotted time, the request times-out.
4. Select the TTS gender, MALE or FEMALE, from the drop-down list.

---

**Note:** GVP does not check whether the voice fonts are installed. It is your responsibility to provision available voices.

---

5. Select the TTS output format from the drop-down list:
  - Mu-law
  - A-law

- Click Next, which opens the Transfer page (see [Figure 19](#)). This property page provisions the transfer type for the IVR profile.

## Step 5—Provision Transfer

**Figure 19: Provision IVR Profile—Transfer Property Page**

- Select the Enable Transfer check box to enable transfer.

---

**Note:** You must select this check box in order to configure the remaining fields on this page.

---

- Select a Transfer Type from the drop-down list:
  - 1SignalChannel—one channel completes the transfer.
  - ExternalTransfer—performs an external CTI transfer.
  - 2SignalChannel—requires two channels to complete the transfer.
- Select a Transfer Option from the drop-down list:

The available options for the 1SignalChannel transfer type are:

- ATTCourtesy—Executes the scripts to perform the Courtesy transfer when connected to AT&T trunks that are configured with this feature. This transfer applies to the VCS and IPCS. For the IPCS, this requires the Media Gateway to be connected to a trunk that supports the transfer option.

- **ATTConsultative**—Executes the scripts to perform the Consultative transfer when connected to AT&T trunks that are configured with this feature. This transfer applies to the VCS and IPCS. For the IPCS, this requires the Media Gateway to be connected to a trunk that supports the transfer option.
- **ATTConference**—Executes the scripts to perform the Conference transfer when connected to AT&T trunks that are configured with this feature. This transfer applies to the VCS and IPCS. For the IPCS, this requires the Media Gateway to be connected to a trunk that supports the transfer option.
- **SIPRefer**—Performs a transfer using the SIP REFER method on the IPCS.
- **DialogicBlindXfer**—No transfer script is executed, and GVP performs a Dialogic Blind Transfer. This transfer applies to the VCS.
- **ATTCourtesy00B**—Executes the scripts to perform the Courtesy Out-of-Band transfer when connected to AT&T trunks that are configured with this feature. This transfer applies to the VCS.
- **ATTConsultative00B**—Executes the scripts to perform the Consultative Out-of-Band transfer when connected to AT&T trunks that are configured with this feature. This transfer applies to the VCS.
- **ATTConference00B**—Executes the scripts to perform the Conference Out-of-Band transfer when connected to AT&T trunks that are configured with this feature. This transfer applies to the VCS.

The available options for the **2SignalChannel** transfer type are:

- **SIPReferWithReplaces**—Performs a transfer using the SIP REFER with Replaces method on the IPCS, and is to be used with the **2SignalChannel** transfer type.
  - **TBCT**—Performs a transfer using the Two B-Channel Transfer method. This transfer applies to the VCS only.
4. If you select one of the AT&T transfer options, enter the **Reclaim Code**. If the transfer fails, the platform reclaims the call by configuring the valid reclaim code. Not all transfer options support reclaim. Check with your service provider.

---

Note: EMPS does not validate the reclaim code. Make sure that you enter the correct value.

---

5. Click **Next**, which opens the ASR property page (see Figure 20 on [page 57](#)). This property page provisions the Automatic Speech Recognition (ASR).



## Step 6—Provision ASR

The screenshot shows the 'Provision IVR Profile—ASR Property Page' with the 'Policy ASR' tab selected. The page includes the following elements:

- ASR Enabled:** ☒
- \* ASR Vendor:**
- Enable ASR Logging:** ☒
- \* Number of ASR Samples:**
- Application Rule2:**
- Navigation:**   ☐ Disable Help

**Figure 20: Provision IVR Profile—ASR Property Page**

1. Select the ASR Enabled check box to activate the ASR service.

---

**Note:** You must select this check box in order to configure the other ASR fields on this page.

---

2. Select an ASR vendor from the drop-down list. To add an ASR vendor to this list, see “Custom Data” on [page 76](#).
3. Select the Enable ASR Logging check box to enable the IVR profile to instruct the ASR server to perform logging and capture utterances.

---

**Note:** You must select this check box in order to complete the next two steps.

---

4. Enter the number of ASR samples required, and then click **Generate Rule**. A default rule is supplied in the **Application Rule2** field. Under normal circumstances, do not modify this rule.

The number of ASR samples that are captured can be greater than the value configured for **Number of ASR Samples**. This can happen because Policy Manager increments the counter only after a sample capture is successfully completed. Therefore, if several samples are being captured

simultaneously, the total number can exceed the value configured for `Number of ASR Samples`. The number of extra samples that can be potentially captured is minimal, and therefore it should not cause any service impact.

Policy Manager counts the number of ASR samples that are captured. Once the limit on the counter has been reached, it will not be reset until midnight of the current day, or when Policy Manager is restarted. If the counter has not yet reached the limit currently provisioned, it can be increased without a restart. Once the counter is reached, enabling, disabling, or changing the value of `Number of ASR Samples` will not take effect unless the Policy Manager is restarted, thereby resetting the counter.

To determine whether the Policy Manager has been updated as per provisioning, one method is to check the `<customer_pm.appname>` section in the `gvp.ini` file on the PM machine. If the corresponding `apprule1` has been updated on the PM machine, the corresponding PM process is also updated. This update is not instantaneous because it takes time to update the PM process. The maximum time observed in testing (15 customers and 50 applications) is three minutes.

For the most accurate testing results, it is very important to make sure that, as different test cases are performed, Policy Manager is restarted between running tests, so the counter is restarted.

The counter in Policy Manager is incremented only once a call ends. PM does not consider that a sample has been gathered until the call ends (not when an utterance is captured), and then it increments the counter by one. If there are several simultaneous calls, then it is expected that utterances will be gathered for each call, and when they are all complete, the counter will be incremented accordingly. A sample is considered a call, rather than an utterance. If there are 10 calls, there could be more than 10 samples captured if there is more than one recognition per call.

5. Click **Next**, which opens the CTI property page (see Figure 21 on [page 59](#)). This property page provisions the IVR Server Client and the Cisco Queue Adapter.

---

**Note:** The CTI property page will be available only if the IVR Server Client or the Cisco Queue Adapter is installed.

---

## Step 7—Provision CTI

**Figure 21: Provision IVR Profile—CTI Property Page**

1. Select the Enable QAdapter check box to enable IVR Server Clients or Queue Adapters.

---

Notes: You can only select this check box if you have provisioned the customer for IVR Server Clients or Queue Adapters.

Processes associated with the IVR Server Client can be found under the GQA node in EMPS > Servers.

---

2. Select the IVR Server Client or QueueAdaptername from the drop-down list.
3. Select the IVR Server Client or Queue Adapter Script Name (webnotify.asp) from the drop-down list.
4. Enter a default route number. This is the number to be used in the event of a platform failure. In particular, the CFA uses this number to dial out.
5. Select the Confirm QAdapter check box if you want the Cisco ICM to control call flow. Clear the check box for IVR controlled mode.
6. Select the retransfer type from the drop-down list. *Retransfer* is the mechanism by which a user is transferred from one agent to another agent. Currently, *reroute* is the only option available, and the IVR Server supports *reroute* in Network mode only. *Reroute* enables the first agent to drop a call after initiating the retransfer to the second agent. *Reroute* also issues treatments to the user leg that is to be executed, and then eventually transferred, to the second agent.

Note: Steps 7–8 are specific to the Cisco Queue Adapter (CQA), which is an optional feature. If you are not using the CQA, skip these steps.

7. Select a value for the Contact Call Router from the drop-down list.
  - A yes value indicates that the CFA must contact the CQA when it receives a new call.
  - A no value indicates that the CFA will not contact the CQA until the call is queued.
8. Enter the Service ID value in the CQA ServiceID field. The Service ID is used for reporting purposes in Cisco ICM. This value can be left blank if desired.
9. Select the QAdapter location from the drop-down list.
10. Click Next, which opens the OBN property page (see Figure 22). This property page provisions Outbound Notification (OBN).

## Step 8—Provision OBN

The screenshot displays the 'OBN' (Outbound Notification) property page within a configuration interface. The top navigation bar includes tabs for CTI, OBN, Debug, IVR, Transfer, Policy, Prov DIDs, ASR, TTS, and Extensions. The OBN tab is active.

Key configuration fields and sections include:

- Enable OBN:** A checkbox that is checked.
- Failure URL:** A text field containing 'http://10.10.10.200/obnmanager/failure.asp'.
- Max. Queue Size:** A text field containing '10000'.
- Servers Selection:** A section with two lists: 'Available' (empty) and 'Selection' (containing 'dev-leela.us.int.genesyslab.com'). Navigation buttons '>>' and '<<' are between the lists.
- Server Group Selection:** A section with two lists: 'Available' (containing 'obn\_test\_grp', 'OBNTTestGroup2', 'OBNTTestGroup', and 'OBNOCSDemoIPCS') and 'Selection' (containing 'gvp\_72\_obn'). Navigation buttons '>>' and '<<' are between the lists.
- OCS Flag:** A checkbox that is unchecked.
- AfterConnect Timeout:** A text field containing '30'.

At the bottom, there are navigation buttons: 'Previous', 'Next', 'Disable Help' (checkbox), 'Save', and 'Cancel'.

Figure 22: Provision IVR Profile—OBN Property Page

1. Select the **Enable OBN** check box.

---

Note: You can select this check box only if you selected **Outbound** as the IVR profile type when you created this new IVR profile.

---

2. Enter the **Failure URL** that the OBN Manager calls if a call is not placed for any reason. If the trigger request contains a value for the `failure_url` parameter, that URL is used instead of this one. However, if a failure URL is not specified as part of the trigger request, this URL is used by OBN Manager for requests of this IVR profile.
3. In the **Max Queue Size** field, enter the maximum number of unprocessed requests that OBN Manager queues for this IVR profile at any given time. The number that you enter should be large enough to accommodate the expected number of requests from the trigger IVR profile.
4. The **OBN Servers** box lists all OBN Manager machines. From this list, select the machines on which you want to process requests for this IVR profile. You must select at least one machine, but there is no upper limit to the number of machines that you can select. If you want to prevent an OBN Manager machine from processing this IVR profile's requests, do not select that machine.
5. The **OBN Groups** lists all groups of the type **OBNCs**. From this list, select one or more groups. The OBN Manager machines that you selected in the previous step will use VCS/IPCS machines that are members of these groups to make calls for this IVR profile.
6. Select the **OCS Flag** check box if you want Outbound Contact Server (OCS) to use this IVR profile as part of a Campaign.
7. Enter a value, in seconds, in the **AfterConnect Timeout** field. This timeout is set when the IVR profile (voice application) needs to detect an answer, answering machine, or fax. If this timeout is set, after the outbound call is answered, it will wait for specified `afterconnecttimeout` seconds to detect a fax or answering machine.
8. Click **Next**, which opens the **Debug** property page (see Figure 23 on [page 62](#)). This property page provisions debugging for the IVR profile.

## Step 9—Provision Debug

The screenshot displays the 'Provision IVR Profile—Debug Property Page'. At the top, there are tabs for IVR, Policy, Bandwidth, and TTS. Under the IVR tab, there are sub-tabs: Transfer, ASR, CTI, OBN, Debug (selected), Prov DIDs, and Extensions. The main area contains the following settings:

- XML Page Recording: ☐
- Enable Debugging: ☒
- Portal Application: ☒
- Trap Hook:
- Debug Hook:
- CallTrace Hook:
- Bad XML Page Hook:
- Other Exception Hook:
- Caller HUP Hook:

At the bottom, there are navigation buttons: 'Previous' and 'Next'. A 'Disable Help' checkbox is also present. On the right, there is a 'Copy' button. At the bottom right, there are 'Save' and 'Cancel' buttons.

**Figure 23: Provision IVR Profile—Debug Property Page**

You may provision IVR profiles for debugging only under special circumstances. Under normal circumstances, skip the Debug property page entirely.

**Note:** To enable debug/trace logs to be generated, you must add the attribute `adenable` with a value of 1 or true on each PopGateway for each VCS/IPCS that is going to be used for logging. For more information about adding attributes, see “Adding and Deleting Attributes” on [page 72](#).

1. Select the XML Page Recording check box to enable the VCS/IPCS to store local copies of all IVR profile XML pages that are fetched.

The XML pages are stored on the VCS/IPCS under the appropriate IVR profile directory (`\customer\application\tfn\did\session id`).

2. Select the Enable Debugging check box to enable an IVR profile to be debugged.

**Notes:** Several debugging and logging capabilities provide IVR profile developers with additional information that they can use to troubleshoot and resolve problems with an IVR profile.

You must select the Enable Debugging check box in order to configure the remaining fields on this property page.

3. Select the Portal Application check box only if debug information is to be sent to the Genesys Code Center solution.

Selecting this option automatically sets default URLs and attributes in the URL query string for the appropriate debug URLs and overrides any values specified.

Whenever IVR profile debug information is generated, GVP sends it to a collector process. GVP performs an HTTP Post or HTTP Get to the appropriate URL based on the specific event(s) to accomplish this. Genesys recommends that for development purposes you write an ASP or JSP page to capture all the information passed from the platform to aid in debugging and troubleshooting IVR profile problems.

4. Enter the appropriate URL for the available hooks:
  - **Trap Hook**—whenever a platform trap is encountered, the platform sends an HTTP Post of trap data to the specified URL.
  - **Debug Hook**—when a VoiceXML <log> tag is encountered, the platform performs an HTTP Post of the debug information contained within the set of <log> tags to the URL specified.
  - **CallTrace Hook**—once a call has terminated, the platform performs an HTTP Post to the specified URL, providing end-of-call summary information.
  - **Bad XML Page Hook**—if the IVR profile returns an XML page that cannot be successfully parsed, for example, because of a syntax error, the platform performs an HTTP Post of the offending XML page to the specified URL.
  - **Other Exception Hook**—when any uncaught exception is encountered the platform performs an HTTP Get to the specified URL, providing information on this exception.
  - **Caller HUP Hook**—When the call is hung up, the platform sends an HTTP Get to the specified URL.
5. Click Next, which opens the Prov DIDs property page (see Figure 24 on [page 64](#)). This property page provisions Direct Inward Dialing (DID).

## Step 10—Prov DIDs

You should assign DIDs only to IVR profiles of type Inbound. It is not required to assign DIDs to Outbound IVR profiles.

**Figure 24: Prov IVR Profile—Prov DIDs Property Page**

You can search for or add DIDs using one of the following options:

- **DID Group**—selects DIDs from a pre-defined group.
- **Range**—selects DIDs that do not exist in the database.
- **Pattern**—selects DIDs that conform to a particular pattern.
- **Assigned**—assigns DIDs to a particular application.

You can only select DIDs that exist in the database for the group or pattern options. To use DIDs that do not exist in the database, use the Range option.

**To use the DID Groups option:**

1. Select the **DID Groups** radio button and highlight a group from the **DID Group** list box.
2. Click **Get DIDs**. The **Available** list box displays the DID numbers in that group.
3. Select the required DID(s) and click the **>>** button. The **Selection** list box displays the selected DIDs.
4. To remove the DIDs, select them and click the **<<** button. The DIDs return to the **Available** list box.



**To use the Range option:**

1. Select the Range radio button.
2. In the From field, enter the first number in the range.
3. In the To field, enter the final number in the range.
4. Click Get DIDs. The Available list box displays the DID numbers in the range.
5. Select the required DIDs and click the >> button. The Selection list box displays the selected DIDs.
6. To remove the DIDs, select them and click the << button. The DIDs return to the Available list box.

**To use the Pattern option:**

1. Select the Pattern radio button and enter the required DID pattern. The DID pattern must consist of only numbers.

---

Note: You can use the asterisk (\*) character as a wildcard.

---

2. Click Get DIDs. The Matching DIDs list box displays the DID numbers in the pattern.
3. Select the required DIDs and click the >> button. The Selection list box displays the selected DIDs.
4. To remove the DIDs, select them and click the << button. The DIDs return to the Available list box.

**To use the Assigned option:**

1. Select the Assigned radio button.
2. Select a Reseller from the drop-down list.
3. Select a Customer from the drop-down list.
4. Select an IVR profile from the drop-down list.
5. Click Get DIDs. The Matching DIDs list box displays the DID numbers in the group.
6. Select the required DIDs and click the >> button. The Selection list box displays the selected DIDs.
7. To remove the DIDs, select them and click the << button. The DIDs return to the Available list box.

To check for errors:

The bottom of the Prov DIDs property page provides the following error-checking options. Selecting these options enables the reporting of any errors that exist with the selected DIDs. No changes are made to the application or DIDs as part of the error checking.

- Report errors if DID is allocated—select this check box if you want to be notified if any of the selected DIDs have been previously allocated.
- Report Errors if DID does not exist—select this check box if you want to be notified if any of the selected DIDs do not exist. To select DIDs that do not exist in the database, ensure that this check box is not cleared. In this case, DID.XML files are generated and DID values are added to the database.

## Step 11—Extensions

**Extend AppXML**

Note: Enter sets of name, value pairs - they will be added to App.XML files.  
No validations are performed on these values, so please be sure you know what impact your input will have.

	XMLSetName		XMLSetValue
Additional Set 01 :	<input type="text"/>	=	<input type="text"/>
Additional Set 02 :	<input type="text"/>	=	<input type="text"/>
Additional Set 03 :	<input type="text"/>	=	<input type="text"/>
Additional Set 04 :	<input type="text"/>	=	<input type="text"/>
Additional Set 05 :	<input type="text"/>	=	<input type="text"/>
Additional Set 06 :	<input type="text"/>	=	<input type="text"/>
Additional Set 07 :	<input type="text"/>	=	<input type="text"/>
Additional Set 08 :	<input type="text"/>	=	<input type="text"/>
Additional Set 09 :	<input type="text"/>	=	<input type="text"/>
Additional Set 10 :	<input type="text"/>	=	<input type="text"/>

◀ Previous    ▶ Next    ☐ Disable Help   

**Figure 25: Provision IVR Profile—Extensions Property Page**

You can enter sets of name-value pairs that EMPS adds to App.XML files. IVR profile developers use them to add particular variables into the IVR profile.

If desired, enter name-value pairs, and then click **Save** to save the IVR profile.

H.323 Session Manager (HSM) can prefix the DNIS value received from an inbound call to associate it with the outbound leg of the same call.

To set up the outbound message:

1. In the `XMLSetName` field, enter `PrefixDNISonOutbound`.
2. In the `XMLSetValue` field, enter:
  - 0—HSM will not prefix the DNIS on the outbound setup message.
  - 1—HSM will prefix the DNIS on the outbound setup message

---

**Note:** EMPS does not validate the custom entries on this page. Be sure to enter the correct values. Also, the copy feature does not copy the data items on this page.

If a new Dispenser is put into service, you must regenerate all existing IVR profiles.

---

## Modifying an IVR Profile

1. On the EMPS navigation tree, expand the `Reseller` object, the reseller, and then the customer.
2. Select the IVR profile that you want to modify, and then do one of the following:
  - Right-click it. From the shortcut menu, select `Edit`.
  - Single-click it. From the main frame, click `Edit IVR Profile`.
  - Double-click it.
3. Make any changes on the `IVR Profile` property page, and then click **Save**.

## Copying IVR Profile Attributes

For IVR profile provisioning, you can copy an entire set of attributes or a single attribute from one IVR profile to another.

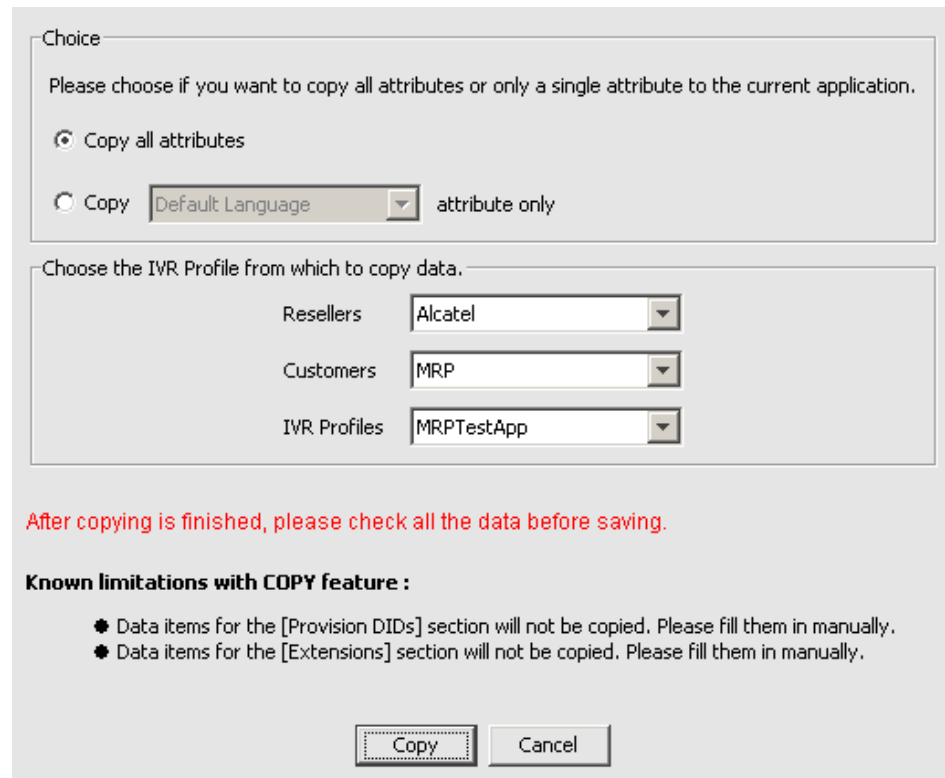
---

**Note:** The copy feature does not copy any transfer-related attributes. The copy feature does not work if pop-up windows are disabled in the browser.

---

To copy an entire set of attributes:

1. In the provision IVR profile section of the current IVR profile, click **Copy**. The `Copy Attribute Values` dialog box opens (see [Figure 26](#)).



**Choice**

Please choose if you want to copy all attributes or only a single attribute to the current application.

☒ Copy all attributes

☐ Copy Default Language attribute only

Choose the IVR Profile from which to copy data.

Resellers Alcatel

Customers MRP

IVR Profiles MRPTestApp

After copying is finished, please check all the data before saving.

**Known limitations with COPY feature :**

- Data items for the [Provision DIDs] section will not be copied. Please fill them in manually.
- Data items for the [Extensions] section will not be copied. Please fill them in manually.

Copy Cancel

**Figure 26: Copy Attribute(s) Values Dialog Box**

2. Select the Copy all attributes radio button.
3. From the drop-down lists, select the IVR profile from which to copy the data.
4. Click Copy.
5. Click Yes when prompted Copying all possible attributes from <IVR\_profile\_name> IVR profile. Would you like to continue?  
EMPS copies the attributes to the current application and the page automatically refreshes to reflect the changes. Genesys recommends that you navigate through all of the pages and verify that you copied the desired values.

To copy a single attribute:

1. In the provision IVR profile section of the current IVR profile, click Copy. The Copy Attribute Values dialog box opens.
2. Select the Copy radio button, and then select the desired attribute from the drop-down list.
3. From the drop-down lists, select the IVR profile from which to copy the data.
4. Click Copy.

5. Click Yes when prompted Copying the <attribute\_name> attribute from <IVR\_profile\_name> IVR profile. Would you like to continue?

EMPS copies the attribute to the current application and the page automatically refreshes to reflect the changes.

## Deprovisioning IVR Profiles

If the IVR profile is part of one or more tasks, the EMPS prompts whether you want to remove the IVR profile from associated tasks. If you select yes, the EMPS removes the IVR profile from tasks and then deprovisions the IVR profile. If you select no, the IVR profile is not deprovisioned.

To deprovision an IVR profile:

1. On the EMPS navigation tree, expand the Reseller object, the reseller, and then the customer.
2. Select the IVR profile that you want to delete, and then do one of the following:
  - Right-click it. From the shortcut menu, select **Deprovision**.
  - Single-click it. From the main frame, click **Deprovision IVR Profile**.
3. Click Yes when prompted, **Deprovision this IVR Profile?** This removes the IVR profile from EMS components, and the following occurs:
  - Calls for a deprovisioned IVR profile do not complete.
  - All network information for this IVR profile is lost.

## Deleting an IVR Profile

Before deleting an IVR profile, make sure that the IVR profile is deprovisioned.

1. On the EMPS navigation tree, expand the Reseller object, the reseller, and then the customer.
2. Do one of the following:
  - Select the IVR profile that you want to delete, and then right-click on it. From the shortcut menu, select **Delete**.
  - Select the IVR profile that you want to delete, and then single-click on it. From the main frame, click **Delete IVR Profile**.
3. Click Yes when prompted **Are you sure you would like to delete this IVR Profile?** This deletes the selected IVR profile.

## Regenerating an IVR Profile

1. On the EMPS navigation tree, expand the **Reseller** object, the reseller, and then the customer.
2. Select the IVR Profile that you want to regenerate, and then do one of the following:
  - From the main frame, click **Regenerate IVR Profile**.
  - Right-click the IVR Profile, and from the shortcut menu, select **Regenerate**.

A message box appears with the text: **Regenerate this IVR Profile [IVR Profile]?**

3. Click **Yes**. EMPS regenerates and redeploys the IVR Profiles and the DID XML files.

## Shortcuts

The **Shortcuts** option enables you see the status of each Dispenser and to view the App.XML files that reside on the Dispenser.

1. On the EMPS navigation tree, expand the **Reseller** object, the reseller, and the customer.
2. Single-click on the IVR profile.

The **IVR Profile Information** screen appears. Scroll to the bottom of the page to see the **Shortcuts** (see [Figure 27](#)).

Shortcuts			
View IVR Profile XML Files (3 dispensers)			
<i>(Opens in a new Browser Window)</i>			
<b>Dispenser:</b> dev-laplace.us.int.genesyslab.com (Active)	<a href="#">IVRProfile.XML</a>	<a href="#">IVRProfileOutbound.XML</a>	<a href="#">IVRProfileOutboundDID.XML</a>
<b>Dispenser:</b> dev-neutron.us.int.genesyslab.com (Active)	<a href="#">IVRProfile.XML</a>	<a href="#">IVRProfileOutbound.XML</a>	<a href="#">IVRProfileOutboundDID.XML</a>
<b>Dispenser:</b> temp5 (Inactive - the files may be old)	<a href="#">IVRProfile.XML</a>	<a href="#">IVRProfileOutbound.XML</a>	<a href="#">IVRProfileOutboundDID.XML</a>

**Figure 27: IVR Profile Shortcuts Screen**

3. From the main frame, click **View Dispenser App.xml**, which opens a new window with the currently selected application's App.XML on the Dispenser.

To view the Dispenser AppOutbound.xml file:

1. On the EMPS navigation tree, expand the Reseller object, the reseller, and the customer.
2. Single-click on the IVR profile.
3. From the main frame, click View Dispenser AppOutbound.xml, which opens a new window with the currently selected application's AppOutbound.XML on the Dispenser.

To view the Dispenser AppOutboundDID.xml file:

1. On the EMPS navigation tree, expand the Reseller object, the reseller, and the customer.
2. Single-click on the IVR profile.
3. From the main frame, click View Dispenser AppOutboundDID.xml, which opens a new window with the currently selected application's AppOutboundDID.XML on the Dispenser.

---

Note: The AppOutboundDID.XML file is not versioned, and the shortcut always point to the default location on the Dispenser. The HTTP Safe AppXML Folders parameter does not have any effect on this shortcut.

---

---

## Servers

The Servers section in the EMPS is divided into two main sections:

- The navigation tree displays all of the server objects. Below each object is a list of servers of that type. Nodes are listed below each server.
- The property pages display information based on what you select in the left frame.

The label for some attributes in the Servers section appear in bold text. This indicates that changing those attributes requires that you restart WatchDog.

## Editing Server Information

1. On the EMPS navigation tree, expand the Servers object, and then expand the server type.
2. Select the server that you want to edit, and then do one of the following:
  - Right-click it. From the shortcut menu, select Edit.
  - Single-click it. From the main menu, click Edit Node.
  - Double-click it.
3. Edit the parameters as needed, and then click Save.

## Copying Nodes

You can only copy custom nodes or nodes within the same server (for example, PopGateway1 to PopGateway2) and expect them to function properly.

Do not copy servers, especially the servers registered in the Consolidated EMS setup.

To copy a node:

1. On the EMPS navigation tree, expand the Servers object, the server type, and then the <ServerName>.
2. Select the node that you want to copy, and then do one of the following:
  - Right-click it. From the shortcut menu, select **Create a copy**.
  - Single-click it. From the main frame, click **Copy Node**.

The **Server** property page opens.

3. Click **Copy** at the bottom of the property page. The **Copy Server Node** dialog box opens.
4. Enter the target node in the **To Node** field, and select the **Copy Sub tree** check box to copy the sub-tree of the current node.
5. Click **Copy** to copy the selected node.

## Deleting Nodes from a Server

1. On the EMPS navigation tree, expand the Servers object, the server type, and then the <ServerName>.
2. Select the node that you want to delete, and then do one of the following:
  - Right-click it. From the shortcut menu, select **Delete**.
  - Single-click it. From the main frame, click **Delete Node**.
3. Select **Yes** when prompted to delete the selected node.

---

**Warning!** When you delete the selected node, all children nodes under it will also be deleted.

---

## Adding and Deleting Attributes

Do not add new attributes unless the attributes you are adding have been approved by Genesys Technical Support. In some cases, it may not be possible to delete attributes once they have been added.

Although it is possible to add attributes to either Static nodes or Dynamic nodes, it is important to understand that attributes are handled differently by each of these two node types.



Static node attributes remain preserved unless you explicitly change them, or if you reinstall the system.

EMPS recreates and deletes Dynamic node attributes each time a relevant change occurs. Dynamic nodes include PM, IVR Server Client, and CQA (optional feature) process nodes. For this reason, do not add attributes to Dynamic nodes.

To add new attributes to a child node:

1. On the EMPS navigation tree, expand the Servers object, the server type, and then the <ServerName>.
2. Select the node to which you want to add new attributes, and then do one of the following:
  - Right-click it. From the shortcut menu, select Edit.
  - Single-click it. From the main menu, click Edit Node.
  - Double-click it.
3. Click the Add New Attribute button at the bottom of the property page. This opens the Attribute Name and Attribute Values fields.
4. Enter the attribute name and attribute value.
5. Click Save to add the attribute to the node.

To delete attributes from a child node:

1. On the EMPS navigation tree, expand the Servers object, the server type, and then the <ServerName>.
2. Select the node to which you want to delete attributes, and then do one of the following:
  - Right-click it. From the shortcut menu, select Edit.
  - Single-click it. From the main menu, click Edit Node.
  - Double-click it.
3. Click the Delete Attributes button. A column of attribute check boxes appear.
4. Select the check box next to the attribute to be deleted and click Save.

## Adding a New Cache Server to the EMPS

A *Cache Server* caches XML files. When the EMPS generates new XML files, it deletes the older XML files from the Cache Servers. New files that the EMPS generates are not used until older files are purged from the Cache Server. The EMPS must know which Cache Servers are present in the network, and then send them requests to delete specific files.

A Sample Cache Server node is created by default with EMPS registration.

To add a new Cache Server:

1. On the EMPS navigation tree, expand the Servers object.
2. Right-click on the Cache Server node.
3. From the shortcut menu that opens, select New Server. The GUI prompts you to enter a server instance name and specify a file that contains details about the server.
4. Enter the FQDN of the Cache Server—for example, `cache1.mycompany.net`.
5. Navigate to the CacheFlow.csv file using the Browse button. The file is in the CN\Config\ folder.

---

Note: The .csv file is provided with the EMPS. If you are on a different machine, you need access to the EMPS machine.

---

6. Click Save. The EMPS creates a new server instance node that is based on the information provided, and the EMPS starts purging XML files from this Cache Server.
7. Add this Cache Server entry to the DNS.

To prevent the EMPS from deleting files on a Cache Server:

1. On the EMPS navigation tree, expand the Servers object, and then the Cache node.
2. Right-click the Cache Server from which you want to stop the purging.
3. From the shortcut menu that opens, select Edit.
4. If there is an Active field, enter a value of 0 (zero) and click Save.  
If there is no Active field, click Add New Attributes. In the two fields that appear, enter the following values:
  - Attribute Name—active
  - Attribute Value—0 (zero)
5. Click Save. The EMPS will not contact this Cache Server for purging XML files.

## Notifying a Server

When you have modified or provisioned a server, notify the server of the changes by clicking Notify Server on the Server shortcut menu or on the Server main frame. This updates the server information.

## Opening the NetMgt GUI

This option opens, in a new window, the NetMgt GUI for the selected server.

---

**Note:** The NetMgt GUI link opens the GUI only on servers where Genesys software is installed. The link will not work on servers where this is not the case, such as IVR servers, Soft Switches, Media Gateway, Cache servers, and so on.

---

To open the NetMgt GUI from the Servers GUI:

1. On the EMPS navigation tree, expand the Servers object, and then expand the server type.
2. Select the desired server.
3. From the main frame, click **Open NetMgt GUI**. The NetMgt GUI for that server opens. The NetMgt GUI is discussed in [Chapter 6](#).

## Importing the Server Instance CSV

This section provides instructions for importing the Server Instance CSV file. These files contain names of the fields that are entered during server provisioning. The file type is .csv. You can use this file to add additional attributes to the respective server's .ini file.

---

**Notes:** You can import both an Instance file as well as a Template CSV file.

If you are creating servers for the first time, you must provide the server type.

---

Use this feature only for the Media Gateways, Cache Servers, and Soft Switches.

To import a Server Instance CSV:

1. On the EMPS navigation tree, expand the Servers object and the server type.
2. Select the desired server, and then do one of the following:
  - Right-click it. From the shortcut menu, select **Import CSV**.
  - Single-click it. From the main frame, click **Import Server Instance CSV**.

The **Import CSV** property page opens.

3. Enter a numeric server version type. The version should correspond to the server version displayed for each server under the Servers link.

4. Enter the path to the Server Instance file or click **Browse** to find the file.
5. Click **Import**.

---

## Custom Data

This section describes the Custom Data feature, which enables you to add new TTS vendors, ASR vendors, as well as numerous other options to various portions of the EMPS.

### Enabling the Custom Data Feature

---

**Warning!** Do not modify any other parameters visible in Custom Data. Modifying any other parameter might cause serious, unrecoverable damage to your installation.

---

To enable the Custom Data feature:

1. Expand the **Servers** object, and then expand the nodes **EMPS > <EMPS Machine Name>**.
2. Select the **SPS** node, and then click **Edit** on the main page, or, right-click the **SPS** node, and then select **Edit** from the shortcut menu. The **Server** property pages for that node opens.
3. Select the **EMPS** tab, and change the value of the **EMPS View** field to **Advanced**.
4. Click **Save**.
5. Log out of EMPS, then log back in to EMPS. The Custom Data feature is now enabled and visible in the EMPS navigation tree.

### Adding TTS Vendors

1. Expand the **Custom Data** object, and then expand **System Lists**.
  - On Solaris hosts, right-click **ttsvendors\_solaris**, and then select **Edit**, or, double-click **ttsvendors\_solaris**.
  - On Windows hosts, right-click **ttsvendors** and then select **Edit**, or, double-click **ttsvendors**.

The **Custom List** property page opens.

2. Enter the TTS vendor in both the **Display Text** field and **Value** field.
3. Click **Add**, which adds the TTS vendor to the **List Options** box.
4. Click **Save**. The TTS vendor now appears in the **TTS Vendor** drop-down list on the IVR profile **Provision TTS** page.

## Adding ASR Vendors

1. Expand the `Custom Data` object, and then expand `System Lists`.
  - On Solaris hosts, right-click `asrvendors_solaris`, and then select `Edit`, or, double-click `asrvendors_solaris`.
  - On Windows hosts, right-click `asrvendors`, and then select `Edit`, or, double-click `asrvendors`.

The `Custom List` property page opens.

2. Enter the ASR vendor in both the `Display Text` field and `Value` field.
3. Click `Add`, which adds the ASR vendor to the `List Options` list box.
4. Click `Save`. The ASR vendor now appears in the ASR Vendor drop-down list on the IVR profile `Provision ASR` page.

## Disabling the Custom Data Feature

1. Expand the `Servers` object, and then expand the nodes `EMPS > <EMPS Machine Name>`.
2. Select the `SPS` node, and then click `Edit` on the main page, or, right-click the `SPS` node, and then select `Edit` from the shortcut menu. The `Server` property pages for that node opens.
3. Select the `EMPS` tab, and change the value of the `EMPS View` field to `Standard`.
4. Click `Save`.
5. Log out of EMPS, then log back in to EMPS. The Custom Data feature is now disabled and is no longer visible in the EMPS navigation tree.

---

## Tasks

This section describes the `Tasks` feature, which enables you to schedule tasks that regenerate IVR Profiles, or change IVR URLs and monitor their status.

---

**Note:** You must schedule and execute tasks in the EMPS according to the EMPS server time.

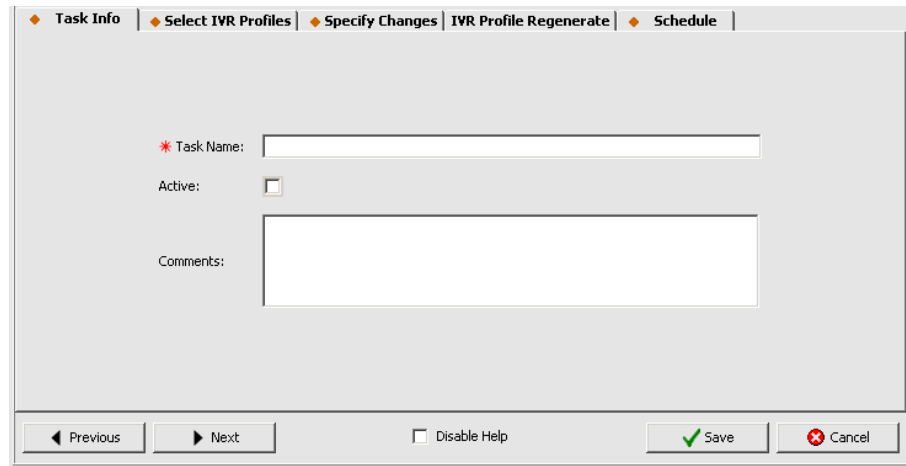
---

## Creating a New Task

1. Select the `Tasks` object, and then right-click it.
2. Select `New Task`. The `Create New Task` property pages open, with `Task Info` as the first property page (see [Figure 28](#)).

There are five steps to adding a task. Once you have completed the Task Info property page, click Next to go to the next property page. When that property page is complete, click Next to open the next property page in the sequence, and so on. Continue this process until all of the property pages are complete.

## Step 1—Task Info

The screenshot shows a web-based form titled "Task Info" with a tabbed interface. The tabs are "Task Info", "Select IVR Profiles", "Specify Changes", "IVR Profile Regenerate", and "Schedule". The "Task Info" tab is active. The form contains a red asterisk followed by "Task Name:" and a text input field. Below this is "Active:" with an unchecked checkbox. Further down is "Comments:" with a larger text area. At the bottom, there are four buttons: "Previous" (disabled), "Next" (active), "Disable Help" (checkbox), and "Save" (with a green checkmark icon) and "Cancel" (with a red X icon).

**Figure 28: Create New Task—Task Info Property Page**

1. Enter a task name.
2. In order for the task to be executed, select the Active check box. If you clear this check box, the EMPS creates the task, but does not execute it.
3. (Optional) Enter any comments or additional descriptive information in the Comments field.
4. Click Next. The Select IVR Profiles property page opens (see [Figure 29](#)).

## Step 2—Select IVR Profiles

The screenshot shows the 'Select IVR Profiles' property page. The 'Task Info' tab is selected. The 'List of Resellers' and 'List of Customers' dropdowns are empty. The 'List of IVR Profiles' field is empty and marked with a red asterisk. The 'Group Selection' section contains two empty list boxes, 'Available' and 'Selection', with '>>' and '<<' buttons between them. The bottom navigation bar includes 'Previous', 'Next', 'Disable Help', 'Save', and 'Cancel' buttons.

**Figure 29: Create New Task—Select IVR Profiles Property Page**

1. Select the desired reseller and customer from their respective drop-down lists. The IVR profiles for that reseller and customer now appear in the List of IVR Profiles field.

---

Note: IVR profiles that are designated as Network Announcement IVR profiles do not appear in this list. You cannot update these IVR profiles by using this type of task.

---

2. Repeat Step 1 as needed to add additional IVR profiles from different resellers and customers.
3. Click Next. The Specify Changes property page opens (see [Figure 30](#)).

## Step 3—Specify Changes

**Figure 30: Create New Task—Specify Changes Property Page**

1. To update the primary IVR URL, select its check box, and then enter the primary IVR URL. You can click `Default QueryString` to get the full query string. To launch the URL, click `View URL`.
2. To update the backup IVR URL, select its check box, and then enter the backup IVR URL. You can click `Default QueryString` to get the full query string. To launch the URL, click `View URL`.
3. Click `Next`. The EMPS applies the changes entered on this page to all of the selected IVR profiles. The `IVR Profile Regeneration` property page opens.

## Step 4—IVR Profile Regeneration

1. To regenerate the `App.XML` pages and push them to the Dispenser after the IVR profiles are updated, select the `Allow IVR Profile Regeneration` check box.
2. Click `Next`. The `Schedule` property page opens.

## Step 5—Schedule

The current EMPS server time displays on this page, and you can use it as a reference timestamp to schedule tasks.

1. Enter the task execution date and time in EN-US format (MM/DD/YYYY HR:MIN:SEC)—for example, `09/07/2007 15:30:20`.

You can schedule a task to be executed at a particular time; however, the execution of the task might not happen at that exact time. The interval after which the EMPS checks for tasks to be executed is defined in the EMPS



configuration by the parameter `Scheduled Tasks Interval`. Consequently, the task execution time can be later than the scheduled time by this amount. If a higher accuracy is desired, reduce the value of this parameter; as a result, the EMPS checks for tasks to be executed more frequently.

2. Click **Save**. The EMPS adds the new task.

## Modifying a Task

1. Expand the **Tasks** object.
2. For the task that you want to modify, do one of the following:
  - Right-click it, then select **Edit** from the shortcut menu.
  - Double-click it.

The property pages for that task open.

3. Edit the desired task page(s) as needed, and then click **Save** to save the changes. The EMPS modifies the task.

## Removing a Task

1. Expand the **Tasks** object.
2. Right-click the task that you want to remove, and then select **Delete** from the shortcut menu.
3. Click **OK** when prompted to confirm the task removal. The EMPS removes the task.

## Viewing Task Status

To view the status of a task, click the **Tasks** object.

The **Task(s) Status** page opens, which displays the following task information:

- Task Name
- Scheduled/Execution Time
- Status
- Result

---

## Server Groups

You can group servers into functional groups, which is a necessary function for ASR servers, TTS servers, Outbound VCSs, and Media Gateways. Any one server can belong to a number of different groups.

For example, you can group ASR servers together. Then, if the VCS/IPCS needs to contact the ASR servers, the VCS/IPCS has additional servers to contact if the first attempt on a given server fails.

## Creating Server Groups

1. On the EMPS navigation tree, select **Server Groups**, and then right-click it.
2. Select **Add New Group**. The **Groups** property page opens.
3. Enter the name of the new group in the **Group Name** field.
4. Select the server group type from the drop-down list. The **Available** field displays a list of all the provisioned servers.
5. To add servers from the **Available** field to the new **Selection** field, which represents the new group, select the server, and then click the **>>** button.
6. Once you have added all of the required servers to the **Selection** field, click **Save**. The new group appears on the left frame when you refresh the EMPS.

## Editing Server Groups

1. On the EMPS navigation tree, expand **Server Groups**, select the server group to be modified, and then right-click it.
2. Select **Edit**. The **Update Server Groups** property page opens. You can edit the **Server Group Type** or the **Server Group Selection** field.
3. To add or remove servers from the group, select the server name and then click **>>** or **<<**.
4. Click **Save**, which saves the changes and updates the group.

## Removing Server Groups

When you delete a group, servers that use the group will no longer be able to see its members, which results in incorrect behavior. To prevent this, before deleting a group, remove it from the configuration of all servers that use it. After removing the group from a server's configuration, notify the server so that changes take effect. When the group to be deleted is not being used by any server, delete it from the EMPS.

To remove a group:

1. On the EMPS navigation tree, expand **Server Groups**, select the server group to be deleted, and then right-click it.
2. Select **Delete**.
3. Click **Yes** when prompted to confirm the deletion of the server group.

## Copying Server Groups

1. On the EMPS navigation tree, expand Server Groups, select the server group to be copied, and then right-click it.
2. Select Create a copy.
3. Specify the target group in the To Group field.
4. Click Save to copy the selected group.

---

## DID Groups

The DID Groups feature in the EMPS enables you to create DID groups and populate them with DIDs. Once you create a DID group, you can edit, remove, view, or transfer it.

## Creating DID Groups

1. Select DID Groups on the Main tab, and then right-click it. Select Add New Group. The Add New Groups page appears (see [Figure 31](#)).



**Figure 31: Create New DID Groups Dialog Box**

2. Enter a name in the Group Name field.
3. Enter the desired range of numbers in the From and To fields, and then click the >> button. The EMPS adds the range to the group.

To remove a DID from the group, select the DID, and then click the << button.

4. Click Save to create the group.

---

Note: This page displays up to 300 existing member DIDs, along with the IVR profile (if any) to which they are assigned. You can add only 250 DIDs to a DID group at one time.

---

---

## Reports

All of the reports in the EMPS have the following features:

- Navigation buttons—Enables you to page through the reports.
- Records Per Page—Enables you to set the number of records per page.
- Show Full Report—Enables you to view the full report without any page breaks.
- Download Report Data in CSV Format—enables you to open the report in a text editor, or in Microsoft Excel.

---

Notes: When downloading report data in .csv format and then using Microsoft Excel to view or edit the data, be aware that Excel does not correctly display any DIDs longer than 16 digits. Excel rounds off the value, which results in inaccurate data.

Additionally, when CSV files are opened in Microsoft Excel, the leading zeros in a DID might not be displayed. If a DID does not start with a zero, it is displayed correctly; however, Microsoft Excel might still use an exponential form to display the DID. If you open the CSV file in Notepad, the DIDs are displayed correctly.

---

- Sort functions—Enables you to sort by a column heading you click on.

## RCA Reports

The following Resellers, Customers, and IVR profiles (RCA) Reports are available:

- RCA Listing—Lists all resellers, customer, and IVR profiles.
- Customer Information—Lists all customers and their details.
- Application Information—Lists all IVR profiles and their details.
- Application DIDs—Lists all IVR profiles with allocated DIDs.

## Servers Reports

The following Servers Reports are available:

- **Servers Listing**—Lists all servers and their details that are in the network and registered with EMPS.
- **Policy Manager**—Lists all PM servers and which customers are using which server. You might find this report useful for determining the load on a specific PM server.
- **QAdapter**—Lists all IVR Server Clients and Queue Adapters, and which customers are using which ones. You might find this report useful for determining the load on a specific Queue Adapter.

## DIDs Reports

The following DIDs Reports are available:

- **DID Group Listing**—Lists all DID groups.
- **DID Listing**—Lists all DIDs.
- **DID Application Status**—Lists all DIDs with allocation status.

## Find

The following Find functions are available:

- **DID Details**—Enables a search of DID numbers.
- **TFN Details**—Enables a search of toll-free numbers (TFNs).

You can use the \* character as a wild card. When using the wild card, it is important to note that it is not a placeholder. For example, if you specify find criteria in **DID Details** as \*1\*2, the result shows you all DIDs that contain 1 and 2, not just DIDs that contain 1 and 2 in the second and fourth place, respectively.

As another example, if you enter 1212, as well as 1212\*, for the search criteria, the EMPS returns several results: 12121, 121291, 191212, and so on.

---

## Users

The Users feature enables you to set user-level security in the EMPS.

- The EMPS supports role-based security, with a set of pre-defined roles. Users will not be able to change the role information.
- The EMPS has one non-removable admin user that will be used to initially configure it.
- GVP users can create and manage more EMPS users through SPS.

- More than one user can login to the EMPS and perform provisioning tasks. If concurrent changes are made to the same object, the last change is saved.
- Changes made by one user will become visible to another user only after the second user refreshes the data or accesses the data again.

To create a new user:

1. Select the Users object, and then right-click it. From the shortcut menu, select Add New User . The Add New Users property page opens (see [Figure 32](#)).

The screenshot shows a software window titled "Users". Inside, there's a "User Management" section with three fields: "User Name", "Password", and "User Role" (which is a dropdown menu currently showing "Administrator"). Below this is a "User Role Summary" section containing text descriptions for four roles: Administrator (full access), Supervisor (privileged, except for certain tasks), Operator (same as Supervisor plus Managing Tasks), and Guest (low privileged, read access only). A link "Click Here" points to more information about roles and permissions. At the bottom of the window are five buttons: "Previous", "Next", "Disable Help" (with a checkbox), "Save" (with a green checkmark icon), and "Cancel" (with a red X icon).

**Figure 32: Add New Users Property Page**

2. Enter the user name and password.
3. From the User Role drop-down list, select the security level that you want to assign to this user.
4. Click Save . The new user is added to the navigation tree underneath the Users object.

You can view, edit or delete users after they have been added depending on the type of user role. [Table 1](#) lists the user roles and permissions for each EMPS node.

**Table 1: User Roles and Permissions**

Node	Menu Item	Admin	Supervisor	Operator	Guest
Reseller	Add New	Y	Y	Y	N
	Edit	Y	Y	Y	N
	View	Y	Y	Y	Y
	Delete	Y	Y	N	N
Customer	Add New	Y	Y	Y	N
	Edit	Y	Y	Y	N
	View	Y	Y	Y	Y
	Delete	Y	Y	N	N
	Provision	Y	Y	N	N
	View Provision	Y	Y	Y	Y
	DeProvision	Y	Y	N	N
	Regenerate	Y	Y	N	N
IVR Profile	Add New	Y	Y	Y	N
	Edit	Y	Y	Y	N
	View	Y	Y	Y	Y
	Delete	Y	Y	N	N
	Provision	Y	Y	N	N
	View Provision	Y	Y	Y	Y
	DeProvision	Y	Y	N	N
	Regenerate	Y	Y	N	N

**Table 1: User Roles and Permissions (Continued)**

Node	Menu Item	Admin	Supervisor	Operator	Guest
Server	Add New	Y	Y	Y	N
	Edit	Y	Y	Y	N
	View	Y	Y	Y	Y
	Delete	Y	Y	N	N
	Create Copy	Y	Y	Y	N
	Import CSV	Y	Y	Y	N
	Notify Server	Y	Y	Y	N
	Restart GVP	Y	N	N	N
	Refresh	Y	Y	Y	N
System Defaults	Edit	Y	N	N	N
	View	Y	Y	Y	Y
System Lists	Edit	Y	N	N	N
	View	Y	Y	Y	Y
Tasks	Add New	Y	Y	N	N
	Edit	Y	Y	N	N
	View	Y	Y	Y	Y
	Delete	Y	Y	N	N
	Check Status	Y	Y	Y	N
Server Groups	Add New	Y	Y	Y	N
	Edit	Y	Y	Y	N
	View	Y	Y	Y	Y
	Delete	Y	Y	N	N



**Table 1: User Roles and Permissions (Continued)**

Node	Menu Item	Admin	Supervisor	Operator	Guest
DID Groups	Add New	Y	Y	Y	N
	Edit	Y	Y	Y	N
	View	Y	Y	Y	Y
	Delete	Y	Y	N	N
	DID Transfer	Y	Y	Y	N
Reports	View	Y	Y	Y	Y
Users	Add New	Y	N	N	N
	Edit	Y	N	N	N
	View	Y	Y	Y	Y
	Delete	Y	N	N	N
Options	View	Y	Y	Y	Y
Diagnostics	Test Again	Y	Y	Y	Y

---

## Options

The Options feature displays the GVP options that have been installed and enabled. The fields on the Options property pages are read-only.

---

**Note:** Installing a GVP component automatically enables options and features associated with the component. There is no need to turn on options manually.

---

To access the Options feature, double-click on the Options object. The Options property page opens (see [Figure 33](#) for an example).

Reporting Monitoring Base	CISCO CTI	H323 Interface	SIP Interface	ASR Log Management
Base	Multi-Tenancy			Enhanced Media
<p>Outbound Notification Feature: <input checked="" type="checkbox"/></p> <p>TDM Feature: <input checked="" type="checkbox"/></p> <p>VoIP Feature: <input checked="" type="checkbox"/></p> <p>ASR Feature: <input checked="" type="checkbox"/></p> <p>Text To Speech Feature: <input checked="" type="checkbox"/></p> <p>Bandwidth Mgmt Feature: <input checked="" type="checkbox"/></p> <p>Policy Mgmt Feature: <input checked="" type="checkbox"/></p> <p>IVRServer Client Feature: <input checked="" type="checkbox"/></p>				

◀ Previous    ▶ Next    ☐ Disable Help       

Figure 33: Options Property Page

## Diagnostics

The **Diagnostics** page in the EMPS enables you to check system connectivity. The EMPS performs the tests automatically every 60 seconds, or you can right-click the **Diagnostics** object, and select <Test Again> on the shortcut menu. The following system connectivity tests are available:

- **EMPS Server connectivity**—Determines if the EMPS server is running on the EMPS machine.
- **Database Server connectivity**—Determines if the EMPS can connect to the EMPS database. This is only used when reporting components are installed.
- **Directory Server connectivity**—Determines if the EMPS can connect to the specified Directory server.

## Viewing Diagnostics

1. Click the **Diagnostics** object. The **View Diagnostics** property page opens (see [Figure 34](#)).

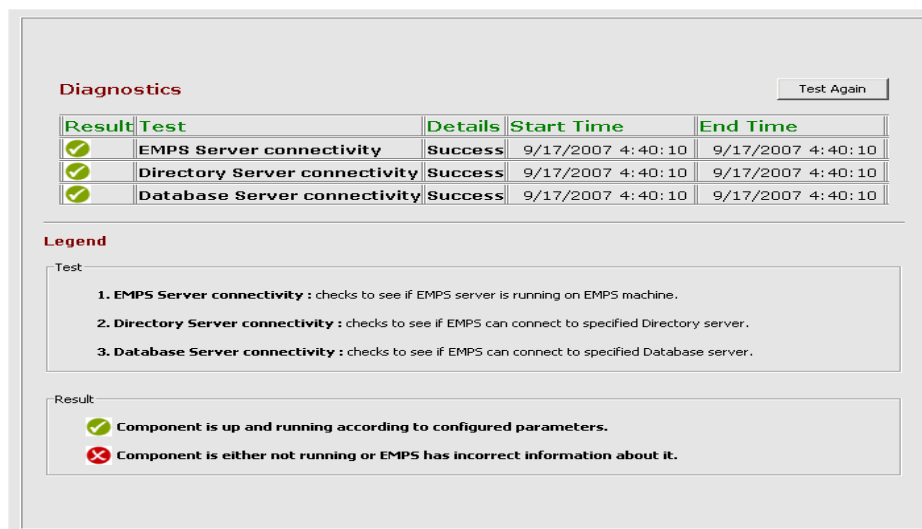


Figure 34: Diagnostics Page

- To perform an immediate test, right-click the Diagnostics object, and then select Test Again, which immediately refreshes the page.

## Recovery from OpenLDAP Data Corruption

In the previous release of Genesys Voice Platform (GVP), if OpenLDAP was used by EMPS, the LDAP database could corrupt if the EMPS machine shut down unexpectedly. This has been fixed in GVP 7.6.

The following sections describe how to recover from data corruption.

### Auto-Recovery by EMPS

When WatchDog starts on the EMPS host, it sends a flag to the SCAConfig requesting auto-recovery of OpenLDAP database. The SCAConfig temporarily stops the OpenLDAP service, runs the OpenLDAP's db\_recover utility, and restarts OpenLDAP. The db\_recover reads the transaction logs and ensures that any uncommitted data is properly synchronized. This allows EMPS to startup properly even if the OpenLDAP data became corrupt because of improper shutdown.

The results of the recovery operation are contained in the <CN\_INSTALL>\logs\EMPS\_OpenLDAPRecover.log file.

### Manual Backup and Recovery

If data corruption is not recovered using the db\_recover utility, and WatchDog on EMPS does not start, perform the following:

- ♦ Schedule a task that runs the `<CN_INSTALL>\openldap\OpenldapDataBackupUtil.bat` file three to four times a day.

This file runs `slapcat` to enable backup of the OpenLDAP database, and creates an `ldif` file (with timestamp) in the `<CN_INSTALL>\openldap\backupData\` folder.

It also cleans any files that are older than seven days.

The above step must be executed regularly to avoid data corruption.

If WatchDog does not start on EMPS because of an improper shutdown, or if auto-recovery failed to recover the OpenLDAP data, you must rebuild the LDAP database from the last `ldif` file using the following steps:

1. Create a copy of the `<CN_INSTALL>\openldap\data\genesys\` directory.
2. Delete all the contents of the `<CN_INSTALL>\openldap\data\genesys\` directory.
3. Run `<CN_INSTALL>\openldap\slapadd -l <ldif_file>`.
4. Start OpenLDAP.

These steps restore the database to the last backed up state; however, you will lose the transactions since this last backup.



## Chapter

# 2

## Bulk Provisioning Tool

This chapter describes how to use the Bulk Provisioning Tool (BPT). It contains the following sections:

- [Overview, page 93](#)
- [Accessing the BPT, page 94](#)
- [Bulk Operations, page 95](#)
- [Progress Bar and Log Window, page 99](#)
- [Canceling a Bulk Task, page 100](#)
- [Log and Audit Files, page 101](#)
- [BPT Configuration, page 102](#)
- [CSV Mapping, page 102](#)

---

## Overview

You can use the Bulk Provisioning Tool (BPT) to create, regenerate, and reprovision IVR profiles in bulk.

The BPT performs the following functions:

- Collects and validates your input, and then passes it to the Element Management Provisioning System (EMPS) server for processing.
- Communicates with the EMPS server by using HTTP web notifications.
- Displays the results of the actions.

---

**Note:** You can still make changes to IVR profiles through the EMPS graphical user interface (GUI), even when the BPT tasks are in progress. However, to avoid unpredictable results, Genesys recommends that you not make changes to the same IVR profile through the BPT and EMPS simultaneously.

---

---

# Accessing the BPT

1. On the server where you installed the BPT, go to `C:\BPT\bin`.

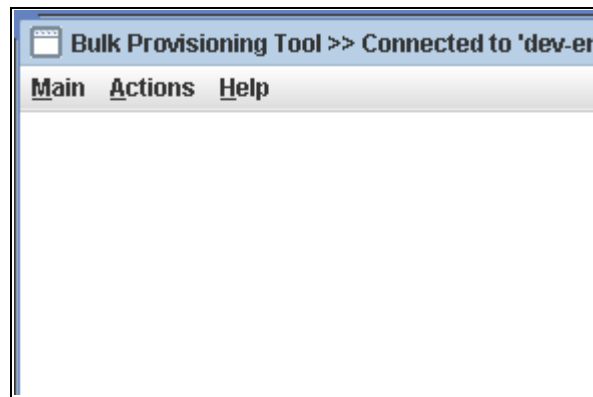
---

Note: The `C:\BPT\bin` is the default installation location. If you did not install it in this location, then navigate to where you installed the BPT.

---

2. Double-click `run_bpt.bat`.
3. On the Login screen, enter the following information to connect to the EMPS server, and then click **Connect**.
  - User Name—The EMPS user name—for example, Admin.
  - Password—The EMPS password, typically password.
  - EMPS Host Name—The EMPS fully qualified domain name or IP address—for example, `emps-hostname.yourcompany.com`

The BPT main screen appears (see [Figure 35](#)).



**Figure 35: Bulk Provisioning Tool Main Screen**

## Main Menu

The Main menu contains the following commands:

- Connect—Opens the Login screen, from which you can connect to the EMPS server.
- Disconnect—Disconnects the session from the EMPS server.
- Exit—Ends the session and closes the BPT application.

### Actions Menu

The Actions menu contains the following commands:

- Applications
  - Swap IVR URLs—Swaps primary and backup IVR URLs for multiple IVR profiles, and regenerates them.
  - Create New Applications—Creates multiple IVR profiles.
- DIDs
  - Regenerate DID Groups—Generates did.xml files for one or more DID groups.

### Help Menu

The Help menu contains the following commands:

- About—Displays the version of the BPT.

---

## Bulk Operations

You can perform the following bulk operations on existing IVR profiles:

- Swap IVR URLs
- Create New Applications

You can perform the following bulk operation on existing DIDs:

- Regenerate DID Groups

### Swap IVR URLs

The BPT enables you to swap the values between the primary IVR URL and the backup IVR URL for multiple IVR profiles, and then regenerate the IVR profiles.

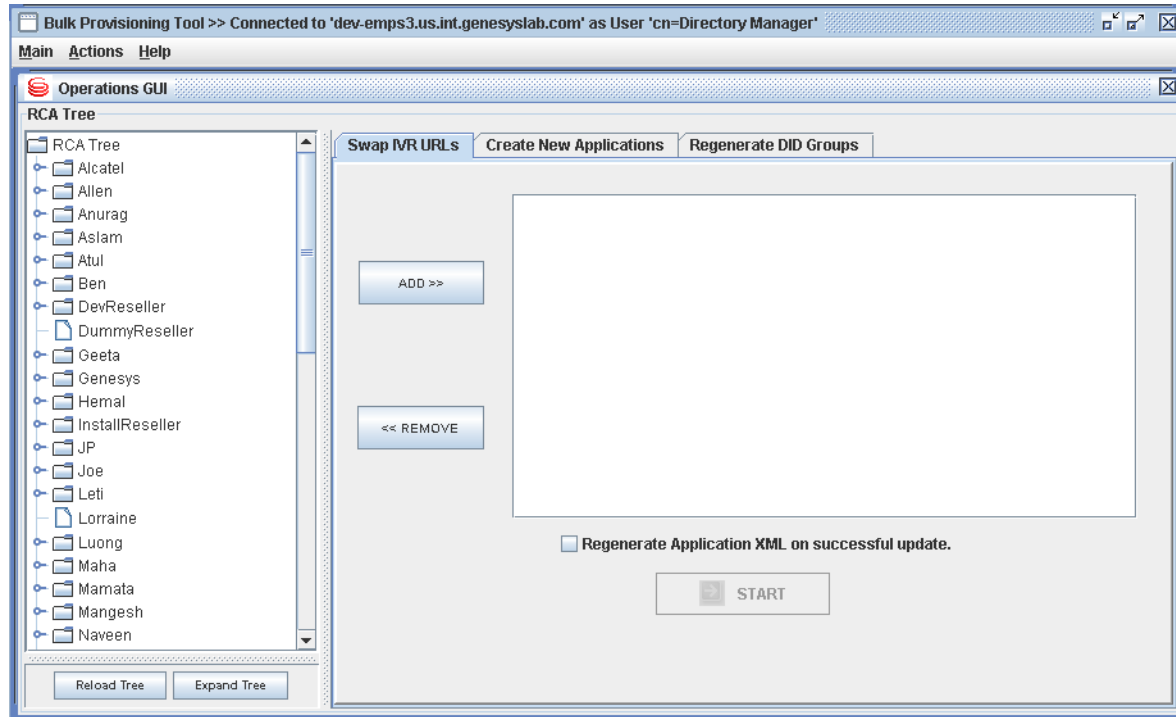
To swap the primary and backup IVR URLs:

1. From the Actions drop-down menu, select Applications > Swap IVR URLs. The Operations GUI opens (see Figure 36 on [page 96](#)).

---

Note: Alternatively, if the Operations GUI is already open, you can click the Swap IVR URLs tab on the main pane.

---



**Figure 36: Operations GUI—Swap IVR URLs Tab**

- From the RCA (Resellers, Customers, Applications) Tree on the left pane, select the desired IVR profiles, and then click ADD.

---

Note: Selecting a customer and clicking ADD will add all of the IVR profiles under that customer. You can also select multiple customers.

---

- To regenerate the IVR profiles after the update, select the Regenerate Application XML on successful update check box.
- Click Start.

If you did not select the Regenerate Application XML on successful update check box, a warning message appears asking for confirmation.

The BPT proceeds to swap the primary and backup IVR URLs. While it is swapping the URLs, if an IVR profile has no value for the backup URL, a warning message appears, asking you to confirm the swapping. Click Yes to continue with swapping process, or click No to skip the swapping for that IVR profile.

A status message also displays during the task and after the completion of the task (see “Progress Bar and Log Window” on [page 99](#)).



## Create New Applications

The BPT enables you to quickly create multiple IVR profiles. This option is useful when you are creating many IVR profiles that have similar attributes.

To create new IVR profiles:

1. Open the `Sample CSV.csv` file that is included with the BPT. The file is located in the `<install_directory>\Data` folder.

By using this sample file as a baseline, you can create your own `.csv` file with the desired values for your IVR profiles. The column headers in the `.csv` file map to the EMPS GUI parameters for creating and provisioning IVR profiles (see Table 2 on [page 103](#)).

2. Create line entries in the sample file. Each line entry represents an IVR profile.

---

Note: By default, the `.csv` file is restricted to 100 lines of IVR profile details.

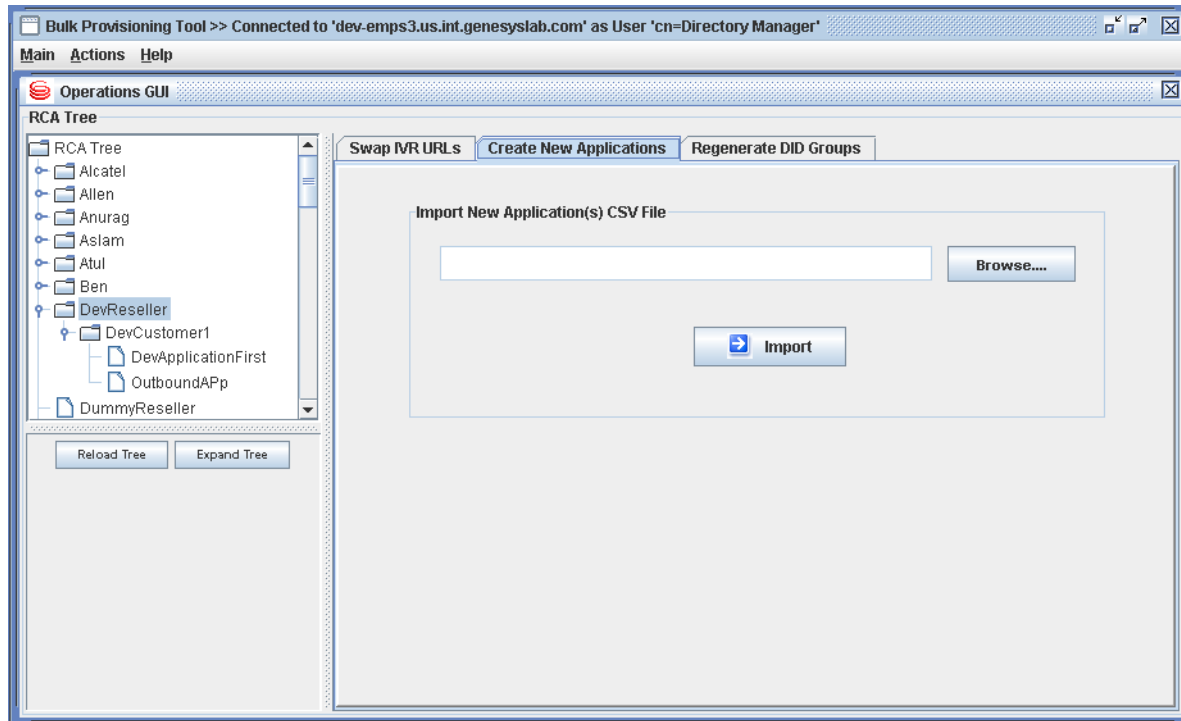
---

3. Save the `.csv` file with a new name.
4. On the BPT GUI, from the **Actions** drop-down menu, select **Applications > Create New Applications**. The Operations GUI opens (see Figure 37 on [page 98](#)).

---

Note: Alternatively, if the Operations GUI is already open, you can click the **Create New Applications** tab on the main pane.

---



**Figure 37: Create New Applications Dialog Box**

5. Click **Browse** and select your newly created .csv file.
6. Click **Import**. The BPT proceeds to create the IVR profiles.  
A status message displays during the task and after the completion of the task (see “Progress Bar and Log Window” on [page 99](#)).
7. When the task has completed successfully, click **Reload Tree** on the left pane to see your newly created IVR profiles.

## Regenerate DID Groups

The BPT enables you to regenerate `did.xml` files for one or more DID groups.

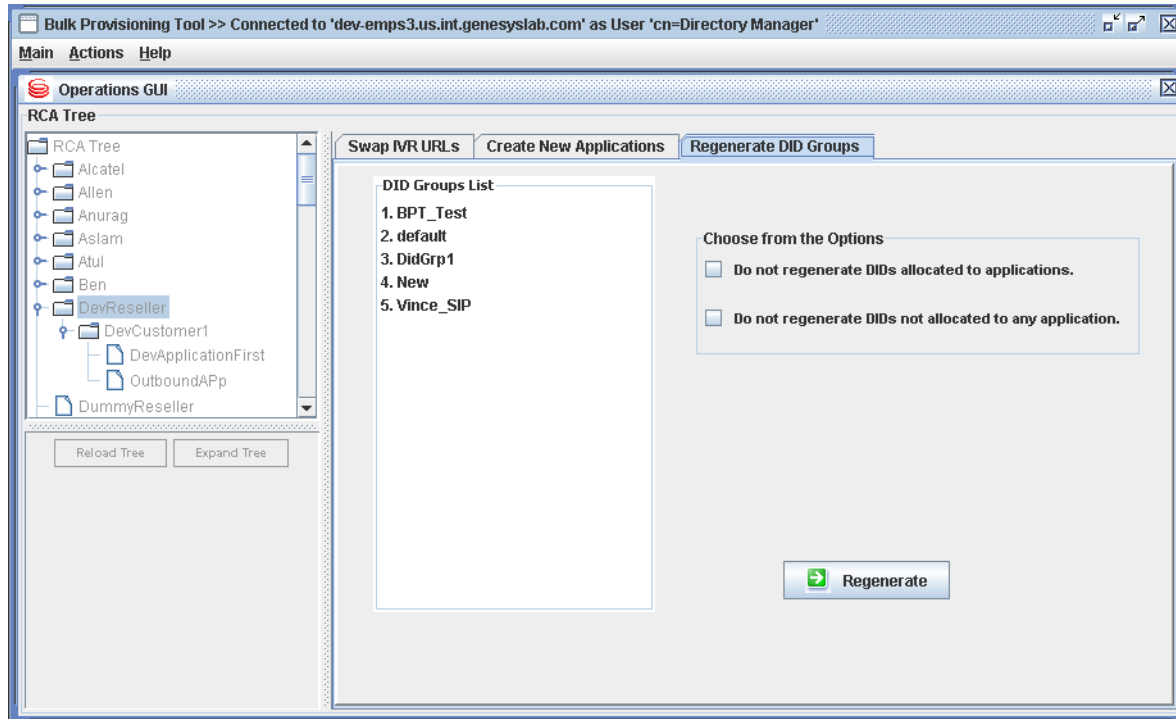
To regenerate DID groups:

1. From the **Actions** drop-down menu, select **DIDs > Regenerate DID Groups**. The Operations GUI opens (see Figure 38 on [page 99](#)).

---

**Note:** Alternatively, if the Operations GUI is already open, you can click the **Regenerate DID Groups** tab on the main pane.

---



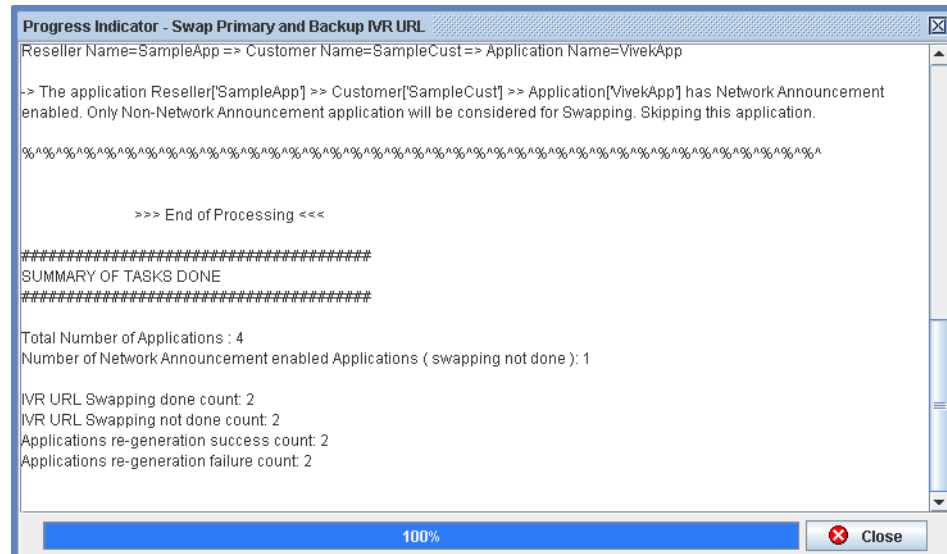
**Figure 38: Regenerate DID Groups Dialog Box**

2. From the DID Groups List, select the DID group(s).
3. (Optional) Select one of the following check boxes:
  - Do not regenerate DIDs allocated to applications
  - Do not regenerate DIDs not allocated to any application
4. Click Regenerate.

A status message displays during the task and after the completion of the task (see “Progress Bar and Log Window” on [page 99](#)).

## Progress Bar and Log Window

Bulk tasks can take a long time to complete. The BPT provides you with continuous feedback on the status of the operation. The BPT GUI remains responsive throughout the operation as processing is performed on one or more worker threads. The GUI provides feedback in the form of an onscreen progress bar, and a log window in which log messages are displayed (see [Figure 39 on page 100](#)).



**Figure 39: Sample Progress Bar and Log Pane**

### Progress Bar

The GUI displays a progress bar when an operation is in progress. The progress bar indicates the status of the operation.

## Scrolling Log Pane

The GUI displays a scrolling log pane that indicates the status of the operations. This scrolling log pane also indicates the success or failure of the operation, as well as the reason/error message in the event of failure.

The following is a sample status message for regenerating IVR profiles:

```
[ Timestamp ] Sending application regeneration request to EMPS Server [
    <EMPS_HOST_NAME> ]
[ Timestamp ] Request accepted by EMPS Server
[ Timestamp ] Application regeneration started
[ Timestamp ] Processing request #1 - Application Name: <Application_Name>
[ Timestamp ] Processing request #2 - Application Name: <Application_Name>
[ Timestamp ] Application Re-generation completed
[ Timestamp ] Purging the older cache from the cache server
[ Timestamp ] Deploying the files
[ Timestamp ] Totally 2 applications were regenerated successfully
```

## Canceling a Bulk Task

After a bulk provisioning operation has started, you can gracefully cancel the task by clicking **Abort**. The **Abort** button appears at the bottom of the BPT GUI, next to the **Start** button.

After clicking **Abort**, an alert prompts you to confirm. Upon confirmation, all of the tasks that were pending will be cancelled. The changes that were already successfully made will not be rolled back.

Since this is a graceful cancellation, the operation that is in progress will be completed, and then the cancellation will occur.

### Example

1. You start a bulk Swap IVR URLs operation for 50 IVR profiles, with the Regenerate Application XML on successful update check box selected.
2. When the operation is in progress on the fifteenth IVR profile, you click **Abort**.
3. The operation is cancelled after the completion of the fifteenth IVR profile.
4. The completion of the fifteenth IVR profile also included the regeneration of the IVR profiles.
5. The BPT provides you with a status message, indicating how many IVR profiles were processed successfully and how many were cancelled.

---

## Log and Audit Files

The BPT creates a detailed log file and audit file, which record the events or exceptions that have occurred. Both the log and audit files roll over to a new file when they reach 256 KB.

---

**Note:** The 256 KB limit is the default value. You can configure a different limit through the BPT property file.

---

These files have the following characteristics:

- The text log file logs all of the events and errors that occur during the operations of the BPT.
- The audit file contains the summary of the BPT process.
- The log and audit files are located in the <Install\_Directory>\Log folder.
- The log file is named `BPT_Detail.log`, and the audit file is named `BPT_AuditFile.log`.

---

**Note:** You can configure the names of the log files through the BPT property file.

---

- If the rollover has occurred, the current file is renamed to `<LOG_FILE_NAME>_<CURRENT_DATE>_<INDEX>.log`. The value of <index> keeps incrementing, based on the number of rollover files.

The following is a sample log file:

```

1 [2006/08/16 09:04:10.859] <<< DebugLog Start, maxsize=262144 >>>
2 [2006/08/16 09:04:10.843] User <USER_NAME> logged in from <IP>
3 [2006/08/16 09:04:10.843] app_regenerate
4 [2006/08/16 09:04:10.843] success
5 [2006/08/16 09:04:12.750] app_url_swap
6 [2006/08/16 09:04:12.843] failed

```

The log file contains:

- A timestamp with the format YYYY/MM/DD HH:MM:SS.MS.
- The user name of the logged-in user and the machine IP, which are logged only at the time of login.
- Descriptions of the operation being performed.
- The results (success or failure) of the operation.
- Descriptions of the errors or exceptions that are caught, if there are any.

---

## BPT Configuration

The `BPT.properties` file is a configuration file for the BPT application, and it is located in the `<Install_Dir>\config\` directory. Using this file, you can change some of the configuration values to meet your requirements. Some values that can be changed in this file are:

### Logging Details

- Enable or disable the creation of log files.
- Log file names.
- Log file size.

### EMPS Server Details

- EMPS Host Name.
- EMPS User Name.
- EMPS Password.

When you set these EMPS details, they automatically appear on the Login screen.

---

## CSV Mapping

You can use `.csv` files to conveniently create multiple IVR profiles (previously referred to as applications in EMPS) through BPT. The sample `.csv` file, found in `C:\BPT\data\Sample CSV.csv`, includes headers in the first row, each of

which is a property of the IVR profile. [Table 2](#) provides the property and its corresponding display name in the IVR profile editing and provisioning GUI of EMPS.

You can add new rows to the .csv file to create additional IVR profiles. You can copy-paste rows, edit their values as desired, and then run BPT to quickly create the new IVR profiles in EMPS.

---

Note: Do not modify the top header row.

---

**Table 2: CSV Mapping**

Column Header in Sample .csv File	Parameter in EMPS GUI
reseller	Reseller Name
customer	Customer Name
application	Application Name
applicationtype	Application Type
description	Description
networkannouncement	Network Announcement
notes	Comments
previousresponsibleorganization	Previous Responsible Organization
responsibleorganization	Responsible Organization
status	Reporting Description
tfn	Toll Free Number
rule1	Application Rule 1
rule2	Application Rule 2
applanguage	Default Language
applicationdrivenby	Application Driven by
apprule1	Application Rule 1
apprule2	Application Rule 2
asrenabled	ASR Enabled
asrvendor	ASR Vendor

**Table 2: CSV Mapping (Continued)**

Column Header in Sample .csv File	Parameter in EMPS GUI
backupivrurl	Backup IVR URL
bwmachine	BWM Machine
bwmurl	BWM URL
ccxmlcontrolled	CCXML Controlled
ccxmlversion	CCXML Version
confirmqadapter	Confirm QAdapter
contactcallcenter	Contact Call Router
cpatimeout	CPA Timeout
cqaserviceid	CQA Service ID
customerani	Customer ANI
defaulttroutenumber	Default Route Number
dialoutnumber	Dial Out Number
dialplan	International Dialing
enableasrlogging	Enable ASR Logging
enabledebugging	Enable Debugging
enableqadapter	Enable QAdapter
enabletransfer	Enable Transfer
enabletransferconnect	Enable Transfer Connect
ivr1rootdir	Primary IVR - Root Dir
ivr1starturl	Primary IVR - Start IVR URL
ivr1url	Primary IVR URL
ivr2rootdir	Backup IVR - Root Dir
ivr2url	Backup IVR - URL
ivrfailureurl	IVR Failure URL
ivrtimeout	IVR Timeout (sec)



**Table 2: CSV Mapping (Continued)**

Column Header in Sample .csv File	Parameter in EMPS GUI
ivrtype	IVR Type
maxports	Maximum Ports
npbadxmlpageexceptionurl	Bad XML Page Exception URL
npcalltraceexceptionurl	Call Trace Exception URL
npdebugexceptionurl	Debug Exception URL
nptrapexceptionurl	Trap Exception URL
numasrsamples	Number of ASR Samples
obnactive	Enable OBN
obnfailureurl	Failure URL
obngroups	OBN Groups
obnmaxqueuesize	Max Queue Size
obnservers	OBN Servers
portalapplication	Portal Application
portalbadxmlpageurlhook	Bad XML Page Hook
portalcallerhupurlhook	Caller HUP Hook
portalcalltraceurlhook	Call Trace Hook
portaldebugurlhook	Debug Hook
portalotherurlhook	Other Exception Hook
portaltrapurlhook	Trap Hook
primaryccxmlurl	CCXML URL
primaryivrurl	Primary IVR URL
primaryorlgrp	Primary ORL Group
processicmlabel	Process ICM Label URL
qadapterlocation	QAdapter Location
qadaptername	QAdapterName

**Table 2: CSV Mapping (Continued)**

Column Header in Sample .csv File	Parameter in EMPS GUI
qadapterscriptname	QAdapter Script Name
reclaimcode	Reclaim Code (ATT only)
retransfertype	Retransfer Type
rule2	Application Rule2
secondaryorlgrp	Secondary ORL Group
transferconnectscript	TransferConnect Script
transferoption	Transfer Option
transferoptionlist	Transfer Option
transferoptionother	Transfer Option (other)
transfertype	Transfer Type
ttsenabled	TTS Enabled
ttsformat	TTS Output Format
ttsgender	TTS Gender
ttstimeout	TTS Timeout (sec)
ttsvendor	TTS Vendor
xmlpagerecording	XML Page Recording
xmlsetname1	XMLSetName1
xmlsetname10	XMLSetName10
xmlsetname2	XMLSetName2
xmlsetname3	XMLSetName3
xmlsetname4	XMLSetName4
xmlsetname5	XMLSetName5
xmlsetname6	XMLSetName6
xmlsetname7	XMLSetName7
xmlsetname8	XMLSetName8

**Table 2: CSV Mapping (Continued)**

Column Header in Sample .csv File	Parameter in EMPS GUI
xmlsetname9	XMLSetName9
xmlsetvalue1	XMLSetValue1
xmlsetvalue10	XMLSetValue10
xmlsetvalue2	XMLSetValue2
xmlsetvalue3	XMLSetValue3
xmlsetvalue4	XMLSetValue4
xmlsetvalue5	XMLSetValue5
xmlsetvalue6	XMLSetValue6
xmlsetvalue7	XMLSetValue7
xmlsetvalue8	XMLSetValue8
xmlsetvalue9	XMLSetValue9
didslst	List of DIDs





## Chapter

# 3

## Bulk DID Operations Tool

This chapter describes how to use the Bulk DID Operations Tool (BDOT). It contains the following sections:

- [Overview, page 109](#)
- [The BDOT, page 110](#)
- [BDOT Error Checking, page 112](#)

---

### Overview

The Bulk DID Operations Tool (BDOT) provides the functionality to perform bulk operations in the Genesys Voice Platform (GVP) 7.6.4 Element Management Provisioning System (EMPS) on a large number of DID numbers (also called DIDs). The DIDs must be listed in a comma separated (CSV) file available for input. The BDOT performs the following operations:

- **Add**—Adds all the DIDs specified in the CSV file unless they already exist.
- **Move**—Changes DID group of all DIDs in input CSV file.
- **Delete**—Deletes all of the DIDs specified in the CSV file.

---

**Notes:** You must have the GVP 7.6.4 MR6(or later) version of EMPS with SunOne LDAP installed and running before you can use the BDOT.

The BDOT uses the `bulkDIDOperation.php` page along with enhancements in the backend EMPS Self Provisioning Server (SPS) to provide the required functionality.

---

---

# The BDOT

The following section lists the pre-requisites, and describes the BDOT operations.

## Pre-requisites

The following are pre-requisites for running Bulk DID Operations Tool:

- The `bulkDIDoperation.php` file must exist in the `<install_dir>\cn\web\spm` folder on the EMPS host. This will automatically be installed after the latest version of EMPS is installed.
- The CSV file containing the list of DIDs can be present in the `<install_dir>\cn\config` folder on the EMPS host. You can also store the file in any directory on the EMPS host as long as the correct path is specified (for example, `c:\temp\sample.csv`) in the Internet Explorer browser. This file must be created using either Excel or TextPad, and list only one DID in each row.

---

Note: If you are using Excel to create the DIDs list, make sure the file is saved with the `.csv` file extension, and not the `.xls` file extension.

---

- Internet Explorer version 6 or later must be installed on the EMPS host. Internet Explorer is used to invoke the PHP script.
- The `max_execution_time` (the PHP timeout) found in the `<install_dir>\cn\bin\PHP\php.ini` file, must be changed from the default value of 30 seconds to 300 seconds.

The success or failure of the operations are returned in the response of the PHP page; however, the details of the operations are logged in the `<install_dir>\cn\log\sps.log` file.

## BDOT Operations

The following section describes how to invoke the Add, Move and Delete operations using the Bulk DID Operations Tool.

---

Note: If no file path is specified, the CSV file will be opened from the default `<CN_INSTALL>/config` folder.

---

### Add DIDs Request

The Add operation adds all the DIDs from the DIDs listed in CSV file to the specified DID group. If the listed DIDs already exist in the GVP system, a warning message is written to the SPS log file.

To add the DIDs:

- In an Internet Explorer browser, type:  
`http://<emps-host-name>:9810/spm/  
 bulkDIDOperation.php?csvfile=<new_dids>.csv&operation=add&didgroup=  
 <addidgroup>`  
 Or, if the CSV file is in a folder other than the <CN\_INSTALL>/config folder,  
 type:  
`http://<emps-host-name>:9810/spm/  
 bulkDIDOperation.php?csvfile=<full_file_path>/<new_dids>.csv&operat  
 ion=add&didgroup=<addidgroup>`

### Move DIDs Request

The Move operation assigns all the DIDs listed in the CSV file to the specified DID group. If the listed DIDs already exist in GVP in another DID Group they are deleted from that DID group.

- In an Internet Explorer browser, type:  
`http://<emps-host-name>:9810/spm/  
 bulkDIDOperation.php?csvfile=<move_DIDs>.csv&operation=move&didgroup  
 p=<movedidgroup>`  
 Or, if the CSV file is in a folder other than the <CN\_INSTALL>/config folder,  
 type:  
`http://<emps-host-  
 name>:9810/spm/bulkDIDOperation.php?csvfile=<full_file_path>/<move_  
 DIDs>.csv&operation=move&didgroup=<movedidgroup>`

### Delete DIDs Request

The Delete operation deletes all the DIDs from GVP that are specified in the DID list. The SPS log file will indicate which DIDs were successfully deleted, and which DIDs failed to delete.

- In an Internet Explorer browser, type:  
`http://<emps-host-name>:9810/spm/  
 bulkDIDOperation.php?csvfile=<delete_DIDs>.csv&operation=delete`  
 Or, if the CSV file is in a folder other than the <CN\_INSTALL>/config folder,  
 type:  
`http://<emps-host-name>:9810/spm/  
 bulkDIDOperation.php?c:svfile=<full_file_path>/<delete_DIDs>.csv&op  
 eration=delete`

---

**Note:** The maximum number of DIDs that each operation can handle is 3000. However, Genesys recommends that no more than 1000 DIDs be listed in the CSV file.

---

## Logging

The BDOT writes entries in the SPS log files on the EMPS host. These entries are identified by the `processBulkDIDOperation` string in the file. For example, `[2009/06/11 19:29:54.191] FAC cnDIDGroup.cpp:1083 C=76:L=2:U=0 processBulkDIDOperation >> Insert DID(1234) failed as it already exists in the group(test), will skip this row.`

The `processBulkDIDOperation` string in each line is useful when extracting output of the Bulk DID Operations Tool for debugging.

---

## BDOT Error Checking

The Bulk DID Operations Tool does the following error checking:

- The `bulkDIDOperation.php` page verifies that the `csvfile` and `operation` parameters are present. If these parameters are not available, an error message prompting you to supply these parameters is displayed.
- If the `csvfile` and `operation` parameters are present without values, an error message prompting you to supply values for these parameters is displayed.
- If the value of the `csvfile` is specified as something other than the default `<install_dir>\cn\config` directory, and that file does not exist, an error message is written to the SPS log file, and an error message is displayed.
- When invoking the Add or Move operation, the `bulkDIDOperation.php` page verifies that the `didgroup` parameter and its value are present. If either of them are missing, an error message prompting you to supply the `didgroup` and its value is displayed.
- If the CSV file is empty, an error message is written to the SPS log file, and an error message is displayed.
- When adding a DID, the Add operation checks to see if the DID already exists in GVP. If the DID does exist, an error message containing the DID and its DID group is written to the SPS log file. The DIDs are read one by one from the list until the end of the list is reached.

When all of the DIDs in the list are read, the Add operation checks to see if any of these DIDs already exist in EMPS/LDAP. If any of these DIDs exist, a partial success message is displayed. If these DIDs do not already exist, a successful message is displayed.

The SPS log file summarizes the total number of DIDs that were successfully added to GVP, and the DIDs that were not successfully added to GVP.

- If the CSV file contains any rows with value of 0, an error message is displayed. Also, an error message is written to the SPS log file indicating that there were 0 values found in the CSV file, and that no DIDs were processed.



- The `bulkDIDOperation.php` page checks that the backend SPS process is running. If it not running, an error is displayed.
- Change the default PHP page timeout (socket connection timeout) from 60 seconds to 300 seconds. This enables the response from the processing of the BDOT operation to be same as the value as the `max_execution_time` parameter that is configured in the `php.ini` file.





## Chapter

# 4 Login Server

This chapter introduces the Login Server and describes the functions of the Login Administration module. It also describes the Web-based services that your customers can access through this server.

This chapter has these sections:

- [Login Server, page 115](#)
- [Login Server Administration, page 117](#)
- [Call Status Monitor, page 131](#)
- [Automatic Speech Recognition Log Server, page 133](#)
- [Reporter, page 133](#)
- [Customizing the Interface, page 138](#)

---

## Login Server

The Login Server provides a single authentication point through which users can access Genesys Voice Platform (GVP) services. The level of information these users can access is determined by their authorizations, which you, as the network operator (or someone else in your enterprise identified as System Administrator), must set through the Administration module. You will also use this module to create and manage services and users.

Before a reseller and customer can use the Login Server, you must add them to the Element Management Provisioning System (EMPS). These tasks were covered in Chapter 1, “Element Management Provisioning System,” on [page 25](#).

## Passwords

By default, a user called *administrator*, with a password *administrator*, is automatically created when you configure the Login Server. You can reset the password whenever you wish.

To set the administrator user (for GVP Solaris):

1. Open an sqlplus session and connect to the database server as unifiedlogin user.
2. If the EMPS and Unified Login schemas are on the same Oracle instance:  
Execute the setadminuser procedure:  
`<unifiedlogin schema name>.setadminuser('<EMPS schema name>');`
3. If the EMPS and Unified Login schemas are on different Oracle instances/servers:
  - a. Obtain the administrative customer\_id from EMPS.
  - b. Update the UL\_USERS table with Admin Customer ID information. The default k\_users value for the administrator is 1. Use the following sqlplus command:  
`update ul_users set customer_id=<ADMIN_CUST_ID> where k_users=1;`
  - c. Commit the transaction by executing the following command:  
`commit;`

To set the administrator user (for GVP Windows):

1. Open an MS SQL Query Analyzer and connect to the UnifiedLogin database as unifiedlogin/unifiedlogin user.
2. If the EMPS and Unified Login databases are on the same server:  
Execute the setadminuser procedure:  
`exec setadminuser '<EMPS Database name>'`
3. If the EMPS and Unified Login databases are on different servers:
  - a. Obtain the administrative customer\_id from EMPS.
  - b. Update the UL\_USERS table with Admin Customer ID information. The default k\_users value for the administrator is 1. Use the following sqlplus command:  
`update ul_users set customer_id=<ADMIN_CUST_ID> where k_users=1`

To reset the password:

1. Login to Unified Login.
2. Select the Change Password link.

## Accessing the Login Server

1. Open a web browser on any client computer.
2. Enter `http://<FQDN of EMPS Machine>:9810/gvpportal` in the address bar. The Portal GUI opens. Click the link under Unified Login.

OR

Enter `http://<servername.domainname>/unifiedlogin` in the address bar.

---

**Note:** The software that serves web browser requests (for example, LoginServer) is in the physical directory called `extweb`. By default, during installation, the web directory for accessing this software (on the Web) is specified as `extweb`.

For GVP Solaris, the web directory name can be modified (to LoginServer) by modifying the `apache.conf` file under the Apache directory, without renaming the physical directory. Consult Apache documentation for help about accomplishing this task.

For GVP Windows, the web directory name can be modified (to LoginServer) by using the IIS Administration tool, without renaming the physical directory. Consult Microsoft documentation for help about accomplishing this task.

---

3. Enter a valid login name, customer name (in a multi-tenant environment only), and password in the appropriate text boxes.
4. (Optional) Save your login information, so the next time you log in, only your password is required:
  - In a single tenant environment, select the `Save User Name Info on my Computer for future login` check box.
  - In a multi-tenant environment, select the `Save User Name and Customer Info on my Computer`.

---

**Note:** For security reasons, the user name and company name settings are saved on the client for one week only, so you must reenter the data once per week.

---

5. Click `Login`. Upon successful login, the Web Services page displays a list of the services to which a customer has access.

The level of service access depends on the user privileges that are granted during login. You must configure those privileges through the Administration module. Access the `Administration` section, which provides links for additional account information and changing passwords, under `User Options`.

---

## Login Server Administration

Use the Login Server Administration module to:

- Create and manage users.
- Associate roles to services.
- Create and modify service types.
- Create and modify services.
- Create and modify roles.

- Authorize user roles for each service.
- Set passwords.

In the Administration module, a red asterisk (\*) beside a field indicates that the information is required. If no asterisk is displayed, the information is optional.

---

Note: Genesys recommends that you tightly restrict Administration access because any misuse can compromise data security.

---

When you start Login Server Administration, the Create New User page opens, (see [Figure 40](#)). Note that, in a single-tenant environment, the Customer field does not appear on this page.

**Figure 40: Create New User Page—Multi-Tenant**

The left frame of any Login Administration, page lists the following options:

- **User Administration**
  - Create New User
  - Manage Users
- **Service Administration**
  - Create New Service
  - Modify Service
- **Advanced Options**

## User Roles

Part of administering users and services in Login Server Administration is the assignment of roles. A *role* is a grouping of privileges. In a multi-tenant environment, there are seven roles defined by default:

- **Customer Admin**—Manages all voice applications for the customer.
- **Customer User**—Views all voice applications for the customer.
- **NSP Admin**—Manages all resellers, customers, voice applications, and server data.
- **NSP User**—Views all resellers, customers, voice applications, and server data.
- **Reseller Admin**—Manages all customers and voice applications for the reseller.
- **Reseller User**—Views all customers and voice applications for the reseller.
- **Super Admin**—Manages Login Server users and services.

In a single tenant Environment, there are only two roles defined by default:

- **Enterprise Admin**—Manages Login Server users and services, and views all voice applications and services for the enterprise.
- **Enterprise User**—Views all voice applications for the enterprise.

You can create additional roles as required (see “To create a new role:” on [page 127](#)).

## User Administration

Users are authorized to access specific services that are set up for the enterprise in a single tenant environment or for individual customers in a multi-tenant environment. You must create users for each enterprise or customer.

To create a new user:

1. Log in to the Login GUI as the Administrator.
2. Click **Login Administration**, which opens the **Create New User** page (see [Figure 40 on page 118](#)).
3. If you are in a multi-tenant environment, select the customer to which the user belongs from the drop-down list.
4. Enter a login name and a password in the corresponding fields.
5. (Optional) Enter contact information.
6. Click **Submit** to save the new user. The **Authorize Users** page opens, displaying:
  - Types of services available in Login Server
  - Services available in Login Server

- Roles eligible for assignment to the service.

See Figure 41 on [page 120](#).

Note: The **Authorize Users** page for a single-tenant environment is identical to that shown in [Figure 41](#), except that single-tenant roles are listed in the **Roles** column, and the **Customer** field is not displayed.

## Authorize Users

**Customer** telera

**User** administrator

Choose Services below and then assign roles for the Service.  
For a brief description of role capabilities for the Service, place your mouse pointer on the radio/checkbox of the corresponding role

Service Type	Select Services	Assign Roles
Unified Login Administration	<input checked="" type="checkbox"/> Administration	<input checked="" type="checkbox"/> Super Admin
Call Status Monitor	<input checked="" type="checkbox"/> Network Call Status Monitor	<input type="radio"/> Customer User <input checked="" type="radio"/> NSP User <input type="radio"/> Reseller User
ASR Log Manager	<input type="checkbox"/> ASR Files Download	
Historical Reports	<input checked="" type="checkbox"/> Network Reports	<input type="radio"/> Customer User <input checked="" type="radio"/> NSP User <input type="radio"/> Reseller User

**Figure 41: Authorize Users Page—Multi-Tenant**

7. Assign appropriate authorizations to this user:
  - a. Select the desired **Select Services** check box, which displays the corresponding roles.



---

Note: For a brief description of role capabilities for a service, place your mouse pointer on the radio button or check box of the corresponding role.

---

- b.** Assign the role for the service. The roles available for each service type vary, depending on whether you are in a single-tenant or multi-tenant environment.

---

Note: A database administrator or equivalent person should create users and allocate roles.

---

- 8.** Click **Submit**.

To manage users:

- 1.** Log in to the Login GUI as the Administrator.
- 2.** Click **Login Administration**, which opens the **Create New User** page.
- 3.** Click **Manage Users**, which opens the **User Management** page containing one drop-down list.
- 4.** If you are in a multi-tenant environment, select the customer from the drop-down list. The **User Management** page reopens with a user selection drop-down list.
- 5.** Select the user from the drop-down list. The **User Management** page displays details about the user and that user's assigned roles (see Figure 42 on [page 122](#)).

---

Note: The **User Management** page for a single tenant is identical to that shown in Figure 42 on [page 122](#), except that single-tenant roles are listed in the **Roles** column, and the **Customer** field is not displayed.

---

### User Management

Customer

AnnCustomer1

User

ann

First Name

Last Name

E Mail

Phone

Modify Information

Authorize Services

Reset Password

Enabled Services	Assigned Roles
Network Call Status Monitor	Customer User
Network Reports	Customer User

**Figure 42: User Management Page with User Details—Multi-Tenant**

6. To modify or delete this user:
  - a. Click **Modify Information**.
  - b. Do one of the following:
    - Edit the user information as needed, and then click **Submit**.
    - Select **Delete this User Permanently**, click **Submit**, and then click **OK** to confirm the deletion.
  - c. Click **Back to Manage User**.
7. To authorize this user:
  - a. Click **Authorize Services**, which opens the **Authorize Users** page (see Figure 41 on [page 120](#)).
  - b. Select the desired **Select Services** check box, which displays the corresponding roles.

---

**Note:** For a brief description of role capabilities for a service, place your mouse pointer on the radio button or check box of the corresponding role.

---

- c. Assign the role for the service. The roles available for each service vary, depending on whether you are in a single-tenant or multi-tenant environment.

---

Note: A database administrator or equivalent person should create users and allocate roles.

---

- d. Click Submit.
  - e. Click Back to Manage User.
8. To reset the password for this user:
- a. Click Reset Password.
  - b. Enter the password in the field provided.
  - c. Click Submit.
  - d. Click Back to Manage User.

## Service Administration

The Login Server provides users with access to different services. That means you must create links to those services. The Login Server has three services packaged with the product that you can activate immediately.

During installation, one default instance of each service type (Administration, Network Call Status Monitor, Network Reports) is created. However, the URLs of these services are incorrect, and the Network Service Provider (NSP) must modify them using the Modify Service option.

If the NSP wants to add more Reporter and Call Status Monitor boxes, you must add new services. Make sure you use a different service ID for each service, and that you configure each service ID in the EMPS.

To create a new service:

1. Log in to the Login Server GUI as the Administrator.
2. Click Login Administration, which opens the Create a New User page.
3. Click Create New Service in the left frame, which opens the Create New Service page (see Figure 43 on [page 124](#)).

### Create New Service

**\*Service ID**   
(Notate this ID. Required for configuring the Service in VWPS)

**\*Service Type**

**\*Service Name**   
(For display in Administration Screens only. Use names that helps to distinguish between Services of same type)

**\*Service Display Name**   
(For display to Customers in Services Menu. Use names by which your customers know it)

**\*URL**   
(Public URL. Fully Qualified Name of the Server for external access)

**\*VPN URL**   
(Private URL. Fully Qualified Name of the Server for VPN access)

**Status**

**Figure 43: Create New Service Page**

4. Enter the required fields for that service, and select the service type from the drop-down list. The default service types are:
  - CONFIG—Unified Login Administration
  - CSM—Call Status Monitor
  - RPT—Historical Reports
5. In the Status field, select the status of the service, which should be one of the following:
  - Active—the service is available for access.
  - Disabled—the service is temporarily not available.
  - Obsolete—the service is no longer in use. A record is kept for archive purposes.
6. Click Submit. This step creates the service and the Service Name appears under the Web Services section when the appropriate user logs in.

To modify a service:

1. Log in to the Login GUI as the Administrator.
2. Click **Login Administration**, which opens the **Create New User** page.
3. Click **Modify Service** in the left frame.
4. From the **Service** drop-down list, select the required service and click **Search**. The **Modify Service** page opens.
5. Modify the fields as needed for that **Service Type**.
6. In the **Status** field, select the status of the service, which should be one of the following:
  - **Active**—the service is available for access.
  - **Disabled**—the service is temporarily not available.
  - **Obsolete**—the service is no longer in use. A record is kept for archive purposes.
7. Click **Submit**, which updates the service.

## Advanced Options

Use the **Advanced Options** page only when you must add custom services and create custom roles for the NSP. You do not have to configure these options when you use only the services that are packaged with the product. The **Advanced Options** page has the following links:

- **Create New Service Type**
- **Modify Service Type**
- **Create New Roles**
- **Modify Roles**
- **Associate Roles to Service Types**

---


**Warning!** Changing service type and role information might cause undesirable system behavior.

---

When you do require these options, use the following procedures.

To create a new service type:

1. Log in to the Login Server GUI as the Administrator.
2. Click **Login Administration**, which opens the **Create New User** page.
3. Click **Advanced Options**, which opens the **Advanced Options** menu page.
4. Click **Create New Service Type**, which opens the **Create New Service Types** page (see Figure 44 on [page 126](#)).



**Create New Service Types**

\*Service Type ID

\*Service Type Name

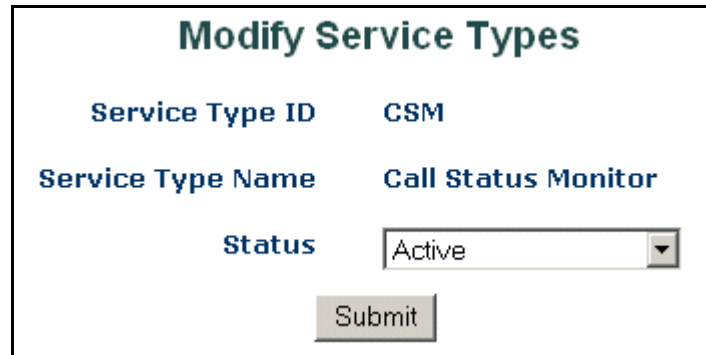
Status

**Figure 44: Create New Service Types Page**

5. Enter the Service Type ID and Name in the fields provided.
6. If you are in a multi-tenant environment, select the Supports Multiple Roles for One User check box.
7. Select the status of the service from the Status drop-down list, which should be one of the following:
  - Active—the service is available for access.
  - Disabled—the service is temporarily not available.
  - Obsolete—the service is no longer in use. A record is kept for archive purposes.
8. Click Submit.

To modify a service type:

1. Log in to the Login Server GUI as the Administrator.
2. Click Login Administration, which opens the Create New User page.
3. Click Advanced Options, which opens the Advanced Options menu page.
4. Click Modify Service, which opens the Modify Service Types page with a drop-down list of available service types.
5. From the Service drop-down list, select the required service and click Search. The Modify Service Types page reopens with details of the selected service type (see Figure 45 on [page 127](#)).



<b>Modify Service Types</b>	
<b>Service Type ID</b>	CSM
<b>Service Type Name</b>	Call Status Monitor
<b>Status</b>	Active
<input type="button" value="Submit"/>	

**Figure 45: Modify Service Types Page**

6. Make the required modifications.
7. Click **Submit**.

To create a new role:

1. Log in to the Login Server GUI as the Administrator.
2. Click **Login Administration**, which opens the **Create New User** page.
3. Click **Advanced Options**, which opens the **Advanced Options** menu page.
4. Click **Create New Roles**, which opens the **Create New Roles** page. This page displays a list of existing roles with the description and status of each (see Figure 46 on [page 128](#)).

---

**Note:** The **Create New Roles** page for a single-tenant environment is identical to that shown in Figure 46 on [page 128](#), except that single-tenant roles are listed in the **Roles** column.

---

### Create New Roles

Role	Description
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Role	Description	Status
<b>cadmin</b>	<b>Customer Admin</b>	<b>Active</b>
<b>cuser</b>	<b>Customer User</b>	<b>Active</b>
<b>nadmin</b>	<b>NSP Admin</b>	<b>Active</b>
<b>nuser</b>	<b>NSP User</b>	<b>Active</b>
<b>radmin</b>	<b>Reseller Admin</b>	<b>Active</b>
<b>ruser</b>	<b>Reseller User</b>	<b>Active</b>
<b>sadmin</b>	<b>Super Admin</b>	<b>Active</b>

**Figure 46: Create New Roles Page—Multi-Tenant**

5. Enter the name of the role in the **Role** field.
6. Enter a description of the role in the **Description** field.
7. Click **Submit**.

To modify a role:

1. Log in to the Login Server GUI as the Administrator.
2. Click **Login Administration**, which opens the **Create New User** page.
3. Click **Advanced Options**, which opens the **Advanced Options** menu page.
4. Click **Modify Roles**, which opens the **Modify Roles** page. This displays the description and status of existing roles (see Figure 47 on [page 129](#)).



Note: The Modify Roles page for a single-tenant environment is identical to that shown in Figure 47, except that single-tenant roles are listed in the Roles column.

Role	Description	Status
<b>cadmin</b>	Customer Admin	Active
<b>cuser</b>	Customer User	Active
<b>nadmin</b>	NSP Admin	Active
<b>nuser</b>	NSP User	Active
<b>radmin</b>	Reseller Admin	Active
<b>ruser</b>	Reseller User	Active
<b>sadmin</b>	Super Admin	Active

**Figure 47: Modify Roles Page—Multi-Tenant**

5. For the desired role, modify the description as needed, and select the status of the role from the Status drop-down list. The possible states of the role are:
  - Active—the service is available for access.
  - Disabled—the service is temporarily not available.
  - Obsolete—the service is no longer in use. A record is kept for archive purposes.
6. Click Submit.

## Associate Roles to Service Types

To associate a role to a service:

1. Log in to the Login Server GUI as the Administrator.
2. Click Login Administration, which opens the Create New User page.
3. Click Advanced Options, which opens the Advanced Options menu page.

4. Click **Associate Roles to Service Types**, which opens the **Associate Roles to Service Types** page containing one drop-down list.
5. From the **Service** drop-down list, select the required service. This action opens the **Associate Roles to Service Types** page for that service (see [Figure 48](#)).

---

Note: The **Associate Roles to Service Types** page for a multi-tenant environment is identical to that shown in [Figure 48](#), except that multi-tenant roles are listed in the **Select Roles** column.

---

**Associate Roles to Service Types**

**Service Type(short name)**    CSM

Select Roles	Description (authorization provided)
<input checked="" type="checkbox"/> <b>Enterprise Admin</b>	View all applications and Server data
<input checked="" type="checkbox"/> <b>Enterprise User</b>	View all applications

**Figure 48: Associate Roles to Service Types Page—Single Tenant**

6. In the **Select Roles** column, select the check box for the required role. [Table 3](#) displays the authorization required for each role.

**Table 3: Role Authorization**

Role	Administration	Reporter	Call Status Monitor
<b>Multi-Tenant Environment</b>			
Customer Admin	Not applicable	Not applicable	Not applicable
Customer User	Not applicable	View all voice applications for the customer.	View all voice applications for the customer.
NSP Admin	Not applicable	Not applicable	Not applicable

**Table 3: Role Authorization (Continued)**

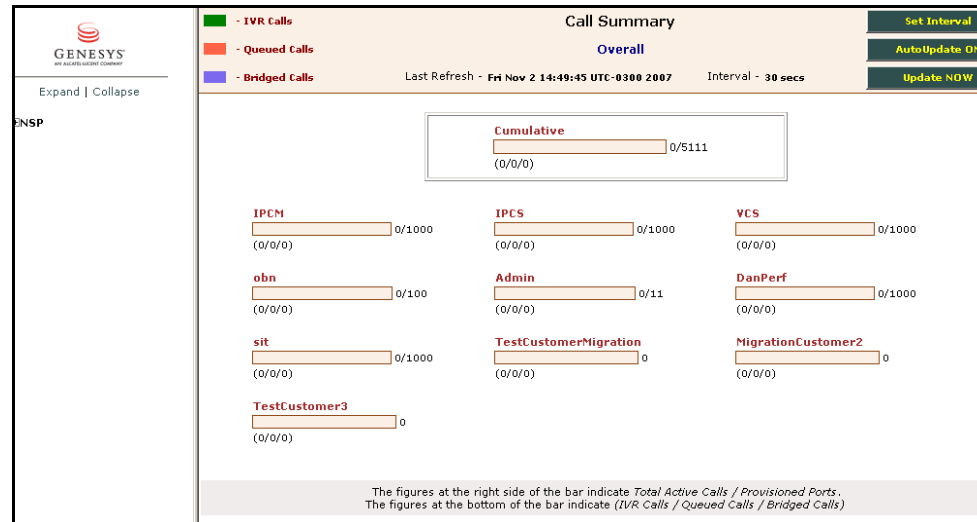
Role	Administration	Reporter	Call Status Monitor
NSP User	Not applicable	View all resellers, customers, voice applications, and server data.	View all resellers, customers, voice applications, and server data.
Reseller Admin	Not applicable	Not applicable	Not applicable
Reseller User	Not applicable	View all customers and voice applications for the reseller.	View all customers and voice applications for the reseller.
Super Admin	Manage Login Server users and services.	Not applicable	Not applicable
Single-Tenant Environment			
Enterprise Admin	Manage Login Server users and services.	View all voice applications and servers for the enterprise	View all voice applications and servers for the enterprise
Enterprise User	Not applicable	View all voice applications for the enterprise.	View all voice applications for the enterprise.

Note: Do not select roles that are not applicable. The service does not recognize them.

7. Click **Submit**.

## Call Status Monitor

The Call Status Monitor service displays real-time call-status reports about current calls. You access the Call Status Monitor GUI (see Figure 49 on [page 132](#)) through the Login Server by clicking **Real Time Reports**. The GUI has a left frame and a main frame.



**Figure 49: Call Status Monitor GUI—Single Tenant**

In a single-tenant environment, the left pane displays the following selections:

- **PM Connections**—Enterprise Admin users have the privilege to view this. Displays the status of the primary and backup Policy Managers in the network.
- **Overall**—The user can view the Current Active Calls Report for all the applications of the enterprise.

In a multi-tenant environment, the left pane displays the following selections:

- **PM Connections**—NSP users have the privilege to view this. Displays the status of the primary and backup Policy Managers in the network.
- **NSP**—Displays all resellers and customers. The NSP can view an Overall Call Summary Report for all resellers, customers, and their applications. The NSP can also view the Policy Manager Connection Status Report.
- **Reseller**—Displays only that reseller and their customers. The Reseller can view their Call Summary Report, and their customer's Current Active Calls Report.
- **Customer**—Displays only that customer. The customer can view their Current Active Calls Report.

The main frame displays call reports for the user selected in the left frame. The call reports vary based on the user.

**Note:** The Call Status Monitor does not show any active calls when the number of active calls is greater than 400 for a particular VoiceXML application.

---

# Automatic Speech Recognition Log Server

You can download Automatic Speech Recognition (ASR) files with Login Server.

Click **ASR Files Download** to access the ASR file download function. A list of available ASR files appears. Click a file name to download that file. Click the file name again to open or save the file.

---

## Reporter

The Reporter service provides historical call data on enterprise traffic for an overview of voice applications or information on a call-by-call basis. Data-access permissions identified at user login control the data that your customers can view.

You access the Reporter GUI through the Login Server by clicking **Historical Reports**.

---

**Note:** Do not use the browser Back and Forward buttons. Using them provides undesirable results. Instead, use the <<Prev and Next>> buttons provided on the Reporter screens. These buttons provide selective backward and forward navigation.

---

The reports are updated approximately every 15 minutes. Users can view reports online by hour, day, week, or month, or by a customized date range. They can download reports in CSV (comma-separated values) format, import the reports using a data-analysis tool, and then create customized reports.

## Reporter GUI

The Reporter GUI has two frames. In a multi-tenant environment, the left frame displays the reseller, customer, and provisioned voice applications; in a single tenant environment, only the provisioned voice applications are displayed. The main frame displays information selected from the left frame. Click a link in the left frame to view details for that item.

The reports are essentially the same in either a single tenant or multi-tenant environment; the only difference is that name of the customer or reseller is given at the top of a report generated in a multi-tenant environment. Figure 50 on [page 134](#) shows an example of an Hourly Summary Report for an enterprise in a single-tenant environment. The layout of the report for a multi-tenant environment is the same, with the customer name displayed in the banner above the graph.

In all reports, the red bar indicates the total number of calls per day or per hour, and the blue bar indicates the average total calls for the past six weeks. The

average is based on the average of total calls for the same day for the past six weeks.

The menu bar at the top of the main frame provides tools for selecting the type of report and the date range.

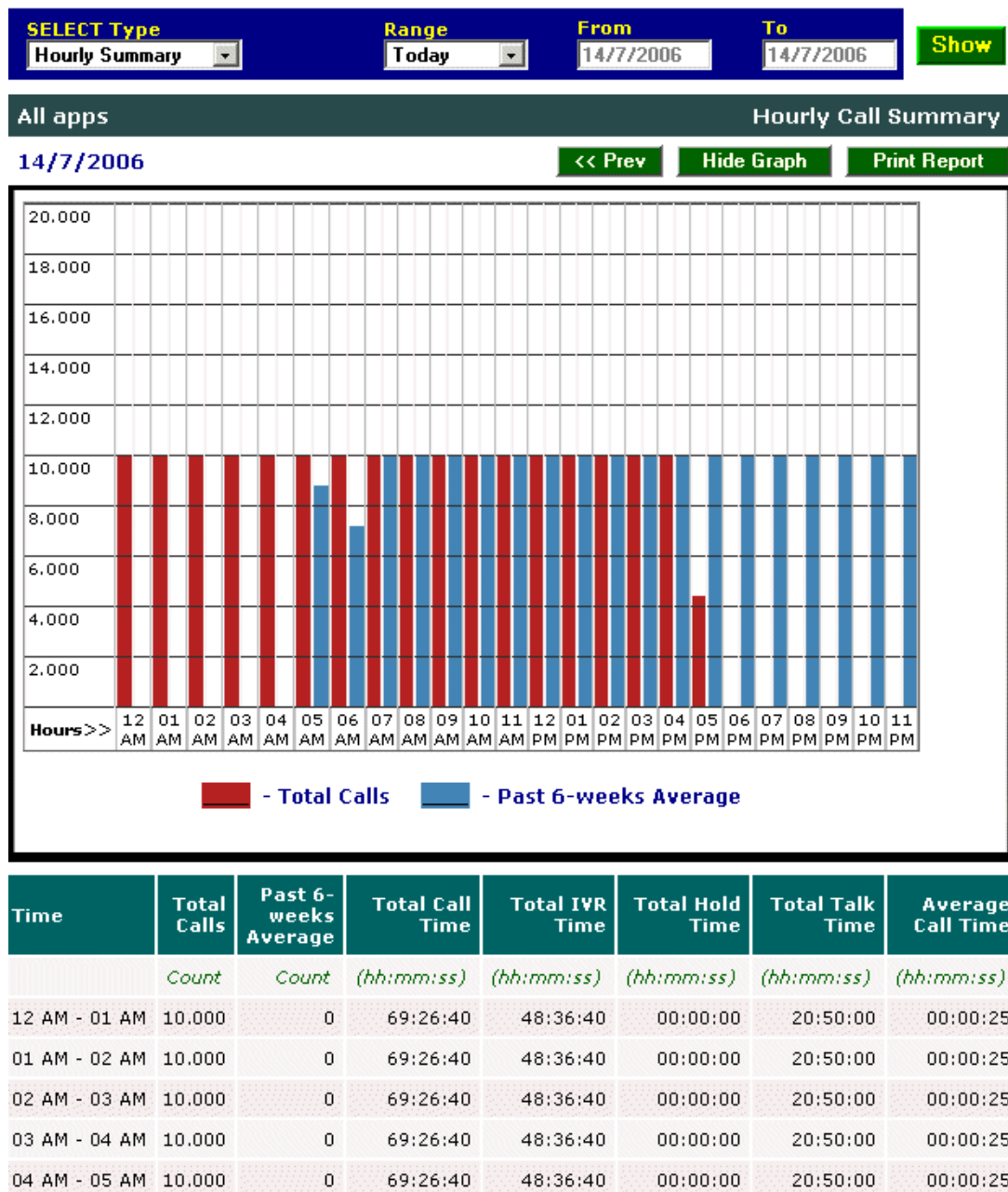


Figure 50: Example of an Hourly Summary Report—Single Tenant

## Hourly Summary Report

---

Note: You can generate the Hourly Summary Report for only a single day.

---

The Hourly Summary Report provides an hourly graph showing call volume and call time, and a six-week average for a voice application, customer, reseller, NSP, VCS, or IPCS server. This information enables the enterprise or customer to track their busy hours and the average time that it takes to handle calls, including self-service time. See Figure 50 on [page 134](#) for an example of an Hourly Summary Report.

On the Hourly Summary Report, a graph is presented that shows the total number of calls per hour. The following details are presented by hour:

- Time
- Total Calls
- Past 6-Weeks Average
- Total Call Time (hh:mm:ss)
- Total IVR Time (hh:mm:ss)
- Total Hold Time (hh:mm:ss)
- Total Talk Time (hh:mm:ss)
- Average Call Time (hh:mm:ss)

Grand totals are presented for:

- Total Calls
- Past 6-weeks Average
- Total Call Time
- Total IVR Time
- Total Hold Time
- Total Talk Time
- Average Call Time

## Call Volume Summary Report

The Call Volume Summary Report allows you to break up the call volume for a period on a reseller, customer, or voice application. This report also displays the percentage of calls for the breakup period.

## Daily Summary Report

The Daily Summary Report provides a daily graph showing call volume and a six-week average for a voice application, customer, reseller, NSP, VCS, or

IPCS server. In this report, for voice applications and customers only, you can click on the date to see an hourly summary for that day.

## Hourly Peaks Report

The Hourly Peaks Report displays the peak number of simultaneous calls every hour and the time the peak occurred. This report is available for a voice application, customer, reseller, NSP, VCS, IPCS, ASR, TTS, IVR Server Client, and Queue Adapter.

---

Note: You can generate the Hourly Peaks Report for only a single day.

---

## Daily Peaks Report

The Daily Peaks Report provides daily peak volume for a voice application, customer, reseller, NSP, VCS, IPCS, ASR, TTS, IVR Server Client, and Queue Adapter. In this report, you can click on the date to see an hourly summary of peaks for that day.

## Call Details Report

The Call Details Report provides a search engine to search for call-by-call information that shows statistics for each caller on the specified date. Additional search criteria are available by time, caller ID, call state (see [Table 4](#)), and so on. The results display the first 100 calls that match the search criteria. For additional listings, use the Download option.

---

Note: This report is not available at the reseller level.

---

**Table 4: Call States**

Call State	Description
IVR	The call ended while the caller was talking to the IVR application.
HOLD	The call ended while it was in the GVP queue and waiting for a transfer. This happens only when GVP queues the call, not in any other switch.
TALK	The call ended while or after the caller was talking to a live agent through a bridge transfer.
XFER	The call ended after a blind transfer was executed.



## Download Report

The Download Report downloads call details, including summary information, at a voice application or customer level (see Figure 51 on [page 138](#)).

Customers can download the report in .csv data format and import it into a data-analysis tool, such as Microsoft Excel. The Download Report process is done in two steps:

### Step 1—Download Request

On the Download Requests screen, you can schedule report creation jobs by selecting the report type and date range. Once the report creation job is scheduled, the report backend process creates the report.

### Step 2—Download Status

On the Download Status screen, you can view the status of the report creation requests that were raised by the login user. The report shows one of the following statuses for each request:

- **In Progress**—The request is still in progress.
- **Available**—The request was successfully completed. Click **Available** to open the report that was generated.
- **Error. Contact Administrator**—An error has occurred in the download process.

## Range

You can choose one of the predefined date ranges for a report, or select **Custom** and enter your desired range in the **From** and **To** fields. These report ranges are available in the Range drop-down list:

- **Today**—displays the data for today's date.
- **Yesterday**—displays the data for yesterday's date.
- **Custom**—displays the data for the custom date range you enter.
- **This Week**—displays the data for the current week, starting from Sunday up until the current day of the current week.
- **Last Week**—displays the data for the previous week, starting from Sunday and ending Saturday.
- **This Month**—displays the data starting from the first day of the month up until the current day.
- **Last Month**—displays the data for the previous month, starting from the first day of the month and ending with the last day of the month.

---

**Note:** The report period for any report cannot be greater than 31 days.

---

SELECT Type <b>Download Status</b> Range <b>This Week</b> From <b>10/28/2007</b> To <b>11/2/2007</b> <b>Show</b>					
Download Status					
Download Reference	Status	Data Type	Start Date	End Date	Customer/ Application
IPCM - Agent_Leg_Hangup_7712	Progress	CD	10/28/2007	11/02/2007	IPCM Agent_Leg_Hangup_7712

Figure 51: Download Report Screen

## Customizing the Interface

Login Server, Call Status Monitor, and Reporter enable you to change the logo, fonts, and colors used in the interface.

### Logo

The logo displayed on the Login Server, User Configuration, Call Status Monitor, and Reporter windows is contained in a file called `telera_new.gif`, which is stored in `<Install Directory>/extweb/customization/images/`. To change the logo, replace the existing file with the new image file, keeping the same file name (`telera_new.gif`).

The logo image must be no more than 90 pixels wide and 50 pixels high. The image file must be in Graphic Interchange format (GIF). If you do not want to display a logo, you must create an image with a background that is either transparent or that matches the background of the voice application, and save the new image as `telera_new.gif`.

### Fonts and Colors

The fonts and colors defined in the interface are defined in style sheets. To change the fonts and colors, modify the appropriate files, as listed in [Table 5](#).

Table 5: File Locations for Customizing Fonts and Colors

To Change Fonts and Colors For:	Modify These Files:
Login Server	<code>&lt;Install Dir&gt;/extweb/customization/unifiedlogin/fonts.css</code>
Call Status Monitor	<code>&lt;Install Dir&gt;/extweb/customization/callstatusmonitor/report_graph.css</code> <code>&lt;Install Dir&gt;/extweb/customization/callstatusmonitor/rcs_tree.css</code>
Reporter	<code>&lt;Install Dir&gt;/extweb/customization/reporter/reporter.css</code> <code>&lt;Install Dir&gt;/extweb/customization/reporter/print_report.css</code>



## Chapter

# 5

## Network Monitor

This chapter describes the Network Monitor. It contains the following sections:

- [Overview, page 139](#)
- [Accessing the Network Monitor Interface, page 140](#)
- [Server Status Summary Report, page 140](#)
- [Component Summary Report, page 143](#)
- [Servers Listing Report, page 143](#)
- [Server Details, page 144](#)

---

## Overview

The Network Monitor enables you to monitor server health across the Genesys Voice Platform (GVP) network through a single graphical user interface (GUI). It provides single-point monitoring of servers running GVP components and services.

---

**Note:** The Network Monitor serves as an indicator for problems. It only verifies if the various conditions in the server status reasons exist. It does not check if other problems exist for the server.

The Network Monitor is not a replacement for Simple Network Management Protocol (SNMP) traps or the EMS GUIs.

---

The Network Monitor runs analysis cycles at regular intervals (the default is three minutes).

For detailed information on each component, check the Element Management System GUI for that component (see Chapter 6, “Element Management System,” on [page 145](#)).

---

# Accessing the Network Monitor Interface

You can access the interface directly through a compliant web browser.

To access the Network Monitor GUI:

1. Open a web browser.
2. Enter `http://<FQDN of EMPS Machine>:9810/gvpportal` in the address bar. The Portal GUI opens. Click the link under Network Monitor.

OR

Enter `http://<servername.domainname>:9811` in the address bar. The Network Monitor GUI opens (see Figure 52 on [page 141](#)).

The Network Monitor GUI has two frames. The left frame displays a directory tree structure. To expand the Server Status node and view the list of servers, click the plus (+) sign beside the node. To collapse the node and hide the list of servers, click the minus (-) sign.

---

Note: By default, the directory tree is collapsed.

---

The main frame displays information based on selected links. The Server Status page is the home page.

The options at the bottom of the screen enable you to change the display settings.

- Refresh—immediately refreshes the onscreen data.
- Auto Refresh—by default, periodically refreshes the onscreen data by the interval specified in the Refresh Rate field. You can enable or disable this option using the check box.
- Refresh Rate (in sec)—displays the automatic refresh rate in seconds for the data. Enter the desired automatic refresh rate in the field provided and click Save.

---

## Server Status Summary Report

The Server Status Summary Report provides a snapshot of the health of all servers in the GVP network. The Server Status Summary Report has these features:

- Provides cumulative counts and provides you with the option to click and view additional details.
- Counts each server only once. You can view this report for the network or for a specific component type.

- Shows the server status category codes and count and percentage of servers that fall under this category. You can expand the category codes to individual status reasons.
- Provides a count and percentage for the individual status reasons.
- Displays a pie chart, which indicates the breakup for the category codes.

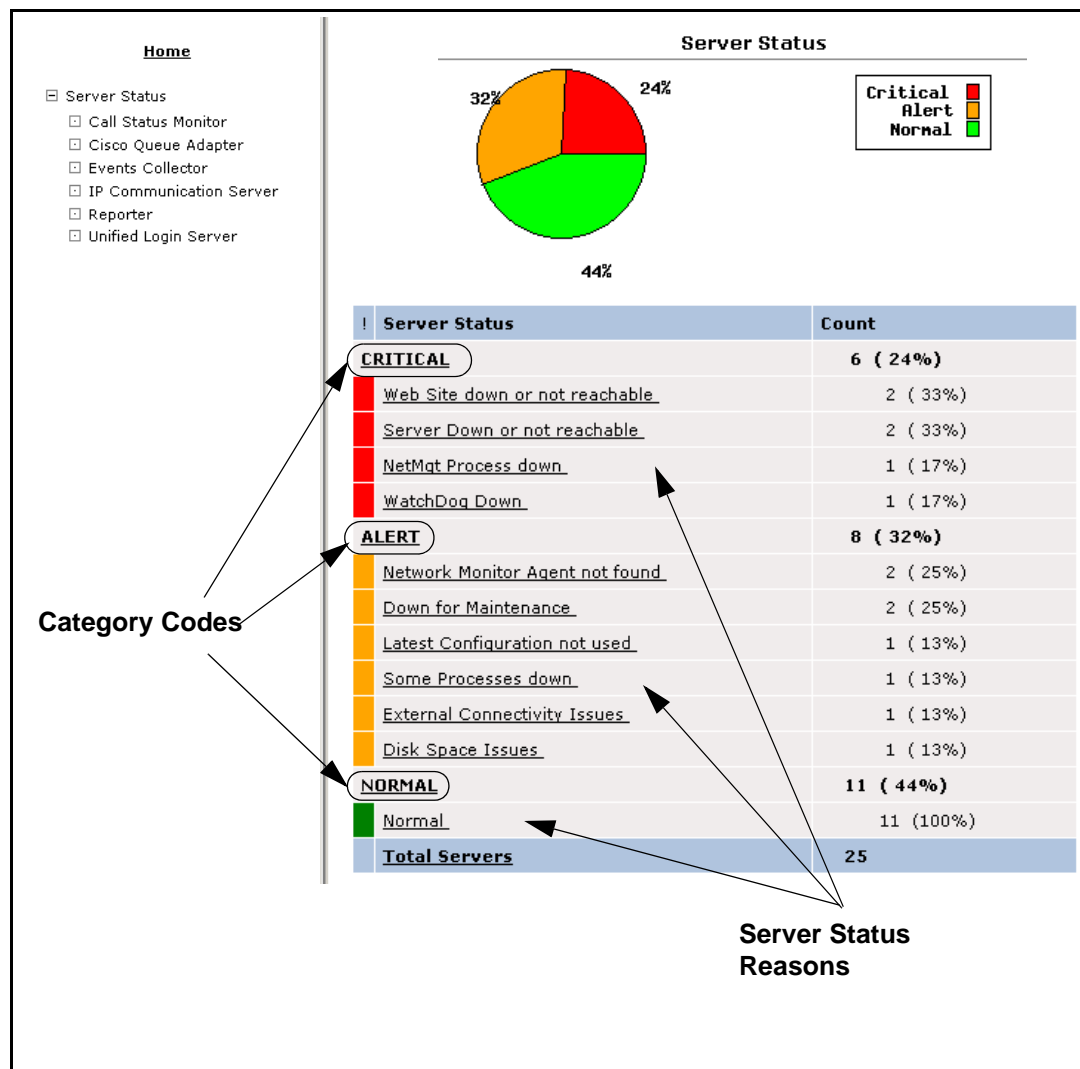


Figure 52: Example—Network Monitor Server Status Page

## Category Codes

The category codes classify servers based on their run condition and the type of response required from the monitoring personnel. You can click on the category code to open the Server Listing page (see “Servers Listing Report” on [page 143](#)).

[Table 6](#) lists the Category Codes and descriptions.

**Table 6: Category Codes**

Category Code	Description
Critical	The <code>Critical</code> state requires immediate action. The GVP services on the server are down without notice.
Alert	The <code>Alert</code> state requires you to monitor the server closely and take suitable action when necessary. This state might be due to some process being down, or the server being down for maintenance, or an upcoming emergency (for example, disk space is running low).
Normal	This state indicates that the server is working normally as per the Network Monitor.

## Server Status Reasons

Within each category, servers are classified based on their status reason. The server status reason explains why the server is classified under that specific category. It also provides subclassification for more detailed troubleshooting.

You can click on a server status reason to open the Server Listing page (see “Servers Listing Report” on [page 143](#)), which provides a list of servers with the same status reason.

[Table 7](#) lists the server status reasons.

**Table 7: Server Status Reasons**

Reason	Category Code	Description
Server Down or Not Reachable	Critical	The server does not respond to basic network connectivity queries (pings).
Web Site Down or Not Reachable	Critical	The web server (IIS/Apache) on the server is down or cannot be accessed.
NetMgt Process Down	Critical	This reason occurs when the server cannot access the Element Management interface under port 9810. An HTTP query returns <code>File Not Found</code> .
WatchDog Down	Critical	This reason occurs when the server cannot ping WatchDog using the webnotify ping.

**Table 7: Server Status Reasons (Continued)**

Reason	Category Code	Description
Network Monitor Agent Not Found	Alert	This reason might occur if the server is running an earlier release of GVP where Network Monitor is not supported (Network Monitor cannot analyze further).
Some Processes Down	Alert	This reason occurs when the server's query to the <code>wdAPTable</code> MIB shows that some processes are not active.
External Connectivity Issues	Alert	This reason occurs when the server encounters problems with external interfaces to software, which includes: <ul style="list-style-type: none"> <li>• Ports for the VCS/IPCS.</li> <li>• DB connection down for EventC.</li> <li>• CTI connection down for queue adapters.</li> </ul>
Disk Space Issues	Alert	This reason occurs when the server's disk space is less than 50 MB in the GVP installation disk or the temporary disk.
Latest Configuration Not Used	Alert	This reason occurs when the server is not running the latest configuration. This is inferred through the presence of an <code>.initds</code> file in the <code>config</code> directory.
Down for Maintenance	Alert	You can switch a server to or from this state through the Network Monitor GUI.
NORMAL	NORMAL	The server is normal.

---

## Component Summary Report

The Component Summary Report provides a component view of the server status report. This report enables you to analyze each component to see if primary and secondary schemes are working (for example, if there are two Policy Managers, you can check if one of them is running).

---

## Servers Listing Report

The Servers Listing Report provides a list of servers (see Figure 53 on [page 144](#)). This is a drill-down from the Server Status Summary or Component Summary Report and uses filters based on selections from that report (for example, if you click VCS/IPCS from the component summary, the list filters VCS/IPCS servers only).

Servers Listing					
		Server Type : ALL			
		Status : CRITICAL			
		Reason : ALL			
!	Server Name	Server Type	Reason	Note	Status as of
	<a href="#">dev-goofy.dev.telera.com</a>	IP Communication Server;	Web Site down or not reachable	Port 9810 down on the Server or not reachable	2004-05-17 14:45:19
	<a href="#">dev-robin.dev.telera.com</a>	IP Communication Server;	Web Site down or not reachable	Port 9810 down on the Server or not reachable	2004-05-17 14:45:19

Figure 53: Servers Listing Page

## Server Details

This screen displays the details for a specific server (see Figure 54). It is a drill-down from the Servers Listing Report.

You can click on the server name to open the Element Management GUI in a new window.

Servers Details : dev-goofy.dev.telera.com	
<b>Name</b>	<a href="#">dev-goofy.dev.telera.com</a>
<b>Components Installed</b>	IP Communication Server;
<b>Status</b>	CRITICAL
<b>Reason</b>	Web Site down or not reachable
<b>Note</b>	Port 9810 down on the Server or not reachable

Switch Server to Maintenance State	
Note :	<input type="text"/>
<input type="button" value="Switch Server to Maintenance State"/>	

Status as of 2004-05-17 14:45:19

Figure 54: Servers Details Page

The Server Details page provides details on the selected server. From this page, you can set the server to a maintenance state and provide a note to help an operator track servers.





## Chapter

# 6

## Element Management System

The Element Management System (EMS) GUI monitors the Genesys Voice Platform (GVP) components. This chapter provides information about the EMS GUIs. It contains the following sections:

- [Overview, page 146](#)
- [System Information Menu, page 148](#)
- [Bandwidth Manager, page 155](#)
- [Cisco Queue Adapter, page 159](#)
- [Element Management Provisioning System, page 165](#)
- [Events Collector, page 165](#)
- [H.323 Session Manager, page 171](#)
- [IP Communication Server, page 176](#)
- [IVR Server Client, page 181](#)
- [MRP SMP Integrator, page 186](#)
- [OBN Manager, page 189](#)
- [Policy Manager, page 191](#)
- [Resource Manager, page 196](#)
- [SIP Session Manager, page 200](#)
- [Text-to-Speech, page 204](#)
- [Voice Communication Server, page 210](#)

# Overview

The Genesys Voice Platform (GVP) Element Management System (EMS) graphical user interfaces (GUIs) are similar in appearance and contain common options (see [Figure 55](#)).

When you invoke the GUI, if WatchDog or the Element Management process is *not* running on the host machine, the GUI provides you with a URL to start the process. The GUI refreshes itself periodically to determine if the process is back up.

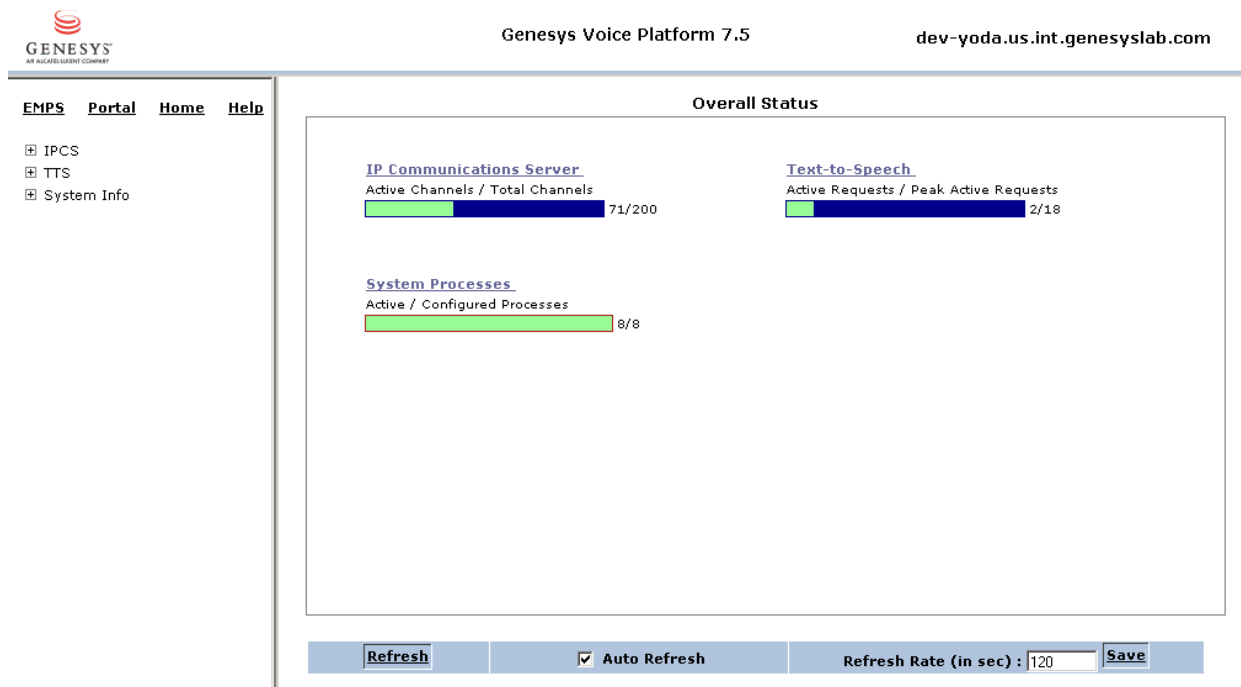


Figure 55: Example—Element Management System GUI

## Top Frame

The top center of the GUI displays the product and version, and the top right displays the respective server.

## Left Frame

The left frame displays a directory tree structure. To expand a node and view its children, click the plus (+) sign beside the node. To collapse the node and hide the children, click the minus (-) sign.

Note: By default, the directory tree is collapsed.

The dot (.) character represents a leaf node (no children) and clicking on it does not change the tree.

The top of the left frame has the following options:

- **EMPS**—opens the Element Management Provisioning System (EMPS) GUI. (See Chapter 1, “Element Management Provisioning System,” on [page 25](#).)
- **Portal**—opens the Portal GUI. (See Chapter 7, “Portal,” on [page 221](#).)
- **Home**—displays the Overall Status page in the main frame.
- **Help**—opens the Help file in a separate window.

## Main Frame

The main frame displays information based on selected links. An Overall Status page (an example is shown in Figure 55 on [page 146](#)) appears in all Element Management GUIs.

### Overall Status

The Overall Status screen displays an overview of each applicable component with a link to that component’s summary page (each component is discussed in detail in this chapter).

The component overview displays as a bar and fraction. For example, in Figure 55 on [page 146](#), where the IP Communication Server (IPCS) overall status is 200 total channels, 71 of which are active.

The Overall Status screen also displays system processes for the applicable component. The System Processes link opens the Processes page (see “Processes” on [page 148](#)).

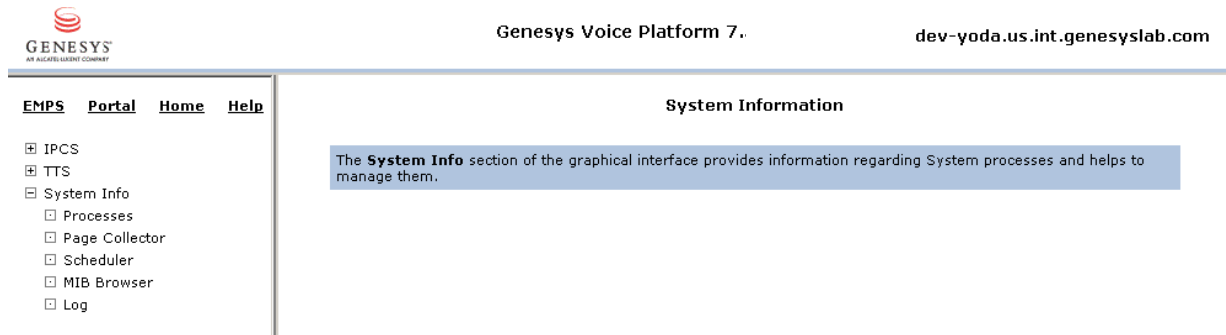
## Display Settings

The options at the bottom of the screen, which you can use to change the display settings, appear on all of the Element Management GUIs.

- **Refresh**—immediately refreshes the on-screen data.
- **Auto Refresh**—by default, periodically refreshes the onscreen data by the interval specified in the Refresh Rate field. You can enable or disable this option using the check box.
- **Refresh Rate (in sec)**—displays the automatic refresh rate in seconds for the data. Enter the desired automatic refresh rate in the field provided and click Save.

# System Information Menu

The System Information menu, in the left frame (see [Figure 56](#)), appears on all of the Element Management GUIs. This menu provides system monitoring information for the respective server.



**Figure 56: System Information Menu**

The System Information menu has the following links:

- Processes
- Page Collector
- Scheduler
- MIB (Management Information Base) Browser
- Log

## Processes

The Processes page (see [Figure 57](#) on [page 149](#)) provides information on the status of each process. Any time a process shuts down and is then restarted, the event is recorded in this page by WatchDog. You can shut down or restart a process on this page.

Processes				
Process Name	Status	Action	Last Restart	Total Restarts
callrecsgenerator1	Active	STOP Graceful GO	Oct 14, 2004 1:19:48 PM	0
eventmanager1	Active	STOP Graceful GO	Oct 14, 2004 1:19:49 PM	0
eventsloader1	Active	STOP Graceful GO	Oct 14, 2004 1:19:50 PM	0
netmgt	Active	RESTART Graceful GO	Oct 14, 2004 1:19:44 PM	0
networkmonitor	Active	STOP Graceful GO	Oct 14, 2004 2:14:30 PM	2
pagecollector	Active	STOP Graceful GO	Oct 14, 2004 1:19:45 PM	0
peaksnsp1	Active	STOP Graceful GO	Oct 14, 2004 1:19:53 PM	0
scheduler	Active	STOP Graceful GO	Oct 14, 2004 1:19:47 PM	0
WatchDog	Active	STOP Graceful GO	Oct 14, 2004 1:19:53 PM	0

☒ Auto Refresh
 Refresh Rate (in sec) :

Figure 57: Process Table Page

To shut down a process:

- Next to the desired Process Name, select the method to perform the shutdown from the Action drop-down list. The shutdown actions are:
  - Graceful—allows calls that are in progress to complete, then shuts down the process. No new calls are accepted.
  - Ungraceful—aborts all calls in progress, cleans up, and then shuts down.
  - Immediate—shuts down the process immediately. Calls in progress are dropped.
- Click Go.

To restart a process:

- Next to the desired Process Name, select Restart from the Action drop-down list.
- Click Go. The process stops and restarts.

## Page Collector

The Page Collector (see Figure 58 on [page 150](#)) provides a statistical analysis of the data transferred on the respective server.

**Page Collector - Statistics**

dev-andes.dev.telera.com				
File Size	Last Round Trip (msec)	No. of Round Trips	Average Round Trip Time (msec)	Last 5 min Average (msec)
Less than 20KB	46	29	73	0
20KB to 50KB	0	0	0	0
50KB to 100KB	0	0	0	0
100KB to 500KB	0	0	0	0
500KB to 1MB	0	0	0	0
1MB to 5MB	0	0	0	0
more than 5MB	0	0	0	0

dev-daffy.dev.telera.com				
File Size	Last Round Trip (msec)	No. of Round Trips	Average Round Trip Time (msec)	Last 5 min Average (msec)
Less than 20KB	62	29	29	0
20KB to 50KB	0	0	0	0

☒ Auto Refresh
 Refresh Rate (in sec) :

**Figure 58: Page Collector Statistics**

[Table 8](#) describes the parameters in the Page Collector Statistics page.

**Table 8: Page Collector Statistics**

Parameter	Description
File Size	Range of file sizes.
Last Round Trip (msec)	Last fetch in milliseconds.
No. of Round Trips	Total number of fetches.
Average Round Trip Time (msec)	Average fetch time in milliseconds.
Last 5 Min Average (msec)	Average fetch time in milliseconds within the last five minutes.

## Scheduler

The Scheduler (see [Figure 59](#) on [page 151](#)) provides information about scheduled processes that were configured in EMPS.

**Scheduler**

Select	Task Name	Start Time	Poll frequency	Task State
<input type="checkbox"/>	<a href="#">GarbageCollector</a>	Sep 23, 2004 3:54:24 PM	1 hrs 0 mins 0 secs	Running

☒ Auto Refresh
 Refresh Rate (in sec) :

**Figure 59: Scheduler Page**

The following options are available from the Scheduler page:

- Suspend Selection—stops the selected task.
- Resume Selected—resumes the selected task.
- Execute—immediately starts the selected task.

Clicking the [Garbage Collector](#) link in the Scheduler page opens the Garbage Collector Statistics page (see [Figure 60](#)).

**Garbage Collector Statistics**

Directory Name	Files to Delete	Clean Sub Dirs	Delete Files after (Days:Hrs:Mins)	Space Gain (Bytes)	Total No. of Files Deleted	Minimum File Size (Bytes)	Maximum File Size (Bytes)
/var/tmp/kandalam/cn/temp	vbf*.tmp	No	00:06:00	0	0	0	0
/var/tmp/kandalam/cn/temp	xml*.tmp	No	01:00:00	0	0	0	0
/var/tmp/kandalam/cn/web\Upload	*.vox	Yes	03:00:00	0	0	0	0
%SystemRoot%\System32\LogFiles	*,*	Yes	07:00:00	0	0	0	0
/var/tmp/kandalam/cn/extweb/reporter/download	*,*	Yes	7:00:00	0	0	0	0

☒ Auto Refresh
 Refresh Rate (in sec) :

**Figure 60: Garbage Collector Statistics**

The Garbage Collector page displays the cleanup conditions that were configured in EMPS. Table 9 on [page 152](#) describes the parameters in the Garbage Collector Statistics page.

**Table 9: Garbage Collector Statistics**

Parameter	Description
Directory Name	Lists the directories to be cleaned.
Files to Delete	Lists the type of files to delete.
Clean Sub Dirs	Indicates if subdirectories are to be cleaned.
Delete Files After (Days:Hrs:Mins)	Displays the cleanup frequency in days, hours, and minutes.
Space Gain (Bytes)	Displays the disk space gained, in bytes, after cleanup.
Total No. of Files Deleted	Displays the total number of files deleted in the directory.
Minimum File Size (Bytes)	Displays the minimum file size in bytes that was deleted.
Maximum File Size (Bytes)	Displays the maximum file size in bytes that was deleted.

---

Note: If you make any changes to the Garbage Collector parameters in EMPS > Servers, you must restart WatchDog in order for those changes to take effect.

---

## Management Information Base

The Management Information Base (MIB) browser provides directory information about the server and is typically only used by Genesys technical support for advanced debugging and troubleshooting. The MIB page is shown in Figure 61 on [page 153](#), with example data displayed.



MIB Tree									
<div> <div>+</div> popwd <div>+</div> popctrl <div>+</div> pagecol <div>+</div> telemgr <div>+</div> netMgt <div>+</div> bwm <div>+</div> trapMgt <div>+</div> CCM <div>+</div> QueueAdapter <div>+</div> GarbageCollector <div>+</div> CallStats <div>+</div> <b>csCustCallVolTbl</b> <div>+</div> csCustAppTbl <div>+</div> csAppCallVolTbl <div>+</div> csAppSessionTbl <div>+</div> csAppCallsByLATATbl <div>+</div> NCES <div>+</div> CFC <div>+</div> scheduler <div>+</div> TeleraCallDistributor <div>+</div> SAP <div>+</div> TTS <div>+</div> ASRPkgLoader <div>+</div> ORL <div>+</div> DMC <div>+</div> SSM </div>									
csCustCallVolTbl									
cs Cust Call Vol Tbl Cust Id	cs Cust INPorts	cs Cust INActive Calls	cs Cust INTotals Calls	cs Cust INTotals Calls Reject	cs Cust OUTPorts	cs Cust OUTActive Calls	cs Cust OUTTotal Calls	cs Cust OUTTotal Calls Reject	
956	0	30	3583	0	0	0	0	0	
1212	0	0	0	0	0	0	0	0	
1444	0	0	0	0	0	0	0	0	
1476	0	0	0	0	0	0	0	0	
1764	0	0	0	0	0	0	0	0	
1964	0	0	0	0	0	0	0	0	
1976	0	0	0	0	0	0	0	0	
2008	0	0	0	0	0	0	0	0	
2044	0	56	3085	0	0	2	217	0	
2244	0	0	0	0	0	0	0	0	
3016	0	0	0	0	0	0	0	0	
3140	0	0	0	0	0	0	0	0	
3200	0	0	0	0	0	0	0	0	
3268	0	0	0	0	0	0	0	0	
3288	0	81	3366	0	0	32	3317	0	
<a href="#">MIB Query URL</a>									
<div> <div>Process</div> <div></div> <div>Query</div> </div>									

Figure 61: MIB Page with Example Data

To view directory information:

1. Select the desired item from the MIB directory tree. The right side of the window displays any data in the selected item.

The MIB Query URL link opens the Extensible Markup Language (XML) source file, which you can then save or print.

## Log

Use the Log Setting page (see Figure 62 on [page 154](#)) to set debug log levels for the processes selected from the Process Name drop-down list.

**Log Setting**

**Process Name :** admin\_admincustomer\_pm ▼

**Log Level :** Error ▼

Apply Changes

Refresh
☒ Auto Refresh
Refresh Rate (in sec) : 120
Save

**Figure 62: Log Setting Page**

The processes whose log levels you can change depend on the processes on a particular computer.

[Table 10](#) lists the log levels for a particular process:

**Table 10: Log Levels**

Log Level	Description
Error	Logs all information indicating that the call was not normally processed. Almost always, an VCS/IPCS host trap error occurs when a log entry is created with this log level. Multiple error log lines in the files may correspond to one VCS/IPCS host trap.
Warning	Logs all information indicating that the call was normally processed, but indicates that future calls may be at risk of not being normally processed.
Information	Logs all information about the call processing at various strategic checkpoints during the call.
Debug	Logs detailed information about the call, including function parameters. This log level results in a high volume of logs and is not recommended for an extended period of time.

**Table 10: Log Levels (Continued)**

Log Level	Description
Full	<p>Logs all of the above and potentially more. A log level of Full indicates increasing levels of detail that appear in the process log file.</p> <p>The Full logging option might use all of the free disk space, so use this option with caution. Enabling full logging capabilities is recommended only for debugging purposes, not for production.</p>
Custom	<p>A Log Flags field appears when you select Custom as the Log Level. Custom logging is for advanced debugging and troubleshooting by Genesys technical support only.</p>

By default, the GVP process logs all errors and warnings. You can change the logging level by selecting the process and the appropriate log level, and then clicking **Apply Changes**. By default, the log files are located at <installation directory>\log.

---

**Note:** For GVP Solaris, do not store any files in the subdirectories of cn/log. Cn/log is a temporary file system and is not persisted across reboots. However, GVP does persist the cn/log contents across reboots, but only if the server was shut down gracefully.

---

## Bandwidth Manager

The Bandwidth Manager (BWM) manages the rate of file transfer for .vox files on the VCS/IPCS. It also performs retries in the event of failures.

### Bandwidth Manager Summary

To open the BWM Summary page, click the Bandwidth Manager link in the left frame or click the Bandwidth Manager link on the Overall Status page. The Summary page (see Figure 63 on [page 156](#)) displays the total number of successful, pending, and failed transfers.

**BWM Summary**

BWM Process	Orders Done	Orders Pending	Orders Failed
bwm1	0	0	2

[Refresh](#)
☒ Auto Refresh
Refresh Rate (in sec) : 
[Save](#)

Figure 63: Bandwidth Manager Summary

[Table 11](#) provides descriptions of the parameters:

---

Note: An *order* is a request for initiating the .vox file transfer to the customer web server from the VCS/IPCS.

---

**Table 11: Bandwidth Manager Summary Parameters**

Parameter	Description
BWM Process	Name of the process.
Orders Done	Total orders processed.
Orders Pending	Total orders waiting to be transferred.
Orders Failed	Total orders that failed. An order fails after the maximum number of transfer attempts is reached.

## Customer Summary

To open the BWM Customer Summary page (see Figure 64 on [page 157](#)), expand the Bandwidth Manager link in the left frame and then click the Customer Summary link. The Customer Summary page displays the number of successful, pending, and failed transfers for customers. It also includes the oldest pending-order information.

The BWM Customer Summary page counts all of the orders for all customers as one customer only when their web application server (WAS) is the same. If the WAS servers are different, it will count the orders for different customers.

BWM Customer Summary								
BWM Process	Customer	WAS	Orders Done	Orders Pending	Orders Failed	Oldest Pending Order Source	Oldest Pending Order Destination	Orders Pending Order Time
bwm1	<a href="#">Telera</a>	atule-2000.callnetcomm.com (10.10.10.150)	0	0	2	mktdemolab.dev.telera.com	atule-2000.callnetcomm.com	2003/01/14 23:29:13 GMT

Refresh

☒ Auto Refresh

Refresh Rate (in sec) :

Save

**Figure 64: BWM Customer Summary**

Table 12 provides descriptions for the parameters.

Note: An *order* is a request for initiating the .vox file transfer to the customer web server from the VCS/IPCS.

### Table 12: BWM Customer Summary Parameters

Parameter	Description
BWM Process	Name of the process.
Customer	Name of the customer. <b>Note:</b> This column appears only for a multi-tenant installation. It does not appear for a single-tenant installation.
WAS	Web server address for the customer.
Orders Done	Total orders processed for the customer.
Orders Pending	Total orders waiting to be transferred for the customer.
Orders Failed	Total orders that failed for the customer. An order fails after the maximum number of transfer attempts is reached.
Oldest Pending Order Source	Location of the .vox file that has been in queue the longest.

**Table 12: BWM Customer Summary Parameters (Continued)**

Parameter	Description
Oldest Pending Order Destination	Location to where the oldest pending .vox file is going to be transferred.
Orders Pending Order Time	Time when the order was received by BWM.

## Customer Orders

To open the Customer Orders page (see [Figure 65](#)) for a specific customer, click that customer's link on the BWM Customer Summary page.

The Customer Orders page provides information on the failed and queued transfers for each web server. You can resume a transfer or delete an item from this page.

---

**Note:** An *order* is a request for initiating the .vox file transfer to the customer web server from the VCS/IPCS.

---

Customer Orders -

Customer
**Telera**

Resume Transfer
Delete Item

Select	Status	BWM Process	Customer	WAS	Source Host	File	BWM Session ID	Time of Entry	Total Attempts	Last Attempt	Last Error
No Data Available											

Refresh
☒ Auto Refresh
Refresh Rate (in sec) : 
Save

**Figure 65: BWM Customer Orders**

[Table 13](#) describes the parameters in the BWM Customer Orders page.

**Table 13: BWM Customer Orders Parameters**

Parameter	Description
Select	Check box to select an order.
Status	Active—The transfer is currently being attempted. Queue—Waiting for transfer.
BWM Process	Name of the process.
Customer	Name of the customer.
WAS	Web server address for the customer.
Source Host	Location of the .vox file.
File	Name of the .vox file.
BWM Session ID	Unique session identification of the order.
Time of Entry	Time the .vox file was received.
Total Attempts	Total number of transfer attempts.
Last Attempt	Time of the last transfer attempt.
Last Error	Error string for the last transfer attempt.

---

## Cisco Queue Adapter

The Cisco Queue Adapter (CQA) communicates with a customer's Cisco call-routing software through a customer's Peripheral Gateway (PG). The CQA passes information between the GVP and the customer's Cisco call-routing software.

---

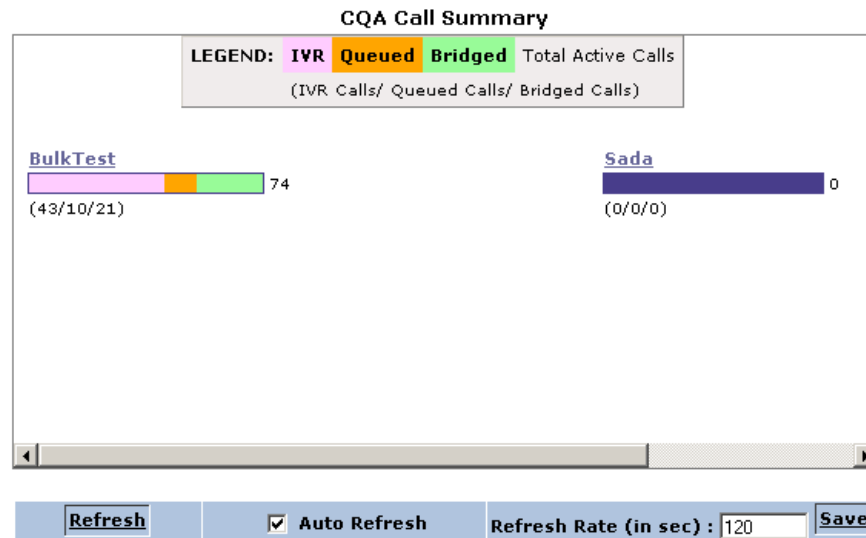
Note: The Cisco Queue Adapter is an optional feature.

---

### Cisco Queue Adapter Call Summary

To open the CQA Call Summary page (see Figure 66 on [page 160](#)), click the Cisco Queue Adapter link in the left frame or on the Overall Status page. The Summary page displays information about the CQA and its connection to a PG.

When multi-tenancy is enabled, the Call Summary page displays the IVR/Queued and Bridged calls for the customer. When multi-tenancy is not enabled, the Call Summary page displays the IVR/Queued and Bridged calls for voice applications.



**Figure 66: Cisco Queue Adapter Call Summary**

The number of active calls displays to the right of the bar, and the state of the active calls displays as a fraction underneath the bar. For example, 43/10/21 means that of the 74 active calls, 43 of them are IVR, 10 are Queued, and 21 are Bridged. A legend at the top of the page explains the color coding.

## Connection Status

To open the CQA Connection Status page, expand the Cisco Queue Adapter node in the left frame, and then click the Connection Status link. The CQA Connection Status page displays the connection status for each CQA and its corresponding PG (see Figure 67 on [page 161](#)).

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the Customer name column.



CQA Connection Status				
Adapter Name	Customer Name	PG Connection State	PG Address	TCP Port
codecenter_devxchange_cqa	Devxchange	NetworkFailure	None	9005
vwap52_cherry_cqa	Cherry	NetworkFailure	None	9008
icm_testing_icm_control_cqa	ICM_Control	NetworkFailure	None	9004
icm_testing_ivr_control_cqa	IVR_Control	NetworkFailure	None	9007
ga51_rc19_cqa	RC19	NetworkFailure	None	9006
kaylyn_cqatest_cqa	cqatest	Normal	10.10.17.204	9004
kaylyn_pmtest_cqa	pmtest	NetworkFailure	None	9001
vwap521_genesys_studio_cqa	Genesys_Studio	NetworkFailure	None	9010

☒ Auto Refresh
 Refresh Rate (in sec) :

Figure 67: Cisco Queue Adapter Connection Status

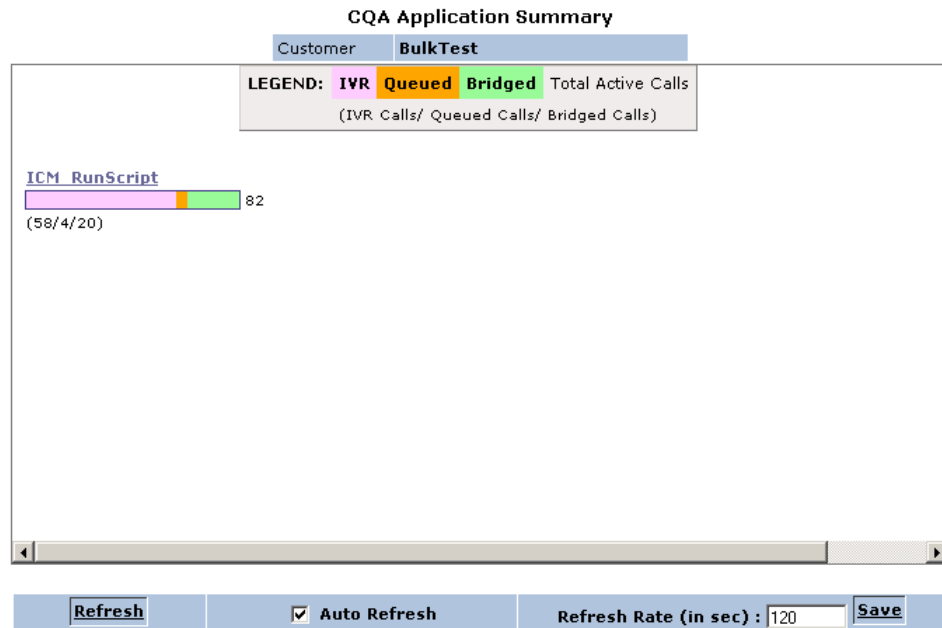
Table 14 describes the parameters in the CQA Connection Status page.

Table 14: CQA Connection Status Parameters

Parameter	Description
Adapter Name	Name of queue adapter process.
Customer Name	Name of the customer.
PG Connection State	Connection state from CQA to PG: <ul style="list-style-type: none"> <li>• Network Failure</li> <li>• Normal</li> </ul>
PG Address	Remote PG address.
TCP Port	TCP listening port of CQA.

## Cisco Queue Adapter Application Summary

To open the CQA Application Summary page for a specific customer, click that customer's link in the left frame or click that customer's link on the CQA Call Summary page. The Summary page displays call statistics for the selected customer (see Figure 68 on [page 162](#)).



**Figure 68: CQA Application Summary**

Each voice application for that customer then has a link to its statistics—**Active Calls** and **Call Volume**.

## Active Calls

The **CQA Active Calls** page (see Figure 69 on [page 163](#)) displays the active call information for the voice application.

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the **Customer name** column.

CQA - Active Calls

Customer	BulkTest
Application	ICM_RunScript

Switch to : [Call Volume](#)

Dialog ID	DNIS	ANI	Dialed Number	Session State	Current Script	Session ID
12379	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{30A2997E-1F48-49A5-BFFB-88BEA5D21A4B}
12398	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{56739196-4E7A-4790-AF98-4C45EC1929D9}
12402	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{D7FD96D4-5EBC-4FEF-9FF8-2333DA80712D}
12406	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{7D2A00C0-A716-4F80-8197-3FCB4F41BD29}
12407	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{6FBB2C66-DABC-4683-9869-FD65DD36980F}
12408	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{644A3080-2A77-40B1-B3AE-597302BB86B2}
12409	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{F50E5D13-08C9-4B11-BE87-A8D5A8516679}
12410	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{37127000-7961-4D89-97DB-28EB59D98B81}
12411	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{EA022C34-27F2-4684-9AE4-6AF763F4C67B}
12412	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{94EE08D0-D589-4B33-8149-06D4955ADC26}
12413	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{D2830E4F-26F5-440E-8E55-ED81C0D9DF74}
12414	4086266820	\$ani\$	8886266822	Connected	Phone Number: 4086266890	{1158B1D1-65ED-4D3F-980F-078998EF023D}

Refresh

☒ Auto Refresh

Refresh Rate (in sec) : 120

Save

Figure 69: CQA Active Calls

Table 15 describes the parameters in the CQA Active Calls page.

Table 15: CQA Active Calls Parameters

Parameter	Description
Dialog ID	Unique identifier of dialog between CQA and PG.
DNIS	Dialed Number Identification Service.
ANI	Automatic Number Identification.
Dialed Number	Number called.
Session State	State of the call. <ul style="list-style-type: none"> <li>Connected—The call has been transferred to an agent.</li> <li>IVR—The call is in IVR state.</li> <li>Queued—The call is waiting for transfer to an agent.</li> <li>Dialing—The call is in the process of being transferred to an agent.</li> </ul>
Current Script	Current IVR script executed at the IVR.
Session ID	Identification of the session between the CQA and the CFA.

## Call Volume

The CQA Call Volume page (see [Figure 70](#)) displays the call volume information for the voice application.

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the Customer name column.

CQA - Call Volume

Customer	BulkTest
Application	ICM_RunScript

Switch to : [Active Calls](#)

Name	Value
Number of active sessions	82
Number of active sessions in queue	7
Number of sessions normal routed	12165
Number of sessions default routed	0
Number of network failures	0
Last network failure time	0
Number of active sessions bridged	58

[Refresh](#)
☒ Auto Refresh
Refresh Rate (in sec) : 
[Save](#)

**Figure 70: CQA Call Volume**

[Table 16](#) describes the parameters in the CQA Call Volume page.

**Table 16: CQA Call Volume Parameters**

Parameter	Description
Number of Active Sessions	Total number of active calls.
Number of Active Sessions in Queue	Total number of active calls waiting for transfer.
Number of Sessions Normal Routed	Total number of calls routed to an agent.
Number of Sessions Default Routed	Total number of calls routed to an error number in case the connection between the CQA and PG is lost.
Number of Network Failures	Total number of network failures between the PG and CQA since the last restart.

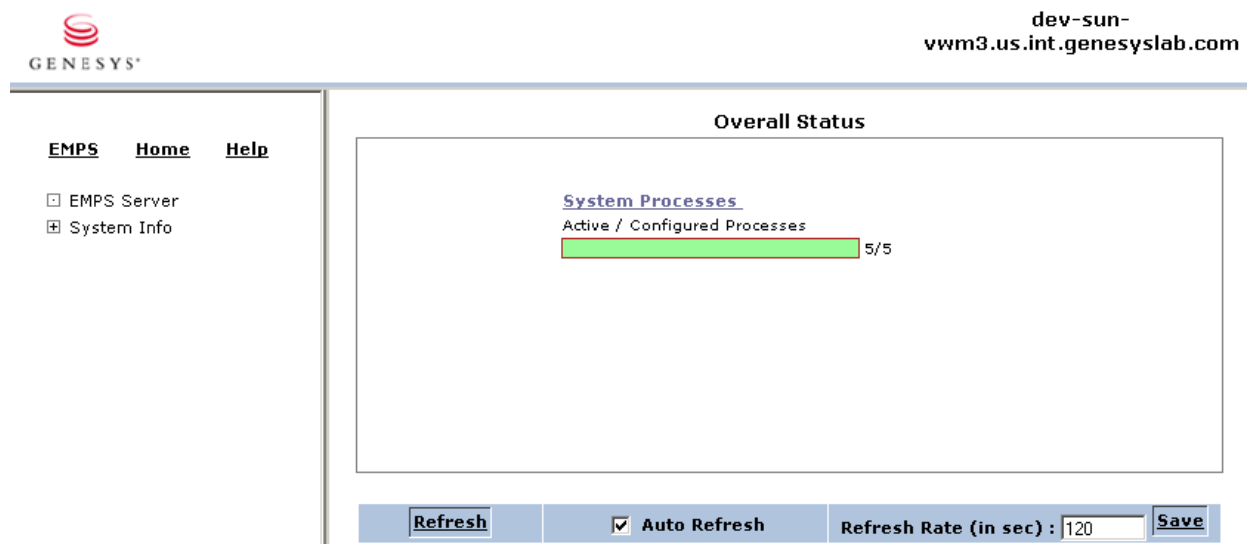
**Table 16: CQA Call Volume Parameters (Continued)**

Parameter	Description
Last Network Failure Time	The time of the last network failure.
Number of Active Sessions Bridged	Total number of calls currently being transferred.

## Element Management Provisioning System

The Element Management Provisioning System (EMPS) is the provisioning interface for all EMS components. For detailed information on provisioning, refer to Chapter 1, “Element Management Provisioning System,” on [page 25](#).

The EMPS Element Management GUI displays as shown in [Figure 71](#).

**Figure 71: EMPS Element Management GUI**




- Overall Status page—displays an active and total/configured processes bar and provides a link to the Process page. See “Processes” on [page 148](#).
- EMPS Server link—opens the EMPS Diagnostics page. See “Diagnostics” on [page 90](#).
- System Info—see “System Information Menu” on [page 148](#).

## Events Collector

The Events Collector receives individual call events from the IP Communication Servers and Voice Communication Servers.

## Events Collector Work-in-Progress

To open the Events Collector Work-in-Progress page (see [Figure 72](#)), click the Events Collector link in the left frame or on the Overall Status page. The Work-in-Progress page displays Events Collector processing information.

Events Collector Work-in-Progress					
Flag	Data Buffer	No. of Items in Buffer	Time Stamp of Earliest Item	Time Stamp of Latest Item	Comment
	Files waiting for Events Loader	0			OK
	Events waiting for CallRecsGenerator	12	14-Oct-2004 05:30:08 PM	14-Oct-2004 05:41:46 PM	Events are being processed
	Events waiting for Peak Calculator	0			OK
<p><b>NOTE</b></p> <p>"Flag" and "Comment" columns are based on assumptions made about normal Events Collector processing Characteristics. They may NOT always accurately reflect the current status of the system. This screen is a helper and is NOT a replacement for monitoring traps from EventC.</p> <p><a href="#">Diagnosis XML</a></p>					
<div> <input type="button" value="Refresh"/> <input checked="" type="checkbox"/> Auto Refresh           Refresh Rate (in sec) : <input type="text" value="120"/> <input type="button" value="Save"/> </div>					

**Figure 72: Events Collector Work-in-Progress**

The Flag and Comment columns are based on assumptions made about normal Events Collector processing characteristics. The data in these columns may not always accurately reflect the current status of the system. This page is certainly helpful, but it is not intended as a replacement for monitoring traps from EventC.

The Flag definitions are:

- Red—indicates that a problem has occurred and must be resolved. Check the Comment column for additional information.
- Orange—indicates that a problem might occur. Check the Comment column for additional information.
- Green—indicates that there are no problems.

The [Diagnosis XML](#) link displays this page in xml.

## Event Collector Statistics

To open the Event Collector Statistics page (see [Figure 73](#) on [page 167](#)), expand the Events Collector node in the left frame and then click the Cycle Statistics link.

[illegible]
















### Figure 73: Event Collector Statistics

The Flag and Comment columns are based on assumptions made about normal Events Collector processing characteristics. The data in these columns may not always accurately reflect the current status of the system. This page is certainly helpful, but it is not intended as a replacement for monitoring traps from EventC.

## Event Collector Configuration Test Results

To open the Event Collector Configuration Test Results page (see Figure 74 on [page 168](#)), expand the Events Collector node in the left frame and then click the Check Configuration link.

This page tests the database parameters configured in the `ConfigEventC` section in EMPS and provides the results. It also determines if you have correctly created database objects and if you have created the necessary information in EMPS.

Event Collector Configuration Test - Results		
Flag	Configuration	Comments
	Current Directory	Directory exists : /var/tmp/kandalam/cn/data/current
	Archive Directory	Directory exists : /var/tmp/kandalam/cn/data/archives
	Exception Directory	Directory exists : /var/tmp/kandalam/cn/data/exceptions
	Collector	Connection works
	State Transitions	State Transition Records exist
	Peaks	Connection works
	Peak Control	Peak Control Records exist
	Reporter	Connection works
	Reporter DB Objects	callrecords table exists
	RepDWH	Connection works
	RepDWH DB Objects	billcallrecords table exists
	VWPS Database	Connection works
	VWPS Applications	Application records found
	VCS Servers	VCS Server records found
	DB User Names	All user Ids are unique
<p><b>NOTE</b></p> <p>This Screen tests the Database parameters configured in the ConfigEventC Section in VWPS and provides the results. It also tests if database objects have been created properly and necessary information is created in VWPS</p> <p>This comments column "suggests" the possible reasons for failure based on previous experiences and may not be accurate</p> <p style="text-align: center;"><a href="#">Diagnosis XML</a></p>		
<div> <input type="button" value="Refresh"/> <input checked="" type="checkbox"/> Auto Refresh           Refresh Rate (in sec) : <input type="text" value="120"/> <input type="button" value="Save"/> </div>		

**Figure 74: Event Collector Configuration Test Results**

The Comments column provides the possible reasons for failure based on previous experiences and may not be accurate.

The [Diagnosis XML](#) link displays this page in XML.

## EventC Manager Activity History

To open the EventC Manager Activity History page (see Figure 75 on [page 169](#)), expand the Events Collector node in the left frame and then click the EventC Manager Activity History link.



This page provides the latest ten run dates for load balancing, EventC cleanup, and resetting peaks.














EventC Manager Activity History	
Flag	Run Date
<b>Activity : Load Balancing</b>	
	23-Sep-2004 12:51:23 PM
	21-Sep-2004 07:37:08 PM
	16-Sep-2004 03:36:22 PM
	14-Sep-2004 12:11:07 PM
	14-Sep-2004 12:11:05 PM
<b>Activity : EventC Cleanup</b>	
	24-Sep-2004 01:26:37 AM
	23-Sep-2004 09:18:28 PM
	23-Sep-2004 08:16:33 PM
	23-Sep-2004 07:14:22 PM
	23-Sep-2004 06:12:30 PM
	23-Sep-2004 05:09:02 PM
	23-Sep-2004 04:00:25 PM
<b>Activity : Reset Peaks</b>	
	21-Sep-2004 08:35:32 PM
<b>NOTE</b> This screen list the latest 10 runs for each type of activity This comments column "suggests" the possible reasons for failure based on previous experiences and may not be accurate  <a href="#">Diagnosis XML</a>	
<div> <input type="button" value="Refresh"/> <input checked="" type="checkbox"/> Auto Refresh           Refresh Rate (in sec) : <input type="text" value="120"/> <input type="button" value="Save"/> </div>	

Figure 75: EventC Manager Activity History

## Analyze a Call

To open the Analyze a Call page (see Figure 76 on [page 170](#)), expand the Events Collector node in the left frame and then click the Analyze a Call link.

This page provides information about a call for a particular Session ID. The Session ID, also referred to as the GUID, can be obtained from the CDR files, log files, and downloaded Call Details report.

When multi-tenancy is enabled, this page displays the reseller and customer names. When multi-tenancy is not enabled, this page does not display the reseller and customer names.

---

Note: GVP generates the Session ID.

---

**Analyze a Call**

**Enter Session ID to Analyze :**

☒ **Auto Refresh**

**Refresh Rate (in sec) :**

**Figure 76: Analyze a Call**

To analyze a call, enter the Session ID in the field provided, and then click Search. The events for the call corresponding to that Session ID appear.

If the Session ID is not found, the following message appears:

No Events found in database for this Session ID.  
Reasons may be:  
The Session ID is not valid.  
The Call is old and its records are deleted during cleanup.  
The Call is yet to be processed by EventC

## EventC Manager Advanced Options

To open the EventC Manager Advanced Options page (see Figure 77 on [page 171](#)), expand the Events Collector node in the left frame and then click the Advanced Options link.

This page enables you to reset peaks and to reset the EventC Manager.

---

**Warning!** The operations in this page should be performed by administrators only. Accidental execution corrupts EventC data.

---

**EventC Manager Advanced Options**

**WARNING : The operations in this screen should be performed by administrators only. Accidental execution can cause eventc data to be corrupted.**

**Reset Peaks**

Click on the button below to trigger off peaks reset. The peak reset activity will be scheduled and will take place in the next run cycle of EventC Manager. Check EventC Manager history after about 10 minutes to see if this operation was successful. Peak data in Reporter will be incorrect for a period of upto 6 hours after running this reset.

Trigger Peaks Reset

**Reset EventC Manager Flags**

Click on the button below to trigger off eventc manager flags reset. Its actions are :

1. It clears up load balancer flags so that events loader and callrecsgenerator processes can proceed. If load balancer has errors, these flags are not cleared.
2. It clears up reset peaks flags if its set accidentally.

Note : Running this reset does not affect any normal operations.

Reset EventC Manager Flags

Refresh ☒ Auto Refresh Refresh Rate (in sec) : 120 Save

Figure 77: EventC Manager Advanced Options

## H.323 Session Manager

The H.323 Session Manager routes calls to a SIP-enabled IPCS acting as a user agent server.

### H.323 Session Manager Summary

To open the H.323 Session Manager Summary page (see Figure 78 on [page 172](#)), click the H323 Session Manager link in the left frame or on the Overall Status page. The Summary page displays information about inbound and outbound calls.

**H323 Session Manager Summary**

Name	Value
Summary Table Session Manager Name	h323sessionmanager
Number Of Active Inbound Calls	0
Number Of Active Outbound Calls	0
Total Active Calls	0
Cumulative Inbound Calls Received	0
Cumulative Inbound Calls Answered	0
Cumulative Inbound Calls Aborted	0
Cumulative Inbound Calls Far End Rejected	0
Cumulative Inbound Calls Rejected Timeout	0
Cumulative Inbound Calls Rejected No Resource	0
Cumulative Outbound Calls Attempted	0
Cumulative Outbound Calls Answered	0

☒ Auto Refresh
 Refresh Rate (in sec) :

**Figure 78: H.323 Session Manager Summary**

Table 17 describes the parameters in the H.323 Session Manager Summary page.

**Table 17: H.323 Session Manager Summary Parameters**

Parameter	Description
Summary Table Session Manager Name	Current session manager name.
Number of Active Inbound Calls	Total number of active inbound calls.
Number of Active Outbound Calls	Total number of active outbound calls.
Total Active Calls	Total number of active calls.
Cumulative Inbound Calls Received	Cumulative number of inbound calls received since last restart.
Cumulative Inbound Calls Answered	Cumulative number of inbound calls answered since last restart.
Cumulative Inbound Calls Aborted	Cumulative number of inbound calls aborted before the call is answered since the last restart.
Cumulative Inbound Calls Far End Rejected	Cumulative number of inbound calls rejected by the far end since the last restart.

**Table 17: H.323 Session Manager Summary Parameters (Continued)**

Parameter	Description
Cumulative Inbound Calls Rejected Timeout	Cumulative number of inbound calls rejected due to timeout since the last restart.
Cumulative Inbound Calls Rejected No Resource	Cumulative number of inbound calls rejected due to resource not available since last restart.
Cumulative Outbound Calls Attempted	Cumulative number of outbound requests received from the IPCS.
Cumulative Outbound Calls Answered	Cumulative number of outbound calls answered since the last restart.
Cumulative Outbound Calls Aborted	Cumulative number of outbound calls aborted before the call is answered, since the last restart.
Cumulative Outbound Calls Far End Rejected	Cumulative number of outbound calls rejected by the far end since the last restart.
Cumulative Outbound Calls Rejected Timeout	Number of outbound calls rejected due to timeout since the last restart.
Cumulative Outbound Calls Rejected No Resource	Cumulative number of outbound calls rejected due to no resource available since the last restart.
Total Calls Rejected	Total number of calls rejected.

## H.323 Session Manager Active Calls

To open the H.323 Session Manager Active Calls page, expand the H323 Session Manager node in the left frame and then click the Active Calls link. This page (see Figure 79 on [page 174](#)) displays detailed information on each active call in the network.

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the Customer name column.

**H323 Session Manager Active Calls**

	Customer Name	Application Name	Calling Party	Called Party	Call State	Call Start Time	Current State Start Time	Source Signaling Address	Destination Signaling Address	Call Type
F	serge	CreateLegAndDial	0007000000	3333	Connected	1059697854	1059697854	10.10.16.38:5060	10.10.16.2:1720	Outbound
F	serge	CreateLegAndDial	0001400000	3333	Connected	1059697856	1059697856	10.10.16.38:5060	10.10.16.2:1720	Outbound
F	serge	CreateLegAndDial	0001300000	3333	Connected	1059697858	1059697858	10.10.16.38:5060	10.10.16.2:1720	Outbound
95	serge	CreateLegAndDial	0002100000	370005	Bridging	1059697818	1059697849	10.10.16.2:1720	10.10.16.38:5060	Inbound
95	serge	CreateLegAndDial	0004000000	370005	Connected	1059697834	1059697847	10.10.16.2:1720	10.10.16.38:5060	Inbound
95	serge	CreateLegAndDial	0001000000	370005	Bridging	1059697834	1059697847	10.10.16.2:1720	10.10.16.38:5060	Inbound
5	serge	CreateLegAndDial	0007000000	370005	Connected	1059697834	1059697848	10.10.16.2:1720	10.10.16.38:5060	Inbound
15	serge	CreateLegAndDial	0001000000	370005	Connected	1059697834	1059697848	10.10.16.2:1720	10.10.16.38:5060	Inbound
95	serge	CreateLegAndDial	0002200000	370005	Connected	1059697835	1059697849	10.10.16.2:1720	10.10.16.38:5060	Inbound
95	serge	CreateLegAndDial	0001400000	370005	Connected	1059697835	1059697849	10.10.16.2:1720	10.10.16.38:5060	Inbound
5	serge	CreateLegAndDial	0003000000	370005	Connected	1059697836	1059697849	10.10.16.2:1720	10.10.16.38:5060	Inbound
5	serge	CreateLegAndDial	0008000000	370005	Connected	1059697838	1059697853	10.10.16.2:1720	10.10.16.38:5060	Inbound
95	serge	CreateLegAndDial	0001300000	370005	Connected	1059697838	1059697852	10.10.16.2:1720	10.10.16.38:5060	Inbound
95	serge	CreateLegAndDial	0001100000	370005	Connected	1059697838	1059697853	10.10.16.2:1720	10.10.16.38:5060	Inbound
95	serge	CreateLegAndDial	0001200000	370005	Connected	1059697847	1059697847	10.10.16.2:1720	10.10.16.38:5060	Inbound
5	serge	CreateLegAndDial	0009000000	370005	Connected	1059697847	1059697847	10.10.16.2:1720	10.10.16.38:5060	Inbound
5	serge	CreateLegAndDial	0002000000	370005	Connected	1059697854	1059697854	10.10.16.2:1720	10.10.16.38:5060	Inbound

☒ Auto Refresh
 Refresh Rate (in sec) :

**Figure 79: H.323 Session Manager Active Calls**

Table 18 describes the parameters in the H.323 Session Manager Active Calls page.

**Table 18: H.323 Session Manager Active Calls Parameters**

Parameter	Description
Session ID	Unique ID that the HSM assigns to each call. The session ID is the same for each leg of the call.
Call Leg ID	Current call leg identification for the call.
Customer Name	Name of the customer.
Application Name	Name of the voice application.
Calling Party	Number of the calling party.
Called Party	Number of the party called.

**Table 18: H.323 Session Manager Active Calls Parameters (Continued)**

Parameter	Description
Call State	State of the call: <ul style="list-style-type: none"> <li>Offering—call is being processed</li> <li>Accepted—call is accepted</li> <li>Connected—call is answered</li> <li>Disconnected—call is currently terminating</li> </ul>
Call Start Time	Start time of the call.
Current State Start Time	Start time of the current call state.
Source Signaling Address	Source address.
Destination Signaling Address	Destination address.
Call Type	Type of the call; inbound or outbound.

## Configuration

To open the H.323 Session Manager Configuration page (see [Figure 80](#)), expand the H323 Session Manager node in the left frame, and then click the Configuration link. This page displays configuration information.

**H323 Session Manager Configuration**

Name	Value
Configuration Table Session Manager Name	h323sessionmanager
SIP Address	10.10.16.17:5060
Address	10.10.16.17:1720
Gatekeeper Address	No Gatekeeper
Resource Manager Address	10.10.16.17:5070

☒ Auto Refresh
 Refresh Rate (in sec) :

**Figure 80: H.323 Session Manager Configuration**

Table 19 describes the parameters in the H.323 Session Manager Configuration page.

**Table 19: H.323 Session Manager Configuration Parameters**

Parameter	Description
Configuration Table Session Manager Name	Current H.323 Session Manager name.
SIP Address	Local SIP IP address and signaling port.
Address	Local H.323 IP address and signaling port.
Gatekeeper Address	The gatekeeper IP address and signaling port.
Resource Manager Address	Address of the Resource Manager.

## IP Communication Server

This section describes the EMS GUIs for the IP Communication Server (IPCS).

### IPCS Call Summary

Click the IPCS link in the left frame or on the Overall Status page to open the IPCS Call Summary page (see Figure 81).

IPCS Call Summary	
Name	Value
Summary Table Process Id	5776
Total Inbound Calls Answered	64653
Total Outbound Calls Answered	44593
Total Inbound Calls Rejected	0
Total Outbound Calls Rejected	19993
Total Inbound Calls Active	1
Total Outbound Calls Active	0
Avg Inbound Calls Duration	15
Avg Outbound Calls Duration	17
Total Inbound Channels	0
Total Outbound Channels	0
Total In Outbound Channels	200
Out REFERAttempts	0
Out REFERSuccess	0
Out REFERFailure	0

☒ Auto Refresh
 Refresh Rate (in sec) :

**Figure 81: IPCS Call Summary**



[Table 20](#) describes the parameters in the IPCS Call Summary page.

**Table 20: IPCS Call Summary Parameters**

Parameter	Description
Summary Table Process ID	Process ID of PopGateway process.
Total Inbound Calls Answered	Number of inbound calls that reached the answer state.
Total Outbound Calls Answered	Number of outbound calls that reached the answer state.
Total Inbound Calls Rejected	Number of inbound calls that were not answered.
Total Outbound Calls Rejected	Number of outbound calls that were not answered.
Total Inbound Calls Active	Current count of active inbound calls.
Total Outbound Calls Active	Current count of active outbound calls.
Avg Inbound Calls Duration	The average number of seconds an inbound call is active.
Avg Outbound Calls Duration	The average number of seconds an outbound call is active.
Total Inbound Channels	Total number of channels from all routes dedicated to handling inbound calls.
Total Outbound Channels	Total number of channels from all routes dedicated to handling outbound calls.
Total In-/Outbound Channels	Total number of channels from all routes configured to handle both inbound or outbound calls.
OutReferAttempts	Number of calls that were attempted to be transferred out using SIP REFER.
OutReferSuccess	Number of calls that were successfully transferred out using SIP REFER.
OutreferFailure	Number of calls that failed to be transferred out using SIP REFER.

## Routes

Click the Routes link in the left frame to open the IPCS Routes page, which provides detailed information on IPCS routes (see [Figure 82](#)).

[illegible]

### Figure 82: IPCS Routes

Table 21 describes the parameters in the IPCS Routes page.

### Table 21: IPCS Routes Parameters

Parameter	Description
Route Table Process ID	Process ID of PopGateway process.
Route ID Number	Logical number of route, unique per PopGateway process.
Route Description	User-friendly text description of route.
Route Type	Direction of call that all the channels from this route can process. Possible values are Inbound, Outbound, or InOut.
Route Signaling	Signaling protocol. Currently, this is always SIP (Session Initiation Protocol).
Route Channel IDs	Range of logical IDs channels that are members of this route.
Route Channels	Number of channels configured for this route.

## Call Flow Assistant

The Call Flow Assistant (CFA) is the interface that initiates an outbound call request and communicates authorizing instructions from the Element Management Provisioning System (EMPS) to the IPCS.

The CFA communicates with the IVR Server Client and Cisco Queue Adapter (optional feature). The CFA also provides certain information to the Policy Manager.

### Call Flow Assistant Statistics

Click the CFA link to open the Call Flow Assistant Statistics page (see [Figure 83](#)), which displays information about currently active calls on the IPCS.

Call Flow Assistant Statistics	
Name	Value
Active Calls	0
Active Calls to Primary IVR	0
Active Calls to Backup IVR	0
Active Calls to Primary PM	0
Active Calls to Backup PM	0

☒ Auto Refresh
 Refresh Rate (in sec) :

**Figure 83: Call Flow Assistant Statistics**

[Table 22](#) describes the parameters in the Call Flow Assistant Statistics page.

**Table 22: CFA Statistics Parameters**

Parameter	Description
Active Calls	Number of active calls for the CFA.
Active Calls to Primary IVR	Number of calls that the CFA directed to the primary IVR URL.
Active Calls to Backup IVR	Number of calls that the CFA redirected to the backup IVR URL.

**Table 22: CFA Statistics Parameters (Continued)**

Parameter	Description
Active Calls to Primary PM	Number of calls for which the CFA contacted the primary Policy Manager (PM) for policy management.
Active Calls to Backup PM	Number of calls for which the CFA contacted the backup PM for policy management.

## Active Sessions

Click the **Active Sessions** link to open the **Call Flow Assistant Active Sessions** page, which displays the number of currently active calls on the CFA (see [Figure 84](#)).

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the **Customer name** column.

Call Flow Assistant Active Sessions

Voice Application	Dialed Number	DNIS	ANI	Call Start	Call State	Current Call State Start	Server Process
CCodec	6324342	5557084045	Anonymous	Jan 09, 2007 2:06:40 PM	bridged	Jan 09, 2007 2:06:43 PM	PopGateway1

[Refresh](#)
☒ Auto Refresh
Refresh Rate (in sec) : 
[Save](#)

**Figure 84: Call Flow Assistant Active Sessions**

[Table 23](#) describes the parameters in the **Call Flow Assistant Active Sessions** page.

**Table 23: CFA Active Sessions Parameters**

Parameter	Description
Voice Application	Name of the voice application.
Dialed Number	Toll-free number dialed.

**Table 23: CFA Active Sessions Parameters (Continued)**

Parameter	Description
DNIS	Direct Number Identification Service.
ANI	Number of the calling party.
Call Start	Time that the call starts.
Call State	<p>Current state of the call. The call states are:</p> <ul style="list-style-type: none"> <li>• <b>Answered</b>—the platform has answered and accepted the call. It is currently executing the voice application.</li> <li>• <b>Bridged</b>—the call has been bridged to an agent on the platform.</li> <li>• <b>Queued</b>—the call has been put into a queued state, awaiting the availability of an agent.</li> <li>• <b>Agent Connecting</b>—the call is in the process of being connected to the agent. The agent phone may be ringing in this case, but has not yet been picked-up.</li> <li>• <b>Agent Connected</b>—indicates that the agent has answered his or her phone, but the call is yet to be bridged.</li> </ul>
Current Call State Start	Date and time the call state started.
Server Process	PopGateway handling the call.
Session ID	Unique ID of the call.

---

## IVR Server Client

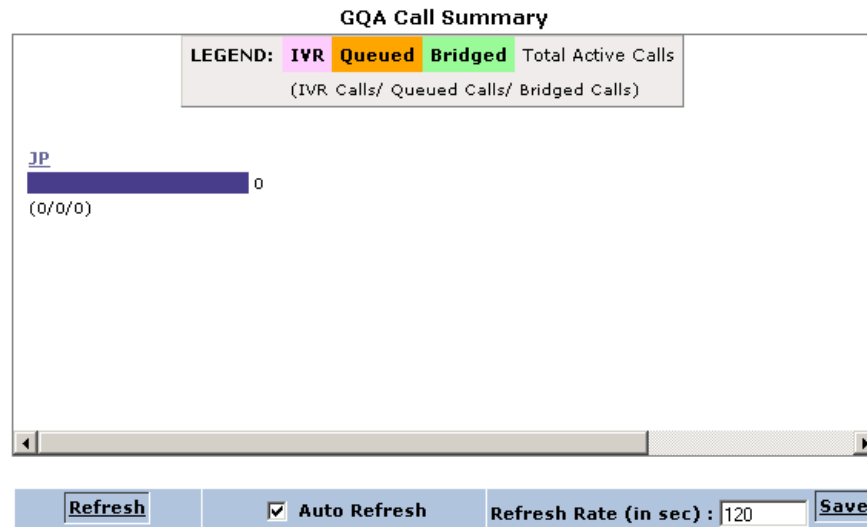
The IVR Server Client communicates with a customer's Genesys Universal Routing Server (URS) through the IVR Server. The IVR Server Client passes information between GVP and the URS.

### IVR Server Client Call Summary

To open the IVR Server Client Call Summary page (see Figure 85 on [page 182](#)), click the Genesys Queue Adapter link in the left frame or on the Overall Status page. The summary displays information about the IVR Server Client and its connection to the various IVR Servers.

When multi-tenancy is enabled, the Call Summary page displays the IVR/Queued and Bridged calls for the customer. When multi-tenancy is not

enabled, the Call Summary page displays the IVR/Queued and Bridged calls for voice application.



**Figure 85: IVR Server Client Call Summary**

The number of active calls displays to the right of the bar, and the state of the active calls displays as a fraction underneath the bar. For example, 43/10/21 means that of the 74 active calls, 43 of them are IVR, 10 are Queued, and 21 are Bridged.

A legend at the top of the page explains the color coding.

## Connection Status

To open the IVR Server Client Connection Status page, expand the IVR Server Client node in the left frame and then click the Connection Status link. The IVR Server Client Connection Status page displays the connection status for each IVR Server Client and its IVR Server (see Figure 86 on [page 183](#)).

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the Customer name column.

GQA Connection Status				
IQA Server Address	IQA Port	IQA Connection State	Total No. of Network Failures	Last Failure Date / Time
10.10.100.79	7849	Connected	0	
10.10.00.00	8001	Disconnected	0	
10.10.100.79	7849	Connected	0	

**Figure 86: IVR Server Client Connection Status**

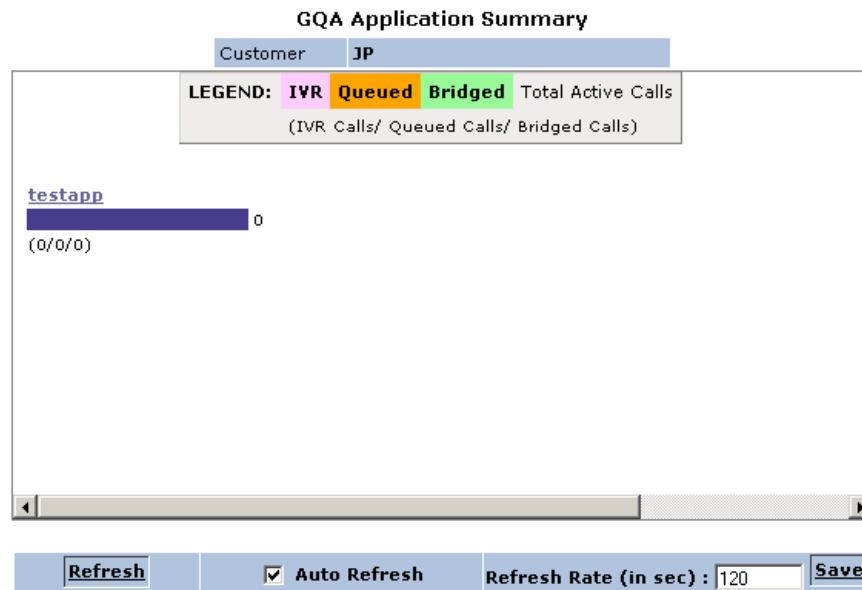
Table 24 describes the parameters in the IVR Server Client Call Volume page.

### Table 24: IVR Server Client Call Volume Parameters

Parameter	Description
IQA Server Address	IP address of the IVR Server.
IQA Port	The port on which this IVR Server is listening for client connections.
IQA Connection State	Connection status to the IVR Server. Value is <b>Connected</b> or <b>Disconnected</b> .
Total No. of Network Failures	Cumulative number of network failures to the IVR Server.
Last Failure Date/Time	Date and time at which the last network failure occurred.

## IVR Server Client Application Summary

To open the IVR Server Client Application Summary page (see Figure 87 on [page 184](#)), click that customer's link in the left frame or click that customer's link on the IVR Server Client Call Summary page. The Application Summary page displays call statistics for the selected customer.



**Figure 87: IVR Server Client Application Summary**

Each voice application for that customer then has a link to its own statistics—Active Calls and Call Volume.

## Active Calls

The IVR Server Client Active Calls page (see Figure 88 on [page 185](#)) displays active call information for the voice application.

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the Customer name column.



**GQA - Active Calls**

Customer	JP
Application	testapp

Switch to : [Call Volume](#)

DNIS	ANI	Session State	Current Script	Session ID
No Data Available				

No Data Available

Refresh ☒ Auto Refresh Refresh Rate (in sec) : 120 Save

**Figure 88: IVR Server Client Active Calls**

[Table 25](#) describes the parameters in the IVR Server Client Active Calls page.

**Table 25: IVR Server Client Active Calls Parameters**

Parameter	Description
DNIS	Dialed Number Identification Service provided with the incoming call.
ANI	Automatic Number Identification of the caller.
Session State	Current state of the call. Possible states are: <ul style="list-style-type: none"> <li>• NewCallRecvd</li> <li>• QueueCallRecvd</li> <li>• ConnectRecvd</li> </ul>
Current Script	Current active script name of the session.
Session ID	Identification of the session.

## Call Volume

The IVR Server Client Call Volume page (see [Figure 89](#) on [page 186](#)) displays call volume information for the voice application.

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the Customer name column.

**GQA - Call Volume**

Customer	JP
Application	testapp

Switch to : [Active Calls](#)

Name	Value
Number of active sessions	0
Number of active sessions in queue	0
Number of active sessions bridged	0

[Refresh](#)
☒ Auto Refresh
Refresh Rate (in sec) :  [Save](#)

**Figure 89: IVR Server Client Call Volume**

[Table 26](#) describes the parameters in the IVR Server Client Call Volume page.

**Table 26: IVR Server Client Call Volume Parameters**

Parameter	Description
Number of active sessions	Current number of active calls for a specific voice application in IVR Server Client.
Number of active sessions in queue	Current number of active calls that are waiting to be transferred to an agent.
Number of active sessions bridged	Current number of active calls that have been transferred to an agent.

## MRP SMP Integrator

This section describes the Element Management GUIs for the MRP SMP Integrator component.

## Agent Summary

To open the Agent Summary page (see [Figure 90](#)), in the left frame, expand the SNMP Management node, and then click the Agent Summary link. This page displays information about the SNMP agents that are configured as a part of the MRP SMP Integrator.

**Agent Summary**

Agent Name	Select
che151	<input type="checkbox"/>
che172	<input type="checkbox"/>
sdfds	<input type="checkbox"/>

---

☒ Auto Refresh Refresh Rate (in sec) :

**Figure 90: Agent Summary**

From the Agent Summary screen, you can add, delete, or trigger SNMP agents as required.

To add an SNMP Agent:

1. On the Agent Summary page, click Add Agent. The Add Agent page appears (see [Figure 91](#)).

**Agent Summary**

Agent Name	<input type="text"/>
IP Address	<input type="text"/>
Port	<input type="text"/>

---

☒ Auto Refresh Refresh Rate (in sec) :

**Figure 91: Add Agent Summary Screen**

2. In the Agent Name box, enter the name of the Agent.

3. In the IP Address box, enter a valid IP address for the Agent.
4. In the Port box, enter the port of the Agent.
5. Click Submit to add the new Agent.

---

Note: You must give access rights to the `/opt/genesys/gvp/cn/config` directory in order to view the new Agent. For more information, see the *Genesys Voice Platform 7.6 Deployment Guide*.

---

#### To delete an SNMP Agent:

1. On the Agent Summary page, select the check box next to each agent that you want to delete.
2. Click Delete Agent.

#### To trigger an SNMP Agent's statistics:

Statistics collection from all configured SNMP Agents is triggered by using the Trigger All option on the Agent Summary page.

## <Agent> Summary

To open the <Agent> Summary page (see Figure 92 on [page 188](#)), in the left frame, expand the Agent Summary node, and then click on the <agent>. This page displays information about the selected Agent.

che151 Summary

Please select to delete

MIB	Select
CCM-MIB	<input type="checkbox"/>
CCXML-MIB	<input type="checkbox"/>
CFC-MIB	<input type="checkbox"/>
CALLSTATS-MIB	<input type="checkbox"/>
H323-MIB	<input type="checkbox"/>
IQA-MIB	<input type="checkbox"/>
OBM-MIB	<input type="checkbox"/>
OSR-MIB	<input type="checkbox"/>
RM-MIB	<input type="checkbox"/>
SSM-MIB	<input type="checkbox"/>
TTS-MIB	<input type="checkbox"/>

Refresh
☒ Auto Refresh
Refresh Rate (in sec) : 
Save

**Figure 92: Selected Agent Summary**

To configure an SNMP Agent's MIBs:

1. On the <Agent> Summary page, select the check box next to each MIB that you want to omit from the configuration.
2. Click **Continue**. The MIB Parameters screen appears, displaying a detailed list of the scalar and vector parameters present in each selected MIB.
3. Select the check box next to each MIB parameter that you want to omit from the configuration.
4. Click **Trigger** to begin the collection of the Agent's statistics.
5. Click **Submit** to save the Agent's configuration.

---

**Note:** All of the MRP SMP Integrator's MIBs that are planned for traps or statistics collection must be copied to a local directory with the extension .txt on the machine where the MRP SMP Integrator is installed. The path where the MIBs are copied must be exported to the MIBSDIRS environment variable using the `MIBSDIRS=/opt/genesys/gvp/snmp/share/MIBS` command.

---

---

## OBN Manager

This section describes the EMS GUI for the Outbound Notification Manager (OBN Manager).

### OBN Manager Summary Page

[Figure 93](#) shows the OBN Manager Summary page, which displays a set of statistics about Outbound Notification Manager.

To open the OBN Manager Summary page:

In the left frame, click the **OBN Manager** link. The OBN Manager Summary page appears in the right frame.

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the **Customer name** column.

OBN Manager Summary									
Customer	Application	Requests in Queue	Requests Completed	Failed Requests with retry count exceeded	Failed Requests with Time-to-Live exceeded	Avg. Time to Complete a Request	Avg. retries per Request	Last request received	Last request dequeued
OBNSigC	OBNAApp1	0	0	0	0	0	0		
OBNQATests	QAApp1	0	0	0	0	0	0		

**Table 27: OBN Manager Summary Parameters (Continued)**

Parameter	Description
Last Request Received	Exact time at which the last request was received.
Last Request Dequeued	Exact time at which the last request was dequeued.

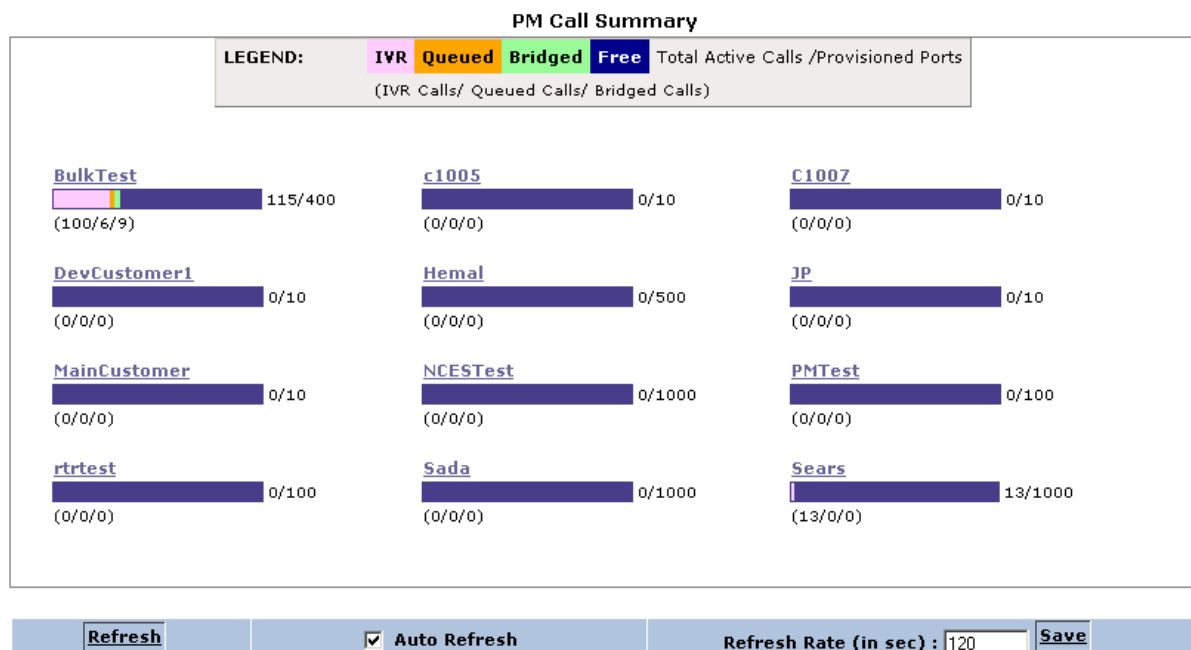
## Policy Manager

The Policy Manager (PM) maintains a list of ports allocated to each customer and each customer's voice application. The PM uses that data to decide whether to accept a call.

### Policy Manager Summary

To open the PM Call Summary page, click the Policy Manager link in the left frame or click the Policy Manager link on the Overall Status page. The PM Summary page (see Figure 94 on [page 191](#)) displays the customers, provisioned ports, and call status.

When multi-tenancy is enabled, the Overall Status page displays the active/total customers. When multi-tenancy is not enabled, the Overall Status page displays the active/total applications.

**Figure 94: Policy Manager Call Summary**

The number of active customer ports displays in a bar as a fraction of the number of available customer ports. For example, 115/400 means that the customer has 400 available ports, 115 of which are active.

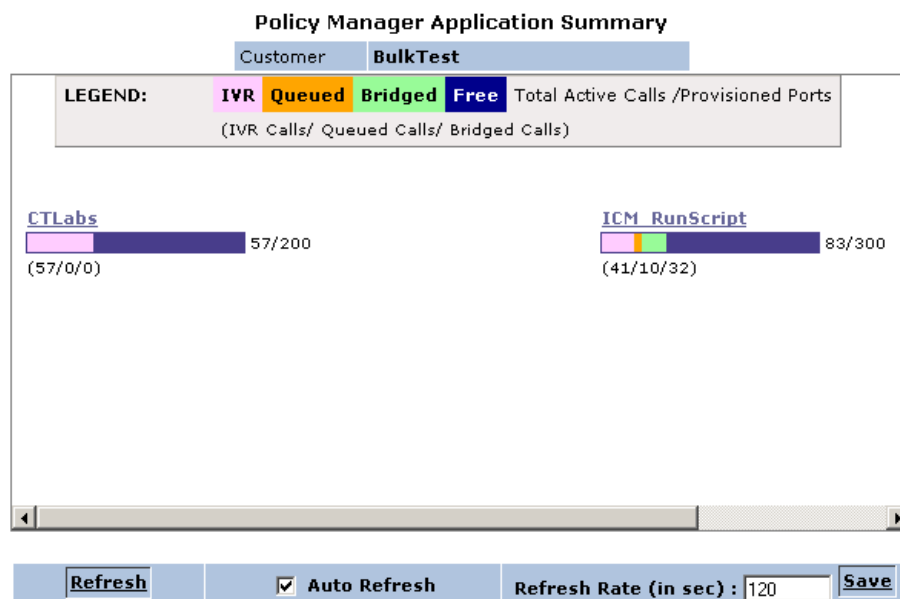
The state of the active port displays as a fraction underneath the bar. For example, 100/6/9 means that of the 115 active ports, 100 of them are IVR, 6 are Queued, and 9 are Bridged.

A legend at the top of the page explains the color coding.

## Policy Manager Application Summary

To open the Policy Manager Application Summary page (see Figure 95 on [page 192](#)) for a specific customer, expand the Policy Manager node in the left frame and then click the desired customer link. Or, you can click the desired customer link on the PM Call Summary page. The Application Summary page displays the provisioned ports and call status for the selected customer.

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the Customer name column.



**Figure 95: Policy Manager Application Summary**

A legend at the top of the page explains the color coding.

Each voice application then has a link to its own statistics—Active Calls and Call Volume.



## Active Calls

The Policy Manager Active Calls page (see [Figure 96](#)) displays information on active calls for this customer/voice application.

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the Customer name column.

**Policy Manager - Active Calls**

Customer	PMTTest
Application	TestApp

Switch to : [Call Volume](#)

ANI	DNIS	Toll Free Num	Start Time (GMT)	Call State	Current State Start Time (GMT)	Session ID	POP Server	POP Gateway
No Data Available								

Refresh
☒ Auto Refresh
Refresh Rate (in sec) : 
Save

**Figure 96: Policy Manager - Active Calls**

[Table 28](#) describes the parameters in the Policy Manager Active Calls page.

**Table 28: Policy Manager - Active Calls Parameters**

Parameter	Description
ANI	Caller ID of the calling party.
DNIS	Number dialed by the calling party.
Toll Free Number	The toll free number the calling party dialed.
Start Time (GMT)	Time when this call began.
Call State	Current state of the call.
Current State Start Time (GMT)	Start time when the call entered the current call state.

**Table 28: Policy Manager - Active Calls Parameters (Continued)**

Parameter	Description
Session ID	Unique identifier to identify this call on GVP.
POP Server	URL of the VCS/IPCS machine where this call was received.
POP Gateway	Module on the VCS/IPCS machine that is handling this call.

## Call Volume

The Policy Manager Call Volume page (see [Figure 97](#)) displays information on customer/voice application call volume.

When multi-tenancy is enabled, this page displays the customer names. When multi-tenancy is not enabled, this page does not display the Customer name column.

**Policy Manager - Call Volume**

Customer	PMTest
Application	TestApp

Switch to : [Active Calls](#)

Name	Value
Time of Last Restart	Jul 29, 2003 2:32:30 PM
Total Inbound Calls	0
Total Outbound Calls	0
Provisioned Number of Sessions	100
Total Number of Sessions	0
Total Number of Sessions Rejected	0
Session Peak Volume	0
Time of Session Peak Volume	Jul 29, 2003 2:32:30 PM
Session Heavy Usage Duration	0
Session Heavy Usage Threshold	80
All Provisioned Sessions Busy Trap Threshold	95
All Provisioned Sessions Not Busy Trap Threshold	90
Total Number of Bridged Sessions	0
Total Number of Queued Sessions	0
Provisioned ASR Samples	0
ASR Samples Captured	0

Refresh
☒ Auto Refresh
Refresh Rate (in sec) : 
Save

**Figure 97: Policy Manager - Call Volume**

Table 29 describes the parameters in the Policy Manager Call Volume page.

**Table 29: Policy Manager - Call Volume Parameters**

Parameter	Description
Time of Last Restart	Last time the Policy Manager module was restarted.
Total Inbound Calls	Total number of inbound calls processed by this PM.
Total Outbound Calls	Total number of outbound calls processed by this PM.
Provisioned Number of Sessions	Number of simultaneous calls allowed for this customer/voice application.
Total Number of Sessions	Total numbers of sessions processed by this PM.
Total Number of Sessions Rejected	Number of calls rejected for this customer/voice application.
Session Peak Volume	Highest number of simultaneous calls processed for this customer/voice application.
Time of Session Peak Volume	Time at which the peak appeared.
Session Heavy Usage Duration	Time for how long the peak lasted.
Session Heavy Usage Threshold	This determines what percentages of calls a particular customer should reach before the heavy usage threshold trap is generated.  For example if a customer has been allocated 100 ports and their Session Heavy Usage Threshold is set to a value of 80, when this customer receives 80 simultaneous calls, a trap will be sent just to warn the operator that this particular customer may be reaching their total allocated ports.
All Provisioned Sessions Busy Trap Threshold	The threshold value at which the PM generates a trap that indicates the peak is nearing. This is basically an alert to the operator that the customer may be running out of provisioned ports.

**Table 29: Policy Manager - Call Volume Parameters (Continued)**

Parameter	Description
All Provisioned Sessions Not Busy Trap Threshold	This value suggests that simultaneous calls have fallen below the alert level. A trap is issued when this occurs.
Total Number of Bridged Sessions	Total number of calls currently in bridged states.
Total Number of Queued Sessions	This is the cumulative number of sessions that went into Queued state for that customer.
Provisioned ASR Samples	This is the number of ASR samples that a customer voice application(s) can collect on the GVP in a day.
ASR Samples Captures	This is the total number of ASR samples that were collected so far for this customer.

---

## Resource Manager

The Resource Manager provides IP Communication Server and Media Gateway availability information to the SIP Session Manager and to the H.323 Session Manager. The Resource Manager can also work as a SIP Redirect Server. This mode is used while working with Genesys SIP Server.

In the EMS GUI, when you expand Resource Manager, all of the devices (Media Gateways and IPCSs) that are registered with the Resource Manager are displayed. When you click on any of these devices, the central pane displays the device properties for that particular device. There is a common set of properties as well as specific properties.

---

**Note:** The Resource Manager supports ten properties per device.

---

## Resource Manager Summary

To open the Resource Manager Summary page (see Figure 98 on [page 197](#)), click the Resource Manager link in the left frame or on the Overall Status page. The Summary page displays the number of active ports out of the total provisioned ports per device.

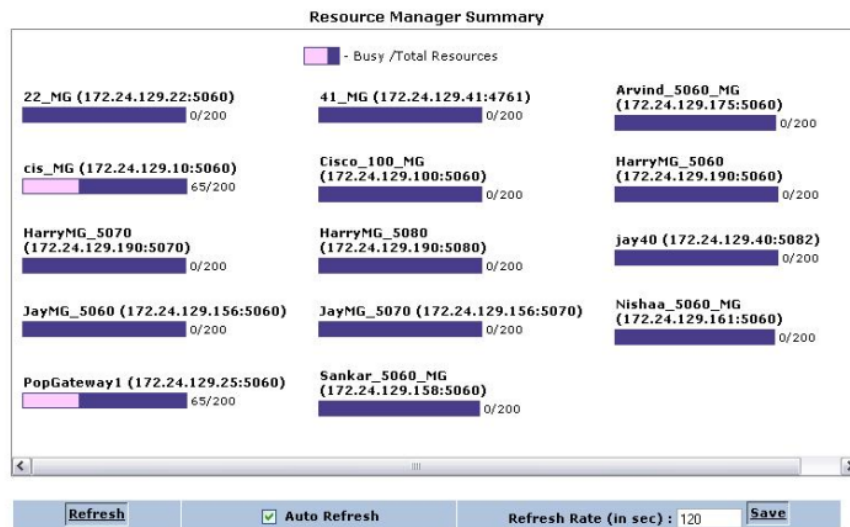


Figure 98: Resource Manager Summary

A legend at the top of the page explains the color coding.

## Resource Manager Configuration

To open the Resource Manager Configuration page (see Figure 99), expand the Resource Manager node in the left frame and click the Configuration link. The Configuration page displays configuration information.

Resource Manager Configuration	
Name	Value
SIP Port	5070
SIP Transport Protocol	UDP
SIP Version	2.0
Database Server Address	10.10.102.7
Database User ID	sa
Database Password	
Database Name	ResourceManager

Buttons: Refresh, ☒ Auto Refresh, Refresh Rate (in sec) : 120, Save

Figure 99: Resource Manager Configuration

Table 30 describes the parameters in the Resource Manager Configuration page.

**Table 30: Resource Manager Configuration Parameters**

Parameter	Description
SIP Port	Port of the SIP.
SIP Transport Protocol	Transport protocol of the SIP.
SIP Version	Version of SIP protocol.
Database Server Address	IP address of the database server.
Database User ID	Not applicable for this release.
Database Password	Not applicable for this release.
Database Name	Not applicable for this release.

## Media Gateway Properties

To open the <Media Gateway> Properties page (see Figure 100), expand the Resource Manager node in the left frame and click the <Media Gateway> link. This page displays the Media Gateway properties.

**rcc\_sipp(10.10.10.223:5062) - Properties**

Name	Value
porttype	pstn
direction	inout
provider	nch
devicecost	0

☒ Auto Refresh

Refresh Rate (in sec) :

**Figure 100: <Media Gateway> Properties**

Table 31 describes the parameters in the <Media Gateway> Properties page.

**Table 31: Media Gateway Properties Parameters**

Parameter	Description
porttype	Specifies a value of pstn, which is a standard value for any Media Gateway.
direction	Specifies the direction of the call as supported by the Media Gateway. The value can be: <ul style="list-style-type: none"> <li>inbound</li> <li>outbound</li> <li>inout</li> </ul>
provider	Specifies optional information, typically the provider name.
devicecost	This value is always 0 for the Media Gateway.

## IPCS/PopGateway Properties

To open the IPCS/PopGateway Properties page (see Figure 101), expand the Resource Manager node in the left frame and click the IPCS/PopGateway link. This page displays the IPCS/PopGateway properties.

**PopGateway1(10.10.30.138:5060) - Properties**

Name	Value
porttype	telera
direction	inout
asr	asr
devicecost	0
featurelist	pcmu:0

Refresh
☒ Auto Refresh
Refresh Rate (in sec) : 
Save

**Figure 101: IPCS/PopGateway Properties**

[Table 32](#) describes the parameters in the IPCS/PopGateway Properties page.

**Table 32: IPCS/PopGateway Properties Parameters**

Parameter	Description
porttype	Specifies the port type as telera (this is standard value for any IPCS).
direction	Specifies the direction of the call as supported by the IPCS. The value can be: <ul style="list-style-type: none"> <li>inbound</li> <li>outbound</li> <li>inout</li> </ul>
asr	Specifies the ASR support information. The value can be: <ul style="list-style-type: none"> <li>dtmf—no ASR support</li> <li>asr—ASR support</li> </ul>
devicecost	Specifies the type of media support for the IPCS. The value can be: <ul style="list-style-type: none"> <li>0—IPCS with basic media support</li> <li>100—IPCS with enhanced media support</li> </ul>
featurelist	Specifies the media and other feature support for the IPCS. The value depends entirely on the IPCS configuration.

## SIP Session Manager

The Session Initiation Protocol (SIP) Session Manager (SSM) acts as a SIP proxy to relay SIP messages between the Media Gateway or SoftSwitch and IP Communication Servers (IPCSs).

### SIP Session Manager Summary

To open the SIP Session Manager Summary page (see Figure 102 on [page 201](#)), click the SIP Session Manager link in the left frame or on the Overall Status page. The Summary page displays information about inbound and outbound calls.



**SIP Session Manager Summary**

Name	Value
Session Manager Name	SIPSessionManager
No. of Active Sessions (Total)	74
No. of Active Inbound Sessions	60
No. of Active Outbound Sessions	14
Cumulative Rejected Calls due to Timeout	0
Cumulative Rejected Calls due to no Resource	175
Cumulative Rejected Calls (total)	175

☒ Auto Refresh
 Refresh Rate (in sec) : 120

**Figure 102: SIP Session Manager Summary**

[Table 33](#) describes the parameters in the SIP Session Manager Summary page.

**Table 33: SIP Session Manager Summary Parameters**

Parameter	Description
Session Manager Name	Name of the running SSM process.
No. of Active Sessions (Total)	Total number of active calls.
No. of Active Inbound Sessions	Total number of active inbound calls.
No. of Active Outbound	Total number of active outbound calls.
Cumulative Rejected Calls Due to Timeout	Cumulative number of calls rejected due to IPCS timeout.
Cumulative Rejected Calls Due to No Resource	Cumulative number of calls rejected due to no resource available.
Cumulative Rejected Calls (total)	Sum of Calls Rejected Timeout and Call Rejected No Resource.

## SIP Session Manager Active Calls

To open the SIP Session Manager Active Calls page (see [Figure 103 on page 202](#)), expand the SIP Session Manager node in the left frame and then click the Active Calls link. This page displays information about active calls.

**SIP Session Manager Active Calls**

Session ID	Application Name	Sip From	Sip To
04CF0133-B9B2-43CD-99E0-7838CCE707A4	transfer	sip:123456789@172.24.129.10	sip:6261397@172.24.129.10
05CA6546-AB23-4F30-8731-733744E838D9	transfer	sip:123456789@172.24.129.10	sip:6261397@172.24.129.10
080F267B-8A29-42DC-AB7E-4044F9CEDF4A	transfer	sip:123456789@172.24.129.10	sip:6261397@172.24.129.10
080F267B-8A29-42DC-AB7E-4044F9CEDF4A	transfer	sip:123456789@172.24.129.25:5060	sip:601@172.24.129.10:5060
08A4F33F-A61B-4598-BF6D-BAAA5C746470	transfer	sip:123456789@172.24.129.10	sip:6261397@172.24.129.10
08A4F33F-A61B-4598-BF6D-BAAA5C746470	transfer	sip:123456789@172.24.129.25:5060	sip:601@172.24.129.10:5060
0D85D170-9E05-47E3-BDB7-8CD8B9D8565D	transfer	sip:123456789@172.24.129.10	sip:6261397@172.24.129.10
0D85D170-9E05-47E3-BDB7-8CD8B9D8565D	transfer	sip:123456789@172.24.129.25:5060	sip:601@172.24.129.10:5060
191D3484-7981-4816-BB86-C105794D561D	transfer	sip:123456789@172.24.129.10	sip:6261397@172.24.129.10
1D1FA7B9-0A86-4BA0-8FA2-42BEDEE6D831	transfer	sip:123456789@172.24.129.10	sip:6261397@172.24.129.10
261D39EE-05E6-4B4F-83AA-6B67EF26D2F0	transfer	sip:123456789@172.24.129.10	sip:6261397@172.24.129.10
298B606A-CEBF-4B24-ABA8-3A6147DAB9A3	transfer	sip:123456789@172.24.129.10	sip:6261397@172.24.129.10
298B606A-CEBF-4B24-ABA8-3A6147DAB9A3	transfer	sip:123456789@172.24.129.25:5060	sip:601@172.24.129.10:5060
2C0A27D8-2EBE-4198-8C9B-28A5D5C271A9	transfer	sip:123456789@172.24.129.10	sip:6261397@172.24.129.10

☒ Auto Refresh
 Refresh Rate (in sec) : 120

**Figure 103: SIP Session Manager Active Calls**

Note: When multi-tenancy is enabled, this page displays the customer names. When multi-tenancy is not enabled, this page does not display the Customer name column.

Table 34 describes the parameters in the SIP Session Manager Active Calls page.

**Table 34: SIP Session Manager Active Calls Parameters**

Parameter	Description
Session ID	Session identification.
Application Name	Name of the voice application for this call.
SIP From	Source address of this call.
SIP To	Destination address of this call.
SIP Call ID	Unique call identifier.
Call State	State of the call: <ul style="list-style-type: none"> <li>Offering—call is being processed</li> <li>Accepted—call is accepted</li> <li>Connected—call is answered</li> <li>Disconnect—call is currently terminating</li> <li>Unknown—state of call is not known</li> </ul>

**Table 34: SIP Session Manager Active Calls Parameters (Continued)**

Parameter	Description
Start Time	Start time of the call.
Source Address	IP address from which the call originated.
Destination IP Address	Address to which the call is routed.
Call Type	Inbound or outbound.

## SIP Session Manager Configuration

To open the SIP Session Manager Configuration page (see [Figure 104](#)), expand the SIP Session Manager node in the left frame and then click the Configuration link. This page displays configuration information.

**SIP Session Manager Configuration**

Name	Value
SIP Session Manager Name	SIPSessionManager
SIP Port	5060
SIP Transport Protocol	UDP
SIP Version	2.0
SIP IP Address	172.24.129.62
Primary Resource Manager	172.24.129.62:5070
Backup Resource Manager	

☒ Auto Refresh
 Refresh Rate (in sec) :

**Figure 104: SIP Session Manager Configuration**

[Table 35](#) describes the parameters in the SIP Session Manager Configuration page.

**Table 35: SIP Session Manager Configuration Parameters**

Parameter	Description
SIP Session Manager Name	Name of running SSM process.
SIP Port	Listening UDP port of SSM.
SIP Transport Protocol	Transport protocol of the SIP.

**Table 35: SIP Session Manager Configuration Parameters (Continued)**

Parameter	Description
SIP Version	Version of the SIP protocol.
SIP IP Address	Listening IP address of SSM.
Primary Resource Manager	Resource Manager address to contact for resource allocation. The format is <IP Address>:<Port>.
Backup Resource Manager	Backup Resource Manager address to contact for resource allocation. The format is <IP Address>:<Port>.

## Text-to-Speech

The Text-to-Speech (TTS) component communicates with the TTS engine, which can run on the same computer or on a remote computer.

### TTS Requests Summary

Click the TTS link in the left frame or on the Overall Status page to open the TTS Requests Summary page (see [Figure 105](#)). The TTS Requests Summary page provides information about the number of active and pending requests currently in the system.

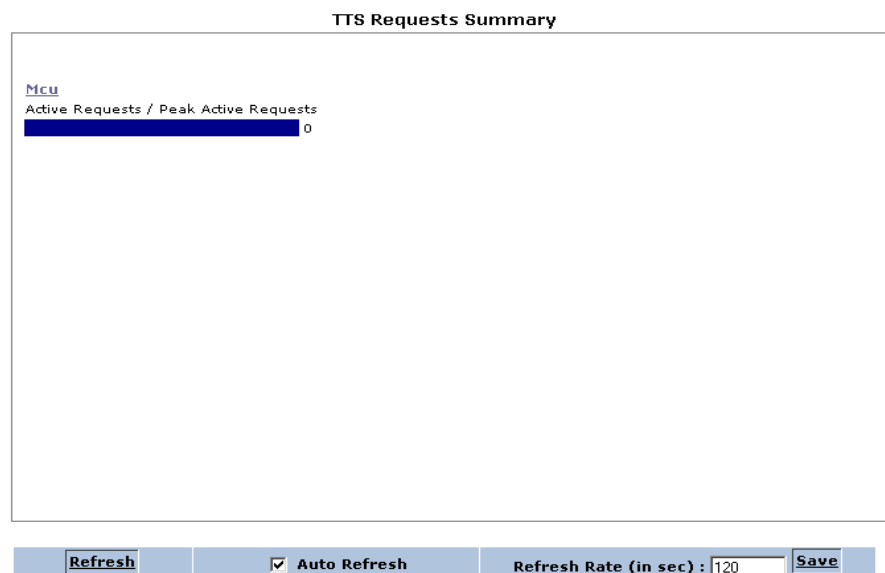
**Figure 105: TTS Requests Summary**

Table 36 describes the parameters in the TTS Requests Summary page.

**Table 36: TTS Requests Summary Parameters**

Parameter	Description
mcu link <b>Note:</b> The mcu link displays when you are using enhanced media service. For VCS the link displays as TTS_<vendor name>.	Opens the Active Requests page.

## Active Requests

Click the tts\_<vendor name> or mcu link in the left frame or on the TTS Requests Summary page to open the Active Requests-Mcu page (see Figure 106). This page provides a snapshot of current information about voice applications that have sent TTS requests to the server.

Active Requests - Mcu								
Voice Application	Dialed Number	DNIS	ANI	Request Start	Language	Gender	Text Size (Bytes)	Session ID
No Data Available								
<div> <input type="button" value="Refresh"/> <input checked="" type="checkbox"/> Auto Refresh           Refresh Rate (in sec) : <input type="text" value="120"/> <input type="button" value="Save"/> </div>								

**Figure 106: Active Requests**

[Table 37](#) describes the parameters in the TTS Active Requests page.

**Table 37: TTS Active Requests Parameters**

Parameter	Description
Voice Application	The name of the voice application as provisioned in the EMPS.
Dial Number	The toll free number that was dialed.
DNIS	The number that was presented to GVP by the switch or gateway.
ANI	Number of the calling party.
Request Start	The time when the TTS request was received for processing.
Language	Indicates the language.
Gender	Female or Male.
Text Size (Bytes)	The size, in bytes, of the TTS request.
Session ID	A unique id that tracks this TTS transaction.

## Statistics

Click the [Statistics](#) link in the left frame to open the TTS Statistics page (see Figure 107 on [page 207](#)). This page provides cumulative information since the TTS process was last started.

**TTS Statistics - tts\_mrcp**

Name	Value
Number of Requests Received	29641
Number of Requests Successful	29308
Number of Invalid Requests	0
Number of Oversize Requests	0
Number of Requests Rejected	0
Number of Requests Abandoned	0
Number of Errors	332
Number of Active Requests	1
Number of Pending Requests	0
Total Text Received (KB)	425
Total Text Successful (KB)	421
Total Text Rejected (KB)	0
Total Text Abandoned (KB)	0

☒ Auto Refresh
 Refresh Rate (in sec) :

**Figure 107: TTS Statistics**

Table 38 describes the parameters in the TTS Statistics page.

**Table 38: TTS Statistics Parameters**

Parameter	Description
Number of Requests Received	Total number of TTS requests received for processing.
Number of Requests Successful	Total number of TTS requests successfully processed.
Number of Invalid Requests	Total number of invalid TTS requests received.
Number of Oversize Requests	Total number of TTS requests that exceed maximum text size.
Number of Requests Rejected	Total number of requests rejected.
Number of Requests Abandoned	Total number of requests abandoned after timing out.
Number of Errors	Total number of TTS requests that had an error.
Number of Active Requests	Number of TTS requests actively being processed.

**Table 38: TTS Statistics Parameters (Continued)**

Parameter	Description
Number of Pending Requests	Number of TTS requests received and awaiting processing.
Total Text Received (KB)	Total kilobytes of text received to convert to speech.
Total Text Successful (KB)	Total kilobytes of text received from successful requests.
Total Text Rejected (KB)	Total kilobytes of text received from rejected requests.
Total Text Abandoned (KB)	Total kilobytes of text received from abandoned requests.
Total Text in Error (KB)	Total kilobytes of text received from error requests.
Total Text in Process	Total bytes of text received from all requests currently in the process.
Total Text Active	Total bytes of text received from currently active requests.
Total Text Pending (Bytes)	Total number of bytes of text received from currently pending requests.
Queue Size	Size of TTS queue.
Number of TTS Engines	Number of engines available for TTS processing.
Max Allowed Text Size (Bytes)	Maximum allowed text size in a TTS request.
Total Output Data (MB)	Total megabytes of audio converted from text.
Total Proc Time (seconds)	Total number of seconds elapsed processing all TTS requests.
Proc Time Per MB of Output (ms)	Average number of milliseconds taken to produce a megabyte of audio data.



**Table 38: TTS Statistics Parameters (Continued)**

Parameter	Description
Average Latency (ms)	Average delay in milliseconds before audio data is received for a TTS request.
Max Latency (ms)	Maximum delay in milliseconds before audio data is received for a request.

## Pending Requests

Click the Pending Requests link in the left frame to open the TTS Pending Requests page (see [Figure 108](#)). This page provides information about the TTS requests waiting in the queue for processing.

TTS Pending Requests - Mcu

Voice Application	Dialed Number	DNIS	ANI	Request Start	Language	Gender	Text Size (Bytes)	Session ID
No Data Available								

No Data Available

[Refresh](#)
☒ Auto Refresh
Refresh Rate (in sec) : 
[Save](#)

**Figure 108: TTS Pending Requests Mcu**

[Table 39](#) describes the parameters in the TTS Pending Requests page.

**Table 39: TTS Pending Requests Mcu Parameters**

Parameter	Description
Voice Application	The name of the voice application as provisioned in the EMPS.
Dialed Number	The toll free number that was dialed.
DNIS	The number that was presented to GVP by the switch or gateway.
ANI	Number of the calling party.
Request Start	The time when the TTS request was received for processing.
Language	Indicates the language.
Gender	Female or Male.
Text Size (Bytes)	The size, in bytes, of the TTS request.
Session ID	A unique id that tracks this TTS transaction.

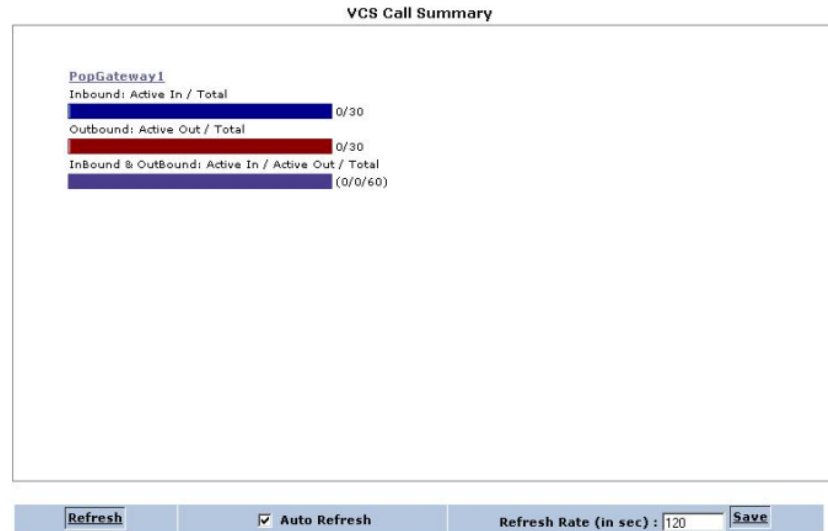
---

## Voice Communication Server

This section describes the Element Management GUIs for the Voice Communication Server (VCS) component.

### Call Summary

Click the VCS link to display the VCS Call Summary screen (see Figure 109 on [page 211](#)). The VCS Call Summary screen provides a snapshot of the inbound, outbound, and inbound/outbound calls on each PopGateway.

**Figure 109: VCS Call Summary**

[Table 40](#) describes the VCS Call Summary parameters.

**Table 40: VCS Call Summary**

Parameter	Description
PopGateway link	Opens the Active Calls screen for that PopGateway (see “Active Calls” on <a href="#">page 213</a> ).
Inbound Active / Total bar	Number of inbound ports that the PopGateway is currently using, displayed as a fraction of the total number of inbound ports that the PopGateway has available. For example, 19/23 means that the PopGateway has 23 available inbound ports, 19 of which are active.
Outbound Active / Total bar	Number of outbound ports that the PopGateway is currently using, displayed as a fraction of the total number of outbound ports that the PopGateway has available.
Inbound and Outbound Active In / Active Out / Total Bar	Number of inbound/outbound ports that the PopGateway is currently using, displayed as a fraction of the total number of inbound/outbound ports that the PopGateway has available.

## Call Volume

Click the Call Volume link to open the Call Volume screen, which displays call volume statistics for each VCS (see [Figure 110 on page 212](#)).

Call Volume					
Process ID	Process Name	Total Inbound Answered	Total Inbound Rejected	Total Outbound Answered	Total Outbound Rejected
4868	popgateway1	4	0	0	0
5700	popgateway2	0	0	0	0
<div> <div>Refresh</div> <div><input checked="" type="checkbox"/> Auto Refresh</div> <div>Refresh Rate (in sec) : <input type="text" value="120"/></div> <div>Save</div> </div>					

Figure 110: Call Volume

Table 41 describes the Call Volume parameters.

Table 41: Call Volume

Parameter	Descriptions
Process ID	Identification number of the process.
Process Name	Name of the process.
Total Inbound Answered	Total number of calls, from among those presented to the VCS, that the VCS answers.
Total Inbound Rejected	Total number of calls, from among those presented to the VCS, that the VCS disconnects before answering.
Total Outbound Answered	Total number of calls, from among those that the VCS initiates, that the far end answers.
Total Outbound Rejected	Total number of calls, from among those that the VCS initiates, that the far end disconnects before answering.

## PopGateway

The PopGateway(s) menu provides detailed information on the selected PopGateway. It has the following links:

- Port Status
- Board Status

## Active Calls

Click the PopGateway link to open the Active Calls - popgateway screen (see [Figure 111](#)). You can also access this screen by clicking the PopGateway link from the VCS Call Summary screen.

**Active Calls - popgateway1**

Port Number	Session ID	Call Type	DNIS	ANI	Start Time (GMT)	Application URL	ConvCtrl ID
No Data Available							

[Refresh](#)
☒ Auto Refresh
Refresh Rate (in sec) : 
[Save](#)

**Figure 111: Active Calls PopGateway Screen**

[Table 42](#) describes the Active Calls PopGateway parameters.

**Table 42: Active Calls PopGateway**

Parameter	Description
Port Number	Telephony port number on which the call is active.
Session ID	Unique ID that the VCS assigns to each call. The Session ID is the same for each leg of the call.
Call Type	Type of call that the VCS initiates; inbound or outbound.
DNIS	Dialed Number Identification Service.
ANI	Number of the calling party.
Start Time (GMT)	Time (Greenwich mean time) that the call starts.
Application URL	Current IVR URL being executed.
ConvCtrl ID	Unique ID that the VCS assigns to each leg.

## Port Status

Click the Port Status link, which displays statistical information about port status. You can disable or enable selected ports from this screen (see [Figure 112](#) on [page 214](#)).

**Port Status - popgateway1**

Reset Selected Ports
Disable Selected Ports

Select	Port Number	Port ID	Port Type	Port Status	Call Status
<input type="checkbox"/>	1	1:1	InBound	InSvc	Idle
<input type="checkbox"/>	2	1:2	InBound	InSvc	Idle
<input type="checkbox"/>	3	1:3	InBound	InSvc	Idle
<input type="checkbox"/>	4	1:4	InBound	InSvc	Idle
<input type="checkbox"/>	5	1:5	InBound	InSvc	Idle
<input type="checkbox"/>	6	1:6	InBound	InSvc	Idle
<input type="checkbox"/>	7	1:7	InBound	InSvc	Idle

[Refresh](#)
☒ Auto Refresh
Refresh Rate (in sec) :  [Save](#)

**Figure 112: Port Status - PopGateway**

[Table 43](#) describes the Port Status - PopGateway parameters.

**Table 43: Port Status - PopGateway**

Parameter	Description
Select check box	Selects the port.
Port Number	Number of the port.
Port ID	Identification number of the port; board/port number.
Port Type	Inbound or outbound.
Port Status	Out of service or in service.

**Table 43: Port Status - PopGateway (Continued)**

Parameter	Description
Call Status	<p>Call status on the port. The call-status states are:</p> <ul style="list-style-type: none"> <li>• <b>Idle</b>—no call on the port.</li> <li>• <b>Offered</b>—a new inbound call has been presented on the port.</li> <li>• <b>Accept</b>—the call is being processed. Ringback (alerting) has been sent to the network, and the VCS is waiting for acknowledgment.</li> <li>• <b>Alerting</b>—an outbound call has been initiated and is ringing. For inbound, ringback is being provided.</li> <li>• <b>Answer</b>—the call is in the process of being answered (the VCS is waiting for the network to acknowledge the answer).</li> <li>• <b>Active</b>—the call has been answered.</li> <li>• <b>Dialing</b>—an outbound call has been initiated.</li> <li>• <b>Proceeding</b>—an outbound call has been initiated and the VCS has received a proceeding acknowledgment from the network.</li> <li>• <b>Disconnect/DropCall/Release</b>—the call is in the process of being disconnected. These call states mark the release of various resources during the disconnect process. When all resources are released, and the call is disconnected, the port returns to the Idle state.</li> </ul>
Reset Selected Ports button	Resets the selected port.
Disable Selected Ports button	Disables the selected port.

## Board Status

Click the **Board Status** link for a specific PopGateway to open the **Board Status** screen, which displays information about the status of the boards for the selected PopGateway (see Figure 113 on [page 216](#)).

**Board Status - popgateway1**

Board ID	Board Name	Board Type	Signalling Protocol	D-Channel Status	Red Alarm	Yellow Alarm	Blue Alarm	Loss of Synch	Framing Error	Bipolar Violation
1	:N_dtiB1:P_isdn	Dialogic DM/V	T1 ISDN	0	0	0	0	0	0	0

<input type="button" value="Refresh"/>	<input checked="" type="checkbox"/> Auto Refresh	Refresh Rate (in sec) : <input type="text" value="120"/>	<input type="button" value="Save"/>
--	--	--	-------------------------------------

Figure 113: Board Status - PopGateway

Table 44 describes the Board Status - PopGateway parameters.

Table 44: PopGateway—Board Status

Parameter	Description
Board ID	ID number of the board. This number starts at 1 and continues up to the number of boards that the PopGateway has.
Board Name	Name of board, as identified by Dialogic.
Board Type	Board model.
Signalling Protocol	ISDN or Robbed-Bit.
The following columns can have the values 0 or 1. If the trunk is experiencing no problems or errors, the value will be 0. A value of 1 indicates a problem. All of the following conditions apply to T1, E1, and ISDN lines.	
D-Channel Status	0=D-Channel is up; 1=D-Channel is down.
Red Alarm	Occurs when loss of synchronization (LOS) has existed for 2.5 seconds on incoming data. This condition continues until the synchronization is recovered and remains recovered for 12 seconds.
Yellow Alarm	The far end sends this alarm to indicate that it detects a red alarm by the near end. The far end sends the yellow alarm for as long as the red alarm condition exists at the near end.
Blue Alarm	The Dialogic boards use this alarm to synchronize the clock in the event of a red alarm.



**Table 44: PopGateway—Board Status (Continued)**

Parameter	Description
Loss of Synch	This Layer 1 error indicates that the trunk cannot establish a connection (synchronize) with the far end. The Dialogic boards generate three alarm conditions—red, yellow, and blue—to indicate the type of LOS.
Framing Error	This Layer 2 characteristic divides the trunk into discrete timeslots/channels. Both ends of the trunk must use the same type of framing. If the trunk cannot synchronize the framing, a framing error is generated. The platform supports ESF frame (Extended Superframe), D4 frame (Superframe), and CEPT multiframe (with or without CRC4).
Bipolar Violation	Indicates that trunk polarity synchronization is incorrect. The platform supports AMI and B8ZS. Both sides of the trunk must use the same type of synchronization.

## Call Flow Assistant

The Call Flow Assistant (CFA) is the interface that initiates an outbound call request, and that communicates authorizing instructions from the Provisioning System to the Voice Communication Server.

The CFA communicates with the IVR Server Client. The CFA also provides certain information to the Policy Manager.

### Call Flow Assistant Statistics

Click the CFA link to open the Call Flow Assistant Statistics screen, which displays information about the currently active calls on the CFA (see Figure 114 on [page 218](#)).

**Call Flow Assistant Statistics**

Name	Value
Active Calls	0

<a href="#">Refresh</a>	<input checked="" type="checkbox"/> Auto Refresh	Refresh Rate (in sec) : <input type="text" value="120"/>	<a href="#">Save</a>
-------------------------	--	--	----------------------

**Figure 114: Call Flow Assistant Statistics**

[Table 45](#) describes the Call Flow Assistant Statistics parameters.

**Table 45: Call Flow Assistant Statistics**

Parameter	Description
Name	Active Calls
Value	Number of currently active calls on the VCS on all PopGateways.

## Active Sessions

Click the [Active Sessions](#) link to open the Call Flow Assistant Active Sessions screen, which displays the number of currently active calls on the CFA (see [Figure 115](#) on [page 219](#)).

When multi-tenancy is enabled, this page includes the customer names. When multi-tenancy is not enabled, this page does not display the Customer name column.

**Call Flow Assistant Active Sessions**

Select	Customer	Application	Dialed Number	DNIS	ANI	Call Start	Call State	Current Call State Start	VCS Process	Session ID
<div style="border: 1px solid black; padding: 5px; display: inline-block;">No Data Available</div>										

☒ Auto Refresh
 Refresh Rate (in sec) :

**Figure 115: Call Flow Assistant Active Sessions**

Table 46 describes the Call Flow Assistant Active Sessions parameters.

**Table 46: VCS—Call Flow Assistant Active Sessions**

Parameter	Description
Select	Check box to select the active session.
Customer	Name of the customer.
Voice Application	Name of the voice application.
Dialed Number	Toll-free number dialed.
DNIS	Dialed Number Identification Service.
ANI	Automatic Number Identification—for example, the number of the calling party.
Call Start	Time that the call starts.

**Table 46: VCS—Call Flow Assistant Active Sessions (Continued)**

Parameter	Description
Call State	<p>Current state of the call. The call states are:</p> <ul style="list-style-type: none"> <li>• <b>Answered</b>—the platform has answered and accepted the call. It is currently executing the voice application.</li> <li>• <b>Bridged</b>—the call has been bridged to an agent on the platform.</li> <li>• <b>Queued</b>—the call has been put into a Queued state, and is awaiting the availability of an agent.</li> <li>• <b>Agent Connecting</b>—the call is in the process of being connected to the agent. The agent phone may be ringing in this case, but it has not yet been picked-up.</li> <li>• <b>Agent Connected</b>—indicates that the agent has answered his or her phone, but the call has not yet been bridged.</li> </ul>
Current Call State Start	Date and time that the call state starts.
VCS Process	The PopGateway handling the call.
Session ID	Unique ID of the call.
Kill Selected Sessions	Ends the selected session.



## Chapter

# 7

# Portal

This chapter describes the Genesys Voice Platform (GVP) Portal. It contains the following sections:

- [Overview, page 221](#)
- [Accessing the Portal Interface, page 222](#)

---

## Overview

The Genesys Voice Platform (GVP) Portal is a website that provides links to all of the GVP web-based user interfaces that are available within a GVP installation. The user interfaces are:

- **Provisioning**  
(Refer to Chapter 1, “Element Management Provisioning System,” on [page 25](#) for detailed information about the EMPS.)
- **Unified Login**  
(Refer to Chapter 4, “Login Server,” on [page 115](#) for detailed information about the Login Server)
- **Network Monitor**  
(Refer to Chapter 5, “Network Monitor,” on [page 139](#) for detailed information about the Network Monitor.)
- **Mgmt GUIs**  
(Refer to Chapter 6, “Element Management System,” on [page 145](#) for detailed information about the EMS.)

The Portal discovers components that are installed in the network by querying the EMPS server. It also discovers which servers carry these components. Based on the component type, the Portal assumes default URLs and provides links to them. If the components are installed in non-default locations, these links will not work. If more than one component of that type is installed, the Portal provides links to all of the components. For the Element Management

graphical user interfaces (GUIs), the Portal provides a way to search these by component type.

Once the links are displayed in the Portal GUI, the Portal also validates them by accessing the URL and ensuring that it returns a status of 200 OK. For this functionality to work, you must use the FQDN of the EMPS machine when accessing the GVP Portal.

---

Note: For Solaris, clicking the Portal link opens a new window and may create an alert stating that the FQDN should be used. You can manually enter the FQDN in this window, and the Portal will appear. To prevent the alert from appearing, the System Administrator must configure the Solaris hosts to return the FQDN when the `gethostbyname` API is called.

---

---

## Accessing the Portal Interface

You can access the interface through a compliant web browser.

To access the Portal GUI:

1. Open a web browser.
2. Enter `http://<FQDN of EMPS Machine>:9810/gvpportal` in the address bar. The Portal GUI opens (see [Figure 116](#) for an example).

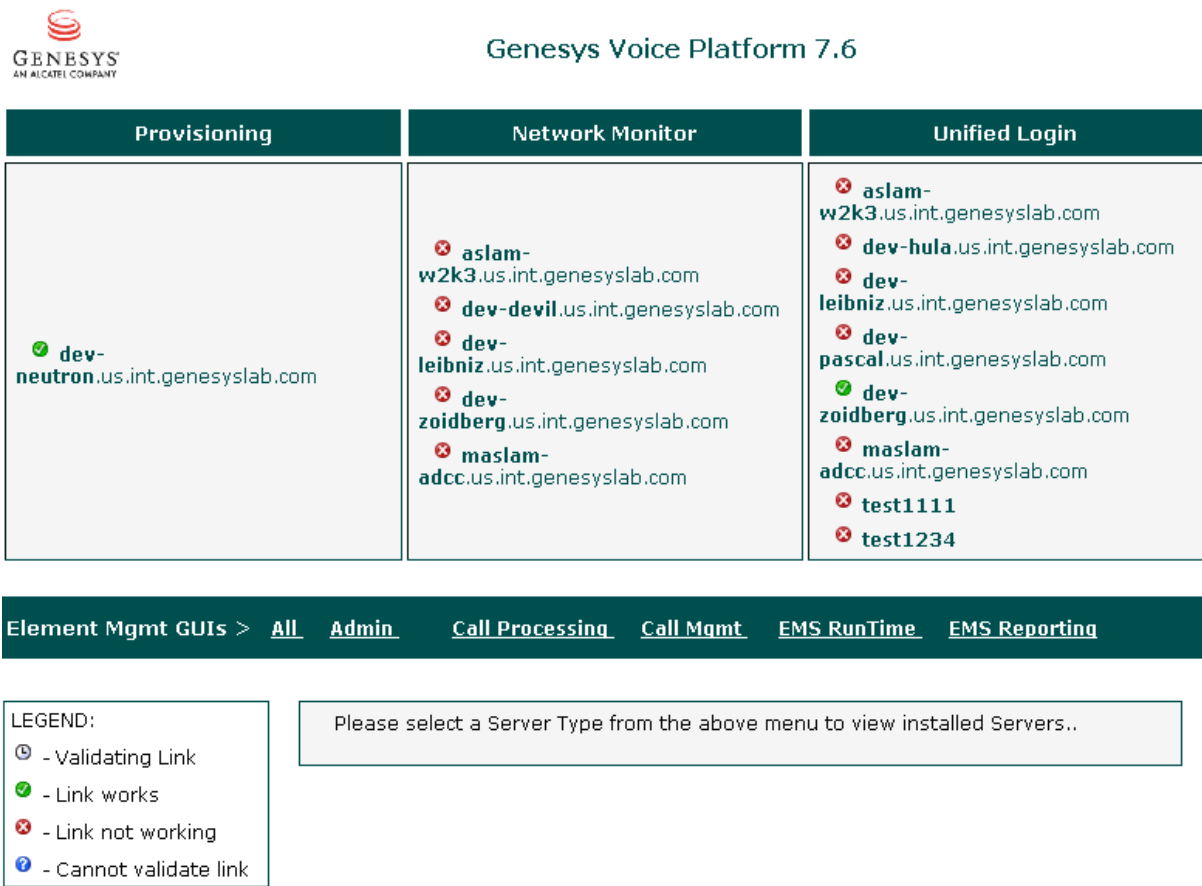


Figure 116: Example Portal GUI

The top of the Portal GUI displays three categories of the GVP GUIs—Provisioning, Network Monitor and Unified Login, along with their corresponding servers and links.

The bottom of the Portal GUI displays the Element Management System GUIs, which are categorized by component type. Only the component types that are installed in your network will be displayed.

The link validations appear as icons and are described in the legend.







## Chapter

# 8

## CTI Simulator for GVP: DE

This chapter describes how to use the computer telephony integration (CTI) Simulator for Genesys Voice Platform: Developer's Edition (GVP: DE).

The CTI Simulator is only available with GVP: DE. If you did not install GVP: DE, you do not have access to this tool.

This chapter contains the following sections:

- [Introduction, page 225](#)
- [CTI Simulator User Interface, page 225](#)
- [Sample Call, page 234](#)

---

### Introduction

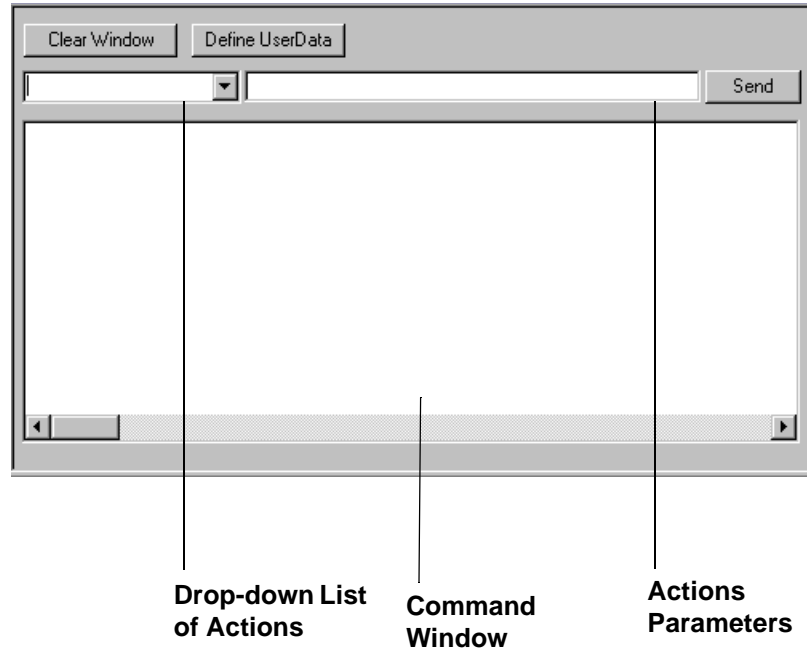
The CTI Simulator is a tool that assists application developers in testing Universal Router Server (URS)-controlled voice applications on GVP: DE that is configured only for In-Front-of-the-Switch mode. The CTI Simulator enables application developers to simulate and test URS-controlled voice applications on GVP: DE, without a need for the Genesys Call Router Framework.

---

### CTI Simulator User Interface

After it is installed, you can access the CTI Simulator from the Microsoft Windows Start > Programs menu.

The CTI Simulator operates in interactive mode. In interactive mode, the application developer selects the appropriate action in the drop-down list of actions (see Figure 117 on [page 226](#)) based on the application logic. The appropriate action must then be sent to the IP Communication Server (IPCS) for execution.



**Figure 117: CTI Simulator**

The CTI Simulator has the following functionality:

- Clear Window
- Define UserData
- Command Window
- Drop-down list of Actions
- Action Parameter Display

## Clear Window

The `Clear Window` button clears all data that appears in the `Command Window`.

## Define UserData

The `Define UserData` button opens the `User Data Dialog` dialog box (see Figure 118 on [page 227](#)), which enables the application developer to define user data variables for the voice application to be received or sent by the CTI Simulator.

A voice application sends user data as defined by the application developer in the `User Data Dialog` dialog box. The `User Data Dialog` dialog box shows previously passed user data as script results, and enables the developer to define new user data variables. Developers can define two types of data in the `User Data Dialog` dialog box:

- **Call Data**—Data used only during the life cycle of a single call and not available after a call ends.
- **Global Data**—Data used during any call and available for all calls during a CTI Simulator session.

---

Note: Once the CTI Simulator is closed, all Global Data is cleared.

---

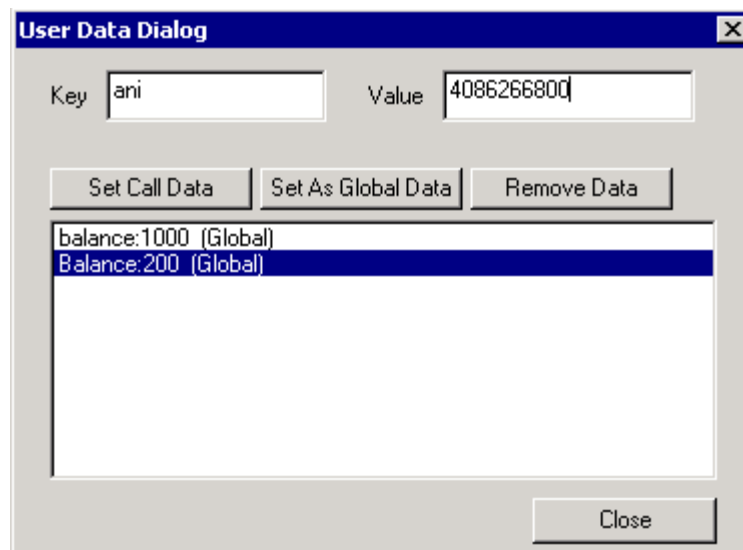
To define Call Data:

1. In the **Key** text box, enter the Key name.
2. In the **Value** text box, enter the value to be passed with that Key (see [Figure 118](#)).
3. Click **Set Call Data**.

To Define Global Data:

1. Repeat Steps 1–2 from the previous procedure.
2. Click **Set As Global Data**.

When sending user data to the voice application, it is important to remember that the voice application retrieves the key-value pair that has exactly the same key name as defined in the voice application. The key name is case sensitive. For example, in [Figure 118](#), the key `balance`, with a lower case `b`, is defined in the voice application. The key/value pair `balance` is passed to the voice application (not the key/value pair `Balance`).



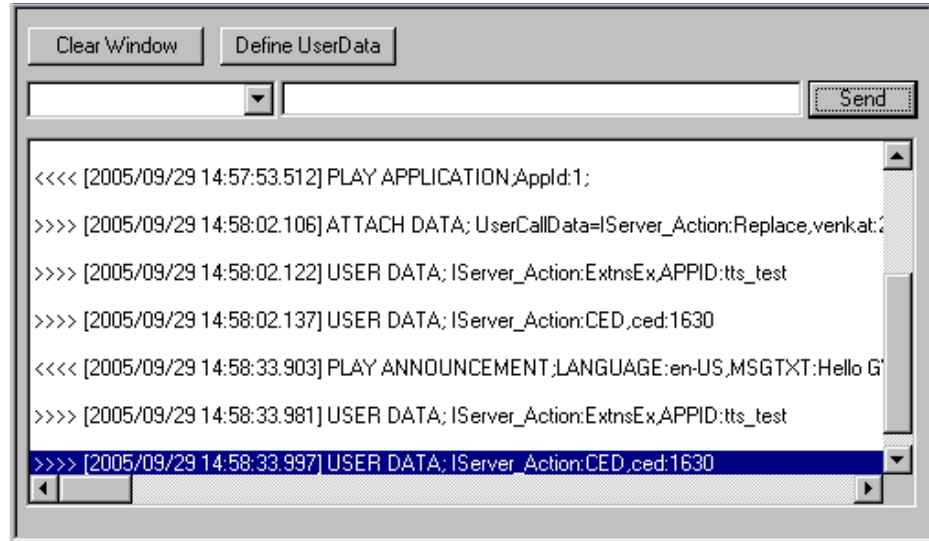
**Figure 118: User Data Dialog Defining Data**

In addition, the CTI Simulator also processes **ATTACH** and **GET DATA** requests from a voice application. In this case, the **ATTACH** and **GET DATA** must be defined as user data, with the **Key** exactly matching the expected result for either the **ATTACH** or **GET DATA** defined in the voice application.

The Remove Data button in the User Data Dialog dialog box clears the key/value pair that is highlighted in the dialog box.

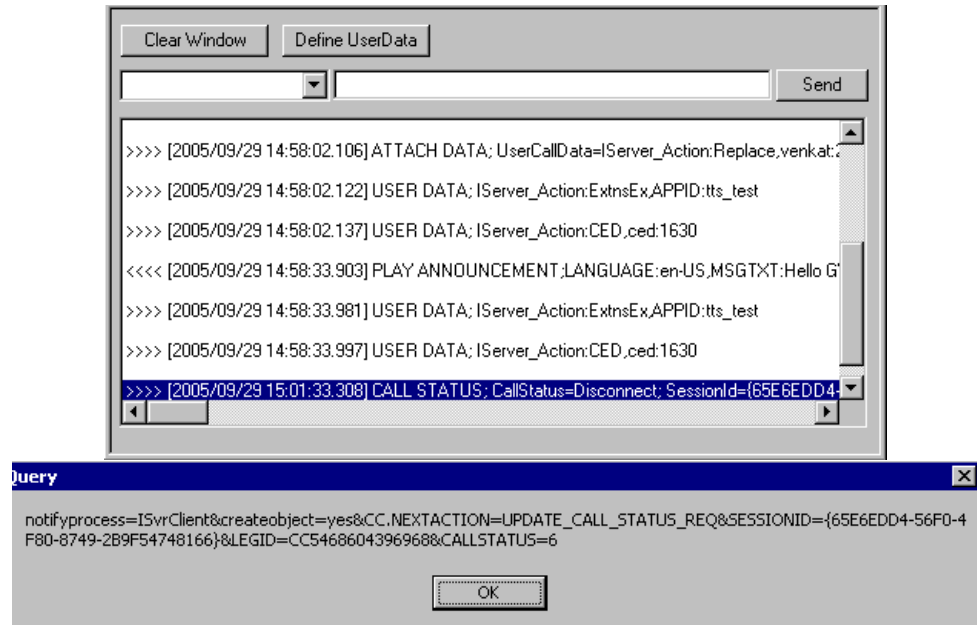
## Command Window

The CTI Simulator displays incoming call requests and Call Router responses in the Command Window (see [Figure 119](#)). The CTI Simulator parses only the mandatory parameters from the requests and responses—for example, application name or session ID—and displays them in the Command Window.



**Figure 119: Command Window**

The application developer can view the complete details for requests and responses by selecting and double-clicking any row from the Command Window (see [Figure 120](#) on [page 229](#)).



**Figure 120: Complete Request and Response Details**

## Drop-down List of Actions

The CTI Simulator provides a drop-down list that you can use to select actions to send to the voice application on GVP: DE. The CTI Simulator supports the following commands:

- Play Application
- Play Announcement
- Play Announcement and Collect Digits
- Music
- Transfer Call

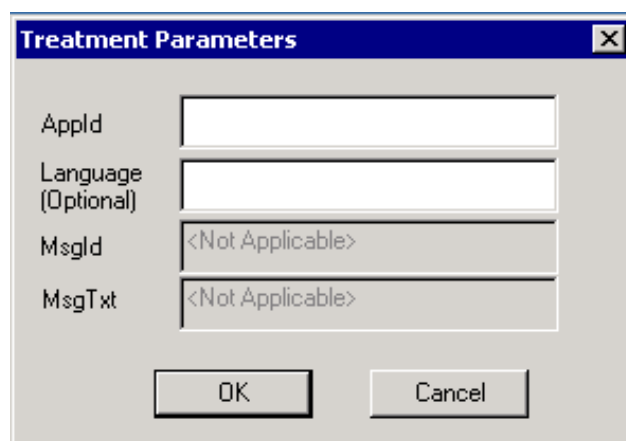
Selecting a command from the drop-down list opens a dialog box in which you can set command parameters. Use the Send button in the CTI Simulator GUI to forward the command to the voice application on GVP: DE.

## Play Application

This treatment executes an application or a script on the voice application. It is possible to pass parameters to the voice application and get return values (see [Figure 121](#)).

### Parameters:

AppId	Application ID (integer) of the application to be run.
Language (Optional)	Language in which the announcement is made. It should contain a string specifying a language in which the announcement is to be made. Currently only U.S. English (en-US) is supported. This is an optional parameter.



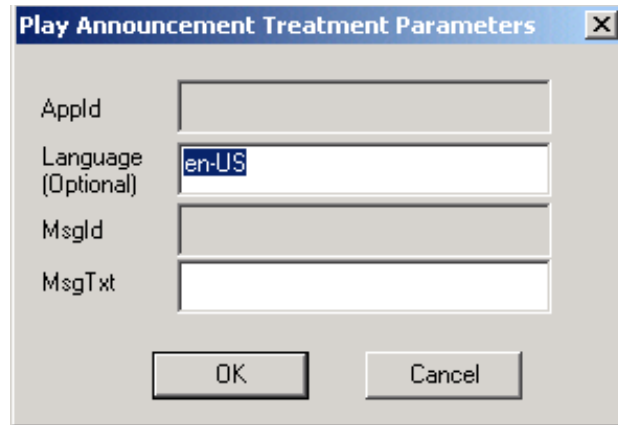
**Figure 121: Play Application Action Treatment**

## Play Announcement

This treatment plays an announcement to the calling party (see [Figure 122](#) on [page 231](#)).

### Parameters:

Language	Language in which the announcement is made. Currently, only U.S. English (en-US) is supported.
MsgTxt	ASCII text to pronounce using text-to-speech technology. This is a text-only field.



**Figure 122: Play Announcement Action Treatment**

## Play Announcement and Collect Digits

This treatment plays an announcement and collects digits from the caller. Typically, the announcement includes instructions that prompt the caller to provide information (see Figure 123 on [page 232](#)).

### Parameters:

Language	Language in which the announcement is made. Currently, only U.S. English (en-US) is supported.
Max_Digits	Maximum length of the collected digits. The default is one digit.
Term_Digits	Termination digit for caller input. The default is no termination digit required by caller.
Digits_Timeout	Inter-digit timeout for input from the caller. The default is 1 (second).
Total_Timeout	Total timeout, in seconds for input from the caller. The default is 1 (second).
MsgTxt	ASCII text to pronounce using text-to-speech technology. This is a text-only field.

---

**Note:** For all these parameters, if no default value is specified, you must supply a value.

---

**Play Announcement & Collect Digits Treatment Parameters**

Language:  Digits\_Timeout:

Max\_Digits:  Total\_Timeout:

Term\_Digits:  MsgTxt:

OK Cancel

**Figure 123: Play Announcement and Collect Digits Action Treatment**

## Music

This treatment connects the interaction to a music source (see [Figure 124](#)).

### Parameters:

**Music\_dn** Music file name—must be the name of either a .vox file or a .wav file.

---

**Note:** Music\_dn is a mandatory parameter. The name of the music file must be entered. Relative references to it from Configuration Server are not valid.

---

### Duration

(Optional) Music duration, in seconds. This parameter is currently not supported.

**Music Teatment Parameters**

Music\_dn:

Duration:

OK Cancel

**Figure 124: Music Action Treatment**

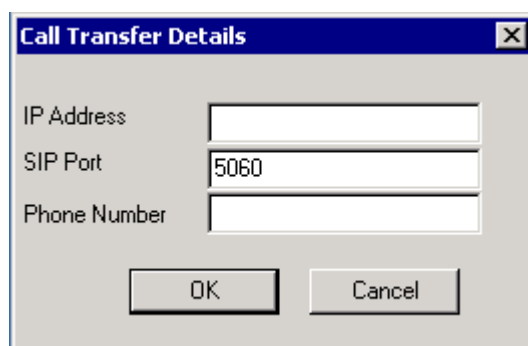


## Transfer Call

This treatment enables Call Router Framework to initiate a call transfer to an agent once the associated routing strategy has been executed ([Figure 125](#)).

### Parameters:

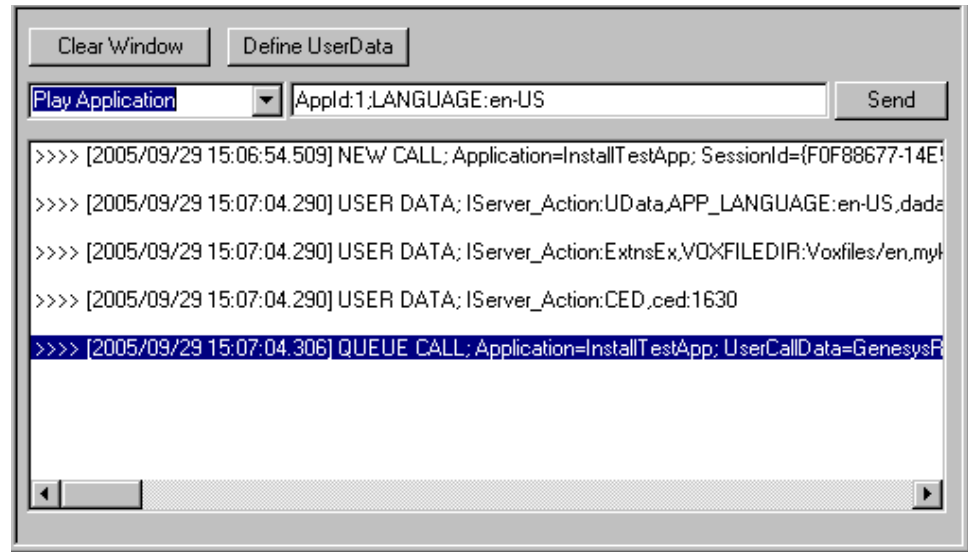
- |              |  |
|--------------|--|
| IP Address   | IP address of the agent's desktop on which the Session Initiation Protocol (SIP) client should be running. |
| SIP Port     | The User Datagram Protocol (UDP) port where the SIP Client is running on the agent's desktop.              |
| Phone Number | Application associated with the SIP client software.   |



**Figure 125: Call Transfer Action Treatment**

## Action Parameter Display

The Action Parameter display shows the action parameter list as entered in the Action Treatment Parameters dialog box or the Call Transfer Details dialog box (see [Figure 126](#) on [page 234](#)).



**Figure 126: Action Parameter Display**

## Sample Call

The CTI Simulator acts as an Interactive Voice Response (IVR) Server/URS in the GVP: DE environment. However, the CTI Simulator does not simulate all of the IVR Server/URS functionality. This section provides a step-by-step example of how to use the CTI Simulator to send URS responses to a voice application with the softphone. For this example, use Studio to create a simple voice application (see Figure 127 on [page 235](#)).

---

**Note:** In this example, the application is referred to by the name `CTISampleApp.vws`; however, the application you create in Studio can have any name.

---

This section explains:

- How to create and set up the sample voice application, `CTISampleApp.vws`, in GVP: DE.
- The sample voice application code interactions during a call.
- How to run a sample call using the softphone, GVP: DE CTI Simulator, and the sample voice application.

## Setting Up the Sample Voice Application

The sample voice application, `CTISampleApp.vws`, shown in Figure 127 on [page 235](#) should be created with Studio (refer to *Studio Help*) and used with the GVP: DE CTI Simulator. To enable the sample voice application to function with GVP: DE, complete the following initial setup and configuration

procedures to generate the source code for the voice application and enable GVP: DE to recognize the voice application.

1. In Studio, create the `CTISampleApp.vws` file.
2. In Studio, generate the code and save it under the `VPM/CTITestApp/` directory.
3. Provision the voice application in the Element Management Provisioning System (EMPS), and set the voice application URL as `http://localhost/EMPS/CTITestApp/Start.asp`.

## Sample Voice Application Code

Create this sample voice application using Studio URS blocks. Then, when you execute it on GVP: DE with the CTI Simulator, simulate a voice application under the control of the URS. Refer to *Studio Help* for information on URS blocks.

This section explains the specific interactions of the Studio sample voice application code as it progresses with a typical call. [Figure 127](#) illustrates the appearance of the voice application when viewed with Studio.

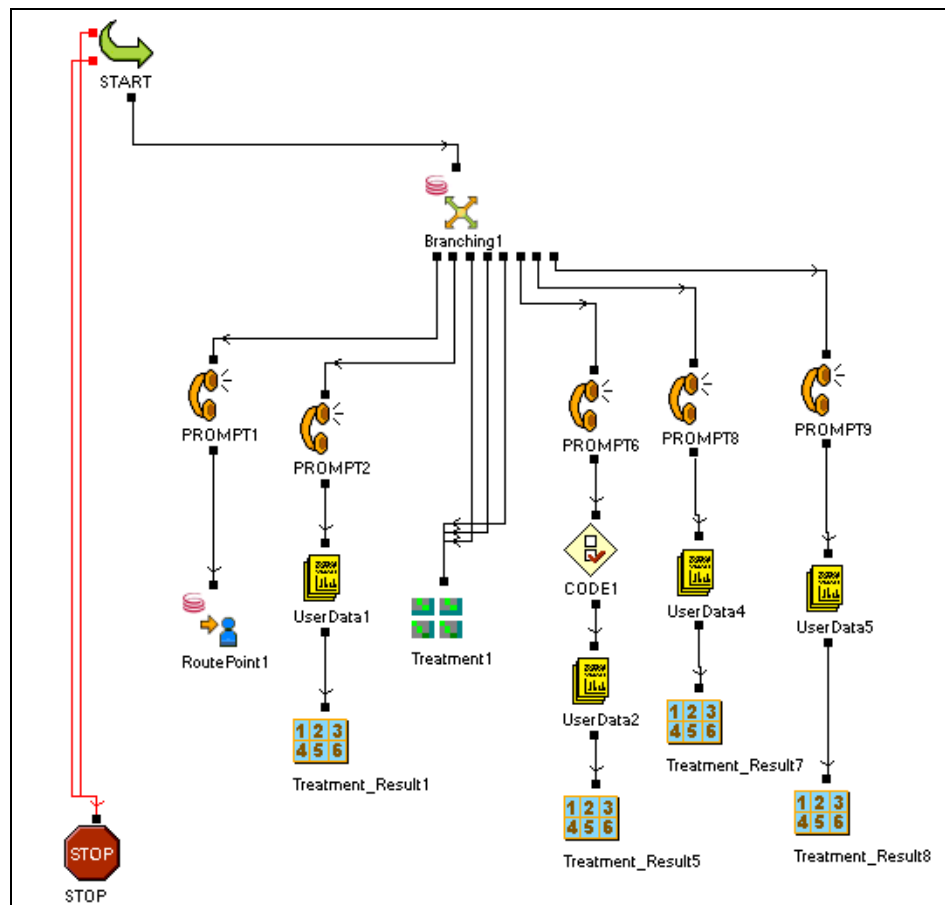


Figure 127: CTISampleApp.vws file in Studio

1. A call arrives at the GVP: DE, and the IPCS contacts the voice application on the web server.
2. The START block of the voice application begins execution. On the Application Settings tab of the START block:
  - a. Set the APPID (this can be any unique value, such as IVRSampleApp).
  - b. Create a variable called GenesysRouteDN and set it to a Route Point controlled by URS.
  - c. Set the ScriptID variable to 0 (zero).
  - d. Set any UserData (global or extension) as per the application design.

---

Note: The User Data blocks in CTISampleApp.vws would require userdata for various operations such as put, get, delete key and delete all, as seen in the UserData properties tab of the User Data block. For example, you can design your sample application so that UserData1, UserData2, UserData4 and UserData5 typically perform put, get, delete key and delete all operations on the user data, respectively. The Code block is used to modify/replace UserData during the course of the call. Please refer to *Studio Help* for more info on the Code block.

---

3. The voice application executes the Branching1 block. This block initiates the playing of the message Welcome to Genesys Voice Platform. The ScriptID variable is then evaluated, to determine the next action. Normally, the URS sends the ScriptID variable; however, when using the GVP: DE CTI Simulator, the CTI Simulator value provides this variable's value. At the beginning of a call, since the value of ScriptID, as set by the START block is 0 (zero), the voice application proceeds to the PROMPT1 block, plays a message, and then proceeds to the RoutePoint1 block.
4. The RoutePoint1 block directs the IPCS to contact the CTI Simulator (or URS), and then passes the User Parameter variables, as defined on the Interaction Data tab of the RoutePoint1 block, to the CTI Simulator (or URS). In this example, the GenesysRouteDN variable is passed to the CTI Simulator. For example, if the RouteDN on the RoutePoint tab of the RoutePoint block is set to 1111, then this will be passed to the CTI Simulator.

---

Note: When using the GVP: DE CTI Simulator the Route Point is not necessary; nevertheless, it should be included for compatibility when running the voice application with an actual URS.

---

5. Upon receiving the GenesysRouteDN from the voice application, the CTI Simulator (or URS) sends a response back to the voice application (a manual step described later in this chapter). For this sample application the response is an AppID.

6. Once the voice application has received a response back from the CTI Simulator (or URS), the control of the call logic returns back to the **START** block in the voice application.
7. The voice application executes the **Branching1** block. In this case the **AppID** received from the CTI Simulator (or URS) becomes the **ScriptID**.
8. The **Branching1** block executes one of several blocks depending on the value of the **ScriptID**. [Table 47](#) shows which block is executed, based on the corresponding **AppID** value.

**Table 47: Branching1 Block AppID**

AppID value	Block Executed
1	Play Application
2	SetUser Data
3	GetUser Data
4	DeleteAllKey
Play Announcement	Treatment
Play Announcement and Collect Digits	Treatment
Music	Treatment

9. The **Treatment** block is used to handle treatments such as **Play Music**, **Play Announcement**, and **Play Announcement and Collect Digits** from the CTI Simulator. The **Wait** parameter on the **Leg Wait** tab should be set to **Wait for Infinite** time. The **Treatment\_Result** block returns call control to the CTI Simulator. You can use the **Interaction Data** tab to send the collected data back to the CTI Simulator. Please refer to *Studio Help* for more information on the **Treatment** and **Treatment\_Result** blocks.
10. This process logic, in which an **AppID** is passed from the CTI Simulator to the voice application, which executes the next block based on the **ScriptID** value, continues until the call is terminated.

## Placing a Sample Call with Pingtel

The CTI Simulator takes the place of the URS for the sample call. During the sample call, the CTI Simulator requires manual input from the developer as the voice application proceeds to simulate a CTI routing situation. This section illustrates step-by-step, how to run a sample call using the Pingtel instant xpressa™ softphone, the GVP: DE CTI Simulator, and the sample voice application.

Before you begin, ensure that the voice application's URL, `http://localhost/VPM/CTITestApp/Start.asp`, has been provisioned in VPM on GVP: DE.

Next, launch the GVP: DE CTI Simulator. At this point, you are ready to launch the Pingtel instant xpressa™ softphone and place a call.

To launch a call with the Pingtel instant xpressa™ softphone application for GVP: DE:

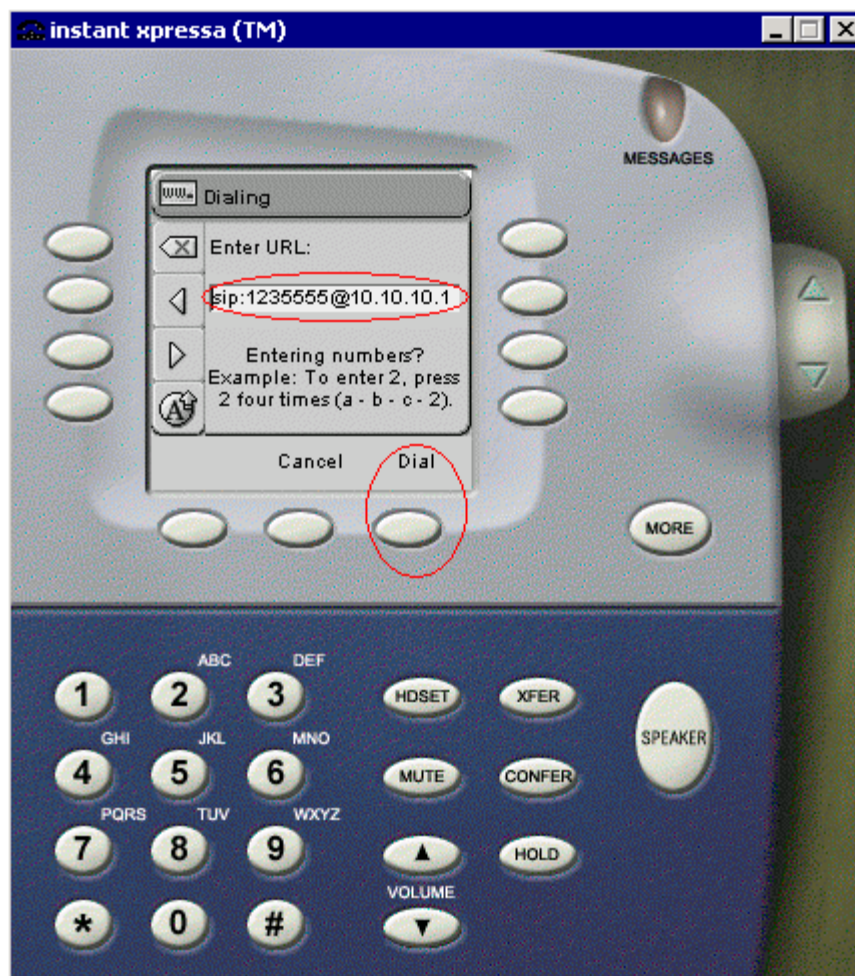
1. Click the **Dial by URL** button.
2. Enter the URL as `GVP: DEdnis@ipcs-hostname`, where `GVP: DEdnis` represents the value of the **Dialed Number Identification Service (DNIS)** field in the VPM for the sample voice application—for example, `1235555@10.10.10.100`.

---

Note: `GVP: DEdnis` represents the user part of the SIP Uniform Resource Identifier (URI).

---

3. Click **Dial** to make the call (see Figure 128 on [page 239](#) for an illustration of this procedure).



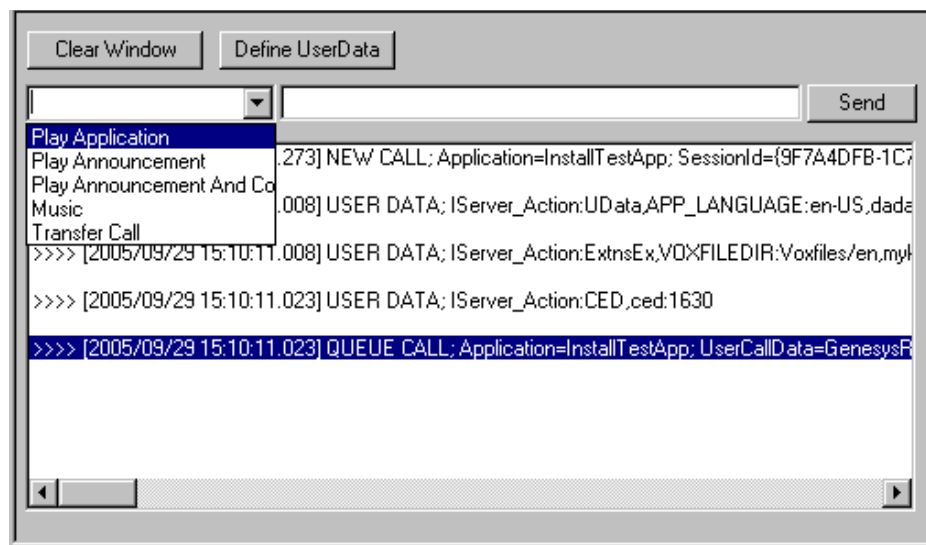
**Figure 128: Launching Instant xpressa™ Softphone**

---

Note: When using the ASR feature, Genesys recommends that you use a high-quality microphone.

---

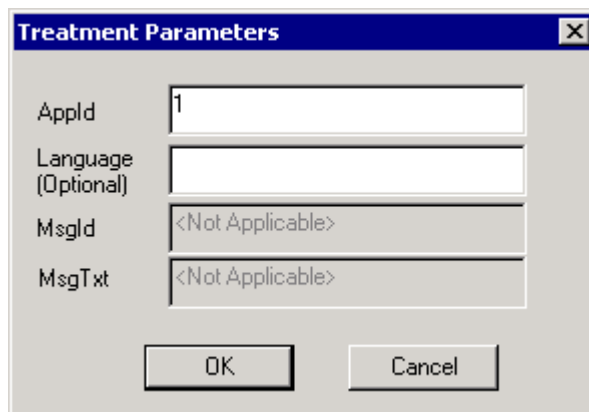
4. The call arrives on the GVP: DE, and the GVP: DE IPCS contacts the voice application on the web server.
5. The voice application answers with the message *Welcome to Genesys Voice Platform*. After a three second pause, the application plays the message *The call is being queued...* The call is then queued to the Call Router network (CTI Simulator in this case). At this point, the CTI Simulator controls the call.
6. The voice application waits for a response from the CTI Simulator. The developer testing the call must manually define and send a response in the CTI Simulator. To do so:
  - a. From the drop-down list of actions, select *Play Application* (see Figure 129 on page 240).



**Figure 129: Defining a Response**

The Treatment Parameters dialog box appears.

- b. In the AppId text box, enter 1 (see [Figure 130](#)) and then click OK.

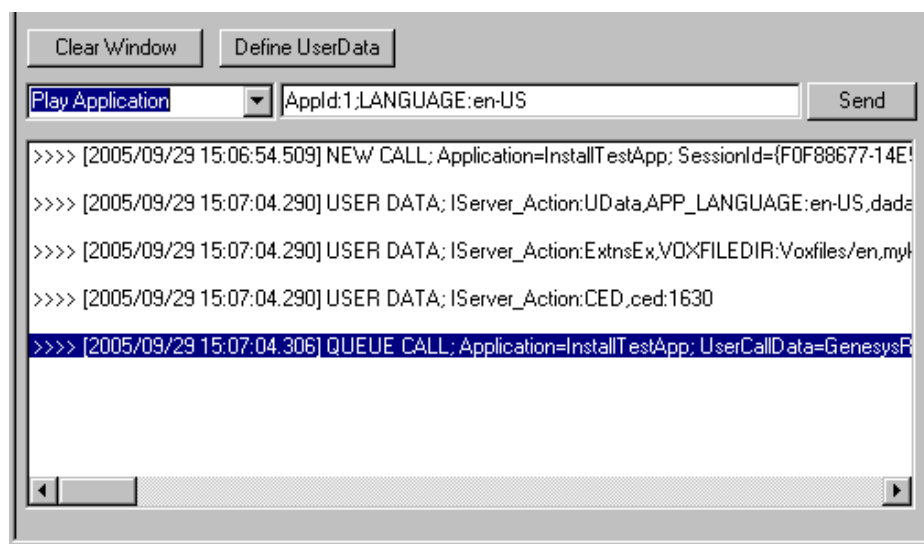


**Figure 130: Defining an AppId**

The CTI Simulator window appears as shown in [Figure 131](#) on [page 241](#).

- c. Click Send to send the AppId of 2 to the voice application.

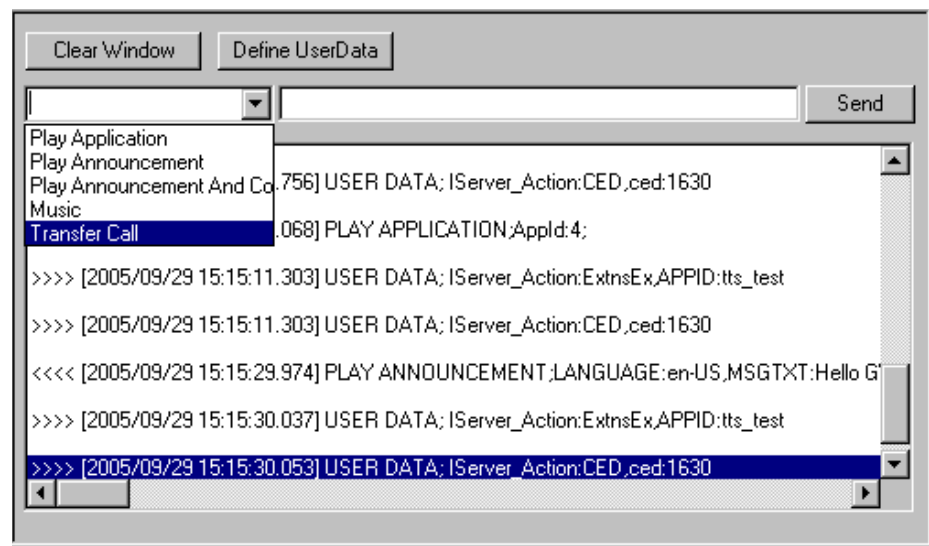




**Figure 131: Sending the AppId**

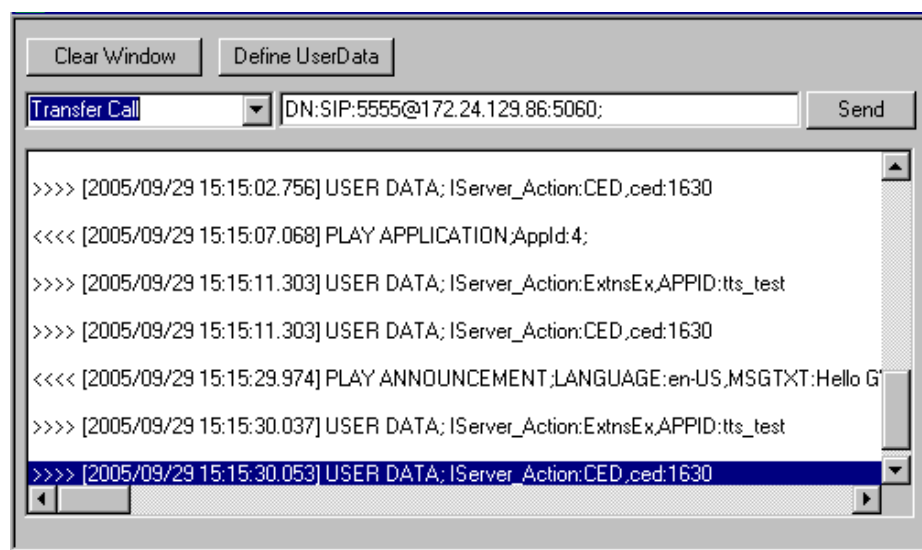
7. The voice application Branching1 block receives the AppId with a value of 1, translates it to a ScriptID of 1, and executes the PlayApplication block. The caller then hears the first prompt, Treatment of Play Application, and, after a three second pause, hears the next prompt, Setting user data with value of 500.
8. The voice application passes the user data to the CTI Simulator. The stored user data can be viewed in the User Data dialog box of the UserData window.
9. The voice application Branching1 block waits for a response from the CTI Simulator. The developer testing the call must manually define and send a response in the CTI Simulator. Follow Steps 6a–6c, but this time enter a value of 2 for the AppId.
10. The voice application Branching1 block receives the AppId of 2, and translates it to a ScriptID of 2. The message played is Setting user data using replace and new value is 1000. The UserData sent earlier as 500 is updated through the Replace option of the User Data block in Studio.
11. The voice application Branching1 block waits for a response from the CTI Simulator. The developer testing the call must manually define and send a response in the CTI Simulator. Follow Steps 6a–6c, but this time enter a value of 3 for the AppId.
12. The voice application Branching1 block receives the AppId of 3, and translates it to a ScriptID of 3. The message played is Getting user data.
13. The voice application Branching1 block waits for a response from the CTI Simulator. The developer testing the call must manually define and send a response in the CTI Simulator. Follow Steps 6a–6c, but this time enter a value of 4 for the AppId.

14. The voice application Branching1 block receives the AppId of 4, and translates it to a ScriptID of 4. The message played is `Deleting all user data`.
15. The voice application Branching1 block waits for a response from the CTI Simulator. The developer testing the call must manually define and send a response from the CTI Simulator. Use the following treatments, as needed:
  - `Play Announcement`—Plays a message specified in `MsgTxt`.
  - `Play Announcement and Collect Digits`—Plays a prompt, and then allows for the collection of digits.
  - `Music`—Enables URS to play a .vox file.
16. To test a call being transferred to an agent on a Pingtel instant xpressa™ softphone:
  - a. From the drop-down list of actions, select `Transfer Call` (see [Figure 132](#)).



**Figure 132: Transferring a Call**

- The `Call Transfer Details` dialog box appears (see [Figure 125](#) on [page 233](#)).
- b. In the `IP Address` text box, enter the IP address; in the `Phone Number` text box, enter the Phone Number.
  - c. Click `OK`.
- The CTI Simulator window appears, as shown in [Figure 133](#) on [page 243](#).
- d. Click `Send` to transfer the call.



**Figure 133: Sending the Call Transfer Request**





Part

## 2 Features and Configurations

Part Two of this manual provides details about GVP features and configurations. This information appears in the following chapters:

- Chapter 9, “Voice Communication Server,” on [page 247](#)
- Chapter 10, “IP Communication Server,” on [page 253](#)
- Chapter 11, “H.323 Session Manager,” on [page 279](#)
- Chapter 12, “IVR Server Client,” on [page 285](#)
- Chapter 13, “Outbound Notification Manager,” on [page 291](#)
- Chapter 14, “MRCP Server Hunt List,” on [page 307](#)
- Chapter 15, “Media Server Hunt List,” on [page 311](#)
- Chapter 16, “Network Announcement,” on [page 315](#)
- Chapter 17, “Transactional Recording,” on [page 319](#)
- Chapter 18, “Multiple PopGateways and MCUs,” on [page 323](#)
- Chapter 19, “Proxy Support,” on [page 329](#)
- Chapter 20, “SIP Registration with Avaya SIP Server,” on [page 333](#)





## Chapter

# 9

## Voice Communication Server

This chapter provides information about configuration options for the Voice Communications Server (VCS).

This chapter contains the following sections:

- [Configuring Outbound Dial Number Format, page 247](#)
- [Configuring Overlap Receive on ISDN, page 248](#)
- [Configuring Enhanced CPA, page 249](#)

---

## Configuring Outbound Dial Number Format

The following rules govern how the outbound number is created. In all of the rules, TELNUM is the original dialed number that is given by the voice application.

**RULE 1**—If the system is E1-ISDN, then TELNUM is dialed without modification. The rest of the rules do not apply.

**RULE 2**—If you are doing a reroute, then the reroute number is dialed without modification. The rest of the rules do not apply.

**RULE 3**—If an voice application's AppId.xml has the \$Dial-Plan\$ parameter set to 1 (using the EMPS), then the number dialed is exactly what is given in the voice application. The rest of the rules do not apply.

**RULE 4**—If the NetType is Enterprise, then the following logic is used to create the actual dialed number (and the rest of the rules do not apply). (NetType, HomeNPA, DialPrefix, MaxNumDigits are in the route configuration):

- If MaxNumDigits=0, then dial TELNUM without any changes.
- If the number of digits in TELNUM is less than or equal to MaxNumDigits, then dial all of the digits of the TELNUM.

- If `MaxNumDigits > 0`, and the number of digits in `TELNUM` is larger than `MaxNumDigits`, then dial the low order of digits (for example, if `TELNUM="1234567890"` and `MaxNumDigits=4`, then `7890` will be dialed). Low order digits are used to allow a PBX to dial extension numbers without modifying the voice application.

**RULE 5**—If the `NetType` is `PSTN`, then the following logic will be used to determine the actual dial number (`NetType`, `HomeNPA`, `DialPrefix`, `MaxNumDigits`, and `InvalidNPA` are in the route configuration). `TELNUM` must have 10 digits. If `TELNUM` has 11 digits, then GVP strips the first (left-most) digit. The rest of the logic is applied to the right-most 10 digits of `TELNUM`.

- Determine whether `TELNUM` is in your home dialing area. This is based only on the `NPA`. If `TELNUM`'s `NPA` is `HomeNPA`, then the dialing sequence is based on `MaxNumDigits`.
  - If `MaxNumDigits=7`, then strip the `NPA` (the first 3 digits from the left) from the `TELNUM` and dial the result.
  - If `MaxNumDigits=10`, then dial the 10-digit `TELNUM`.
  - If `MaxNumDigits=11`, then dial `DialPrefix + TELNUM`.
- If `TELNUM`'s `NPA` is not `HomeNPA`, and `TELNUM` is a toll-free call (800-123-4567), then the dial sequence will be `1 + TELNUM`. The toll-free NPAs are defined using the `TollFreeNPA` parameter in the `PopGateway` section of the configuration.
- If `TELNUM`'s `NPA` is one of the invalid `InvalidNPA`, then an error is returned to the voice application; otherwise, the dialed number is `DialPrefix + TELNUM`.

---

## Configuring Overlap Receive on ISDN

Configuring Overlap Receive consists of two sets of configuration changes. One is to enable Overlap Receive itself and the second is to (optionally) set the `T.302` timer.

### Enabling Overlap Receive

For each applicable `Route`, add the parameter `OverlapReceiveEnabled`:

In the `Route` GUI, click `Add New Attribute`, and then add the `OverlapReceiveEnabled` parameter with a value of `1`.

### SETUP\_ACK Message for Overlap Receive

The VCS turns off the `SETUP_ACK` message for an ISDN/E1 route where Overlap Receive is not enabled. For a route where Overlap Receive is enabled, the Dialogic firmware sends it automatically.



---

Note: This functionality is currently supported only for JCT boards.

---

## Setting the T.302 Timer for ISDN Protocols

The T.302 timer specifies, in milliseconds, how long GVP waits for DNIS digits between two ISDN INFORMATION messages.

For each applicable Route, add the parameter `T302Duration`:

In the Route GUI, click **Add New Attribute**, and then add the `T302Duration` parameter with a value of `<timer duration in milliseconds>`.

To turn off the timer, set the value to `0`.

---

Note: Genesys recommends that you set the timer to a value of less than 5000 milliseconds.

---

---

## Configuring Enhanced CPA

You can provision the VCS for enhanced Call Progress Analysis (CPA) to detect an answering machine.

To enable this option for DMV boards, set the following parameters in **EMPS > Servers > VCS > PopGateway**:

- `CpaOption`
- `CpaFailTime`
- `CpaContNoSignal`
- `CpaPamdOption`

To enable this option for JCT boards, set the following parameters in **EMPS > Servers > VCS > PopGateway**:

- `CpaOption`
- `CpaMinRing`
- `CpaFailTime`
- `CpaMaxInterRing`
- `CpaQualTemplate`
- `CpaPamdOption`
- `CpaContinuousNoSignal`
- `CpaStartDelay`

For more information about these parameters and their possible values, refer to the Dialogic documentation. These parameters have one-to-one mappings to the `DX_CAP` parameters of Dialogic (see Table 48 on [page 250](#)):

**Table 48: CPA Parameters**

VCS PopGateway Parameter	Dialogic DX_CAP Parameter
CpaOption	ca_intflg
CpaMinRing	ca_pamd_minring
CpaFailTime	ca_pamd_failtime
CpaQualTemplates	ca_pamd_qtemp
CpaMaxInterRing	ca_maxintering
CpaPamdOption	ca_pamd_spdval
CpaStartDelay	ca_stdely
CpaContNoSignal	ca_cnosig

## Qualification Parameters

To enable robust detection of Positive Answering Machine Detection (PAMD) in DMV boards, modify the qualification parameters in the `ml2_dsa_<xxx>.config` or `ml2_qsa_<xxx>.config` file, where `xxx` represents the protocol name. Refer to the Dialogic documentation for more information about the location and use of these configuration files.

[Table 49](#) lists the PAMD qualification parameters.

**Table 49: PAMD Qualification Parameters**

PAMD Qualification Parameter	Description
maxAnsiz1	Maximum size of the answer (salutation). Default value is 125.
maxAnsiz2	Maximum size of the answer when connect to voice threshold 1 is used. Default value is 50.
maxAnsiz3	Maximum size of the answer when connect to voice threshold 2 is used. Default value is 220.
loHiss	Low hiss (noise) range. Default value is 22.

**Table 49: PAMD Qualification Parameters (Continued)**

<b>PAMD Qualification Parameter</b>	<b>Description</b>
hiHiss	High hiss (noise) range. Default value is 16.
Bhparm	Early classification to measure lohiss. Default value is 5.
cvThresh1	Maximum threshold time between when the call is connected and when the actual voice starts. Default value is 390.
cvThresh2	Threshold to measure connect-to-voice time. Its usage depends on lohiss. Default value is 80.
maxCvThresh	Threshold to measure connect-to-voice time. Its usage depends on bhparm. Default value is 165.
NMaxBroad	Maximum broad above which it will not be classified as noise. Default value is 2.
nMaxErg	Maximum energy above which it will not be classified as noise. Default value is 65.
maxSilence	Maximum silence to check whether the salutation is finished. Default value is 30.
VoiceThresh	The energy level above which it will be classified as voice. Default value is 25.
SilenceThresh	The energy level below which it will be classified as silence. Default value is 30.





## Chapter

# 10 IP Communication Server

This chapter provides information about configuring the IP Communications Server (IPCS) as well as supported features.

This chapter contains the following sections:

- [Supported SIP Features, page 253](#)
- [Early Media, page 254](#)
- [Media Support, page 254](#)
- [Media Server Configuration, page 261](#)
- [G.729 Support, page 262](#)
- [Outbound Call Setup, page 264](#)
- [SIP INFO, page 265](#)
- [SIP Re-INVITE, page 267](#)
- [Propagation of SIP Header Values, page 274](#)
- [Session Timers, page 274](#)
- [DTMF Rendering, page 276](#)
- [RTP Tone Detection, page 277](#)

---

## Supported SIP Features

IPCS supports the following (Session Initiation Protocol) SIP features:

- INVITE, ACK, BYE, CANCEL, REGISTER, REFER, PRACK, NOTIFY
- 1xx, 2xx, 302, 4xx, 5xx, 6xx

---

Note: The IPCS will not generate any 6xx responses. If a 4xx, 5xx, or 6xx message is given as a response to an outbound call, the call will be torn down, and an error will be sent to the voice application.

---

---

## Early Media

Early media enables a media stream to be setup before a call is answered. SIP support of early media is defined in the *draft-ietf-sipping-early-media-02*. The IPCS supports the following media models:

- Offer/Answer
- Gateway (supported as described below)

### Gateway Model Outbound Calls

In a response in which the call recipient sends a `180` reliable provisional response, the IPCS sends back a `PRACK` message.

Any early media received on the RTP ports is not forwarded to another leg (for example, an inbound call bridged to an outbound call).

The outbound calls are configured for Early Media with the `PopGateway` parameter `Enable Reliable Provisional Messages`.

### Gateway Model Inbound Calls

If an `INVITE` request is received with a `Require` header field containing the option tag `100rel`, it will be rejected if the `Reliable Provisional Messages` parameter is not configured on the system. If this parameter is configured on the system, a `Reliable 180 Ring` message will be sent out.

---

## Media Support

This section describes the media capabilities of IPCS. `NativeRTP` is bundled with IPCS; however, IPCS also integrates third party media processing software and hardware—Intel Host Media Processing (HMP), Convedia, and Alcatel MRF.

### HMP Support

The IPCS integrates with HMP using an application programming interface (API) integration to provide media functionality, such as:

- Call progress analysis
  - Fax/Modem
  - Answering Machine
  - Operator Intercept
  - Far End Busy
  - Ring No Answer

- Codec support
  - G729/G729A
  - G729B/G729AB
  - G723
  - G711A/Mulaw
- Support for final silence and beep attributes for <record>

---

Notes: TTS is integrated within the MCU process and does not run as a separate process. The TTS audio will be streamed to HMP, which, in turn, streams the audio to the caller.

HMP integration using MSML is not supported.

Transaction Recording with Intel HMP is not supported.

Keyahead during ASR is not supported.

---

To enable IPCS-HMP integration, you must install the IPCS, and install Intel HMP on the same machine as the IPCS, and then configure the IPCS as follows:

- In EMPS Servers configuration, go to IP Communication Server > MCU > MediaController, and set the Media Controller parameter to Intel HMP.

## License Usage

RTP port licenses are used as described in [Table 50](#). The licenses referred to are G.711 licenses. If you are using G.729, you will need an RTP license in addition to the G.711 license.

**Table 50: RTP Port Licenses**

Call Scenario	HMP RTP License Usage
Inbound or Outbound call	One license is used for the duration of the call.
ASR	One additional license is used from the time the first recognition is triggered until the call is dropped or the ASR resource is released.
TTS	One additional license is used for the duration of a TTS play. The license is allocated at the beginning of a TTS play and released at the end of the TTS play.

**Table 50: RTP Port Licenses (Continued)**

Call Scenario	HMP RTP License Usage
Local Bridged Transfer (calls bridged via HMP)	Two licenses are used, one for each respective call. Additionally, a license for ASR may have been allocated for each call, if ASR was previously active on the respective calls. The license for ASR may be explicitly or implicitly freed.
Remote Bridged Transfer (calls via re-INVITEs)	All licenses are released (the respective call licenses plus ASR licenses on those calls).

## Convedia Support

The IPCS integrates with Convedia CMS-8000 via MSML over SIP to provide media functionality.

The following items are important to note about Convedia support:

- When using ASR, the DTMF tones must be received through SIP INFO. Otherwise, the MRCP server will not properly receive DTMF tones.
- IPCS integrates with MRF through MSML over SIP to provide media functionality. To enable this functionality, configure IPCS as follows:
  - In EMPS Servers configuration, to go to IP Communication Server > MCU > MediaController, and set the Media Controller parameter to MxML.
  - In EMPS Servers configuration, go to IP Communication Server > MCU > MediaController > MxML and choose the Media Servers Group, which was configured in “Media Server Configuration” on [page 261](#).
- The prerecorded audio file must be .wav files. The .vox format is not supported.
- Key-ahead during ASR is not supported.
- Recordings can only terminate on a specific DTMF key (for example, # only), and not any DTMF keys (for example, use of dtmfterm <record> attribute, grammar with multiple DTMF keys, and so on).
- The finalsilence attribute for <record> is supported.
- The beep attribute for <record> is not supported.
- TTS is integrated within the MCU process and will not run as a separate process. The TTS audio will be streamed to Convedia which in turn streams the audio to the caller.
- For outbound calls, IPCS lists the codecs in the SIP INVITE SDP in the exact order of preference as they are received from Convedia.

---

Note: Convedia does not support audio filenames with embedded spaces or hyphens.

---



## Port Usage

Table 51 describes the port usage for Conveda.

**Table 51: Port Usage**

Call Scenario	MSML Server Port Usage
Inbound or Outbound call	One port is used for the duration of the call.
ASR	One additional port is used from the time the first recognition is triggered until the call is dropped or the ASR resource is released.
TTS	One additional port is used for the duration of a TTS play. The port is allocated at the beginning of a TTS play, and released at the end of the TTS play.
Local Bridged Transfer (calls bridged via Conveda)	Two ports are used, one for each respective call. Additionally, a port for ASR may have been allocated for each call, if ASR was previously active on the respective calls. The port for ASR may be explicitly or implicitly freed.
Remote Bridged Transfer (calls via re-INVITEs)	All ports are released (inbound, outbound call licenses plus ASR licenses on those calls).

## NativeRTP Support

The Real-Time Transfer Protocol (RTP) stack is installed by default with IPCS. To use the NativeRTP functionality, in EMPS, go to IP Communication Server > MCU > MediaController, and for the Media Controller parameter, select NativeRTP.

The following features are supported with NativeRTP:

- Rich codec support—see “Supported Codecs” on [page 258](#) for more information.
- Transcoding—IPCS can transcode all configured codecs.
- Transaction recording—IPCS supports full-duplex transaction recording on inbound and outbound calls.

---

Note: IPCS does not record DTMF in a transaction recording.

---

- Local bridging—IPCS conferences inbound and outbound media streams, so that media operations such as transaction recording is available after the call is transferred.
- Media files—IPCS plays supported codec encoded .vox and .wav files.
- Intelligent bridging—If the inbound leg and the outbound leg of a call does not have a common codec, IPCS bridges the media.

## Supported Codecs

IPCS supports the following codecs for accepting inbound and outbound calls:

- G711ALaw
- G711ULaw
- G726-32
- G729 (G729, G729A, G729B, G729AB)
- GSMfr

IPCS also supports the following additional codec for transcoding only.

- AMR

---

Note: The G729 codec is not supported for Solaris IPCS.

---

To configure the additional codecs for IPCS in EMPS:

1. Go to Servers > IP Communication Server > MCU > Media Controller, and double-click the NativeRTP node.
2. Click Add New Attribute.
3. In the Parameter Name field, enter codec.
4. In the Parameter Value field, enter the required codecs separated by a space. For example, if you want to support the G711A, G711U, G726, AMR, and G729 codecs, in the Parameter Value field enter pcma pcmu g726 g726 amr g729.

---

Note: The sequence of codecs defines your preference of codecs to use for outbound calls.

---

5. Click Add New Attribute.
6. In the Parameter Name field, enter transcoders.
7. In the Parameter Value field, enter the same codec values that were added for the codec parameter. For example, if you want to use the same values as in step 4, enter PCM g726 AMR g729 in the Parameter Value field. PCM includes both PCMA and PCMU.

This parameter is needed to allow transcoding from other codecs to the additional codecs.

---

Notes: TTS is integrated within the MCU process and does not run as a separate process. The TTS audio will be streamed to NativeRTP, which in turn, streams the audio to the caller.

Genesys recommends that you always add PCMU and PCMA in the list of supported codecs because MRCP servers support these codecs only. If PCMU and PCMA are not included in this list, IPCS will not transcode media to and from PCMU and PCMA, which causes TTS play and ASR recognition to fail.

---

## MRF Support

The IPCS integrates with MRF through MSML over SIP to provide media functionality. To enable this functionality, you must configure IPCS as follows:

- In EMPS Servers configuration, go to IP Communication Server > MCU > MediaController, and set the Media Controller parameter to MxML.
- In EMPS Servers configuration, go to IP Communication Server > MCU > MediaController > MxML and select the Media Servers Group that was configured in “Media Server Configuration” on [page 261](#).

The following items are important to note about MRF support:

- MRF does not support Transcoding.
- The supported audio codecs are G711Alaw, and G711Mulaw.
- The prerecorded audio file must be .wav files. The .vox format is not supported.
- TTS is integrated within the MCU process and will not run as a separate process. The TTS audio is streamed to MRP which in turn streams the audio to the caller.
- For outbound calls, IPCS lists the codecs in the SIP INVITE SDP in the order of preference as they are received from the MRF.
- MRF only supports RFC2833 DTMF. It does not support Inband DTMF.
- MRF supports full Duplex Transaction Recording and is controlled by the VoiceXML application.
- Transaction recording is only supported in audio/wav and audio/x-wav format. That is, audio with .wav header. 8 bit mono.

## Port Usage

Table 52 describes the port usage for the MRF.

**Table 52: Port Usage**

Call Scenario	MSML Server Port Usage
Inbound or Outbound call	One port is used for the duration of the call.
ASR	One additional port is used from the time the first recognition is triggered until the call is dropped or the ASR resource is released.
TTS	One additional port is used for the duration of a TTS play. The port is allocated at the beginning of a TTS play, and released at the end of the TTS play.
Local Bridged Transfer	Two ports are used, one for each respective call. Additionally, a port for ASR may have been allocated for each call, if ASR was previously active on the respective calls. The port for ASR may be explicitly or implicitly freed.
Remote Bridged Transfer (calls via re-INVITEs)	All ports are released (inbound, outbound call licenses plus ASR licenses on those calls).

## Resource Manager

During registration, each IPCS provides its supported features to the Resource Manager (RM). The feature list contains a comma-separated list that includes attributes such as codec, CPA, file play format, and so on. The IPCS will be selected during a call based on this feature list.

A *preferred destination* is a list of preferred IPCSs. The RM tries to match from this list first, and if there is no match, the RM searches the non preferred destinations.

The RM checks for the additional parameter, `IPCSFeatureList`, in the `Extensions` section of the IVR profile (refer to “Step 11—Extensions” on [page 66](#)). For example, if you set the `XMLSetName1` parameter to `IPCSFeatureList`, and the `XMLSetValue1` parameter to `CPA,WAV`, Resource Manager searches for an IPCS that has CPA support and that can also play .wav files. The feature lists supported by HMP are `CPA` and `LocalBridge`.

The `IPCSFeatureList` parameters are mandatory—those parameters take precedence, along with the other mandatory criteria such as call direction (in/out), ASR support, and so on.

# Media Server Configuration

To configure the IPCS to use Convedia or other MSML servers, such as MRF:

1. In EMPS, go to the Servers > Media Server node. Configure all media servers under this node.
2. Right-click the SampleMediaServer node, and then click Create a copy.
3. Enter the name for the Media Server. For example, MedSrv1.
4. Select Copy Subtree.
5. Click Copy.
6. Under the new node, double-click MediaServerInfo, and enter the attributes shown in [Table 53](#).

**Table 53: Media Server Configuration**

Node	Tab	Attribute	Description
MedSrv1	General	Media Server URL	Specifies the URL to the Media Server machine; for example, <code>machinename:portnumber</code>
		Media Server Type	Specifies the name of the Media Server Type. Valid values: <ul style="list-style-type: none"> <li>• MRF</li> <li>• Convedia</li> </ul>
		Feature List	Features that media server supports, separated by semicolons. <b>Note:</b> The <code>pcum:0;pcma:8;cpa;localbridge</code> feature list is applicable for the MRF Media Server only.

Next, create a group, selecting Group Type as MEDIASVRGRP, containing the Media Server(s) to be used for primary and backup Media Server groups. (Refer to “Server Groups” on [page 81](#) for instructions on how to create a server group.)

Finally, configure your IPCS to point to the Media Server group(s) configured, as described in [Table 54](#) on [page 262](#).

**Table 54: IPCS Configuration for Media Server Groups**

Node	Tab	Attribute	Description
<IP Communication Server> IPCS Machine > Mcu > MediaController > MxML	General	Local SIP Port	Specifies the UDP port that will be used to listen for SIP message.
		Primary Media Server Group(s)	One or more media server group(s) that will be the primary resource used for any RTP media streaming.
		Backup Media Server Group(s)	One or more media server group(s) that will be used in case resources from the primary group are unavailable.
		Out of Service Ping Interval (seconds)	Specifies the interval, in seconds, between pings to out-of-service servers.

## G.729 Support

The IPCS, through NativeRTP, Intel Host Media Processing (HMP) or Convedia, supports calls using G.729, G.729A, G.729B, and G.729AB. Transcoding of those protocols to or from G.711 is also supported on bridged connections (refer to “Bridge Transfer” on [page 351](#) for information about Bridge transfers).

---

Note: The G729 codec is not supported for Solaris IPCS.

---

## Host Media Processing

For inbound calls, IPCS uses G.711 if it is a supported codec in the incoming INVITE. This is to minimize use of more expensive licenses.

For outbound calls that are bridged calls, the preferred codec matches the first leg. For pure outbound calls (no bridging), G.711 is the preferred codec. IPCS reserves the license(s) when the INVITE is sent out, but the license(s) is not allocated until the far end answers and chooses the codec. A G.711 license is required by Host Media Processing (HMP) for each call. If all of the G.711 ports are in use, no additional calls can be accepted even if G.729 ports are still available. If an enhanced RTP license is available, it is also reserved for the outbound call in addition to the G.711 license.

If an enhanced RTP license is reserved, the outgoing INVITE lists all of the codecs supported by the G.711 and enhanced licenses, with the preferred codec as described in the preceding paragraph. If the far end chooses G.711, a plain G.711 license is allocated and the enhanced RTP port is unreserved. If a G.729 codec is chosen, the enhanced RTP and G.711 license is allocated.

### Limitations

This section describes limitations that might occur with the G.729 media codec.

In the event of pure outbound calls that originate from the GVP media IPCS (which hosts the HMP media services), the SDP that goes in the outbound INVITE would be similar to the following example:

```
v=0
o=GenesysLab 3138817882 33456791 IN IP4 172.24.129.40
s=GenesysLab SIP Call
c=IN IP4 172.24.129.40
t=0 0
m=audio 49152 RTP/AVP 0 8 4 18
a=rtpmap:0 pcmu/8000
a=rtpmap:8 pcma/8000
a=rtpmap:4 g723/8000
a=rtpmap:18 g729/8000
a=fmtp:18 annexb=yes
```

In such an event, the following limitations or conditions might occur if the UAS that receives this INVITE supports only G.729/G.729A.

- If the UAS receiving the outbound INVITE from the GVP IPCS (with SDP that always contains payload=18, annexb=yes) responds with a 415 unsupported media, the call will be dropped and there is no retry even though the HMP IPCS supports G.729/G.729A.
- If the UAS responds with annexb=no by altering the preceding SDP, the IPCS will correctly process it and activate the G.729 license on HMP.

## LConvedia

For inbound calls, IPCS presents the codecs from the incoming INVITE to Convedia, and Convedia determines which codec to use for the call.

For outbound calls, IPCS presents in the outgoing INVITE all of the codecs that Convedia supports.

## Outbound Call Setup

The following process determines where the INVITE message will be sent and the value of the SIP TO header (in order of precedence):

1. If Primary Call Manager IP Address, Backup Call Manager IP Address, and Default Media/Signalling Gateway IP Address are not configured, and if the voice application does not provide an IP address as part of the DID, the voice application receives an error.
2. If Primary Call Manager IP Address is configured, the INVITE message will be sent to it. The TO header contains the number/username provided by the voice application. If the voice application does not contain the hostname, the hostname of the TO field will be set to the Primary Call Manager IP Address. If the call fails and Backup Call Manager IP Address is configured, another attempt will be made by sending the INVITE message to Backup Call Manager IP Address. If all attempts fail, the voice application receives an error.
3. If Default Media/Signalling Gateway IP Address is configured, an INVITE message will be sent to it. The TO header contains the number/username provided by the voice application. If the voice application does not contain the hostname, the hostname of the TO field will be set to the Default Media/Signalling Gateway IP Address. If the call fails, the voice application receives an error.
4. If Primary Call Manager IP Address, Backup Call Manager IP Address, and Default Media/Signalling Gateway IP Address are not configured, the INVITE message will be sent to the number/username and hostname provided by the voice application in the DID. If the voice application does not provide a hostname or the call is unsuccessful, the voice application receives an error.

## MRF

For outbound calls, IPCS adds all the codecs that MRF supports in the outgoing INVITE message.

IPCS pings the MRF server(s) every 30 seconds with the OPTIONS message.

## Outbound Call Resolution

Table 55 on [page 265](#) shows samples of outbound INVITE address resolutions.

**Note:** The resolved information only gives the username and hostname. It does give the exact SIP TO header format. This is not an exhaustive list of all possibilities.



**Table 55: Samples of Outbound INVITE Address Resolutions**

VoiceXML Destination (name_did@hostname: port)	Default Media Gateway (IPAddr: Port)	Session Manager (IPAddr: Port)	INVITE Destination (IPAddr:Port)	Resolved TO Values
abc123	(not configured)	(not configured)	ERROR	ERROR
abc123@11.11.11.11	(not configured)	(not configured)	11.11.11.11:5060	abc123@11.11.11.11
abc123@11.11.11.11:4444	(not configured)	(not configured)	11.11.11.11:4444	abc123@11.11.11.11: 4444
abc123	22.22.22.22	(not configured)	22.22.22.22: 5060	abc123@22.22.22.22
abc123@11.11.11.11	22.22.22.22	(not configured)	22.22.22.22: 5060	abc123@11.11.11.11
abc123@11.11.11.11:4444	22.22.22.22	(not configured)	22.22.22.22: 5060	abc123@11.11.11.11: 4444
abc123@11.11.11.11:4444	22.22.22.22: 5555	(not configured)	22.22.22.22: 5555	abc123@11.11.11.11: 4444
abc123	(ignored)	33.33.33.33	33.33.33.33: 5060	abc123@33.33.33.33
abc123@11.11.11.11	(ignored)	33.33.33.33	33.33.33.33: 5060	abc123@11.11.11.11
abc123@11.11.11.11:4444	(ignored)	33.33.33.33	33.33.33.33: 5060	abc123@11.11.11.11: 4444
abc123@11.11.11.11:4444	(ignored)	33.33.33.33: 6666	33.33.33.33: 6666	abc123@11.11.11.11: 4444

---

## SIP INFO

The IPCS supports SIP INFO to send and receive out-of-band DTMF tones. The IPCS also supports mid-call data exchange between the voice application and the far end using SIP INFO.

---

Note: If two call legs are connected/bridged using either call transfer or audio bridging, SIP messages from one leg will not be forwarded to the connected call.

---

## SIP INFO Message Details

The IPCS uses the SIP INFO method to transport data between the voice application and the far end, as outlined in RFC 2976. The transferring of data between the voice application and the far end can occur any time after the call is answered until the time the call is ended. For user data that the IPCS sends, the following features are supported:

- The SIP INFO header body type is set to `application/text`.
- The SIP INFO message body contains the user-defined data.

You can use the IPCS to send and receive DTMF data. Therefore, if the SIP INFO body type header field is `application/dtmf-relay`, the message will not be sent to the voice application. All other SIP INFO body types will be given to the voice application using the Genesys VoiceXML extension objects. Refer to the *Genesys Voice Platform 7.6 VoiceXML 2.1 Reference Manual* for more information.

### Example SIP INFO Message

```
INFO sip:4444@10.10.10.114 SIP/2.0
From: <sip:6261395@10.10.16.28>; tag=ds-4823-6b85031e
To: <sip:4444@10.10.10.114>; tag=1c28994
Contact: <sip:User_Name@10.10.16.28:5060; transport=udp>
Max-Forwards: 70
Call-ID: call-1123276076-1@10.10.10.114
CSeq: 4 INFO
Content-Length: 31
Via: SIP/2.0/UDP 10.10.16.28:5060; branch=z9hG4bK779f3e48-05f5-11da-98be-8cc100835a83
Content-Type: application/text
Supported: timer
U=0
My account number is 1234567890
```

## VoiceXML Extension

When the IPCS receives SIP INFO messages that are not DTMF-related, it appends them to the `Genesys.sip` array. The `sip.msgtype` is set to `INFO` and all header and body is assigned appropriately. For sending user data, use the `telephonydata.put` object class.

---

# SIP Re-INVITE

The IPCS supports incoming SIP `re-INVITE`. During the SIP session, a SIP endpoint can decide to change the characteristics of the media session. This is accomplished by sending a `re-INVITE`.

## SDP Updates of IP Address and/or Port

During the SIP session, an IP Address and/or RTP port might be changed for a SIP endpoint. This can either happen by IPCS receiving an SDP update in a SIP `re-INVITE`, or in an SDP update in an `ACK` to a `200` that the IPCS sent in response to a `re-INVITE` that it received with no Session Description Protocol (SDP).

### IVR State

The following are descriptions of IPCS behavior when receiving SDP changes in IP address and/or port in various IVR states:

- **Play Prompt (File or TTS)**—The current play prompt operation continues from the old SIP endpoint to a new SIP endpoint.
- **GetTones/SendTones**—The current send or receive tones operation continues from the old SIP endpoint to a new SIP endpoint.
- **Record**—The current record operation continues from the old SIP endpoint to a new SIP endpoint.
- **ASR**—The current ASR operation continues and starts receiving the audio data from a new SIP endpoint.

### Bridged Call

The following are descriptions of IPCS behavior when receiving SDP changes in IP address and/or port in various bridge modes:

- **Media (Local) Bridge**—Receiving changes in IP address and/or port while the call is bridged locally is supported. The current bridged calls continue without side effects.  
Hotword recognition, if active, is also unaffected.
- **Remote Bridge**—Receiving changes in IP address and/or port while the call is bridged remotely is supported. The changed SDP information will be sent to the other SIP endpoint.

## Sample SIP Call Flow

### Re-INVITE with No SDP

```

INVITE sip:301352@10.10.30.135 SIP/2.0
Via: SIP/2.0/UDP
    10.10.10.229;rport;branch=z9hG4bK0a0a0ae50000002544e4a14c00002cae0000001e
Content-Length: 0
Contact: <sip:10.10.10.229:5060>
Call-ID: 18A0D138-3623-4755-BEDF-333AF6B882D1@10.10.10.229
CSeq: 1 INVITE
From: "unknown"<sip:10.10.10.229>;tag=16965410917236
Max-Forwards: 70
To: <sip:301352@10.10.30.135>
User-Agent: SJphone/1.60.289a (SJ Labs)

SIP/2.0 200 OK
Via:
    SIP/2.0/UDP10.10.10.229;branch=z9hG4bK0a0a0ae50000002544e4a14c00002cae0000001e;rport
From: "unknown" <sip:10.10.10.229>;tag=16965410917236
To: <sip:301352@10.10.30.135>;tag=ds-4823-e6c41da1
Call-ID: 18A0D138-3623-4755-BEDF-333AF6B882D1@10.10.10.229
CSeq: 1 INVITE
Content-Length: 216
Contact: <sip:User_Name@10.10.30.135:5060;transport=udp>
Content-Type: application/sdp

v=0
o=GenesysLab 3345914514 33456789 IN IP4 10.10.30.15
s=GenesysLab SIP Call
c=IN IP4 10.10.30.15
t=0 0
m=audio 32842 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

ACK sip:User_Name@10.10.30.135:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP
    10.10.10.229;rport;branch=z9hG4bK0a0a0ae50000002544e4a14d0000576f00000022
Content-Length: 216
Call-ID: 18A0D138-3623-4755-BEDF-333AF6B882D1@10.10.10.229
CSeq: 1 ACK
From: "unknown"<sip:10.10.10.229>;tag=16965410917236
Max-Forwards: 70
To: <sip:301352@10.10.30.135>;tag=ds-4823-e6c41da1
User-Agent: SJphone/1.60.289a (SJ Labs)

v=0
o=GenesysLab 3345914514 33456789 IN IP4 10.10.30.15
s=GenesysLab SIP Call

```

```

c=IN IP4 10.10.30.15
t=0 0
m=audio 32842 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

```

### Re-INVITE with SDP

```

INVITE sip:User_Name@10.10.30.135:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP
      10.10.10.229;rport;branch=z9hG4bK0a0a0ae50000002544e4a1540000433200000023
Content-Length: 214
Contact: <sip:10.10.10.229:5060>
Call-ID: 18A0D138-3623-4755-BEDF-333AF6B882D1@10.10.10.229
Content-Type: application/sdp
CSeq: 2 INVITE
From: "unknown" <sip:10.10.10.229>; tag=16965410917236
Max-Forwards: 70
To: <sip:301352@10.10.30.135>; tag=ds-4823-e6c41da1
User-Agent: SJphone/1.60.289a (SJ Labs)

```

```

v=0
o=- 3364822988 3364822989 IN IP4 10.10.10.229
s=SJphone
c=IN IP4 10.10.10.230    Changed IP Address
t=0 0
a=direction:active
m=audio 49182 RTP/AVP 8 101    Changed RTP Port
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11,16

```

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP
      10.10.10.229;branch=z9hG4bK0a0a0ae50000002544e4a1540000433200000023;rport
From: "unknown" <sip:10.10.10.229>; tag=16965410917236
To: <sip:301352@10.10.30.135>; tag=ds-4823-e6c41da1
Call-ID: 18A0D138-3623-4755-BEDF-333AF6B882D1@10.10.10.229
CSeq: 2 INVITE
Content-Length: 207
Contact: <sip:User_Name@10.10.30.135:5060;transport=udp>
Content-Type: application/sdp

```

```

v=0
o=Genesys 487993409 487993410 IN IP4 10.10.30.15
s=Genesys SIP Call
c=IN IP4 10.10.30.15
t=0 0
m=audio 32842 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000

```

```
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

```
ACK sip:User_Name@10.10.30.135:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP
    10.10.10.229;rport;branch=z9hG4bK0a0a0ae50000002544e4a15400001a8200000025
Content-Length: 0
Call-ID: 18A0D138-3623-4755-BEDF-333AF6B882D1@10.10.10.229
CSeq: 2 ACK
From: "unknown"<sip:10.10.10.229>;tag=16965410917236
Max-Forwards: 70
To: <sip:301352@10.10.30.135>;tag=ds-4823-e6c41da1
User-Agent: SJphone/1.60.289a (SJ Labs)
```

## Call Hold Support

The IPCS supports incoming SDP updates when `c = 0.0.0.0`, `a=sendonly`, or `a=inactive`. This can either happen by IPCS receiving an SDP update in a SIP re-INVITE, or in an SDP update in an ACK to a 200 that IPCS sent in response to a re-INVITE that it received with no SDP.

The purpose of the `c=0.0.0.0`, `a=sendonly`, or `a=inactive` line is to notify IPCS to stop sending RTP packets and place the call on hold. The SIP originating endpoint takes the call off hold by sending a re-INVITE with the actual IP address of the remote SIP entity in the `c=` line (in place of `0.0.0.0`).

The SIP endpoint can put the call on hold in two ways:

- Use a connection IP address of `0.0.0.0` (`c=0.0.0.0`) in the SDP.
- Use `a=sendonly` or `a=inactive` in the SDP. The `a=sendonly` line indicates that the endpoint is willing only to send the media stream, not to receive it. The offer of `a=inactive` indicates that the endpoint is willing neither to send nor receive the media stream.

## IVR State

The following are descriptions of IPCS behavior when receiving SDP changes to place the call on hold.

- **Play Prompt (File or TTS)**—The current play prompt operation still continues internally, except that the GVP platform stops sending RTP packets to the SIP endpoint. When taking the call back off hold, the prompt will not resume as if it has been paused; instead, it resumes as if it had been muted. The IPCS resumes sending the RTP packets to the new SIP endpoint.
- **Get Tones**—The current get tones operation still continues, unaffected by the call being on hold. The DTMF (SIP INFO or RFC 2833) input processing will be supported unless `a=inactive` is set in the SDP.

- **Send Tones**—The current send tones operation will be affected for RFC2833 calls and IPCS stops sending tones to the SIP endpoint. If SIP INFO is being used, sending of tones is unaffected.
- **Record**—The current record operation will be affected when `c=0.0.0.0` and `a=inactive` are sent by the SIP endpoint. No RTP will be received for the recording. The record operation may be completed with a `TIMEOUT`.  
For `a=sendonly`, IPCS still receives RTP packets for the recording.
- **ASR**—The current ASR operation will be affected when `c=0.0.0.0` and `a=inactive` is sent by SIP endpoint. No RTP will be received for the recognition. The ASR operation may complete with a `noinput` result.  
For `a=sendonly`, IPCS still receives RTP packets for the recognition.

## Bridged Call

The following are descriptions of IPCS behavior when receiving SDP changes to place the call on hold in various bridge modes.

- **Media (Local) Bridge**—The leg requesting to be put on hold does not receive any more RTP packets. The other leg is unaffected, except that, if `a=inactive` is received in the re-INVITE, the other leg hears silence.  
Hotword recognition, if active, will be affected when `c=0.0.0.0` and `a=inactive` are sent by the SIP endpoint. No RTP will be received for recognition.  
For `a=sendonly`, IPCS still receives RTP packets for the hotword operation.
- **Remote Bridge**—If one leg requests to be put on hold, IPCS sends a re-INVITE to the other leg to also place the call on hold.

## Sample SIP Call Flow

```

INVITE sip:User_Name@10.10.30.135:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP
      10.10.10.229; rport; branch=z9hG4bK0a0a0ae50000002544e4a1540000433200000023
Content-Length: 214
Contact: <sip:10.10.10.229:5060>
Call-ID: 18A0D138-3623-4755-BEDF-333AF6B882D1@10.10.10.229
Content-Type: application/sdp
CSeq: 2 INVITE
From: "unknown"<sip:10.10.10.229>; tag=16965410917236
Max-Forwards: 70
To: <sip:301352@10.10.30.135>; tag=ds-4823-e6c41da1
User-Agent: SJphone/1.60.289a (SJ Labs)

v=0
o=- 3364822988 3364822989 IN IP4 10.10.10.229
s=SJphone
c=IN IP4 0.0.0.0  Changed IP Address

```

```

t=0 0
a=direction:active
m=audio 49162 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11,16

SIP/2.0 200 OK
Via: SIP/2.0/UDP
      10.10.10.229;branch=z9hG4bK0a0a0ae50000002544e4a1540000433200000023;rport
From: "unknown" <sip:10.10.10.229>;tag=16965410917236
To: <sip:301352@10.10.30.135>;tag=ds-4823-e6c41da1
Call-ID: 18A0D138-3623-4755-BEDF-333AF6B882D1@10.10.10.229
CSeq: 2 INVITE
Content-Length: 207
Contact: <sip:User_Name@10.10.30.135:5060;transport=udp>
Content-Type: application/sdp

v=0
o=Genesys 487993409 487993410 IN IP4 10.10.30.15
s=Genesys SIP Call
c=IN IP4 10.10.30.15
t=0 0
m=audio 32842 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

ACK sip:User_Name@10.10.30.135:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP
      10.10.10.229;rport;branch=z9hG4bK0a0a0ae50000002544e4a15400001a8200000025
Content-Length: 0
Call-ID: 18A0D138-3623-4755-BEDF-333AF6B882D1@10.10.10.229
CSeq: 2 ACK
From: "unknown"<sip:10.10.10.229>;tag=16965410917236
Max-Forwards: 70
To: <sip:301352@10.10.30.135>;tag=ds-4823-e6c41da1
User-Agent: SJphone/1.60.289a (SJ Labs)

```

## Taking Call off Hold

If a call is already on hold, IPCS supports incoming SDP updates when the `c=` line is not `0.0.0.0`, or `a=sendrecv` or `a=active`. This can either happen by IPCS receiving an SDP update in a SIP re-INVITE, or in an SDP update in an ACK to a 200 that the IPCS sent in response to a re-INVITE that it received with no SDP. This takes the call off hold.



## Re-INVITE Received When Bridging

Receiving SIP re-INVITE when the calls are in process of bridging is not supported. IPCS returns a SIP response of 491 - Request Pending to the SIP endpoint.

## SDP Updates When DTMF or Audio Codec Changes

The IPCS does not support SDP changes to DTMF or audio codecs. This can either happen by IPCS receiving an SDP update in a SIP re-INVITE, or in an SDP update in an ACK to a 200 that the IPCS sent in response to a re-INVITE that it received with no SDP.

The IPCS responds with a 488 - Not Acceptable Here.

## Convedia

The IPCS does not support changes to the SDP in Convedia integrations. The IPCS responds with a 488 - Not Acceptable Here.

## MRP

The IPCS does not support changes to the SDP in MRP integrations. The IPCS responds with a 488 - Not Acceptable Here.

## Adding New Media Streams

The SIP/SDP RFC permits media streams to be dynamically removed, declined, modified, or added. However, the IPCS supports only one media stream per connection; therefore, the IPCS declines the SIP request by sending a SIP response of 488, for any additions that increase the number of media streams beyond one for a single connection.

## Re-INVITE Requests Before a Final Response to Initial INVITE

If the GVP receives a second INVITE request before it sends the final response to the first INVITE request that has a lower CSeq sequence number on the same dialog, the IPCS, through the GVPSipMgr stack, returns a 500 Server Internal Error response to the second INVITE request.

---

## Propagation of SIP Header Values

IPCS propagates the `P-Asserted-Identity` and the `Call-ID` SIP headers to the VoiceXML application. This feature is enabled by default. If the incoming SIP message has multiple values for these two headers, they are sent as a comma separated list to the VoiceXML application.

### P-Asserted-Identity

A SIP server can provide a privacy service by asserting the identity of the end user or end system into a SIP message `P-Asserted-Identity` header. When IPCS receives an INVITE with this header, IPCS passes it, as is, to the VoiceXML application.

### Call-ID

Every INVITE message must have a `Call-ID` header. When IPCS receives an INVITE with this header, IPCS passes it, as is, to the VoiceXML application.

### Implementation Details

When IPCS receives an INVITE with a `P-Assert-Identity` header, it will verify that IPCS is configured to propagate the value of this header to the VoiceXML application, then collect all the values and present them as a comma separated list to the VoiceXML application.

For more information about SIP Headers, see the *Genesys Voice Platform 7.6 VoiceXML 2.1 Reference Manual*.

---

## Session Timers

The IPCS supports RFC-4028, which defines a keep-alive mechanism for SIP sessions. The configuration parameters shown in Table 56 on [page 275](#) are used for Session Timers:

**Table 56: Session Timer Parameters**

Node	Tab	Attribute	Description
IPCS > PopGateway	Session	Enable Session Timers	Check box that specifies whether Session Timer support is enabled for a call session.
		Session Timer Interval (secs)	Specifies the time interval, in seconds, during which a call session must be refreshed; otherwise, the session expires. Values are: Range: 90–86400 Default: 1800
		Session Timer Refresher	Specifies which user agent initiates refreshing of a call session. Choices are: Local—IPCS refreshes the session. Remote—The far end refreshes the session.  For inbound calls, if the refresher is already specified by the far end, this parameter will be ignored.

Table 57 shows example behavior.

**Table 57: Example Behavior**

Enable Session Timers Check Box Selected, Session Timer Interval=1800		
	Session Timer Refresher = Local	Session Timer Refresher = Remote
Outbound Calls	Outgoing INVITE contains the following headers: Supported: timer Session-expires: 1800;refresher=uac Min-SE: 90	Outgoing INVITE contains the following headers: Supported: timer Require: timer Session-expires: 1800;refresher=uas Min-SE: 90

**Table 57: Example Behavior (Continued)**

Enable Session Timers Check Box Selected, Session Timer Interval=1800				
Inbound Calls	Far-end supports Session Timer?		Far-end supports Session Timer?	
	Yes	No	Yes	No
	<p>If INVITE has a Session-Expires header, the timer value is copied in the 2xx response.</p> <p>If refresher is present, it is also copied in the 2xx response.</p> <p>If refresher is absent, refresher is set to UAS.</p>	<p>The following headers are added in the outgoing 200 OK message:</p> <p>Supported: timer</p> <p>Session-expires: 1800;refresher=uas</p> <p>Min-SE: 90</p>	<p>If INVITE has a Session-Expires header, the timer value is copied in the 2xx response.</p> <p>If refresher is present, it is also copied in the 2xx response.</p> <p>If refresher is absent, refresher is set to UAC.</p>	<p>The following headers are added in the outgoing 200 OK message:</p> <p>Supported: timer</p> <p>Session-expires: 1800;refresher=uas</p> <p>Min-SE:90</p>

GVP adds the following headers to support Session Timers:

- Supported
- Require
- Session-Expires
- Min-SE

Session Timer and refresher values are negotiated by GVP.

---

Note: GVP does not handle the 422 error code.

---

## DTMF Rendering

The IPCS always uses RFC 2833 for DTMF if it is supported by the far end; otherwise, it falls back to a configurable DTMF mode if RFC 2833 cannot be negotiated.

For DTMF detection, the IPCS always detects both RFC 2833 and SIP INFO tones. If RFC 2833 cannot be negotiated, and if the fallback is Inband DTMF, Inband DTMF will also be detected.

MRP does not support DTMF as InBand DTMF. That is, it does not detect InBand DTMF even if IPCS is configured to detect it. It only supports RFC 2833 DTMF.

For NativeRTP stack, fallback DTMF detection is SIP INFO and InBand DTMF.

See Table 58 on [page 277](#) to configure the IPCS:

**Table 58: IPCS Configuration for DTMF Rendering**

Node	Tab	Attribute	Description
IPCS > Mcu	DTMF	Fallback DTMF Mode	<p>Specifies the type of DTMF used if RFC 2833 cannot be negotiated. The DTMFs that are generated fall back to this type. DTMF detection always recognizes both RFC 2833 and SIP INFO. If Inband is selected, Inband DTMF will also be detected as a fallback. Values are:</p> <ul style="list-style-type: none"> <li>• SIP INFO Msg</li> <li>• Digitized Inband RTP</li> </ul> <p>The default value is SIP INFO Msg.</p>

---

## RTP Tone Detection

The IPCS supports DTMF tones using RFC 2833, regardless of the media codec used by a particular voice stream. The IPCS can detect tones encoded in raw digitized format. RFC 2833 supports multiple ways to encode and decode tones in an RTP packet.

### Generating Tone Packets

RFC 2833 allows each RTP packet to contain one or more DTMF tones. The IPCS generates a single tone for each packet.

### Detecting Tone Packets

Since different SIP/RTP phones and media gateways interpret RFC 2833 differently, the IPCS allows configuration of the tone detection mechanism. Table 59 on [page 278](#) lists the supported tone packets.

**Table 59: Supported Tone Packets**

Mode	Tone per Packet Support	Description
0 (Default)	Single Tone per Packet	RTP Header Timestamp Only The RTP header timestamp remains constant for each tone instance. The timestamp changes for a new tone. RTP Header Marker bit is ignored. This is the default.
1	Single Tone per Packet	RTP Header Marker Bit Only Marker bit is set to 1 for each new tone. Only the first packet for a particular tone has this bit set to 1. All subsequent packets for same tone have marker bit set to 0. The RTP timestamp is ignored.
2	Single Tone per Packet	Both RTP Header Market Bit and Timestamp Marker bit is set to 1 for each new tone. Only the first packet for a particular tone has this bit set to 1. All subsequent packets for same tone have marker bit set to 0. The RTP header timestamp remains constant for each tone instance. The timestamp changes for a new tone.
3	Single Tone per Packet	Either Header Marker or Timestamp Marker bit is set to 1 for each new tone, and packets for same tone have marker bit set to 0. Or timestamp changes for new tones.
4	Multiple tones per packet	The E (end bit) of the RTP body is used to differentiate instances of packets. The RTP header timestamp and mask bits are ignored.



## Chapter

# 11

## H.323 Session Manager

This chapter provides information about configuring the H.323 Session Manager.

This chapter contains the following sections:

- [Detecting DTMF, page 279](#)
- [Gatekeeper, page 280](#)
- [Codec, page 280](#)
- [Bridge and Transfer, page 281](#)
- [Numbering Type and Plan, page 282](#)
- [Fast Start and Tunneling, page 282](#)
- [Configuring Media Gateway, page 283](#)

---

## Detecting DTMF

Depending on the IP Communication Server (IPCS) configuration, Genesys Voice Platform (GVP) supports the following:

- H.245 alphanumeric and H.245 signal.
- RFC2833.

---

**Note:** The H.323 Session Manager is not able to determine whether the IPCS uses Digitized Inband RTP.

---

GVP supports DTMF tones only to the IPCS, and only the digit is provided.

---

# Gatekeeper

You can configure GVP to send all outgoing calls to a gatekeeper. H.323 Session Manager also accepts calls from the gatekeeper.

Configure the H.323 Session Manager for `Enable RAS Messages` and enter the IP address and port of the gatekeeper. Also configure the H.323 Session Manager for the `Alias Address` parameter.

Configure the gatekeeper to accept multiple calls from the same alias address and to accept calls from a non-registered end point.

The gatekeeper can also be configured to be functioning in the semi-routed mode.

- H.225 semi-routed call mode—Only H.225 signaling is routed through the gatekeeper
- H.225-H.245 semi-routed call mode—Both H.225 and H.245 signaling are routed through the gatekeeper

---

Note: Under semi-routed mode, RAS messages are not exchanged between HSM and GK.

The `Enable RAS message` check box in the EMPS configuration must be cleared.

---

You can configure GVP to send outgoing calls to the backup gatekeeper by configuring the backup gatekeeper IP address and port in the H.323 Session Manager. When an outgoing call through the primary gatekeeper fails with the reason `Resource Unavailable`, the H.323 Session Manager tries to place the call using the backup gatekeeper configuration.

---

Note: The backup gatekeeper works in semi-routed mode only.

---

---

# Codec

The following codecs are supported as part of codec negotiation for inbound and outbound calls.

- G711Alaw64k
- G711Ulaw64K
- G729
- G729AnnexA
- G729wAnnexB
- G729AnnexAwAnnexB
- G7231



The following codecs are supported as part of codec negotiation while bridging calls.

- G711Alaw64k
- G711Ulaw64K
- G729
- G729AnnexA
- G729wAnnexB
- G729AnnexAwAnnexB
- G7231
- gsmFullRate

The parameters shown in [Table 60](#) are used for codec negotiation. You can add these parameters through the Add New Attribute function in the H323SessionManager node.

**Table 60: Additional Codec Parameters**

Attribute	Value	Description
AllowG729Sibbling	1	<p>Enables the HSM to consider the G729 codec and the G729AnnexA codec as the same. This is also the case for the G729wAnnexB and G729AnnexAwAnnexB codecs.</p> <p>Values are:</p> <ul style="list-style-type: none"> <li>• 0—Disables</li> <li>• 1—Enables</li> </ul>

## Bridge and Transfer

GVP supports the bridging and blind transfer of two calls.

**Note:** Bridging calls is supported with the Cisco Media Gateway only.

### Bridged Calls:

When two calls are bridged, both control flows go through the IPCS. To bridge calls:

1. The voice application's VoiceXML transfer must specify `bridge="true"`.
2. The Media Gateway must provide the same media channel throughout the duration of a call, even when the capabilities change.

### Blind Transfer Calls:

When two calls are blind transferred, the control flow leaves GVP. To blind transfer calls:

1. The voice application's VoiceXML transfer must specify `bridge="false/blind"`.
2. The H.323 Session Manager must be configured so that `Call Transfer Method` is set to `H.450.2`.
3. The following values must be set in `EMPS > Provision IVR Profile > Transfer`:
  - a. `Enable Transfer Check Box`—selected
  - b. `Transfer Type`—`1SignalChannel`
  - c. `Transfer Option`—`SIPRefer`
4. The phone number specified for the transfer in VoiceXML must be recognized by the Media Gateway from which the inbound call arrived, because the blind transfer is performed by that Media Gateway.

---

Note: The H.323 Session Manager supports H.225 forwarding for active calls; however, since this is not part of the H.323 recommendation, not all Media Gateways support it.

---

---

## Numbering Type and Plan

Media Gateways that receive outbound calls from the H.323 Session Manager must have the same numbering type and plan as the H.323 Session Manager. Your voice application must provide the proper outbound call format for outbound calls.

---

## Fast Start and Tunneling

### Fast and Slow Start

GVP supports both Fast Start and Slow Start. For inbound calls, the H.323 Session Manager uses these characteristics as they are used by the incoming call. For outbound calls, the H.323 Session Manager uses these characteristics as specified in its configuration. The H.323 Session Manager initiates the outbound call with Fast Start, but if the terminating party does not support Fast Start, the H.323 Session Manager switches to Slow Start.

### H245 Tunneling

GVP supports H245 Tunneling, in which H.245 messages are passed within the Q.931 Call Signaling Channel.

To enable this feature, set the H.245 Tunneling parameter under H.323 Session Manager.

---

## Configuring Media Gateway

When you are not using a gatekeeper, GVP may send outbound calls to any of the Media Gateways specified in the Resource Manager's configuration. Therefore, you must configure all Media Gateways to receive any outbound number sent by the voice application(s).

The H.323 Session Manager exchanges empty capabilities with the Media Gateway in order to re-establish a media session during a call-transfer bridge.





## Chapter

# 12 IVR Server Client

This chapter describes the IVR Server Client heartbeat, the `FlowControl` message, and the Universal Connection ID.

This chapter contains the following sections:

- [IVR Server Client Heartbeat, page 285](#)
- [Flow Control, page 288](#)
- [Universal Connection ID, page 289](#)

---

## IVR Server Client Heartbeat

The IVR Server Client heartbeat option uses `KeepAlive` messages to determine the health of the IVR Server.

The IVR Server Client periodically sends the `KeepAliveRequest` message to the IVR Server and waits for the `KeepAliveResponse` from the IVR Server.

If the IVR Server Client does not receive the `KeepAliveResponse` from the IVR Server or it times-out, it marks that particular IVR Server as unavailable. The IVR Server Client sends an error message to the Call Flow Assistant (CFA) for all of the active and new calls in this case.

The IVR Server Client periodically pings the IVR Server that was unavailable to re-establish the TCP/IP connection.

## Configuring GVP

To enable this feature, you must configure specific parameters in the Element Management Provisioning System (EMPS).

1. In a web browser, access the EMPS login screen by entering the URL `http://<EMPS-hostname>:9810/spm`.
2. Log in as `Admin` and enter your password.

3. On the EMPS navigation tree, expand the Servers object > ISVR > <ServerName>, and then right-click IServerInfo.
4. Select Edit.
5. Configure the parameters shown in [Table 61](#), and then click Save.

**Table 61: IVR Server Keep Alive Parameters**

Parameter	Description
Enable KeepAlive Request	Check box that enables or disables the KeepAlive Request option from the IVR Server Client to the IVR Server.
KeepAlive Request Interval	Specifies, in seconds, the interval in which the IVR Server Client sends the KeepAlive request to the IVR Server. Range: 2–3600 seconds Default: 5 seconds
Number of KeepAlive Request	Specifies the number of requests to be sent to the IVR Server before being marked as unavailable. Range: 2–5 Default: 3
KeepAlive Response Timeout	Specifies, in seconds, how long the IVR Server Client waits for the KeepAlive Response from the IVR Server. Range: 2–5 seconds Default: 3 seconds

## Success and Failure Scenarios

This section describes different success and failure scenarios with the KeepAliveRequest message.

### KeepAliveRequest Success

1. After the IVR Server Client has successfully logged into the IVR Server, it checks if the KeepAliveRequest is enabled.
2. If the KeepAliveRequest is enabled, the IVR ServerClient starts sending the KeepAliveRequest as configured in the EMPS.
3. If a KeepAlive response is received, the IVR Server Client does not take any action.

## KeepAliveRequest Failure

1. If the IVR Server fails to send a `KeepAliveResponse` back to the IVR Server Client, the IVR Server Client times-out according to the timeout period configured in the EMPS.
2. The IVR Server Client keeps sending the `KeepAliveRequest` message to the IVR Server for a preconfigured number of times. If all of the attempts fail to get a response from the IVR Server, the IVR Server Client marks the IVR Server as unavailable.

### Single IVR Server Configuration

1. The IVR Server Client sends the `RESULT=FAILURE&REASON=FAILED TO CONTACT I-SERVER` response to the CFA for all new calls and route requests.
2. The IVR Server Client sends the `QUEUE_ADAPTER_STATE_REQ&devicestate=down&response=I-Server Down` response to the CFA for other than new calls and route requests. The IVR Server Client does not resend this message if any subsequent request or message comes from the CFA for the same call.
3. The IVR Server Client cleans the call details upon receiving the `EndSession` and `UPDATE_CALL_STATUS_REQ&CALLSTATUS=6` from the CFA.

---

Note: The IVR Server Client does not send `QUEUE_ADAPTER_STATE_REQ` back to the CFA if the IVR Server is marked as unavailable.

---

### Multiple IVR Servers Configuration

1. The IVR Server Client sends the `RESULT=FAILURE&REASON= FAILED TO CONTACT I-SERVER` response to the CFA for all route requests.
2. The IVR Server Client sends the `QUEUE_ADAPTER_STATE_REQ&devicestate=down&response=I-Server Down` response to the CFA for other than new calls and route requests. The IVR Server Client does not resend this message if any subsequent request or message comes from the CFA for the same call.
3. The IVR Server Client cleans the call details upon receiving the `EndSession` and `UPDATE_CALL_STATUS_REQ&CALLSTATUS=6` from the CFA.

---

Note: The IVR Server Client does not send `QUEUE_ADAPTER_STATE_REQ` back to the CFA if the IVR Server is marked as unavailable.

---

4. New calls will be placed on the available IVR Servers.

---

**Note:** The IVR Server can operate in load balancing mode. For load balancing, you can configure two or more IVR Servers to support the same set of IVR Server Clients. The IVR Server Client uses the round-robin method for distributing calls. There is no shared state between IVR Servers, so once a call has been started on a particular IVR Server, all further operations for that call occur on that same IVR Server.

---

## After KeepAliveRequest Failure

1. The IVR Server Client periodically pings the IVR Server that was unavailable to re-establish the TCP/IP connection.
2. Once the connection is re-established, the IVR Server Client resets the KeepAliveRequest timer and starts periodically sending the KeepAliveRequest.

---

# Flow Control

The IVR Server Client supports the FlowControl message. This message enables an IVR Server to be taken out of service, and brought back into service, with minimal impact to service. The FlowControl message is useful when you are using load-balanced IVR Servers and you want to take one member of the group offline (for example, for an upgrade).

The FlowControl message is triggered by a configuration option in the IVR Server application configured in Configuration Manager. When FlowControl is turned on, the IVR Server is marked out of service, and GVP will not send any new calls to it.

When FlowControl is turned off, the IVR Server is marked in service, and new calls can be sent to it.

---

**Note:** The IVR Server Client marks the IVR Server as down. It does not disconnect the TCP/IP connection, and it does not log out of the IVR Server.

This feature does not have any impact on the Heartbeat message on either the IVR Server Client or the IVR Server. They continue working as-is (that is, even after the IVR Server is marked as down, the Heartbeat message still can flow between the IVR Server Client and the IVR Server).

---

For additional information about the FlowControl message, refer to the *IVR Interface Option 7.x IVR Server System Administrator's Guide*.



### Single IVR Server Configuration

- After the IVR Server has been marked as down, existing calls proceed normally.
- The IVR Server Client sends a `RESULT=FAILURE&REASON=FAILED TO CONTACT I-SERVER` response to the CFA for all new calls.
- If the IVR-Server Client receives the `FlowControl` message more than one time with the same value (`STATUS=ON` or `STATUS=OFF`), it processes only the first message.

### Multiple IVR Servers Configuration

- After the IVR Server has been marked as down, existing calls proceed normally.
- New calls are placed on the working IVR Servers (the servers that are not marked as down by the IVR Server Client).
- If the IVR-Server Client receives the `FlowControl` message more than one time with the same value (`STATUS=ON` or `STATUS=OFF`), it processes only the first message.

---

## Universal Connection ID

The IVR Server Client retrieves the Universal Connection ID from Genesys Framework and passes it back to the voice application.

---

Note: If the IVR Server sends the Universal Connection ID value back to the IVR Server Client, the IVR Server Client sends the Universal Connection ID value to the CFA in the `CONNID` parameter (because the Universal Connection ID is the preference).

If the IVR Server fails to send the Universal Connection ID value back to the IVR Server Client, the IVR Server Client sends the Connection ID value to the CFA in the `CONNID` parameter.

If the CFA gets the Universal Connection ID parameter from the IVR Server Client, it sends this value to the PopGateway.

---

For more information, refer to the *Genesys Voice Platform 7.6 VoiceXML 2.1 Reference Manual*.





## Chapter

# 13 Outbound Notification Manager

This chapter describes the Outbound Notification Manager (OBN Manager), its components, and its workflow.

This chapter contains the following sections:

- [Overview, page 291](#)
- [OBN Manager Components and Workflow, page 292](#)
- [OBN Manager Interfaces, page 294](#)
- [Error Codes Returned by OBN Manager, page 298](#)
- [Provisioning Voice Applications, page 299](#)
- [Integrating with Outbound Contact Server, page 299](#)

---

## Overview

Outbound Notification (OBN) Manager enables Genesys Voice Platform (GVP) customers to make outbound calls using GVP, and to initiate these calls using simple HTTP requests. It is a high-performance, scalable solution for single or multiple customers. OBN Manager provides simplified configuration, provisioning, and troubleshooting.

OBN Manager, along with other components in GVP, supports both single-tenancy and multi-tenancy—but not simultaneously.

OBN Manager accepts HTTP requests from the customer's trigger voice application(s), and it uses one or more Voice Communication Server/IP Communication Server (VCS/IPCS) machines to create a new outbound connection.

After a connection is successfully established, OBN Manager transfers control to VCS/IPCS, and then executes a pre-provisioned Voice Extensible Markup

Language (VoiceXML) Interactive Voice Response (IVR) application on that outbound connection.

## OBN Manager Implementation Example

This section provides an example of how one type of customer—in this case, an airline—might utilize the functionality of OBN Manager.

For example, an airline can use Outbound Notification Manager to make automated calls when it is necessary to notify passengers about a flight change, and to reschedule their flights.

Using OBN Manager, the customer can instruct GVP to place a call to a given phone number, and then play a provisioned voice application on that call. Outbound Notification Manager places the call by contacting VCS/IPCS, which then executes the voice application on that call.

The voice application itself can be as complex and diverse as required. It can suggest alternative flights, make a new reservation interactively, and perform other functions, depending on how it is coded.

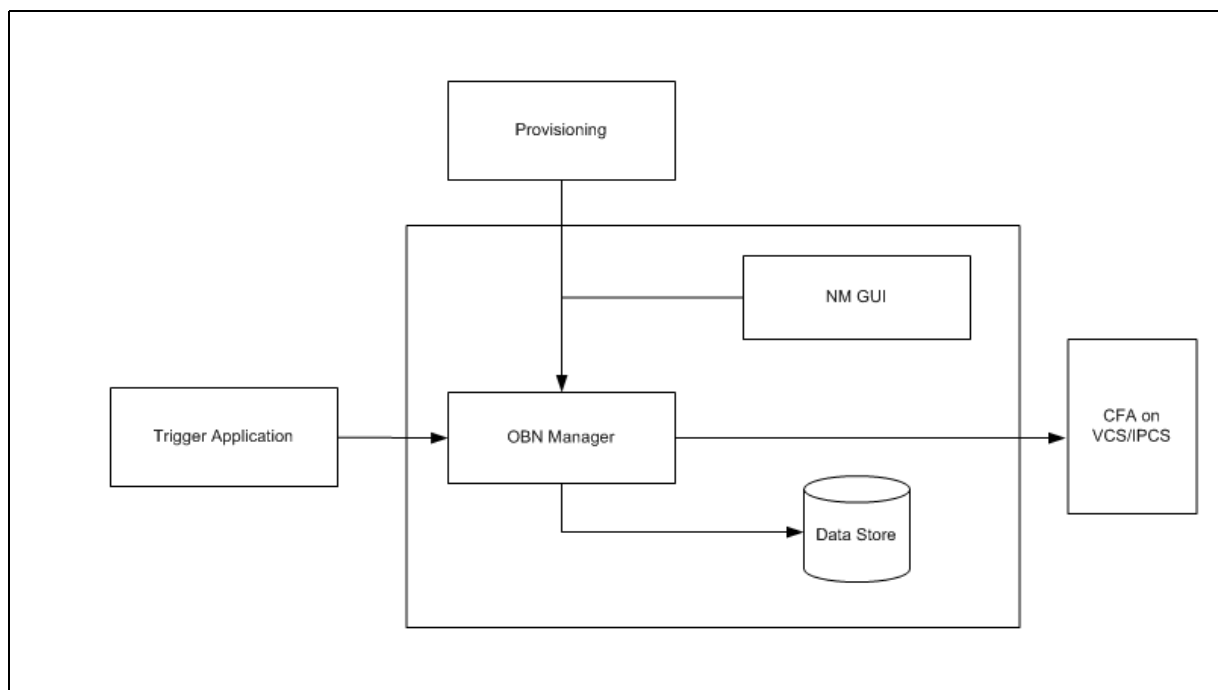
---

## OBN Manager Components and Workflow

This section provides an overview of the steps involved in placing an outbound call with OBN Manager, and it describes the components involved in that process.

### OBN Manager Components

Figure 134 on [page 293](#) illustrates the software components and processes for OBN, and shows how they interact.



**Figure 134: Outbound Notification Manager Architecture**

## Trigger Applications

A trigger application (TA), which is located at the customer's site, sends notifications (also referred to as triggers in this context) to OBN Manager whenever an outbound call needs to be initiated (triggered). This trigger is an HTTP request in the format described in "OBN Manager Interfaces" on [page 294](#).

OBN Manager receives this trigger request, and then assigns an ID to it, validates it, and stores it in its database. If the request contains errors, OBN Manager sends an error message to the trigger application. (See Table 62 on [page 298](#) for a list of the possible error codes.)

After successful storage, OBN Manager returns a Success message response to the trigger application in order to indicate that the request is now queued in OBN Manager. However, this does not mean that the call has been placed.

OBN Manager retrieves the request data from its database, and then makes a request to Call Flow Assistant (CFA) on the VCS/IPCS machine to make a call. If it is able to connect to CFA, OBN Manager assumes that the request has been successfully processed, and it treats the request as finished.

OBN Manager waits for a configured amount of time (the default is 5-minutes) before deleting such a request from its database. During this time period, if CFA notifies OBN Manager that it was not able to make the outbound call for any reason, OBN Manager resets the status of the request to unprocessed.

At this time, OBN Manager checks the values of the `timeToLive` and `max_attempts` parameters associated with the request, and it also checks the number of retries associated with the request.

If either `timeToLive` or `max_attempts` has expired, OBN Manager calls the Failure URL associated with the request, and then deletes the request from its database. In this case, the request does not result in a call, and it is assumed that, by calling the Failure URL, OBN Manager has notified the customer about the outcome.

If neither `timeToLive` nor `max_attempts` has expired, OBN Manager sends the request again after a certain time interval.

## Provisioning Applications

Multiple applications can be provisioned for a single OBN Manager machine. In this case, whenever a change is made to an application that uses one or more OBN Manager machines, EMPS notifies each of those OBN Manager machines that data related to their applications has changed. If this happens, OBN Manager re-initializes itself with the new application data.

---

Note: The OBN Manager process is not restarted; the application data is merely refreshed.

---

If a new application is provisioned and configured to use OBN Manager, all of the selected OBN Manager machines receive the new application's data. As soon as this happens, they are ready to process trigger requests for that application.

For more information about provisioning applications for OBN Manager, see “Provisioning an IVR Profile” on [page 49](#).

The following sections describe the format of the HTTP requests that the trigger application must use in order to work with OBN Manager.

---

## OBN Manager Interfaces

The requests that the trigger application sends can be single requests or bulk requests; each type of request has a different format, which the following sections will illustrate.

### Interface Parameters

This section describes the parameters that are used in both the single request interface and the bulk request interface:

**notifyprocess:** Process name of the new OBN Manager—that is, `obnmanager`. (Mandatory)

<b>action:</b>	Trigger application action. The value must be trigger . (Mandatory)
<b>token:</b>	Unique identifier generated by the trigger application (TA) for this request. (Mandatory)
<b>appname:</b>	Application name that has been provisioned to handle this outbound call. (Mandatory)
<b>customername:</b>	Customer that has been provisioned for this request. (Mandatory)
<b>resellername:</b>	Reseller that has been provisioned for this request. (Optional, for backward compatibility with older applications)
<b>telnum:</b>	Outbound telephone number to dial out. (Mandatory)
<b>ANI:</b>	The telephone number that is sent to the VCS/IPCS as the identification for the outbound call. (Optional)
<b>timetolive:</b>	Amount of time, in seconds, that this request is valid in OBN Manager. (Mandatory) The default value is 10 minutes. The maximum value allowed is 1440: any supplied value greater than this is logged as a warning, and a value of 1440 is set for this parameter.
<b>max_attempts:</b>	Maximum number of times that OBN Manager tries to place the call on VCS/IPCS machines, before giving up the request. (Mandatory) The default value is 5. The maximum value allowed is 25: any supplied value greater than this is logged as a warning, and a value of 25 is set for this parameter.
<b>failure_url:</b>	TA's Failure URL, which OBN Manager calls, if the request is unsuccessful. (Optional) There should be a valid default value in the application provisioning. If neither value is present, the request is rejected. <b>Note:</b> This value must be URL-encoded; otherwise, any parameters appended to the URL are not processed correctly.

## Single Request Interface

The following is an example of a single request from the trigger application:

Request:

```
http://dev-test:9810/obninterface.php?notifyprocess=obnmanager&action=trigger&token=abc123
&appname=OBNAApp3&customername=OBNSigC&resellername=OBNSigR&telnum=626138&ani=123456789
&timetolive=20&max_attempts=5&failure_url=http%3A%2F%2Ftest.genesyslab.com%2Fobnfai%2F
obnfai lure.php
```

Success Response:

```
<?xml version="1.0" ?>
  <RESPONSE RESULT="SUCCESS" TOKEN="abc123" />
```

**Failure Responses:**

```
<?xml version="1.0" ?>
  <FAILURE REASONCODE="100" REASON="Missing Token" />

  <?xml version="1.0" ?>
  <FAILURE TOKEN="abc1" REASONCODE="106" REASON="Missing Max Attempts Value" />
```

Failure Response after request was queued and error in placing the call:

```
http://test.genesyslab.com/obnfailures/obnfailure.php?TOKEN=abc123&REQUEST_ID=1112831499
&REASONCODE=300&REASON=Unable%20to%20place%20call.%20[Maximum%20Attempts%20have%20been%2
0reached]
```

If the OBN request in the incoming message is valid, the single request interface sends a Success response.

For the request item in the post data, validation is performed—that is, all of the mandatory parameters are validated. Any request with a Failure URL must be encoded.

If any request contains an error, an error message is sent. (See “Error Codes Returned by OBN Manager” on [page 298](#) for details.) This is done for each request that contains an error. The OBN requests within the single request that contains an error must be corrected and resent.

---

**Note:** After the successful requests from a single request have been queued, OBN Manager failures are communicated by calling the Failure URL.

---

## Bulk Request from the Trigger Application

The following is an example of a bulk request from the trigger application:

```
http://dev-test:9810/obninterface.php?notifyprocess=obnmanager&action=trigger
```

Please note this is the post data: obnbulk=<?xml version='1.0' ?>

```
<OBN>
  <Request>
    <token>abc123</token>
    <customername>OBNSigC</customername>
    <appname>OBNAppl</appname>
    <max_attempts>4</max_attempts>
    <TIMETOLIVE>5</TIMETOLIVE>
    <Telnum>4190</Telnum>
    <Ani>12345</Ani>
    <failure_url>ivrmachine</failure_url>
  </Request>

  <Request>
    <token>abc124</token>
```



```

    <customername>OBNSigC</customername>
    <appname>OBNAApp1</appname>
    <max_attempts>4</max_attempts>
    <TIMETOLIVE>5</TIMETOLIVE>
    <Telnum>4191</Telnum>
    <Ani>123</Ani>
    <failure_url>ivrmaschine</failure_url>
</Request>

<Request>
    <token>abc125</token>
    <customername>OBNQATests</customername>
    <appname>QAApp1</appname>
    <max_attempts>4</max_attempts>
    <TimeToLive>5</TimeToLive>
    <Telnum>4192</Telnum>
    <Ani>1111</Ani>
    <failure_url>ivrmaschine</failure_url>
</Request>

<Request>
    <token>abc126</token>
    <customername>OBNQATests</customername>
    <appname>QAApp1</appname>
    <max_attempts>4</max_attempts>
    <TimeToLive>5</TimeToLive>
    <Telnum>4193</Telnum>
    <Ani>4444444</Ani>
    <failure_url>ivrmaschine</failure_url>
</Request>
</OBN>

```

**Response:**

(In case of success)

```

<?xml version="1.0" ?>
<BULK_RESPONSE>
  <RESPONSE RESULT="SUCCESS" TOKEN="abc123"/>
  <RESPONSE RESULT="SUCCESS" TOKEN="abc124"/>
  <RESPONSE RESULT="SUCCESS" TOKEN="abc125"/>
  <RESPONSE RESULT="SUCCESS" TOKEN="abc126"/>
</BULK_RESPONSE>

```

(In case of error)

```

<?xml version="1.0" ?>
<BULK_RESPONSE>
  <FAILURE TOKEN="abc123" REASONCODE="200" REASON="Invalid Max Attempts Value"/>
  <FAILURE TOKEN="abc125" REASONCODE="201" REASON="Invalid TimeToLive Value"/>
  <FAILURE REASONCODE="100" REASON="Missing Token"/>
  <RESPONSE RESULT="SUCCESS" TOKEN="abc124"/>
</BULK_RESPONSE>

```

If all of the OBN requests in the incoming message are valid, the bulk request interface sends a Success response for each of them.

For each request item in the post data, validation is performed just as it is for a single request—that is, all of the mandatory parameters are validated. In the bulk request, each request with a Failure URL must be encoded.

If any of the requests contains an error, an error message is sent. (See “Error Codes Returned by OBN Manager” on [page 298](#) for details.) This is done for each request that contains an error. The OBN requests within the bulk request that contain an error must be corrected and resent.

---

**Note:** After the successful requests from a bulk request have been queued, they are treated as individual requests, and OBN Manager failures are communicated by calling the Failure URL, as in the case of a single request.

---

## Error Codes Returned by OBN Manager

[Table 62](#) shows the error code and error text that OBN Manager sends to the trigger application if OBN fails to queue the input request.

**Table 62: Error Codes and Error Text**

Error Code	Description
100	Missing Token
101	Missing Application
102	Missing Customer Name
104	Missing Outbound Number
105	Missing TimeToLive Value
106	Missing Max Attempts Value
200	Invalid Max Attempts Value
201	Invalid TimeToLive Value
202	Invalid Application Name
203	Invalid Customer Name.
204	Invalid Reseller Name
205	Invalid XML Format for Bulk Request

**Table 62: Error Codes and Error Text (Continued)**

Error Code	Description
303	Request Expired while in Memory.
304	Unable to place request in queue. [Application Queue is Filled]
400	Unable to place request in queue. [Database Access Error]
500	Unable to place request, Shutdown in progress.
501	Unable to process the messages, Initialization in progress.

If there are errors after the request is queued, OBN Manager calls the TA's Failure URL. [Table 63](#) show the error conditions that are returned.

**Table 63: Subsequent Errors for a Queued Request**

Error Code	Error Description
300	Unable to place call. [Maximum Attempts have been reached]
302	Unable to place call. [Request Expired]

---

## Provisioning Voice Applications

To use Outbound Notification, you must create and provision an IVR profile in the EMPS. The instructions for doing this are explained in Chapter 1, "Element Management Provisioning System," on [page 25](#).

---

## Integrating with Outbound Contact Server

You can integrate GVP OBN with Genesys Outbound Contact to create the Proactive Notification-Outbound Notification (PN-OBN) solution. This solution enables the Outbound Contact Server (OCS) to trigger OBN calls in GVP, and receive responses and results. To enable this solution, you must configure the IVR profile and the VCS (there are no special configurations for the IPCS).

If the network connection between OBN Manager and OCS goes down, the OBN Manager continues to send responses to the OCS. To avoid this, the OCS application must be configured to communicate with OBN Manager using Automatic Disconnect Detection Protocol (ADDP) in Configuration Manager.

---

Note: For information about Outbound Contact, refer to the *Outbound Contact 7.6 Deployment Guide*.

---

### Configure Voice Communication Server

For PN-OBN support, GVP VCS has been integrated with the Call Progress Detection (CPD) library to provide for superior call progress analysis (CPA) detection through the combination of T-Server and Dialogic technology. To enable CPD, you must configure the server parameters shown in [Table 64](#).

---

Notes: When the VCS is behind a Nortel Symposium switch, and the VCS has been configured to use the CPD library for outbound calls, you must set these two parameters as follows in order for the calls to go through:

- CPD Off-hook Delay: -500
- CPD Calls Cleared by TServer: selected

When the VCS is behind a Nortel Symposium switch, and the CPD library is enabled to make outbound calls, the AutoLogin option in the Symposium should be turned off. If the AutoLogin option is turned on, the switch provides a special dialtone instead of the regular dialtone. The VCS will not recognize this special dialtone and will not start dialing after offhook.

---

**Table 64: Call Progress Detection Parameters**

Node	Tab	Parameter	Description
Route	CPD	Enable Genesys CPD Library	Check box that specifies whether outgoing calls are to be made using the Genesys CPD library.
		Range of Directory Numbers	Specifies the directory number range for the route. Specify directory numbers that are separated by a dash or commas—for example, 101-110, 115, 120-130

**Table 64: Call Progress Detection Parameters (Continued)**

Node	Tab	Parameter	Description
CPD	General	IP Address of primary TServer	Specifies the IP address of the primary T-Server.
		Primary TServer listening port	Specifies the port at which the primary T-Server accepts requests.
		IP Address of backup TServer	Specifies the IP address of the backup T-Server.
		Backup TServer listening port	Specifies the port at which the backup T-Server accepts requests.
		TServer Reconnect Timeout	Specifies the reconnect timeout for T-Server in milliseconds. Default: 10000
		Use TServer to make calls	Specifies whether outgoing calls are to be made by T-Server when using the Genesys CPD library.
		Calls Cleared by TServer	Specifies whether outgoing calls are to be cleared by T-Server when using the Genesys CPD library.
		Off-hook Delay	This parameter is used only if the parameter CPD Calls Made by TServer is selected. Specifies the off-hook delay in milliseconds. A negative value specifies to go off-hook first, wait for the specified time, and then dial a number. A positive value specifies to dial first, wait for the specified time, and then set the channel off-hook. Default value: 0

**Table 64: Call Progress Detection Parameters (Continued)**

Node	Tab	Parameter	Description
		Wait for Offhook Confirmation	This parameter is used only if the parameter <code>CPD Offhook Delay</code> has a negative value.  If this parameter is selected, the CPD library waits for the off-hook confirmation event from T-Server before dialing.
		Preconnect Priority	Specifies whether priority should be given to either T-Server or Dialogic in the event of conflicting CPD results. Values are: • <code>TServer</code> . • <code>Dialogic</code> .
		Postconnect Priority	Specifies whether priority should be given to T-Server or Dialogic in the event of conflicting CPD results. Values are: • <code>TServer</code> . • <code>Dialogic</code> .
		FAX2 Tone as Answering Machine	Check box that specifies whether the CPD library should accept the FAX2 tone as answering machine.

## User Data from OCS

User data passed from OCS is made available to the VoiceXML application via \$variables. User data is passed as key-value pairs from OCS. The GVP Call Flow Assistant (CFA) passes these to the PopGateway in `<DIAL_CALL>` as \$variables. All \$variables passed from CFA are, in turn, made available to the VoiceXML application.

If the key of a key-value pair of the user data is `<token>`, then `$$<token>$` is used by the VoiceXML application to access the value.

## User Data to OCS

The VoiceXML application can post user data back to OCS by using the VoiceXML 2.1 `<data>` tag. The URL is provided by OCS via `$obn-url$`.

## Framework Port

For the PN-OB solution, VCS/IPCS passes to CFA the Framework port number of the channel used for the outbound call. This enables the VoiceXML application to interface with Framework as it does with inbound calls. Refer to the *Genesys Voice Platform 7.6 VoiceXML 2.1 Reference Manual* for details.

## VoiceXML Application

This section provides information for users who write stand-alone VoiceXML applications (not using Genesys Studio) for the PN-OBN solution. It describes the set of OCS keys that form the user data between the OCS and the VoiceXML application.

The following variables are required in the VoiceXML applications.

### OCS Flag Variable

The voice application checks for the OCS flag in the arrived data from the OCS. If this flag is set to 0, the voice application stops the data processing, otherwise, it processes the rest of the data.

#### Example

```
<var name="OCSApplicationFlag" expr="session.genesys.OCSFlag" />
```

This will be used as follows:

```
<if cond="session.genesys.OCSflag == 0">
  <throw event="Throw your error" message="Not configured as an outbound application" />
</if>
```

### CPA Result Variable

The `session.genesys._cpareresult` variable branches out the voice application logic. The voice application checks for the values `CPA_NORMAL` and `CPA_ANSWERMACHINE` for this variable. The other values received by the voice application for this variable are `CPA_BUSY`, `CPA_NOANSWER`, and so on, but the voice application can ignore these values.

#### Example

```
<var name="CPAResult" expr="session.genesys._cpareresult" />

<block>
  <if cond=" OCSApplicationFlag == 1 and
    CPAResult == 'CPA_NORMAL'">
    <var name="user_data" expr="'GSW_CALL_RESULTS=0'" />
    <data method="post" namelist="user_data" srcexpr="session.genesys.obn_url" />
  </if>

  <if cond=" OCSApplicationFlag ==1 and
    OCSCPAResult == 'CPA_ANSWER_MACHINE'">
    <var name="user_data" expr="'GSW_CALL_RESULTS=9'" />
    <data method="post"
      namelist="user_data" srcexpr="session.genesys.obn_url"/>
  </if>
</block>
```

## User Data from OCS

The `session.genesys.User_Data` variable receives the posted OCS User Data.

### Example

```
<var name="OCSUserData" expr="session.genesys.User_Data" />
```

The OCS user data looks like the following:

```
GSW_TZ_OFFSET=-28800&GSW_PHONE=6504664689&BusinessStringData1=Hello
World&BusinessIntegerData1=12345&GSW_CALLING_LIST=obn_call_list&GSW_CAMPAIGN_NAME=obn_campaign&GSW_CONTACT_MEDIA_TYPE=voice&GSW_RECORD_HANDLE=178&GSW_APPLICATION_ID=106&GSW_CALL_ATTEMPT_GUID=C6083088F3BK5F50LPDM6I70EC00002P&GSW_CAMPAIGN_GROUP_DBID=101&GSW_CAMPAIGN_GROUP_NAME=obn_campaign@OBN Agent Group&GSW_CAMPAIGN_GROUP_DESCRIPTION=&GSW_CALLING_LIST_DBID=101&GSW_CHAIN_ID=3&GSW_SWITCH_DBID=0&GSW_ATTEMPTS=33&GSW_CALL_RESULT=1&InteractionType=Outbound&InteractionsType=OutboundNew
```

The voice application usually receives the OCS keys in key-value form in the user data from the OCS. [Table 65](#) lists some of the user data attributes from the OCS.

**Table 65: OCS User Data Attributes**

OCS Key Name	Data Type	Description
GSW_ATTEMPTS	Integer	Number of attempts made for the outbound DN.
GSW_CALLING_LIST	String	Name of the outbound calling list.
GSW_CAMPAIGN_NAME	String	Name of the Outbound campaign.
GSW_RECORD_HANDLE	Integer	Unique identifier of the calling list record.
GSW_TZ_OFFSET	Integer	Time offset between GMT and the dialed DN's time zone.
GSW_PHONE	String	Outbound dialed DN.

## Call Result User Data

The OCS key `GSW_CALL_RESULT` sends the call result back to the OCS. The values are as follows:

```
GSW_CALL_RESULT = 51 > Don't call Record Action
GSW_CALL_RESULT = 52 > Cancel Record Action
GSW_CALL_RESULT = 33 > Answer
```

The `GSW_CALL_RESULT` is part of `user_data`, and it is sent in HTTP Post from the voice application. The following is sample code:



```
<var name="user_data" expr="'GSW_CALL_RESULT=3'" />
  <data name="PutOCSUserData" method="post" namelist="user_data"
    srcexpr="session.genesys.obn_url" />
```

## User Data for Schedule Call Back or Campaign Reschedule

The OCS keys GSW\_PHONE, GSW\_DATE\_TIME, and GSW\_TZ\_TIME are used in conjunction with each other for rescheduling.

- **GSW\_PHONE**—Used for the outbound dialed DN. This key is part of the user data from either the OCS or the voice application. It is a string data type.
- **GSW\_DATE\_TIME**—Used to reschedule the campaign. This key is part of the user data, and it is present in the response from the voice application to the OCS. It is a string data type in (MM/DD/YYYY MM:MM) format.
- **GSW\_TZ\_NAME**—Represents the time zone. This key is part of the user data from the voice application to the OCS. It exists in the user data whenever GSW\_DATE\_TIME exists in the user data from the voice application to the OCS. It is a string data type. The values for this are various time zones such as PST, CST, EST, and so on.
- **GSW\_CAMPAIGN\_NAME** and **GSW\_CALLING\_LIST**—Represents the active campaign name and the calling list name from which the user data has arrived to the voice application from the OCS. The voice application has the capability to reschedule the call at different active campaign calling lists. Therefore, when the voice application needs to reschedule the call at a different phone number than the number that it received from the OCS, it must also send the valid active campaign name and calling list name using these keys. The values for these keys can be the same values that the voice application has received in the user data from the OCS or new valid values.

The voice application handles the Campaign Rescheduling or Scheduled Call Back in four different ways:

- The voice application can use the same GSW\_PHONE value that it received in the user data from the OCS, and build the new user data with GSW\_PHONE, GSW\_DATE\_TIME, and GSW\_TZ\_NAME. As a result, the OCS reschedules the campaign on the same phone number at a different time.

The following is sample code:

```
<var name="user_data" expr="'GSW_DATE_TIME=01/01/2007
10:20&GSW_PHONE=408xxxxxxx&GSW_TZ_NAME=PST'" />
  <data name="PutOCSUserData" method="post" namelist="user_data"
    srcexpr="session.genesys.obn_url" />
```

- The voice application can set the no value for the GSW\_PHONE value. In such a case, OCS uses the same value that it sent out in its user data. The voice application builds the new user data with GSW\_PHONE (no value is set), GSW\_DATE\_TIME, and GSW\_TZ\_NAME. As a result, the OCS reschedules the campaign on the same phone number at a different time.

The following is sample code:

```
<var name="user_data" expr="'GSW_DATE_TIME=01/01/2007
10:20&GSW_PHONE=&GSW_TZ_NAME=PST'" /> <data name="PutOCSUserData" method="post"
namelist="user_data" srcexpr="session.genesys.obn_url" />
```

- The voice application can remove the GSW\_PHONE key from its response to the OCS. The voice application builds the new user data with GSW\_DATE\_TIME, and GSW\_TZ\_NAME. As a result, the OCS reschedules the campaign on the same phone number at a different time.

The following is sample code:

```
<var name="user_data" expr="'GSW_DATE_TIME=01/01/2007 10:20&GSW_TZ_NAME=PST'" />
<data name="PutOCSUserData" method="post" namelist="user_data"
srcexpr="session.genesys.obn_url" />
```

- The voice application can modify the GSW\_PHONE value that it received in the user data from the OCS, and builds the new user data with GSW\_PHONE, GSW\_DATE\_TIME, and GSW\_TZ\_NAME. As a result, the OCS reschedules the campaign at a different phone number at a different time. The OCS adds a new record in its campaign list.

The following is sample code:

```
<var name="user_data" expr="'GSW_DATE_TIME=01/01/2007
10:20&GSW_PHONE=650xxxxxxx&GSW_TZ_NAME=PST&
GSW_CAMPAIGN_NAME=Campaign1&GSW_CALLING_LIST=CallingList1'" />
<data name="PutOCSUserData" method="post" namelist="user_data"
srcexpr="session.genesys.obn_url" />
```

## Customized User Data to OCS from the Voice Application

The voice application can also update the customized user data from the OCS, and send it back to the OCS by using the in HTTP Post method.

The following code shows how to send the user data back to the OCS. The keys `BusinessString1` and `BusinessIntegerData1` are customized keys between the OCS and the voice application; they are not pre-defined keys.

```
<var name="user_data" expr="'BusinessStringData1=Hello
World&BusinessIntegerData1=12345'" />
<data name="PutOCSUserData" method="post" namelist="user_data"
srcexpr="session.genesys.obn_url" />
```



## Chapter

# 14 MRCP Server Hunt List

This chapter describes the MRCP Server Hunt List feature.

This chapter contains the following sections:

- [Overview, page 307](#)
- [Out-of-Service Designation, page 307](#)
- [Heartbeat, page 308](#)
- [Load Balancing, page 308](#)
- [Traps, page 310](#)

---

## Overview

The MRCP Server Hunt List provides the following features for MRCP Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) server management:

- Servers that GVP determines to be out of service will not be used until GVP determines that they are up.
- GVP sends a heartbeat to out-of-service servers, to determine when they are back up.
- Load balancing clearly defines primary and backup group usage.

---

## Out-of-Service Designation

When GVP first connects to an MRCP server, if it does not receive a response from the server, the server is marked `Out of Service`, and GVP throws a trap.

---

## Heartbeat

After an MRCP server is marked `Out of Service`, GVP initiates a heartbeat to the server at a configurable interval, until such time that the server becomes available. The heartbeat is in the form of an RTSP `DESCRIBE` message. If GVP receives a response, the server is marked `In Service`, and it is then available to be used. When a server is marked back to `In Service`, GVP throws a trap.

The `Out of Service Ping Interval` parameter configures the heartbeat interval. To configure the parameter in the `EMPS > Servers`:

### ASR:

On the VCS, go to `PopGateway > ASR > MRCP`.

On the IPCS, go to `Mcu > ASR > MRCP`.

### TTS:

On the VCS, go to `TTS_MRCP`.

On the IPCS, go to `Mcu > TTS > MRCP`.

---

## Load Balancing

GVP uses a round-robin selection of MRCP servers, as well as primary and backup groups. As a general rule, GVP always uses the primary servers, and it uses the backup servers only if a primary server fails to respond.

### First Attempt

GVP uses the following rules, in order of highest precedence, to determine which MRCP server group to use for the first attempt. GVP iterates through the list until a server is chosen.

1. Try an in-service server from the Primary Group, unless all servers in the Primary Group are marked `Out of Service`.
2. Try an in-service server from the Backup Group, unless all servers in the Backup Group are marked `Out of Service`, or unless there is no Backup Group configured.
3. Try a server from the Primary Group, even if it is currently marked `Out of Service`. If it responds, the server is also marked `In Service`.

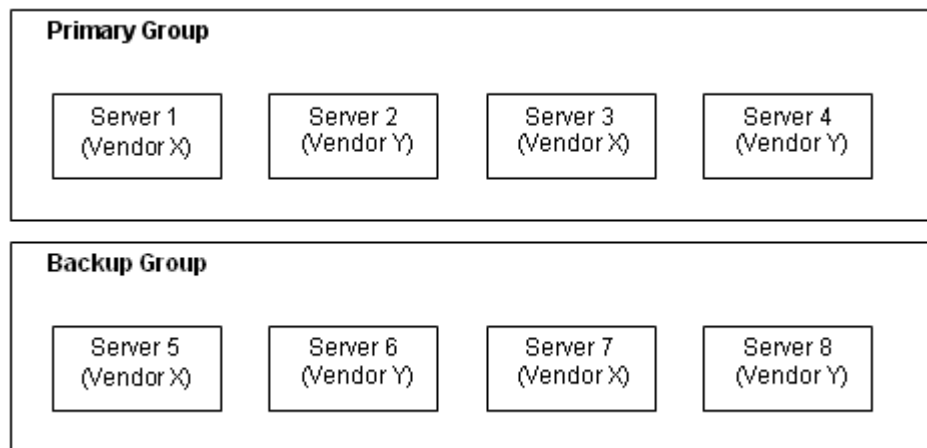
### Second Attempt

If the first attempt does not result in a response from the MRCP Server, GVP attempts a single retry. GVP uses the following rules, in order of highest

precedence, to determine which MRCP server group to use for the second attempt. GVP iterates through the list until a server is chosen.

1. Try an in-service server from the Backup Group, unless all servers in the Backup Group are marked *Out of Service*, or unless there is no Backup Group configured.
2. Try an in-service server from the Primary Group, unless all servers in the Primary Group are marked *Out of Service*.
3. Try a server from the Primary Group, even if it is currently marked *Out of Service*. If it responds, the server is also marked *In Service*.

Individual groups are divided into subgroups, according to the Vendor name with which it was configured. Once the preceding rules have determined the group from which a server will be chosen, a server will be chosen, in a round-robin manner, from the Vendor subgroup.



**Figure 135: Sample Primary and Backup Groupings**

Using [Figure 135](#) as an example, and assuming that all servers are initially in-service, the following is an example of how the server selection works for ASR:

1. Call 1 requires an ASR MRCP server of Vendor X, as provisioned in the voice application. GVP selects Server 1 from the Primary Group.
2. Call 2, which occurs moments later, also requires an ASR MRCP server of Vendor X. Using a round-robin algorithm among Primary Group servers that are of Vendor X, GVP selects Server 3, because Server 1 was selected for Call 1.
3. In Step 1, the server does not respond. GVP attempts a single retry, this time using Server 5, which is a Vendor X server from the Backup Group.
4. Call 3 requires an ASR MRCP server of Vendor Y, as provisioned in the voice application. GVP selects Server 2 from the Primary Group.

5. Call 4 requires an ASR MRCP server of Vendor X, as provisioned in the voice application. Using a round-robin algorithm among Primary Group servers that are of Vendor X, GVP selects Server 1, because Server 3 was selected for Call 2.

Using Figure 135 on [page 309](#) as an example, and assuming that all servers are initially in-service, the following is an example of how the server selection works for TTS:

---

Note: More than one TTS server can be used in a single call, depending on the availability of the server (in service or out of service) and the requests generated, as per the application logic.

---

1. TTS Request 1, Call 1, requires a TTS MRCP server of Vendor X, as provisioned in the voice application. GVP selects Server 1 from the Primary Group.
2. TTS Request 2, Call 1, moments later also requires a TTS MRCP server of Vendor X. Using round-robin algorithm among Primary Group servers that are of Vendor X, GVP selects Server 3, because Server 1 was selected in Step 1.
3. In Step 1, the server does not respond. GVP attempts a single retry, this time using Server 5, a Vendor X server from the Backup Group.
4. TTS Request 1, Call 3, requires a TTS MRCP server of Vendor Y, as provisioned in the voice application. GVP selects Server 2 from the Primary Group.
5. TTS Request 1, Call 4, requires a TTS MRCP server of Vendor X, as provisioned in the voice application. Using round-robin algorithm among Primary Group servers that are of Vendor X, GVP selects Server 1, because Server 3 was selected in Step 2.

---

## Traps

GVP throws a trap when an MRCP server is marked Out of Service, or when an MRCP server is marked back to In Service.

Refer to the *Genesys Voice Platform 7.6 Troubleshooting Guide* for information about GVP traps.



## Chapter

# 15 Media Server Hunt List

This chapter describes the Media Server Hunt List feature.

This chapter contains the following sections:

- [Overview, page 311](#)
- [Out-of-Service Designation, page 311](#)
- [Heartbeat, page 311](#)
- [High Availability, page 312](#)

---

## Overview

The Media Server Hunt List feature enhances the existing Media Server management functionality that exists for Media Servers.

- Servers that are determined to be Out-of-Service (OOS) will not be used until they are seen as back in service.
- A heartbeat is sent to the OOS servers to determine when they are back up.

---

## Out-of-Service Designation

When GVP first connects to a Media Server, if it does not receive a response from the server, the server is marked `Out of Service`, and IPCS generates a trap.

---

## Heartbeat

After a Media Server is marked `Out of Service`, IPCS initiates a heartbeat to the server at a configurable interval, until such time that the server becomes available. The heartbeat is in the form of a SIP Options request. If IPCS

receives a response, the server is marked `In Service`, and it is then available to be used. When a server is marked back to `In Service`, IPCS generates a trap. For more information about the traps generated, see the *Genesys Voice Platform 7.6 Troubleshooting Guide*.

The `Out of Service Ping Interval` parameter configures the heartbeat interval for IPCS to ping the Media Server. To configure this parameter;

1. Go to the EMPS > Servers > IP Communication Server > <IPCS hostname> > Mcu > MediaController > MxML node.
2. Click Add New Attribute.
3. Add `Out of Service Ping Interval` and set it to the desired value.

---

## High Availability

GVP uses a round-robin selection of Media Servers, as well as primary and backup groups. As a general rule, GVP always uses the primary servers, and it uses the backup servers only if a primary server fails to respond.

### First Attempt

GVP uses the following rules, in order of highest precedence, to determine which Media Server group to use for the first attempt. GVP iterates through the list until a server is chosen.

1. Try an in-service server from the Primary Group, unless all servers in the Primary Group are marked `Out of Service`.
2. Try an in-service server from the Backup Group, unless all servers in the Backup Group are marked `Out of Service`, or unless there is no Backup Group configured.
3. Try a server from the Primary Group, even if it is currently marked `Out of Service`. If it responds, the server is also marked `In Service`.

### Second Attempt

If the first attempt does not result in a response from the Media Server, GVP attempts a single retry. GVP uses the following rules, in order of highest precedence, to determine which Media Server group to use for the second attempt. GVP iterates through the list until a server is chosen.

1. Try an in-service server from the Backup Group, unless all servers in the Backup Group are marked `Out of Service`, or unless there is no Backup Group configured.
2. Try an in-service server from the Primary Group, unless all servers in the Primary Group are marked `Out of Service`.



3. Try a server from the Primary Group, even if it is currently marked Out of Service. If it responds, the server is also marked In Service.

Individual groups are divided into subgroups, according to the Vendor name with which it was configured. Once the preceding rules have determined the group from which a server will be chosen, a server will be chosen, in a round-robin manner, from the Vendor subgroup.





## Chapter

# 16 Network Announcement

This chapter describes how to configure the Network Announcement option with Genesys Voice Platform (GVP).

This chapter contains the following sections:

- [Overview, page 315](#)
- [Requirements, page 315](#)
- [SIP Functions, page 316](#)

---

## Overview

This chapter describes the functions of the SIP-based Network Announcement platform and how it will impact other GVP components. In general, the function of the Network Announcement platform is to provide media service. The service can be from a simple announcement to more complex interaction, such as prompting and collecting user information, to determine where to transfer the call.

When GVP is deployed as a Network Announcement platform, it can be used for announcements, DTMF collection, and transfers. Most of the Element Management System (EMS) functionality, except for Element Management Provisioning System (EMPS), will not be required in the deployment.

---

## Requirements

Some solution deployments can have 100,000 or more customers. Each customer can have a separate toll-free number. Both Configuration Manager and GVP provisioning becomes challenging with such a high number of customers. Currently, GVP needs to be provisioned with a DNIS to point to a voice application. Due to an extremely high number of customers, it is preferable that GVP need not be provisioned for every customer. The main

requirement is to have GVP be invoked in a generic way irrespective of DNIS. The external signaling entity provides required information to contact the voice application.

GVP supports the following method of voice application invocation: based on VoiceXML URL in the INVITE request.

---

## SIP Functions

This sections describes the SIP functions in a Network Announcement environment.

### Overview

In a SIP-based Network Announcement server environment, the user part of the request URI is used as the service indicator. Upon receiving the INVITE request, the Network Announcement server examines the service indicator and, depending on the type of service requested, it can decide to accept the request or return a failure response. There are currently three types of service defined by the SIP community:

- `annc`—announcement
- `dialog`—prompting and collecting user information
- `conf`—call conferencing

GVP falls into the *prompt and collect* service category, also known as *dialog service*.

The form of the SIP request URI for dialog service is the following:

```
sip:dialog@mediaserver.example.net;  
voicexml=http://<hostname>/<scriptname>.vxml
```

The dialog service takes a parameter, `voicexml=`, which indicates the URI of the VoiceXML script to execute. The Network Announcement server may accept additional SIP request URI parameters and deliver them to the VoiceXML interpreter session as session variables.

### Formal Syntax for Dialog Service

```
DIALOG-URL = "sip:" dialog-ind "@" hostport dialog-parameters  
dialog-ind = "dialog"  
dialog-parameters = ";" dialog-param [vxml-parameters]  
dialog-param = "voicexml=" dialog-url  
vxml-parameters = vxml-param [vxml-parameters]  
vxml-param = ";" vxml-keyword "=" vxml-value
```

`vxml-keyword = token`

`vxml-value = token`

The `dialog-url` is the URI of the VoiceXML script. If present, other parameters get passed to the VoiceXML interpreter session with the assigned `vxml-keyword vxml-value` pairs.

---

Note: All `vxml-keywords` must have values. The `dialog-ind` is case insensitive.

---

If the Network Announcement server fails to retrieve the VoiceXML script, it must respond with **404 NOT FOUND** response code.

For more details, refer to the *IETF draft Basic Network Media Services With SIP [draft-burger-sipping-netann-06]*.

## Call Manager Requirements

To support the requirements, the IP Call Manager (IPCM) performs in the following manner:

If the incoming INVITE message has the service indicator in the request URI, the IPCM does not fetch the voice application. Instead, it forwards the request to a specific IPCS as per the current behavior. The IPCM simply routes calls based on available IPCS ports. It will not be able to perform resource selection based on any other attributes.

## IPCS Requirements

You must configure the following IPCS parameters for the Network Announcement option:

- Primary Generic URL Mapper
- Backup Generic URL Mapper

## EMPS Requirements

You must perform certain steps in the EMPS when creating and provisioning a voice application for Network Announcement. Refer to “IVR Profiles” on [page 47](#) for instructions.





## Chapter

# 17

## Transactional Recording

This chapter describes how to configure Genesys Voice Platform (GVP) Voice Communication Server (VCS) to support the transactional recording feature. For information about voice applications and transactional recording for GVP IP Communication Server (IPCS), refer to the *Genesys Voice Platform 7.6 VoiceXML 2.1 Reference Manual*.

This chapter contains the following section:

- [Configuring the VCS, page 319](#)

---

## Configuring the VCS

This section describes how to configure the VCS to support the transactional recording feature when using either a JCT board or a DM/V board.

### Using a Dialogic JCT Board

1. In the Element Management Provisioning System (EMPS), expand the Servers object.
2. Expand the nodes Voice Communication Server > <ServerName>, and then right-click PopGateway[x].
3. Select Edit.
4. In the text box for the Transaction Recording Resources parameter, specify the channels for transactional recording in the following format:

X:Y-Z

Where X = board number

Y = starting channel number

Z = ending channel number

For example, your configuration will appear similar to this:

1:20-23

Where  $I$  = board number  
 20 = starting channel number  
 23 = ending channel number

The preceding configuration example implies that at any time, GVP will perform transactional recording on four channels simultaneously.

---

Note: You must not use these channels in any other route configurations.

---

5. Click **Save** to save the configuration.  
 You must now configure the Route on which the transactional recording needs to occur.
6. In the EMPS, expand the **Servers** object.
7. Expand the nodes **Voice Communication Server** > <Server> > **PopGateway[x]**, and then right-click **Route[x]**.
8. Select **Edit**.  
 The Route can be inbound or outbound.
9. Select the **Enable Transaction Record** check box.
10. Make sure that the value for the **For CSP: Media Resource Board to use** parameter is 2, which is JCT specific.

---

Note: Channels that are specified in the Route section should not overlap with the resources allocated for transactional recording.

---

11. Click **Save** to save the configuration.  
 The following is an example configuration for D/60 > 2E1 JCT. This configuration enables you to record ten simultaneous bridged calls.

Transactional Recording Resources—1:21-30  
 Route1: Inbound and Channels—1:1-10  
 Route2: Outbound and Channels—1:11-20

## E1-JCT Boards

The following configurations are for CSP enabled E1-JCT boards only when two or more JCT boards are connected through the CT Bus.

When CSP is enabled on a JCT 2E1 Board, Dialogic considers the two spans as one network slot. Because of this, the first span on the second board is considered as the second network slot. However, this is not the case when transaction recording resources are configured. The first span of the second board is considered as the third network slot.



The following is an example configuration for three D/600 > 2E1 JCT boards when transactional recording is not required.

Route1: Channels—1:1-30

Media Board Resources to Use—2

Route 2: Channels—2:1-30

Media Board Resources to Use—4

Route 3: Channels—3:1-30

Media Board Resources—6

The following is an example configuration for three D/600 > 2E1 JCT boards with the last five channels in every odd span used for transactional recording.

Transactional Recording resource—1:26-30,3:26-30,5:26-30

Route 1: Channels—1:1-25

Media Board Resources to Use—2

Route 2: Channels—2:1-25

Media Board Resources to Use—4

Route 3: Channels—3:1-25

Media Board Resources to Use—6

## Using a Dialogic DMV-A/DMV-B Board

1. In the EMPS, expand the Servers object.
2. Expand the nodes Voice Communication Server > <ServerName>, and then right-click PopGateway[x].
3. Select Edit.
4. In the text box for the Transaction Recording Resources parameter, specify the channels for transactional recording in the following format:

X:Y-Z

Where X = board number

Y = starting channel number

Z = ending channel number

For example, your configuration will appear similar to this:

1:20-23

Where 1 = board number

20 = starting channel number

23 = ending channel number

The preceding configuration example implies that at any time, GVP will perform transactional recording on four channels simultaneously.

---

Note: You must not use these channels in any other route configurations.

---

5. Click **Save** to save the configuration.  
You must now configure the Route on which the transactional recording needs to occur.
6. In the EMPS, expand the **Servers** object.
7. Expand the nodes **Voice Communication Server** > <Server> > **PopGateway[x]**, and then right-click **Route[x]**.
8. Select **Edit**.  
The route can be inbound or outbound.
9. Select the **Enable Transaction Record** check box.

---

Note: Channels that are specified in the Route section should not overlap with the resources allocated for transactional recording.

---

10. Click **Save** to save the configuration.



## Chapter

# 18 Multiple PopGateways and MCUs

This chapter provides an overview of the multiple PopGateways and multiple Media Control Units (MCUs) feature, and how to configure the IP Communication Server (IPCS) to support this feature. It contains the following sections:

- [Overview, page 323](#)
- [Configuring Multiple PopGateway Processes, page 324](#)
- [Configuring Multiple Mcu Processes for IPCS, page 326](#)
- [Symmetric RTP Ports, page 327](#)

---

## Overview

The IPCS supports multiple PopGateways and Media Control Units (MCUs) on a single machine or in a distributed environment. The benefit of this feature is to limit the number of active calls that are affected if a PopGateway or MCU process fails.

You can configure as many PopGateways as the system allows, based on CPU and memory; however, Genesys recommends that the number of ports supported by each PopGateway be between 50–100. For example, if a machine supports 400 total IPCS ports, you can divide that number among the PopGateways so that each PopGateway supports between 50–100 ports.

---

**Note:** The IPCS supports multiple PopGateways, but each PopGateway can still contain only one route.

---

## Configuring Multiple PopGateway Processes

1. In Element Management Provisioning System (EMPS), expand the Servers object.
2. Expand the nodes IP Communication Server > <host-name>.
3. Right-click the PopGateway1 node, and then select Create a Copy.
4. On the property page, scroll to the bottom, and then click Copy.
5. In the To Node field, enter the new PopGateway process name (for example, PopGateway2), make sure that the Copy Subtree check box is selected, and then click Copy.

You have just created a new PopGateway2 node.

6. On the EMPS navigation tree, right-click your new node, and then select Edit to configure this new node.
7. Enter the attributes and values as shown in [Table 66](#) for the new PopGateway process:

**Table 66: IPCS Attributes and Values**

Tab	Attribute	Description	Value
General	Log File	Specifies the log file for the PopGateway process. Each process must point to its own unique log file.	popgateway.log

**Table 66: IPCS Attributes and Values (Continued)**

Tab	Attribute	Description	Value
SIP	Local SIP Port	Specifies the port used for SIP communications. The port number must be an available (unused) port which is local to this PopGateway. The default value is 5060.  <b>Note:</b> When configuring multiple PopGateways, this SIP port must be unique for every PopGateway.	5060
	Starting Number for Port IDs / Channel IDs	Specifies the start of unique channel / port numbering. A minimum value of 1 should be entered, which ensures that the channels have unique numbers across the PopGateway processes.	1
Media	Media Server Process	Specifies the name of the Media Server process to use.  <b>Note:</b> When configuring multiple PopGateways, this Media Server process must be unique for every PopGateway. Some example values are: Mcu, Mcu1, Mcu2, and so on.	MCU

If the Media MCU process is on a different machine than the PopGateway, also set the parameter shown in [Table 67](#).

**Table 67: IPCS Attributes and Values**

	Attribute	Description	Value
Media	Media Server Address	Specifies the Media Server IP address. This value defaults to the IP address of the local machine.	<ip address>

**8. Click Save.**

Repeat this entire procedure to create the required number of PopGateway processes.

## Configuring Multiple Mcu Processes for IPCS

1. In the EMPS, expand the Servers object.
2. Expand the nodes IP Communication Server > <host-name>.
3. Right-click the Mcu node, and then select Create a Copy.
4. On the property page, click Copy.
5. In the To Node field, enter the new Mcu process name (for example, Mcu2), make sure that the Copy Subtree check box is selected, and then click Copy. You have just created a new Mcu2 node.
6. On the EMPS navigation tree, right-click your new node, and then select Edit to configure this new node.
7. Enter the attributes and values as shown in [Table 68](#) for the new Mcu process.

**Table 68: Mcu Attributes and Values**

Tab	Attribute	Description	Value
General	Log File for Mcu Process	Specifies the log file for the Mcu process. Each process must point to its own unique log file.	mcu.log
DTMF	Fallback DTMF Mode	Specifies the type of DTMF used if RFC 2833 cannot be negotiated. The DTMFs that are generated fall back to this type. DTMF detection always recognizes both RFC 2833 and SIP INFO. If Inband is selected, Inband DTMF will also be detected as a fallback.	SIP INFO Msg

8. Click Save.
9. On the EMPS navigation tree, under the Mcu node previously created, expand the ASR node, right-click MRCP, and then select Edit.
10. Select the attributes and values as shown in [Table 69](#) for the new Mcu process.

**Table 69: IPCS Attributes and Values**

Tab	Attribute	Description	Value
General	Primary MRCP ASR Server Group(s)	Specifies the primary ASR Server Group.	Group Name
	Backup MRCP ASR Server Group(s)	Specifies the backup ASR Server Group.	Group Name

**11.** Click **Save**.

Repeat this entire procedure to create the required number of Mcu processes.

---

## Symmetric RTP Ports

Prior to GVP 7.2, the sending and receiving of RTP streams during Voice over IP (VoIP) call handling could be done on either the same port or on different ports. However, due to security issues, some of the components in the VoIP network blocked IP traffic from unknown ports. In order to avoid this issue, the RTP stack code has been modified so that the same RTP port can be used for sending and receiving RTP data. This functionality is known as symmetric RTP ports.







## Chapter

# 19 Proxy Support

This chapter describes the HTTP Proxy feature, and how to configure Genesys Voice Platform (GVP) to support this feature.

This chapter contains the following sections:

- [Overview, page 329](#)
- [Configuring Page Collector, page 330](#)

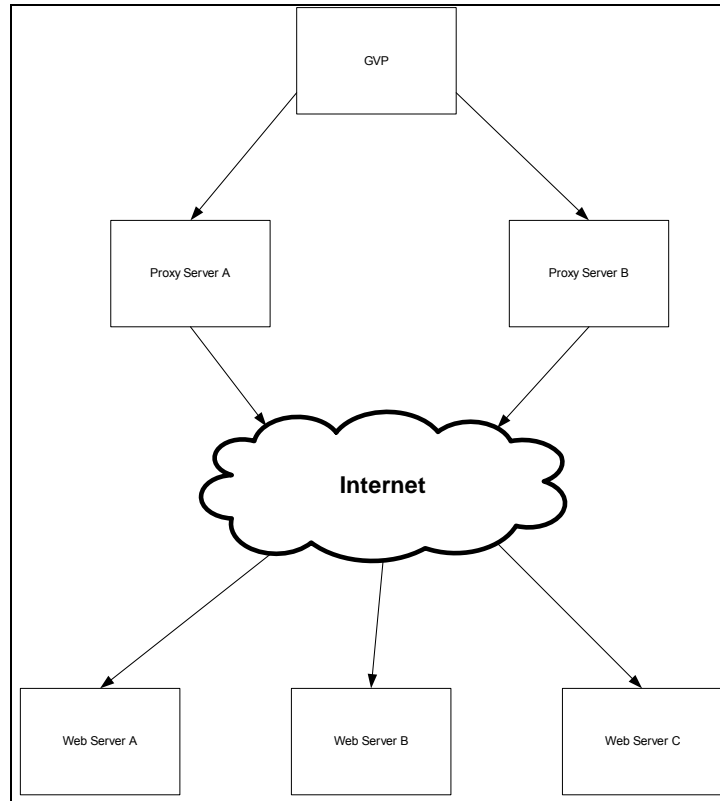
---

## Overview

The Page Collector component of GVP can interoperate with any proxy server—for example, Microsoft proxy, squid proxy, Netscape proxy, and so on. In order to support the proxy server, GVP performs in the following manner:

- sends an HTTP request to the proxy server
- sends an HTTP request, bypassing the proxy server
- handles 305 proxy required response
- handles failover of proxy server(s)

Figure 136 on [page 330](#) illustrates GVP and proxy servers.



**Figure 136: GVP and Proxy Servers**

## Configuring Page Collector

When Page Collector is configured with multiple proxy servers, it performs round-robin load balancing among them for dispatching HTTP requests. If one of the proxy servers fails, its load will be shared among the remaining proxy servers. When the proxy server is brought back up, Page Collector will not immediately distribute load to it; this is because of the keep-alive socket mechanism in Page Collector. However, over time, Page Collector gradually starts dispatching requests to the new proxy server.

To enable the proxy feature, you must configure specific parameters in the Element Management Provisioning System (EMPS).

1. In the EMPS, expand the Servers object.
2. Expand the node Voice Communication Server OR IP Communication Server>, <host-name> > and then right-click PageCollector.
3. Select Edit, and then select the General tab.
4. Configure the parameters shown in Table 70 on [page 331](#), and then click Save.

**Table 70: Page Collector Parameters for Proxy Support**

Tab	Parameter	Description	Example
General	ProxyServerList	Specifies the URL of the proxy server. Multiple proxy URLs are separated by a comma operator. The URL format is: http://<hostname>:<port> Where: hostname—the hostname can be either the IP address or the fully qualified domain name of the proxy server. port—specifies the port to which the proxy server listens. The default port number is 80.	http://<hostname>:<port>
	ProxyBypassList	Specifies one or more hostnames or IP addresses of the web servers that will be contacted directly, bypassing the proxy server. Multiple proxy URLs are separated by a comma operator.	dev.emps.adcc.alcatel.be, 10.10.10.200





## Chapter

# 20 SIP Registration with Avaya SIP Server

This chapter describes how to implement SIP Registration with the Avaya SIP Server.

This chapter contains the following sections:

- [Overview, page 333](#)
- [SIP Registration, page 334](#)
- [Configuring IPCS, page 337](#)
- [Requirements and Functionality, page 339](#)

---

## Overview

Registering the IP Communication Server (IPCS) with the Avaya SIP Enablement Services (SES) enables Genesys Voice Platform (GVP) to take advantage of the communication services layer offered within the Avaya Communications architecture that mediates between Avaya MultiVantage applications and a wide range of standards-based user agents, web-based applications, and communication devices. These services combine the standard functions of a SIP proxy/registrar server with SIP trunking support and duplicated server features to create a highly scalable, highly reliable SIP communications network. Figure 137 on [page 334](#) illustrates how GVP interacts with the Avaya SES.

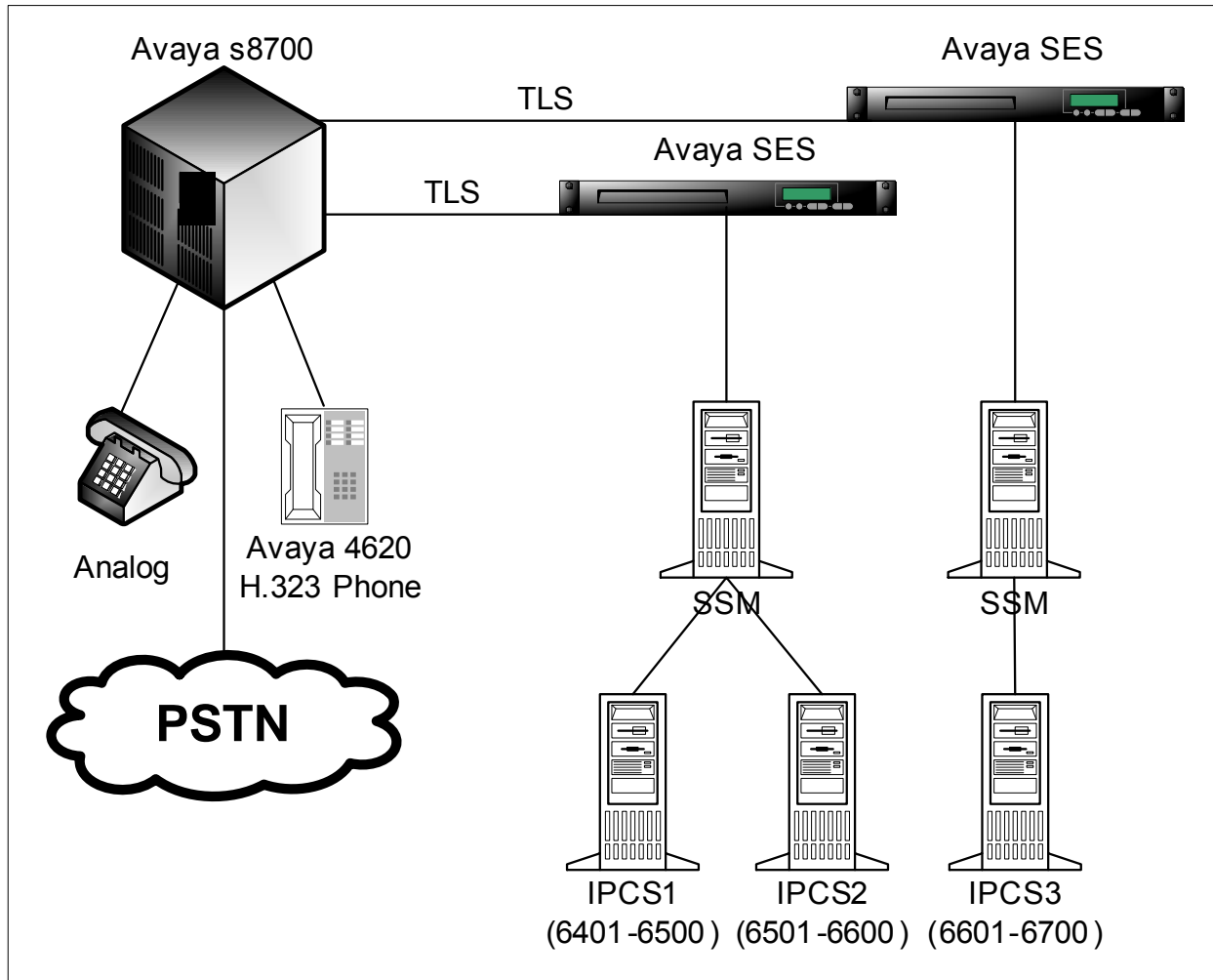


Figure 137: SIP Registration Architecture

## SIP Registration

This section describes the SIP Registration with the Avaya SIP Server.

### Registering with Port Number

When GVP first starts, the IPCS sends registration requests to the Avaya SIP Server for each port it has provisioned. The registration request contains a user name that the Avaya s8700 uses for call assignment. The user name is based on port number, and is calculated using both the starting port number and the number of ports provisioned in GVP. For example, if the starting port number is 200 and there are 10 ports provisioned, the IPCS registers users 200–209. The IPCS port numbers must be unique across the entire system and must match the user name provisioned on the Avaya.

---

**Warning!** It is the customer's responsibility to ensure uniqueness of port numbers across the entire system. The IPCS does not have a prevention mechanism against the same port numbers being used on different servers.

---

A password is not required for registration as long as the IPCS and the SIP Session Manager (SSM) are added to the Avaya's trusted host table. See "Configuring Trusted Hosts on the Avaya Switch" on [page 339](#) for details on how to add the IPCS and the SSM to the Avaya's trusted host table.

SIP Registration is controlled by the SIP Registrar parameter. If this parameter is empty, registration requests will not be sent. The SIP Registrar parameter is set in the Element Management Provisioning System (EMPS) under the PopGateway node. Refer to "Configuring IPCS" on [page 337](#) for details on the SIP Registrar parameter.

If the IPCS receives a 423 Registration Too Brief error message during registration, it will be treated the same as any other error response in this release. The work-around is to manually adjust the registration frequency interval. Refer to the section "[Registration Frequency](#)" for details.

## Registration Frequency

Registration is initially performed during GVP startup and is then repeated periodically. Registration frequency is controlled by the registration frequency interval (SIP Registration Refresh Interval), and is set through the EMPS. When GVP starts, it reads this interval from the .INI file, however; the final interval value is queried from the 200 OK responses it receives from the far end. The local IPCS timer is adjusted based on the far end response. The IPCS sends a registration refresh to the same destination after half of the interval has expired. Refer to "Configuring IPCS" on [page 337](#) for details on the SIP Registration Refresh Interval parameter.

## Handling SIP Messages

SIP requests should not receive any authentication challenges as long as the IPCS and the SSM are added into the SIP server's trusted host table. However, if a SIP server sends a 401 Unauthorized or a 407 Proxy authentication required SIP message during a call, an error event will be returned to the voice application.

Any 401 or 407 SIP messages received during a SIP registration attempt will be handled using the binary exponential backoff method described in the section "Handling Registration Errors" on [page 336](#).

## Handling Registration Errors

If an error is encountered during SIP registration or during a registration refresh, the error will be retried using the binary exponential backoff method. This method enables the IPCS to attempt a registration retry in one minute. If this registration retry attempt fails, then the next retry occurs in two minutes. The retry cycle increases exponentially with subsequent retry attempts made after four minutes, then eight minutes, and finally after 16 minutes. If registration attempts still fail, retries continue every 16 minutes until a successful registration occurs.

## DID Lookup

In order for the IPCS to know which voice application to play, it must get the Direct Inward Dial (DID). The IPCS obtains the Direct Inward Dial (DID) from the History-Info header of the INVITE message. If the History-Info header is not present or the DID is invalid, the T0 header will be used to obtain the DID. This feature is controlled by the SIP Header for DID parameter. The SIP Header for DID parameter is set in the EMPS under the PopGateway node. Refer to “Configuring IPCS” on [page 337](#) for details on the SIP Header for DID parameter.

## Contact Header Settings

This section describes the process IPCS uses for updating the Contact SIP Header:

- If no primary and backup SSM are configured, the IPCS updates the Contact SIP Header information with its own information.
- If a primary and backup SSM are configured, the IPCS includes both SSMs contact information into the Contact SIP Header, and it assigns a higher priority to the primary SSM.
- If there is only a primary SSM configured, its contact information will be included into the Contact SIP Header.
- If there is only a backup SSM configured, the configuration is considered invalid, and the IPCS includes its own contact information into the Contact Header.
- If a primary and backup SSM are configured, and they are the same, the IPCS uses the primary SSMs contact information in the Contact SIP Header.

## Assigning IVR Ports for Inbound Calls

Currently, when an inbound call arrives at the IPCS, the IPCS assigns a random port number from a configured range of port values. This port number is sent to the Genesys Framework as the IVR Port to use for the call.



IPCS now has the ability to override random port assignments. If the SIP Header for IVR Port parameter is set in the EMPS, the IPCS uses a number obtained from the SIP Header as the IVR Port. If the SIP Header for IVR Port parameter is left empty, or the port number cannot be obtained from the SIP Header, the IPCS uses the random assignment method. See “Configuring IPCS” on [page 337](#) for details on how to configure the SIP Header for IVR Port parameter.

---

## Configuring IPCS

To enable this feature, you must configure specific IPCS > PopGateway attributes in EMPS.

1. In the EMPS, expand the Servers object.
2. Expand the nodes IP Communication Server > <host-name>, and then right-click PopGateway.
3. Select Edit.
4. Enter values for the attributes shown in [Table 71](#), and then click Save.

**Table 71: SIP Registration Parameters**

Tab	Parameter	Description	Value
SIP	SIP Registrar	Enables SIP Registration. To enable this feature, specify an IP address and port in the following format:  <ip address>:port For example, 10.10.10.10:5060 If this parameter is left empty, no registration requests will be sent.	<ip address>:port
	SIP Registration Refresh Interval	Specifies, in seconds, the interval used by IPCS for sending registration requests to the SIP server. The minimum value is 3600 seconds.  Range: 3600–31536000 Default: 604800 (1-week)	604800
	SIP Header for DID	Specifies where IPCS looks to retrieve the Direct Inward Dial (DID). Choices are: <ul style="list-style-type: none"><li>History-Info.</li><li>&lt;empty&gt;</li></ul> The default value is <empty>. If this field is left empty, IPCS uses the To Header for DID lookup.	History-Info
	SIP Header for IVR Port	Specifies the SIP header from which the IVR port value is obtained and sent to the Framework. Choices are: <ul style="list-style-type: none"><li>To</li><li>&lt;empty&gt;</li></ul> The default value is <empty>. If this parameter is left empty, or the port number cannot be obtained from the SIP header, the IPCS reports the telephony port as the IVR port.	To

---

## Requirements and Functionality

In addition to configuring parameters in GVP, you must follow some requirements in order for SIP registration with the Avaya s8700 to work properly.

- The user needs to be provisioned on the Avaya Converged Communications Server.
- The Avaya SIP Enablement Services (SES) must be configured to support only User Datagram Protocol (UDP) transport protocol for end-points.
- The IPCS and SSM IP addresses must be included in the trusted host table of the SES. Refer to “Configuring Trusted Hosts on the Avaya Switch” on [page 339](#) for details.

---

Note: GVP does not support authentication. Any 401/407 SIP responses will be treated as error messages.

---

- Every IPCS port must have a corresponding username which matches an extension provisioned on the Avaya s8700.
- Genesys recommends that the Avaya registration refresh interval match the refresh interval set for the IPCS.

## Configuring Trusted Hosts on the Avaya Switch

In order to avoid authentication during either registration or when a call is established, you must add the IPCS and SSM hosts as trusted hosts on the Avaya switch.

To configure a trusted host:

- Telnet to the Avaya SES IP address and login using the administrative login and password.
- At the Linux shell prompt, enter the following trustedhost command:

```
trustedhost -a 20.1.1.54 -n k2.devcon.com -c AGN_Procy
```

Arguments:

- -a—Specifies the address to be trusted.
- -n—Specifies the SES host name.
- -c—adds a comment.
- To verify that the above entry is correct, type:  

```
trustedhost -L
```
- Return to the main Avaya SES Administration web page, and click the Update link to complete the trusted host configuration.





Part

# 3

## GVP Transfers

Part Three of this manual provides details about the transfers that Genesys Voice Platform (GVP) supports. Part Three contains the following chapters:

- Chapter 21, “Transfers,” on [page 343](#)
- Chapter 22, “Explicit Call Transfer,” on [page 353](#)
- Chapter 23, “AT&T Out-of-Band Transfer Connect,” on [page 357](#)
- Chapter 24, “Empty Capability Set-Based Semi-Blind Transfer,” on [page 365](#)
- Chapter 25, “Empty Capability Set-Based Customized Consultation Transfer,” on [page 369](#)





## Chapter

# 21 Transfers

This chapter describes the transfer types that Genesys Voice Platform (GVP) supports.

This chapter contains the following sections:

- [VCS Transfers, page 343](#)
- [IPCS Transfers, page 346](#)

---

## VCS Transfers

Table 72 on [page 344](#) displays the transfer types that Voice Communication Server (VCS) supports. Table 72 on [page 344](#) also displays the Element Management Provisioning System (EMPS) VCS server settings, EMPS Interactive Voice Response (IVR) profile settings, and the VoiceXML application transfer types or the TXML application bridge types that are required to invoke the transfer.

**Table 72: VCS Transfer Types and Settings**

Transfer Type	EMPS > Servers > VCS		EMPS IVR Profile Transfer Setting		VoiceXML Application	TXML Application
	PopGateway > Route > One Channel Transfer Type	PopGateway > Route > Type of Two Channel Transfer	Transfer Type	Transfer Option	<transfer> Type Attribute	<CREATE_LEG_AND_DIAL> Bridge Attribute
ATT Courtesy	<blank>	None	1 channel	ATT Courtesy	blind	no
ATT Consultative	<blank>	None	1 channel	ATT Consultative	blind	no
ATT Conference	<blank>	None	1 channel	ATT Conference	blind	no
ATT Courtesy OOB	<blank>	None	1 channel	ATT Courtesy OOB	blind	no
ATT Consultative OOB	<blank>	None	1 channel	ATT Consultative OOB	blind	no
ATT Conference OOB	<blank>	None	1 channel	ATT Conference OOB	blind	no
TBCT	<blank>	None	2 channel	TBCT	blind/ consultation/ bridge	yes/no
Nortel RLT	<blank>	nortelRLT	2 channel	TBCT	blind/ consultation/ bridge	yes/no
ECT Explicit	<blank>	ECTexplicit	2 channel	TBCT	blind/ consultation/ bridge	yes/no
ECT Explicit NZ	<blank>	ECTexplicit_NZ	2 channel	TBCT	blind/ consultation/ bridge	yes/no



**Table 72: VCS Transfer Types and Settings (Continued)**

Transfer Type	EMPS > Servers > VCS		EMPS IVR Profile Transfer Setting		VoiceXML Application	TXML Application
	PopGateway > Route > One Channel Transfer Type	PopGateway > Route > Type of Two Channel Transfer	Transfer Type	Transfer Option	<transfer> Type Attribute	<CREATE_LEG_AND_DIAL> Bridge Attribute
ECT Explicit UK	<blank>	ECTexplicit_UK	2 channel	TBCT	blind/consultation/bridge	yes/no
Dialogic Blind Transfer	Dialogic Blind Transfer	None	1 channel	Dialogic BlindXfer	blind	no
Bridge	<blank>	None	<blank>	<blank>	bridge	yes
External	<blank>	None	External Transfer	<blank>	blind	no
CTI	<blank>	None	External Transfer	<blank>	blind	no

### TBCT Transfer

In addition to the settings in [Table 72](#), you must also add the following attribute and value to the Voice Communication Server > PopGateway node:

- Attribute: tbct\_allowed
- Value: true

After you add this attribute and value, it displays in the EMPS GUI as TBCT Enabled with the check box selected.

### External Transfer

In addition to the settings in [Table 72](#), External Transfer requires the following EMPS > Servers > Voice Communication Server > CFA configuration:

1. Set Transfer Type to External Transfer.
2. Set the Primary CTA URL and Backup CTA URL.

### CTI Transfer

In addition to the settings in [Table 72](#), CTI Transfer requires the following EMPS > Servers > VCS > CFA configuration:

1. Set Transfer Type to Transfer through CTI.
2. Set the I-Server Client URL.

## IPCS Transfers

[Table 73](#) displays the transfer types that IP Communication Server supports. [Table 73](#) also displays the EMPS IVR profile settings, and the VoiceXML application transfer types or the TXML application bridge types that are required to invoke the transfer.

**Table 73: IPCS Transfer Types**

Transfer Type	EMPS IVR Profile Transfer Setting		VoiceXML Application	TXML Application
	Transfer Type	Transfer Option	<transfer> Type Attribute	<CREATE_LEG_AND_DIAL> Bridge Attribute
SIP Refer	1 channel	SipRefer	blind	no
SIP Refer with Replaces	2 channel	REFERWITH REPLACES	consultation	yes/no
ATT Courtesy	1 channel	ATTCourtesy	blind	no
ATT Consultative	1 channel	ATTConsultative	blind	no
ATT Conference	1 channel	ATTConference	blind	no
Bridge	<blank>	<blank>	bridge	yes/no
External	ExternalTransfer	<blank>	blind	no

Note: SIP Refer with Replaces, although supported through VoiceXML blind transfer, is not an optimal solution because it requires two call legs on the IPCS, whereas SIP Refer only requires one leg.

## External Transfer

In addition to the settings in [Table 73](#), External Transfer requires the following EMPS > Servers > IP Communication Server > CFA configuration:

1. Set Transfer Type to External Transfer.
2. Set the Primary CTA URL and Backup CTA URL.

## SIP REFER

The IPCS supports call transfer using the SIP REFER method as outlined in RFC 3515. A call transfer occurs when an existing call on an IPCS is connected to an agent without having any call context present on the IPCS. In such a transfer, all context of the original caller (both media and signaling) is moved to the external switch/gateway and no longer exists on the IPCS. Also, the IPCS does not create any context of the agent. After a call is transferred, the call exists on a Voice over IP (VoIP) Media Gateway or on a TDM switch, but not on the IPCS.

The following features of RFC 3515 are not supported:

- Encryption
- SIP REFER requests (incoming). The IPCS generates, but does not respond to, SIP REFER requests.
- Multiple Refer-To headers
- Fork requests
- Subscribe/Unsubscribe. When GVP initiates a transfer using REFER, this implicitly performs Subscribe. GVP does not need to explicitly send a Subscribe message.

Voice applications will receive the final transfer result only if the IPCS receives this information from the individual Gateway. If call transfer fails for any reason and the Media Gateway indicates this information in the NOTIFY response, IPCS forwards this information to the voice application. The voice application then determines whether another attempt is to be made.

## SIP REFER with Replaces

The IPCS can initiate a REFER with the Replaces header to perform an attended call transfer. This should be used for voice applications using VoiceXML consultation transfer, because SIP limitations for REFER transfer do not properly handle consultation transfer when the transfer party does not answer.

Note: The IPCS support of REFER with Replaces is dependent on the support of REFER and Replaces by the far end. Also, it is assumed that Contact-URIs received by IPCS are globally routable even outside a dialog, otherwise, Refer with Replaces does not complete properly, because the transferee will not be able to reach the transfer target.

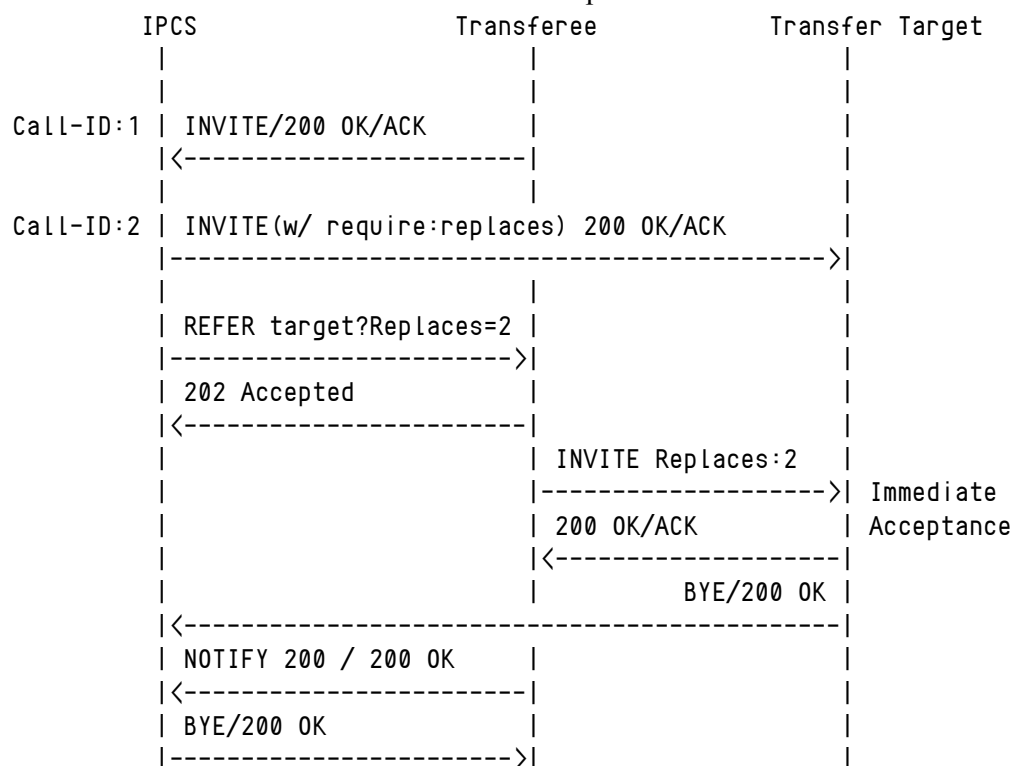
The implementation is based on the IETF draft: *draft-ietf-sipping-cc-transfer-06.txt*.

## Scenarios

### Far End Supports Feature

In this scenario, the IPCS is connected on an existing call to the transferee and initiates a call to the transfer target. The IPCS, while calling the transfer target, inserts the `require:replaces` header to make sure the Replaces header is supported. The IPCS then REFERS the transferee to the transfer target using Replaces.

When the transferee receives a REFER with a Replaces attribute in the refer-to header, it sends out an INVITE to the transfer target and takes the Replaces attribute from REFER and sends it out as a Replaces header in the INVITE. This causes the transfer target to replace IPCS with the transferee. The transfer target sends a BYE to the IPCS, and the IPCS in turn hangs up its call with the transferee. The transferee and transfer target are now talking to each other and the IPCS is out of the loop.



**Example REFER Message with Replaces Header Attribute in Refer-to Header:**

```

REFER sips:CALLER@client.atlanta.example.com SIP/2.0
  Via: SIP/2.0/TLS client.biloxi.example.com:5061
    ;branch=z9hG4bKnashds2g
  Max-Forwards: 70
  From: GVP <sips:GVP@biloxi.example.com>;tag=23431
  To: CALLER <sips:alice@atlanta.example.com>;tag=1234567
  Call-ID: 1@atlanta.example.com
  CSeq: 1025 REFER
  Refer-To: <sips:TRANSFER_TARGET@chicago.example.com?Replaces=
    2%40biloxi.example.com%3Bto-tag%3D5f35a3
    %3Bfrom-tag%3D8675309>
  Referred-By: <sips:GVP@biloxi.example.com>
  Contact: <sips:GVP@client.biloxi.example.com>
  Content-Length: 0

```

**Example INVITE Message as a Result of REFER Message Above:**

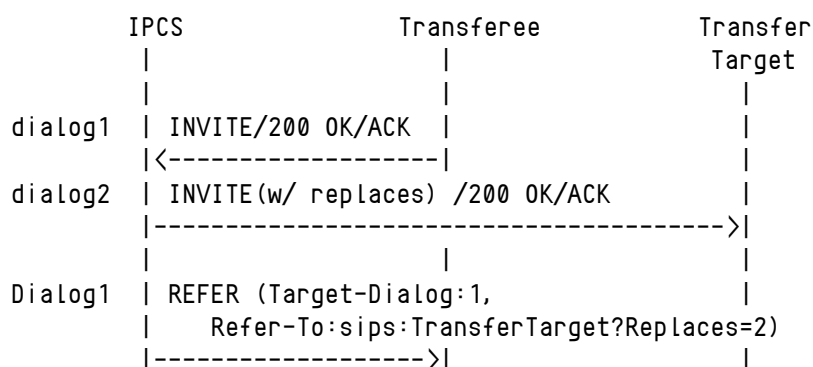
```

INVITE sips: TRANSFER_TARGET@chicago.example.com SIP/2.0
  Via: SIP/2.0/TLS chicago.example.com:5061
    ;branch=z9hG4bKadfe4ko
  To: TRANSFER_TARGET <sips:39itp34klkd@chicago.example.com>
  Max-Forwards: 70
  From: TRANSFEREE <sips:alice@atlanta.example.com>;tag=3461
  Call-ID: 9435674543@atlanta.example.com
  CSeq: 1 INVITE
  Referred-By: <sips:GVP@biloxi.example.com>
  Replaces: 2@biloxi.example.com
    ;to-tag=5f35a3;from-tag=8675309
  Contact: <sips:CALLER@client.atlanta.example.com>
  Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
  Supported: replaces

```

**Recovery When Transferee Does Not Support REFER**

When the IPCS tries REFER with Replaces, and if the transferee does not support REFER, then the IPCS can try sending the REFER to the other leg to see if it supports it.



```

Dialog1 | 501 Not Implemented |
|<-----|
Dialog2 | REFER (Refer-To:sips:Transferee?Replaces=dialog1)
|----->|
Dialog2 | 202 Accepted |
|<-----|
Dialog2 | NOTIFY (100 Trying)|
|<-----|
Dialog2 | | 200 OK |
|----->|
Dialog3 | INVITE (Replaces:dialog1)/200 OK/ACK
|<-----|
Dialog2 | NOTIFY (200 OK) |
|<-----|
Dialog2 | | 200 OK |
|----->|
dialog1 | BYE/200 OK |
|<-----|
Dialog2 | BYE/200 OK |
|----->|
Dialog3 | | BYE/200 OK |
|----->|

```

### When Transfer Target Does Not Support INVITE with Replaces

In this scenario, the target party does not support INVITE with Replaces. A regular INVITE is sent to the target party and REFER with Replaces is sent to the transfer target.

	IPCS	Transferee	Transfer Target
dialog1	INVITE/200 OK/ACK		
dialog2	INVITE(w/ replaces) /420 Bad Extension/ACK		
Dialog3	INVITE(w/o replaces) /200 OK /ACK		
Dialog3	REFER (Refer-To:sips:Transferee?Replaces=dialog1)		
Dialog3	202 Accepted		
Dialog3	NOTIFY (100 Trying)		
Dialog3		200 OK	
Dialog4	INVITE (Replaces:dialog1)/200 OK/ACK		
Dialog3	NOTIFY (200 OK)		

```

Dialog3 | <-----|
        |           | 200 OK |
        |----->|
dialog1 | BYE/200 OK |
        | <-----|
Dialog3 | BYE/200 OK |
        |----->|
Dialog4 |           | BYE/200 OK |
        |----->|

```

## Configuring VoiceXML Application

To configure a voice application to use SIP REFER with Replaces for its transfer, configure the IVR Profile in the EMPS to use the transfer option, SIPReferWithReplaces, which can be used with transfer type of 2SignalChannel. Refer to “Provisioning an IVR Profile” on [page 49](#) for information about provisioning.

## Bridge Transfer

The VoiceXML application invokes the Bridge transfer. For these VoiceXML details, refer to the VoiceXML specification published by the World Wide Web Consortium (W3C).

The IPCS performs a Bridge transfer differently depending on whether it is an IPCS with basic media or an IPCS with enhanced media.

On an IPCS with basic media, the two endpoints stream their audio directly to each other, not through the IPCS. Therefore, the IPCS ignores any active grammars after a call is bridged. This is referred to as remote *bridging*.

On an IPCS with enhanced media, local bridging is supported where the endpoints stream their audio to the IPCS, and the IPCS locally bridges or connects the two audio streams together. In this mode, the IPCS is capable of supporting active grammars and monitoring speech and DTMF specified after a call is bridged.

GVP with MRCP is optimized to free voice recognition licenses during a bridge transfer.







## Chapter

# 22 Explicit Call Transfer

This chapter provides an overview of Explicit Call Transfer (ECT) as supported by the Genesys Voice Platform (GVP) Voice Communication Server (VCS), as well as directory assistance for ECT.

This chapter contains the following sections:

- [Overview, page 353](#)
- [Directory Assistance for ECT, page 353](#)

---

## Overview

Explicit Call Transfer (ECT) enables an ISDN PRI (Primary Rate Interface) user to request the switch to connect together two independent calls on the user's interface. The two calls can be served by the same PRI trunk or by different PRI trunks. If the switch accepts the request, the user is released from the calls and the two calls are connected directly. ECT can be used to free ports on the Voice Communication Server (VCS).

Refer to “VCS Transfers” on [page 343](#) for information about configuring Genesys Voice Platform (GVP) and the voice application to support ECT.

---

## Directory Assistance for ECT

This section describes the Directory Assistance for ECT feature, and how to configure GVP to support it.

---

**Note:** This option is supported on the VCS only, not on the IPCS.

---

## Redirecting Number

The Redirecting Number Information Element (IE) identifies the number from which a call diversion or transfer was invoked. It is contained in the ISDN set-up message of an inbound call from the network. The Redirecting Number IE is optional and controlled by the network.

When an incoming call that is to be transferred lands on GVP, and the Redirecting Number IE is available from the network, GVP captures the Redirecting Number, stores it as part of the call set-up data, and makes it available to the voice applications for further processing.

GVP stores the information in the following VoiceXML extension object:

```
session.connection.inboundcalldata.redirectingnumber
```

The voice application can retrieve the information as follows:

```
<prompt>
  <expr="session.connection.inboundcalldata.redirectingnum"/>
</prompt>
```

---

Note: The information is read-only and cannot be set by the voice application.

---

When the Redirecting Number IE is not available from the network, GVP returns an empty string to the voice application.

## Presentation and Screening Indicators

The Calling Party Number Information Element (IE) identifies the origin of a call, and its attributes control the presentation and screening of the Calling Party Number to the destination/target party. The Calling Party Number IE is contained in the ISDN set-up message of an inbound call from the network.

GVP extracts the presentation and screening indicators from the Calling Party Number IE of an inbound leg, and transfers them to the voice application as call set-up data. The voice application then transmits the indicators to Calling Party Number IE of the ISDN set-up message of the outbound leg during call transfer.

GVP stores the information in the following VoiceXML extension objects:

```
session.connection.inboundcalldata.screeningIndicator
session.connection.inboundcalldata.presentationIndicator
```

The voice application can retrieve the information as follows:

```
<prompt>
  <expr="session.connection.inboundcalldata.screeningIndicator "/>
  <expr="session.connection.inboundcalldata.presentationIndicator "/>
</prompt>
```

---

Note: The information is read-only and cannot be set by the voice application.

---

## Configuring VCS

To enable Directory Assistance for ECT on the VCS, you must add and configure a VCS attribute in the Element Management Provisioning System (EMPS).

1. In the EMPS, select the Servers object.
2. Expand the nodes Voice Communication Server > <host-name>, and then right-click PopGatewayx.
3. Select Edit.
4. Click the Add New Attribute button, and then enter the following attribute and value:
  - Attribute—HandleRedirNumInfoElem
  - Value—1
5. Click Save.





## Chapter

# 23 AT&T Out-of-Band Transfer Connect

This chapter describes the AT&T Out-of-Band Transfer Connect feature, and how to configure Genesys Voice Platform (GVP) to support this feature.

---

Note: The Voice Communication Server (VCS) supports Out-of-Band and Inband transfers. The IP Communication Server (IPCS) supports only the AT&T Inband transfer.

---

This chapter contains the following sections:

- [Overview, page 357](#)
- [Provisioning Voice Applications, page 360](#)
- [Voice Applications, page 360](#)
- [Results Returned to Voice Application, page 361](#)
- [Example Voice Applications, page 362](#)

---

## Overview

GVP usually transfers the calling party to the target party using two Dialogic ports, one for the calling party and the other for the target party. GVP will not process additional calls on those ports until the bridged calls on GVP are torn down. OOB Transfer Connect is an AT&T service that enables GVP to transfer, or redirect a calling party to a target party by releasing the call to the network, which bridges the calling party and target party, thereby not using two GVP ports.

In addition to call redirection, the service supports Data Forwarding from GVP to the transfer party. A prerequisite for Data Forwarding is that GVP and the target party have an Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) connection to the AT&T network. Data Forwarding enables

GVP to send data to the target party using the Message-Associated User-to-User Information (MAUI) signaling procedure described by the AT&T standard. GVP and the target party also must have subscribed to the AT&T toll-free MEGACOM service. More specifically, for the Data Forwarding feature, the VCS must incorporate the data to be transferred to the target party in the User-to-User Information Element (IE) of the ISDN FACILITY message sent from GVP.

GVP requests the redirection of an answered call by signaling on the ISDN PRI D-channel (Out-Of-Band Trigger). Once the trigger has been entered, the calling party is placed on hold by the network. GVP then redirects the call by either direct dialing or speed dialing. The AT&T network then attempts to transfer the call to the target party based on the dialed number or the Speed Dial Code (SDC) entered. For Data Forwarding voice applications, GVP enters the data after the trigger and the redirection number of the target party.

For Out-Of-Band Triggers, GVP must have ISDN PRI, as OOB signaling occurs over the D-channel. For OOB Data Forwarding, both GVP and the target party must have ISDN PRI directly connected to the AT&T switched network. OOB signaling between GVP and the network is performed using the ISDN FACILITY and FACILITY\_REJECT messages. The service permits call redirections in which the telephone number of the target party and the data are forwarded in a single FACILITY message. In some instances, two FACILITY messages are permitted in which the first message transports the target party's telephone number and optionally contains data, and the second FACILITY message transports data only. For all OOB feature types involving data forwarding, the network validates the target party's telephone number and the length of the data to be forwarded. If the validation fails because the target party's telephone number is a plain old telephone service (POTS) number or because the data length exceeds 100 bytes, the network still redirects the call and informs GVP of the failure. In doing so, the network sends the RP FACILITY message to indicate the validation failure followed by FACILITY (Return Result) to confirm the redirection (without data). The Transfer Connect service initiation at GVP is governed by its voice applications. Once GVP determines that a calling party must be redirected, it initiates the transfer request by issuing a FACILITY message.

User-to-User Data Forwarding from GVP to agent is sent in the UU Information Element (UUIE) of the ISDN FACILITY message. This element can not exceed 100 octets and is supported for AT&T specific Codeset 6.

The following are the three offerings of the AT&T toll-free transfer connect service:

- Courtesy Transfer
- Consult and Transfer
- Conference and Transfer

## Courtesy Transfer with Data

For Courtesy Transfer with data, when provisioned for OOB Triggers and OOB Data Forwarding, GVP sends all data in the FACILITY message. Additionally, GVP includes the redirection information and the data in a single FACILITY message. That is, GVP can not issue the redirection information in one FACILITY message followed by a second FACILITY message containing the data, since GVP is disconnected after the first FACILITY message.

## Consult and Transfer with Data

For Consult and Transfer, GVP remains on the redirected call until a successful connection is established between GVP and the target party. In this case, trigger and data must be sent in a single FACILITY message; however, the network does not disconnect GVP until it has received a connect indication from the target party.

## Conference and Transfer with Data

Conference and Transfer does not enable 3-way connections between the calling party, GVP, and the target party; however, Conference and Transfer supports private conversation between GVP and the target party while the calling party is on hold. Once GVP drops out of the above conference, the AT&T switch patches the caller and Agent at the switch end.

Caller leg treatment by GVP is not feasible since the AT&T network puts the caller on hold. In a redirection failure scenario, control will go back to the voice application, and the voice application decides which action should be taken for processing the call. No telephony level re-attempt to some other target party will be provided to handle the preceding scenario.

## User-to-User Data Forwarding Information Tags

The User-to-User Information Element (UUIE) is used as the data transport mechanism for the AT&T Toll-FreeTransfer ConnectSM Data Forwarding feature.

Data to be sent from the GVP (Redirecting Party) to the Agent (Target Party) is first forwarded to the Network through a FACILITY message. When the Network receives a single FACILITY message containing both the redirection number and the data to be forwarded (for example, as in Courtesy Transfer or Consult and Transfer), the data is sent to the Agent (Target Party) in the following SETUP message.

GVP can redirect the incoming call to a toll free number, a Speed Dial number, or a POTS number; however, OOB data will not be forwarded to the POTS number, or to the Speed Dial Code, if it maps to a POTS number.

## Provisioning Voice Applications

1. Log in to the EMPS.
2. Select your IVR profile, and then right-click it. From the shortcut menu, select **Provision**.
3. Select the **Transfer** property page.
4. Select the **Enable Transfer** check box.
5. From the **Transfer Option** drop-down list, select **ATTCourtesy00B**, **ATTConsultative00B**, or **ATTConference00B**.
6. Enter a **Reclaim Code** in the **Reclaim Code (ATT only)** box.
7. Click **Next**, and then provision the rest of the voice application.

## Voice Applications

The voice application can trigger the OOB Transfer Connect using VoiceXML or TXML, as shown in [Table 74](#).

**Table 74: Voice Applications**

Feature	Calls Bridged at the Switch
VoiceXML transfer with bridge = true	Not applicable for OOB Transfer Connect configuration.
Create Leg and Dial with bridge = yes	Yes
Create Leg and Dial with bridge = no	Yes
VoiceXML transfer with bridge = false	Yes
VoiceXML transfer with type = blind	Yes



## Results Returned to Voice Application

Table 75 lists results returned to the voice application in various scenarios.

**Table 75: Results Returned to the Voice Application**

Test Result	VoiceXML/TXML Tag Used	Result Sent to the Voice Application
BUSY	VoiceXML transfer tag bridge=false	<code>connection.disconnect.transfer</code> will be thrown to the voice application.
	TXML CREATE_LEG_AND_DIAL with BRIDGE=NO/YES consultative transfer	Results are not returned to the voice application. (For errors, DIAL_ERROR is thrown.)
	TXML CREATE_LEG_AND_DIAL with BRIDGE=NO/YES conference and transfer	Results are not returned to the voice application. (For errors, DIAL_ERROR is thrown.)
	VoiceXML transfer tag type=blind	<code>connection.disconnect.transfer</code> will be thrown to the voice application.
NOANSWER	VoiceXML transfer tag bridge=false	<code>connection.disconnect.transfer</code> will be thrown to the voice application.
	TXML CREATE_LEG_AND_DIAL with BRIDGE=NO/YES consultative transfer	Results are not returned to the voice application. (For errors, DIAL_ERROR is thrown.)
	TXML CREATE_LEG_AND_DIAL with BRIDGE=NO/YES conference and transfer	Results are not returned to the voice application. (For errors, DIAL_ERROR is thrown.)
	VoiceXML transfer tag type=blind	<code>connection.disconnect.transfer</code> will be thrown to the voice application.

**Table 75: Results Returned to the Voice Application (Continued)**

Test Result	VoiceXML/TXML Tag Used	Result Sent to the Voice Application
ANSWERED	TXML CREATE_LEG_AND_DIAL with BRIDGE=NO/YES consultative transfer	No control to the voice application.
	TXML CREATE_LEG_AND_DIAL with BRIDGE=NO/YES conference and transfer	Results are not returned to the voice application. (For errors, DIAL_ERROR is thrown.)
	VXML transfer tag type=blind	connection.disconnect.transfer will be thrown to the voice application.
OOB XferConnect Failure	VXML transfer tag bridge=false	No control to the voice application.
	TXML CREATE_LEG_AND_DIAL with BRIDGE=NO/YES consultative transfer	Results are not returned back to the voice application. (For errors, DIAL_ERROR is thrown.)
	TXML CREATE_LEG_AND_DIAL with BRIDGE=NO/YES conference and transfer	Results are not returned to the voice application. (For errors, DIAL_ERROR is thrown.)
	VXML transfer tag type=blind	No control to the voice application.

## Example Voice Applications

### Bridge = False with UUI

```
<?xml version="1.0" encoding="UTF-8"?>
  <vxml version="2.0" xmlns="http://www.w3.org/2001/vxml"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.w3.org/2001/vxml
      http://www.w3.org/TR/voicexml20/vxml.xsd">
    <property name="com.telera.speechenabled" value="false"/>
```

```

<form id="xfer">
  <block>
    <!-- queued and played before starting the transfer -->
    <prompt>
      Transferring the call to an agent. Please wait.
    </prompt>
  </block>
<!-- Play music while attempting to connect to far-end -->
  <transfer name="mycall" dest="18001112222"
    transferaudio="Spring-Vivaldi.wav" bridge="false" aai="this is test uui">
  </transfer>
</form>
</vxml>

```

## BRIDGE = Yes Create Leg and Dial

The voice application root page can have the error catch handlers for all call control related errors events. Refer to the *Genesys Voice Platform 7.6 VoiceXML 2.1 Reference Manual*.

```

<?xml version="1.0" encoding="utf-8" ?>
  <XMLPage TYPE="IVR" PAGEID="" SESSIONID="" HREF="" >
    <CREATE_LEG_AND_DIAL TELNUM="18001112222" ANI="" BRIDGE="YES" IVRURL="LEG_WAIT"
      ENDESESSIONONHUP='YES' />
    <LEG_WAIT/>
  </XMLPage>

```

## BRIDGE = No Create Leg and Dial

The voice application root page can have the error catch handlers for the dial\_error event.

```

<?xml version="1.0" encoding="utf-8" ?>
  <XMLPage TYPE="IVR" PAGEID="" SESSIONID="" HREF="" >
    <CREATE_LEG_AND_DIAL TELNUM="18001112222" ANI="" BRIDGE="NO" IVRURL="LEG_WAIT"
      ENDESESSIONONHUP='YES' />
    <LEG_WAIT/>
  </XMLPage>

```





## Chapter

# 24 Empty Capability Set-Based Semi-Blind Transfer

This chapter describes the Empty Capability Set (ECS)-based semi-blind transfer feature, and how to configure Genesys Voice Platform (GVP) to support this feature.

This chapter contains the following sections:

- [Overview, page 365](#)
- [Configuring H.323 Session Manager, page 366](#)
- [Requirements and Functionality, page 366](#)

---

## Overview

The H.323 Session Manager (HSM) supports Empty Capability Set (ECS)-based semi-blind transfer, and the HSM also exchanges the actual capabilities of the Media Gateways involved in the session. This feature enables the Media Gateways to communicate in different audio media codec's after the call is transferred, and it eliminates the dependency of the outbound Media Gateways to have the same media codec as GVP. While performing ECS-based semi-blind transfer, GVP stays in the call signaling path and has control over the call; however, GVP is not in the media path after transferring the call. Additionally, HSM does not reserve IP Communication Server (IPCS) ports for the outbound call leg.

To support ECS-based semi-blind transfer, GVP performs in the following manner:

- The IPCS sends a REFER to initiate a blind call transfer.
- Upon receiving the blind call transfer, the HSM initiates a new outbound call (agent leg) to the Gatekeeper and outbound Media Gateway, or to the Cisco Call Manager, and then bridges the call with the caller to the agent using Empty Capability Set.

- The HSM stays in the call signaling path until the call is ended by either the caller or the agent.

## Configuring H.323 Session Manager

To enable this feature, you must add and configure specific HSM attributes in the Element Management Provisioning System (EMPS).

1. Log in to the EMPS.
2. Through the Servers object, expand the nodes H323 Session Manager > <host-name>, and then right-click H323SessionManager.
3. From the shortcut menu, select Edit.
4. Click the Add New Attribute button. Enter the following attribute and value as shown in [Table 76](#), and then click Save.

**Table 76: HSM Attributes for Blind Call Transfer**

Attribute Name	Value	Description
ProxyBridging	1	Enables ECS-based semi-blind transfer. Values are: 0—disables 1—enables

## Requirements and Functionality

In addition to adding and configuring the preceding HSM attributes, you must follow the below requirements in order for the ECS-based semi-blind transfer to work properly.

- The voice application must use VoiceXML <transfer> (bridge=false). This causes the IPCS to generate the SIP REFER message.
- The inbound Media Gateway must support the codec with which GVP is configured.
- Terminal capabilities of the inbound/outbound Media Gateways must not change for a call that is already in progress, an active call, or a call in a transfer stage.
- The voice application or billing records will not have the result of the transfer. Call events that are reported by the IPCS to the Reporter are the same as a blind call transfer.
- After the successful transfer of the caller and the agent, redirecting the caller to the GVP leg is not supported because this solution is based on the Blind Call Transfer mode.

- After the successful transfer of the call, the HSM only handles a disconnect call control event from the Media Gateway and the Gatekeeper.
- H.245 Tunneling is not supported when proxy bridging is enabled.
- The outbound call initiated by GVP is always in Slow Start when proxy bridging is enabled. Fast Start is not supported for an outbound call initiated by GVP when proxy bridging is enabled.
- RAS is not supported when proxy bridging is enabled.

## Cisco Call Manager Requirements and Functionality

The following requirements are specific to the Cisco Call Manager:

- The following codec's (as supported by the Cisco Media Gateway), are supported as part of codec negotiation:
  - G711Alaw64k
  - G711Ulaw64K
  - G729
  - G729wAnnexB
  - gsmfullrate
  - G7231

You must disable any other codec's at the Media Gateways/Terminals that are not included in the preceding list.

- You configure the Cisco Call Manager IP address and port information in the EMPS parameter `Primary Gatekeeper IP Address` and `Backup Gatekeeper IP Address`.







## Chapter

# 25 Empty Capability Set-Based Customized Consultation Transfer

This chapter describes the Empty Capability Set (ECS)-based customized consultation transfer feature, and how to configure Genesys Voice Platform (GVP) to support this feature.

This chapter contains the following sections:

- [Overview, page 369](#)
- [Configuring H.323 Session Manager, page 370](#)
- [Requirements and Functionality, page 371](#)

---

## Overview

H.323 Session Manager (HSM) can now perform an ECS-based customized consultation transfer.

In an ECS-based customized consultation transfer, when an outbound call is connected, and the IPCS initiates a consultation transfer request (SIP Refer with Replaces), HSM maintains two bridged H.323 sessions, and switches to proxy mode. In proxy mode, HSM processes H.225 Release Complete and H.245 End Session messages only. All other messages are passed transparently from one session directly to the other.

This feature enables the Gateways, Gatekeepers and H.323 endpoints to communicate using different audio codecs, which eliminates the need for outbound gateways to use the same media codec as GVP.

# Configuring H.323 Session Manager

To enable this feature, you must add and configure specific HSM attributes in the Element Management Provisioning System (EMPS).

## HSM Configuration

1. Log in to the EMPS.
2. Through the Servers object, expand the nodes H323 Session Manager > <host-name>, and then right-click H323SessionManager.
3. From the shortcut menu, select Edit.
4. Click the Add New Attribute button. Enter the following attribute and value as shown in [Table 77](#), and then click Save.

**Table 77: HSM Attributes for Custom Consultation Transfer**

Attribute Name	Value	Description
ProxyBridging	1	Enables ECS-based custom consultation transfer. Values are: 0—disables 1—enables

5. Restart WatchDog on the IPCM host.

## Application Provisioning in EMPS

1. On the EMPS navigation tree, expand the Reseller object, the reseller, and then the customer.
2. Select the IVR profile that you want to modify, and then do one of the following:
  - Right-click it. From the shortcut menu, select Provision.
  - Single-click it. From the main frame, click Edit IVR Profile.
  - Double-click it.
3. On the Transfer tab,
  - Set Transfer Type to 2SignalChannel.
  - Set Transfer Option to SIP Refer with Replaces.
4. Click Save.

## VoiceXML Application Changes

To enable this feature in the VoiceXML application:

- Set `<transfertype="consultation">`.

---

## Requirements and Functionality

In addition to adding and configuring the preceding HSM attributes, you must follow the below requirements in order for the ECS-based customized consultation transfer to work properly.

- Both inbound and outbound Media Gateway and Endpoints must be configured for H.245 tunneling in order to work with H.245 tunneling mode.
- Both the inbound and outbound Media Gateways must support at least one media codec supported by HSM.
- The call events sent from IPCS to Reporter are the same as those for a consultation call transfer.
- After the successful transfer of the caller and the agent, redirecting the caller to the GVP leg is not supported.

## HSM Supported Codecs

HSM now supports the following codecs:

- G711Alaw64k
- G711Ulaw64K
- G729
- G729wAnnexA
- G729wAnnexB
- G729AnnexAwAnnexB
- G7231

In addition to this list, HSM also supports the `gsmFullRate` codec as part of codec negotiation between the caller and the agent when HSM bridges the call. This codec is not supported for inbound calls (between the caller and GVP), or for outbound calls (between GVP and the agent).

---

Note: Previously, HSM supported the G711Alaw64k and G711Ulaw64k codecs only.

---

## Caller Preferred Codecs

For inbound calls using fast start, HSM always uses the caller preferred codecs.

For inbound calls using slow start, by default, HSM uses the IPCS preferred codecs. To use the caller preferred codecs, add the following new parameter:

1. Log in to the EMPS.
2. Through the Servers object, expand the nodes H323 Session Manager > <host-name>, and then right-click H323SessionManager.
3. From the shortcut menu, select Edit.
4. Click the Add New Attribute button. Enter the following attribute and value as shown in [Table 78](#), and then click Save.

**Table 78: HSM Attributes for Caller Preferred Codecs**

Attribute Name	Value	Description
UseCallerPreferredCodec	1	Enables caller preferred codecs. Values are: 0—disables 1—enables

5. Restart WatchDog on the IPCM host.



Part

# 4

## Appendixes

Part Four of this manual contains the following appendixes:

- Appendix A, “Call Data Records,” on [page 375](#)
- Appendix B, “Default Settings,” on [page 409](#)
- Appendix C, “Call Control Adapter,” on [page 411](#)
- Appendix D, “Integration with Genesys Framework,” on [page 417](#)
- Appendix E, “Reporting GVP in Framework,” on [page 431](#)
- Appendix F, “System Prompts,” on [page 435](#)
- Appendix G, “Scaling EventC,” on [page 439](#)
- Appendix H, “IP Call Manager High Availability,” on [page 447](#)





## Appendix

# A

## Call Data Records

This appendix documents the call data records generated by the EventC and processing components. The customer can use these data records for billing purposes. This appendix also provides recommendations about data cleanup and resetting peaks in EventC.

This appendix has these sections:

- [Events File, page 375](#)
- [Collector Database, page 377](#)
- [Peaks Database, page 383](#)
- [Reporter Database, page 390](#)
- [RepDWH Database, page 400](#)
- [EventC and Reporter Data Cleanup, page 405](#)
- [Resetting Peaks for EventC, page 406](#)

---

## Events File

The events file is a flat ASCII file that has records separated by NEWLINE and fields in the format of name-value pairs.

It looks like this:

```
TYPE=CALL&POPCRID=8000003800000001&EVENT=08&ANI=&DNIS=4086261386&GUID={FE1F2B56-5EFA-11D4-86B8-00508BA5437D}&DATE=20000721&TIME=114100&APPNAME=ASR_Test&CUSTNAME=QA_ASR_Regression
```

Table 79 lists the details of the events file.

**Table 79: Events File**

Column	Type/Size	Description
type	String	Whether the record is a CALL record or BWM record.
popcrid	Number	The LegID for the Event.
event	Number	Event identifier (Call Start, Call End, and so on).
time	Time	Time of event in HHMMSS.
date	Date	Date of event in YYYYMMDD.
ani	String	Calling Number.
dnis	String	Called Number—DID and not the TFN.
guid	Guid	Unique identifier for the call.
resellername	String	Name of the reseller.
resellerid	String	ID for the Reseller as in EMPS.
custname	String	Name of the customer.
custid	String	ID for the customer as in EMPS.
appname	String	Name of the application.
appid	String	ID for the application as in EMPS.
termsrc	String	Termination Source if it's a termination event.
termreason	Number	Reason for Hang-up, if it's a termination event.
reroute	String	Name of the VCS/IPCS complex to which rerouting occurs, if the call is rerouted.
burstlevel	String	Level of bursting: level1, level2, and so on.
did	String	Direct Inward dialing.
genericcallid	String	SIP call leg ID. This is available for GVP 7.0.3 only.
ConnID	String	Universal Connection ID.



# Collector Database

The EventC Collector Database holds work-in-progress events data during events processing. Raw data from the VCS/IPCS is loaded into this database and processed. An archive of processed call events and exception call events is available in this database. Data related to load balancing and data clean up are also stored in the collector database.

The Collector Database produces the following CDR data tables:

- raw\_events
- call\_events
- call\_exceptions
- eventc\_manager
- eventc\_stats
- load\_balancer
- state\_transitions

## raw\_events

[Table 80](#) holds the raw events records to be processed by the EventsLoader. The processed records are deleted from the table.

**Table 80: raw\_events**

Column	Type/Size	Description
session_id	Char(38)	Unique identifier for the call.
event_type	Char(2)	Type of event: 01/ 02 and so on.
crid	Char(17)	ID of the event's leg.
utc_dt	Date	Date and Time (GMT) when the event occurred; accurate to the second.
ani	Char(32)	The calling number. Called number if it's a notify@net event.
did	Char(32)	The called number (not TFN). Calling number if it's a notify@net event.
teleserver_id	Char(32)	IP of the VCS/IPCS server that handled the event.
junk_id	Number(19)	Internal serial number.
rr_status	Number(10)	Indicates if reroute has happened.

**Table 80: raw\_events (Continued)**

Column	Type/Size	Description
app_id	Number(6)	Application ID.
cust_id	Number(6)	Customer ID.
reseller_id	Number(6)	Reseller ID.
reroute_ts	Char(32)	Rerouted Teleserver.
burst_level	Char(10)	Burst level used by the call.
term_src	Char(10)	Source of call termination.
term_reason	Char(10)	Reason for call termination.
generic_call_id	Char(256)	SIP call leg ID.
CallUUID	Char(38)	Universal Connection ID.

## call\_events

[Table 81](#) acts as an archive for the event records.

**Table 81: call\_events**

Column	Type/Size	Description
session_id	Char(38)	Unique identifier for the call.
event_type	Char(2)	Type of event: 01/ 02 and so on.
crid	Char(17)	ID of the event's leg.
utc_dt	Date	Date and Time (GMT) when the event occurred, accurate to the second.
ani	Char(32)	The calling number. Called number if it's a notify@net event.
did	Char(32)	The called number (not TFN). Calling number if it's a notify@net event.
teleserver_id	Char(32)	IP of the VCS/IPCS that handled the event.
junk_id	Number(19)	Internal serial number.
rr_status	Number(10)	Indicates if reroute occurred.
app_id	Number(6)	Application ID.

**Table 81: call\_events (Continued)**

Column	Type/Size	Description
cust_id	Number(6)	Customer ID.
reseller_id	Number(6)	Reseller ID.
reroute_ts	Char(32)	Rerouted Teleserver.
burst_level	Char(10)	Burst level used by the call.
term_src	Char(10)	Source of call termination.
term_reason	Char(10)	Reason for call termination.
generic_call_id	Char(256)	SIP call leg ID.
CallUUID	Char(38)	Universal Connection ID.

## call\_exceptions

Table 82 holds the exceptions thrown by the Call Records Generator process.

**Table 82: call\_exceptions**

Column	Type/Size	Description
session_id	Char(38)	Unique identifier for the call.
crid	Char(17)	ID of the event's leg.
utc_dt	Date	Date and Time (GMT) when the event occurred; accurate to the second.
ani	Char(32)	The calling number. Called number if it's a notify@net event.
did	Char(32)	The called number (not TFN). Calling number if it's a notify@net event.
IVR_time	Number (10)	Total time spent in the IVR phase.
hold_time	Number (10)	Total time spent in the hold phase.
call_time	Number(10)	Total duration of the call (call start to call end; does not necessarily equal IVR+hold+talk time).
outcallnum	Char(32)	First outbound dialed number of the call.
end_state	Char(10)	Last state of the call.

**Table 82: call\_exceptions (Continued)**

Column	Type/Size	Description
app_id	Number(6)	Application ID.
teleserver_id	Char(32)	IP address of the VCS/IPCS that handled the event.
rr_dest	Char(50)	The destination VCS/IPCS in the reroute.
apptype_id	Number(12)	Application type ID as in EMPS.
startdate_of_service	Date	Date on which this application has been used.
max_app_ports	Number(10)	Maximum application ports (not used).
ports_level1	Number(10)	Maximum ports for burst level 1.
ports_level2	Number(10)	Maximum ports for burst level 2.
ports_level3	Number(10)	Maximum ports for burst level 3.
reseller_id	Number(6)	Reseller ID.
event_seq	Char(100)	The sequence of events that occurred for the call. For example: -01-03-05-02-06.
custpeak	Number(10)	The call peak value for the customer at the start of this call, including this call (it should be at least 1).
talk_time	Number(10)	The total duration spent in all agent legs within a call. An agent leg is when a caller is speaking with a live agent.
tfn	Char(32)	Toll Free Number.
billable_ports	Number(10)	The number of ports for which the customer will be billed.
cust_date	Date	GMT Date adjusted to customer time zone.
resell_date	Date	GMT Date adjusted to reseller time zone.
telera_date	Date	GMT Date adjusted to Genesys time zone.
asr_id	Char(25)	ID for ASR product used.
tts_id	Char(25)	ID for TTS product used.

**Table 82: call\_exceptions (Continued)**

Column	Type/Size	Description
qa_id	Char(25)	ID used for the Queue Adapter/IVR Server Client.
ts_ani	Char(25)	ANI of the teleserver.
excp_reason_code	Char(32)	Code for the exception reason.
cust_id	Number(10)	Customer ID.
generic_call_id	Char(256)	SIP call leg ID.
CallUUID	Char(38)	Universal Connection ID.

## eventc\_manager

[Table 83](#) lists internal processing information.

**Table 83: eventc\_manager**

Column	Type/Size	Description
act_type	Char(32)	Activity type.
act_time	Date	Activity time.
act_errors	Number(1)	Errors encountered in the activity.

## eventc\_stats

[Table 84](#) lists internal processing information and stores the statistics of EventC processes and displays them in the EventC Statistics GUI.

**Table 84: eventc\_stats**

Column	Type/Size	Description
process_name	Char(32)	Name of the EventC process in which to have the statistics.
process_units	Char(25)	Processing units.
last_cycle_at	Date	Time at which last cycle was run.
last_proc_at	Date	Time when last process was run.

**Table 84: eventc\_stats (Continued)**

Column	Type/Size	Description
last_proc_recs	Number(10)	Number of records processed in the last cycle.
last_proc_success	Number(10)	Number of records processed successfully in the last cycle.
last_proc_exception	Number(10)	Number of records that had exceptions in the last cycle.
last_proc_skipped	Number(10)	Number of records skipped in the last cycle.
last_error_at	Date	Time when the last error occurred.
last_error_count	Number(10)	Error count during the last cycle.
last_error_desc	Char(1000)	Last error description.
cycle_start_at	Date	Cycle start time.

## load\_balancer

[Table 85](#) lists internal processing information.

**Table 85: load\_balancer**

Column	Type/Size	Description
instance_name	Char (32)	Instance name of the EventC subcomponent.
module_name	Char (32)	Name of the EventC subcomponent to which the instance belongs.
instance_seq	Number	Sequence of the instance.
start_range	Char (32)	Starting IP address for the instance.
end_range	Char (32)	Ending IP address for the instance.
proceed	Number	Can proceed - 1 / 0.

## state\_transitions

[Table 86](#) lists internal processing information.

**Table 86: state\_transitions**

Column	Type/Size	Description
next_event	Char (2)	Event type.
call_status	Char (32)	State of the call.
leg_status	Char (32)	State of the leg.
phase_status	Char (32)	State of the phase.
actions	Char (32)	List of actions for this event.

---

## Peaks Database

The EventC Peaks database holds work-in-progress, control, and peak counter data from peak calculation.

This database produces the following CDR data tables:

- etrackforpeak
- current peak
- eventc\_stats
- peak\_control

## etrackforpeak

[Table 87](#) lists internal processing information and stores the start and end of call events. The etrackforpeak table also calculates peaks.

**Table 87: etrackforpeak**

Column	Type/Size	Description
session_id	Char(38)	Unique identifier for the call.
utc_dt	Date	GMT date and time when the event occurred; accurate to the second.
ani	Char(32)	The calling number. Called number if it's a notify@net event.
did	Char(32)	The called number (not TFN). Calling number if it's a notify@net event.

**Table 87: etrackforpeak (Continued)**

Column	Type/Size	Description
app_id	Number(6)	Application ID.
teleserver_id	Char(32)	IP of the VCS/IPCS that handled the event.
cust_id	Number(6)	Customer ID.
apptype_id	Number(2)	Application type ID in EMPS.
reseller_id	Number(6)	Reseller ID.
event_type	Char(2)	Type of event: 01/02 and so on.
peak_status	Number(2)	Internal processing flag.
cust_offset	Date	Date adjusted to customer offset.
resell_offset	Date	Date adjusted to reseller offset.
telera_offset	Date	Date adjusted to Genesys offset.
asr_id	Char(32)	ASR product ID.
tts_id	Char(32)	TTS product ID.
qa_id	Char(32)	Queue Adapter/IVR Server Client ID.
telera_id	Number(2)	NSP ID=1.

## current peak

The following tables keep track of the current peak (as of the peak calculation timeline) for various criteria and they have a similar structure.

- App\_currpeaks (application)
- Cust\_currpeaks (customer)
- Resell\_currpeaks (reseller)
- Ts\_currpeaks (teleserver)
- Telera\_currpeaks (overall)
- ASR\_currpeaks (ASR product)
- TTS\_currpeaks (TTS product)
- QA\_currpeaks (Queue Adapter/IVR Server Client)



## app\_currpeaks

Table 88 stores the current peak records for applications.

**Table 88: app\_currpeak**

Column	Type/Size	Description
channels_active	Number(10)	Current peak value for the application.
last_event_time	Date	Date and time when the last event occurred for that criteria.
app_id	Number(6)	Application ID.

## cust\_currpeaks

Table 89 stores the current peak records for customers.

**Table 89: cust\_currpeaks**

Column	Type/Size	Description
channels_active	Number(10)	Current peak value for customers.
last_event_time	Date	Date and time when the last event occurred for that criteria.
cust_id	Number(6)	Customer ID.

## resell\_currpeaks

Table 90 stores the current peak records for resellers.

**Table 90: resell\_currpeaks**

Column	Type/Size	Description
channels_active	Number(10)	Current peak value for resellers.
last_event_time	Date	Date and time when the last event occurred for that criteria.
resell_id	Number(6)	Reseller ID.

**ts\_currpeaks**

[Table 91](#) stores the current peak records for teleservers.

**Table 91: ts\_currpeaks**

Column	Type/Size	Description
channels_active	Number(10)	Current peak value for teleservers.
last_event_time	Date	Date and time when the last event occurred for that criteria.
teleserver_id	Char(32)	IP address of the VCS/IPCS that handled the event.

**telera\_currpeaks**

[Table 92](#) stores the current peak records for a Parent NSP.

**Table 92: telera\_currpeaks**

Column	Type/Size	Description
channels_active	Number(10)	Current peak value for a Parent NSP.
last_event_time	Date	Date and time when the last event occurred for that criteria.
telera_id	Number(6)	NSP ID=1.

**asr\_currpeaks**

[Table 93](#) stores the current peak records for ASR servers.

**Table 93: asr\_currpeaks**

Column	Type/Size	Description
channels_active	Number(10)	Current peak value for ASR servers.
last_event_time	Date	Date and time when the last event occurred for that criteria.
asr_id	Char(25)	ID used for the ASR product.

## tts\_currpeaks

Table 94 stores the current peak records for TTS servers.

**Table 94: tts\_currpeaks**

Column	Type/Size	Description
channels_active	Number(10)	Current peak value for Text-to-Speech servers.
last_event_time	Date	Date and time when the last event occurred for that criteria.
tts_id	Char(25)	ID used for the TTS product.

## qa\_currpeaks

Table 95 stores the current peak records for the Queue Adapter/IVR Server Client.

**Table 95: qa\_currpeaks**

Column	Type/Size	Description
channels_active	Number(10)	Current peak value for the Queue Adapter/IVR Server Client.
last_event_time	Date	Date and time when the last event occurred for that criteria.
qa_id	Number(6)	ID used for the Queue Adapter/IVR Server Client.

## eventc\_stats

Table 96 lists internal processing information and stores statistics of peak processes.

**Table 96: eventc\_stats**

Column	Type/Size	Description
process_name	Char(32)	Name of the EventC process in which to have the statistics.
process_units	Char(25)	Processing units.
last_cycle_at	Date	Time at which the last cycle was run.

**Table 96: eventc\_stats (Continued)**

Column	Type/Size	Description
last_proc_at	Date	Time when the last process was run.
last_proc_recs	Number(10)	Number of records processed in the last cycle.
last_proc_success	Number(10)	Number of records processed successfully in the last cycle.
last_proc_exception	Number(10)	Number of records that had exceptions in the last cycle.
last_proc_skipped	Number(10)	Number of records skipped in the last cycle.
last_error_at	Date	Time when the last error occurred.
last_error_count	Number(10)	Error count during the last cycle.
last_error_desc	Char(1000)	Last error description.
cycle_start_at	Date	Cycle start time.

## peak\_control

Table 97 lists internal processing information.

**Table 97: peak\_control**

Column	Type/Size	Description
criteria_name	Char(50)	Name of the criteria, for example, Application.
peak_exe	Char(50)	Peak calculator executable that calculates peak for this criteria.
criteria_datatype	Char(50)	Data type of the criteria; Number or String only.
criteria_field	Char(50)	Column in Etrackforpeak that stores this criteria.
criteria_reldate	Char(50)	Column in Etrackforpeak that stores the related date for this criteria.

**Table 97: peak\_control (Continued)**

Column	Type/Size	Description
currpeak_table	Char(50)	Name of currpeaks table for this criteria in Peaks database.
currpeak_criteria	Char(50)	Criteria column name in currpeaks table.
currpeak_channels	Char(50))	Channels_active column name in currpeaks table.
currpeak_lastevent	Char(50)	Last_event column name in currpeaks table.
peak_table	Char(50)	Name of the peaks table in Reporter database for this criteria.
peak_criteria	Char(50)	Criteria column name in peaks table.
peak_dtpeak	Char(50)	Dt_peak column name in peaks table.
peak_hr	Char(50)	Peak_hr column name in peaks table.
peak_field	Char(50)	Peak column name in peaks table.
peak_time	Char(50)	Peak_time column name in peaks table.
peak_lastpeak	Char(50)	Last_peak column name in peaks table.
peak_lastpeaktime	Char(50)	Last_peak_time column name in peaks table.
peak_gmtoffset	Char(50)	Gmtoffset column name in peaks table.
process_order	Number(10)	Gmtoffset column name in peaks table.
runable	Number	Can run-1/0.
process_status	Number	Status of the process-1/0.

# Reporter Database

The Reporter database holds base data that Network Reports uses. This data is the result of EventC processing. The data includes call summaries, peaks, and call details.

The Reporter database produces the following CDR data tables:

- callrecords
- hr\_call\_status
- ts\_hr\_call\_status
- report\_tables
- peak\_tables
- download\_request

## callrecords

[Table 98](#) holds records for the calls.

**Table 98: callrecords**

Column	Type/Size	Description
session_id	Char(38)	Unique identifier for the call.
crid	Char(17)	Leg ID for the inbound leg.
utc_dt	Date	Date and Time (GMT) when the call started; accurate to the second.
ani	Char(32)	Calling number.
did	Char(32)	Called number.
ivr_time	Number(10)	Total time spent in IVR phase.
hold_time	Number(10)	Total time spent in hold phase.
call_time	Number(10)	Total duration of the call (call start to call end; does not necessarily equal IVR+hold+talk time).
outcallnum	Char(32)	First outbound dialed number in the call.
end_state	Char(10)	Last state of the call.
app_id	Number(6)	Application ID for the call.
teleserver_id	Char(32)	IP of the VCS/IPCS that handled the call.

**Table 98: callrecords (Continued)**

Column	Type/Size	Description
cust_id	Number(6)	Customer ID.
apptype_id	Number(2)	Application type ID as in EMPS.
reseller_id	Number(6)	Reseller ID.
talk_time	Number(10)	The total duration spent in all agent legs within a call. An agent leg is when a caller is speaking with a live agent.
tfn	Char(32)	Toll Free Number.
cust_date	Date	GMT Date adjusted to customer time zone.
resell_date	Date	GMT Date adjusted to reseller time zone.
telera_date	Date	GMT Date adjusted to Genesys time zone.
asr_id	Char(25)	ID for ASR product used.
tts_id	Char(25)	ID used for the TTS product.
qa_id	Char(25)	ID used for the Queue Adapter/IVR Server Client.
utc_end_dt	Date	Timestamp when call ended.
CallUUID	Char(38)	Universal Connection ID.

## hr\_call\_status

Table 99 provides hourly summary information for applications.

**Table 99: hr\_call\_status**

Column	Type/Size	Description
app_id	Number(6)	Application ID.
curr_date	Date	The date and hour to which this summary belongs.
curr_hr	Char(8)	The hour string, for example, 15:00:00.
total_calls	Number(10)	Total calls in that hour for the application.

**Table 99: hr\_call\_status (Continued)**

Column	Type/Size	Description
total_call_time	Number(10)	Total call time in that hour for the application in seconds.
avg_call_time	Number(10)	Average call time in that hour for the application.
hold_time	Number(10)	Total hold time in that hour for the application.
ivr_time	Number(10)	Total IVR time in that hour for the application.
cust_id	Number(6)	Customer ID.
reseller_id	Number(6)	Reseller ID.
past_average	Number(10)	Average for past six weeks.
talk_time	Number(10)	The total duration spent in all agent legs within a call. An agent leg is when a caller is speaking with a live agent.
cust_date	Date	GMT date adjusted to a customer time zone.
resell_date	Date	GMT date adjusted to a reseller time zone.
telera_date	Date	GMT date adjusted to the Genesys time zone.

## ts\_hr\_call\_status

[Table 100](#) stores the hourly call status records for the VCS/IPCS.

**Table 100: ts\_hr\_call\_status**

Column	Type/Size	Description
teleserver_id	Char(32)	IP address of the VCS/IPCS that handled the call.
curr_date	Date	The date and hour to which this summary belongs.
curr_hr	Char(8)	The hour string, for example, 15:00:00.



**Table 100: ts\_hr\_call\_status (Continued)**

Column	Type/Size	Description
total_calls	Number(10)	Total calls in that hour for the VCS/IPCS.
total_call_time	Number(10)	Total call time in that hour for the VCS/IPCS in seconds.
hold_time	Number(10)	Total hold time in that hour for the VCS/IPCS.
ivr_time	Number(10)	Total IVR time in that hour for the VCS/IPCS.
telera_date	Date	GMT date adjusted to the Genesys time zone.
past_average	Number(10)	Past six weeks average.
talk_time	Number(10)	The total duration spent in all agent legs within a call. An agent leg is when a caller is speaking with a live agent.
eventc_ip	Char(32)	IP address of the EventC server.

## report\_tables

The Reporter database uses the report\_tables for internal processing. Report\_tables include these reports:

- tlra\_reports
- tlra\_report\_display\_table
- tlra\_report\_sqls

## tlra\_reports

[Table 101](#) lists internal processing information.

**Table 101: tlra\_reports**

Column	Type/Size	Description
report_id	Number(10)	Identifier for the reports.
report_display_id	Number(10)	Identifier for the report display.
report_desc	Char(255)	Description of the report.
report_display_name	Char(100)	Display name for the report.

**Table 101: tlra\_reports (Continued)**

Column	Type/Size	Description
report_footer	Char(500)	Footer for the report.
show_graph	Number(10)	Show graph for reports - 1 / 0.
x_axis_field	Number(10)	Column to the referred in the x-axis.
y-axis_field_1	Number(10)	Column to be referred in the first y-axis attributes of graph.
y_axis_field_2	Number(10)	Column referred to in the second y-axis attributes of graph.
x_axis_desc	Char(50)	Description for the x-axis attributes.
y_axis_desc	Char(50)	Description for the y-axis attributes.
report_context	Char(20)	For whom the report is meant.
report_type	Char(20)	Type of the report.
default_for_context	Number(10)	Default report for the context - 1 / 0.
valid_logins	Char(5)	Who can view the report.

**tlra\_report\_display\_table**

Table 102 lists internal processing information.

**Table 102: tlra\_report\_display\_table**

Column	Type/Size	Description
report_display_id	Number(10)	Identifier for the report display.
column_id	Char(255)	Identifier for report column.
column_query_seq	Number(10)	Column query sequence.
column_display_seq	Number(10)	Column display sequence.
column_type	Char(10)	Unit of the column.
summary_type	Char(10)	Summary type.
column_heading	Char(50)	Column heading.
column_postscript	Char(50)	Post script for the column in the graph.

## tlra\_report\_sqls

Table 103 lists internal processing information.

**Table 103: tlra\_report\_sqls**

Column	Type/Size	Description
report_id	Number(10)	Identifier for the reports.
db_platform	Char(10)	Identifier for the database platform.
report_sql	Char(4000)	SQL query for the report.

## peaks tables

The following tables store the peak data for various criteria and have a similar structure:

- App\_peaks (application)
- Cust\_peaks (customer)
- Resell\_peaks (reseller)
- Ts\_peaks (teleserver)
- Telera\_peaks (Telera)
- Asr\_peaks (ASR ID)
- Tts\_peaks (TTS ID)
- Qa\_peaks (Queue Adapter/IVR Server Client ID)

---

Note: These tables are also part of the Peaks database.

---

## app\_peaks

Table 104 stores the hourly peak records for applications.

**Table 104: app\_peaks**

Column	Type/Size	Description
dt_peak	Date	The date and hour to which this peak belongs.
peak	Number(10)	Peak value for the hour.
peak_time	Date	The time at which the peak occurred.

**Table 104: app\_peaks (Continued)**

Column	Type/Size	Description
app_id	Number(6)	Application ID.
tz_date	Date	Time zone adjusted date.

**cust\_peaks**

[Table 105](#) stores the hourly peak records for customers.

**Table 105: cust\_peaks**

Column	Type/Size	Description
dt_peak	Date	The date and hour to which this peak belongs.
peak	Number(10)	Peak value for the hour.
peak_time	Date	The time at which the peak occurred.
cust_id	Number(6)	Customer ID.
tz_date	Date	Time zone adjusted date.

**resell\_peaks**

[Table 106](#) stores the hourly peak records for resellers.

**Table 106: resell\_peaks**

Column	Type/Size	Description
dt_peak	Date	The date and hour to which this peak belongs.
peak	Number(10)	Peak value for the hour.
peak_time	Date	The time at which the peak occurred.
resell_id	Number(6)	Reseller ID.
tz_date	Date	Time zone adjusted date.

## Ts\_peaks

Table 107 stores the hourly peak records for teleservers.

**Table 107: ts\_peaks**

Column	Type/Size	Description
dt_peak	Date	The date and hour to which this peak belongs.
peak	Number(10)	Peak value for the hour.
peak_time	Date	The time at which the peak occurred.
teleserver_id	Char(32)	Teleserver ID.
tz_date	Date	Time zone adjusted date.
dt_peak	Date	The date and hour to which this peak belongs.

## telera\_peaks

Table 108 stores the hourly peak records for a Parent NSP.

**Table 108: telera\_peaks**

Column	Type/Size	Description
dt_peak	Date	The date and hour to which this peak belongs.
peak	Number(10)	Peak value for the hour.
peak_time	Date	The time at which the peak occurred.
telera_id	Number(6)	NSP ID=1.
tz_date	Date	Time zone adjusted date.

## asr\_peaks

Table 109 stores the hourly peak records for ASR servers.

**Table 109: asr\_peaks**

Column	Type/Size	Description
dt_peak	Date	The date and hour to which this peak belongs.
peak	Number(10)	Peak value for the hour.
peak_time	Date	The time at which the peak occurred.
asr_id	Char(26)	ID that the ASR product uses.
tz_date	Date	Time zone adjusted date.

## tts\_peaks

Table 110 stores the hourly peak records for Text-to-Speech servers.

**Table 110: tts\_peaks**

Column	Type/Size	Description
dt_peak	Date	The date and hour to which this peak belongs.
peak	Number(10)	Peak value for the hour.
peak_time	Date (7)	The time at which the peak occurred.
tts_id	Char(25)	ID that the TTS product uses.
tz_date	Date	Time zone adjusted date.
dt_peak	Date	The date and hour to which this peak belongs.

## qa\_peaks

Table 111 stores the hourly peak records for Queue Adapters/IVR Server Clients.

**Table 111: qa\_peaks**

Column	Type/Size	Description
dt_peak	Date	The date and hour to which this peak belongs.
peak	Number(10)	Peak value for the hour.
peak_time	Date	The time at which the peak occurred.
qa_id	Char(25)	ID that the Queue Adapter/IVR Server Client uses.
tz_date	Date	Time zone adjusted date.

## download\_request

Table 112 stores the download requests and the status of those requests.

**Table 112: download\_request**

Column	Type/Size	Description
request_id	Numeric (10)	Unique identifier for the report requests.
request_date	Datetime	Date/Time when the report creation was requested.
user_id	Numeric (10)	Uses Login Server user ID. UL_USERS table.
report_id	Numeric (10)	Uses Report ID reporter.tlra_reports.
report_type	Varchar (10)	Hourly summary (HS) / Call details (CD).
selected_customer	Varchar (32)	Customer selected in the report request.
selected_application	Varchar (32)	Application selected in the report request.
start_date	Datetime	Start date selected in the report request.
end_date	Datetime	End date selected in the report request.

**Table 112: download\_request (Continued)**

Column	Type/Size	Description
download_desc	Varchar (64)	Description given by the user for the report request.
report_status	Varchar (10)	Status of the report creation. Progress / Error / Available (download link).
completion_dt	Datetime	Date/Time when the report creation was completed.
filepath	Varchar (1024)	URL of the report file created.
app_id	Numeric (10)	Application ID selected in the report request.
cust_id	Numeric (10)	Customer ID selected in the report request.
reseller_id	Numeric (10)	Customer's Reseller's ID.
report_display_id	Numeric (10)	Display ID of the report.
valid_logins	Varchar (10)	Type of login from which the report request was made.

---

## RepDWH Database

The RepDWH database holds call records that the NSP uses for billing calculations. Each call record includes application and customer attributes that are required for billing, such as port levels.

The RepDWH database produces the following CDR data tables:

- call\_phases—stores one record per leg of the call
- billcallrecords—stores one record per call

The records in the tables are related by the session\_id column, which identifies a call uniquely.



## call\_phases

[Table 113](#) lists internal processing information and stores the Call Phases used for billing purposes. This table provides one record per phase of the call. The significant columns are:

- phase\_time
- phase\_type
- did

**Table 113: call\_phases**

Column	Type/Size	Description
session_id	Char(38)	Unique identifier for the call.
phase_id	Number(10)	Identifier for a phase.
phase_type	Char(10)	Type of phase: IVR, TALK, HOLD, OBWAIT. <b>Note:</b> You can discard OBWAIT for billing calculations since it represents the state of the inbound leg (waiting for outbound to complete) when an agent talk is active.
start_time	Date	Date/time at which the phase started.
end_time	Date	Date/time at which the phase ended.
ani	Char(32)	The calling number.
did	Char(32)	Represents the DNIS for IVR and HOLD phases. Represents the number dialed-out (agent) for TALK and OBWAIT phases.
crid	Char(16)	Leg ID for the phase.
phase_time	Number(10)	Total time in seconds spent in the leg.
app_id	Number(6)	Application ID.
cust_id	Number(6)	Customer ID.
apptype_id	Number(2)	Application type.
reseller_id	Number(6)	Reseller ID.
generic_call_id	Char(256)	SIP call leg ID.

## billcallrecords

**Table 114** holds the billing records used for billing purposes. Total call durations for the call are provided in the billcallrecords table in the following columns:

- call\_time
- ivr\_time
- hold\_time
- talk\_time

**Table 114: billcallrecords**

Column	Type/Size	Description
session_id	Char(38)	Unique identifier for the call.
crid	Char(17)	ID for the event's leg.
utc_dt	Date	Date and Time (GMT) when the call started; accurate to the second.
ani	Char(32)	Calling number.
did	Char(32)	Called number.
ivr_time	Number(10)	Total time spent in IVR phase.
hold_time	Number(10)	Total time spent in hold phase.
call_time	Number(10)	Total duration of the call (call start to call end; does not necessarily equal IVR+hold+talk time).
outcallnum	Char(32)	First outbound dialed number in the call.
end_state	Char(10)	Last state of the call.
app_id	Number(6)	Application ID for the call.
teleserver_id	Char(32)	IP address of the VCS/IPCS that handled the call.
cust_id	Number(6)	Customer ID.
apptype_id	Number(2)	Application type ID as in EMPS.
startdate_of_service	Date	Date on which this application started.
max_app_ports	Number(10)	Not used.
ports_level1	Number(10)	Ports for the customer - level1 bursting.

**Table 114: billcallrecords (Continued)**

Column	Type/Size	Description
ports_level2	Number(10)	Ports for the customer - level2 bursting.
ports_level3	Number(10)	Ports for the customer - level3 bursting.
reseller_id	Number(6)	Reseller ID.
event_seq	Char (100)	The sequence of events that occurred for the call. For example: -01-03-05-02-06.
custpeak	Number(10)	The call peak value for the customer at the start of this call, including this call (it will at least be 1).
talk_time	Number(10)	The total duration spent in all agent legs within a call. An agent leg is when a caller is speaking with a live agent.
tfn	Char(32)	Toll Free Number.
billable_ports	Number(10)	The number of ports for which the customer will be billed.
cust_date	Date	GMT date adjusted to customer time zone.
resell_date	Date	GMT date adjusted to reseller time zone.
telera_date	Date	GMT date adjusted to Genesys time zone.
asr_id	Char(25)	ID that the ASR product uses.
tts_id	Char(25)	ID that the TTS product uses.
qa_id	Char(25)	ID that the Queue Adapter/IVR Server Client uses.
ts_ani	Char(25)	ANI of the teleserver.
generic_call_id	Char(256)	SIP call leg ID.
CallUUID	Char(38)	Universal Connection ID.

## Scenarios

For the scenarios in Table 115 on [page 404](#), only one record will appear in the billcallrecords table. The number of records vary in call\_phases depending on the call scenario as described below.

**Table 115: Scenarios**

Scenario	Records in Call Phase
<p><b>Scenario 1</b></p> <p>Call is self-service application without forwarding to any agent (Configuration Manager or dialing of GVP to an ACD).</p> <ul style="list-style-type: none"> <li>• A &gt; B (call is handled on GVP)</li> <li>• A or B hang up the call</li> </ul>	<p>An IVR record for the self-service phase.</p>
<p><b>Scenario 2</b></p> <p>GVP handles the call. After the caller has decided by menu which service is wanted, the caller is forwarded (by GVP dialing without Configuration Manager involvement) to an ACD (ACD then forwards to agent by ACD routing).</p> <ul style="list-style-type: none"> <li>• A &gt; B (parking/preselection on GVP)</li> <li>• A &gt; B &gt; &gt; C (customer talks to agent after parking, no Configuration Manager involvement)</li> <li>• A or C hang up the call</li> </ul>	<ol style="list-style-type: none"> <li>1. An IVR record for the self-service phase.</li> <li>2. An OB_WAIT record for the agent talk phase for the inbound leg.</li> <li>3. A TALK record for the talk phase.</li> </ol>
<p><b>Scenario 3</b></p> <p><b>Note:</b> This scenario is similar to Scenario 2, but with Configuration Manager involvement.</p> <p>GVP script triggers a strategy, URS decides which agent/location to forward the call to, ExternalRouting is initiated, and IVR Server tells GVP which number to dial.</p> <ul style="list-style-type: none"> <li>• A &gt; B (parking on GVP)</li> <li>• A &gt; B &gt; &gt; C (customer talks to agent after parking)</li> <li>• A or C hang up the call</li> </ul>	<ol style="list-style-type: none"> <li>1. An IVR record for self-service phase.</li> <li>2. A HOLD record for the queueing phase.</li> <li>3. An OB_WAIT record for the agent talk phase for the inbound leg.</li> <li>4. A TALK record for the agent talk phase.</li> </ol>

**Table 115: Scenarios (Continued)**

Scenario	Records in Call Phase
<b>Scenario 4</b> Call is transferred (after Agent 1 has talked to caller) from Agent 1 to Agent 2 locally on the ACD. <ul style="list-style-type: none"> <li>• A &gt; B (parking on GVP)</li> <li>• A &gt; B &gt; &gt; C (customer talks to agent after parking)</li> <li>• A &gt; B &gt; &gt; on hold C &gt; &gt; D; new call on ACD, Agent 1 transfers call locally</li> <li>• A &gt; B &gt; &gt; D Agent 2 now talks to agent (transfer or conference)</li> <li>• A or D hang up the call</li> </ul>	<ol style="list-style-type: none"> <li>1. An IVR record for self-service phase.</li> <li>2. A HOLD record for the queueing phase.</li> <li>3. An OB_WAIT record for the agent talk phase (all phases) for the inbound leg.</li> <li>4. A TALK record for the first agent talk phase (C).</li> <li>5. A TALK record for the second agent talk phase (D).</li> </ol>
<b>Scenario 5</b> Call is transferred (after Agent 1 has talked to caller) from Agent 1 to Agent 2 (on another site) with multisite routing. <ul style="list-style-type: none"> <li>• A &gt; B (parking on GVP)</li> <li>• A &gt; B &gt; &gt; C (customer talks to agent after parking)</li> <li>• A &gt; B; A &gt; C (customer is rerouted from Agent 1 to Agent 2 via GVP; multisite routing)</li> </ul>	<ol style="list-style-type: none"> <li>1. An IVR record for self-service phase.</li> <li>2. A HOLD record for the queueing phase.</li> <li>3. An OB_WAIT record for the agent talk phase (all phases) for the inbound leg.</li> <li>4. A TALK record for the first agent talk phase (Agent 1).</li> <li>5. A TALK record for the second agent talk phase (Agent 2).</li> </ol>

---

## EventC and Reporter Data Cleanup

EventC and Reporter databases automatically perform data cleanup. You can edit the values of the cleanup parameters in EMPS. To do so, log in to EMPS, and go to Servers > EVENTC > <server name> > ConfigEventC > Edit Node.

Edit the following parameters:

- Save raw events for (days)
- Save reporter data for (days)
- Save billing data for (days)
- Perform database internal cleanup (minutes)

## Billing Data Files

The VCS/IPCS servers archive data files called Billing Data files, which are located under the archive directory in EventC. Files are placed in separate folders for each day. The file name is in the format YYYYMMDD. The administrator can delete the directories for the days earlier than the desired period.

These files are usually required in case of debugging. The recommended period for keeping these files is seven days.

---

## Resetting Peaks for EventC

This section describes how to reset peaks.

The Peak Calculator maintains a continuous count of calls started and calls completed as it traverses through the call stream. If the counter is interrupted for any reason (for example, an unexpected database shutdown that corrupts data), an offset could be introduced in the count; this offset would then be carried over into all calculations. The Peak Calculator logs show the timestamp mismatch. In these situations, Genesys recommends that you reset peaks, which sets all peak counters to zero and starts counting from the next call.

---

**Warning!** Since this procedure resets peaks to zero and starts peak calculation from the next available call, peak data will be incorrect for some time. It may take close to six hours before peaks become accurate again. The period of inaccuracy starts from the latest record displayed in Reporter (peak reports) at the time you run the reset procedure.

---

## Resetting Peaks

1. Open the EventC Element Management System GUI.
2. Select **Advanced Options** under the **Events Collector** node.
3. Click **Trigger Peaks Reset**.

## After Resetting Peaks

1. Restart the following EventC processes:
  - CallRecsGenerator
  - PeaksNSP

2. Monitor the Peak Calculator log files for some time to verify that no errors were reported.
3. Monitor the Peak reports through Reporter to verify that the data appears correct.







## Appendix

# B

## Default Settings

This appendix describes how to change the Voice Communication Server/IP Communication Server (VCS/IPCS) to another EventC.

This appendix contains the following section:

- [Changing VCS/IPCS to Another EventC, page 409](#)

---

## Changing VCS/IPCS to Another EventC

The following procedure describes how to switch a VCS/IPCS to a different EventC in a graceful manner. This procedure is required in situations where a customer already has running calls in a VCS/IPCS, with billing events being sent to an existing EventC, and the customer wants to switch to a new EventC box for scaling or maintenance reasons.

- Important** The procedure requires a restart of the VCS/IPCS box, so plan the switch in such a way as to not affect peak traffic.
1. Set up the new EventC box and ensure that it starts and runs without errors. This box can also be an existing one that is already handling events.

---

Note: Refer to the *Genesys Voice Platform 7.6 Deployment Guide* for instructions on how to set up the EventC.

---

2. Gracefully shutdown the WatchDog process on the VCS/IPCS box.
3. Ensure that all billing files under CN\_ROOT\data have been cleaned up.

---

Note: The data directory should be empty. Files in the folder are automatically cleaned up when you shut down the WatchDog process.

---

4. Start WatchDog.





## Appendix

# C

## Call Control Adapter

This appendix describes the functions and messages of the Call Control Adapter (CCA).

This appendix contains the following sections:

- [Overview, page 411](#)
- [CCA Messages, page 412](#)
- [Error Handling, page 415](#)
- [Summary of Message Flows, page 415](#)

---

## Overview

The Call Control Adapter (CCA) interface enables call transfers to be performed using the service provider's signaling entity, such as a Service Control Point (SCP).

All communication between Genesys Voice Platform (GVP) and the CCA is over HTTP and uses query strings and XML response pages. Both web server and client support are required on the platform that is hosting the CCA.

- CFA > CCA requests are query strings.
- CCA > CFA responses are query strings.
- CCA > CFA requests are query strings.
- CFA > CCA responses are XML pages.

## CFA to CCA Requests

Each message from the CFA to the CCA includes the NOTIFYPROCESS=<process name> field to identify the CCA. Each request must have the following:

`http://queueadapterurl?NOTIFYPROCESS=<processname>`

---

**Note:** The requests from the CFA are in HTTP1.1 format. Genesys recommends that the CCA follow HTTP1.1 parsing rules (RFC 2616). If the CCA developer decides to perform any other kind of parsing (such as string parsing), it is very important to be aware that the order of the request parameters is not guaranteed—the parameters can be issued in any order. Any unknown parameters not specified in this appendix should be dropped by the CCA and not flagged as an error.

---

## CCA to CFA Requests

The CFA passes its own URL in the first request (NEW\_CALL\_REQ) that it sends to the CCA. The CCA must use this URL to communicate with the CFA.

Each message can have multiple fields appended to the NEW\_CALL\_REQ request. As with any other HTTP request, the ampersand (&) character is the field separator.

The response to each request begins with the following fields. Depending on the request type, the response page can contain one or more fields.

RESULT=<SUCCESS/FAILURE/REJECT>&REASON=<Reason string in case of failure>

---

## CCA Messages

This section describes the CCA messages, their field names, and values.

### NEW\_CALL\_REQ

This message is from the CFA to the CCA, and it informs the CCA that a new call has arrived on GVP. [Table 116](#) describes the message.

**Table 116: NEW\_CALL\_REQ Message**

Field Name	Value	Mandatory or Optional Field
cc.nextaction	NEW_CALL_REQ	Mandatory
application	<String to identify the IVR application>	Mandatory
sessionid	<Unique string to identify this call>	Mandatory
legid	<Unique string to identify the individual leg of the call>	Mandatory
dnis	Dialed Number Identification Service	Mandatory
ani	Automatic Number Identification	Optional

**Table 116: NEW\_CALL\_REQ Message (Continued)**

Field Name	Value	Mandatory or Optional Field
tollnumber	<800 number or dialed number>	Optional
CTA_Interface_Version	1.0 This specifies the CTA interface version number. This number will be increased whenever the interface document changes. The CCA can use this number to find out what interface is supported by GVP.	Mandatory

**Valid Response** The valid response from the CCA is RESULT=SUCCESS&REASON=Normal. This response is sent if the CCA is accepting the call.

**Error Response** The RESULT=FAILURE&REASON=<error description>&ERRORCODE=<error number> response is sent when the CCA encounters any error on its end. The ERRORCODE specifies a number for the error, and the REASON specifies the error string.

The valid error code is GENERIC\_ERROR. The CFA logs this error and raises a trap. If this was the response from the primary CCA, the CFA tries the backup CCA.

When the CFA experiences a timeout with the primary CCA, it contacts the backup CCA.

## UPDATE\_CALL\_STATUS\_REQ

This message is sent from the CFA to the CCA to indicate the end of a call.  
[Table 117](#) describes the message.

**Table 117: UPDATE\_CALL\_STATUS\_REQ Message**

Field Name	Value	Mandatory or Optional Field
cc.nextaction	UPDATE_CALL_STATUS_REQ	Mandatory
sessionid	<Unique string to identify this call>	Mandatory
callstatus	6 <6 = Disconnect>	Mandatory
legid	<Unique string to identify individual leg of the call>	Mandatory

**Valid Response** The valid response from the CCA is RESULT=SUCCESS&REASON=Normal or RESULT=FAILURE&REASON=<error description>&ERRORCODE=<error number>

In either response, the CFA just removes the call from GVP.

## INITIATE\_TRANSFER\_REQ

This message is sent by the CFA to the CCA to initiate a call transfer to a specific target specified by Telnum. [Table 118](#) describes the message.

**Table 118: INITIATE\_TRANSFER\_REQ Message**

Field Name	Value	Mandatory or Optional Field
cc.nextaction	INITIATE_TRANSFER_REQ	Mandatory
Sessionid	<Unique string to identify this call>	Mandatory
Telnum	<The phone number to dial to connect to an agent>	Mandatory
TransferType	CallTransfer	Mandatory

The TransferType specifies the type of transfer that will be initiated by GVP.

TransferType = CallTransfer implies that the caller leg will not be dropped by GVP, and that any errors encountered during the transfer by the CCA will be propagated back to the IVR application. The entity responsible for performing the call transfer initiates the hang up of the caller leg when the call is successfully transferred.

---

Note: The CFA waits for two minutes for a response from the CCA. If it does not receive a response, it times out and assumes that a successful transfer has occurred.

---

**Valid Response** The valid response from the CCA is RESULT=SUCCESS&REASON=Normal. This response is sent if everything went correctly.

**Error Response** RESULT=FAILURE&REASON=<BUSY/NO\_ANSWER/GENERIC\_ERROR>&ERRORCODE=<number>  
This response signifies a failure to transfer the call and the CFA takes corrective action based on the VoiceXML and TXML specification.

The valid error codes are:

- GENERIC\_ERROR
- BUSY
- NO\_ANSWER

The following TXML and VoiceXML tags are supported to initiate a transfer:

- CREATE\_LEG\_AND\_DIAL (bridge=yes) (TXML tag)
- transfer (bridge=false) (VoiceXML tag)

## PING\_REQ

This message is sent by the CFA to the CCA, and it can be sent to check the health of the CCA. In response to this request, the CCA can return

RESULT=Success. The CCA also can return additional status strings, such as host name, IP address, CCA interface version, and the status of its back-end connection to any other components. The additional status strings can be used by Network Operation Center personnel to check the health of the CCA in the event of problems. [Table 119](#) describes the message.

**Table 119: PING\_REQ Message**

Field Name	Value	Mandatory or Optional Field
cc.nextaction	PING_REQ	Mandatory

## Error Handling

If the CFA receives any unsupported messages from the CCA, it returns an error XML page:

```
<?xml version="1.0" ?>
<XMLPage TYPE="CC" CUSTID="CallNet" PAGEID="CC-111" VERSION="1.0" Sessionid="{13455}"
  HREF="" >
<RESPONSE RESULT="FAILURE" REASON="Unsupported message." />
</XMLPage>
```

## Summary of Message Flows

[Table 120](#) summarizes the message flows between the CFA and the CCA.

**Table 120: Message Flows**

Message	From	To
NEW_CALL_REQ	CFA	CCA
UPDATE_CALL_STATUS_REQ	CFA	CCA
INITIATE_TRANSFER_REQ	CFA	CCA
PING_REQ	CFA	CCA







## Appendix

# D Integration with Genesys Framework

This appendix describes Genesys Voice Platform (GVP) integration with Genesys Framework. It contains the following sections:

- [Integration, page 417](#)
- [Configuring Objects, page 418](#)
- [Activating Routing, page 421](#)
- [Solution Control Interface, page 422](#)
- [Integration Features, page 426](#)
- [Feature Comparison, page 428](#)

---

## Integration

Genesys Voice Platform (GVP) interfaces with other Genesys products through Genesys Framework.

Calls, along with any data associated with them, are passed to the Genesys Interactive Voice Response (IVR) Server. The IVR Server, in turn, transmits the information to other elements of the Genesys suite for integrated call-handling purposes, such as:

- Real-time and historical reporting (through CCPulse+ and Contact Center Analyzer, respectively) for integrated reporting.

---

Note: For detailed information, refer to your Genesys Reporting documentation.

---

- Intelligent queuing and call delivery through Genesys Universal Routing Server (URS).

- Workflow and workforce management through Genesys Workforce Management.

The IP Communication Server (IPCS)/Voice Communication Server (VCS) includes an IVR Server Client that communicates with a Genesys IVR Server on a remote host. The IVR Server Client informs the IVR Server of new calls arriving at the IPCS/VCS and of the termination of existing calls.

The IVR Server is contacted at call setup. In an IPCS/VCS Behind-the-Switch configuration, the IVR Server furnishes the Automatic Number Identification (ANI) and Dialed Number Identification Service (DNIS) of the incoming call. During call setup, the IVR Server, along with the URS controls the VoiceXML script executed by the IPCS/VCS, which relays call-related data to IVR Server. When necessary, the IVR Server orchestrates the transfer of the call to the appropriate agent at the end of the call flow for the voice application.

---

## Configuring Objects

To enable GVP integration with Genesys Framework and, in particular, with T-Server, you must configure objects for a switch, directory numbers (DNs), IVRs, and IVR Ports in Configuration Manager.

The configuration procedures that follow are written with the assumption that no switch or IVR objects are configured yet. The configuration procedures differ, depending on whether the IVR is located behind or in front of the switch.

## Modifying the IVR Server

To enable the IVR Server to communicate with GVP, modify the configuration of the virtual T-Server application that corresponds to your IVR Server:

1. Open Configuration Manager.
2. Open the Properties dialog box of the virtual T-Server application.
3. On the Options tab, select the `gli_server_group_1` section.
4. Within this section, select the `gli-server-address` option, and set its value to the host name of the IVR Server. Follow this with a free port number (that is, a port number not associated with any application that is currently running on the IVR Server host).

Use a colon to separate the two parts of the option value, as follows:

```
host:port
```

If more than one GVP server is used, configure a separate section for each. Make the section names unique by using the following syntax:

```
gli_server_group_x
```

Where *x* is an arbitrary but unique number—for example:

```
gli_server_group_1.
```

For more information on how to configure the IVR Server, refer to your IVR Server documentation.

## With an IVR-Behind-the-Switch Configuration

### Configuring DNs

1. Open Configuration Manager:
2. Create a `Switching Office` object for the real switch that GVP uses.
3. Create a `Switch` configuration object that represents your real switch, and associate it with this `Switching Office`.
4. Under the `Switch`, configure DNs of the `Voice Treatment Port` type. These should match DNs of the `Extension` or `Position` type that are configured on the physical switch that GVP uses.

### Configuring IVRs and IVR Ports

1. In the `Resources` section of Configuration Manager, under `IVRs`, create an IVR object of any type except `Unknown`:
  - a. The value of the `IVR Name` field is the `IVR Client Name` specified in the IPCS/VCS configuration. Refer to the *Genesys Voice Platform 7.6 Deployment Guide*.
  - b. Specify a valid version of the IVR.
  - c. Use the `Browse` button to select the IVR Server application.
2. Under the IVR object, create `IVR Port` objects for all active IVR ports:
  - a. Use a two-digit format (such as 01) to specify a `Port Number` (see [“Ports”](#)).
  - b. Browse for the `Associated DN`, which should be the `Voice Treatment Port DN` that you created in Step 4 of [“Configuring DNs”](#).  
Make sure that this association reflects the actual association between a particular number and an IVR (IVR Port) in the switch configuration.

## Ports

A *port* is defined as the capability to receive or send a discrete call. For example, a hardware platform supporting 23 simultaneous and discrete conversations would require 23 ports.

The GVP architecture has universal ports, which deliver features such as Automatic Speech Recognition (ASR), Text-to-Speech (TTS), and inbound call processing.

GVP can simultaneously handle multiple calls for one or more voice applications. In the IPCS/VCS, a set of physical ports is not dedicated to a

particular voice application. A call received on any physical port can access any configured voice application.

You can deploy the IPCS/VCS component of GVP in front of or behind the switch. Each mode has Universal Port capability. Different approaches are used in each configuration to identify the desired voice application.

## Behind-the-Switch Deployment

When the IPCS/VCS is deployed behind the switch, the enterprise switch is configured with a unique Directory Number (DN) for each Digital Signal Zero (DS0) from the enterprise switch that terminates on the IPCS/VCS. A DN is a unique logical number associated with each port on the enterprise switch. The Genesys Configuration Manager environment permits the association of an IPCS/VCS port with a DN, with the help of an IVR Server application. Each instance of IPCS/VCS must be registered manually as an IVR object under the **Resources > IVRs** section, as described in Step 1 of “Configuring IVRs and IVR Ports” on [page 419](#). Each IPCS/VCS is configured with a corresponding set of DNs.

Identifying the voice application in a behind-the-switch configuration also requires the Genesys IVR Server. The IPCS/VCS registers itself with the Genesys IVR Server at startup. Each IPCS/VCS universal port (IVR port) is labeled with a unique IVR port number on each IPCS/VCS. The IVR Server reads objects in Configuration Manager with the mapping of each IVR port to its designated DN from the IVR.

When an incoming call arrives at the enterprise switch:

1. The call is presented to an available IVR port on the IPCS/VCS.
2. Simultaneously, the enterprise switch provides the IVR Server, through the CTI Link, with the incoming call's ANI and DNIS.
3. The IPCS/VCS contacts IVR Server and solicits caller information that is associated with that unique IVR port number.
4. The IVR Server associates the number received from the IPCS/VCS with an enterprise switch DN, and returns the associated information to the IPCS/VCS.

## In-Front-of-the-Switch Deployment

When the IPCS/VCS is deployed in front of the switch, it receives the incoming call's ANI and DNIS directly from the Public Switched Telephone Network (PSTN).

---

**Note:** As noted above, you need a different IVR object for each IPCS/VCS with port numbers starting with 01—for example, 01, 02, ...99. If the total number of ports on a IPCS/VCS is less than 100, use two-digit port numbers. If there are more than 100 ports on one IPCS/VCS, use three-digit port numbers—for example, 101, 102, 199, and so on. Do *not* use single-digit port numbers; for example, do not use 1, 2, and so on.

---

## With an IVR-In-Front-of-the-Switch Configuration

### Configuring DNs

1. Create a `Switching Office` object of the `Virtual Switch` for `IVR-in-Front` type.
2. Create a `Switch` configuration object that represents your virtual switch, and associate it with this `Switching Office`.
3. On the `Switches` tab of the virtual T-Server application, associate the `Switch` with a virtual T-Server application that represents your IVR Server.
4. Under the `Virtual Switch`, configure DNs of the `Voice Treatment Port` type. These DNs are “fake” DNs, because they are in a virtual switch, not a real switch.

### Configuring IVRs and IVR Ports

1. Create an IVR object of any type except `Unknown`:
  - a. The value of the `IVR Name` field is the `IVR Client Name` specified in the IPCS/VCS configuration. Refer to the *Genesys Voice Platform 7.6 Deployment Guide*.
  - b. Specify a valid version of the IVR Server.
  - c. Use the `Browse` button to select the IVR Server application.
2. Under the IVR object, create `IVR Port` objects for all active IVR ports:
  - a. For VCS and IPCS, enter the IP address of the CFA host plus a three digit number to specify a `Port Number`. For example, 1720412904001.
  - b. Browse for the `Associated DN`, which should be the `Voice Treatment Port DN` you created in Step 4 of “[Configuring DNs](#)”.

---

## Activating Routing

You can use Genesys Universal Routing with Genesys Voice Platform. To route calls from GVP through URS, you must configure Routing Points for the IVR-in-Front-of-the-Switch configuration, or Virtual Routing Points (VRPs)

for the IVR-Behind-the-Switch configuration. Routing Points or VRPs are used in the voice application that is generated through Studio. See the *Studio Help* for more information.

You must configure Switch objects and DN objects of the corresponding types (Routing Points or Virtual Routing Points) in Configuration Manager as described in the following sections.

The configuration procedure differs, depending on whether the IVR is located behind or in front of the switch.

---

**Note:** If routing strategies specify Agents or Agent Groups as routing targets, the Agents must be logged in and have Ready status in order to be available for routing. See *Genesys Universal Routing* documentation for more information.

---

### With an IVR-Behind-the-Switch Configuration

Under the real switch, create DNs of the Virtual Routing Point type.

---

**Note:** Virtual Routing Points are typically created in the real switch.

---

### With an IVR-In-Front-of-the Switch Configuration

Under the virtual switch, create DNs of the Routing Point type.

---

## Solution Control Interface

You must configure the GVP application in Configuration Manager and install the Local Control Agent (LCA) on the VCS/IPCS prior to the IPCS/VCS installation. To verify that the application has been configured correctly in Configuration Manager:

1. Open SCI.

The application should be visible in the SCI graphical user interface (GUI). In the Type column, the application type should be listed as GVP-Voice Communication Server (see [Figure 138](#)).

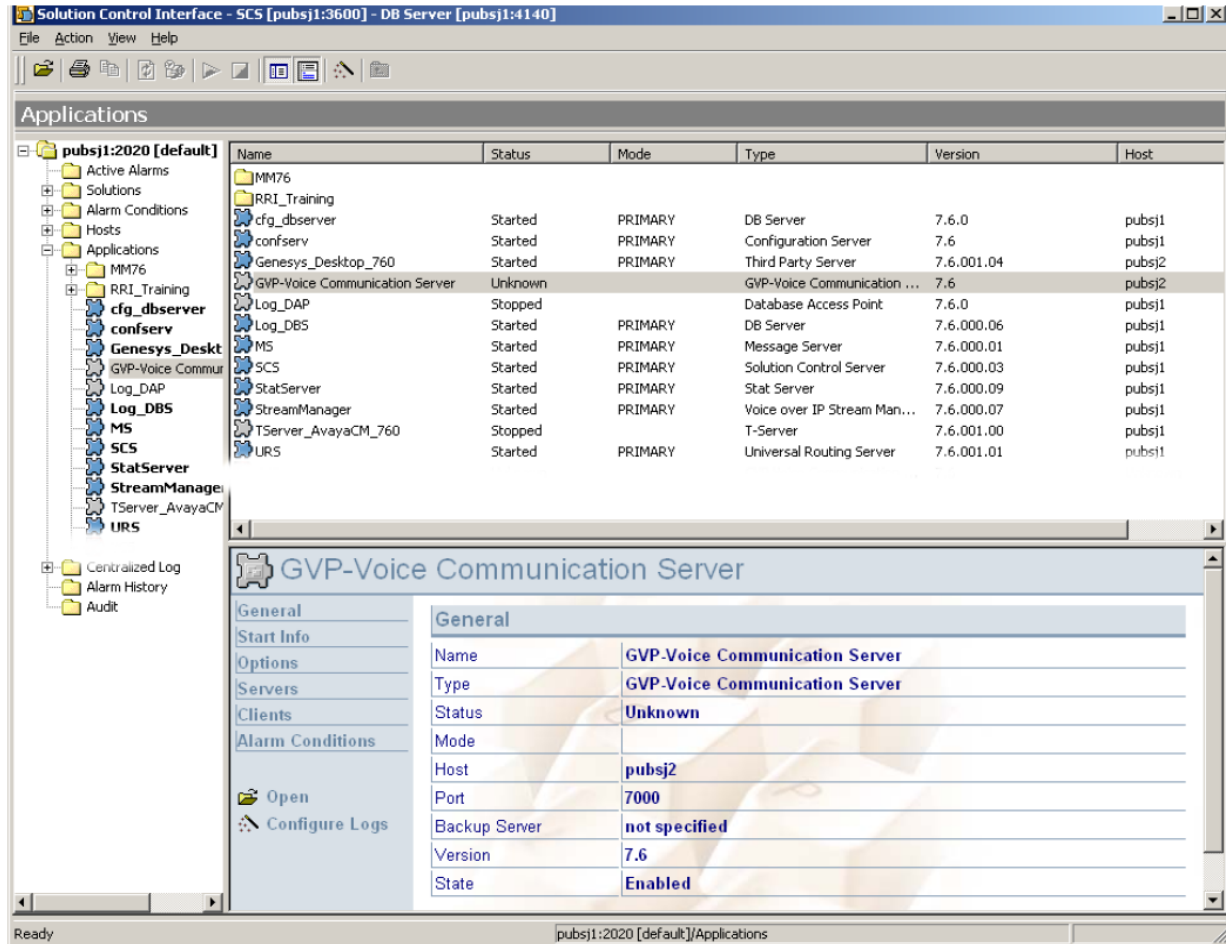


Figure 138: Solution Control Interface

2. To start the application, highlight it, right-click the application name, and select Start from the shortcut menu that appears.

A dialog box appears, asking you to confirm the application start.

3. Click Yes.

Once the application is started, it can be stopped.

4. To stop an application, highlight the application and click Stop.

5. Click Open to open an application. The log window opens.

On the Standard Log Records tab, the IPCS/VCS-generated Simple Network Management Protocol (SNMP) trap messages are shown as Standard Logs.

Table 121 lists the message IDs and descriptions.

Note: For more detailed information on traps, see the *Genesys Voice Platform 7.6 Troubleshooting Guide*.

**Table 121: IPCS/VCS Message IDs and Descriptions**

Message ID	Description
<b>Generic Trap Message</b>	
21000	Generic Trap Message
21001	Internal Error
21002	Invalid Parameter
21003	Out of Memory
<b>WatchDog Trap Messages</b>	
31000	Server Started
31001	Server Shutdown Initiated
31002	Server Stopped
31003	Bad Configuration File
31004	Process Exited
31005	Process Started
31006	Process Restarted
31007	Automatic Shutdown Initiated
31008	System Check Alert
31009	Partial Start
<b>Pop Controller Trap Messages</b>	
41000	CC Error
41001	IVR Error
41007	Dial Error
41008	Call Dropped
41009	Abnormal Call Termination
41010	Resource Not Found
41011	Bad XML Page
41012	Network Timeout



**Table 121: IPCS/VCS Message IDs and Descriptions (Continued)**

Message ID	Description
41013	Network Error
41014	Telephony Error
41015	Call Transferred
<b>Text-To-Speech (TTS) Trap Messages</b>	
211000	TTS
211001	TTS Request Abandoned
211002	TTS Request Rejected
211003	TTS Max Size Exceeded
211004	TTS No Language Support
211005	TTS Request Invalid
211006	TTS Conversion Error
211007	TTS Initialization Error
211008	TTS Write Error
211009	TTS Server Error
211010	TTS Request Timeout
211011	TTS Request Connection Failure
211012	TTS Error Response
211013	TTS Error Event
<b>IVR Server Client Trap Messages</b>	
341000	IQA Started
341001	IQA Down
341002	IQA Network Failure
341003	IQA Heartbeat Failure
341004	IQA Failure Event
341005	IQA Network Up

**Table 121: IPCS/VCS Message IDs and Descriptions (Continued)**

Message ID	Description
341006	IQA ISVR Timeout
341007	IQA ISVR Not Avail
341008	IQA Invalid Remote Address

---

## Integration Features

As a result of GVP integration with Genesys Framework, various features are made available to the contact center.

### Call Flow Types

The IVR-Controlled and URS-Controlled call flow types are examples of the different degrees of call flow integrations available when using GVP with Genesys Framework. Most call flows will use some aspects of the two examples specified below.

#### IVR-Controlled Call Flow

In this call-flow type, the self-service phase can continue without IVR Server assistance. The IVR Server is contacted when the call is queued by the voice application through the TXML `<QUEUE_CALL>` tag using Genesys Studio's RoutePoint Block. For reporting purposes, the IVR Server is always notified of call arrival and the hang-up of events.

#### URS-Controlled Call Flow

In this call-flow type, the self-service phase cannot continue without IVR Server assistance. GVP waits for URS to instruct it as to which voice application to execute.

### Route Request

This feature enables the voice application to park a call on IPCS/VCS and issue a request to Genesys Framework to identify a target to which the call can be transferred. The voice application makes the request through the TXML `<QUEUE_CALL>` tag using Genesys Studio's RoutePoint Block.

## Treatments

Genesys Studio generated applications are able to process the following treatments from URS:

- Play Application
- Play Announcement
- Play Announcement and Collect Digits
- Music

## Launching of Routing Strategy on URS

The GVP voice application can launch a routing strategy on the URS by using the `RoutePoint` Block in Genesys Studio, and specifying a Route Point or Virtual Route Point in the Route DN. The routing strategy (routing script) logic controls how the call is handled.

## Call Transfer

The voice application can transfer the call by providing a phone number directly, rather than requesting the URS to provide a target. In this scenario, no data from the self-service phase is attached with the transfer. However, it can be provided to the IVR Server before issuing transfer by using User Data (Put).

The transfer can be done either through the VoiceXML `<Transfer>` tag using Genesys Studio's Transfer Block, or through the TXML `<CREATE_LEG_AND_DIAL>` tag using Studio's Connect Block.

## Whisper

The Whisper feature enables the voice application to perform a whisper on the agent leg before the caller and the agent legs are bridged. This feature is available for In-Front-of-the-Switch IPCS/VCS configurations when the voice application performs a transfer through the TXML `<CREATE_LEG_AND_DIAL>` tag with `bridge=false`.

## Detecting Operator Hang Up

This feature returns call control to the voice application after the caller has finished speaking to the agent. This feature is available for In-Front-of-the-Switch GVP configurations with bridging enabled.

## Sending Caller-Entered Data

The IVR application can send Caller-Entered Data at any time during or at the end of a call to the IVR Server through the VoiceXML<OBJECT> tag by using User Data (Put) in Genesys Studio.

## Load Balancing Between IVR Servers

This feature enables you to configure two or more IVR Servers to support the same set of IVR Server Clients. The IVR Server Client uses a round-robin methodology for distributing calls between IVR Servers.

## Invoking IVR Application Based on User Data from the IVR Server

This feature enables GVP to retrieve user data from the IVR Server when it is presented with a call. The data can be retrieved through the VoiceXML <OBJECT> tag by using Studio's User Data (Get). The IVR application determines which script to launch based on the data retrieved from the IVR Server.

This feature is useful when GVP is being used in a mode similar to Voice Treatment Option (VTO).

## Treating Missing DNIS

When no DNIS is received, IPCS/VCS contacts an application that is specifically deployed to handle the default DNIS. This is specified in `Default DNIS URL` in the IPCS/VCS configuration, under the EMPS.

## Log Server Integration

This feature enables GVP to view the IPCS/VCS generated SNMP trap log messages on the Centralized Logging system.

---

## Feature Comparison

The availability of integrated features is dependent on the type of GVP network-deployment architecture that has been implemented. Call-transfer features are dependent on the type of transfer connect. [Table 122](#) and [Table 123](#) highlights the integrated features, and their availability based on their dependencies.

**Table 122: Availability of Integrated Features**

Feature	In-Front-of-the-Switch Configuration	Behind-the-Switch Configuration
Call-Flow Type: IVR-Controlled Call Flow	Available	Available
Call-Flow Type: URS-Controlled Call Flow	Available	Available
Route Request	Available	Available
Launching of Routing Strategy at URS	Available (limited to one routing strategy per toll-free number)	Available (voice application can specify the RouteDN to launch a strategy)
Transfer of CED	Available (Route Request, Script Result, and OBJECT tag)  These features are available using Studio's RoutePoint, Script Result, and User data (Put) respectively.	Available (Route Request, Script Result, and OBJECT tag)
Call Transfer	See <a href="#">Table 123</a>	See <a href="#">Table 123</a>
Whisper	Available	Available
Operator Hang up Detect	Available	Not available
Sending Caller-Entered Data	Available	Available
Load Balancing Between IVR Servers	Available	Available
Invoking IVR Application Based on User Data From the IVR Server	Available	Available
Treating Missing DNIS	Not available	Available
Log Server Integration	Available	Available
Support for Outbound Calling	Available	Not available

**Table 122: Availability of Integrated Features (Continued)**

Feature	In-Front-of-the-Switch Configuration	Behind-the-Switch Configuration
Support for Treatments <ul style="list-style-type: none"> <li>• Music</li> <li>• Play Announcements</li> <li>• Play Announcement and Collect Digits</li> <li>• Play Application</li> </ul>	Available	Available
Re-Route	Available (Network Mode only)	Not available

**Table 123: Availability of Integrated Transfer Types**

Transfer Tag	In-Front-of-the-Switch (Bridged Transfer)	In-Front-of-the-Switch (Transfer Connect)	Behind-the-Switch
VoiceXML Transfer (bridge = true). Allows for take back of IVR control.	Available using Studio's Transfer Block	Not available	Not available
VoiceXML Transfer (bridge = false). Does not allow for take back of IVR control. Also considered blind transfer.	Available using Studio's Transfer Block	Available using Studio's Transfer Block	Available using Studio's Transfer Block
TXML CREATE_LEG_AND_DIAL (bridge = YES)	Available using Studio's Connect Block	Available using Studio's Connect Block	Available using Studio's Connect Block
TXML CREATE_LEG_AND_DIAL (bridge = NO)	Available using Studio's Connect Block	Not Available	Not Available
TXML QUEUE_CALL with AgentURL (for whisper)	Available using Studio's RoutePoint Block	Not Available	Not Available
TXML QUEUE_CALL without AgentURL	Available using Studio's RoutePoint Block	Available using Studio's RoutePoint Block	Available using Studio's RoutePoint Block



## Appendix

# E

## Reporting GVP in Framework

This appendix describes how to configure and use reporting functions. These reporting functions are useful if Universal Routing Server (URS) integrated call flows are used, and they are different from the Genesys Voice Application Reporter feature.

This appendix contains the following section:

- [Activating Reporting, page 431](#)

---

## Activating Reporting

Although Reporting templates dedicated exclusively to Genesys Voice Platform (GVP) are not yet available, you can use the Reporting templates for Enterprise Routing Solution (ERS) for your reporting needs, or you can create your own customized reports.

Genesys Voice Platform processes calls that are distributed to Directory Numbers (DNs) of the Voice Treatment Port type. If you are creating customized reports, base them on Directory Numbers (DNs) of the Voice Treatment Port type. If you decide to use the Reporting templates for ERS, keep in mind that they are mostly based on the Agent status as opposed to the DN status. The following section describes how to configure objects that represent “fake” agents and that, in fact match your actual DN, so that you can receive accurate reports for GVP. With this approach, you will be able to request statistics for Agent, GroupAgents, Place, and GroupPlaces Stat Server objects.

The configuration procedure depends on whether the Interactive Voice Response (IVR) is located behind or in front of the switch.

## With an IVR-Behind-the-Switch Configuration

To enable the collection of Reporting statistics for GVP by using default Reporting templates for ERS, open Configuration Manager and complete the following steps:

1. Under the **Switch** object for GVP, configure **Agent Login** objects. These should match the login IDs on the physical switch. IVR Server uses this information to log in agents to DNs.
2. Under the same **Switch** object, configure DNs of the **Voice Treatment Port** type. These should match DNs of the **Extension** or **Position** type that are configured on the physical switch that GVP uses.
3. Create **Place** objects. Assign **Voice Treatment Port** DNs to the **Places** by copying and pasting (or dragging and dropping) the DN objects to a **Place**.
4. Create **Place Group** objects. Assign **Places** to **Place Groups** by copying and pasting (or dragging and dropping) the **Place** objects to a **Place Group**. Keep these associations in line with your contact center layout.
5. Create an **IVR** object of any type except **Unknown**:
  - a. The value of the **IVR Name** field should be the same as the **CME IVR Client Name** specified in **IP Communication Server (IPCS)/Voice Communication Server (VCS)** configuration.
  - b. Specify a valid version of the IVR.
  - c. Use the **Browse** button to select the IVR Server application.
6. Under the **IVR** object, create **IVR Port** objects for all active IVR ports:
  - a. Use a two-digit format (such as 01) to specify a **Port Number**.
  - b. Browse for the **Associated DN**, which should be the **Voice Treatment Port DN** you created in Step 2. Make sure this association reflects the actual association between a particular number and an IVR (IVR Port) in the switch configuration, if applicable.
  - c. To enable automatic agent login at IVR Server startup, click the **Annex** tab of the **IVR Port** object and then create a section called **AutoLogin** and create the following options:
    - **AgentId**—For an option value, specify the **Agent Login** value.
    - **Queue**—For an option value, specify the number of the **Automatic Call Distribution (ACD) Queue** to which an agent logs in.
    - **SetLoggedIn**—Set the value of this option to **true**.
    - **SetReady**—Set the value of this option to **true**.

---

**Note:** If you do not create an **AutoLogin** section, manually log in a fake agent to its corresponding DN and change the agent status to **Ready** via a softphone.

---



If a number of IVR Ports are associated with the same DN, AutoLogin can be specified for only one of them. An agent must not log in to this DN more than once, either automatically or manually.

7. Create Person objects to emulate agents:
  - a. Specify fake first and last names, the employee ID, and user name.
  - b. On the General tab of the Person object's properties dialog box, select the Is Agent check box.
  - c. Click the Agent Info tab and browse for the Default Place.
  - d. Leave the Person object's Properties dialog box. In the Configuration Manager main window:
    - Find the Place that you just assigned as the Default Place for the agent and check which Voice Treatment Port DN is assigned to this Place.
    - Find the IVR Port which is associated with this DN.
  - e. Go back to the Agent Info tab of the Person object's dialog box, and associate the agent with one of the created Agent Logins. Select the same Agent Login as you have specified for AutoLogin on the IVR Port associated with the Voice Treatment Port DN assigned to the Default Place for this Agent.
8. Create Agent Group objects. Assign agents to Agent Groups by copying and pasting (or dragging and dropping) the Person objects to an Agent Group. Keep these associations in line with your contact center layout.

## With an IVR-In-Front-of-the-Switch Configuration

Follow the same configuration procedure as with the IVR-Behind-the-Switch configuration, but create "fake" Agent Logins instead of using the real ones. With the IVR-In-Front-of-the-Switch configuration, there is no match to login IDs on the physical switch.

Also, the association between an IVR Port and a DN of the Voice Treatment Port type reflects the actual association between a particular number and an IVR (IVR Port) on the Service Provider's Public Switched Telephone Network (PSTN) configuration, if applicable.





## Appendix

# F

## System Prompts

This appendix describes how to create and install Alaw system prompts.

It contains the following sections:

- [Overview, page 435](#)
- [Creating ALaw System Prompts, page 435](#)
- [Installing ALaw System Prompts, page 436](#)

---

### Overview

Genesys Voice Platform (GVP) provides default system prompts for errors that might occur in the Voice Extensible Markup Language (VoiceXML) applications, or in the platform itself. GVP provides Mulaw as the default format, which is suitable for users in North America. For users in other countries, the Alaw format is necessary.

---

Note: The IP Communication Server (IPCS)/Voice Communication Server (VCS) supports only Mulaw/Alaw PCM files as prompts (raw or WAV).

---

---

### Creating ALaw System Prompts

To create Alaw system prompts, proceed as follows:

1. Create Alaw prompts with the same file names as the default (Mulaw) system prompts.
2. Translate the content of the default system prompts into the language that you require.

[Table 124](#) lists the system prompts that you must record in Alaw format

**Table 124: System Prompts**

<b>Vox File (8 KHz Alaw)</b>	<b>Prompt Content</b>	<b>Error</b>
BadFetchError.vox	Sorry. You have got a bad fetch error. Exiting.	error.badfetch
NoAuthorizationError.vox	Sorry. No Authorization error. Exiting.	error.noauthorization
SemanticError.vox	Sorry. You have got a semantic error. Exiting.	error.semantic
UnsupportedAudioFormatError.vox	Sorry. The specified audio format is not supported. Exiting.	error.unsupported.format
UnsupportedLangError.vox	Sorry. The specified language is not supported. Exiting.	error.unsupported.language
Error.vox	Sorry. You have got an error. Exiting.	error
SpokeTooEarly.vox	Sorry. Could you please repeat? You spoke too early.	nomatch.com.telera.speechtooeearly
NoMatch.vox	Sorry. I did not understand.	nomatch
NoInput.vox	Sorry. I did not hear you.	noinput
Help.vox	Sorry. There is no help provided.	help
MaxSpeechTimeout.vox	Sorry. The speech input is too long.	maxspeechtimeout
NoCatchHandler.vox	Sorry. There is no catch handler provided. Exiting.	All other errors

## Installing ALaw System Prompts

To install alaw system prompts, proceed as follows:

1. On the IPCS/VCS, copy your newly created vox files to the `<InstallDir>\cn\web\VXMLRoot\VoxFiles\en-US\` directory. As a convenience, a copy of the alaw default system prompts are provided at `<InstallDir>\cn\web\VXMLRoot\VoxFiles\en-US\alaw`.

---

Note: These default alaw prompts are in US English. The Alaw prompts provided may not be suitable for deployment if a non-US version of English is desired.

---

2. If your system prompts are in a language other than U.S. English, create a language-specific folder under `VoxFiles\` - for example, `es-MX`. Copy the foreign-language system prompts to the new folder.
3. GVP automatically points to `<InstallDir>\cn\web\VMLRoot\VoxFiles\<language>`, and the language is provided when the application is provisioned.





## Appendix

# G

## Scaling EventC

This appendix describes how to scale EventC up to three boxes, to increase handling capacity. It contains the following sections:

- [EventC Subsystem Components, page 439](#)
- [Deployment Considerations, page 440](#)
- [Database Considerations, page 442](#)
- [Installing EventC on Multiple Boxes, page 444](#)

---

## EventC Subsystem Components

An EventC subsystem consists of two sets of component processes and databases:

- Single-instance set—A GVP deployment can have only one instance of the set of components.
- Multi-instance set—A GVP deployment can have multiple instances of the set of components.

[Table 125](#) describes the EventC components.

**Table 125: EventC Subsystem Components**

Category	EventC Component	Description
Single-instance set	PeaksNSP process	Calculates call volume peak for selected time periods (hours, days, weeks).
	Peaks database	Stores peaks control and work-in-progress information.
	Reporter database	Stores summary, peaks, and call details for reporting.
	RepDWH database	Stores Call Detail Records (CDRs) for billing.

**Table 125: EventC Subsystem Components (Continued)**

Category	EventC Component	Description
Multi-instance set	Billing URL	Point of contact to which the IP Communication Server (IPCS) or Voice Communication Server (VCS) sends events.
	Events Loader process	Stores events in the database.
	Call Records Generator process	Generates billing and reporting information.
	EventC Manager process	Cleans up the databases and resets peaks.
	Collector database	Work-in-progress database used by the Events Loader, Call Records Generator, and EventC Manager processes.

## Deployment Considerations

You can distribute an EventC subsystem over multiple physical servers. The following rules apply:

- The multi-instance set is scalable as a group only and not as individual components. For example, you can deploy two sets of the scalable components (so that your deployment includes two Collector databases, two Events Loader processes, and so on), but you cannot deploy one Collector database, two Events Loaders, three Call Records Generators, and so on.
- There can be only one instance of each single-instance component in a deployment. However, the individual components can be distributed across multiple servers.
- Each physical server (box) can have only one instance of the multi-instance set. Additional, single-instance components can co-reside on the same server. For example, a box can have one billing URL, one Events Loader, one Call Records Generator, one EventC Manager, and one Collector database.
- Each multi-instance set should have its own Collector database. The database is not sharable across sets.
- To divide the call processing load among multiple sets, set the billing URL of individual VCSs/IPCSs to point to different EventC servers. Ensure that you split the load equally. For example, if you have ten IPCS/VCS boxes and two multi-instance sets, point five IPCS/VCS boxes to one set and the remaining five IPCS/VCS boxes to the other set.



## Deployment Scenarios

Table 126 shows sample deployments for scaling EventC.

Note: Genesys does not support scaling beyond three boxes or handling more than 200,000 calls per hour.

**Table 126: Sample EventC Deployments**

EventC Server	EventC Component		IPCS/VCS Load	Capacity	
	Processes	Databases		Peak Traffic (calls/hr)	Call Volume (calls/day)*
One-Box Solution					
Eventc_one	BillingURL EventsLoader EventC Manager CallRecsGenerator PeaksNSP	Collector Peaks Reporter RepDWH	100%	100,000	1 million
Two-Box Solution					
Eventc_one	BillingURL(1) EventsLoader(1) EventC Manager(1) CallRecsGenerator(1) PeaksNSP	Collector(1) Peaks	50%	150,000	1.5 million
Eventc_two	BillingURL(2) EventsLoader(2) EventC Manager(2) CallRecsGenerator(2)	Collector(2) Reporter RepDWH	50%		
*The traffic pattern is assumed to be a bell curve, with peak volumes at midday and low traffic during off-peak hours.					

**Table 126: Sample EventC Deployments (Continued)**

EventC Server	EventC Component		IPCS/VCS Load	Capacity	
	Processes	Databases		Peak Traffic (calls/hr)	Call Volume (calls/day)*
Three-Box Solution					
Eventc_one	BillingURL(1) EventsLoader(1) EventC Manager(1) CallRecsGenerator(1) PeaksNSP	Collector(1) Peaks	30%	200,000	2 million
Eventc_two	BillingURL(2) EventsLoader(2) EventC Manager(2) CallRecsGenerator(2)	Collector(2) RepDWH	35%		
Eventc_three	BillingURL(3) EventsLoader(3) EventC Manager(3) CallRecsGenerator(3)	Collector(3) Reporter	35%		
*The traffic pattern is assumed to be a bell curve, with peak volumes at midday and low traffic during off-peak hours.					

## Database Considerations

Input/Output (I/O) configuration is critical, because EventC operations require a huge volume of database inserts, updates, and deletions.

The following hardware and network planning recommendations supplement information in the *Genesys Hardware Sizing Guide*.

## Hardware Recommendations

Genesys recommends the following hardware specifications for the EventC servers:

- Dual CPU with minimum 3 GHz processor speed
- At least 2 GB of memory

- Hard disks: SCSI 15,000 RPM

Genesys recommends that you have as many physical disks as the number of databases on the EventC server. If you have both Collector and Peaks on a server, have two physical drives (for example, C: and D:). This recommendation does not refer to RAID and logical partitioning. The reason for multiple disk drives is to increase the amount of parallel I/O.

- Individual disk controllers for each disk, to further improve parallel I/O.
- Two NIC cards for each server. Use one card to connect to the general network, and the other card to connect the EventC servers in an exclusive network.

When you configure the SQL Server clients, use the IP address of the second card, to ensure that all SQL traffic goes through the exclusive network. Because SQL traffic can have sudden bursts, separating SQL traffic from regular IP traffic helps overall performance.

## Database Sizing and Configuration

The following EventC considerations and recommendations for EventC supplement information in the *Genesys Hardware Sizing Guide*.

[Table 127](#) provides sizing estimates for the EventC databases. In addition to the requirements that are estimated in [Table 127](#), also consider:

- The disk space required by the operating system and other software
- Buffer disk space (approximately 30% more) to handle spikes

**Table 127: EventC Databases**

Database	Size per Call	Size per Day*	Database Capacity (for typical archival duration)
Collector	10 KB	10 GB	150 GB for 15 days
Peaks	< 1 KB	5 GB	5 GB
RepDWH	1 KB	1 GB	45 GB for 45 days
Reporter	1 KB	1 GB	90 GB for 90 days
CDR Files	2 KB	2 GB	14 GB for 7 days
*Assumes 1 million calls/day.			

## Microsoft SQL Recommendations

Genesys has the following additional recommendations for Microsoft SQL Server configuration and setup:

- Consider your requirements for scalability, performance, high availability and manageability features. Your plans in connection with these features will determine whether you require Microsoft SQL Server 2000 or Microsoft SQL Server 2005.
- Consider your requirements for redundancy, load balancing, backup, recovery, replication, and so on. Your plans in connection with these features will determine whether you require the Standard Edition or the Enterprise Edition of the Microsoft SQL Server software.
- Use Device CAL licenses for Microsoft SQL Server. When you calculate the number of devices that access a database server, consider non-EventC components (such as EMPS and Reporter) as well as the number of multi-instance EventC components that would access a single-instance component.
- Set Microsoft SQL Server memory consumption so that it does not use more than half the memory available on the host. Do this through SQL Enterprise Manager, with the assistance of your DBA.
- When you create the databases, distribute them on multiple physical disks. Genesys recommends one database on each disk, to increase parallel I/O.
- Distribute the transaction log to a dedicated disk that is not being used by the data files.
- Have a dedicated SCSI drive for each hard disk, because this enables parallel writes.

---

## Installing EventC on Multiple Boxes

The following procedure describes the steps to install and configure EventC on up to three boxes.

### Installing and Configuring EventC on Multiple Boxes

For a three-box solution, install three instances of the Collector database (one on each box) for load balancing, and a single instance of the Peaks, Reporter, and RepDWH databases for the entire solution. Each process points to its local Collector database.

For the boxes that do not host a specific server (for example, the boxes that do not host the PeaksNSP process), delete the EMPS node for that process for the host.

1. Install the complete EventC software on each server. For more information, see the *Genesys Voice Platform 7.6 Deployment Guide*.
2. On each server, create and set up the databases that are required on that server. For more information, see the *Genesys Voice Platform 7.6 Deployment Guide*.
3. Configure EventC in the EMPS.  
Ensure that each EventC subsystem process points to the Collector database that is on the same server as the process itself. In the case of the other databases, because there is only one instance of each of them, all components will point to the same instance.
4. Restrict which EventC processes run on each server:
  - a. On the EMPS navigation tree, expand the nodes Servers > Events Collector > <ServerName>.
  - b. Select the node for the process that you do not want to run. (Typically, this is the PeaksNSP process on servers on which you do not want the peaks calculator to run.)
  - c. Delete the node.
  - d. Verify that the process does not start on the box.
5. Disable the Peaks process on the EventC server(s) that you do not want to run Peaks. For more information, see the *Genesys Voice Platform 7.6 Deployment Guide*.





## Appendix

# H

## IP Call Manager High Availability

This appendix describes the high availability for IP Call Manager (IPCM). It contains the following sections:

- [Call Manager—SIP, page 447](#)
- [Call Manager—H.323, page 448](#)
- [Deployment Methods, page 449](#)
- [High Availability Using Microsoft Cluster Service, page 453](#)

---

### Call Manager—SIP

The IP Session Initiation Protocol (SIP) Call Manager is an intelligent, call-stateful SIP proxy that coordinates between various SIP elements participating in the Genesys Voice Platform (GVP) application.

### Components

The IP SIP Call Manager consists of a set of components that coordinates and assigns the resources needed for a call.

The key components in the IP SIP Call Manager are:

- **SIP Session Manager (SSM)**—The SSM process acts as a SIP proxy to relay SIP messages between a Media Gateway or Signaling Gateway, and IP Communication Servers.
- **Resource Manager (RM)**—The RM process maintains resource states for IP Communication Server and Media Gateway, or Signaling Gateway resources.

- Arbitrator—The arbitrator process uses transmission control protocol (TCP) and performs the following tasks:
  - Spawning its local real-time relational database (RTRDB) process.
  - Monitoring database process through heartbeat mechanism.
  - Controlling the operation mode (standby or master) of the database process.
  - Ensuring only one database is master.
  - Instructing a standby database to run as master in the event of failure of the current master.
  - Heartbeat mechanism with other arbitrator processes.

---

## Call Manager—H.323

The IP H.323 Call Manager is an intelligent, call-stateful H.323 proxy that coordinates between various H.323 elements participating in the GVP application.

### Components

The IP H.323 Call Manager consists of a set of components that coordinates and assigns the resources needed for a call.

The key components in the IP H.323 Call Manager are:

- H.323 Session Manager (HSM)—HSM acts as a H.323 Proxy to relay H.323 messages between a Media Gateway or Signaling Gateway, and SIP messages between IP Communication Servers (IPCS).

---

Note: The HSM process does not interact with the database and the call information is stored in-memory only.

---

- Resource Manager (RM)—The Resource Manager process maintains the resource state for IPCS and the Media Gateway, or Signaling Gateway resources. The RM communicates with the database.

---

Note: If an H.323 gatekeeper is present in the network, the Media Gateway resources are not managed by IPCM.

---

- Arbitrator (ARB)—The arbitrator process uses TCP protocol and performs the following tasks:
  - Spawning its local RTRDB database process.
  - Monitoring database process through heartbeat mechanism.
  - Controlling the operation mode (standby or master) of the database process.
  - Ensuring only one database is master.



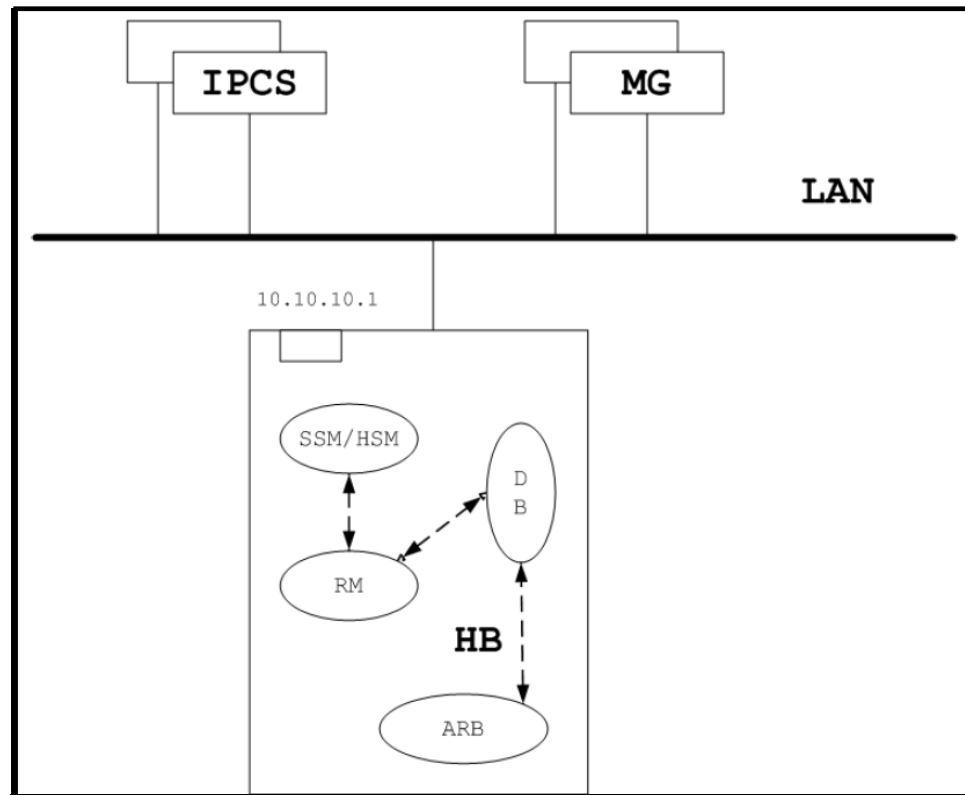
- Instructing a standby database to run as master in the event of failure of the current master.
- Heartbeat mechanism with other arbitrator process.

## Deployment Methods

This section describes different configurations for IPCM deployment. The configuration varies in the level of fault tolerance provided. The advantages, disadvantages, and features of each configuration are listed.

### Single IPCM

This setup consists of a single IPCM server. This server uses an in-memory database, RTRDB, which is provided by a third-party vendor (Polyhedra Ltd.), and an arbitration mechanism to control the database (see [Figure 139](#)).



**Figure 139: Single IPCM**

#### Advantages

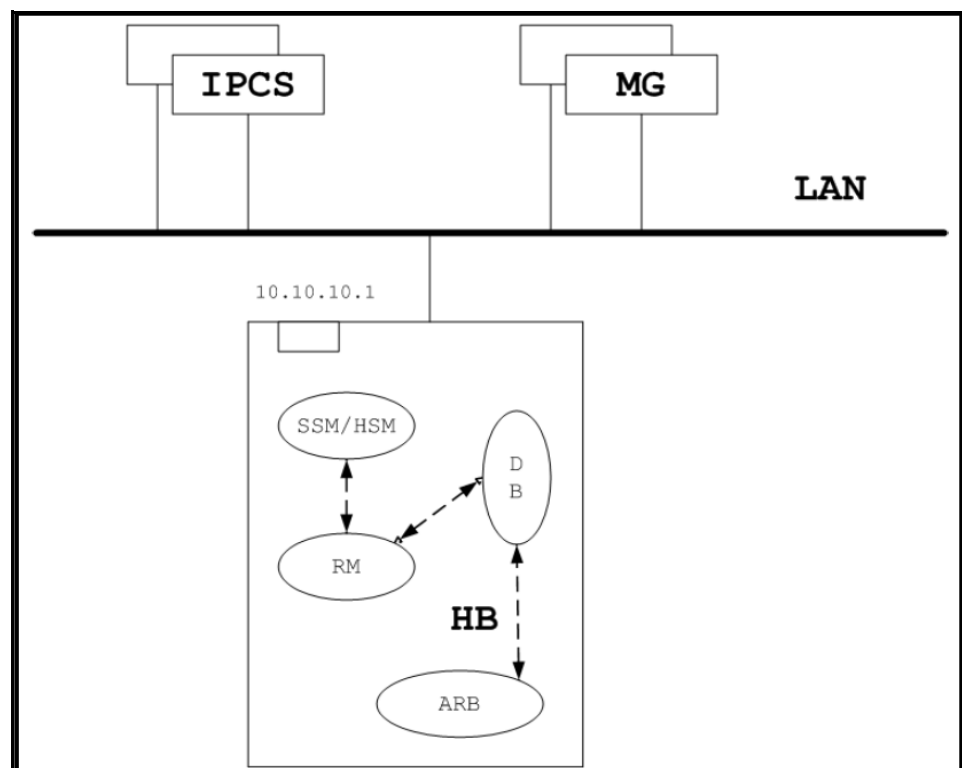
- The customer can buy less equipment.
- Quick to install.
- Simple to maintain.

### Disadvantages

This mode of deployment would result in a single-point-of-failure. When IPCM stops functioning, either because of software or hardware failure, calls cannot be routed from, or to the IPCS.

## Dual IPCMs with Redundancy

This setup consists of two IPCM servers that run in the ACTIVE/Hot-Standby mode. To achieve High Availability (HA), the IPCM HA uses a primary-secondary server configuration, a dual redundant in-memory database system (RTRDB), and an arbitrator to exchange heartbeats and switch between databases (see [Figure 140](#)).



**Figure 140: Dual IPCM**

### Advantages

- When the primary IPCM stops functioning, either because of software or hardware failure, the IPCS and other SIP devices within the GVP network can contact the backup IPCM. The backup IPCM will only handle new calls, not existing calls. In this scenario, you must configure the IPCS (and other SIP elements) with the IP addresses of both IPCM servers.
- When there is a communication failure between the IPCS and the primary IPCM, new call requests can still be sent to the backup IPCM.

- When the primary RTRDB (database) server stops functioning, the backup RTRDB server will become primary and will continue to handle requests to the database. The call handling is not affected.

### Additional Configuration—SIP

In order to enable redundancy between the two IPCM servers, certain parameters have to be configured through the Element Management Provisioning System (EMPS) server. The additional steps required to enable redundancy between the IPCMs are provided below. Before configuring these parameters, both IPCMs must be configured individually, capable of performing in the Simplex mode.

1. Using a web browser, connect to the uniform resource locator (URL) `http://<EMPS>:9810/prov`.
2. Log into EMPS, and then click Servers from the top menu.
3. Expand the node SSM and select the primary IPCM.
4. Click Arbitrator and then click Edit Node. Set the appropriate values for the following attributes.  
Backup Database Address: <Backup IPCM IP Address>  
Save the configuration.
5. In the left pane, click SIPSessionManager, and then click Edit Node. Set the appropriate values for the following attributes.  
Backup database IP address and port: <Backup IPCM IP address>:16500  
Save the configuration.
6. In the left pane, click ResourceManager, and then click Edit Node. Set the appropriate values for the following attributes.  
Backup database IP address and port: <Backup IPCM IP address>:16500  
Save the configuration.
7. Expand SIP Session Manager, and then select the backup IPCM.
8. Click Arbitrator and then click Edit Node. Set the appropriate values for the following attributes.  
Backup Database Address: <Primary IPCM IP Address>  
Save the configuration.
9. In the left pane, click SipSessionManager, and then click Edit Node. Set the appropriate values for the following attributes.  
Backup database IP address and port: <Primary IPCM IP address>:16500  
Save the configuration.
10. In the left pane, click ResourceManager, and then click Edit Node. Set the appropriate values for the following attributes.  
Backup database IP address and port: <Primary IPCM IP address>:16500  
Save the configuration.

## 11. Start the IPCM WatchDog.

### Additional Configuration—H.323

In order to enable redundancy between the two IPCM servers, certain parameters have to be configured through the EMPS server. The additional steps required to enable redundancy between the IPCMs are provided below. Before configuring these parameters, both IPCMs must be configured individually, capable of performing in the Simplex mode.

1. Using a web browser, connect to the URL `http://<EMPS>:9810/prov`.
2. Log into EMPS, and then click **Servers** from the top menu.
3. Expand the node **H323 Session Manager** and select the primary IPCM.
4. Click **Arbitrator** and then click **Edit Node**. Set the appropriate values for the following attributes.  
Backup Database Address: `<Backup IPCM IP Address>`  
Save the configuration.
5. In the left pane, click **ResourceManager**, and then click **Edit Node**. Set the appropriate values for the following attributes.  
Backup database IP address and port: `<Backup IPCM IP address>:16500`  
Save the configuration.
6. Expand **H323 Session Manager**, and then select the backup IPCM.
7. Click **Arbitrator** and then click **Edit Node**. Set the appropriate values for the following attributes.  
Backup Database Address: `<Primary IPCM IP Address>`  
Save the configuration.
8. In the left pane, click **ResourceManager**, and then click **Edit Node**. Set the appropriate values for the following attributes.  
Backup database IP address and port: `<Primary IPCM IP address>:16500`  
Save the configuration.
9. Start the IPCM WatchDog.

## Recommended Deployment

Genesys recommends the Dual IPCMs with redundancy mode of deployment. The customer does have the option of choosing between single IPCM and Dual IPCMs, depending on the desired level of redundancy.

---

# High Availability Using Microsoft Cluster Service

---

Notes: IPCM High Availability using Microsoft Cluster Service (MSCS) is applicable on Windows only.

IPCM High Availability using MSCS is supported for SIP only (not H.323).

---

Currently, IPCM can operate in a dual IPCM architecture. This means that when both servers are active, there is ongoing replication between the two servers. If one of the IPCM servers fails, new calls will be processed successfully by the active IPCM server; however, existing calls will not be handled because SIP communication is through the physical IP address of the IPCMs.

By using Microsoft Cluster Service (MSCS), the IPCM pair can operate in an Active/Hot Standby mode. This is achieved by having all SIP communication go through a virtual IP address, common to both IPCMs. If failure of one of the IPCMs occurs, the existing calls will be constructed from the replicated data and all SIP communication continues on the virtual IP.

## Deployment Architecture

In order to make the IPCMs Highly Available, a virtual IP address handles all SIP communication. Only one IPCM possesses the virtual IP address at any time. The Windows Clustering Software controls the possession of the virtual IP address by either server. All SIP entities (such as Media Gateways, Soft Switches, and IPCSs) are aware of only the virtual IP address and not the physical IP addresses of the two IPCMs.

---

Note: The virtual IP must be hosted on the same physical Ethernet Interface as the physical IP, and must be on the same subnet as the physical IP.

---

All SIP communication is directed toward the virtual IP; however, database replication and heartbeat exchange between the two IPCMs is through the physical IP addresses. The database is replicated using the primary Network Interface Card (NIC), so a secondary NIC is not necessary for either IPCM. Figure 141 on [page 454](#) illustrates the deployment architecture.

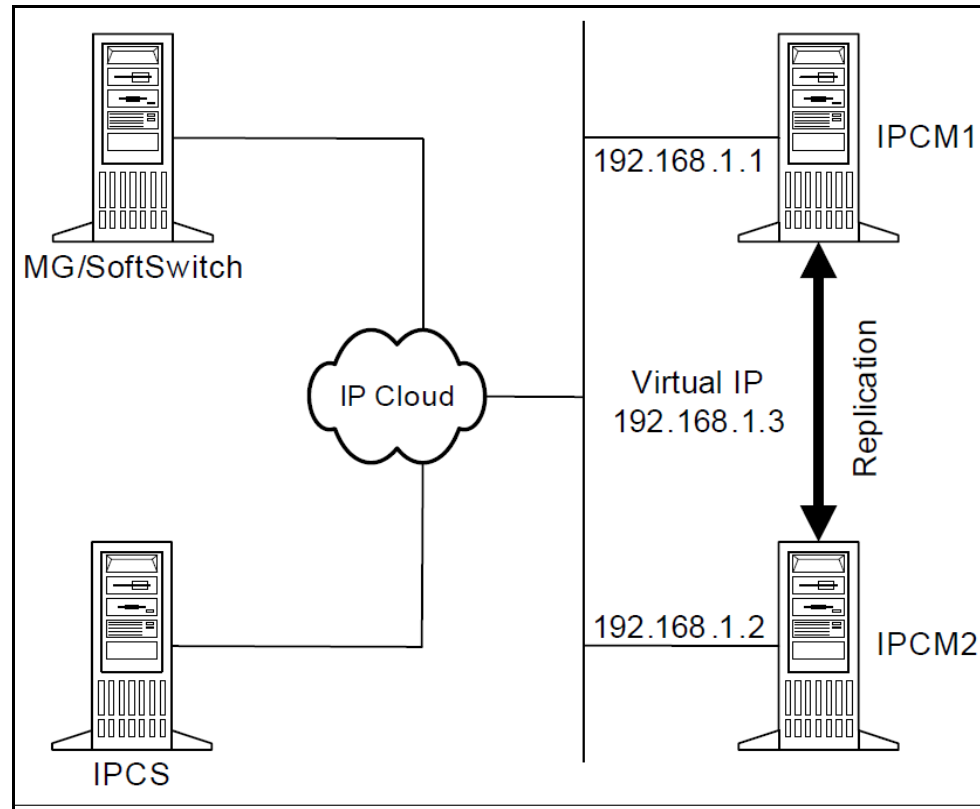


Figure 141: IPCM HA using MSCS

## Windows Clustering—Quorum Options

A quorum is a configuration database for MSCS, and it is stored in the quorum log file. While configuring the Windows Cluster Manager, based on available hardware and network constraints, you must select one of the following quorum policies:

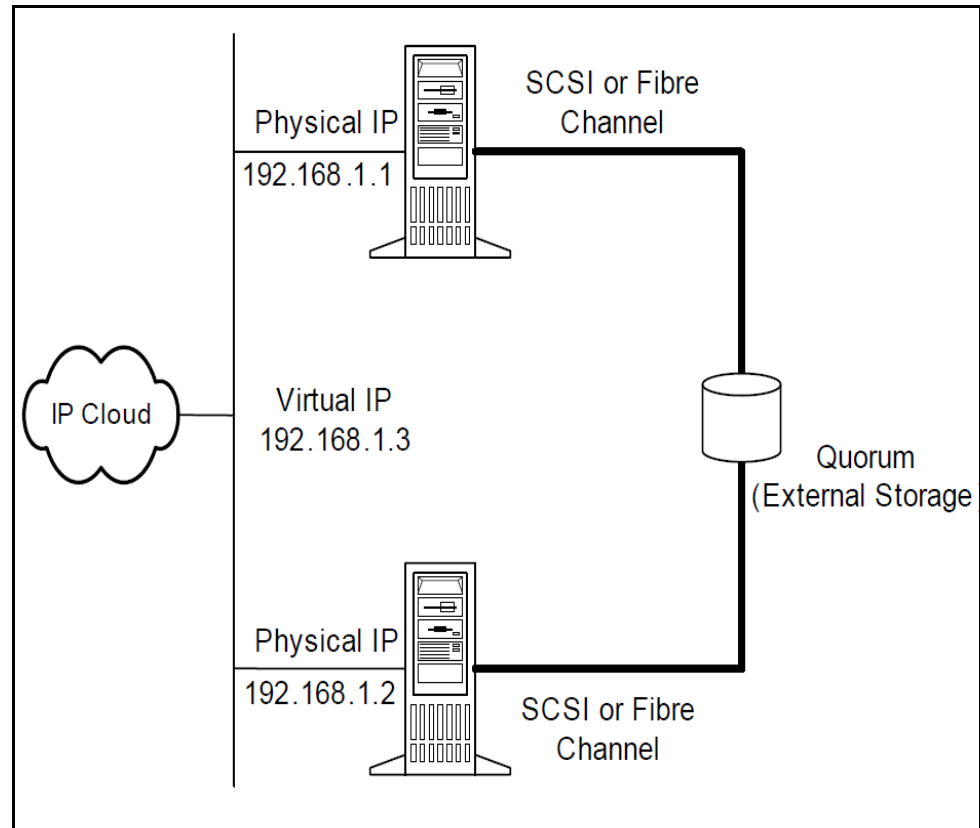
- Standard Quorum
- Majority Node Set

### Standard Quorum

A standard quorum uses a quorum log file that is located on a disk hosted on a shared storage interconnect that is accessible by all members of the cluster. Standard quorums are available on:

- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Datacenter Edition

Figure 142 illustrates an example of a standard quorum in a two-node cluster.



**Figure 142: Standard quorum in a two node cluster**

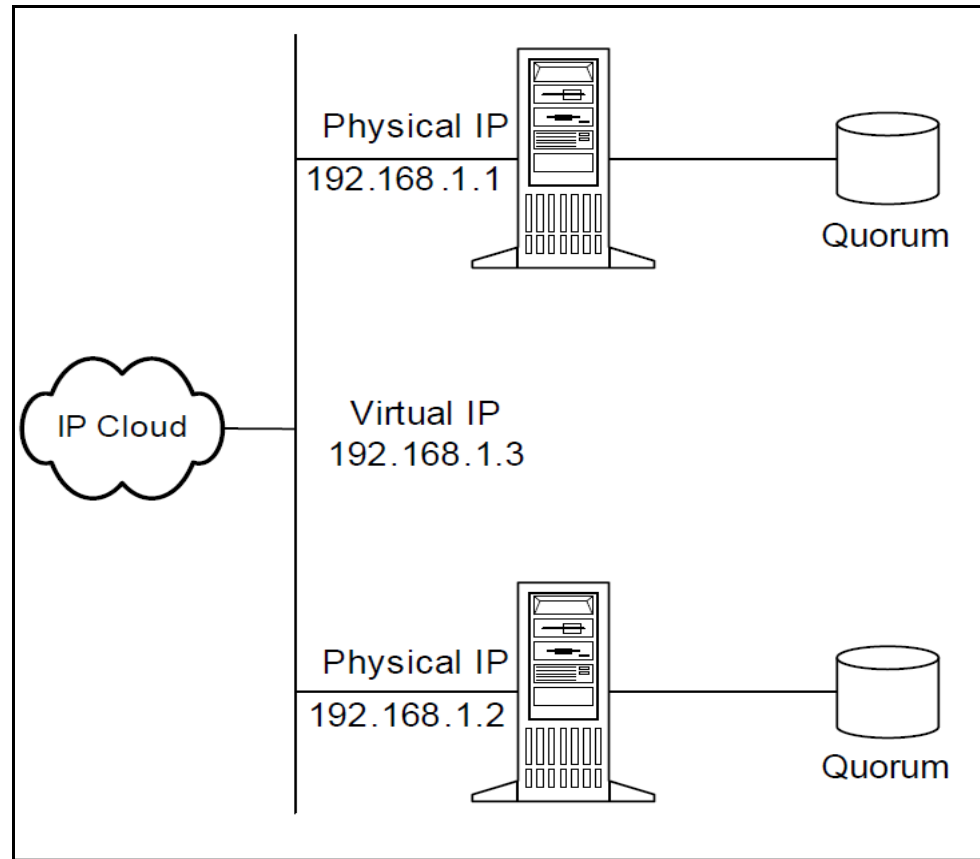
**Note:** Based on input from Microsoft Technical Support, ungraceful failover duration can be approximately ten seconds when using this quorum configuration. An ungraceful failover is an event in which the active cluster (for example, IPCM1) fails without notifying the other server (for example, IPCM2). The failover duration is defined as the time between one server becoming unavailable and the other server becoming active.

## Majority Node Set

A Majority Node Set (MNS) quorum is a single quorum resource from a server cluster perspective; however, the data is actually stored by default on the system disk of each member of the cluster. The MNS resource ensures that the cluster configuration data stored on the MNS is consistent across the different disks. MNS quorums are available on:

- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Datacenter Edition

Figure 143 illustrates an example of an MNS quorum in a two-node cluster.



**Figure 143: MNS quorum in a two node cluster**

Note: Based on input from Microsoft Technical Support, ungraceful failover duration can be between two and seven minutes when using this quorum configuration.

## Recommended Deployment

Due to the significant difference in failover duration between a standard quorum and a MNS quorum, Genesys recommends that you use the standard quorum option while configuring Windows Cluster for IPCM functionality.

## Restart Policy

The GVP attribute `MonitorProcess` supports Windows Clustering. You can add this attribute through EMPS. When you add this attribute to any component with a value set to 0 (zero), WatchDog will not restart that component if the



process hangs or terminates. If High Availability through Windows Clustering is desired for IPCM, you must set this attribute to 0 for both SSM and RM. MSCS controls the SSM and RM restart policy.

## SSM Processing

The SSM processes mid-call SIP requests in the case of a failure. If a failure occurs, the backup SSM processes these mid-call requests for calls that have already been established. The following SIP requests are handled during mid-call failover:

- REINVITE
- INFO
- REFER
- NOTIFY
- BYE

## Configuring IPCM

This section describes how to configure your IPCMs through EMPS.

### Primary IPCM

1. Using a web browser, connect to the URL `http://<EMPS>:9810/prov`.
2. Log into EMPS, and then click Servers from the top menu.
3. Expand the node SIP Session Manager and select the primary IPCM.
4. Click Arbitrator, and then click Edit Node.
5. Set the Backup Database Address attribute to the physical IP address of the backup IPCM.
6. Click Submit.
7. In the left pane, click SipSessionManager, and then click Edit Node. Set the appropriate values for the attributes shown in [Table 128](#).

**Table 128: SIP Session Manager Attributes**

Parameter	Value
Primary database IP address and port	<Primary IPCM Physical IP address>:16500
Backup database IP address and port	<Backup IPCM Physical IP address>:16500

**Table 128: SIP Session Manager Attributes (Continued)**

Parameter	Value
SIP Listening IP Address	<Virtual IP Address>
Resource Manager IP Address and Port	<Virtual IP Address>:5070

8. Click Add New Attribute twice, and then add the new attributes and parameters shown in [Table 129](#).

**Table 129: New Attributes**

Parameter	Value
NodeType	1
MonitorProcess	0

9. Click Submit.
10. In the left pane, click ResourceManager, and then click Edit Node. Set the appropriate values for the attributes shown in [Table 130](#).

**Table 130: Resource Manager Attributes**

Parameter	Value
Primary Database IP Address and Port	<Primary IPCM Physical IP Address>:16500
Backup Database IP Address and Port	<Backup IPCM Physical IP Address>:16500
SIP Listening IP Address	<Virtual IP Address>

11. Click Add New Attribute twice, and then add the new attributes and parameters shown in [Table 131](#).

**Table 131: New Attributes**

Parameter	Value
NodeType	1
MonitorProcess	0

12. Click Submit.

## Backup IPCM

1. Using a web browser, connect to the URL `http://<EMPS>:9810/prov`.
2. Log into EMPS, and then click Servers from the top menu.
3. Expand the node SIP Session Manager and select the backup IPCM.
4. Click Arbitrator, and then click Edit Node.
5. Set the Backup Database Address attribute to the physical IP address of the primary IPCM.
6. Click Submit.
7. In the left pane, click SipSessionManager, and then click Edit Node. Set the appropriate values for the attributes shown in [Table 132](#).

**Table 132: SIP Session Manager Attributes**

Parameter	Value
Primary Database IP Address and Port	<Backup IPCM Physical IP address>:16500
Backup Database IP Address and Port	<Primary IPCM Physical IP address>:16500
SIP Listening IP Address	<Virtual IP Address>
Resource Manager IP Address and Port	<Virtual IP Address>:5070

8. Click Add New Attribute twice, and then add the new attributes and parameters shown in [Table 133](#).

**Table 133: New Attributes**

Parameter	Value
NodeType	1
MonitorProcess	0

9. Click Submit.
10. In the left pane, click ResourceManager, and then click Edit Node. Set the appropriate values for the attributes shown in [Table 134](#).

**Table 134: Resource Manager Attributes**

Parameter	Value
Primary Database IP Address and Port	<Backup IPCM Physical IP Address>: 16500
Backup Database IP Address and Port	<Primary IPCM Physical IP Address>: 16500
SIP Listening IP Address	<Virtual IP Address>

11. Click Add New Attribute twice, and then add the new attributes and parameters shown in [Table 135](#).

**Table 135: New Attributes**

Parameter	Value
NodeType	1
MonitorProcess	0

12. Click Submit.

## Configuring MSCS for Use with IPCM

This section describes how to configure MSCS through the MSCS Cluster Administrator.

When enabling the high availability feature for GVP IPCM, the MSCS Cluster Administrator must be used to create the appropriate Cluster Nodes for IPCM.

The following information provides details about several of the key configuration steps required during the installation procedure of MSCS.

---

**Note:** This is not a complete step-by-step guide to configure the cluster. Please consult the MSCS installation procedures for step-by-step instructions.

---

1. When starting the MSCS Cluster Administrator to create the appropriate Cluster Nodes for IPCM, select the Advanced (minimum) configuration option.
2. On the Add Nodes Wizard screen, log in using a domain account as the cluster service account.

---

**Note:** This account information will be used for both adding nodes and configuring some of the IPCM components in the MSCS.

---

3. Once the appropriate login information for the cluster administrator has been entered, create an IPCS group.
4. On the New Resource screen, create a Resource Manager resource, and add the following resources as shown in [Table 136](#).

**Table 136: Resource Manager resource parameters**

Parameter	Value
Name	RM
Description	Resource Manager
Resource type	Generic Application
Group	IPCM

---

Note: Do *not* select the check box labeled Run this resource in a separate Resource Monitor.

---

5. On the Generic Application Parameters screen for the Resource Manager resource, add the following parameters as shown in [Table 137](#):

**Table 137: Generic Application parameters**

Parameter	Value
Command line	Specify the absolute path of the RM executable, and the absolute path of the configuration parameter file for RM.
Current directory	Specify the directory where the GVP binaries are located.

6. On the New Resource screen, create a SIP Session Manager resource, and add the following resources as shown in [Table 138](#):

**Table 138: SIP Session Manager resource parameters**

Parameter	Value
Name	SSM
Description	SIP Session Manager
Resource type	Generic Application
Group	IPCM

---

Note: Do *not* select the check box labeled Run this resource in a separate Resource Monitor.

---

On the Generic Application Parameters screen for the SIP Session Manager resource, add the following parameters as shown in [Table 139](#):

**Table 139: Generic Application parameters**

Parameter	Value
Command line	Specify the absolute path of the SSM executable, and the absolute path of the configuration parameter file for SSM.
Current directory	Specify the directory where the GVP binaries are located.

7. The group properties for the IPCM group must be modified. On the IPCM Properties screen, under the tab labeled Fail over, ensure:
  - Threshold = 1
  - Period = 0.
8. On the IPCM Properties screen, under the tab labeled Fail back, ensure that the Prevent fail back option is selected.
9. On the RM Properties screen, under the tab labeled Advanced, ensure that the Restart option is selected, and specify the following parameters as shown in [Table 140](#):

**Table 140: RM parameters**

Parameter	Value
Threshold	0
Period	10
Looks Alive	10 (milliseconds)
Is Alive	60 (milliseconds)
Pending timeout	10 (seconds)

10. On the IPCM Properties screen, under the tab labeled Fail back, ensure that the Prevent failback option is selected.
11. On the Cluster Service Properties (Local Computer) screen, add Watchdog as a dependent service to the cluster service.

12. On the ResourceMgr screen, using dcomcnfg (under Component Services -> My Computer -> DCOM Config -> <component>), set the account information of the ResourceMgr component to the account that was used to create the cluster.
13. On the SIPSessionMgr screen, using dcomcnfg (under Component Services -> My Computer -> DCOM Config -> <component>), set the account information of the SIPSessionMgr component to the account that was used to create the cluster.







# Index

## A

adding	
ASR vendor	77
attribute to child node	72
cachebox to EMPS	73
DID group	83
new attributes	72
new media streams	273
reseller	32
server group	82
task	77
TTS vendor	76
advanced options	125
Alaw system prompts	
creating	435
installing	436
app_currpeaks	385
app_peaks	395
application, OBN	294
appoutbound.xml file	71
appoutbounddid.xml file	71
ASR Log Manager	133
ASR vendor, adding	77
asr_currpeaks	386
asr_peaks	398
ASR, provisioning IVR profile	57
assigned option, using	65
associate roles	129
ATT Conference OOB transfer	344
ATT Conference transfer	344, 346
ATT Consultative OOB transfer	344
ATT Consultative transfer	344, 346
ATT Courtesy OOB transfer	344
ATT Courtesy transfer	344, 346
ATT OOB transfer	357
audience	
defining	15
audit file, BPT	101

## B

Bandwidth Manager	155
customer orders	158
customer summary	156
provisioning IVR profile	53
summary	155
behind-the-switch	41
billcallrecords	402
billing	375
billing data file	406
blind call transfer, empty capability set	365, 369
blind transfer, Dialogic	345
BPT	93, 109
accessing	94, 110
audit file	101
bulk operations	95
canceling bulk task	100
configuration file	102
creating new IVR profile	97
csv mapping	102
log file	101
log window	99
progress bar	99
regenerating DID group	98
bridge transfer	345, 346
bridge transfer, IPCS	351
bridging calls, H.323	281
bulk operations	95
Bulk Provisioning Tool	
See BPT	
bulk request, trigger application	296
bulk task, canceling	100

## C

cachebox, adding	73
Call Control Adapter	
See CCA	
call data records	375
call details report	136

- call events . . . . . 377, 381
- call events excp . . . . . 381
- Call Flow Assistant . . . . . 179, 217
  - active sessions . . . . . 180, 218
  - statistics . . . . . 179, 217
- call flow types . . . . . 426
- call flow, IVR controlled . . . . . 426
- call flow, URS controlled . . . . . 426
- call hold support . . . . . 270
  - bridged call . . . . . 271
  - IVR state . . . . . 270
  - sample SIP call flow . . . . . 271
- call off hold . . . . . 272
- call phases . . . . . 401
- call progress analysis
  - See CPA
- call progress detection
  - See CPD
- call records . . . . . 390
- Call Status Monitor . . . . . 131
- call summary parameters . . . . . 190
- call transfer . . . . . 427
- call volume summary report . . . . . 135
- call\_events . . . . . 378
- call\_exceptions . . . . . 379
- call\_phases . . . . . 401
- caller entered data, sending . . . . . 428
- call-id . . . . . 274
- callrecords . . . . . 390
- category codes . . . . . 141
- CCA . . . . . 411
  - error handling . . . . . 415
  - message flow summary . . . . . 415
  - messages . . . . . 412
- chapter summaries
  - defining . . . . . 16
- child node, adding new attributes . . . . . 72
- Cisco Queue Adapter . . . . . 159
  - active calls . . . . . 162
  - application summary . . . . . 161
  - call summary . . . . . 159
  - call volume . . . . . 164
  - connection status . . . . . 160
  - provisioning customer . . . . . 44
  - provisioning IVR profile . . . . . 59
- codec, H.323 . . . . . 280
- codecs
  - supported . . . . . 258
- collector database . . . . . 377
- commenting on this document . . . . . 21
- component summary report . . . . . 143
- conference and transfer with data . . . . . 359
- configuring
  - IVR behind-the-switch . . . . . 419
  - IVR in-front-of-the-switch . . . . . 421
  - IVR server . . . . . 418
- configuring objects
  - IVR behind configuration . . . . . 418
- connection ID . . . . . 289
- consult and transfer with data . . . . . 359
- contact header settings . . . . . 336
- Conveda . . . . . 256, 263, 273
  - port usage . . . . . 257
- copying
  - IVR profile attributes . . . . . 67
  - nodes . . . . . 72
  - server groups . . . . . 83
- courtesy transfer with data . . . . . 359
- CPA
  - configuring enhanced . . . . . 249
  - qualification parameters . . . . . 250
- CPD . . . . . 300
- creating
  - customers . . . . . 34
  - DID group . . . . . 83
  - groups . . . . . 82
  - IVR profiles . . . . . 47
  - new service . . . . . 123
  - server group . . . . . 82
  - service . . . . . 123
  - service type . . . . . 125
  - task . . . . . 77
  - user . . . . . 119
- crg events . . . . . 377, 381
- CTI Simulator . . . . . 225
  - accessing . . . . . 225
  - action parameter . . . . . 233
  - actions . . . . . 229
  - actions list . . . . . 229
  - clear window . . . . . 226
  - Command window . . . . . 228
  - Command window, clearing . . . . . 226
  - defining user data . . . . . 226
  - music . . . . . 232
  - play announcement . . . . . 230
  - play announcement and collect digits . . . . . 231
  - play application . . . . . 230
  - sample call . . . . . 234, 237
  - sample voice application code . . . . . 235
  - sample voice application, setting up . . . . . 234
  - transfer call . . . . . 233
- CTI transfer . . . . . 345, 346
- current peak . . . . . 384
- cust\_currpeaks . . . . . 385
- cust\_peaks . . . . . 396
- custom consultation call transfer, empty
  - capability set . . . . . 369
- custom data . . . . . 76
  - disabling . . . . . 77
  - enabling . . . . . 76
- customer . . . . . 34
  - creating . . . . . 34

deleting	45
deprovisioning	46
modifying	45
provisioning	36
<b>D</b>	
daily peaks report	136
daily summary report	135
data cleanup	405
data forwarding	359
data records	375
data recovery	
openLDAP	91
database	
collector	377
peaks	383
RepDWH	400
reporter	390
deleting	
attributes	72
customer	45
IVR profiles	69
node	72
nodes	72
deploying, behind-the-switch	420
deploying, in-front-of-the-switch	420
deployment methods, IPCM high availability	449
deprovisioning	
customer	46
IVR profiles	69
diagnostics viewing, EMPS	90
Dialogic blind transfer	345
DID	
creating group	83
groups	83
groups option	64
lookup	336
provisioning	63
range option	65
regenerating group with BPT	98
reports	85
directory assistance, ECT	353
dispenser files	70
display settings	147
DNIS	
treating unknown	428
document	
conventions	18
errors, commenting on	21
version number	18
download report	137
download_request	399
DTMF detecting	279
DTMF rendering	276

<b>E</b>	
early media	254
gateway	254
gateway, inbound calls	254
gateway, outbound calls	254
offer answer	254
ECT explicit NZ transfer	344
ECT explicit transfer	344
ECT explicit UK transfer	345
ECT transfer	353
directory assistance	353
presentation and screening indicators	354
redirecting number	354
editing groups	82
Element Management GUI, opening	75
Element Management Provisioning System	
See EMPS	
Element Management System	145
EMPS	165
accessing	26
adding cachebox	73
ASR vendor, adding	77
customer	34
GUI	25
help	30
information panel	28
IVR profiles	47
main frame	28
mandatory attributes	29
navigation tree	27
objects	27, 28
options	89
reports	84
resellers	32
saving changes	30
servers	71
tasks	77
top menu	30
TTS vendor, adding	76
users	85
users roles and permissions	87
view mode	30
view URL button	30
viewing diagnostics	90
empty capability set	365, 369
errors, OBN Manager	298
etrackforpeak	383
EventC	
data cleanup	405
eventc	
scaling	439
eventc_manager	381
eventc_stats	381, 387
events collector	165
analyze call	169

configuration test results	167
manager activity history	168
manager advanced options	170
statistics	166
work in progress	166
events file	375
explicit call transfer	353
See ECT	
extend AppXML	66
extensions, provisioning	66
external transfer	345, 346, 347

## F

fast start and tunneling, H.323	282
feature list	260
flow control, IVR Server Client	288
Framework, integrating	417
Framework, operating with	418

## G

G.729	262
garbage collector	151
gatekeeper, H.323	280
generic trap messages	424
groups	
creating	82
DID	83
editing	82
server	81
groups option, using	64
GVP DE, CTI Simulator	225

## H

H.323 Session Manager	171, 279
active calls	173
blind call transfer using ECS, configuring	366, 370
configuration	175
custom consultation call transfer using ECS, configuring	370
summary	171
heartbeat	
MRCP server hunt list	308, 311
high availability, IP Call Manager	447
HMP	262
HMP support	254
host media processing	
See HMP	
hourly peaks report	136
hourly summary report	135
hr_call_status	391

## I

importing server instance csv	75
in-front-of-the-switch	40
INITIATE_TRANSFER_REQ	414
integration features	426
IP Call Manager, H323	448
IP Call Manager, SIP	447
IPCS	176, 253
bridge transfer	351
call summary	176
feature list parameter	260
network announcement requirements	317
routes	178
transfers	346
IVR application, invoking with user data	428
IVR behind-the-switch	
configuring DNSs	419
configuring IVRs and IVR ports	419
creating virtual route points	422
IVR in-front-of-the-switch	
configuring	421
configuring DNSs	421
configuring IVRs and IVR ports	421
creating virtual route points	422
IVR ports, inbound calls	336
IVR profiles	47
attributes, copying	67
creating	47
deleting	69
deprovisioning	69
modifying	67
provisioning	49
shortcuts	70
IVR server	
configuring	418
load balancing	428
IVR Server Client	181, 285
active calls	184
application summary	183
call summary	181
call volume	185
connection status	182
flow control	288
KeepAliveRequest message	286
provisioning	39, 59
universal connection ID	289
IVR trap messages	425

## L

license usage	255
load balancing, MRCP server	308, 312
load_balancer	382
log	153
log file, BPT	101

log levels	154
log server integration	428
log window, BPT	99
Login Server	115
accessing	116
administration module	117
interface, customizing	138
modifying roles	128
modifying service	126
password	115
user administration	119
user roles	119

## M

management information base	152
managing user	121
Media Gateway	
configuring for H.323	283
media resource control protocol	
See MRCP	
media server, configuring	261
media support	254
MIB	152
Microsoft Cluster Service	453
modifying	
customer	45
IVR profiles	67
reseller	33
role	128
service	125, 126
tasks	81
MRCP server	
load balancing	308, 312
traps	310
MRCP server hunt list	307, 311
heartbeat	308, 311
out-of-service designation	307, 311
MRF support	259
Mulaw system prompts	435
multiple MCUs	323
multiple popgateways	323

## N

native RTP	257
navigation tree, EMPS	27
network announcement	48, 50, 315
call manager requirements	317
formal syntax, dialog service	316
IPCS requirements	317
requirements	315
SIP functions	316
network mode	40
Network Monitor	139

accessing	140
category codes	141
component summary report	143
server details	144
server status reasons	142
server status summary report	140
servers listing	143
network reports	133
network reports GUI	133
new IVR profile, creating with BPT	97
new media streams, adding	273
new service, creating	123
NEW_CALL_REQ	412
nodes	
copying	72
deleting	72
Nortel RLT transfer	344
notify server	74
numbering type and plan, H.323	282

## O

objects, configuring	418
OBN Manager	189, 291
application, provisioning	294
bulk request	296
components	292
interface parameters	294
interfaces	294
IVR profile, provisioning	299
Outbound Contact Server, integrating	299
single request interface	295
summary page	189
trigger applications	293
openLDAP recovery	91
auto-recovery	91
manual recovery	91
operator hang up, detecting	427
options	
advanced	125
EMPS	89
outbound call resolution	264
outbound call setup	264
Outbound Contact Server, integrating	299
outbound dial number format, configuring	247
outbound INVITE resolutions, samples	265
outbound notification	
See <i>also</i> OBN Manager	291
outbound notification, provisioning	60
overall status	147
overlap receive	
configuring on ISDN	248
enabling	248
SETUP_ACK message	248

## P

Page Collector	149
proxy support	329
proxy support, configuring	330
parameters	
call summary	190
IVR Server Keep Alive	286
p-asserted-identity	274
password, Login Server	115
pattern option, using	65
peak_control	388
peaks	
database	383
resetting	406
tables	395
peaks report	
daily	136
hourly	136
PING_REQ	414
PN-OBN	299
call result user data	304
CPA result variable	303
Framework port	302
OCS flag variable	303
user data attributes	304
user data from OCS	302, 304
user data to OCS	302
user data to OCS, customized	306
user data, campaign reschedule	305
user data, schedule call back	305
VoiceXML application	303
Policy Manager	191
active calls	193
application summary	192
call volume	194
provisioning	52
provisioning customer	38
summary	191
pop controller trap messages	424
port number, SIP registration	334
Portal	221
accessing	222
ports	419
presentation indicator, ECT	354
proactive notification-outbound notification	299
processes	148
progress bar, BPT	99
prompts	
Alaw	435
Mulaw	435
recording	435
provisioning	
ASR	57
Bandwidth Manager	53
Cisco Queue Adapter	44, 59

customer	36
debug	62
DIDs	63
extensions	66
IVR	50
IVR profiles	49
IVR Server Client	39, 59
OBN	60
Policy Manager	38, 52
Reporter	43
text-to-speech	54
transfer type	55
proxy support	329

## Q

qa_currpeaks	387
qa_peaks	399
queued request, subsequent errors	299
quorum, majority node set	455
quorum, standard	454

## R

range option, using	65
raw_events	377
RCA reports	84
redirecting number, ECT	354
refresh navigation tree	36
registration errors, handling	336
re-INVITE	273
receiving when bridging	273
removing	
server groups	82
tasks	81
RepDWH database	400
report ranges	137
report_tables	393
Reporter	133
data cleanup	405
database	390
GUI	133
provisioning customer	43
reporting	431
activating	431
IVR behind switch configuration	432
IVR in front switch configuration	433
reports	
DID	85
EMPS	84
find function	85
RCA	84
servers	85
resell_currpeaks	385
resell_peaks	396

resellers	32
deleting	34
modifying	33
resetting peaks	406
Resource Manager	196, 260
configuration	197
summary	196
role	
authorization	130
modifying	128
roles and permissions	87
route request, sending	426
routing, activating	421
routing, behind-the-switch configuration	422
routing, in-front-of-the-switch configuration	422
RTP	
native support	257
RTP ports, symmetric	327
RTP tone detection	277

## S

sample call	234
setup	234
scaling eventc	439
database	442
deployment	440
installing	444
subsystem components	439
scheduler	150
SCI	422
SCI traps	
generic	424
IVR	425
pop controller	424
text-to-speech	425
watchdog	424
screening indicator, ECT	354
SDP update	267
bridged call	267
DTMF or audio codec	273
IVR state	267
sample SIP call flow	268
server	
deleting nodes	72
server details	144
server group	
creating	82
server groups	81
copying	83
editing	82
removing	82
server instance csv, importing	75
server status reasons	142
server status summary report	140
servers	71
adding attributes	72
copying nodes	72
deleting attributes	72
editing information	71
notifying	74
servers listing	143
servers reports	85
service	
administration	123
creating	123
modifying	125, 126
session timers	274
shortcuts	70
single request interface	295
SIP	
handling messages	335
registration	334
registration frequency	335
registration, configuring IPCS	337
supported features	253
SIP functions, network announcement	316
SIP header values	
propagation	274
SIP headers	
call-id	274
p-asserted-identity	274
SIP INFO	265
message details	266
VoiceXML extension	266
SIP REFER	347
SIP REFER transfer	346
SIP refer with replaces	347
SIP refer with replaces transfer	346, 347
SIP reinvoke	267
SIP Session Manager	200
active calls	201
configuration	203
summary	200
Solution Control Interface	422
state transitions	382, 383
state_transitions	383
summary report	
call volume	135
daily	135
hourly	135
support	
MRF	259
supported codecs	258
swap IVR URL	95
symmetric RTP ports	327
system information menu	148

## T

T302 timer	249
task	



- adding . . . . . 77
- IVR profile, regenerating . . . . . 80
- schedule . . . . . 80
- select IVR profiles . . . . . 79
- specify changes . . . . . 80
- task info . . . . . 78
- tasks . . . . . 77
  - modifying . . . . . 81
  - removing . . . . . 81
  - viewing status . . . . . 81
- TBCT transfer . . . . . 344, 345
- telera\_currpeaks . . . . . 386
- telera\_peaks . . . . . 397
- terms of use banner url . . . . . 30
- Text-to-Speech
  - See TTS
- text-to-speech trap messages . . . . . 425
- text-to-speech, provisioning . . . . . 54
- tira\_report\_display\_table . . . . . 394
- tira\_report\_sqls . . . . . 395
- tira\_reports . . . . . 393
- tone packets
  - detecting . . . . . 277
  - generating . . . . . 277
  - supported . . . . . 278
- transactional recording . . . . . 319
  - VCS, configuring . . . . . 319
- transfer
  - ATT Conference . . . . . 344, 346
  - ATT Conference OOB . . . . . 344
  - ATT Consultative . . . . . 344, 346
  - ATT Consultative OOB . . . . . 344
  - ATT Courtesy . . . . . 344, 346
  - ATT Courtesy OOB . . . . . 344
  - ATT OOB . . . . . 357
  - blind call using ECS . . . . . 365, 369
  - bridge . . . . . 345, 346, 351
  - CTI . . . . . 345, 346
  - custom consultation call using ECS . . . . . 369
  - Dialogic blind transfer . . . . . 345
  - ECT . . . . . 353
  - ECT explicit . . . . . 344
  - ECT explicit NZ . . . . . 344
  - ECT explicit UK . . . . . 345
  - external . . . . . 345, 346, 347
  - Nortel RLT . . . . . 344
  - SIP REFER . . . . . 346, 347
  - SIP refer with replaces . . . . . 346, 347
  - TBCT . . . . . 344, 345
- transfer type, provisioning . . . . . 55
- transferring a call . . . . . 427
- transferring calls, H.323 . . . . . 281
- transfers . . . . . 343
  - IPCS . . . . . 346
  - VCS . . . . . 343
- treatments . . . . . 427

- trigger applications . . . . . 293
- trigger applications, OBN . . . . . 293
- ts\_currpeaks . . . . . 386
- ts\_hr\_call\_status . . . . . 392
- ts\_peaks . . . . . 397
- TTS . . . . . 204
  - active requests . . . . . 205
  - pending requests . . . . . 209
  - requests summary . . . . . 204
  - statistics . . . . . 206
- TTS vendor, adding . . . . . 76
- tts\_currpeaks . . . . . 387
- tts\_peaks . . . . . 398
- typographical styles . . . . . 18

## U

- universal connection ID . . . . . 289
- UPDATE\_CALL\_STATUS\_REQ . . . . . 413
- URS routing strategy, launching . . . . . 427
- user
  - creating . . . . . 119
  - managing . . . . . 121
- user administration, Login Server . . . . . 119
- user roles, Login Server . . . . . 119
- users, EMPS . . . . . 85, 87

## V

- VCS . . . . . 210, 247
  - active calls . . . . . 213
  - board status . . . . . 215
  - call summary . . . . . 210
  - call volume . . . . . 211
  - popgateway . . . . . 212
  - port status . . . . . 213
  - transfers . . . . . 343
- version numbering
  - document . . . . . 18
- view mode, EMPS . . . . . 30
- Voice Communication Server
  - See VCS

## W

- watchdog trap messages . . . . . 424
- whispering . . . . . 427