Genesys Voice Platform 7.6

Deployment Guide

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 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

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 or +506-674-6767	support@genesyslab.com
Europe, Middle East, and Africa	+44-(0)-127-645-7002	support@genesyslab.co.uk
Asia Pacific	+61-7-3368-6868	support@genesyslab.com.au
Japan	+81-3-6361-8950	support@genesyslab.co.jp

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

Document Version: 76gvp_dep_07-2011_v7.6.401.00

Table of Contents

List of Procedures

Preface

Welcome to the *Genesys Voice Platform 7.6 Deployment Guide*. This document provides detailed installation, and configuration instructions for Genesys Voice Platform (GVP).

This document is valid only for the 7.6 release.

Note: For releases 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.

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

GVP is a group of software components that complement other Genesys products in order to provide a complete solution to customers who require voice self-service. Although it is complex, GVP has a relatively easy graphical user interface (GUI) that customers can use to configure, tune, and activate applications. With flexible configuration and deployment options, GVP is targeted to both single-tenant and multi-tenant configurations. GVP can be integrated with the Genesys Framework in order to enable interaction with other Genesys components. This enables Genesys customers to deploy GVP in conjunction with other solutions such as Enterprise Routing Solution (ERS), Network Routing Solution (NRS), and Network-based Contact Solution (NbCS).

Intended Audience

This document, primarily intended for system integrators and 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 the Genesys Framework architecture.

Chapter Summaries

In addition to this preface, this Deployment Guide contains the following chapters and appendixes:

- Part 1: "Planning" on page 25
    - Chapter 1, "GVP Architecture," on page 27, describes the primary components and basic architecture of GVP.
    - Chapter 2, "Prerequisites and Planning," on page 57, describes the prerequisites and planning considerations for deploying GVP. It includes information about required software and recommended hardware.
- Part 2: "Windows Installation" on page 73
    - Chapter 3, "Windows Deployment Task Summaries," on page 75, provides summaries of the activities you must perform to install and maintain GVP in a Windows environment.
    - Chapter 4, "Preparing Your Windows Environment," on page 81, describes activities you must perform to prepare the GVP and non-GVP servers in your Windows deployment.
    - Chapter 5, "GVP Deployment Tool," on page 97, describes the GVP Deployment Tool (GDT) and how it works with the GVP Deployment Agent (GDA) to install GVP.
    - Chapter 6, "Installing GVP Components Using the GDT," on page 111, describes how to use the GDT to install GVP on the Windows operating system.
    - Chapter 7, "Installing GVP: DE with the GVP Deployment Tool," on page 161, describes how to use the GDT to install GVP: DE on the Windows operating system.
    - Chapter 8, "Installing Dialogic," on page 173, describes the steps to install the software to run the Dialogic boards in deployments that use Voice Communication Server (VCS).
    - Chapter 9, "Installing the Bulk Provisioning Tool," on page 179, describes how to install the optional Bulk Provisioning Tool.

- Chapter 10, “Post-Installation Activities on Windows Hosts,” on page 181, describes activities you must perform after installation of the EMS Reporting or OBN Manager components, as well as how to start and stop WatchDog on all GVP servers.
- Chapter 11, “Maintaining GVP,” on page 201, describes how to use the GDT to upgrade the GDA, to upgrade GVP to release 7.6, to install 7.6.x hot fixes, to repair GVP servers, and to uninstall GVP components and the GDA.

- Part 3: “Solaris Installation” on page 219
  - Chapter 12, “Solaris Deployment Task Summaries,” on page 221, provides summaries of the activities you must perform to install and maintain GVP in a Solaris environment.
  - Chapter 13, “Preparing Your Solaris Environment,” on page 225, describes activities you must perform to prepare the GVP and non-GVP servers in your Solaris deployment.
  - Chapter 14, “Installing GVP on Solaris,” on page 235, describes how to install GVP on the Solaris operating system.
  - Chapter 15, “Post-Installation Activities on Solaris Hosts,” on page 271, describes activities you must perform after installation of the EMS Reporting or OBN Manager components, as well as how to start and stop WatchDog on all GVP servers.
  - Chapter 16, “Uninstalling GVP on Solaris,” on page 285, describes how to uninstall GVP in a Solaris environment.
- Part 4: “GVP Configuration” on page 287
  - Chapter 17, “Configuring EMPS in the EMPS,” on page 289, describes how to configure the EMPS component.
  - Chapter 18, “Configuring EMS Runtime in the EMPS,” on page 301, describes how to configure the Element Management System (EMS) Runtime components.
  - Chapter 19, “Configuring EMS Reporting and OBN Manager in the EMPS,” on page 309, describes how to configure the EMS Reporting components and OBN Manager.
  - Chapter 20, “Configuring IPCS in the EMPS,” on page 341, describes how to configure the IP Communication Server (IPCS) component.
  - Chapter 21, “Configuring VCS in the EMPS,” on page 363, describes how to configure the VCS component.
  - Chapter 22, “Configuring MRCP ASR and TTS in the EMPS,” on page 391, describes how to configure the IPCS and VCS components for Media Resource Control Protocol (MRCP) Automatic Speech Recognition (ASR) and Text-to-Speech (TTS).
  - Chapter 23, “Configuring IP Call Manager in the EMPS,” on page 403, describes how to configure the IP Call Manager (IPCM) components.

  - Chapter 24, “ASR Log Manager System,” on page 421, describes the Automatic Speech Recognition (ASR) Log Manager system, its architecture, and how to configure the system.
- Part 5: “GVP Integrations” on page 439
  - Chapter 25, “Integrating GVP with Management Framework,” on page 441, describes how to integrate GVP IPCS or VCS with Genesys Management Framework.
  - Chapter 26, “SIP Server Integration,” on page 451, describes how to install and configure GVP for integration with the Genesys SIP Server.
- Part 6: “Appendixes” on page 459
  - Appendix A, “Configuring Dialogic,” on page 461, describes how to manually configure the Dialogic software and troubleshoot the Dialogic Driver.
  - Appendix B, “Manual Installation on Windows,” on page 505, describes how to manually install GVP on the Windows operating system.
  - Appendix C, “Behind-the-Switch,” on page 523 describes how to configure GVP for behind-the-switch operation.
  - Appendix D, “Sample SNMP Configuration and Log Files (Solaris),” on page 527, provides samples of the `snmpd.conf` and SNMP log files.

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:

```
72fr_ref_09-2005_v7.2.000.00
```

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]
```

Use of 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 the following additional resources as necessary:

- *Genesys Voice Platform 7.6 Reference Manual,* which provides information about the GUIs and configuration options for the GVP components. It describes the interfaces, their function, and how to use them.
- *Genesys Voice Platform 7.6 Troubleshooting Guide,* which provides information about SNMP traps as well as some basic troubleshooting information.
- *Genesys Voice Platform 7.6 Studio Deployment Guide*, which provides installation instructions for Genesys Studio, a GUI for development of VoiceXML-based applications.
- *Genesys Studio Help*, which provides online information about Genesys Studio.
- *Genesys Voice Platform 7.6 Voice Application Reporter Deployment and Reference Manual*, which provides installation instructions for VAR. 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 VAR database and generate application reports.
- *Genesys Voice Platform 7.6 VoiceXML 2.1 Reference Manual*, which provides information about developing VoiceXML 2.1 applications on GVP. It presents VoiceXML 2.1 concepts, and provides examples that focus on the GVP implementation of VoiceXML. It also describes the platform extensions that Genesys provides for VoiceXML.
- *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.
- *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 implementation by the developer community.
- *Genesys Technical Support Troubleshooting Guide*, which provides 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 higher to all Genesys 7.x releases. For more information, contact Genesys Technical Support at `http://genesyslab.com/support.`
- *IVR Interface Option 7.2 IVR Server Administrator's Guide*, which provides detailed information about how to deploy, configure, and use the the Interactive Voice Response (IVR) Server.
- Release Notes and Product Advisories for this product, which are available on the Genesys Technical Support website at `http://genesyslab.com/support.`

Information about 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 Reference Manual*
- *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.

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.

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

- Chapter 2, Prerequisites and Planning:
  - Table 3 on page 58, has been updated to include Windows 2008 and 2008 R2.
- Chapter 10, Post-Installation Activities on Windows Hosts:
  - Two new procedures, Creating a website for Unified Login (Windows 2008), page 191 and Creating a website for Network Monitor (Windows 2008), page 196 have been added to configure Windows 2008.

Part

1 Planning

Part One of this manual describes the architecture and how to plan the deployment of the Genesys Voice Platform (GVP). This information appears in the following chapters:

- Chapter 1, “GVP Architecture,” on page 27
- Chapter 2, “Prerequisites and Planning,” on page 57

Chapter

1 GVP Architecture

This chapter describes the primary components and basic architecture of Genesys Voice Platform (GVP). It contains the following sections:

Overview

Genesys Voice Platform (GVP) is the compilation of software, telephony servers, and management servers that integrate with traditional Time Division Multiplex (TDM) digital telephony networks, and also with Voice over Internet Protocol (VOIP) networks, to deliver web-driven telephony services to callers.

GVP consists of two main parts:

- Telephony servers—Voice Communication Server (VCS) for TDM-based networks, and IP Communication Server (IPCS) for VOIP-based networks.
- Element Management System (EMS)—Provides support, management, and maintenance server processes.

GVP supports both Voice Extensible Markup Language (VoiceXML) 2.0 and VoiceXML 2.1, following the recommendations listed in Table 1. Any application server that is part of a GVP deployment is required to store and execute VoiceXML-based applications. VoiceXML documents can be generated dynamically using any number of Web technologies, such as Active

Server Pages (ASPs) or Java Server Pages (JSPs), or using a complete application development and execution environment, such as IBM's Websphere.

GVP fully supports automatic speech recognition (ASR) and speech synthesis (or text-to-speech [TTS]) as part of a VoiceXML dialog, following the recommendations listed in Table 1.

Communications between GVP and ASR and TTS engines are accomplished through the use of the Media Resource Control Protocol (MRCP), following the recommendation listed in Table 1. MRCP is a Media Resource Control Protocol that was developed by Cisco, Nuance, and SpeechWorks.

Table 1: Supported Recommendations

Feature	Supported Recommendation
VoiceXML 2.0	W3 standard Voice Extensible Markup Language (VoiceXML) Version 2.0, W3C Recommendation, 16 March 2004
VoiceXML 2.1	W3 standard Voice Extensible Markup Language (VoiceXML) Version 2.1, W3C Candidate Recommendation, 13 June 2005
Supported ASR grammar formats	W3C standard Speech Recognition Grammar Specification Version 1.0, W3C Recommendation, March 2004
TTS	W3C standard Speech Synthesis Markup Language (SSML) Version 1.0, W3C Recommendation 7 September 2004
MRCP	Internet Engineering Task Forces RFC 4463

GVP Single-Tenant

The GVP Single-Tenancy provisioning system, when integrated with Genesys Framework, delivers next-generation voice processing that meets advanced call-routing and voice self-service needs for a contact center enterprise.

The GVP application is different from traditional Interactive Voice Response (IVR) solutions. The GVP solution does not rely on proprietary hardware, and executes voice applications that are created in a nonproprietary coding language, VoiceXML. By using standards such as VoiceXML, GVP separates the voice application from the call processing environment.

GVP software resides on a server that terminates calls and that contains the VoiceXML voice browser that interprets VoiceXML documents into call-processing events. GVP incorporates third-party ASR and TTS technologies using the MRCP standard. GVP also supports VOIP technology with the GVP

IP Communication Server (IPCS) component and TDM technology using Dialogic boards, and the GVP Voice Communication Server (VCS) component.

You can position GVP as a solution in-front-of or behind a premise-based switch. In an In-Front-of-the-Switch configuration, calls terminate on the IPCS/VCS and do not pass through an on-site Automatic Call Distributor (ACD). In a Behind-the-Switch configuration, calls pass through an ACD first and are then sent to the IPCS/VCS. GVP is uniquely positioned to provide a comprehensive voice contact center solution for universal queuing, routing, CTI, and reporting.

In addition, the GVP voice applications and the optional Voice Application Reporter (VAR) reside on separate web server(s). Voice applications (IVR Profiles) are configured and managed with the Element Management Provisioning System (EMPS). To complete the solution, a web server is added to the GVP configuration for hosting VoiceXML applications.

GVP Multi-Tenant

The GVP Multi-Tenancy provisioning system is a carrier-grade voice self-service system, that is inherently multi-tenanted. GVP Multi-Tenant telephony sessions can be managed as a universal pool of resources, available to any application because the EMS is centralized. Telephony sessions can be TDM, VOIP, or a combination of both, available as part of a single GVP Multi-Tenant deployment, and transparent to all applications (see Figure 1 on page 30).

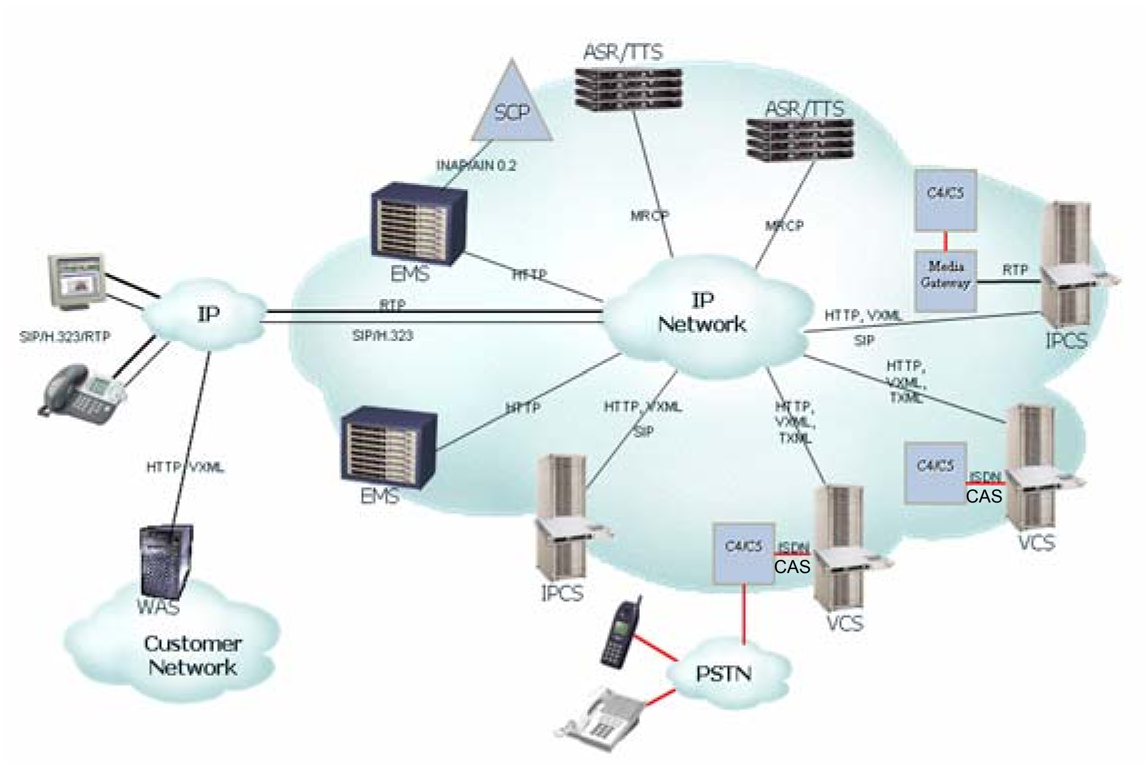


Figure 1: GVP Distributed Deployment

Developer's Edition

Genesys Voice Platform: Developer's Edition (GVP: DE) provides the platform and resources that are required for the development and testing of voice applications designed for GVP.

GVP: DE provides VOIP functionality that is integrated with the Genesys product suite and a flexible, standards-based voice-processing platform.

It also includes speech recognition, and text-to-speech client software for using MRCP to communicate with MRCP ASR/TTS servers, thereby facilitating the creation of speech-enabled applications.

The Developer's Edition provides seamless integration with the Genesys Framework, while providing an option to develop applications with, or without the Genesys Framework. Developers can utilize the simulation capabilities provided for CTI interactions, and optionally use the complete Genesys Framework setup, should such a setup be available for development.

Features

GVP provides a variety of features that support call handling for a voice application through either TDM or VOIP functionality. GVP also expands traditional IVR functionality with self-service capabilities that are tightly integrated with the Genesys product suite, and a flexible standards-based voice-processing platform.

Core Telephony Features

The following core telephony features are available:

- Call acceptance and processing through standard Integrated Services Digital network (ISDN) and robbed-bit signaling.
- Call handling through VOIP.
- Support for major PBX switches.
- Voice termination and processing using standard DM3 Dialogic hardware.
- Call transfers with support for Europe and the United States, including AT&T Transfer Connect, WorldCom Takeback and Transfer, Sprint Agent Transfer (inband transfers), and Call Bridging with the inbound and outbound leg maintained (for the call duration) when GVP sits in front of the switch.
- Telephony ports for sending and receiving calls. For example, a hardware platform supporting 23 simultaneous and discrete conversations would require 23 ports. GVP ports are universal, in that they can terminate any call for any application. A dialed number identification service (DNIS) determines what application to run.
- Support for major Media Gateways.
- Media services including voice prompts, menus, and data (dual-tone multi-frequency [DTMF] or speech) collection.
- Acceptance and processing of information delivered with a call from the Media Gateway, including Automatic Number Identification (ANI), DNIS, and Calling Line Identification (CLID).

Advanced Features

The following advanced features are available:

- Automatic Speech Recognition (ASR)
- Text-to-Speech (TTS)
- Outbound Calling
- TeleraXML (TXML) extensions for advanced call-control capabilities beyond the current scope of VoiceXML 2.1

- XML-based, back-end data capture
- Intelligent call routing provided by Genesys Enterprise Routing Solution and Network Routing Solution
- Call parking, providing multi-site contact centers with the ability to enable self-service and call queuing on GVP, prior to transferring or bridging the call to an agent
- Graphical user interface (GUI) for the development of VoiceXML applications
- Real-time call monitoring and management, as well as historical reporting and analysis
- Web-based GUI for configuration of system features and voice applications, as well as diagnostics and other administrative functions
- Flexible deployment options

Reporting Features

The optional Voice Application Reporter (VAR) provides web-based reports that display hourly, daily, and weekly application usage. The reports show total calls received, calls abandoned, calls completed in IVR, and calls transferred in IVR-controlled applications.

Note: The Voice Application Reporter is packaged on its own CD.

In addition, real-time and historical reporting for calls landing on GVP is provided by the Genesys CCPulse+ and Contact Center Analyzer (CC Analyzer) components, which are part of the Genesys Enterprise Routing Solution. The GVP IPCS/VCS Monitor displays active calls in real time.

Voice Application Features

A GVP voice application resides on a web server that interacts with the IPCS/VCS on every call. GVP supports interactions with multiple web servers using standard Hypertext Transfer protocol (HTTP). If voice applications reside on separate web servers, these web servers can be located on a web farm architecture in a local or remote network configuration.

Coding Language

Voice applications written for GVP must be in standard VoiceXML. GVP supports the World Wide Web Consortium (W3C) standards for VoiceXML 2.1. GVP also supports extensions to assist in the call-control requirements of a voice application.

Developer Tools

Genesys provides a voice-application development tool called Genesys Studio to assist customers with the development of VoiceXML applications. This tool is a GUI that you can use to build and test voice applications using the Drag-and-Drop paradigm. Genesys Studio generates Active Server Pages (ASPs) or Java Server Pages (JSPs). These pages generate VoiceXML when processed by the web server. Genesys Studio supports touch-tone and ASR voice applications, and provides a common mechanism to link to databases. In addition to Genesys Studio, the EMPS also provides the ability to manage the capture of caller utterances in order to help the developer to fine-tune ASR voice applications.

Note: Genesys Studio is packaged on its own CD.

Integration with Genesys Components

The following Genesys components integrate with GVP:

- Reporting (Genesys Info Mart, CCPulse+, and Contact Center Analyzer)
- IVR Server, SIP stack, and SIP Server
- Outbound Contact release 7.5 or later

Outbound Contact System (OCS)

OCS is an integrated component based on the Outbound Notification (OBN) component. OCS integrates with GVP to reduce resource costs through the use of automated agents to proactively contact customers. Custom VoiceXML applications can automatically process the GVP-dialed outbound calls for self-service, or the calls can be passed to an agent for assisted service if agent involvement is necessary.

The integrated solution is referred to as Proactive Contact.

The Proactive Contact solution can be used in single-tenant or multi-tenant deployments.

Outbound Contact integrates with GVP when operating in Power GVP mode. GVP contains an Outbound Notification (OBN) server that can be configured as an OBN application in the EMPS. The following is an architectural drawing of GVP integrating with OCS (see Figure 2 on page 34).

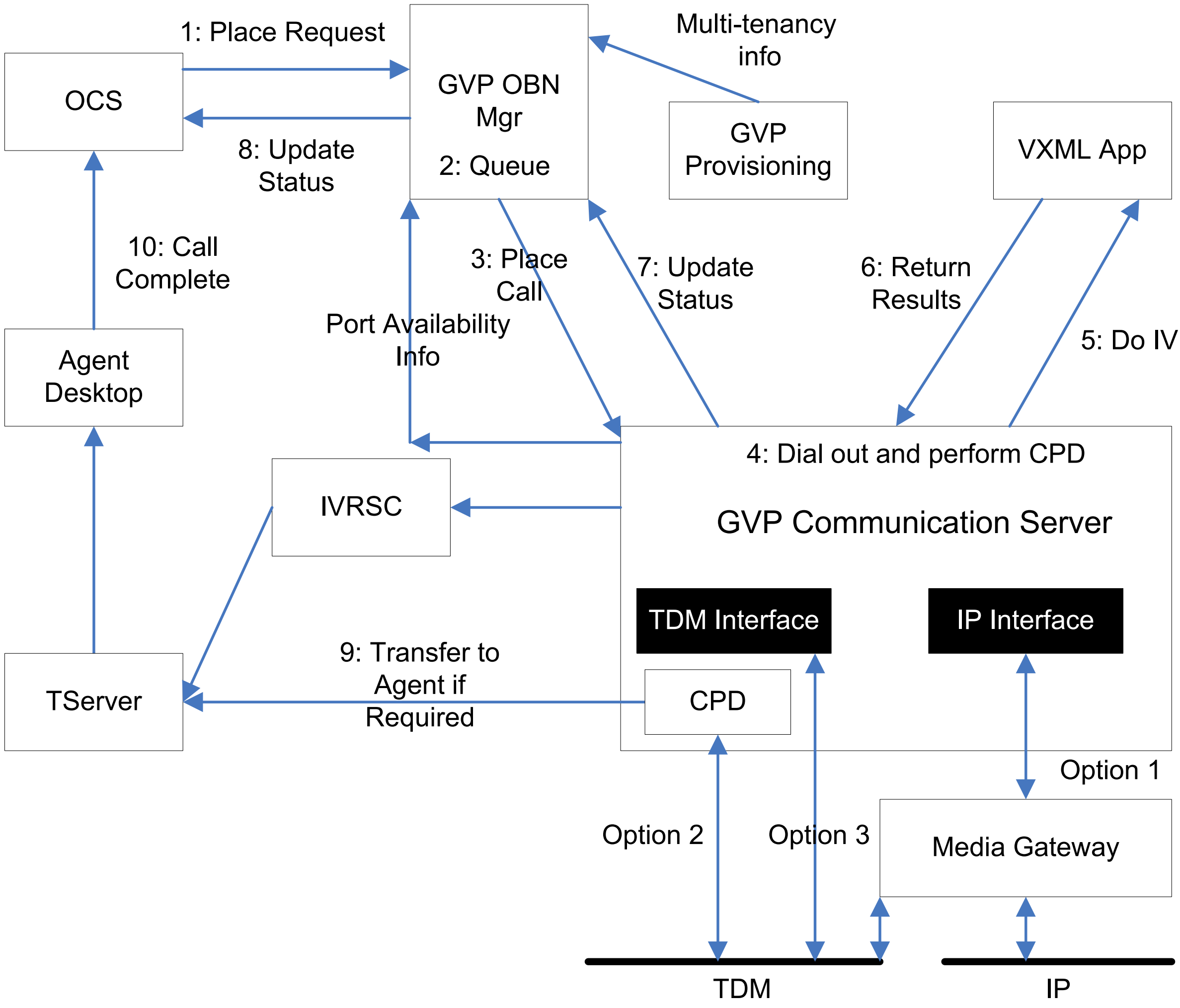


Figure 2: Proactive Contact Solution Call Flow

For more information, see the *Genesys 7.6 Proactive Contact Solution Guide* and the *Outbound Contact 7.6 Deployment Guide*.

Element Management System

The Element Management System (EMS) consists of runtime and non-runtime components.

The runtime components are:

- Resource Manager (RM)/SIP Session Manager (SSM)/H.323 Session Manager (HSM)
- Policy Manager
- IVR-Server Client/Cisco Queue Adapter
- Bandwidth Manager

- MRP SMP Integrator

The non-runtime components are:

- Element Management Provisioning System (EMPS)
- Event Collection (EventC) system
- Network Monitoring System

Figure 3 depicts the EMS architecture.

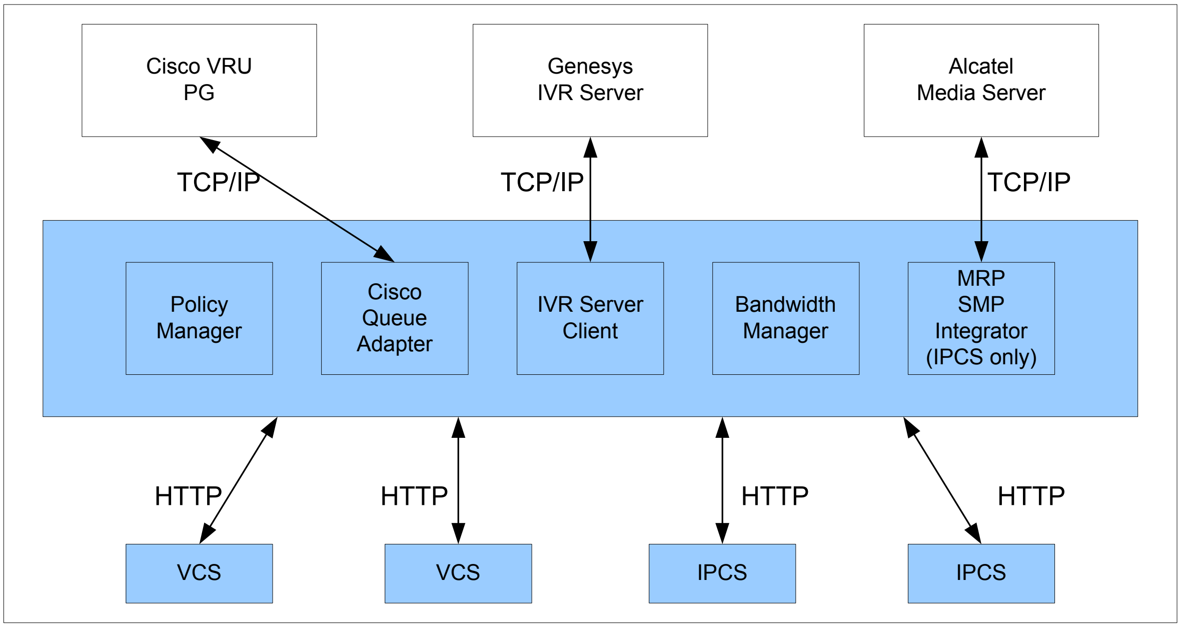


Figure 3: EMS Architecture

IP Call Manager

IP Call Manager (IPCM) is a set of components that co-ordinate the resources to process VOIP calls using Session Initiation Protocol (SIP).

There are two setup combinations for IPCM:

- SIP Session Manager and Resource Manager
- H.323 Session Manager and Resource Manager

For a brief description of the components, see “IP Call Manager Components” on page 50.

Starting with GVP 7.5, Resource Manager also integrates with the Genesys SIP Server. Refer to Chapter 26, “SIP Server Integration,” on page 451 for installation and configuration instructions.

Figure 4 shows the interaction between SIP Server and GVP Resource Manager from the point of view of an overall Genesys solution.

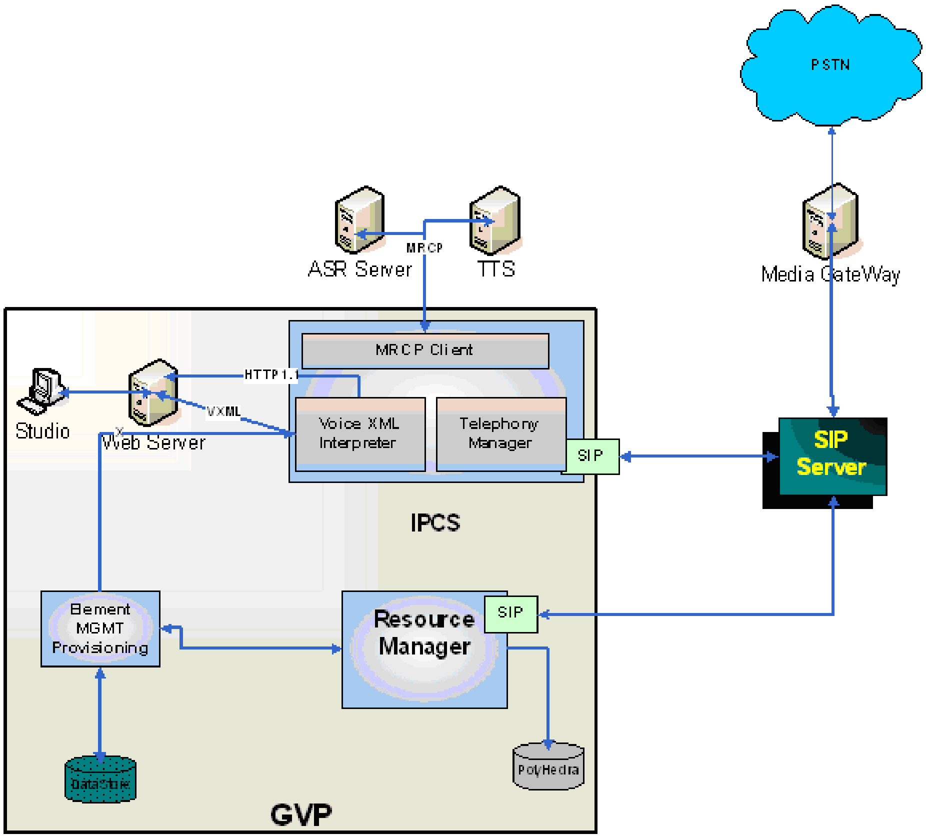


Figure 4: IPCM architecture with SIP Server

GVP Components

This section describes all of the base and optional components for GVP. Any differences between a Solaris and Windows installation will be noted (see Table 2 on page 36 for a quick summary of the supported operating system for each installation package).

Quick Reference Table

Table 2 provides a list of the installation packages and the supported operating system for each.

Table 2: Installation Package and Supported OS

Installation Package	Windows	Solaris
Common	✓	✓
IP Communication Server	✓	✓

Table 2: Installation Package and Supported OS (Continued)

Installation Package	Windows	Solaris
Voice Communication Server	✓	
IVR Server Client	✓	✓
Installation Wizard	✓	
Launcher		✓
Element Management Provisioning System	✓	✓
Dispenser	✓	✓
Bandwidth Manager	✓	✓
Policy Manager	✓	✓
Management Information Base	✓	✓
Text-to-Speech	✓	✓
Outbound Notification Manager	✓	✓
Bulk Provisioning Tool	✓	
Third-Party Apache Solaris		✓
SNMP		✓
MRP SMP Integrator		✓
Cisco Queue Adapter	✓	✓
Call Status Monitor	✓	✓
EventC	✓	✓
Reporter	✓	✓
Login Server	✓	✓
Network Monitor	✓	✓
Dialogic Installer	✓	
Resource Manager	✓	✓

Table 2: Installation Package and Supported OS (Continued)

Installation Package	Windows	Solaris
SIP Session Manager	✓	✓
H.323 Session Manager	✓	✓
Portal	✓	✓
ASR Log Manager	✓	
ASR Log Agent	✓	
ASR Log Server	✓	
Developer’s Edition IP Communication Server	✓	
Developer’s Edition CTI Simulator	✓	

Common

The Common component contains all of the common modules for GVP. The common modules are:

- WatchDog
- Page Collector
- Scheduler
- Network Management

WatchDog

WatchDog monitors all components to ensure that they are up and running. It also has a user interface to enable the manual stopping and starting of processes.

GVP Configuration File

Each GVP server runs its own WatchDog process. WatchDog is responsible for starting other GVP processes on that GVP server. WatchDog starts the other GVP processes in the order specified in the `gvp.ini` configuration file. When WatchDog starts or restarts, it re-creates the `gvp.ini` file, based on configuration information that it obtains from the EMPS.

Failover on Error

When WatchDog is starting, it checks the validity of the new `gvp.ini` configuration file.

- If the new configuration file is valid, it is used during startup, and the existing `gvp.ini` file is overwritten.
- If the new configuration file is invalid, WatchDog fails over to an existing configuration file if the following conditions are met:
  - A `gvp.ini` file already exists on the local host.
  - The processes listed in the process startup list in the existing configuration file have their own sections and `CLSID` parameters.

  If WatchDog fails over, then the existing configuration file is used during startup, and it is not overwritten.

WatchDog Modes of Operation

WatchDog can operate in two modes:

- Normal
- Safe

Normal Mode WatchDog attempts to sequentially start all the processes that are specified in the new `gvp.ini` startup list. If WatchDog encounters a problem while it is starting any of the processes, it shuts down the processes it has already started (including itself). The previous (existing) `gvp.ini` file is not overwritten.

Safe Mode WatchDog attempts to sequentially start all the processes that are specified in the new `gvp.ini` startup list. If WatchDog encounters a problem while it is starting a process, it sends a `cnpartialStart` trap and does not attempt to start any additional processes. However, WatchDog does not terminate any processes it has already started. The previous (existing) `gvp.ini` file has been overwritten.

For information about starting, restarting, and stopping WatchDog, see “Starting and Stopping GVP on Windows” on page 198 or “Starting and Stopping GVP on Solaris” on page 282.

Page Collector

The Page Collector fetches Extensible Markup Language (XML) pages that need to be executed. It also determines the document format and passes the pages to the appropriate parser (VoiceXML or TXML).

Scheduler

The Scheduler provides information about scheduled processes, and launches tasks to be executed periodically.

Network Management

Network Management interfaces with the Simple Network Management Protocol (SNMP) subsystem. It fields SNMP Management Information Base

(MIB) requests, and generates traps for processing by a network management system. Network Management can also provide activity logging for information and debugging purposes. Network Management also contains a user interface that displays statistics on the number of active ports, and enables the manual stopping and restarting of IPCS components.

IP Communication Server

The IP Communication Server (IPCS) handles calls through Voice over IP (VOIP). To send or receive a call using a Media Gateway, the IPCS sets up a Session Initiation Protocol (SIP) session, handles security, generates events, retrieves customer applications as necessary, maintains the media stream, and closes the SIP session at the end of the call.

The IPCS also interfaces with the third-party MRCP automatic speech recognition server. The MRCP ASR Client defines the requests, responses, and events that are needed in order to control the media processing resource. The MRCP ASR Client side is responsible for formulating outgoing request messages to the MRCP Server, and for decoding incoming MRCP response messages from the MRCP Server.

IPCS Subcomponents

This section provides an overview of each subcomponent and its process found in the IPCS.

The IPCS software has the following primary functions:

- Communicates with Media Gateways.
- Parses, interprets, and executes the VoiceXML commands in the XML documents served by the web server.
- Integrates with TTS and ASR software.

IPCS performs several integrated, internal processes.

Note: The following subcomponents are common across IPCS and Voice Communication Server (VCS):

TXML Parser

VoiceXML Parser

Call Flow Assistant (CFA)

MRCP client

Figure 5 illustrates the subcomponents that comprise the IPCS, and depicts how they interact.

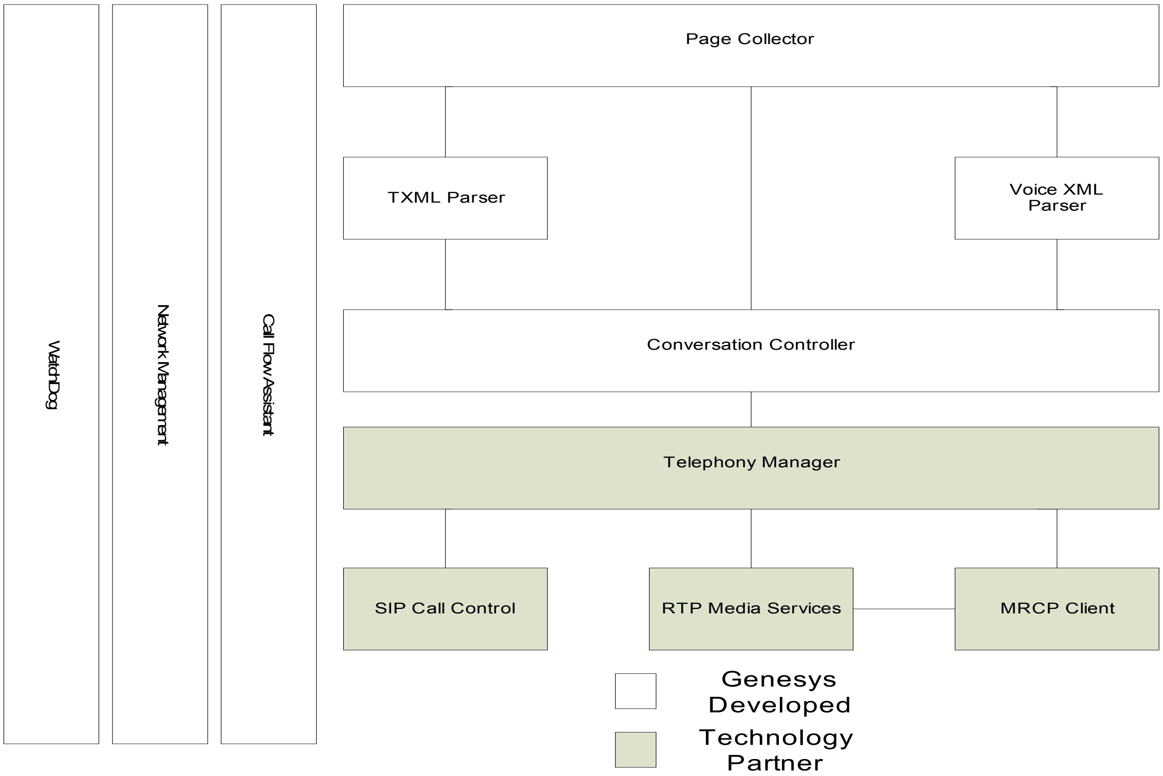


Figure 5: IPCS Subcomponent Architecture

TXML Parser

The TXML Parser parses XML documents using the Telera XML (TXML) tag set, and sends the interpreted telephony commands to the Conversation Controller.

VoiceXML Parser

The VoiceXML Parser parses Voice XML documents using the VoiceXML tag set, and sends the interpreted telephony commands to the Conversation Controller.

Call Flow Assistant

The Call Flow Assistant (CFA):

- Provides call control capability to the PopGateway module of the IPCS/VCS components. The PopGateway consults the CFA to do call control for call transfers and call routing whenever there is call control functionality to be performed.
- Provides two-way communication with the IVR Server Client.

Conversation Controller

The Conversation Controller drives the conversation with the web application. It creates a parsed stream of the commands, and using the appropriate API's, executes the stream of commands. For standard voice processing, such as playing a voice file, it dispatches the play request to the Media Control Unit (MCU). If TTS is required, the request is dispatched to TTS by the MCU, which plays the resulting TTS-generated voice data.

Telephony Manager

The Telephony Manager controls the physical voice-processing media. Through the media's driver interface, the Telephony Manager can issue requests such as setting up and tearing down a call, playing a voice file, or bridging a call. The Telephony Manager executes call control commands from the Conversation Controller/Action Execution Engine.

SIP Call Control

This component implements call control signaling using the standard Session Initiation Protocol (SIP) protocol. Its purpose is to set up, tear down, and transfer call sessions. It always maintains call states.

RTP Media Services

This component manages Real-time Transport Protocol (RTP) media streams for call sessions. It provides functionality, such as playing prompts, recording prompts, interacting with speech recognition software, and detecting and generating DTMF (Dual-Tone Multi-Frequency) tones.

MRCP Client

The MRCP client communicates with ASR and TTS engines that support the MRCP protocol. It consists of three major modules:

- MRCP stack, which encodes the requests as MRCP messages and decodes responses from the MRCP server.
- Real-time Streaming Protocol (RTSP) stack, which establishes sessions between the MRCP client and server.
- Real-time Transport Protocol (RTP) stack, which is also required to establish sessions between MRCP client and server.

The MRCP client interacts with the Telephony Manager.

MRCP Stack The MRCP stack defines the requests, responses, and events needed to control the media-processing resource. The MRCP stack and its messaging are designed to be carried over RTSP, or another protocol as a MIME-type, similar to the Session Description Protocol (SDP).

The MRCP client:

- Formulates outgoing request messages to the MRCP server, and decodes incoming MRCP response messages from the MRCP server.
- Accesses an RTSP stack (RFC 2326) to send requests and receive responses from the MRCP server.
- Accesses an RTP stack (RFC 1889) to stream audio and DTMF packets.

RTSP Stack The RTSP stack formulates outgoing RTSP request messages, and decodes the incoming RTSP response messages. The RTSP stack acts as a tunnel for sending all MRCP messages.

The MRCP client implements the RTSP methods.

The RTSP session uses transmission control protocol (TCP), a connection-oriented interface when connecting to the MRCP server. If an RTSP connection is dropped during a session, the MRCP client reestablishes the connection. All messages for a given session are sent on the same socket connection, even when both ASR and a TTS resource are requested.

RTP Stack The RTP stack sends and receives audio packets, and non-telephony event packets. The RTP packet stream uses the User Datagram Protocol (UDP) connectionless protocol.

The MRCP client optimizes the required local area network (LAN) bandwidth by stopping transmission of RTP packets as soon as recognition is complete. The MRCP client resumes sending RTP packets when the next recognition request is sent, and it ensures that packet sequence numbers. Timestamps increase monotonically, using the same numbering space.

The DTMF events conform to RFC 2833 (the default payload type is configurable).

Voice Communication Server

Note: The Voice Communication Server is available for Windows installations only.

The VCS parses, interprets, and executes the VoiceXML commands in the XML documents served by the web server. The VCS communicates with Dialogic circuit boards, and instructs the boards what action to take—for example, play prompts or listen for DTMF. The VCS software processes voice calls that arrive on Time-division Multiplexing (TDM) circuits.

The VCS also interfaces with the third-party Media Resource Control Protocol automatic speech recognition server. The MRCP ASR Client defines the requests, responses, and events that are needed in order to control the media processing resource. The MRCP ASR Client side is responsible for formulating outgoing request messages to the MRCP Server, and for decoding incoming MRCP response messages from the MRCP Server.

VCS Subcomponents

In an In-Front-of-the-Switch configuration, the VCS uses a Dialogic circuit board that connects to T1 or E1 line(s) that carry the voice calls. For a Behind-the-Switch configuration, the VCS uses a Dialogic circuit board that connects to the premise-based switch.

VCS performs several integrated, internal processes.

Figure 6 illustrates the VCS subcomponents, processes, and interactions, which are discussed in more detail in subsequent sections.

Note: For information about the VCS subcomponents and their functions, refer to "IPCS Subcomponents" on page 40:

TXML Parser

VoiceXML Parser

Call Flow Assistant (CFA)

MRCP client

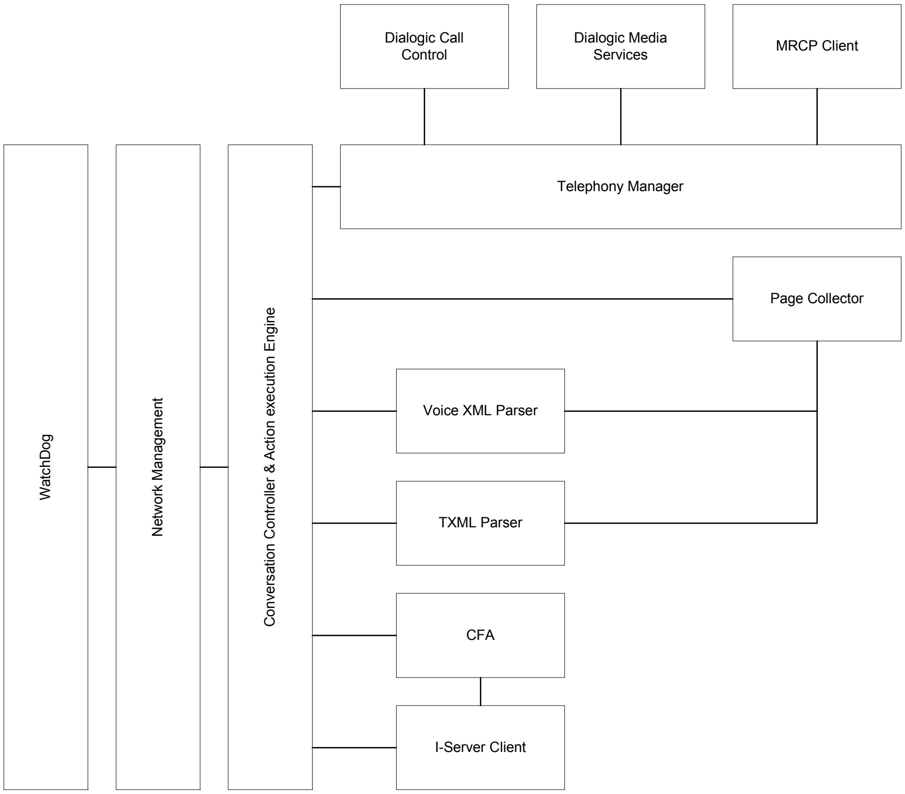


Figure 6: VCS Subcomponent Architecture

Dialogic Call Control

The Dialogic Call Control component processes the actual voice calls and manages the Dialogic telephony interfaces.

Dialogic Media Services

These are the Dialogic-provided call-management and media-processing services used by the Telephony Manager.

Telephony Manager

The Telephony Manager controls the physical voice-processing media and communicates with Dialogic Call Control and Dialogic Media Services. Through the Media Service's driver interface, the Telephony Manager can issue requests such as setting up and tearing down a call, playing a voice file, or bridging a call. The Telephony Manager executes call-control commands from the Conversation Controller and Action Execution Engine.

Conversation Controller and Action Execution Engine

The Conversation Controller drives the conversation with the voice application. It creates a parsed stream of the commands, and using the appropriate Advanced Interface Modules (AIM), executes that stream. For standard voice processing, such as playing a voice file, it dispatches the play request to the Telephony Manager. If TTS is required, Telephony Manager dispatches the request to the MRCP Client, which then provides the necessary information to the Telephony Manager to play the resulting TTS-generated voice.

IVR Server Client

The IVR Server Client provides the communications link between the IPCS/VCS and the IVR Server when integrating GVP with Genesys Framework. It can be installed on any host, including the VCS/IPCS host.

Installation Wizard

Note: The Installation Wizard is used for Windows installations only, but is not a requirement.

The Voice Platform Wizard helps you install and configure the GVP solution.

Launcher

Note: The Launcher is used for Solaris installations only, but is not a requirement.

The Launcher enables you to install groupings of components, as well as the installation of each component individually.

Element Management Provisioning System

The Element Management Provisioning System (EMPS) is an entry interface, and repository for GVP server configurations, customer configurations, and customer application profiles. The EMPS stores its data using a Lightweight Directory Access Protocol (LDAP) compliant directory server.

Dispenser

The Dispenser component is a web directory that hosts XML files generated by the EMPS which represent IVRProfiles (VoiceXML application profiles), and their mapping to direct inward dialing (DID)s/DNISs. GVP components such as IPCS, VCS, and RM access these files to determine how to process calls, and what VoiceXML scripts to execute for the call. There may be multiple dispensers in a GVP deployment.

Bandwidth Manager

The Bandwidth Manager manages the transfer rate of caller audio files recorded on the IPCS/VCS that are posted to the web server. It also performs retries in the event of failures.

Policy Manager

The Policy Manager (PM) maintains and enforces policies for each customer and each application, on an individual basis. Policies include those that allocate ports, authorize the placement of calls, and enable features. The Policy Manager tracks the ports currently in use for all customers and applications, and it determines what to do with each incoming call. The PM communicates with the Call Status Monitor and receives information from the EMPS.

Management Information Base

The Management Information Base (MIB) manages trap and variable definitions for GVP.

Text-to-Speech

This component interfaces with the third-party MRCP TTS server. The MRCP TTS Client defines the requests, responses, and events needed to control the media processing resource. The MRCP TTS client side is responsible for formulating outgoing request messages to the MRCP Server, and for decoding incoming MRCP response messages from the MRCP Server.

Note: This component is embedded in the IPCS Installation Package for Enhanced Media Services, and should not be explicitly installed. However, for VCS and IPCS Basic Media Services, this component must be installed separately.

OBN Manager

The Outbound Notification Manager (OBN Manager) enables GVP customers to make outbound calls by using GVP, and to initiate these calls by using simple HTTP requests. It is a high-performance, scalable solution for single or multiple customers. OBN Manager provides simplified configuration, provisioning, troubleshooting, and Outbound Contact Server requests. OBN Manager, along with other components in GVP, supports multi-tenancy.

Bulk Provisioning Tool

Note: The Bulk Provisioning Tool is available for Windows installations only.

The Bulk Provisioning Tool enables you to create, regenerate, and reprovision VoiceXML applications (called IVRProfiles in GVP) in bulk.

Third-Party Apache Solaris

Note: The Third-Party Apache Solaris is available for Solaris installations only.

The Third-Party Apache Solaris component is a web server that GVP uses for inter-machine communications, and to display GUIs.

SNMP

Note: The SNMP is available for Solaris installations only.

GVP uses the SNMP component to send traps to a Simple Network Management Protocol (SNMP) Manager. SNMP Managers also use this component to query the MIB data from Genesys processes

MRP SMP Integrator

Note: The MRP SMP Integrator is available for Solaris installations only.

The MRP SMP Integrator converts industry standard SNMP traps to Alcatel's Open Service Platform Media Extensions (OSPME) proprietary SMP format so that Alcatel's management systems can understand them.

The MRP SMP Integrator is comprised of three components.

- SnmpSmpConverter—converts SNMP traps to SMP format.
- StatHandler—converts the SNMP Agent statistics to SMP format.
- SMPLocalManager—listens for and sends messages to the Global Manager (GM).

Cisco Queue Adapter

When GVP connects to the Cisco ICM Enterprise Call Routers it uses the Cisco Queue Adaptor (CQA). The CQA communicates directly with the IPCS/VCS and the premise-based Cisco Peripheral Gateway. The EMPS manages all network and application provisioning of the CQA.

Call Status Monitor

The Call Status Monitor enables Service Providers and their customers to have access to the most current data about call activity.

The Call Status Monitor performs the following functions:

- Reads data directly from the Policy Manager (PM). This ensures that the data viewed in Call Status Monitor is consistent with that of the Policy Manager.
- Enables you to install and run multiple Call Status Monitor servers. In this way, each server can show data for any customer and reseller, or it can report network-wide operations.
- Enables you to have multiple resellers on each machine.

- Eliminates the need to provision Call Status Monitor in customer provisioning. All customer data is available in all Call Status Monitor servers.

EventC

The EventC component receives individual call events such as Call Start, Call End, and Calls Transferred from the IPCS/VCS. It stores call events in files in a shared directory. These are then processed by EventC subcomponents to populate the Billing and Reporter database.

The EventC system in GVP 7.6 has the following features:

- Precalculates summaries for easy reporting
- Calculates peak port usage by Service Provider, Reseller, customer, application and voice servers
- Populates provisioning data in CDR for accurate billing
- Automatic purging of data based on configuration
- Automatic load balancing between multiple instances on the same box
- Automated peaks accuracy diagnosis and resetting
- EMS GUI provides Configuration test, work-in-progress, and call event analysis features

Reporter

The Reporter provides historical data describing call traffic. It updates reports approximately every 15 minutes. You can view reports by hour, date, week, or month, or by a customized date range. You can view reports online, or download them to create customized reports.

Login Server

The Login Server authenticates customers who use GVP web-based services. The Call Status Monitor and Reporter services are accessible from the Login Server.

GVP administrators who log in to the Login Server have access to the Administration module, in addition to web-based services. Administrators can use this module to create services, manage services, and manage customer service access. The Administration module provides the flexibility to customize a customer’s service access, and enable independent releases/sales/deployment of the individual services.

Network Monitor

The Network Monitor is a GUI-controlled utility that analyzes the performance of individual servers comprising a GVP installation.

The Network Monitor queries servers at a regular interval. When the Network Monitor is active, it queries the EMS NetMon database for the server list. For each server, the Network Monitor determines whether the server is connected to the network, whether it is active, and whether it can return a valid XML page. The Network Monitor then updates the NetMon database and returns a server report to the GUI.

Dialogic Installer

The Dialogic Installer enables you to install the Dialogic software.

Note: The Dialogic Installer is used for Windows installations only when installing VCS.

IP Call Manager Components

IP Call Manager (IPCM) consists of Resource Manager with SIP Session Manager, or Resource Manager with H.323 Session Manager. The IPCM uses an in-memory database.

Resource Manager

Resource Manager (RM) maintains resource states for IPCS and Media Gateway resources. The RM dynamically maintains the status of each IPCS and Media Gateway resource (in use or available, healthy or not healthy). The RM can use a round-robin algorithm to perform load balancing of the IPCS resources, or it can select the IPCS resource based on specific feature requirements.

SIP Session Manager

SIP Session Manager (SSM) acts as a SIP Proxy to relay SIP messages between a Media or Signaling Gateway and IPCS. When a new call arrives at the SSM, the SSM fetches the application profile from the EMPS based on the dialed number or URI. The RM helps the SSM to route the call to an IPCS based on the application profile requirement. When the call is disconnected, the SSM informs the RM to free the IPCS resource.

H.323 Session Manager

The H.323 Session Manager (HSM) acts as an H.323 Proxy. It processes H.323 messages received from a Media or Signaling Gateway, and forwards equivalent SIP messages to IPCS. When a new call arrives at the HSM, the RM helps the HSM to route the call to an IPCS, based on the application profile requirement. When the call is disconnected, the HSM informs the RM to free the IPCS resource.

Portal

The GVP Portal is a website links to all web-based user interfaces in a GVP deployment. These user interfaces include:

- Provisioning
- Network Monitor
- Unified Login
- Element Management System GUIs

For instructions on how to use the Portal, see the *Genesys Voice Platform 7.6 Reference Manual*.

ASR Log Manager

The ASR Log Manager (ASRLM) is a centralized entity that initiates and monitors ASR Log transfers between the various SWMS servers, and the ASR Log Server.

ASR Log Server

The ASR Log Server (ASRLS) is an entity that parses transferred ASR Log files, and distributes them to different customers. It has a web interface enabling customers and administrators to view, and download the logs and wave captures. The web interface is accessible through the Unified Login Server for security reasons.

ASR Log Agent

The ASR Log Agent (ASRLAGT) should reside on the speech server. It uses PageCollector to transfer ASR logs and utterances to the ASR Log Server machine when initiated by ASR Log Manager.

Developer’s Edition IP Communication Server

The IPCS handles calls through Voice over IP (VOIP). The IPCS parses, interprets, and executes the VoiceXML commands in the XML documents served by the web server. The IPCS also integrates with TTS and ASR software through the MRCP standard.

Developer's Edition CTI Simulator

The CTI Simulator is a tool to assist application developers in testing Universal Routing Server (URS) controlled voice applications on GVP: DE (In-Front-of-the-Switch). The CTI Simulator allows application developers to simulate, and test URS controlled voice applications on GVP: DE without the need of the Genesys Call Router Framework.

Web Server

Communication between the web server and GVP is analogous to the desktop web browser model. In a standard web-based application, servers issue instructions to desktop browsers using HTML. The browser responds by rendering a page on a computer display, and establishing links to other pages on the Web. When you click a link, the browser issues a request to the designated URL, which results in the retrieval and rendering of another web page. When the page or its contents change, the next request from any browser retrieves the changed page, as illustrated in Figure 7.

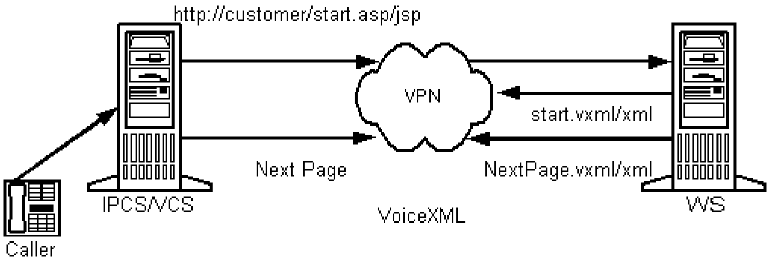


Figure 7: Communication Path Between IPCS/VCS and Web Server

Requests and information exchanged on GVP are handled in a similar fashion, but the markup language is VoiceXML instead of HTML. The IPCS/VCS has a VoiceXML-enabled web client that retrieves pages from web servers. Voice applications are generally developed as Active Server Pages (ASPs) or Java Server Pages (JSPs) that render and deliver instructions in VoiceXML form.

The IPCS/VCS parses the VoiceXML and affects:

- Call handling (answering, bridging, and disconnecting calls).
- Media management (plays greetings, prompts, and messages using cached voice files and text-to-speech).
- Caller input (collects touch-tone digits, and performs speech recognition).

VoiceXML enables a voice application to drive an interaction with a caller in the same way that the application would interact with a desktop web browser to render a screen, and react to keyboard or mouse input. As with the desktop browser, any changes to the voice application software at the web server become effective the next time a page is requested.

Caching

The VoiceXML interpreter context, like visual browsers, can use caching to improve performance in fetching documents and other resources; audio/video recordings (which can be quite large) are as common to VoiceXML documents as images are to HTML pages. In a visual browser, it is common to include end user controls to update or refresh content that is perceived to be stale. This is not the case for the VoiceXML interpreter context, since it lacks equivalent end user controls. Therefore, enforcement of cache refresh is at the discretion of the document through appropriate use of the `maxage` and `maxstale` attributes.

Caching is typically used with large, multi-tenant GVP implementations. GVP can perform the caching itself, or, you can add another server—a caching appliance, or a web proxy server. The benefit of having an external caching server is, for example, if you have a site with ten GVP servers and an audio file expires, each server must go fetch a new copy of the audio file. If there is an external cache server, fetching a new copy of the audio file occurs only once. Also, the external cache servers typically have very robust cache management tools to purge and refresh content.

Third-Party Software

The following section describes the third-party software used in conjunction with GVP.

Automatic Speech Recognition

GVP uses MRCP speech-recognition technology to incorporate Automatic Speech Recognition (ASR) for use in voice applications. The GVP ASR architecture is economically scalable as the volume of the calls requiring speech recognition rises, and new voice applications are acquired.

Text-to-Speech

GVP uses MRCP speech-recognition technology to incorporate Text-to-Speech (TTS) for use in voice applications.

Dialogic

VCS uses Dialogic software to provide telephony T1/E1 telephony access, and media operations.

Dialogic HMP

Used by IPCS Enhanced Media Services to provide RTP streaming and media operations.

Alcatel Media Server

Used by IPCS Enhanced Media Services to provide RTP streaming and media operations.

New in This Release

The 7.6 release of GVP provides the following additional or changed functionality:

- Uses a native RTP stack that enables transcoding and bidirectional recording.

  There is no longer any distinction between Basic and Enhanced media services. There is a single media control process.

  For more information about the new codecs that are supported for transcoding and recording, see the *Genesys Voice Platform 7.6 Reference Manual.*
- Supports Nuance 5.0 Speech Server with Nuance Recognizer 9.0 (for ASR) and Nuance RealSpeak 4.5 (for TTS).
- Provides ASR Log Manager system support for Nuance Recognizer 9.0.
- Provides access for the VoiceXML application to additional SIP Header fields, such as `P-Asserted-Identity` and `Call-Id`. IPCS propagates the values it receives for these headers in incoming SIP `INVITE` messages. For more information about using SIP Header information in the voice application, see the *Genesys Voice Platform 7.6 VoiceXML 2.1 Reference Manual.*
- Supports billing for outbound calls over H.323, by enabling the DNIS of an incoming call to be prefixed to the called party number of the related outgoing call. To provision this feature, see the information about the `PrefixDNISonOutbound` parameter in the *Genesys Voice Platform 7.6 Reference Manual.*
- Improves EMPS usability, including an enhanced Data Migration Tool.
- Provides support in Studio for GVP platform enhancements.

- Supports Genesys Management Layer (Local Control Agent [LCA], Solution Control Server [SCS], and Solution Control Interface [SCI]). For more information about integrating GVP with Genesys Management Framework, see Chapter 25 on page 441.
- Support for Dialogic System Release 6.0 System Update 174 for Dialogic Boards.
- Provides improved performance on Solaris T1 Ultra Sparc processors.
- Discontinues support for Windows 2000.

Chapter

2 Prerequisites and Planning

This chapter describes the prerequisites and planning considerations for deploying Genesys Voice Platform (GVP) 7.6. It includes information about required hardware and software.

This chapter contains the following sections:

GVP Installation CDs

The Genesys Voice Platform (GVP) components are contained on the following CDs:

- Genesys Voice Platform: Base Software
- Genesys Voice Platform: Developer’s Edition
- Genesys Voice Platform: Cisco Queue Adapter
- Genesys Voice Platform: Reporting and Monitoring
- Genesys Voice Platform: Dialogic SR 6.0
- Genesys Voice Platform: H.323 Call Manager
- Genesys Voice Platform: SIP Call Manager
- Genesys Voice Platform: ASR Log Manager
- Genesys Voice Platform: MRP SMP Integrator

Windows Prerequisites

Table 3 summarizes the hardware and software requirements for GVP 7.6 deployments on Windows hosts.

Note: Genesys recommends that you review "Windows Host Setup" on page 68 and "Windows Deployment Task Summaries" on page 75 before you install any software.

Table 3: Hardware and Software Requirements for Windows

Category	Requirement	Comment
	Hardware Requirements	
GVP servers	See the *Genesys Hardware Sizing Guide*.	Genesys strongly recommends that all IP Communication Server (IPCS) hosts have two Network Interface Cards (NICs). This enables the call audio (Session Initiation Protocol [SIP]/Real-time Transport Protocol [RTP]) data to be sent to a separate network that is optimized to efficiently transfer SIP/RTP data to Media Gateways.
TDM Telephony integration	To use TDM Telephony in your deployment, you must install Dialogic boards on the Voice Communication Server (VCS). For a list of the supported Dialogic boards, see the *Genesys Supported Media Interfaces Reference Manual*.	It is your responsibility to obtain and install this hardware.

Table 3: Hardware and Software Requirements for Windows (Continued)

Category	Requirement	Comment
Software Requirements		
Operating System on GVP servers (Mandatory)	For Genesys Voice Platform 7.6: • Microsoft Windows Server 2003, Standard Edition, Service Pack 2 • Microsoft Windows Server 2003, Enterprise Edition, Service Pack 2 • Microsoft Windows Server 2008, Standard and Enterprise Editions • Microsoft Windows Server 2008 R2, Standard and Enterprise Editions For Genesys Voice Platform: Developer's Edition [GVP: DE] only: • Microsoft Windows XP, 32-bit	**Warning!** Before you begin the GVP installation, make sure that all of the latest Windows 2003 or 2008 patch levels are installed.
OS supporting components (Mandatory)		
• Database access	• Microsoft Data Access Component (MDAC) 2.7 SP1 Refresh	You can download this component from the Microsoft download website.
• Extensible Markup Language (XML)	• Microsoft Extensible Markup Language (XML) 4.0 SP2 (or higher) Parser and Software Development Kit (SDK)	You can download this component from the Microsoft download website.

Table 3: Hardware and Software Requirements for Windows (Continued)

Category	Requirement	Comment
• Microsoft Internet Information Server (IIS) components	Internet Information Server (IIS) 5, IIS 6, or IIS 7. • IIS 6 Management Compatibility (for IIS 7, IIS 7.5) • IIS 7 Administration Pack (for IIS 7) • Common Files • File Transfer Protocol (FTP) Server • Internet Information Server Snap-In • World Wide Web Server	
• Management and Monitoring Tools	• Simple Network Management Protocol (SNMP) Service	
• Specific services and settings	You must configure certain specific services and settings on each host before you install GVP.	For more information, see “Windows Services and Settings” on page 81.
Dialogic boards (Mandatory, for VCS only)	Dialogic SR 6.0 Service Update 174 (SU174) This software includes Dialogic Global Call Protocols 4.3.	The software is available on the GVP Dialogic SR 6.0 CD. For information about installing the software, see Chapter 8, “Installing Dialogic,” on page 173.
Directory Server for the Element Management Provisioning System (EMPS) (Mandatory)	One of the following: • OpenLDAP—An open source implementation of Lightweight Directory Access Protocol (LDAP) that comes packaged with the EMPS software.	If you use OpenLDAP, you do not need to obtain any other third-party LDAP software.

Table 3: Hardware and Software Requirements for Windows (Continued)

Category	Requirement	Comment
	• SunOne Directory Server—SunOne/iPlanet Directory Server 5.1 SP 4, or SunOne/iPlanet Directory Server version 5.2 plus Patch 117667-02 **Note:** OpenLDAP is recommended for small-sized deployments of GVP. For medium-sized and large-sized deployments, Genesys recommends that you use SunOne Directory Server.	It is your responsibility to obtain the software and the appropriate licenses. For information about installing and configuring the SunOne Directory Server software on the EMPS host, see "Preparing the SunOne Directory Server" on page 88.
Database Server and Client (Mandatory if your deployment includes EMS Reporting components or OBN Manager)	One of the following types of database server: • Microsoft SQL Server 2000 SP3, U.S. English locale • Microsoft SQL Server 2005, U.S. English locale You may need to use more than one SQL Server, depending on the anticipated network activity and redundancy requirements.	It is your responsibility to obtain the software and the appropriate licenses. The SQL Server hosts tables for the EMPS, Element Management System (EMS), Outbound Notification (OBN) Manager, and processing components. You can install the actual SQL Server on any host, but Genesys recommends installing it on an EMS Reporting host, to minimize network traffic. You must prepare the database server and clients for GVP database access. For information about the required preparations, see "Preparing Database Connectivity for Windows" on page 93.
Web browser (Mandatory)	Microsoft Internet Explorer (IE) 6.0 SP1 or 7.0	
Java Runtime (Mandatory)	Java Runtime Environment (JRE) 1.5.x or 1.6.x	You can download JRE from the Sun MicroSystem website. You must install Java Runtime on each machine from which the EMPS GUI will be accessed.

Table 3: Hardware and Software Requirements for Windows (Continued)

Category	Requirement	Comment
HMP IPCS enhanced media (Optional)	Dialogic Host Media Processing (HMP) release 3.0 SU 150	It is your responsibility to obtain and install this software.
Automatic Speech Recognition (ASR) (Optional) GVP provides a Media Resource Control Protocol (MRCP) ASR-compliant interface.	Genesys has validated the following third-party software: • Nuance SpeechWorks Media Server (SWMS) 3.1.x with Nuance OpenSpeech Recognizer (OSR) 3.0.x • Nuance 5.0 Speech Server with Nuance Recognizer 9.0 • IBM WebSphere Voice Server (WVS) 5.1.3 ASR or higher	It is your responsibility to obtain the software and the appropriate licenses. For additional speech information, see the *Genesys Supported Media Interfaces Reference Manual*.
Text-to-Speech (TTS) (Optional) GVP provides an MRCP TTS-compliant interface.	Genesys has validated the following third-party software: • Nuance SpeechWorks Media Server (SWMS) 3.1.x with Nuance RealSpeak TTS 4.0 • Nuance 5.0 Speech Server with Nuance RealSpeak 4.5 • IBM WebSphere Voice Server (WVS) 5.1.3 TTS or higher, with IBM Text-to-Speech Connector	It is your responsibility to obtain the software and the appropriate licenses. For additional speech information, see the *Genesys Supported Media Interfaces Reference Manual*.
IVR Server (Optional)	Genesys Interactive Voice Response (IVR) Server release 7.2 or higher **Note:** To support the UUID feature, you must install IVR Server 7.5 or higher.	Required if you plan to use Genesys Framework in your deployment.

Table 3: Hardware and Software Requirements for Windows (Continued)

Category	Requirement	Comment
SNMP Manager (Mandatory)	Any SNMP management software	For example, HP OpenView.
Recommended third-party software	• Softphone such as eStara or PingTel (for testing GVP: DE) • pcAnywhere version 10.0 or higher • Adobe Acrobat Reader 6.0 or higher • WinZip • Etheral for debugging • Any Third Party licensing software	

Solaris Prerequisites

Table 4 summarizes the hardware and software requirements for GVP 7.6 deployments on Solaris hosts.

Note: Genesys recommends that you review “Solaris Host Setup” on page 70 and “Solaris Deployment Task Summaries” on page 221 before you install any software.

Table 4: Hardware and Software Requirements for Solaris

Category	Requirement	Comment
Hardware Requirements		
GVP servers	See the *Genesys Hardware Sizing Guide.*	Genesys strongly recommends that all IP Communication Server (IPCS) hosts have two Network Interface Cards (NICs). This enables the call audio (Session Initiation Protocol [SIP]/Real-time Transport Protocol [RTP]) data to be sent to a separate network that is optimized to efficiently transfer SIP/RTP data to Media Gateways.

Table 4: Hardware and Software Requirements for Solaris (Continued)

Category	Requirement	Comment
Software Requirements		
Operating System on GVP servers (Mandatory)	For information about the version of SPARC Solaris that is supported with GVP 7.6, see *Genesys Supported Operating Systems and Databases*.	**Warning!** Before you begin the GVP installation, make sure that all of the latest Solaris patches are installed.
Directory Server for the Element Management Provisioning System (EMPS) (Mandatory)	One of the following: • OpenLDAP—An open source implementation of Lightweight Directory Access Protocol (LDAP) that comes packaged with the EMPS software.	If you use OpenLDAP, you do not need to obtain any other third-party LDAP software.
	• SunOne Directory Server—SunOne/iPlanet Directory Server 5.1 SP 4, or SunOne/iPlanet Directory Server version 5.2 plus Patch 117667-02 **Note:** OpenLDAP is recommended for small-sized deployments of GVP. For medium-sized and large-sized deployments, Genesys recommends that you use SunOne Directory Server.	It is your responsibility to obtain the software and the appropriate licenses. For information about installing and configuring the SunOne Directory Server software on the EMPS host, see “Preparing the SunOne Directory Server” on page 225.

Table 4: Hardware and Software Requirements for Solaris (Continued)

Category	Requirement	Comment
Database Server and Client (Mandatory if your deployment includes EMS Reporting components or OBN Manager)	One of the following types of database server: • Oracle Database 9i R2 Server with 32-bit Client Libraries • Oracle Database 10g Standard Edition Server with 32-bit Client Libraries	It is your responsibility to obtain the software and the appropriate licenses. The Oracle Server hosts tables for the EMPS, Element Management System (EMS), Outbound Notification (OBN) Manager, and processing components. Genesys recommends that you install the Oracle database server on the EMS Reporting/OBN Manager host, and the Oracle client on the EMPS host. You must prepare the database server and clients for GVP database access. For information about the required preparations, see "Preparing the Oracle Database Server and Clients" on page 231.
Web browser (Mandatory)	Mozilla Internet browser version 1.6 or higher for Sun Java Desktop System (Solaris Operating System Edition)	To view the EMPS GUI in the Mozilla browser, your monitor resolution must be at least 1024 x 768. In the Mozilla browser, to view any link that provides an XML string, right-click in the page that is displayed in the browser window, and then select `View Page Source`.
Java Runtime (Mandatory)	Java Runtime Environment (JRE) 1.5.x or 1.6.x	You can download JRE from the Sun MicroSystem website. You must install Java Runtime on each machine from which the EMPS GUI will be accessed.
HMP IPCS enhanced media (Optional)	Dialogic Host Media Processing (HMP) release 3.0 SU 150	It is your responsibility to obtain and install this software.

Table 4: Hardware and Software Requirements for Solaris (Continued)

Category	Requirement	Comment
Automatic Speech Recognition (ASR) (Optional) GVP provides a Media Resource Control Protocol (MRCP) ASR-compliant interface.	Genesys has validated the following third-party software: • Nuance SpeechWorks Media Server (SWMS) 3.1.x with Nuance OpenSpeech Recognizer (OSR) 3.0.x • Nuance 5.0 Speech Server with Nuance Recognizer 9.0 • IBM WebSphere Voice Server (WVS) 5.1.3 ASR or higher	It is your responsibility to obtain the software and the appropriate licenses. For other speech information, see the *Genesys Supported Media Interfaces Reference Manual*. **Note:** If the IPCS uses Intel HMP Enhanced Media Services or Alcatel MRF Enhanced Media Services with SWMS 3.1.13 as the MRCP ASR/TTS Server, you must specify certain parameters in the configuration file (see “Special Setting for Enhanced Media Services” on page 282).
Text-to-Speech (TTS) (Optional) GVP provides an MRCP TTS-compliant interface.	Genesys has validated the following third-party software: • Nuance SpeechWorks Media Server (SWMS) 3.1.x with Nuance RealSpeak TTS 4.0 • Nuance 5.0 Speech Server with Nuance RealSpeak 4.5 • IBM WebSphere Voice Server (WVS) 5.1.3 TTS or higher, with IBM Text-to-Speech Connector	
IVR Server (Optional)	Genesys Interactive Voice Response (IVR) Server release 7.2 or higher **Note:** To support the UUID feature, you must install IVR Server 7.5 or higher.	Required if you plan to use Genesys Framework in your deployment.
SNMP Manager (Mandatory)	Any SNMP management software	For example, HP OpenView.

Antivirus Software

Antivirus software can potentially impact system performance and may affect call response time. In an ideal deployment, antivirus software would be disabled in GVP systems. However, Genesys understands the need to have antivirus protection on servers. Genesys therefore recommends, at a minimum, that you exclude the GVP directory from virus scanning, and schedule system scans to occur at times when traffic is low.

Also, be aware that antivirus software may interfere with the installation of GVP during initial deployment. Make sure that the server is not running antivirus software, or any other third-party software, during installation.

Host Setup

GVP provides considerable flexibility in combining various components on one host; however, the following restrictions apply:

- You must first install the Voice Platform Common component on all hosts in the GVP network when performing a manual installation. Voice Platform Common is installed automatically when using the GVP Deployment Tool (GDT) to deploy GVP for Windows installations, or when using the Launcher for Solaris installations.
- Genesys recommends that the EMPS be installed and running next, prior to the installation of any other GVP component with the exception of Common.
- You must also install the following GVP components on all Solaris hosts:
    - Voice Platform SNMP
    - Voice Platform Third-Party Apache Solaris
- VCS and IPCS cannot be installed in the same GVP installation.
- You must install the IPCS and Dialogic HMP software on the same host.
- The VCS operates independently of, and does not register with, IP Call Manager (IPCM).
- For IP Call Manager (IPCM), the following considerations apply:
    - The SIP Session Manager (SSM) and H.323 Session Manager (HSM) do not share IPCS and Media Gateway resources.
    - If you plan to use both SIP and H.323 in your deployment, install SSM and HSM on separate hosts.
    - Do not install IPCM components on the IPCS host.
- You must install the Voice Platform TTS component on the VCS host only if you are performing a manual installation. If you are using the GDT, you will be prompted to install TTS.
- You can install OBN Manager on the EMS Reporting host. There, it will share the SQL/Oracle Server database installation with EMS Reporting components.

  However, if the call volume for OBN Manager will be high, you must install it on its own machine and that must also have an SQL/Oracle Server database installation. In this case, you must install SQL/Oracle Server before OBN Manager, and this SQL/Oracle Server database installation must be dedicated to OBN Manager.

- You can install the Bulk Provisioning Tool (a Windows-only component) on any host or desktop; however, it is not a Web-based tool, and therefore it can be accessed only from the machine on which it is installed.
- You can install MRP SMP Integrator on a stand-alone machine that has Common, SNMP, and Apache installed, or it can be installed and co-exist on a machine where other GVP components, such as IPCM, are installed.

The following sections describe the host setup that Genesys recommends for Windows and Solaris lab testing.

Windows Host Setup

Genesys recommends the following Windows host setup for lab testing.

Note: Your exact host setup will be determined by various factors—for example, high availability, number of ports, and so on. Consider the following host setups as a starting point for planning purposes.

Host 1: EMPS

Software provided by customer:

- For Windows 2003 Server, SunOne/iPlanet Directory Server—required only if you do not use OpenLDAP (which is bundled with EMPS)
- Microsoft SQL Server 2000 SP3 or Microsoft SQL 2005 Client Network Libraries

Software provided by Genesys:

- Voice Platform Common
- Voice Platform Element Management Provisioning System
- Voice Platform Dispenser

Host 2: EMS Runtime

Software provided by Genesys:

- Voice Platform Common
- Voice Platform IVR Server Client
- Voice Platform Bandwidth Manager
- Voice Platform Policy Manager
- (Optional) ASR Log Manager
- (Optional) ASR Log Server*
- (Optional) Voice Platform Cisco Queue Adapter

*If more than one EMS Runtime host is available, install the ASR Log Manager and ASR Log Server on separate hosts.

Host 3: EMS Reporting

Software provided by customer:

- Microsoft SQL Server 2000 SP3

Software provided by Genesys:

- Voice Platform Common
- Voice Platform EventC
- Voice Platform Login Server
- Voice Platform Reporter
- Voice Platform Call Status Monitor
- Voice Platform Network Monitor
- Voice Platform OBN Manager

Host 4 (for TDM telephony option): VCS

Hardware provided by customer:

- Dialogic boards

Software provided by Genesys:

- Dialogic System Release
- Voice Platform Common
- Voice Platform Voice Communication Server
- Voice Platform TTS

Host 4 (for IP telephony option): IPCS

Software provided by customer:

- (Optional) Dialogic HMP

Software provided by Genesys:

- Voice Platform Common
- Voice Platform IP Communication Server
- Voice Platform TTS

Host 5: IPCM

Software provided by Genesys:

- Voice Platform Common
- Voice Platform Resource Manager
- Voice Platform SIP Session Manager or Voice Platform H.323 Session Manager

Host 6: Third-Party MRCP Speech Server

Software provided by customer:

- ASR MRCP server
- TTS MRCP server

Software provided by Genesys:

- (Optional) ASR Log Agent

Solaris Host Setup

Genesys recommends the following Solaris host setup for lab testing.

> Note: Your exact host setup will be determined by various factors—for example, high availability, number of ports, and so on. Consider the following host setups as a starting point for planning purposes.

System 1: EMPS

Software provided by customer:

- SunOne/iPlanet Directory Server—required only if you do not use OpenLDAP (which is bundled with EMPS)
- Oracle 9i R2 or 10g Standard Edition 32-bit Client Software

Software provided by Genesys:

- Voice Platform SNMP
- Voice Platform Third-Party Apache Solaris
- Voice Platform Common
- Voice Platform Element Management Provisioning System
- Voice Platform Dispenser

System 2: EMS Runtime

Software provided by Genesys:

- Voice Platform SNMP
- Voice Platform Third-Party Apache Solaris
- Voice Platform Common
- Voice Platform IVR Server Client
- Voice Platform Bandwidth Manager
- Voice Platform Policy Manager
- Voice Platform MRP SMP Integrator
- (Optional) Voice Platform Cisco Queue Adapter

System 3: EMS Reporting

Software provided by customer:

- Oracle 9i R2 or 10g Standard Edition 32-bit Server

Software provided by Genesys:

- Voice Platform Third-Party SNMP Solaris
- Voice Platform Third-Party Apache Solaris
- Voice Platform Common
- Voice Platform EventC
- Voice Platform Login Server
- Voice Platform Reporter
- Voice Platform Call Status Monitor
- Voice Platform Network Monitor
- Voice Platform OBN Manager

System 4: IPCS

Software provided by Genesys:

- Voice Platform SNMP
- Voice Platform Third-Party Apache Solaris
- Voice Platform Common
- Voice Platform IP Communication Server
- Voice Platform TTS (explicit installation is required only for Basic Media Services)

System 5: IPCM

Software provided by Genesys:

- Voice Platform SNMP
- Voice Platform Third-Party Apache Solaris
- Voice Platform Common
- Voice Platform Resource Manager
- Voice Platform SIP Session Manager or Voice Platform H.323 Session Manager

System 6: Third-Party MRCP Speech Server

Software provided by customer:

- ASR MRCP server
- TTS MRCP server

Part

2 Windows Installation

Part Two of this manual describes the installation of Genesys Voice Platform (GVP) on the Windows operating system using the GVP Deployment Tool.This information appears in the following chapters:

- Chapter 3, "Windows Deployment Task Summaries," on page 75
- Chapter 4, "Preparing Your Windows Environment," on page 81
- Chapter 5, "GVP Deployment Tool," on page 97
- Chapter 6, "Installing GVP Components Using the GDT," on page 111
- Chapter 7, "Installing GVP: DE with the GVP Deployment Tool," on page 161
- Chapter 8, "Installing Dialogic," on page 173
- Chapter 9, "Installing the Bulk Provisioning Tool," on page 179
- Chapter 10, "Post-Installation Activities on Windows Hosts," on page 181
- Chapter 11, "Maintaining GVP," on page 201

Chapter

3 Windows Deployment Task Summaries

This chapter provides summaries of various deployment tasks for a Genesys Voice Platform (GVP) installation on Windows, and provides links to detailed information about the required tasks.

This chapter contains the following sections:

Note: Genesys does not recommend that you install its components through a Microsoft Remote Desktop connection. Instead, you should perform the installation locally.

Installing GVP Using the GDT

Table 5 summarizes the steps to install GVP in a Windows environment, using the GVP Deployment Tool (GDT).

Table 5: Task Summary—Installing GVP with the GDT

Objective	Related Procedures and Actions
1. Plan the deployment.	For specific restrictions and recommendations to consider, see “Host Setup” on page 67.
2. Prepare your environment.	**1.** Install and configure third-party hardware and software. • If you are using Automatic Speech Recognition (ASR) and/or Text-to-Speech (TTS), install the third-party Media Resource Control Protocol (MRCP) speech server host(s). For more information, see your MRCP vendor’s documentation. • If your deployment will include EMS Reporting and/or OBN Manager, install the Microsoft SQL Server software and Client libraries, and prepare the EMS Reporting and EMPS hosts for database connectivity. For more information, see Table 11, “Preparing the Microsoft SQL Server and Clients,” on page 94. • If your deployment will use Voice Communication Server (VCS) (for TDM telephony), install the Dialogic boards. For more information, see the Dialogic documentation. For information about installing and configuring the Dialogic software, see “Installing Dialogic Software” on page 173. • If you are using the SunOne Directory Server for the EMPS, install and configure the directory server on the EMPS host. For more information, see “Preparing the SunOne Directory Server” on page 88. For more information about prerequisite software, see “Windows Prerequisites” on page 58. **2.** Configure the required Windows services and settings on the systems that will host GVP components. For more information, see “Windows Services and Settings” on page 81. **3.** Stop antivirus software that may be running on systems that will host GVP components.
3. Obtain the GVP software.	For information about the GVP software CDs, see “GVP Installation CDs” on page 57. Ensure that the software is accessible to the GDT.
4. Obtain server and database information.	See the Prerequisites item for Using the GVP Deployment Wizard to install GVP components (Windows only), page 113. During installation, you will need to provide information such as fully qualified domain names (FQDNs) of GVP and non-GVP servers, database names, and database user names and passwords.

Table 5: Task Summary—Installing GVP with the GDT (Continued)

Objective	Related Procedures and Actions
5. Install the GVP Deployment Agent (GDA) on all systems that will host GVP components.	See Installing the GVP Deployment Agent, page 112.
6. Run the GDT installation wizard to install GVP components, with basic configuration.	See Using the GVP Deployment Wizard to install GVP components (Windows only), page 113.
7. Verify or modify GVP server configurations in the EMPS.	See the various GVP configuration chapters in Part 4: “GVP Configuration” on page 287.
8. Depending on the features you have installed, perform post-installation activities.	• Configure ASR/TTS (see “Enabling MRCP ASRand TTS” on page 391). • Create the database schemas for EMS Reporting and OBN Manager (see “Creating the Microsoft SQL Server Databases” on page 181). • For EMS Reporting, modify file permissions as required (see “Setting File Permissions for EMS Reporting” on page 185). • Configure Unified Login (see “Enabling Unified Login” on page 186). • Configure Network Monitor (see “Enabling Network Monitor” on page 194). • Configure IP Call Manager (IPCM) (see “Enabling IPCM” on page 403). • Configure the ASR Log Manager System (see “Enabling the ASR Log Manager System” on page 425).
9. Start or restart WatchDog on all GVP servers.	See Starting/Restarting GVP in Normal mode (Windows), page 198.
10. Install the Bulk Provisioning Tool on any host or desktop (optional).	See Chapter 9 on page 179.

Installing GVP Manually

Table 6 summarizes the steps to perform a manual installation of GVP in a Windows environment.

Table 6: Task Summary—Installing GVP Manually on Windows

Objective	Related Procedures and Actions
1. Plan the deployment and prepare the environment.	See Table 5 on page 76, Steps 1 through 4.
2. Install Common, EMPS, and Dispenser on the EMPS host.	See “Manually installing Common (Windows)” on page 506, “Manually installing EMPS (Windows)” on page 508, and “Manually installing Dispenser (Windows)” on page 512.
3. If your deployment will include EMS Reporting and/or OBN Manager, create the EMPS database schema.	See “Setting Up the Databases” on page 182.
4. Start the EMPS WatchDog in safe mode.	See “Starting/Restarting GVP in Safe mode (Windows)” on page 199.
5. Install the IPCS/VCS and other GVP components, as required for your deployment. You must install Common on every GVP server.	See Appendix B, “Manual Installation on Windows” on page 505.
6. Perform post-installation configuration and other activities.	See Table 5 on page 76, Steps 7 through 10.

Maintaining GVP

Table 7 summarizes the activities to maintain your GVP deployment.

Table 7: Task Summary—Maintaining GVP

Objective	Related Procedures and Actions
Upgrade to GVP 7.6.	**1.** Upgrade the GDA (see Upgrading the GDA using the GDT, page 202). **2.** If required, uninstall the existing EMPS before installing the new one (see Installing a new EMPS on an existing EMPS server (Windows), page 210). **3.** Upgrade GVP components (see Upgrading GVP using the GDT, page 202). **4.** Restart WatchDog on the upgraded servers (see Starting/Restarting GVP in Normal mode (Windows), page 198).
Install a 7.6.x hot fix.	**1.** Upgrade the GDA (see Upgrading the GDA using the GDT, page 202). **2.** Upgrade the GVP component(s) (see Installing a hot fix using the GDT, page 211). **3.** If required, perform related upgrades, such as database updates or upgrades of associated components (such as Common). For any required related activities, see the applicable release notes and release advisories. **4.** Restart WatchDog on the upgraded servers (see Starting/Restarting GVP in Normal mode (Windows), page 198).

Table 7: Task Summary—Maintaining GVP (Continued)

Objective	Related Procedures and Actions
Repair a GVP server.	**1.** Upgrade the GDA (see Upgrading the GDA using the GDT, page 202). **2.** Repair the server(s) (see Repairing a GVP server using the GDT, page 213).
Uninstall GVP components.	**1.** Upgrade the GDA (see Upgrading the GDA using the GDT, page 202). **2.** Uninstall the GVP component(s) in one of the following ways: • Using the GDT **i.** Uninstall the component(s) (see Uninstalling GVP components using the GDT, page 214). **ii.** Uninstall the GDA (see Uninstalling the GVP Deployment Agent, page 216). • Manually (see Uninstalling GVP components manually (Windows), page 216). **3.** For a VCS deployment, uninstall Dialogic (see Uninstalling Dialogic, page 217).

Chapter

4 Preparing Your Windows Environment

This chapter describes the prerequisites to prepare hardware and software for Genesys Voice Platform (GVP) 7.6 deployments on Windows hosts.

This chapter contains the following sections:

For information about all the hardware and software prerequisites for Windows deployments, see “Windows Prerequisites” on page 58.

Windows Services and Settings

Table 8 summarizes the required services and settings you must configure on each GVP host. You must configure these settings before you install GVP.

Warning! When you name a computer, do not use the underscore (_) character, even though Windows Setup permits this. Using the underscore character causes serious problems with several web services that the GVP software uses.

Table 8: Specifying Windows Services and Settings

Objective	Related Procedures and Actions

Modify Windows OS settings:	**On Windows 2008 only:**
	If you are installing VCS and Dialogic, disable Pysical Address Extentions (PAE) by issuing the following commands in the CLC:
	`C:\bcdedit /set nx OptOut`
	`C:\bcdedit /set pae ForceDisable`
	Then, restart the server.

Enable or disable the required services, and set service start modes.	For the required Services settings, see Table 9 on page 83.
Specify the settings that are required for the web server to function correctly:	
• If you use Recording, change the Internet Information Server (IIS) 6.0 default limit that has been imposed on the amount of data that can be sent in a Hypertext Transfer Protocol (HTTP) `POST`.	Change the `AspMaxRequestEntityAllowed` setting in the `Metabase.xml` file. For more information, see Enabling longer call recordings (Windows), page 84.
• If you use the URLScan security tool to restrict the types of HTTP requests that IIS will process, modify the filter settings.	Enable the `AllowDotInPath` and ASP requests settings. For more information, see Modifying URLScan filter settings for GVP (Windows), page 84.
• Specify the Multipurpose Internet Mail Extensions (MIME) type settings.	Define a new MIME type to process `.vox` files. For more information, see Specifying MIME Type settings for audio files (Windows), page 85.
Specify the required Internet Explorer (IE) settings. This needs to be done on all machines that access GVP GUIs.	Set the Internet Options for LAN Connections, Privacy, and Security as described in Setting Internet Explorer options for the GVP GUIs (Windows), page 86.
Specify the recommended system and system performance settings.	• Configuring system settings (Windows), page 87. • Configuring system performance settings (Windows), page 88.

Windows Services

Table 9 lists the Windows Services settings that are required on each computer.

Table 9: Windows Services

Name	Startup Type
Alerter	Disabled
Application Management	Manual
Clipbook	Manual
Com + Event System	Manual
Computer Browser	Disabled
DHCP Client	Automatic
Event Log	Automatic
FTP Publishing Services	Automatic
IIS Admin Service	Automatic
License Logging	Disabled
Messenger	Disabled
Net Logon	Manual
Network DDE	Manual
NT LM Security Support Provider	Manual
Plug and Play	Automatic
Protected Storage	Automatic
Remote Procedure Call (RPC) Locator	Manual
Remote Procedure Call (RPC)	Automatic
Server	Automatic
SNMP Service	Automatic
SNMP Trap Service	Manual
System Event Notification	Automatic
Task Scheduler	Automatic
TCP/IP NetBIOS Helper	Automatic
Telephony	Manual

Table 9: Windows Services (Continued)

Name	Startup Type
Uninterruptible Power SupplyPS	Manual
Workstation	Automatic
World Wide Web Publishing Service	Automatic

Web Services Settings

This section provides the detailed procedures to enable the web server and browser to perform their functions in your GVP deployment.

Procedure: Enabling longer call recordings (Windows)

Purpose: To increase the amount of data that can be sent in an HTTP `POST` with IIS 6.0.

You do not need to stop IIS in order to make this change.

Start of procedure

1. Open IIS.
2. Right-click the server, and then select `Properties`.
3. Select the `Enable Direct Metabase Edit` check box, and then click `OK`.
4. Open the `MetaBase.xml` file, which is located in `C:\WINNT\System32\Inetsrv`.
5. Locate the line `AspMaxRequestEntityAllowed`, and change it to `524288000`.

   This enables longer recordings for each call.

End of procedure

Procedure: Modifying URLScan filter settings for GVP (Windows)

Purpose: To modify the URLScan `AllowDotInPath` and ASP requests settings so that IIS will process GVP requests.

Start of procedure

1. From the Windows `Start` menu, select `Run` and then enter `inetmgr`.
2. Select the machine name and right-click `Properties`.

   A shortcut menu appears.
3. Verify that there is a `URLScan` entry in `Master Properties > WWW Service > Edit > ISAPI Filters`.
4. Navigate to `C:\WINNT\system32\inetsrv\urlscan`, and open the `urlscan.ini` file.
5. Change the value of the `AllowDotInPath` option from `0` (zero) to `1` (one).
6. In the `Deny asp requests` section, comment out the `.asp` line.

End of procedure

Procedure: Specifying MIME Type settings for audio files (Windows)

Purpose: To set the Multipurpose Internet Mail Extensions (MIME) type for `.vox` files in IIS.

Start of procedure

1. Open `IIS`.
2. Select `Web Sites`, right-click `Default web site`, and then select `Properties`.
3. Click the `HTTP Headers` tab, and then click `MIME Types`.
4. Click `New`.
5. Define the following parameters:
   - Extension: `.vox`
   - Mime type: `audio/wav`
6. Click `OK`.

End of procedure

Procedure:
Setting Internet Explorer options for the GVP GUIs (Windows)

Purpose: To enable the GVP GUIs to display and function correctly in Internet Explorer (IE).

Perform this procedure on each host from which GVP GUIs will be accessed.

Start of procedure

1. In IE, select `Tools > Internet Options`.

   The `Internet Options` dialog box appears.
2. On the `General` tab, in the `Address` text box, enter `http://localhost:9810`.
3. Disable Proxy settings:
   a. Go to `Tools > Internet Options > Connections > LAN Settings`.
   b. Clear all check boxes.
4. Set `Privacy` to `Medium`, so that you can view the `EMPS Login` page with default IE settings:
   a. Go to `Tools > Internet Options > Privacy`.
   b. Move the Privacy setting slider to `Medium`.
5. Add all GVP IP addresses or host names to the list of trusted websites, so that the drill-down menus will work correctly in the GVP GUIs:
   a. Go to `Tools > Internet Options >Security`.
   b. Click the `Trusted sites` icon, and click `Sites`.

      The `Trusted Sites` dialog box appears.
   c. In the `Add this Web site to the zone` text box, enter the IP address or host name.
   d. Click `Add`.

End of procedure

System Settings

This section describes the system and system performance settings that Genesys recommends.

Procedure: Configuring system settings (Windows)

Purpose: To specify the required settings for Event Viewer logs, Domain Name Service (DNS) for the LAN, and Simple Network Management Protocol (SNMP) trap destinations.

Perform this procedure on each GVP server in your deployment.

Start of procedure

1. Set the Event Viewer maximum log sizes for the System log and Application log to 1024 KB, and set events to overwrite as needed:
   a. Go to `Control Panel > Administrative Tools > Event Viewer`.
   b. Right-click `System`, and select `Properties`.
   c. In the `System Properties` dialog box, set the `Maximum log size` to `1024`.
   d. Select the option to overwrite events as needed when the maximum log size is reached.
   e. Click `OK`.
   f. Repeat substeps b through e for `Application`.
2. Configure DNS settings for the LAN:
   a. Go to `Control Panel > Network Connections > Local Area Connection`, and click `Properties`.
   b. On the `General` tab of the `Local Area Connection Properties` dialog box, select `Internet Protocol (TCP/IP)`, and then click `Properties`.
   c. In the `Internet Protocol (TCP/IP) Properties` dialog box, specify the IP address settings that are required for your network.
   d. Click `OK` to exit all dialog boxes.
3. Specify the SNMP trap destinations:
   a. From the `Start` menu, select `Programs > Administrative Tools > Services`.
   b. In the right pane of the `Services` window, right-click `SNMP Service`, and then select `Properties`.
   c. In the `SNMP Service Properties` dialog box, select the `Traps` tab.
   d. From the `Community name` drop-down list, select a community name.
   e. Click `Add`.

      The name is added to the `Trap destinations` list.
   f. Click `OK`.

End of procedure

Procedure: Configuring system performance settings (Windows)

Perform this procedure on each GVP server in your deployment.

Start of procedure

1. Go to Control Panel > System > Advanced.
2. In the Performance section, click Settings.
3. The Performance Options dialog box appears.
4. Click the Advanced tab.
5. In the Processor scheduling section of the Advanced tab, select Background services.
6. Set the Virtual Memory size:
    a. In the Virtual memory section of the Advanced tab, click Change.
    The Virtual Memory dialog box appears.
    b. Select Custom size, and then set the following:
        - Initial size (MB): 1.5 times your RAM
        - Maximum size (MB): 2 times your RAM
    c. Click Set.
7. Click OK to exit all dialog boxes.
8. When prompted, restart the computer.

End of procedure

Preparing the SunOne Directory Server

If you plan to use OpenLDAP as the Directory Server for the Element Management Provisioning System (EMPS), no preparation is required.

If you plan to use SunOne/iPlanet Directory Server, you (or your system administrator) must install the software on the EMPS host, and then configure it to set up the appropriate access controls and directory structure elements. The following procedures provide the details:

- Installing SunOne Directory Server (Windows), page 89
- Creating a root node in SunOne Directory Server 5.1 SP4 (Windows), page 90
- Creating a root node in SunOne Directory Server 5.2 (Windows), page 91
- Setting a password for the root node in SunOne Directory Server 5.1 SP4 or 5.2 (Windows), page 92

Procedure: Installing SunOne Directory Server (Windows)

Start of procedure

1. Follow the instructions from SunOne to set up SunOne Directory Server version 5.1 SP4 or SunOne Directory Server version 5.2.

   During the installation, note all the information that you specify for user names, passwords, administration URLs, and administration ports.

   Table 10 provides recommendations for the parameters that you must provide during installation.

Table 10: SunOne Directory Server Parameter Recommendations

Parameter	Value	Comment
Installation location on hard drive	c:\sun\mps	Avoid spaces in paths.
LDAP Port	389	GVP requires this value, and you must retain it.
Administration Port	555	The installer suggests random values for administration ports. Genesys recommends that you standardize on one value.

2. If you are using SunOne Directory Server version 5.2, install Patch 117667-02:
   a. Stop the SNMP service.
   b. Follow the instructions from SunOne to install Patch 117667-02.
   c. Restart the SNMP service.

End of procedure

Next Steps

- Configure Directory Server:
  - Create a root node. Do one of the following, as applicable:
    - Creating a root node in SunOne Directory Server 5.1 SP4 (Windows), page 90
    - Creating a root node in SunOne Directory Server 5.2 (Windows), page 91
  - Set a password for the root node. For more information, see Setting a password for the root node in SunOne Directory Server 5.1 SP4 or 5.2 (Windows), page 92.

Procedure: Creating a root node in SunOne Directory Server 5.1 SP4 (Windows)

Purpose: To create the root node for GVP data (`o=genesys`, or a name that is more suitable for your environment).

The root node is also referred to as the *Root Suffix* or *Root DIT.*

Start of procedure

1. Open the SunOne Server Console.
2. Log in using `cn=Directory Manager` and your password.
3. In the tree view on the left pane, click the plus sign (+) to expand the server node (for example, `ldap.mycompany.com`).
4. Expand the `Server Group` node, and then select `Directory Server`.

   Verify that the version is correct (5.1 SP4).
5. Right-click `Directory Server`, and then select `Open`.

   The Directory Server Console appears.
6. Create the root suffix:

   a. In the Directory Server Console, click the `Configuration` tab.

   b. Select the `Database` icon, and then expand it.

   c. Select `Object > New Root Suffix`.

   The `Create New Root Suffix` dialog box appears.

   d. In the `New Suffix` field, enter a suffix name of your choice.

   Note: Restrict the values to 8 to 12 lowercase letters.

   The GVP installation uses `o=genesys.net` as the default value.

   e. Select the `Create associated database automatically` check box.

   f. Enter the name of the database—for example, `genesys`.

   Note: Do not use the period (.) character or any other special characters.

   g. Click `OK`.
7. Add the new root object to the directory tree:

   a. In the Directory Server Console, click the `Directory` tab.

   b. Select your local server, and then select `Object > New Root Object > <your newly created root suffix>`.

   A dialog box appears.

c. Select `Organization`, and then click `OK`.

A dialog box appears.

d. Click `OK` to accept the default values.

The new root node now appears in the directory tree. All data that is relevant to GVP is populated under this node.

End of procedure

Next Steps

- Set the password for the GVP root node. For more information, see Setting a password for the root node in SunOne Directory Server 5.1 SP4 or 5.2 (Windows), page 92.

Procedure: Creating a root node in SunOne Directory Server 5.2 (Windows)

Purpose: To create the root node for GVP data (`o=genesys`, or a name that is more suitable for your environment).

The root node is also referred to as the *Root Suffix* or *Root DIT.*

Start of procedure

1. Open the SunOne Server Console.
2. Log in using `cn=Directory Manager` and your password.
3. In the tree view on the left pane, click the plus sign (`+`) to expand the server node (for example, `ldap.mycompany.com`).
4. Expand the `Server Group` node, and then select `Directory Server`.

   Verify that the version is correct.
5. Right-click `Directory Server`, and then select `Open`.

   The Directory Server Console appears.
6. Create the root suffix:

   a. In the Directory Server Console, click the `Configuration` tab.

   b. Select the `Data` icon, and then expand it.

   c. Select `Object > New Suffix`.

   A dialog box appears.

   d. In the `Suffix DN` box, enter a suffix name of your choice (for example, `o=genesys`). Observe the following naming conventions:

   - Format is `o=xyz`, where `o` is lowercase letter *o,* not zero (`0`).
   - Restrict the length to 8 to 12 letters.

- Use lowercase, without spaces.

e. Click OK.

7. Add the new root object to the directory tree:

a. In the Directory Server Console, click the Directory tab.

b. Select your local server, and then select Object > New Root Object > <your newly created root object>.

A dialog box appears.

c. Select organization, and then click OK.

A dialog box appears.

d. Click OK to accept the default values.

The new root node now appears in the directory tree. All data that is relevant to GVP is populated under this node.

End of procedure

Next Steps

- Set the password for the GVP root node. For more information, see Setting a password for the root node in SunOne Directory Server 5.1 SP4 or 5.2 (Windows).

Procedure:
Setting a password for the root node in SunOne Directory Server 5.1 SP4 or 5.2 (Windows)

Purpose: To provide password-secured access to the root node, which the EMPS uses as a system account for scheduled tasks.

Start of procedure

1. In the Directory Server Console, click the Directory tab.

2. Select the root node that you created in Creating a root node in SunOne Directory Server 5.1 SP4 (Windows), page 90 or Creating a root node in SunOne Directory Server 5.2 (Windows), page 91.

3. Select Object > Edit With Generic Editor.

   A dialog box appears.

4. Click Add Attribute.

   A dialog box appears.

5. Select userpassword, and then click OK.

   A new attribute, labeled Password, appears.

6. Enter a password, and then click OK.

Note: Make note of your password. EMPS uses this password for executing scheduled tasks.

7. Close all SunOne windows.

End of procedure

Next Steps

- From the Windows Services panel, restart the SunOne Directory Server to verify that Directory Server is installed and running.

  When all of the services successfully start, the Directory Server configuration is complete.

Preparing Database Connectivity for Windows

If your GVP deployment will include Element Management System (EMS) Reporting or Outbound Notification (OBN) Manager, you must install Microsoft SQL Server and configure the Microsoft SQL Clients in your environment.

Note: Microsoft SQL Server is required only if EMS Reporting or OBN Manager is installed.

For the supported versions of Microsoft SQL Server, see “Database Server and Client” on page 61.

Table 11 summarizes the steps that you or your database administrator must perform to prepare Microsoft SQL Server and Clients.

Table 11: Preparing the Microsoft SQL Server and Clients

Objective	Related Procedures and Actions
1. Install the server software.	Follow the instructions provided by Microsoft to install Microsoft SQL Server on the EMS Reporting/OBN Manager host. **Note:** The Microsoft SQL Server locale must be U.S. English.
2. Install the client libraries.	Install the Microsoft SQL Server Client libraries on all hosts that must access the Microsoft SQL Server: • EMPS • EMS Reporting components (EventC, Login Server, Call Status Monitor, Reporter, Network Monitor) • OBN Manager
3. Configure the Microsoft SQL Server Client.	Specify the network protocol order selection for the SQL Server Client. For more information, see Configuring the SQL Server Client, page 94.
4. Specify the connection between the database server and clients.	Create a Data Source Name (DSN) for each SQL Server Client on every host that connects to the Microsoft SQL Server(s). For more information, see Creating DSN connections to SQL Servers, page 95.

Procedure: Configuring the SQL Server Client

Purpose: To configure the network protocol order selection for the SQL Server Client.

Start of procedure

1. Open the SQL Server Client Network Utility.
2. Select `Named Pipes Protocol > Add to enabled protocol > Set Named Pipes To Order First`.
3. Click `OK`.

End of procedure

Procedure: Creating DSN connections to SQL Servers

Purpose: To create the Data Source Name (DSN) that specifies the client connection to the SQL Server.

Create a DSN for each Microsoft SQL Server Client on every host that connects to Microsoft SQL Server(s). The DSN points to the Microsoft SQL Server, not to a specific database.

Start of procedure

1. Go to Start > Settings > Control Panel > Administration Tools > Data Sources.
2. Select the System DSN tab.
3. Click Add.

   The Create New Data Source dialog box displays.
4. Select SQL Server from the list of driver names.
5. Click Finish.

   The wizard to create a new data source to SQL Server displays.
6. Specify the data source:
   a. In the Name text box, enter a logical name for the connection (typically the fully qualified domain name [FQDN] of the server).
   b. In the Description text box, enter a suitable description.
   c. In the Server text box, enter the FQDN of the server.
7. Click Next.
8. Select SQL Server Authentication.
9. Click Client Configuration.
10. Select TCP/IP as the protocol.
11. Change the Server Name field to the server name or IP address of the database server.
12. Click Close.
13. Enter the following values in the authentication screen:
    - Login ID—valid user name for the server.
    - Password—valid password for the server.
14. Click Next.
15. Click Finish.

16. Test the connection.

End of procedure

Chapter

5 GVP Deployment Tool

This chapter describes the Genesys Voice Platform (GVP) Deployment Tool. It contains the following sections:

For information about using the GVP Deployment Tool (GDT) to deploy a GVP solution, see Chapter 6, "Installing GVP Components Using the GDT," on page 111.

Note: The GDT applies only for Windows deployments.

Overview of the GDT

The GDT provides a structured and centralized method to plan, deploy, and configure GVP software. Although manual installations are still supported, Genesys recommends that you use the GDT to install GVP in new Windows deployments, deployment upgrades, or additions to existing GVP deployments.

You can also use the GDT for maintenance and to uninstall GVP.

The GDT consists of two main components:

- GDT User Interface (UI)
- GVP Deployment Agent (GDA)

The GDT collects configuration information, and delegates the installation and configuration tasks to the GDA residing on the GVP Server. The GDT UI also displays response messages from the GDA.

For more information about the GDT UI, see “GDT User Interface Components” on page 100.

For more information about how the GDT works with the GDA to deploy GVP, see “How the GDT Works” on page 99.

Deployment Models and Profiles

Deployment Model

The GDT collects configuration information from the user into a *deployment model.* A deployment model is a stored description of the features that each machine will host.

The deployment model is created the first time that you run the GVP Deployment Wizard. The GDT saves the deployment model to the Element Management Provisioning System (EMPS) if available, as well as to an XML file (the default file name is `DataStore.xml`). You can modify or delete the deployment model as necessary.

Profile

A *profile* is a stored description, within the deployment model, of specific configuration settings for a particular GVP machine type, to configure a particular feature. The profile enables configuration information to be reused, because a profile can be assigned to multiple servers.

You can create profiles for the following features:

- IPCS
- VCS
- Reporting (including, for example, Reporter and Network Monitor)
- OBN Manager
- ASR Log Manager

Updating the Deployment Model

If you relaunch the GDT to reconfigure the system after an initial deployment, the GDT receives the latest server configurations along with the latest saved version of the deployment model, and it uses this information to build a new deployment model. You can modify the updated deployment model, and reconfigure one or more of the GVP servers. Commands on the GDT `Deployment > Deployment Model` menu enable you to export and import deployment models (see Table 13 on page 103).

If any of the server configurations cannot be mapped to the GDT supported settings (see “Validating System Requirements” on page 107), warning messages are displayed.

Deployment Model Information

Table 12 shows an example of the information that a deployment model might store.

Table 12: Deployment Model Storage Example

Machine Name	Feature	Profile
Machine1.com	IPCS	ProfileIPCS1
Machine2.com	VCS	ProfileVCS1
Machine3.com	VCS	ProfileVCS2
Machine4.com	EventC	ProfileEventC1

`ProfileIPCS1` contains specific information for a particular IPCS configuration, such as default Media Gateway and licensed ports. `ProfileVCS1` and `ProfileVCS2` similarly contain specific information for particular VCS configurations, which can differ from each other—for example, one VCS might use MRCP whereas the other does not, or one VCS might use a different type of protocol for its TDM signaling. Finally, `ProfileEventC1` contains information about the EventC.

How the GDT Works

The following describes the events in a typical deployment:

1. The GDT copies the installation software from a CD or network location into a temporary location, and compresses the software into separate `.zip` files for each component.
2. The GDT installs and configures the EMPS software.
3. You provide information about non-GVP servers in the deployment (such as MRCP, SQL Server, and TDM), as well as information about EMPS connection settings.
4. The GDT discovers servers on which the GDA is running, or you add information about additional GVP servers in other subnets.
5. You specify the GVP features that you want to install on each GVP server (for example, VCS or IPCS).
6. You instruct the GDT to transfer the installation software from the GDT machine to the target machines.
7. Each GDA downloads only those `.zip` files that it requires for the features that you have specified for the server. The GDA on each GVP server unzips the files, and puts the GVP installation software into the `<SystemDrive>\GDT\Media\<CDVersion>` folder.
8. After the GDAs have finished extracting the `.zip` files locally, the GDT sends an `install components` request to the GDAs, along with the EMPS connection information.

9. Each GDA invokes the installation packages (IPs) that are required for its components, in a predetermined order. The software is silently installed on each GVP machine and registered with the EMPS. The status of the installation, including errors, is displayed in the GDT.
10. When the GVP software installation has been completed, the GDA informs the GDT.
11. After the wizard has completed, you provide additional configuration settings through the EMPS (if required).
12. You start WatchDog on the GVP servers, either from the GDT or directly from the `Services` panel on each GVP machine. For more information, see Starting/Restarting GVP in Normal mode (Windows), page 198.

GDT User Interface Components

The GDT consists of two main UI sub-components:

- The GDT installation wizard (see "GVP Deployment Wizard")
- The user interface for using the GDT and managing GVP deployment (see "Management UI" on page 100)

GVP Deployment Wizard

The GVP Deployment Wizard is a sequence of pages on which you specify the configuration information and features for the GVP servers in your deployment. The GVP options that you select determine which pages the wizard displays.

When you launch the GDT UI on a machine for a new deployment, the wizard enables you to do the following:

- Add all GVP servers on which the GVP software is to be installed and configured.
- Select the GVP options that must be configured on all defined GVP servers.
- Configure each of the selected GVP options for all servers.

The first page of the wizard is a Welcome screen, and subsequent pages lead you through a series of configuration steps. The wizard opens when the GDT is launched using the `GVPLaunch.bat` file.

For more information about using the wizard to deploy GVP, see Chapter 6, "Installing GVP Components Using the GDT," on page 111.

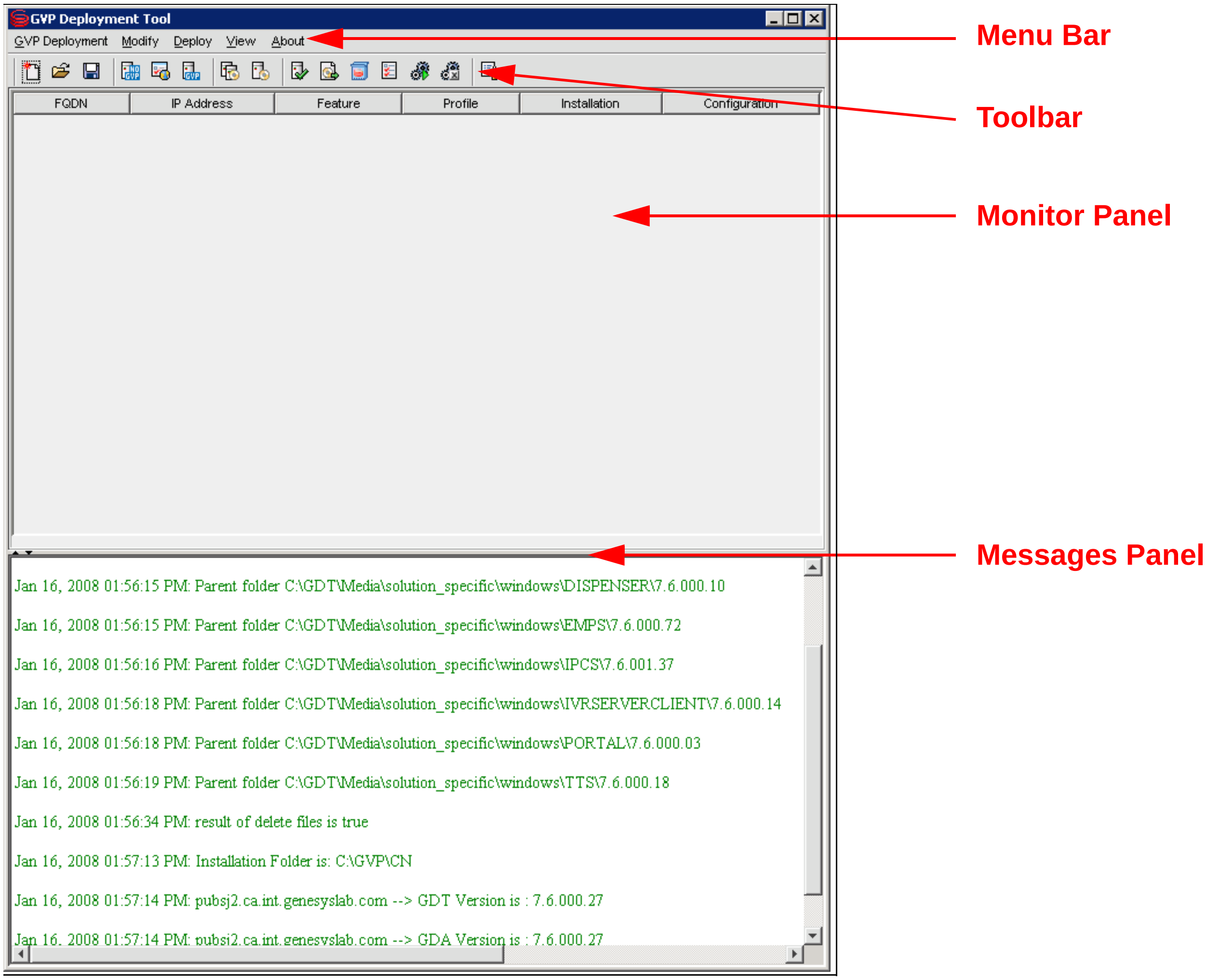
Management UI

The Management UI is the main GDT user interface. It invokes the wizard and stores configuration information.

The Management UI consists of the following elements:

- Menu bar—Enables you to perform specific tasks. For more information about the available menu commands, see “GDT Menus” on page 102.
- Toolbar—Enables you to use a single mouse click to invoke the most commonly used commands from the menus on the menu bar.
- Monitor Panel—Displays the overall status of the GVP deployment, so that you can monitor progress.
- Messages Panel—Displays messages resulting from the ongoing activities of the GDT and the GDAs.

Figure 8 shows the elements of the GDT Management UI.



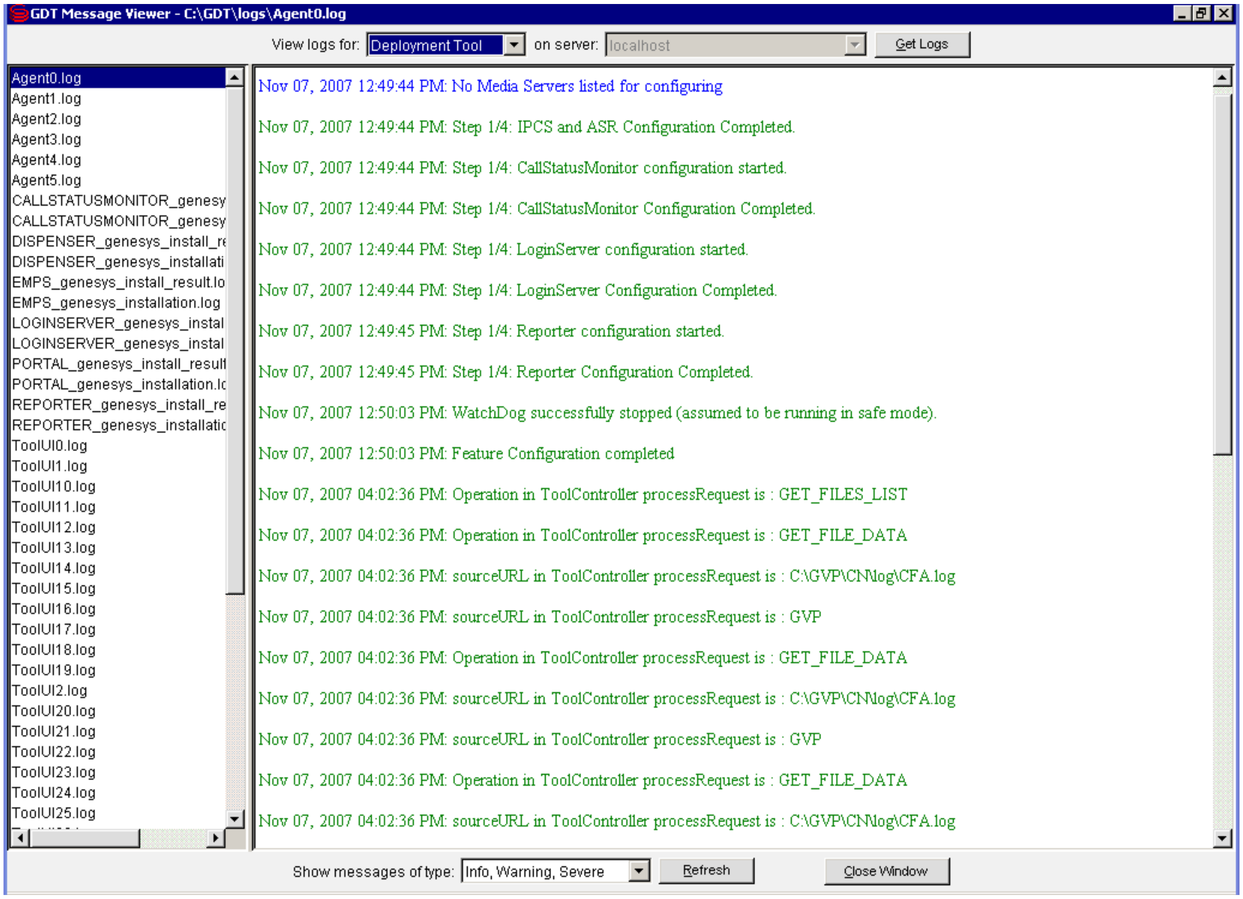
```
Jan 16, 2008 01:56:15 PM: Parent folder C:\GDT\Media\solution_specific\windows\DISPENSER\7.6.000.10

Jan 16, 2008 01:56:15 PM: Parent folder C:\GDT\Media\solution_specific\windows\EMPS\7.6.000.72

Jan 16, 2008 01:56:16 PM: Parent folder C:\GDT\Media\solution_specific\windows\IPCS\7.6.001.37

Jan 16, 2008 01:56:18 PM: Parent folder C:\GDT\Media\solution_specific\windows\IVRSERVERCLIENT\7.6.000.14

Jan 16, 2008 01:56:18 PM: Parent folder C:\GDT\Media\solution_specific\windows\PORTAL\7.6.000.03

Jan 16, 2008 01:56:19 PM: Parent folder C:\GDT\Media\solution_specific\windows\TTS\7.6.000.18

Jan 16, 2008 01:56:34 PM: result of delete files is true

Jan 16, 2008 01:57:13 PM: Installation Folder is: C:\GVP\CN

Jan 16, 2008 01:57:14 PM: pubsj2.ca.int.genesyslab.com --> GDT Version is : 7.6.000.27

Jan 16, 2008 01:57:14 PM: pubsj2.ca.int.genesyslab.com --> GDA Version is : 7.6.000.27
```

Figure 8: The GDT Management UI

Logging

You can display log files for the GDT, the GDA, and GVP processes. Log files display in the `Message Viewer`, which is a separate GDT window (see

Figure 9). For more information about displaying log files in the GDT, see “Log Message Viewer” on page 106 and Viewing log files in the GDT, page 158.



GDT Message Viewer - C:\GDT\logs\Agent0.log

View logs for: Deployment Tool on server: localhost

```
Nov 07, 2007 12:49:44 PM: No Media Servers listed for configuring

Nov 07, 2007 12:49:44 PM: Step 1/4: IPCS and ASR Configuration Completed.

Nov 07, 2007 12:49:44 PM: Step 1/4: CallStatusMonitor configuration started.

Nov 07, 2007 12:49:44 PM: Step 1/4: CallStatusMonitor Configuration Completed.

Nov 07, 2007 12:49:44 PM: Step 1/4: LoginServer configuration started.

Nov 07, 2007 12:49:44 PM: Step 1/4: LoginServer Configuration Completed.

Nov 07, 2007 12:49:45 PM: Step 1/4: Reporter configuration started.

Nov 07, 2007 12:49:45 PM: Step 1/4: Reporter Configuration Completed.

Nov 07, 2007 12:50:03 PM: WatchDog successfully stopped (assumed to be running in safe mode).

Nov 07, 2007 12:50:03 PM: Feature Configuration completed

Nov 07, 2007 04:02:36 PM: Operation in ToolController processRequest is : GET_FILES_LIST

Nov 07, 2007 04:02:36 PM: Operation in ToolController processRequest is : GET_FILE_DATA

Nov 07, 2007 04:02:36 PM: sourceURL in ToolController processRequest is : C:\GVP\CN\log\CFA.log

Nov 07, 2007 04:02:36 PM: sourceURL in ToolController processRequest is : GVP

Nov 07, 2007 04:02:36 PM: Operation in ToolController processRequest is : GET_FILE_DATA

Nov 07, 2007 04:02:36 PM: sourceURL in ToolController processRequest is : C:\GVP\CN\log\CFA.log

Nov 07, 2007 04:02:36 PM: sourceURL in ToolController processRequest is : GVP

Nov 07, 2007 04:02:36 PM: Operation in ToolController processRequest is : GET_FILE_DATA

Nov 07, 2007 04:02:36 PM: sourceURL in ToolController processRequest is : C:\GVP\CN\log\CFA.log
```

Show messages of type: Info, Warning, Severe

Figure 9: GVP Deployment Tool Message Viewer Window

GDT Menus

The GDT menu bar contains the following menus:

- `GVP Deployment`—Includes commands to initiate deployment activity and to manage deployment models. For more information about the available commands, see Table 13 on page 103.
- `Modify`—Includes commands to access the GVP Deployment Wizard to specify the type of setup and manage GVP and non-GVP server configurations. For more information about the available commands, see Table 14 on page 104.
- `Deploy`—Includes commands to manage WatchDog, to access the GVP Deployment Wizard to perform various installation and configuration steps, and to perform maintenance. For more information about the available commands, see Table 15 on page 104.

- View—Includes commands to display log messages and deployment progress messages. For more information about the available commands, see Table 16 on page 106.
- About—Displays information about the GDT, including the release number.

Tables 13 through 16 describe the commands that are available on the menus in the GDT menu bar.

GVP Deployment Menu

Table 13 describes the commands on the GVP Deployment menu and submenus.

Table 13: GVP Deployment Menu Commands

Menu Item	Submenu Item	Description
Perform Activity		Opens the Select Activity page of the GVP Deployment Wizard. This enables you to relaunch the GVP Deployment Wizard to perform a new GVP deployment, upgrade to the new GVP release, or add components to an existing GVP deployment. For more information, see Using the GVP Deployment Wizard to install GVP components (Windows only), Step 4 on page 116.
Deployment Model	Open	Connects to an existing EMPS, and retrieves the existing deployment model. If a model does not exist, you are informed of this fact, and a new model is created.
	Save	Saves the current model to the EMPS.
	Save to	Opens the EMPS Connection Settings page of the GVP Deployment Wizard. This enables you to specify the EMPS to which you want to save the model.
	Import from XML file	Imports an existing XML file that was created by using the Export to XML file menu item.
	Export to XML file	Exports the current model to an XML file. This feature enables you to use the tool to plan a deployment.
Exit		Closes the GDT.

Modify Menu

Table 14 describes the commands on the Modify menu.

Table 14: Modify Menu Commands

Menu item	Description
Non-GVP Servers	Opens the Non-GVP Servers portion of the GVP Deployment Wizard. For more information, see "Non-GVP Servers" on page 124.
Global Settings	Opens the Specify Setup Type portion of the GVP Deployment Wizard. For more information, see "Specify Setup Type" on page 117.
GVP Servers	Opens the GVP Servers configuration portion of the GVP Deployment Wizard. For more information, see "GVP Servers Configuration" on page 129.

Deploy Menu

Table 15 describes the commands on the Deploy menu and submenus.

Table 15: Deploy Menu Commands

Menu Item	Submenu Item	Description
Deploy	EMPS Server	Opens the Install EMPS portion of the GVP Deployment Wizard. For more information, see "Install EMPS" on page 121.
	Selected servers	Opens the Select servers page of the GVP Deployment Wizard, so that you can select the GVP server(s) on which you want to deploy GVP software. For more information about the Deploy GVP Software portion of the GVP Deployment Wizard, see "Deploy GVP Software" on page 153.
Watchdog	Start	Starts the WatchDog service on servers that you select.
	Stop	Stops the WatchDog service on servers that you select.

Table 15: Deploy Menu Commands (Continued)

Menu Item	Submenu Item	Description
Advanced	Validate Servers	Sends a validation request to all GDAs that are running on all GVP servers to verify prerequisites, and then displays the results. For more information about system validation, see “Validating System Requirements” on page 107.
	Transfer CD Image	Copies the CD Image software to servers that you select, which will host the GDAs.
	Install	Sends an installation request to the GDAs on servers that you select, to install components. The specific components that will be installed by each GDA depend on the deployment model in the EMPS.
	Configure	Sends a configuration request to the GDAs on servers that you select, to configure components. The specific component configurations that will be implemented by each GDA depend on the deployment model in the EMPS. You can use this feature to configure the system for the first time, to restore previous configurations, or to update existing configurations.

Table 15: Deploy Menu Commands (Continued)

Menu Item	Submenu Item	Description
Maintenance	Repair	Sends a repair request to the GDAs on servers that you select, to reinstall currently installed components. For more information, see Repairing a GVP Server, page 212.
	Uninstall	Sends an uninstall request to the GDAs on servers that you select, to uninstall currently installed components. Further submenu commands enable you to do the following: • Uninstall all components • Uninstall selected components • Uninstall EMPS For more information, see Uninstalling GVP Components, page 213.
	GDA Upgrade	Enables remote upgrade of the GDAs. For more information, see Upgrading GVP Using the GDT, page 201.
	Hotfix GVP	Performs a hot fix upgrade on servers that you specify. For more information, see Installing a Hot Fix, page 211.

View Menu Table 16 describes the commands on the `View` menu.

Table 16: View Menu Commands

Menu Item	Description
Log Message Viewer	Displays the Log Message Viewer. You select the server and log level you wish to view. You can view log messages for the GDT, the GDA, and GVP processes.
Messages Panel	Displays the Messages Panel (see Figure 8 on page 101). This shows all of the operations performed by the GDT.

Validating System Requirements

The System Validator is a utility that uses a set of rules to validate whether a particular system meets a predefined set of criteria for a successful GVP deployment. The validation rules are contained in an XML file.

The GVP Deployment Wizard invokes the System Validator before it deploys the GVP software (see Using the GVP Deployment Wizard to install GVP components (Windows only), Step 18 on page 122 and Step 66 on page 154).

The System Validator checks the following system software prerequisites:

- Internet browser—The installed browser must be Microsoft Internet Explorer (IE) 6.0 SP1 or 7.0.
- Management and monitoring tools—Simple Management Network Protocol (SNMP) must be installed.
- Operating system and Service Packs (SPs)—The version of the installed operating system must be one of the following:
    - Windows 2003 Enterprise Edition SP2
    - Windows 2003 Standard Edition SP 2
    - Windows XP Professional SP2 (for Genesys Voice Platform: Developer’s Edition [GVP: DE] only)
- Web server—The installed version of Microsoft Internet Information Server (IIS) must be one of the following:
    - IIS 5
    - IIS 6
    - IIS 7

For more information about the GVP software requirements for Windows, see “Windows Prerequisites” on page 58.

The System Validator also checks for compatibility between the GDT and the GDAs on all the GVP servers.

Installing GVP Components

The InstallRunner performs the installation of all GVP components by launching the installation packages in the correct order, and interpreting the response codes for error handling. The GDA on each server invokes the InstallRunner to install the required components on that server.

The InstallRunner launches the setup for each installation package (IP), and then waits for the installation to be completed. If an error occurs during the installation of an IP, the InstallRunner stops the installation and returns control back to the GDA. It also sends an error message. The GDA, in turn, forwards the error message to the GDT, which displays the message in the Log Message Viewer.

The InstallRunner installs the following GVP components, as required:

- Common—Contains all the common modules. Common must be installed before the other IPs are executed.
- EMPS—Provides the interface to provision and configure customer and application profiles.
- Dispenser—Hosts the `did.xml` and `app.xml` files generated by EMPS.
- Portal—A website that provides a single point of access to all web-based user interfaces available within a GVP installation.
- IP Communication Server (IPCS)—Software that processes IP-based calls.
- Voice Communication Server (VCS)—Software that processes calls through traditional Time-division Multiplexing (TDM) circuits.
- Text-to-Speech (TTS)—Uses Media Resource Control Protocol (MRCP) to communicate to the TTS MRCP servers. Provides native TTS support.
- IVR Server Client—Manages the requests to and from the IVR Server.
- Resource Manager—Provides IPCS and Media Gateway availability information to SIP Session Manager (SSM) and H.323 Session Manager (HSM).
- SSM—Acts as a Session Initiation Protocol (SIP) proxy to relay SIP messages between the Media Gateway or SoftSwitch and the IPCS.
- HSM—Routes calls to a SIP-enabled IPCS acting as a user agent server.
- Event Collector (EventC)—Receives and stores individual call events from IPCS.
- Network Monitor—Provides a single interface to monitor server health across the network.
- Call Status Monitor—Provides instantaneous data on call activity.
- Login Server—Authenticates customers who use the Element Management System (EMS) web services.
- Reporter—Provides historical data on enterprise traffic for an overview of applications, or information on a call-by-call basis.
- OBN Manager—Enables customers to make outbound calls using GVP, and to initiate these calls using simple Hypertext Transfer Protocol (HTTP) requests.
- Policy Manager—Maintains and enforces policies on a per customer and per application basis, including IP requests from Outbound Contact Server.
- BandWidth Manager—Manages the rate of transfer of files on the IPCS/VCS.
- ASR Log Server—Parses the transferred automatic speech recognition (ASR) log files and distributes to different customers.
- ASR Log Manager—Responsible for initiating and monitoring ASR Log transfers between the various Open Speech Recognizer (OSR) Servers and the ASR log Server.

- ASR Log Agent—Responsible for transferring ASR Logs and utterances to the ASR Log Server machine when initiated by the ASR Log Manager.

For more information about the GVP components, see “GVP Components” on page 36.

For more information about using the GDT to install GVP components, see “Using the GVP Deployment Wizard to install GVP components (Windows only)” on page 113.

Chapter

6 Installing GVP Components Using the GDT

This chapter describes how to use the GVP Deployment Agent (GDA) and the GVP Deployment Tool (GDT) to install Genesys Voice Platform (GVP) components on the Windows operating system, and to use the GDT to view GVP log files both during and after installation.

This chapter contains the following sections:

Genesys strongly recommends that you use the GDT to install GVP components, but its use is optional. See Appendix B, "Manual Installation on Windows," on page 505 for instructions on how to install GVP without using the GDT.

For information about using the GDT to upgrade and maintain your GVP deployment, see Chapter 11 on page 201.

For more information about how the GDT works, see Chapter 5 on page 97.

Installing GVP Components with the GDT

This section describes how to use the GDT to install GVP in a new deployment or to add GVP components to an existing deployment.

This section contains the following procedures:

Note: The GDA version must be compatible with the GDT version. Ensure that you install the GDA from the same software installation CD or installation package (IP) as the GDT. Ensure that you use the GDT from the same software installation CD or IP as the GVP software you are installing.

Procedure:
Installing the GVP Deployment Agent

Purpose: To install the agent to which the GDT delegates the actual performance of the GVP software installation and configuration on each GVP server.

Perform this procedure on each machine on which GVP 7.6 software will be installed.

Note: Do not install the GDA on the machine that is running the GDT unless that machine also hosts GVP software.

Prerequisites

- Verify that no earlier versions of the GDA have been installed on the host. If there is an earlier version, upgrade it (see Upgrading the GDA using the GDT, page 202).

Start of procedure

1. Execute the batch file to install the agent:
   - If you are using the GVP Base Software CD, double-click `InstallAgent.bat` in the `<CDImage>\solution_specific\windows\install` folder.
   - If the CD Image is on a network drive, copy the `<CDImage>\solution_specific\windows\install` folder to the local machine, and then double-click `InstallAgent.bat` in the local folder.

   A Disk Operating System (DOS) window appears for approximately 30 seconds, showing the progress of the GDA installation. The DOS window closes when the installation is completed and the GDA service has started.

2. From the Windows `Start` menu, go to `Control Panel > Administrative Tools > Services`, and verify that the `GVP Deployment Agent` service has started.

   If necessary, start or restart the GDA service.

End of procedure

Next Steps

- After the GDA has been installed on each server, use the GDT to install GVP or to modify your GVP deployment. For more information, see Using the GVP Deployment Wizard to install GVP components (Windows only).

Procedure:
Using the GVP Deployment Wizard to install GVP components (Windows only)

Purpose: To install and perform basic configuration of GVP components in a Windows deployment.

Summary

When you launch the GDT, you simultaneously launch the GVP Deployment Wizard. The wizard guides you through the process of creating the deployment model.

The main portions of the wizard are the following:

- Overview (page 117)
- Install GDA (page 117)
- Specify Setup Type (page 117)
- Copy Software (page 119)
- Install EMPS (page 121)
- Non-GVP Servers (page 124)
- GVP Servers Configuration (page 129)
- Profiles (page 138)
- Deploy GVP Software (page 153)

From the `Overview` section onwards, the left pane of the wizard pages contains a task list that indicates those tasks that you have completed, and those that you still need to complete.

Aside from the EMPS software (which is installed in the Install EMPS stage), no software is actually installed on the GVP servers until the last stage of the wizard (Deploy GVP Software), when the GDT instructs the GDAs to install the GVP software on the servers, in accordance with the deployment model.

The deployment model is first saved after the EMPS is installed, and then before installation and configuration of the GVP software (see Step 68 on page 155). You can also save the deployment model by executing the save or export commands on the GDT `Deployment > Deployment Model` menu.

Prerequisites

- The servers on which you will install GVP software conform to the GVP system requirements. For more information about the GVP requirements for Windows, see “Windows Prerequisites” on page 58 and “Windows Services and Settings” on page 81.
- The GDA has been installed on each server on which you will install GVP software, and the GDA service is running. For more information, see Installing the GVP Deployment Agent, page 112.
- The fully qualified domain names (FQDNs) of GVP servers do not contain special characters, such as the underscore (_).

  `Note:` In order for the GVP detection software to work properly, FQDNs must contain only standard characters, such as letters (A–Z, a–z), digits (0–9), and hyphens (-).

  Take note of the FQDN and IP address of any GVP servers that are not in the same subnet as the host that is running the GDT, because you need to specify this information when using the GDT.
- All non-GVP servers that you want to include in your deployment (for example, MRCP ASR server, IVR Server, or SQL Server) have been installed and configured. For more information, see the appropriate vendor documentation.

  Take note of the FQDN and IP address of each non-GVP server, because you need to specify this information when using the GDT.
- If your deployment includes EMS Reporting or OBN Manager, the database server and clients have been prepared, and database information (database names, user names, and passwords) is available. The scripts to create the database schemas are unpacked during the installation, and you create the actual database schemas after the wizard has completed. For more information, see “Preparing Database Connectivity for Windows” on page 93.
- If your GVP deployment is for TDM telephony, Dialogic telephony boards have been installed and configured on the machine that will host the Voice Communication Server (VCS). For more information, see “Installing Dialogic Software” on page 173.
- All third-party software, especially antivirus software, has been stopped on the server that is running the GDT and on the servers on which GVP software will be installed.

Start of procedure

1. Execute the batch file to launch the GDT:
   - If you are using the GVP Base Software CD, double-click `GVPLaunch.bat` in the `<CDImage>\solution_specific\windows\install` folder.
   - If the CD Image is on a network drive, copy the `<CDImage>\solution_specific\windows\install` folder to the local machine, and then double-click `GVPLaunch.bat` in the local folder.

   The GDT and the GVP Deployment Wizard open simultaneously, in separate windows.

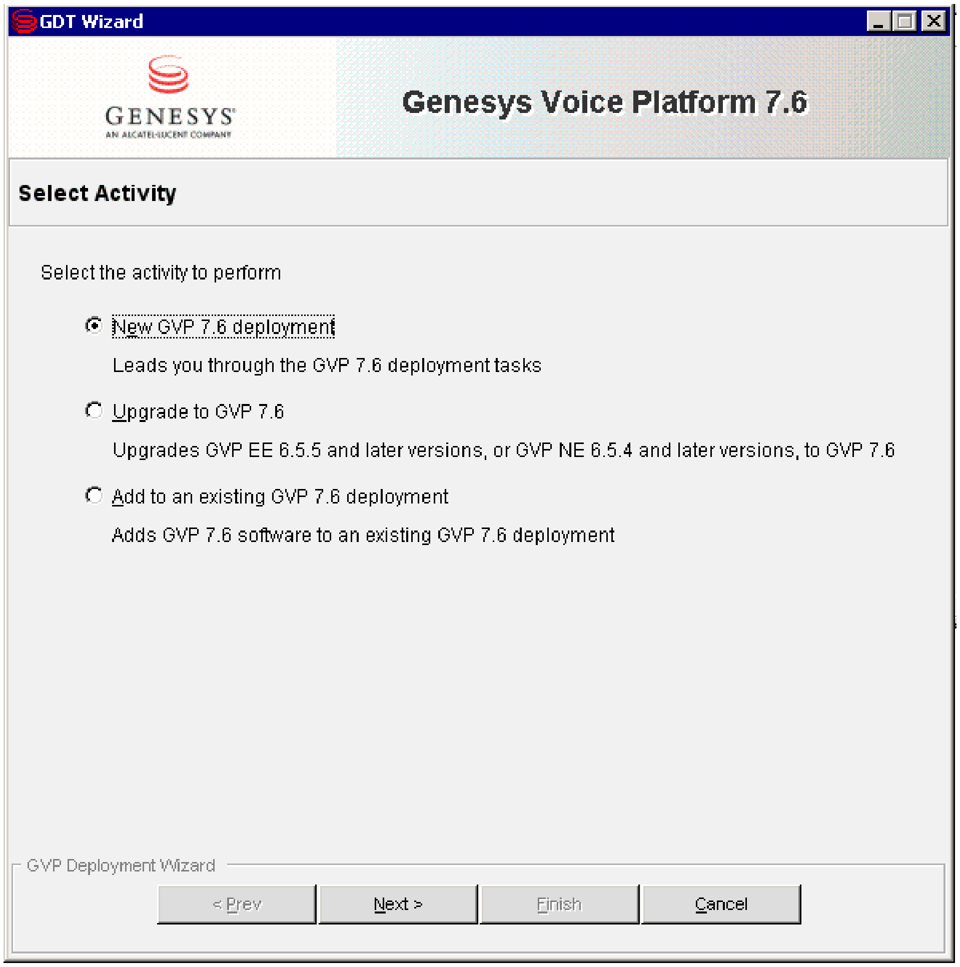
   Note: If the GDT is already open, you can launch the wizard by selecting `GVP Deployment > Perform Activity` from the `Deployment Model` menu of the GDT. Continue at Step 4.

2. On the `Welcome` page of the wizard, click `Next`.

   The `Genesys License Agreement` page appears.

3. On the `Genesys License Agreement` page, select the `I accept the above agreement` check box, and then click `Next`.

   The `Select Activity` page appears (see Figure 10).



Select Activity

Select the activity to perform

● New GVP 7.6 deployment

Leads you through the GVP 7.6 deployment tasks

○ Upgrade to GVP 7.6

Upgrades GVP EE 6.5.5 and later versions, or GVP NE 6.5.4 and later versions, to GVP 7.6

○ Add to an existing GVP 7.6 deployment

Adds GVP 7.6 software to an existing GVP 7.6 deployment

Figure 10: Select Activity Page

4. On the `Select Activity` page, select the type of activity that you wish to perform:
   - If this is the first time that you are running the wizard to deploy GVP, select `New GVP 7.6 deployment`, then click `Next`. This option will create a new deployment model.
   - If you are adding servers to an existing deployment or if your installation activity was interrupted after you installed EMPS and you want to resume using the wizard to complete an initial deployment, select `Add to an existing GVP 7.6 deployment`, then click `Next`. This option modifies the existing deployment model in the EMPS.

Note: For information about upgrading to GVP 7.6, see Upgrading GVP Using the GDT, page 201.

Overview

The `Overview` page appears. The left pane of the `Overview` page, and all subsequent pages of the wizard, contains a GVP Deployment Task List that shows your progress through the GVP deployment process. The tasks that appear in the GVP Deployment Task List depend on options that you select in this step.

5. On the `Overview` page, click `Next`.

The `Install GDA` page appears.

Install GDA

6. On the `Install GDA` page, select the `GDA is installed and running on all servers on which GVP software will be installed` check box, and then click `Next`.

- If this is the first time that you are running the wizard to deploy GVP, the `Specify Setup Type` information page appears. Continue at Step 8.
- If you selected the option to add to an existing deployment (Step 4), the `EMPS Connection Settings` page appears. Continue at Step 7.

7. On the `EMPS Connection Settings` page, specify the settings to connect to the EMPS:

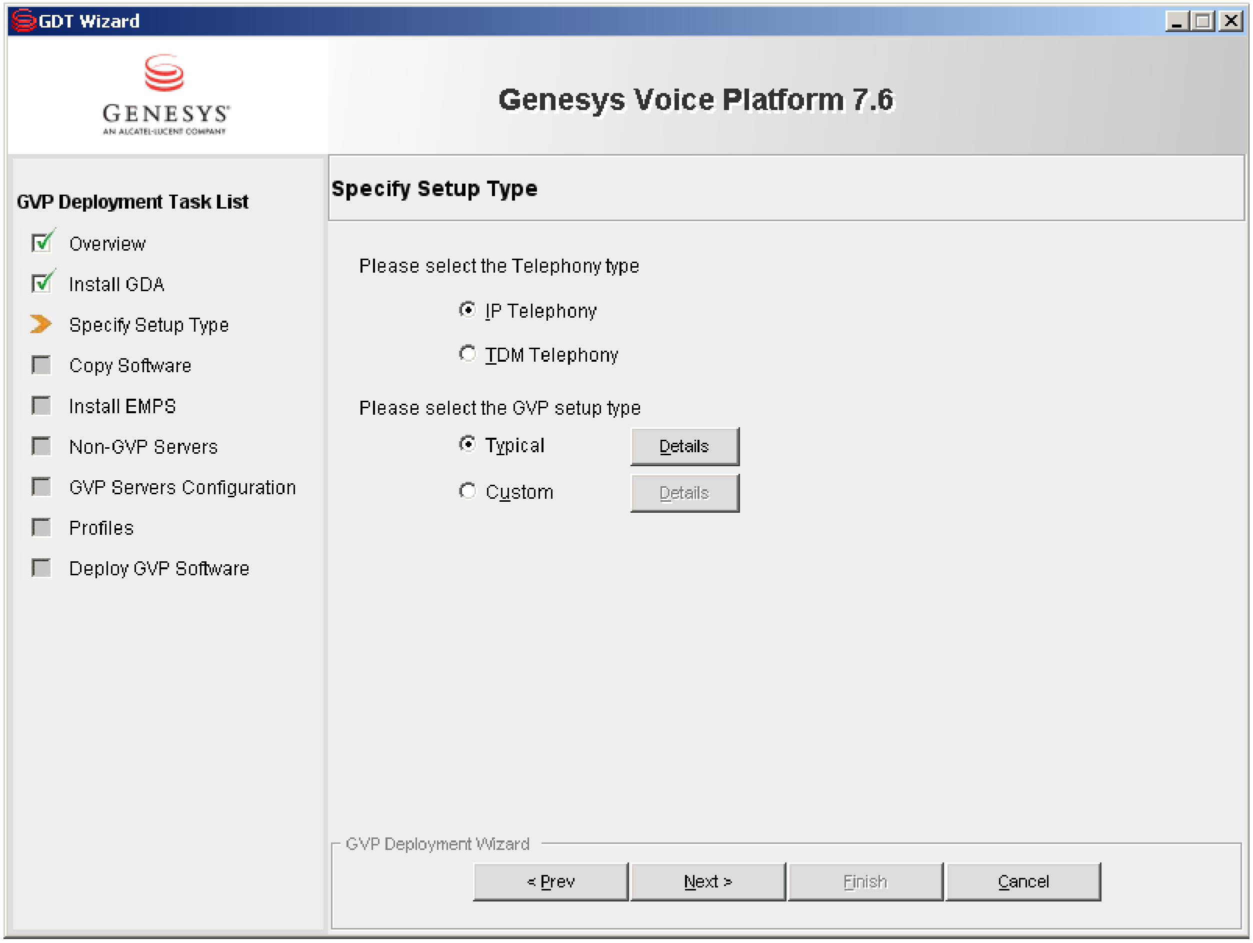
- `Server Name`—The FQDN of the server that is hosting the EMPS.
- `User Name`—The user name that is used to log in to the EMPS. The default is `Admin`.
- `Password`—The password that is used to log in to the EMPS. The default is `password`.

The `Specify Setup Type` information page appears.

Specify Setup Type

8. On the `Specify Setup Type` information page, read the information about telephony types, and then click `Next`.

The `Specify Setup Type` task page appears (see Figure 11).



Genesys Voice Platform 7.6

GVP Deployment Task List

- ☑ Overview
- ☑ Install GDA
- ➤ Specify Setup Type
- □ Copy Software
- □ Install EMPS
- □ Non-GVP Servers
- □ GVP Servers Configuration
- □ Profiles
- □ Deploy GVP Software

Specify Setup Type

Please select the Telephony type

● IP Telephony

○ TDM Telephony

Please select the GVP setup type

● Typical

○ Custom

GVP Deployment Wizard

Figure 11: Specify Setup Type Task Page

9. On the `Specify Setup Type` task page, select the options to specify the type of GVP deployment and installation.

   a. Telephony type:

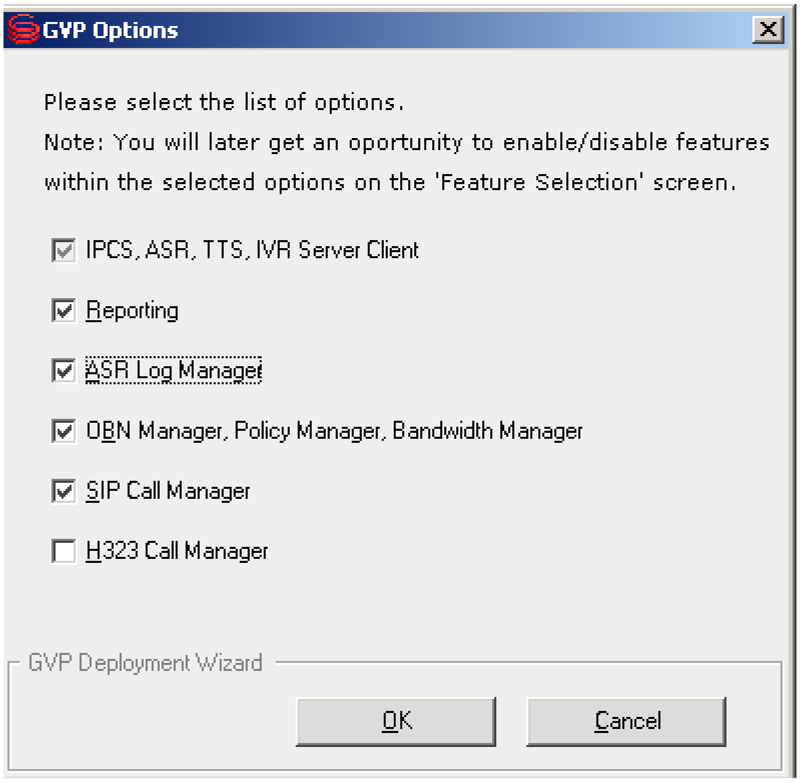
      - `IP Telephony`—Uses IPCS to receive calls. Optionally uses Session Initiation Protocol (SIP) Call Manager or H.323 Call Manager to manage them. Enhanced media (Dialogic HMP or MSOL/MSML) is also available.
      - `TDM Telephony`—Uses Dialogic telephony boards on VCS to receive calls.

   b. GVP setup type:

      - `Typical`—Includes IPCS (for `IP Telephony` type) or VCS (for `TDM Telephony` type), as well as ASR, TTS, and IVR Server Client. If you select the `Typical` setup, continue at Step 11.
      - `Custom`—Includes everything under `Typical`, plus the following options:
        — Reporting
        — ASR Log Manager

- Outbound Notification (OBN) Manager, Policy Manager, Bandwidth Manager
- SIP Call Manager
- H.323 Call Manager

To specify the custom components that you want to install and configure, select `Custom`, and then click `Details`. The `GVP Options` page appears (see Figure 12).



GVP Options

Please select the list of options.
Note: You will later get an oportunity to enable/disable features within the selected options on the 'Feature Selection' screen.

☑ IPCS, ASR, TTS, IVR Server Client

☑ Reporting

☑ ASR Log Manager

☑ OBN Manager, Policy Manager, Bandwidth Manager

☑ SIP Call Manager

□ H323 Call Manager

Figure 12: GVP Options Page

10. On the `GVP Options` page, select the custom components that you want to install, then click `OK`.

    You are returned to the `Specify Setup Type` task page.

11. After you have selected all the required options to determine the type of setup to perform, click `Next` on the `Specify Setup Type` task page.

    The `Copy Software` information page appears.

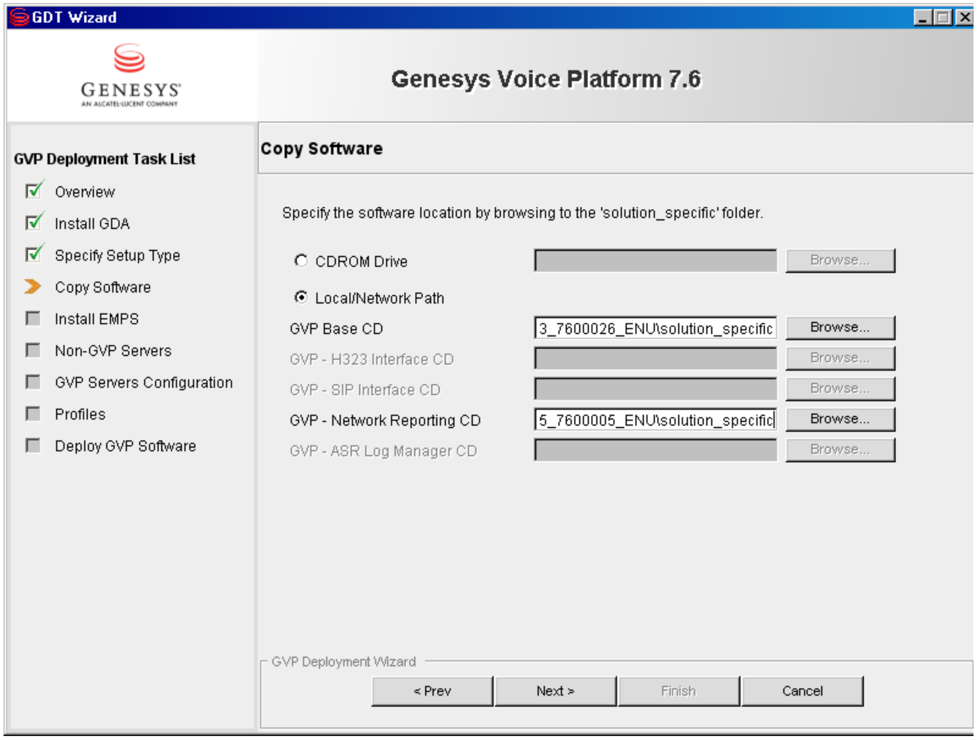
Copy Software

12. On the `Copy Software` information page, read the information about copying software, and then click `Next`.

    The `Copy Software` task page for specifying the GVP software location appears.

13. On the `Copy Software` task page, specify the location of the installation software, and then click `Next`.

    Figure 13 is an example of the `Copy Software` task page for a `Custom` setup that includes EMS Reporting, where the installation software is on a network drive.



Specify the software location by browsing to the 'solution_specific' folder.

○ CDROM Drive

● Local/Network Path

GVP Base CD: 3_7600026_ENU\solution_specific

GVP - H323 Interface CD

GVP - SIP Interface CD

GVP - Network Reporting CD: 5_7600005_ENU\solution_specific

GVP - ASR Log Manager CD

Figure 13: Copy Software Page

- If the GVP installation software is on a CD, select `CDROM Drive`, and then click `Browse` to locate the `solution_specific` folder on the CD drive that contains the GVP installation software.

  If you selected the `Custom` setup type option in Step 9 on page 118, start with the GVP Base Software CD. After the software has been copied, you will be prompted for additional GVP software CDs, based on the options you selected in Step 10 on page 119.
- If the GVP installation software is located on your hard drive or on a mapped network drive, select `Local/Network Path`, and then click the applicable `Browse` button to locate the `solution_specific` folder that contains the GVP software that you want to install.

The GDT copies the installation software to its working directory (typically at `C:\GDT\Media`) for later transfer to each GVP server.

Note: It can take several minutes for the software to be copied.

After the GVP software has been copied, one of the following pages appears, depending on the option you selected in Step 4 on page 116:

- If this is the first time that you are running the wizard to deploy GVP, the Install EMPS information page appears. Continue at Step 14.
- If you selected the option to add to an existing deployment, the Non-GVP Servers information page appears. Continue at Step 24 on page 124.

Install EMPS

14. On the Install EMPS information page, read the information about installing the EMPS, and then click Next.

The Install EMPS task page appears.

15. On the Install EMPS task page, specify the following:

- In the EMPS Server FQDN text box, enter the fully qualified domain name (FQDN) of your EMPS server.
- Select the appropriate tenancy option:
  - — Select Single-tenancy if there is only one reseller.
  - — Select Multi-tenancy if you have purchased the Multi-tenancy option, and there is more than one reseller.

Click Next.

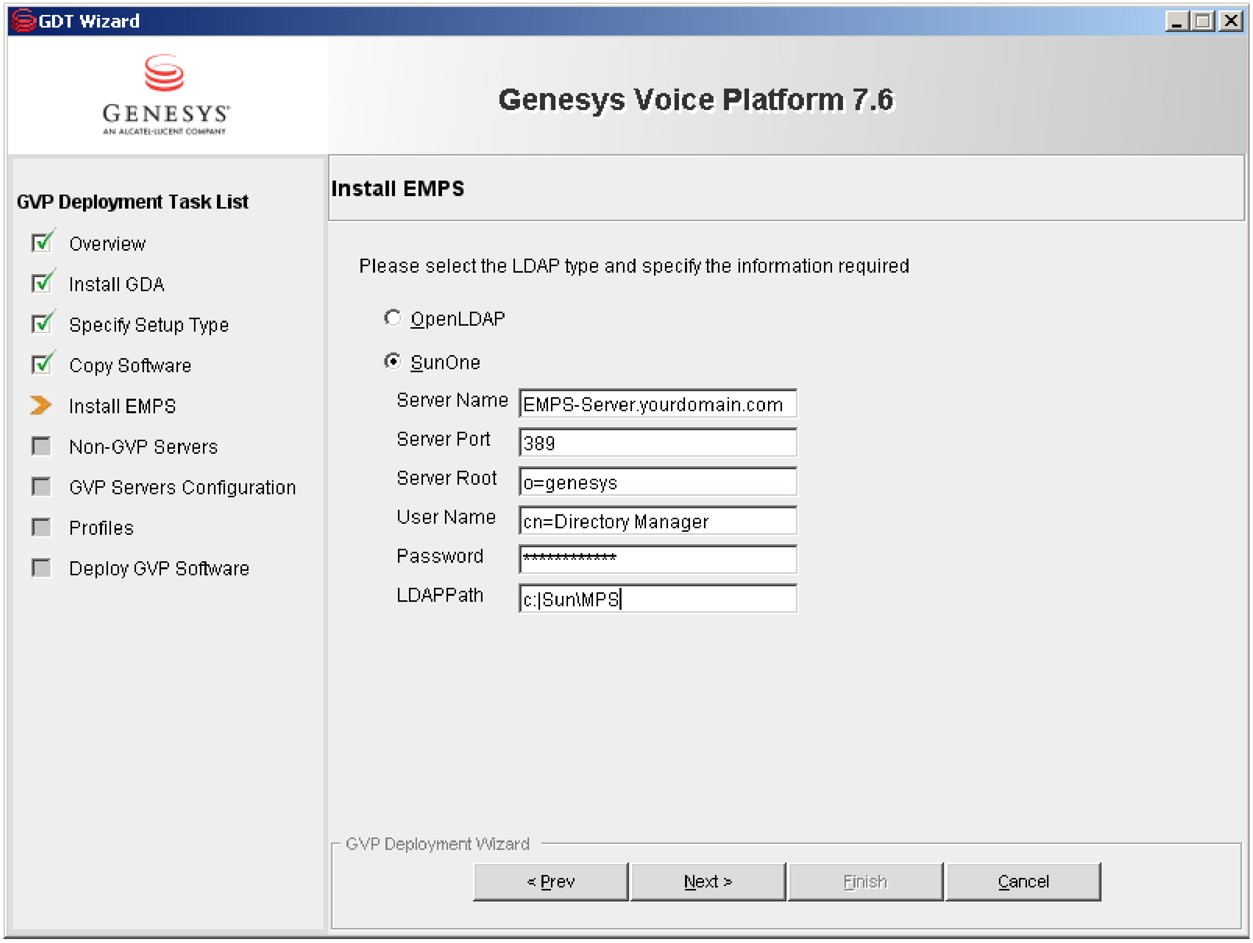
The Install EMPS task page for specifying the Lightweight Directory Access Protocol (LDAP) type and settings appears.

16. On the Install EMPS LDAP settings page, specify the LDAP type, and then click Next.

- OpenLDAP—Recommended for small-size GVP deployments.
- SunOne—Recommended for medium- to large-size GVP deployments.

  If you select SunOne, also specify the following required settings (see Figure 14):

  - Server Name—The FQDN of the machine that is hosting the Directory Server (this is typically the EMSP server).
  - Server Port—The listening port of the Directory Server. You must set the value to 389.
  - Server Root—The LDAP Root or BaseDN. You must set the value to o=genesys.
  - User Name—The name that is used to log in to SunOne. You must set the value to cn=Directory Manager.
  - Password—The password that is used to log in to SunOne. Use the password that you created when you set up your SunOne Directory Server. The password is case sensitive.
  - LDAPPath—The path to the SunOne installation folder. Typically, this is C:\Sun\MPS.



GVP Deployment Task List

- ☑ Overview
- ☑ Install GDA
- ☑ Specify Setup Type
- ☑ Copy Software
- ➤ Install EMPS
- □ Non-GVP Servers
- □ GVP Servers Configuration
- □ Profiles
- □ Deploy GVP Software

Install EMPS

Please select the LDAP type and specify the information required

○ OpenLDAP

● SunOne

Server Name	EMPS-Server.yourdomain.com
Server Port	389
Server Root	o=genesys
User Name	cn=Directory Manager
Password	*************
LDAPPath	c:|Sun\MPS

Figure 14: Install EMPS Task Page—Specifying the LDAP Type and Settings

After you click `Next`, the `Install EMPS` task page for specifying the EMPS installation folder appears.

17. On the `Install EMPS` installation folder page, specify the installation path by accepting the default value or entering a new path in the `Default Location` text box, and then click `Next`. The default path is `C:\GVP\CN`.

    An `Install EMPS` information page appears, with information about validation.

18. On the `Install EMPS` information page, read the information about validation, and then click `Next`.

    The GDT validates the Windows prerequisites for the EMPS, then displays the results.

    - If validation is successful, a `Validation Successful` page appears. Continue at Step 19.

- If the EMPS server fails to meet the software prerequisites, a `Validation Failed` page appears. Click `Finish` to exit the wizard. After you have installed the required operating system and other software prerequisites on the EMPS server machine, rerun the wizard, starting at Step 1 on page 115.

  For more information about GDT validation of software prerequisites, see "Validating System Requirements" on page 107.

19. On the `Validation Successful` page, click `Next`.

- If you are installing the EMPS on another server (in other words, not the server on which the GDT is running), the GDT transfers the installation software to the EMPS server.

  The `CD Image Transfer` page appears. Continue at Step 20.
- If you are installing the EMPS on the same server on which the GDT is running, no software transfer is necessary because the installation software is already in the `C:\GDT\Media` folder.

  The `Install EMPS` page appears. Continue at Step 21.

20. On the `CD Image Transfer` page, click `Next`.The CD image is transferred to the target, the EMPS server.

The `Install EMPS` page appears.

21. On the `Install EMPS` page, click `Next`.

The GDT installs EMPS on the server, then displays the results. If installation is successful, WatchDog automatically starts on the EMPS.

Note: To configure additional parameters for EMPS, see Chapter 17, "Configuring EMPS in the EMPS," on page 289.

22. Verify that EMPS installation was successful:

a. Open the EMPS GUI by launching Internet Explorer and navigating to `http://<EMPS Server>:9810`.

b. Verify that the Net Management page appears.

c. In the left pane, click the `EMPS` link.

The `EMPS Login` page appears.

d. Log in to the EMPS with `User Name` = `admin` and `Password` = `password`.

e. Verify that the EMPS `Welcome` page appears.

23. On the successful `Install EMPS` page of the wizard, click `Next`.

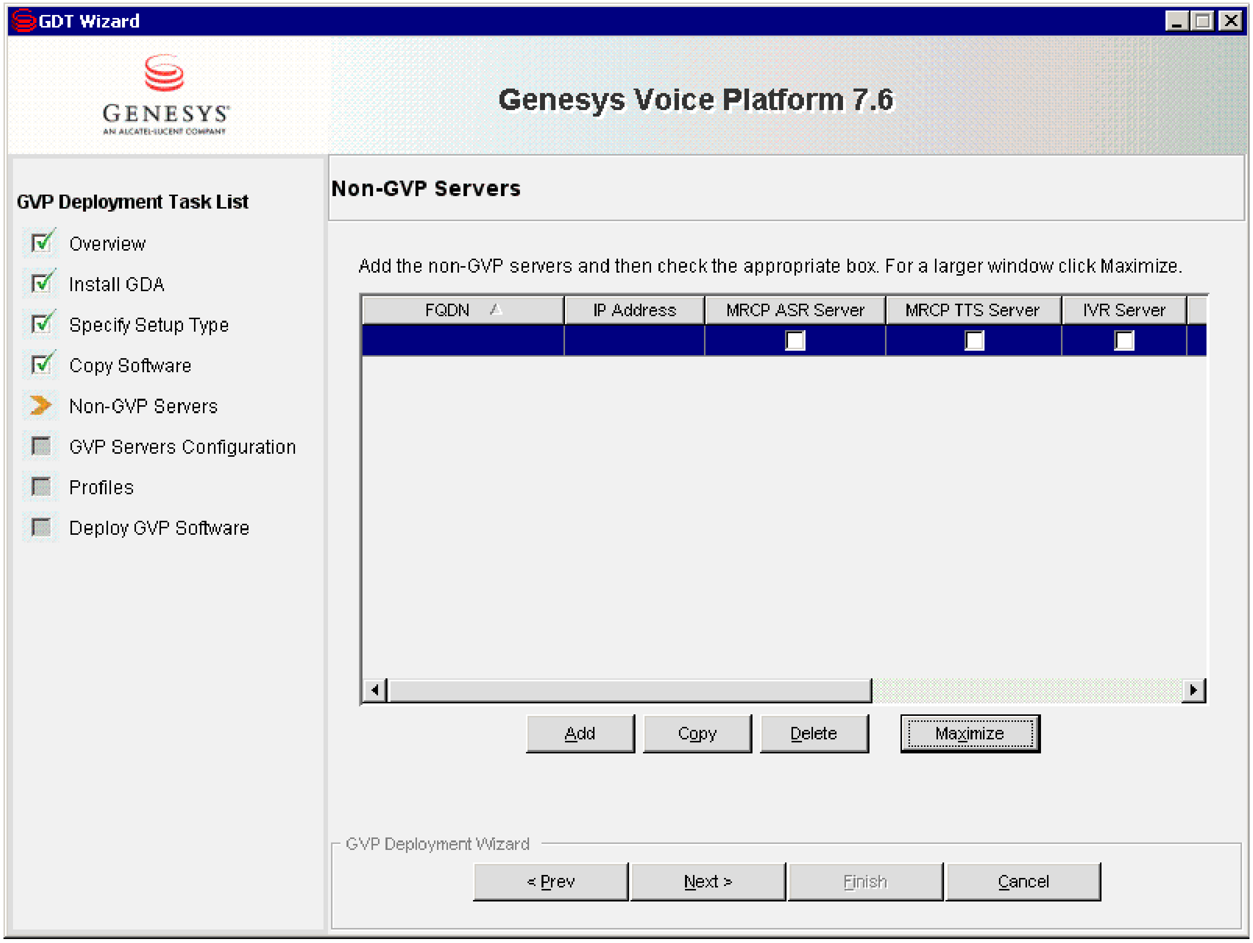
The `Non-GVP Servers` information page appears.

Note: The deployment model is saved to the EMPS for the first time after the EMPS is installed.

Non-GVP Servers

24. On the `Non-GVP Servers` information page, read the information about non-GVP servers, and then click `Next`.

The `Non-GVP Servers` task page for adding non-GVP Servers appears (see Figure 15).



Add the non-GVP servers and then check the appropriate box. For a larger window click Maximize.

FQDN	IP Address	MRCP ASR Server	MRCP TTS Server	IVR Server
		□	□	□

Figure 15: Non-GVP Servers Task Page—Adding Non-GVP Servers

25. On the `Non-GVP Servers` task page, specify the non-GVP servers that you want to include in the deployment.

Buttons on the `Non-GVP Servers` task page enable you to do the following:

- `Add`—Add a new server to the GVP deployment.
- `Copy`—Create a copy of the selected server, as a shortcut for configuring another server.
- `Delete`—Remove a server from the GVP deployment.
- `Maximize`—Open the `Advanced Grid` page, which provides a larger working area for selecting features. To return to the previous view, click `OK` on the `Advanced Grid` page.

To add a non-GVP server to the deployment:

a. Click Add.

b. Double-click the FQDN box in the highlighted row, and specify the fully qualified domain name of the non-GVP server.

c. Double-click the IP Address box, and specify the IP address of the non-GVP server.

d. Use the check boxes to specify the non-GVP software with which the GVP software will interact on the selected server. This information is used to configure the GVP software.

The following features are available:

- MRCP ASR Server
- MRCP TTS Server
- IVR Server
- Media Gateway
- Media Server
- SQL Server
- SIP Server

e. Click Next.

For each check box that you selected in substep d, a Non-GVP Servers task page for configuring the corresponding third-party software appears, in sequence.

26. On each Non-GVP Servers task page, specify the required settings for the applicable non-GVP server.

a. Access the Modify Item page to modify settings:

- On the Non-GVP Servers task page for all server types except SQL Server, select the server, and then click Modify.

  The Modify Item page appears.

- On the Non-GVP Servers task page for SQL Server:

  — To add a new database, click Add.

  — To modify settings for an existing database, select the database and then click Modify.

  The Modify Item page appears.

Note: If the table on the Non-GVP Servers task page for SQL Server displays databases that are not required for the GVP deployment, remove the databases from the deployment model. To remove a database from the deployment model, select the database in the table on the Non-GVP Servers task page for SQL Server, and click Delete.

b. On the Modify Item page, specify the required server settings:

i. Review the default values in the active text boxes. If there is no information or you do not want to accept the default values, enter new information for the applicable server settings.

On the Modify Item page for SQL Server, some of the information is selected from drop-down lists.

For more information about the settings you must provide for the respective non-GVP servers, see Table 17.

ii. To specify settings for additional non-GVP servers of the same type, click Next Item, and repeat the previous substep.

iii. Click OK.

You are returned to the Non-GVP Servers task page for the applicable non-GVP server.

Table 17 summarizes the configuration settings that you are required to specify for non-GVP servers.

Table 17: Non-GVP Server Configuration Settings

Non-GVP Server	Required Configuration Settings
MRCP ASR Server	• FQDN—The FQDN of the MRCP ASR Server (read-only information, as specified in Step 25, substep c, on page 125). • MRCP URL—The URL of the MRCP ASR Server. For example, rtsp://MRCP-Server.yourdomain.com:4900/media/speechrecognizer
MRCP TTS Server	• FQDN—The FQDN of the MRCP TTS Server (read-only information, as specified in Step 25, substep c, on page 125). • MRCP URL—The URL of the MRCP TTS Server. For example, rtsp://MRCP-Server.yourdomain.com:4900/media/speechsynthesizer

Table 17: Non-GVP Server Configuration Settings (Continued)

Non-GVP Server	Required Configuration Settings
IVR Server	• `IP Address`—The IP address of the IVR Server (read-only information, as specified in Step 25, substep c, on page 125). • `IVR Name`—The name of the IVR object exactly as it is configured in the Genesys Configuration Layer. This value is case-sensitive, and it must exactly match the name of the IVR object. In a multi-tenant environment, the IVR object is located in the `IVRs` folder for your tenant; in a single-tenant environment, it is located under the `Resources` folder. • `GLI Port`—The port number exactly as it is configured in the `gli-server-address` option in the Configuration Layer. For example, if `gli-server-address = 10.10.23.126:7080,` enter `7080` in the `GLI Port` text box. The `gli-server-address` option is located in the `gli_server_group_[x]` section (typically `gli_server_group_1`) of the application that represents the virtual T-Server. The application resides in the `Applications` folder under `Environment` in the Configuration Layer.

Table 17: Non-GVP Server Configuration Settings (Continued)

Non-GVP Server	Required Configuration Settings
SQL Server	• Database Name—The name of the SQL Server database to which GVP will connect. If you are adding a database, select the appropriate database from the drop-down list. If you are modifying the information for an existing SQL Server database, this field is read-only. The following databases are available in the drop-down list: emps obnmanager networkmonitor reporter unifiedlogin collector repdwh peaks • SQL Server—The FQDN of the server that is hosting the SQL Server database. • User Name—The user name that GVP will use to access the SQL Server database. The GVP user should be assigned as the db owner of the database. • Password—The password that GVP will use to access the SQL Server database. **Note:** If the databases have not yet been created, ensure that you note the User Name and Password that you specified in this step, so that you can create a GVP user with this User Name and Password when you set up the database.
Media Gateway	• IP Address—The IP address of the Media Gateway (read-only information, as specified in Step 25, substep c, on page 125). • Port—The listening port of the Media Gateway. The default is 5060. • Number of Ports—The number of ports that are used for the Media Gateway. The default is 2.

Table 17: Non-GVP Server Configuration Settings (Continued)

Non-GVP Server	Required Configuration Settings
Media Server	• IP Address—The IP address of the Media Server (read-only information, as specified in Step 25, substep c, on page 125). • Port—The listening port of the Media Server. The default is 5060.
SIP Server	• IP Address—The IP address of the SIP Server (read-only information, as specified in Step 25, substep c, on page 125). • Port—The port of the SIP Server. The default is 5060.

c. On the Non-GVP Servers task page, click Next.

The Non-GVP Servers task page for the next type of server appears.

27. Repeat Step 26 as many times as required to configure the settings for the servers you specified in Step 25 on page 124 (see substep d).

After you click Next on the last Non-GVP Servers task page, the GVP Servers configuration information page appears.

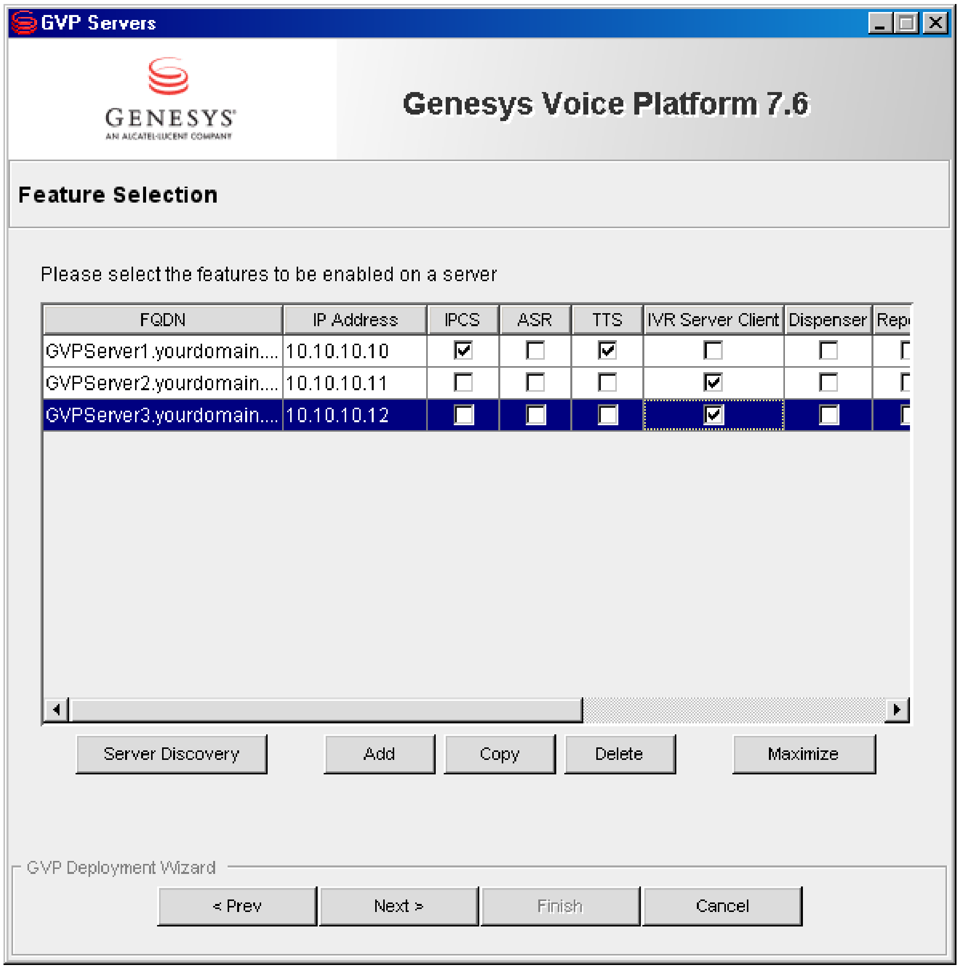
GVP Servers Configuration

28. On the GVP Servers configuration information page, read the information about configuring GVP servers, and then click Next.

29. When prompted, Do you want to discover the GVP servers on which agent is running, click Yes.

After the GVP servers have been located on the network, the GVP Servers Configuration task page for selecting features appears. The page is populated with the FQDN and IP address of each server in the subnet that is running the GDA (see Figure 16).

If you click No at the prompt to discover GVP servers, an empty GVP Servers Configuration task page for selecting features appears.



Feature Selection

Please select the features to be enabled on a server

FQDN	IP Address	IPCS	ASR	TTS	IVR Server Client	Dispenser	Rep
GVPServer1.yourdomain....	10.10.10.10	☑	□	☑	□	□	□
GVPServer2.yourdomain....	10.10.10.11	□	□	□	☑	□	□
GVPServer3.yourdomain....	10.10.10.12	□	□	□	☑	□	□

Figure 16: GVP Servers Configuration Task Page—Selecting Features

Note: The GDT will discover (display) only those servers that are running within the same subnet as the server on which the GDT is running. Genesys recommends that you run the GDT from one central location, even if there are GVP servers in various subnets in your network. If you are running the GDT from one central location, you must manually add any servers that are in other subnets. Otherwise, you will have to run the GDT again on a server in each subnet.

To add servers manually, see Step 32 on page 131.

30. On the `GVP Servers Configuration` task page, verify that all the GVP servers in your deployment appear on the page, with the correct FQDN and IP address.

Buttons on the `GVP Servers Configuration` task page enable you to do the following:

- `Server Discovery`—Detect GVP servers that are on the subnet and are running the GDA.
- `Add`—Add a new server to the GVP deployment.
- `Copy`—Create a copy of the selected server, as a shortcut for configuring another server.
- `Delete`—Remove a selected server from the GVP deployment.
- `Maximize`—Open the `Advanced Grid` page, which provides a larger working area for selecting features. To return to the previous view, click `OK` on the `Advanced Grid` page.

If all the GVP servers in your deployment appear on the `GVP Servers Configuration` task page, continue at Step 33.

If GVP servers are in the same subnet as the server that is running the GDT, but they do not appear on the `GVP Servers Configuration` task page, continue at Step 31.

If GVP servers are not in the same subnet as the server that is running the GDT, add them manually (see Step 32).

31. If GVP servers are in the same subnet as the server that is running the GDT, but they do not appear on the `GVP Servers Configuration` task page, do the following:

a. Verify that the GDA is installed on the GVP servers, and that the GDAs are running (started) as services. If necessary, install the GDA (see Installing the GVP Deployment Agent, page 112), and start or restart the `GVP Deployment Agent` service.

b. Verify connectivity between the server that is hosting the GDT and the servers that are hosting the GDAs. Correct as required.

c. On the `GVP Servers Configuration` task page, click `Server Discovery` to detect all GVP servers that are on the same subnet as the GDT.

After the GDT has finished searching, you are returned to the updated `GVP Servers Configuration` task page.

d. If the GDT still fails to detect GVP servers in the subnet, add them manually (see Step 32).

32. If there are GVP servers in other subnets, or if the GDT failed to detect any GVP servers in its subnet, add the servers manually.

a. On the `GVP Servers Configuration` task page, click `Add` to add a row.

b. Double-click the `FQDN` box in the new row, and specify the fully qualified domain name of the GVP server.

c. Double-click the `IP Address` box, and specify the IP address of the GVP server.

33. On the `GVP Servers Configuration` task page, in each server row, use the check boxes to specify the features that you want to install on the GVP server (for example, IPCS or VCS, ASR, TTS), then click `Next`.

    The available options depend on the setup type that you selected in Step 9 on page 118.

    > Note: You cannot install SIP Session Manager (SSM) and H.323 Session Manager (HSM) on the same host machine.
    >
    > For more information about software distribution and host considerations in your GVP deployment, see "Host Setup" on page 67.

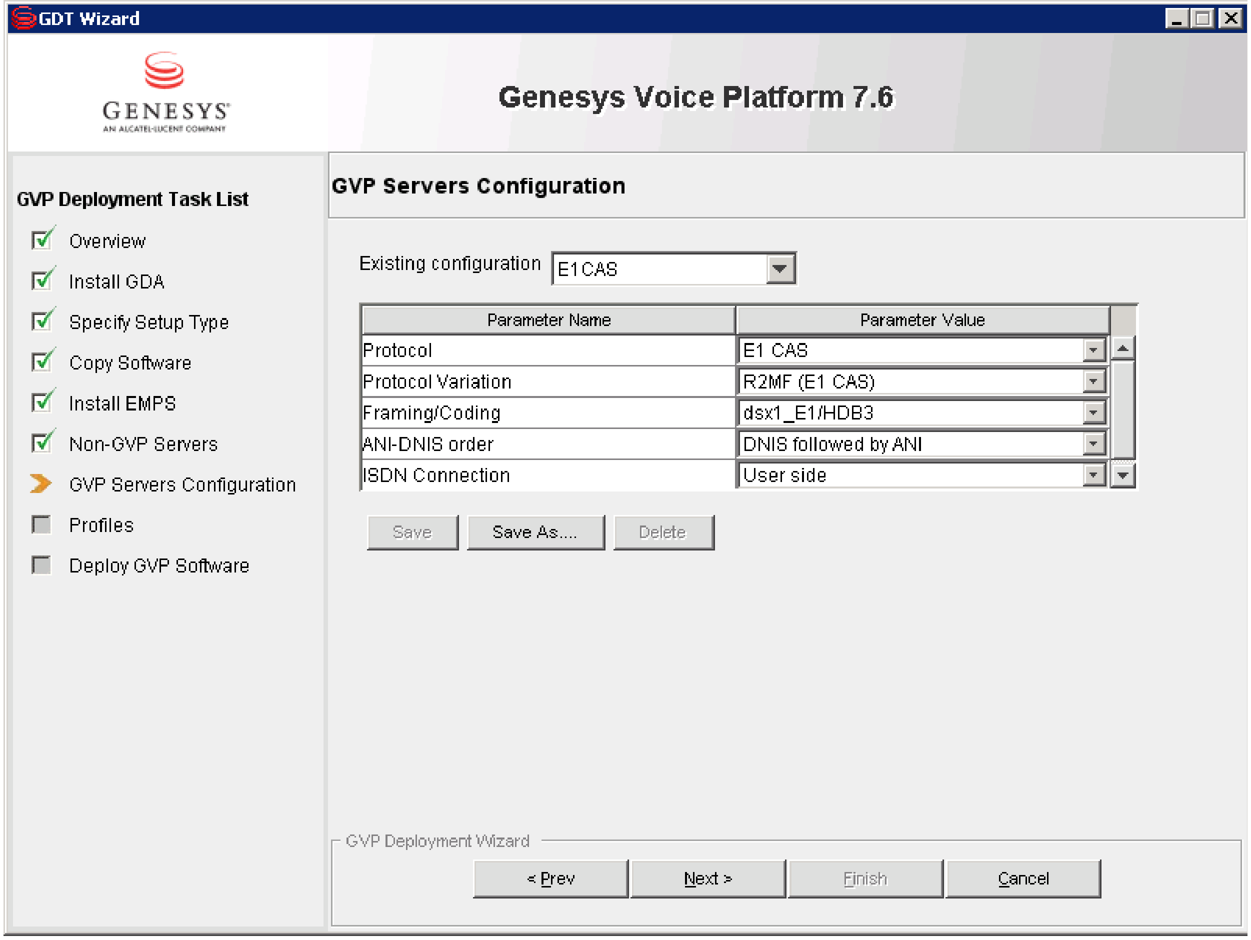
    After you click `Next`:

    - If you are performing an IP Telephony type of installation (as selected in Step 9 on page 118), the `Profiles` information page appears. Continue at Step 40 on page 138.
    - If you are performing a TDM Telephony type of installation (as selected in Step 9 on page 118), the `GVP Servers configuration` task page appears, to configure trunk parameters. Continue at Step 34.

GVP Servers Configuration—VCS

34. On the `GVP Servers Configuration` task page to configure trunks, verify that the trunk configuration parameters match your environment, and modify them if required.

    Figure 17 is an example of the `GVP Servers Configuration` task page to configure trunks.



Existing configuration: E1CAS

Parameter Name	Parameter Value
Protocol	E1 CAS
Protocol Variation	R2MF (E1 CAS)
Framing/Coding	dsx1_E1/HDB3
ANI-DNIS order	DNIS followed by ANI
ISDN Connection	User side

Figure 17: GVP Servers Configuration Task Page for VCS—Trunk Configuration

To modify the trunk configuration parameters:

a. From the `Existing configuration` drop-down list, select a trunk configuration.

The table is populated with the configuration information for that trunk.

b. If the parameters and values do not exactly match your environment, use the `Parameter Value` drop-down lists to customize your configuration.

Note: Use the `Dialogic Trunk Definitions` table to define new configurations, and to modify existing configurations so that they can be applied to your Dialogic boards.

Table 18 lists the trunk parameters and their possible values for different types of trunks.

Table 18: GVP Servers Configuration—Trunk Configuration Parameter Values

Protocol	Protocol Variation	Framing/Coding	ANI-DNIS order	ISDN Connection
E1 CAS	R2MF (E1 CAS)*	dsx1_E1/AMI dsx1_E1/HDB3* dsx1_E1_CRC/AMI dsx1_E1_CRC/HDB3	No ANI and DNIS ANI followed by DNIS DNIS followed by ANI* DNIS only	Not Applicable User side* Network side
E1 ISDN	QSIG-ISDN (E1 ISDN) Euro-ISDN (E1 ISDN)*	dsx1_E1/AMI dsx1_E1/HDB3* dsx1_E1_CRC/AMI dsx1_E1_CRC/HDB3	No ANI and DNIS*	Not Applicable User side* Network side
T1 ISDN	DMS (T1 ISDN) 4ESS (T1 ISDN) 5ESS (T1 ISDN)*	D4/AMI ESF/B8ZS*	No ANI and DNIS*	Not Applicable User side* Network side
T1 Robbed Bit	Wink Start (T1 Robbed bit)*	D4/AMI ESF/B8ZS*	No ANI and DNIS ANI followed by DNIS DNIS followed by ANI* DNIS only	Not Applicable User side* Network side
*Default value for the existing (standard) configuration.				

c. Save your customized configuration to the datastore.xml file.

i. To save your modified trunk configuration for the first time, click Save As.

ii. When prompted, specify a name for the trunk configuration.

You must provide a new name, because you cannot modify the standard configuration.

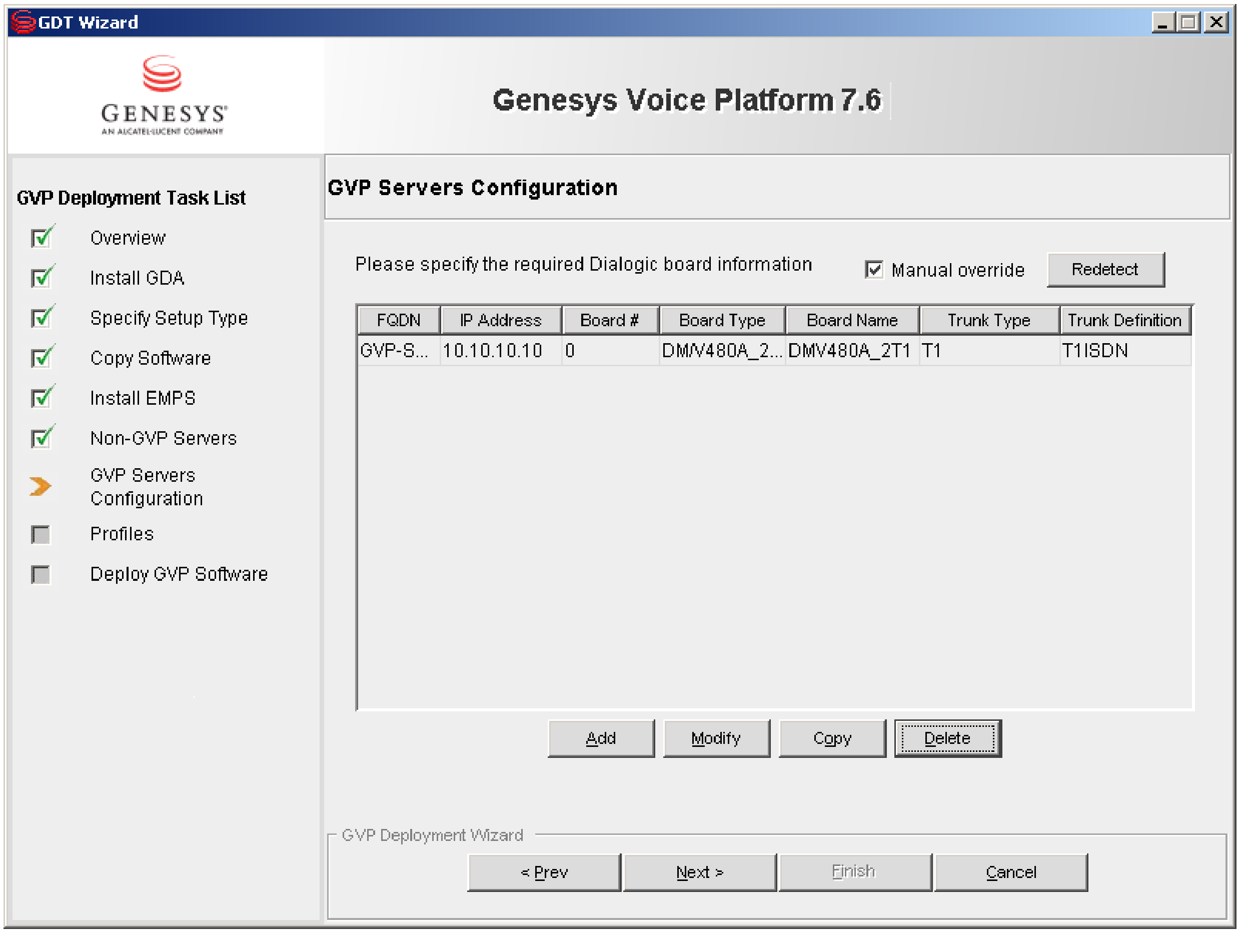
iii. Click OK.

The name of your customized configuration is added to the Existing configuration drop-down list, so that it is available for future selection and further modification.

iv. To save an existing, modified trunk configuration after further modification, click Save.

35. After you are satisfied that the trunk configuration parameters match your environment, click `Next`.

The `GVP Servers Configuration` task page for specifying Dialogic board parameters appears (see Figure 18). The page is populated with Dialogic board information for all installed Dialogic boards that the GVP Deployment Wizard detects on the VCS servers that you identified in Step 33 on page 132.



GVP Deployment Task List

- ☑ Overview
- ☑ Install GDA
- ☑ Specify Setup Type
- ☑ Copy Software
- ☑ Install EMPS
- ☑ Non-GVP Servers
- > GVP Servers Configuration
- ☐ Profiles
- ☐ Deploy GVP Software

GVP Servers Configuration

Please specify the required Dialogic board information ☑ Manual override

FQDN	IP Address	Board #	Board Type	Board Name	Trunk Type	Trunk Definition
GVP-S...	10.10.10.10	0	DMV480A_2...	DMV480A_2T1	T1	T1ISDN

Figure 18: GVP Servers Configuration Task Page—Specifying Dialogic Board Information

36. On the `GVP Servers Configuration` task page for specifying Dialogic board parameters, verify that all the Dialogic boards in your deployment appear on the page, with the correct server, board, and trunk information.

Buttons on the `GVP Servers Configuration` task page enable you to do the following:

- `Redetect`—Instruct the wizard to attempt redetection of installed Dialogic boards.

- Modify—Modify the Dialogic board information for a selected board (see Step 38 on page 138).

After you select the Manual override check box, the following additional buttons become visible:

- Add—Add a new Dialogic board to the GVP deployment.
- Copy—Create a copy of the selected Dialogic board, as a shortcut for configuring another Dialogic board with the same information.
- Delete—Remove a selected Dialogic board from the GVP deployment.

Table 19 describes the Dialogic board parameters.

Table 19: Dialogic Board Parameters

Parameter	Description
FQDN	The fully qualified domain name of the server that is hosting the Dialogic board.
IP Address	The IP address of the machine that is hosting the Dialogic board.
Board #	The unique Dialogic board number that identifies the board to the Dialogic drivers.
Board Type	The type of Dialogic board. GVP supports the following board types: • D/480JCT-1T1 • D/480JCT-2T1 • D/600JCT-1E1 • D/600JCT-2E1 • DMV480A_2T1 • DMV960A_4T1 • DMV600A_2E1 • DMV1200A_4E1 • DMV600BTEP • DMV1200BTEP
Board Name	The name of the Dialogic board as seen in the Dialogic Configuration Manager (DCM).

Table 19: Dialogic Board Parameters (Continued)

Parameter	Description
Trunk Type	The type of trunk with which the board is interfacing. The valid values are: • T1 • E1
Trunk Definition	The trunk protocol, as configured in Step 34 on page 132. The default valid values are: • E1CAS • E1EuroISDN • T1ISDN • T1RobbedBit_Wink • T1 Loopstart • None **Note:** If you defined additional protocol configurations in Step 34, your user-defined protocols will also be available.

If all the installed Dialogic boards in your deployment appear on the `GVP Servers Configuration` task page, and their associated information is correct, continue at Step 39 on page 138.

If all the installed Dialogic boards in your deployment were not detected, you will be prompted to redetect them. If redetection fails, add them manually (see Step 37).

If all the installed Dialogic boards in your deployment appear on the `GVP Servers Configuration` task page, but their associated information is not correct, modify the information as required (see Step 38).

37. If the wizard fails to detect installed Dialogic boards in your deployment, add the boards manually.

a. On the `GVP Servers Configuration` task page, select the `Manual override` check box.

b. Click `Add` to add a row.

c. Double-click the `FQDN` box in the new row, and specify the fully qualified domain name of the server that is hosting the Dialogic board.

d. Double-click the `IP Address` box, and specify the IP address of the server that is hosting the Dialogic board.

e. Select the new row, and then click `Modify`.

The `Modify Item` page appears.

f. Specify the information for the Dialogic board parameters (see Step 38, substep b).

g. Click OK.

   You are returned to the GVP Servers Configuration task page for specifying Dialogic board information. Continue at Step 39 on page 138.

38. To modify the information for a Dialogic board:

    a. On the GVP Servers Configuration task page, select a row, and then click Modify.

       The Modify Item page appears.

    b. Specify the information for the Dialogic board parameters.

       i. In the Board Number text box, enter the unique board number that identifies the board to the Dialogic drivers.

       ii. From the Board Type drop-down list, select the type of board.

       iii. From the Trunk Type drop-down list, select the type of trunk with which the board interfaces.

       iv. From the Trunk Definition drop-down list, select the trunk protocol.

       For more information about the Dialogic board parameters, see Table 19 on page 136.

    c. To modify the parameters for additional Dialogic boards, click Next Item, and repeat the previous substep.

    d. Click OK.

       You are returned to the GVP Servers Configuration task page for specifying Dialogic board information.

39. After you are satisfied that all the required Dialogic board information on the GVP Servers Configuration task page is correct, click Next.

    The Profiles information page appears.

Profiles

40. On the Profiles information page, read the information about profiles and how to create them, and then click Next.

    Depending on the check boxes that you selected in Step 33 on page 132, Profiles task pages for configuring the corresponding profiles appear, in the following sequence.

    - For the typical GVP setup type (as selected in Step 9 on page 118), the Profiles task page for the applicable communication server:
      - — IPCS (for IP Telephony). Continue at Step 50 on page 144.
      - — VCS (for TDM Telephony). Continue at Step 55 on page 148.
    - For a custom GVP setup type (as selected in Step 9 on page 118), the Profiles task page for one or more of the following features, as applicable:
      - — Reporting. Continue at Step 41 on page 139.

— OBN Manager. Continue at Step 46 on page 143.

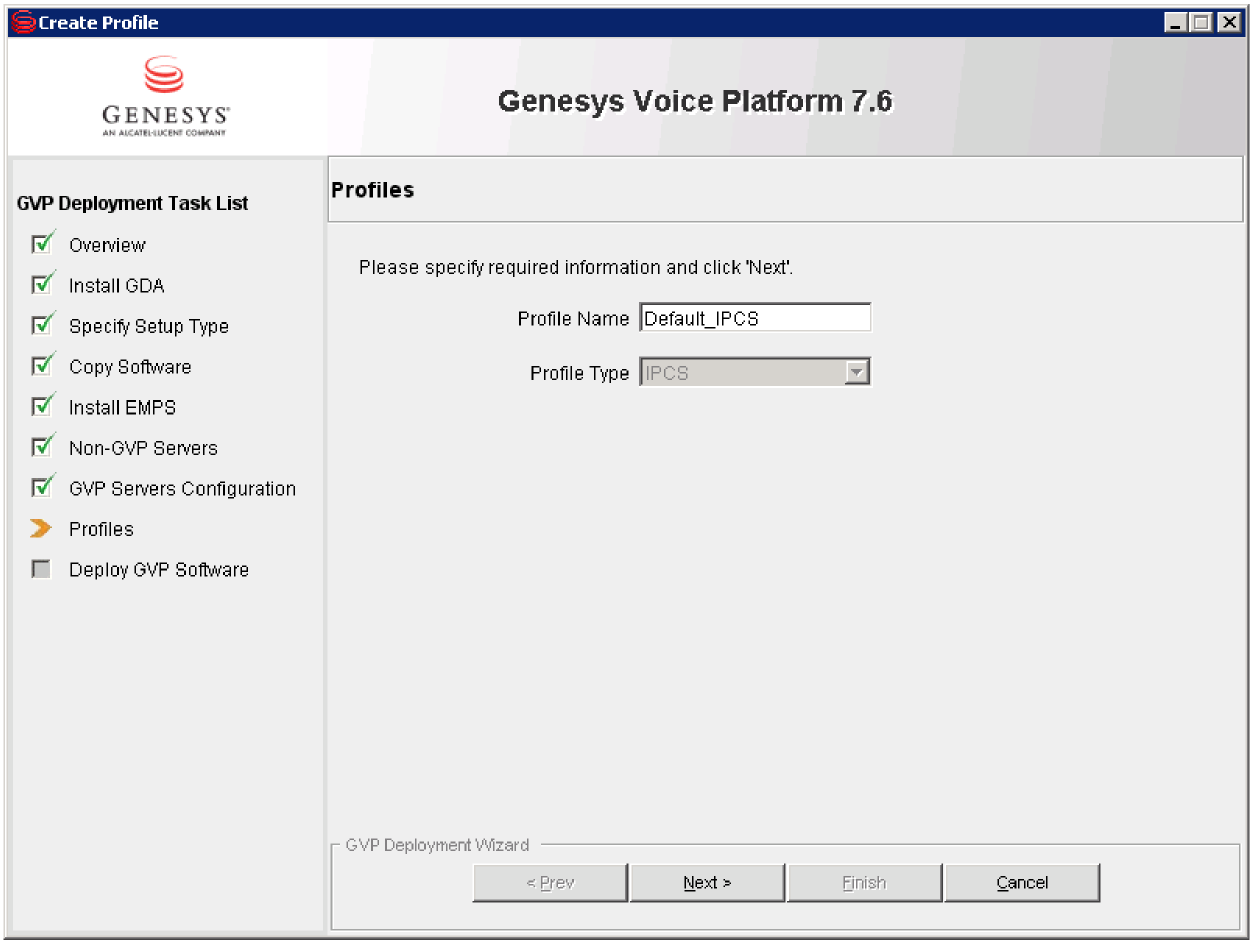
— IPCS (for IP Telephony) or VCS (for TDM Telephony).

For IPCS, continue at Step 50 on page 144.

For VCS, continue at Step 55 on page 148.

— ASR Log Manager. Continue at Step 59 on page 150.

Figure 19 is an example of the Profiles task page for configuring a profile (in this case IPCS).



Create Profile

Genesys Voice Platform 7.6

GVP Deployment Task List

- ☑ Overview
- ☑ Install GDA
- ☑ Specify Setup Type
- ☑ Copy Software
- ☑ Install EMPS
- ☑ Non-GVP Servers
- ☑ GVP Servers Configuration
- ➤ Profiles
- □ Deploy GVP Software

Profiles

Please specify required information and click 'Next'.

Profile Name: Default_IPCS

Profile Type: IPCS

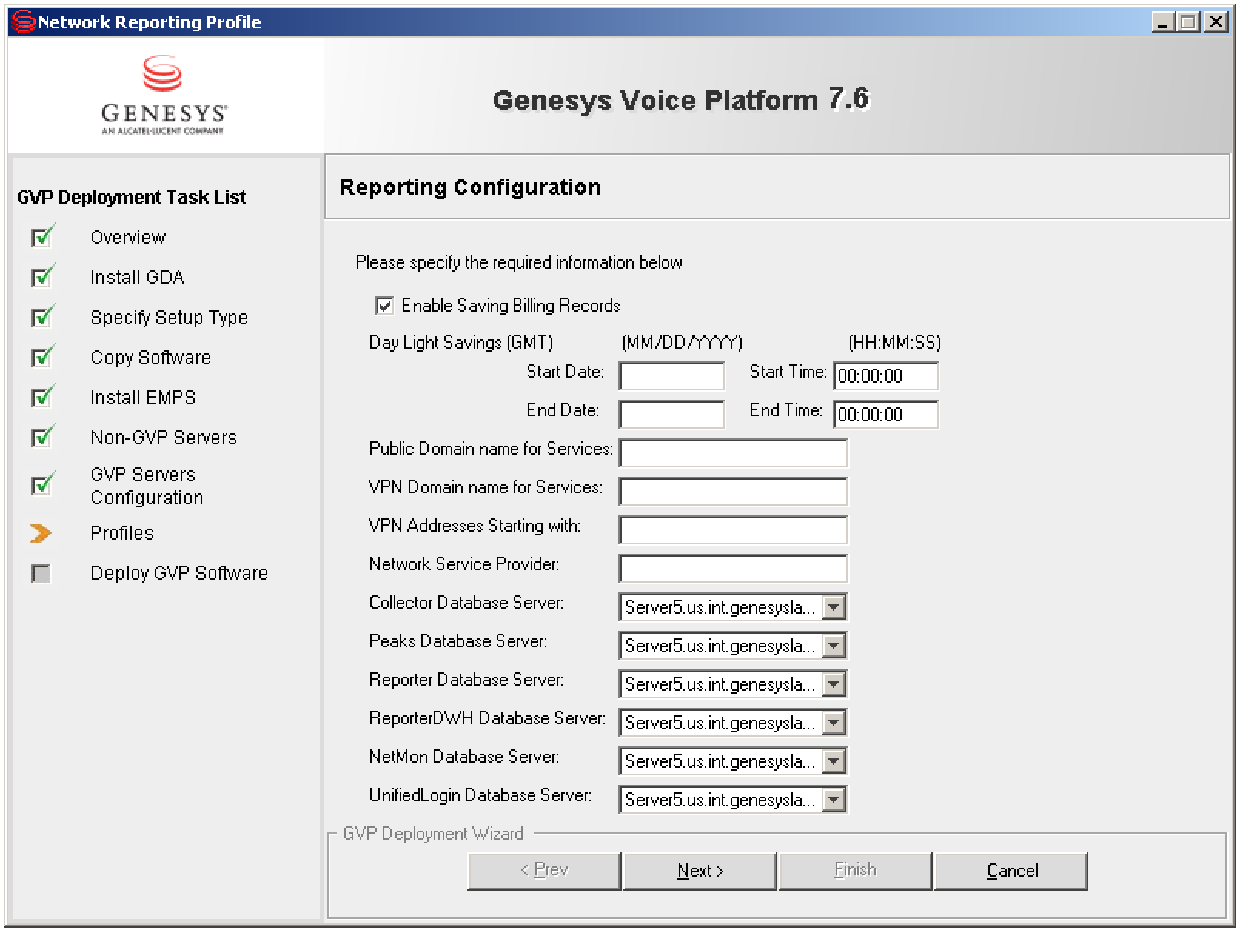
Figure 19: Profiles Task Page (IPCS)

Reporting

41. If you selected one of the Reporting features in Step 33 on page 132 (Reporter, Event C, Network Monitor, Call Status Monitor, or Login Server), the Profiles task page for configuring a Reporting profile appears. (The page is similar to the example shown in Figure 19 on page 139, for IPCS.)

To create or modify a Reporting profile, either accept the default name in the Profile Name text box on the Profiles task page, or enter a new name, and then click Next.

The Reporting Configuration page appears (see Figure 20).



Network Reporting Profile

Genesys Voice Platform 7.6

GVP Deployment Task List

- ☑ Overview
- ☑ Install GDA
- ☑ Specify Setup Type
- ☑ Copy Software
- ☑ Install EMPS
- ☑ Non-GVP Servers
- ☑ GVP Servers Configuration
- ➤ Profiles
- □ Deploy GVP Software

Reporting Configuration

Please specify the required information below

☑ Enable Saving Billing Records

Day Light Savings (GMT) (MM/DD/YYYY) (HH:MM:SS)

Start Date: Start Time: 00:00:00

End Date: End Time: 00:00:00

Public Domain name for Services:

VPN Domain name for Services:

VPN Addresses Starting with:

Network Service Provider:

Collector Database Server: Server5.us.int.genesysla...

Peaks Database Server: Server5.us.int.genesysla...

Reporter Database Server: Server5.us.int.genesysla...

ReporterDWH Database Server: Server5.us.int.genesysla...

NetMon Database Server: Server5.us.int.genesysla...

UnifiedLogin Database Server: Server5.us.int.genesysla...

Figure 20: Reporting Profile—Reporting Configuration Page

42. Using the text boxes and drop-down lists on the `Reporting Configuration` page, specify the required parameters for the Reporting profile. Table 20 describes the required parameters.

Table 20: Reporting Profile Parameters

Parameter	Description
Enable Saving Billing Records	Specifies whether billing records will be logged. Select the check box to enable logging.
Day Light Savings (GMT)	The Daylight Savings period for a location. • `Start Date`—The start date of daylight savings time. The date format is `MM/DD/YYYY`. • `Start Time`—The start time of daylight savings time, expressed in GMT. The time format is `HH:MM:SS`. • `End Date`—The end date of daylight savings time. The date format is `MM/DD/YYYY`. • `End Time`—The end time of daylight savings time, expressed in GMT. The time format is `HH:MM:SS`.
Public Domain name for Services	The public domain name for services. For example: `us.int.genesyslab.com`
VPN Domain name for Services	The Virtual Private Network (VPN) name for services. For example: `us.int.genesyslab.com`
VPN Addresses Starting with	The network portion of the IP addresses for the servers in the VPN domain. For example: `192.168.52`
Network Service Provider	The name of the Network Service Provider. The default value is `NSP`.
Collector Database Server	The FQDN of the database server that hosts the Collector database, as specified when you configured the SQL Server in Step 26 on page 125.
Peaks Database Server	The FQDN of the database server that hosts the Peaks database, as specified when you configured the SQL Server in Step 26 on page 125.

Table 20: Reporting Profile Parameters (Continued)

Parameter	Description
Reporter Database Server	The FQDN of the database server that hosts the Reporter database, as specified when you configured the SQL Server in Step 26 on page 125.
ReporterDWH Database Server	The FQDN of the database server that hosts the billing (ReporterDWH) database, as specified when you configured the SQL Server in Step 26 on page 125.
NetMon Database Server	The FQDN of the database server that hosts the network monitor (NetMon) database, as specified when you configured the SQL Server in Step 26 on page 125.
UnifiedLogin Database Server	The FQDN of the database server that hosts the unified login management (UnifiedLogin) database, as specified when you configured the SQL Server in Step 26 on page 125.

43. After you are satisfied that the Reporting profile parameters on the `Reporting Configuration` page are correct, click `Next`.

The `Profiles` page for assigning the Reporting profile appears. (For an example of the profile assignment page, for IPCS, see Figure 23 on page 147).

44. On the `Profiles` assignment page, verify that the list box on the right lists the server(s) to which you want to assign the profile.

- If the list box on the right is empty, or if you want to assign the profile to an additional GVP server, select the appropriate server from the list box on the left, and then click `Add` to move that server to the list box on the right.
- If the list box on the right contains an incorrect server, select the server, and then click `Remove` to move it to the list box on the left. This breaks the profile assignment.

45. After you are satisfied that the Reporting profile has been assigned to the correct servers on the `Profiles` assignment page, click `Next`.

The task page for configuring the next profile appears, as applicable:

- If you selected `OBN Manager` in Step 33 on page 132, the `Profiles` task page for configuring OBN Manager appears. Continue at Step 46.
- If you are performing a `Custom` installation but you did not select `OBN Manager` in Step 33 on page 132, the task page for configuring the applicable communication server profile appears:

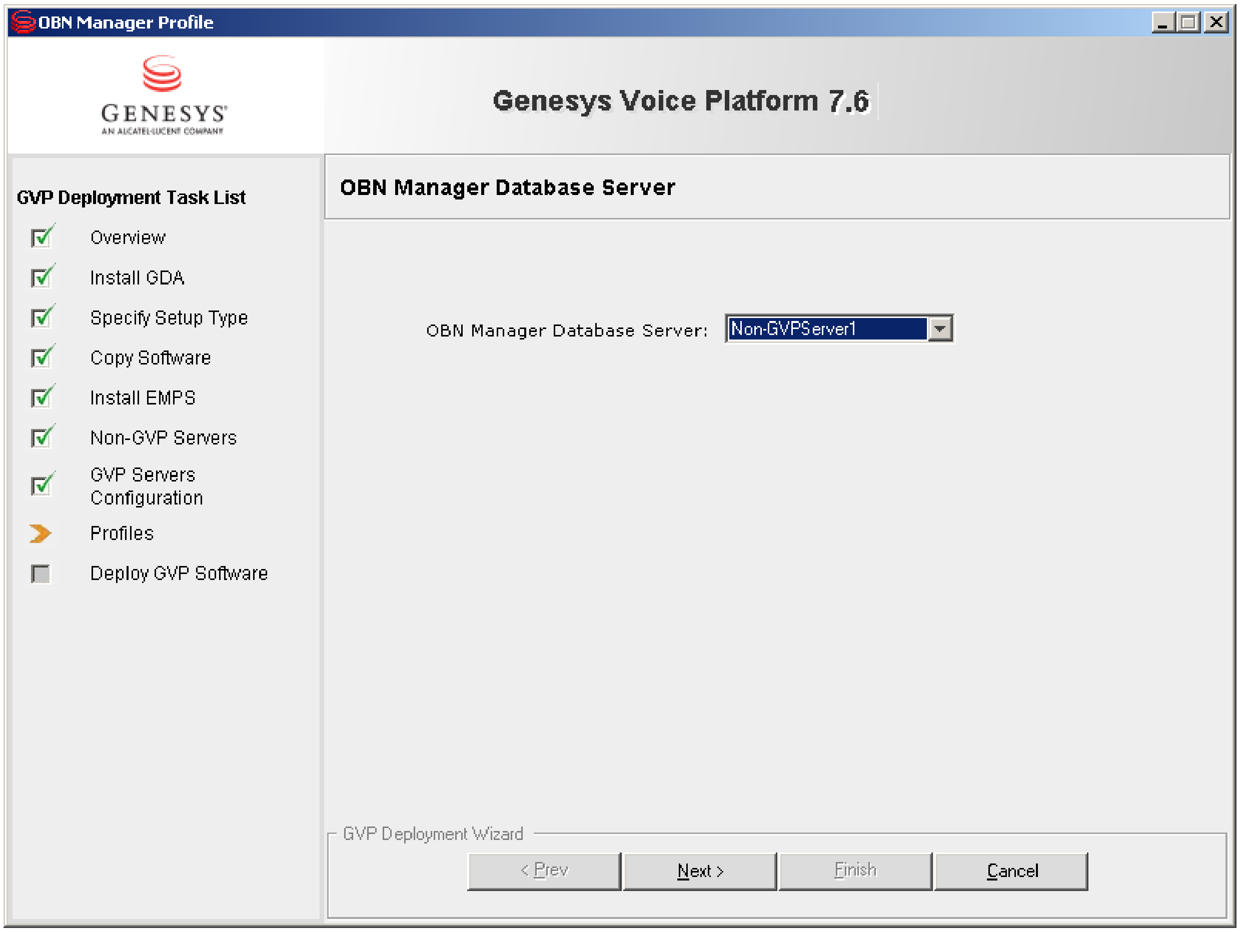
- — IPCS (for IP Telephony). Continue at Step 50 on page 144.
- — VCS (for TDM Telephony). Continue at Step 55 on page 148.

OBN Manager

46. If you selected `OBN Manager` in Step 33 on page 132, the task page for configuring an OBN Manager profile appears. (The page is similar to the example shown in Figure 19 on page 139, for IPCS.)

    To create or modify an OBN Manager profile, either accept the default name in the `Profile Name` text box on the `Profiles` task page, or enter a new name, and then click `Next`.

    The `OBN Manager Database Server` page appears (see Figure 21).



OBN Manager Database Server: Non-GVPServer1

Figure 21: OBN Manager Profile—OBN Manager Database Server Page

47. From the drop-down list on the `OBN Manager Database Server` page, select the name of the database server that hosts the OBN Manager database, as specified when you configured the SQL Server in Step 26 on page 125.

    Click `Next`.

    The `Profiles` page for assigning the OBN Manager profile appears. (For an example of the profile assignment page, for IPCS, see Figure 23 on page 147).

48. On the Profiles assignment page, verify that the list box on the right lists the server(s) to which you want to assign the profile.
    - If the list box on the right is empty, or if you want to assign the profile to an additional GVP server, select the appropriate server from the list box on the left, and then click Add to move that server to the list box on the right.
    - If the list box on the right contains an incorrect server, select the server, and then click Remove to move it to the list box on the left. This breaks the profile assignment.

49. After you are satisfied that the OBN Manager profile has been assigned to the correct servers on the Profiles assignment page, click Next.

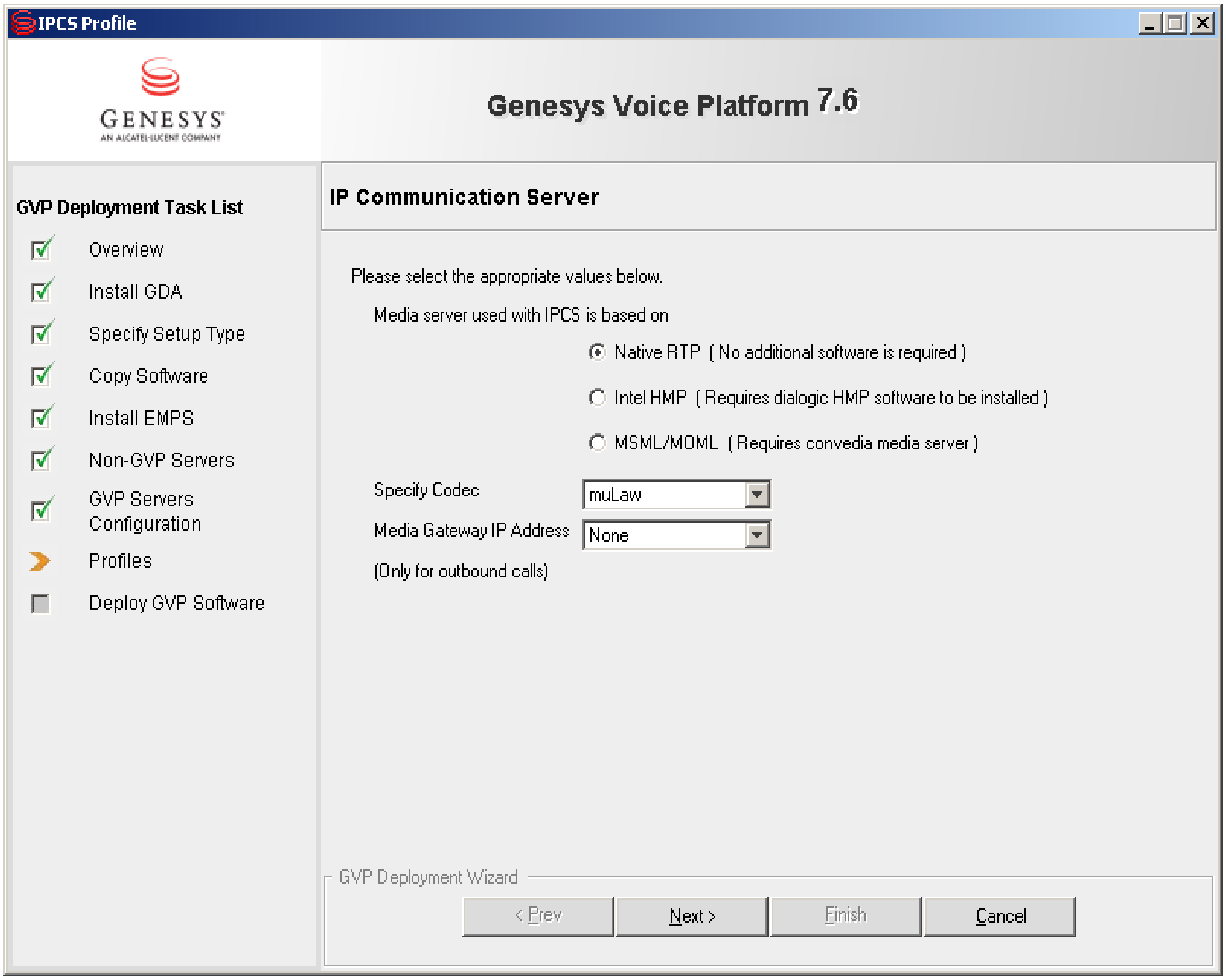
    The task page for configuring the next profile appears, as applicable:
    - If you selected IP Telephony in Step 9 on page 118 and IPCS in Step 33 on page 132, the Profiles task page for configuring an IPCS profile appears. Continue at Step 50.
    - If you selected TDM Telephony in Step 9 on page 118 and VCS in Step 33 on page 132, the Profiles task page for configuring a VCS profile appears. Continue at Step 55 on page 148.

IPCS

50. If you selected IPCS in Step 33 on page 132, the Profiles task page for configuring an IPCS profile appears (see Figure 19 on page 139).

    To create or modify an IPCS profile, either accept the default name in the Profile Name text box on the Profiles task page, or enter a new name, and then click Next.

    The IP Communication Server page appears (see Figure 22).



IP Communication Server

Please select the appropriate values below.

Media server used with IPCS is based on

● Native RTP (No additional software is required)

○ Intel HMP (Requires dialogic HMP software to be installed)

○ MSML/MOML (Requires convedia media server)

Specify Codec: muLaw

Media Gateway IP Address: None

(Only for outbound calls)

Figure 22: IPCS Profile—IP Communication Server Configuration Page

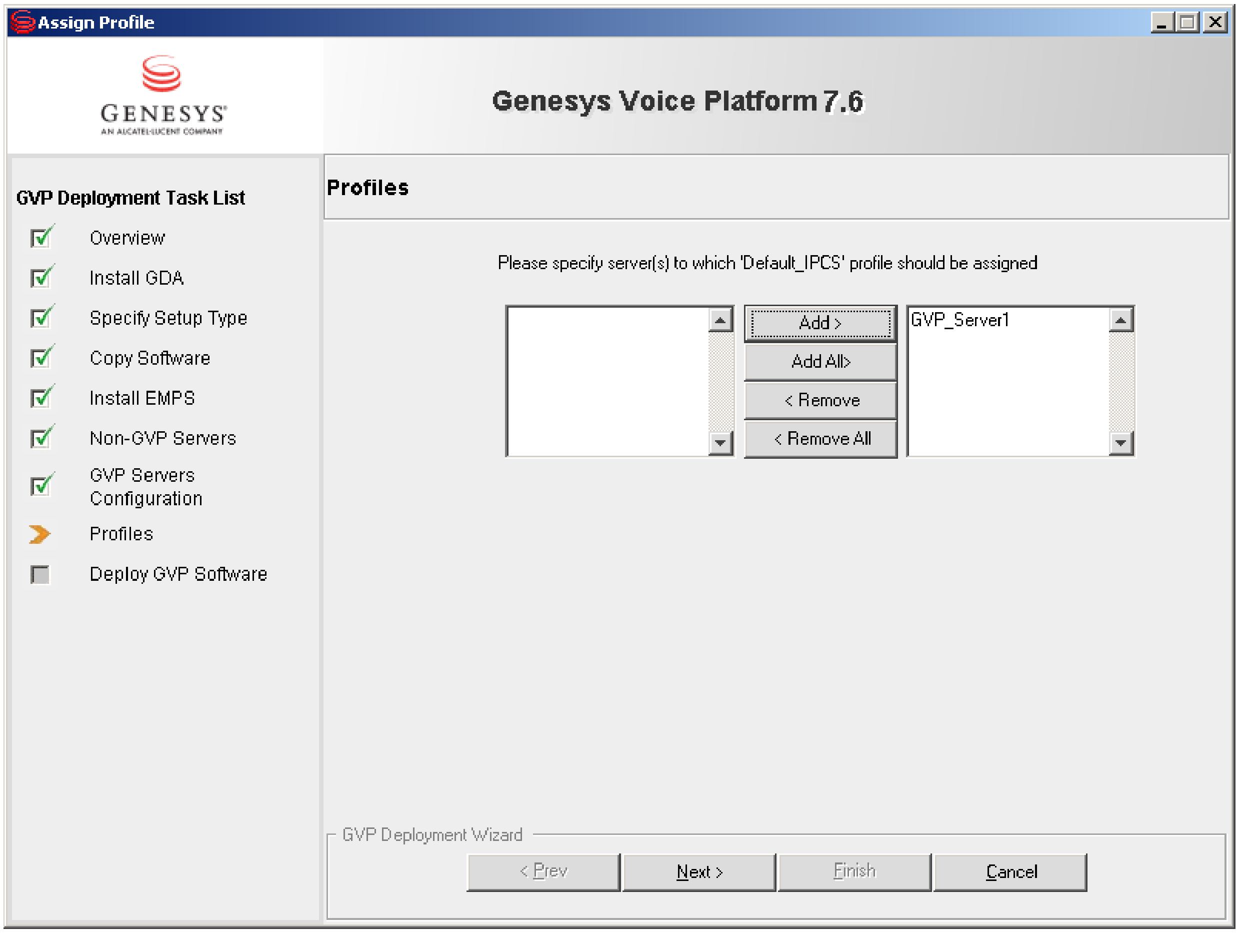
51. Using the radio buttons and drop-down lists on the `IP Communication Server` page, specify the required IPCS parameters. Table 21 describes the required parameters.

Table 21: IP Communication Server Profile Parameters

Parameters	Description
Media server used with IPCS is based on	The protocol that Media Server uses to communicate with IPCS. The valid values are: • `Native RTP` • `Intel HMP`—used with Dialogic HMP software • `MSML`—used with Convedia Media Server
Specify Codec	The codec that Media Server uses. The values that you can specify in the wizard are: • `muLaw`—usual in North America and Japan • `aLaw`—usual in countries other than North America and Japan If you want to specify support for additional features, modify the Media Server configuration in the EMPS after installation. **Note:** Ensure that the Media Gateway and MRCP servers use the same codec value.
Media Gateway IP Address	The IP address of the Media Gateway. **Note:** This parameter is for Outbound calls only.
Dispenser Server.	The FQDN of the server that hosts Dispenser. **Note:** This parameter is visible only if you selected the Dispenser feature in Step 33 on page 132.

52. After you are satisfied that the IPCS profile parameters on the `IP Communication Server` page are correct, click `Next`.

The `Profiles` page for assigning the IPCS profile appears (see Figure 23).



Please specify server(s) to which 'Default_IPCS' profile should be assigned

GVP_Server1

Figure 23: Profiles Task Page—Assigning the Profile

53. On the `Profiles` assignment page, verify that the list box on the right lists the server(s) to which you want to assign the profile.
    - If the list box on the right is empty, or if you want to assign the profile to an additional GVP server, select the appropriate server from the list box on the left, and then click `Add` to move that server to the list box on the right.
    - If the list box on the right contains an incorrect server, select the server, and then click `Remove` to move it to the list box on the left. This breaks the profile assignment.

54. After you are satisfied that the IPCS profile has been assigned to the correct servers on the `Profiles` assignment page, click `Next`.
    - If you are performing a `Typical` GVP setup (as selected in Step 9 on page 118), or if you are performing a `Custom` installation and you did not select `ASR Log Manager` in Step 33 on page 132, the `Profiles` task page for managing your profiles appears. Continue at Step 63 on page 152.

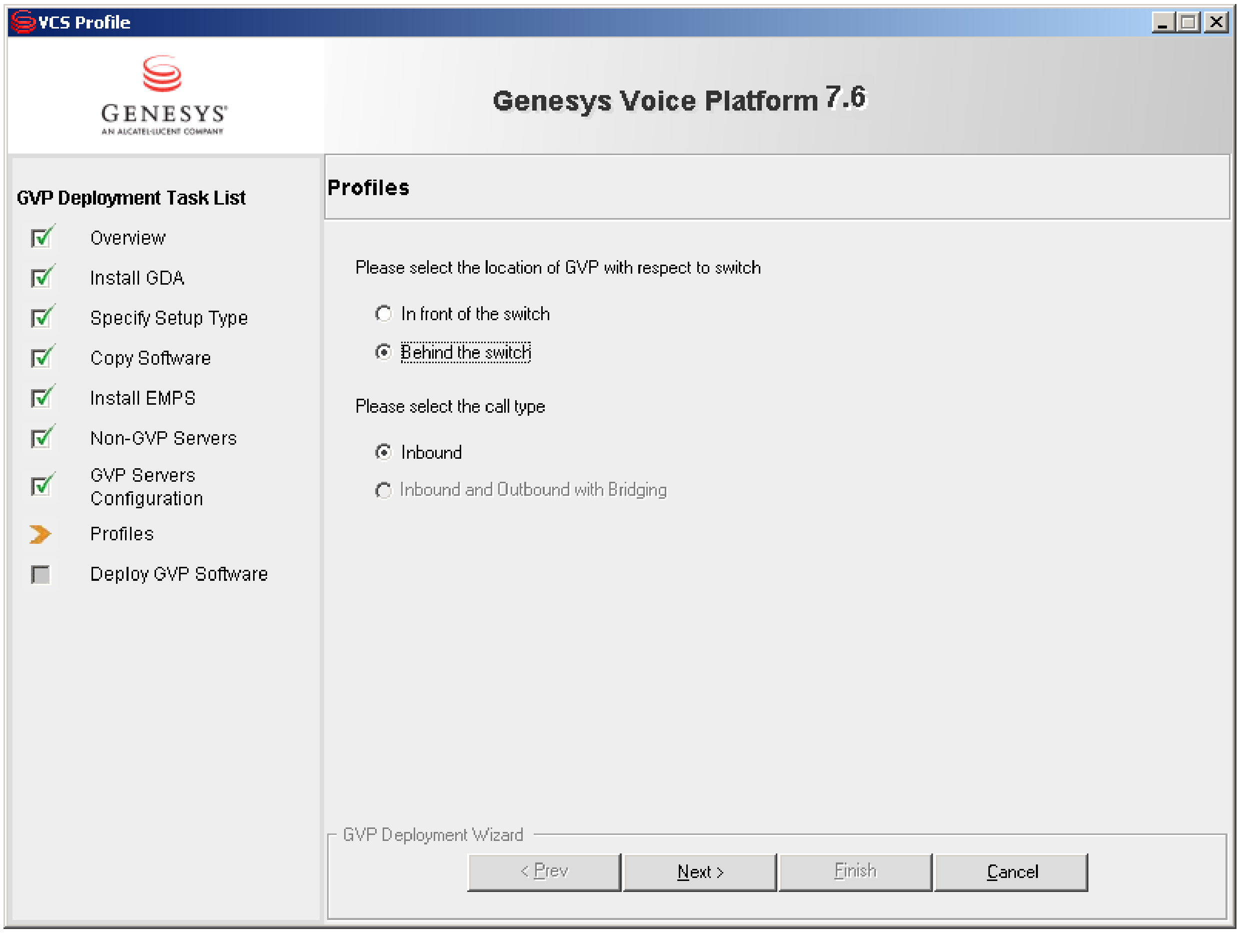
- If you are performing a `Custom` installation and you selected `ASR Log Manager` in Step 33 on page 132, the `Profiles` task page for configuring the ASR Log Manager profile appears. Continue at Step 59 on page 150.

VCS

55. If you selected `VCS` in Step 33 on page 132, the `Profiles` task page for configuring a VCS profile appears. (The page is similar to the example shown in Figure 19 on page 139, for IPCS.)

To create or modify a VCS profile, either accept the default name in the `Profile Name` text box on the `Profiles` task page, or enter a new name, and then click `Next`.

The `Profiles` task page for selecting the location of GVP with respect to the switch appears (see Figure 24).



Please select the location of GVP with respect to switch

○ In front of the switch

● Behind the switch

Please select the call type

● Inbound

○ Inbound and Outbound with Bridging

Figure 24: VCS Profile—Profiles Task Page for GVP Location with Respect to the Switch

56. Using the radio buttons on the `Profiles` task page:

a. Specify the location of GVP with respect to the switch.

- `In front of the switch`—The VCS determines which VoiceXML application to execute based on the DNIS given by the call signaling that is used to setup the call.

- Behind the switch—The VCS determines which VoiceXML application to execute based on information provided by IVR Server. When a call arrives on the VCS, the VCS contacts the IVR Server to determine which application to execute.

b. Specify the call type.

- Inbound
- Inbound and Outbound with Bridging—Refers to the capability of transferring an inbound call by creating an outbound leg, and then bridging the outbound leg with the inbound caller's leg.

Note: The Inbound and Outbound with Bridging option is not available in a behind-the-switch configuration. In a behind-the-switch configuration, the transfer to an agent happens with the help of the Private Branch Exchange (PBX).

c. Click Next.

The Profiles page for assigning the VCS profile appears. (For an example of the profile assignment page, for IPCS, see Figure 23 on page 147).

57. On the Profiles assignment page, verify that the list box on the right lists the server(s) to which you want to assign the profile.

- If the list box on the right is empty, or if you want to assign the profile to an additional GVP server, select the appropriate server from the list box on the left, and then click Add to move that server to the list box on the right.
- If the list box on the right contains an incorrect server, select the server, and then click Remove to move it to the list box on the left. This breaks the profile assignment.

58. After you are satisfied that the VCS profile has been assigned to the correct servers on the Profiles assignment page, click Next.

- If you are performing a Typical GVP setup (as selected in Step 9 on page 118), or if you are performing a Custom installation and you did not select ASR Log Manager in Step 33 on page 132, the Profiles task page for managing your profiles appears. Continue at Step 63 on page 152.

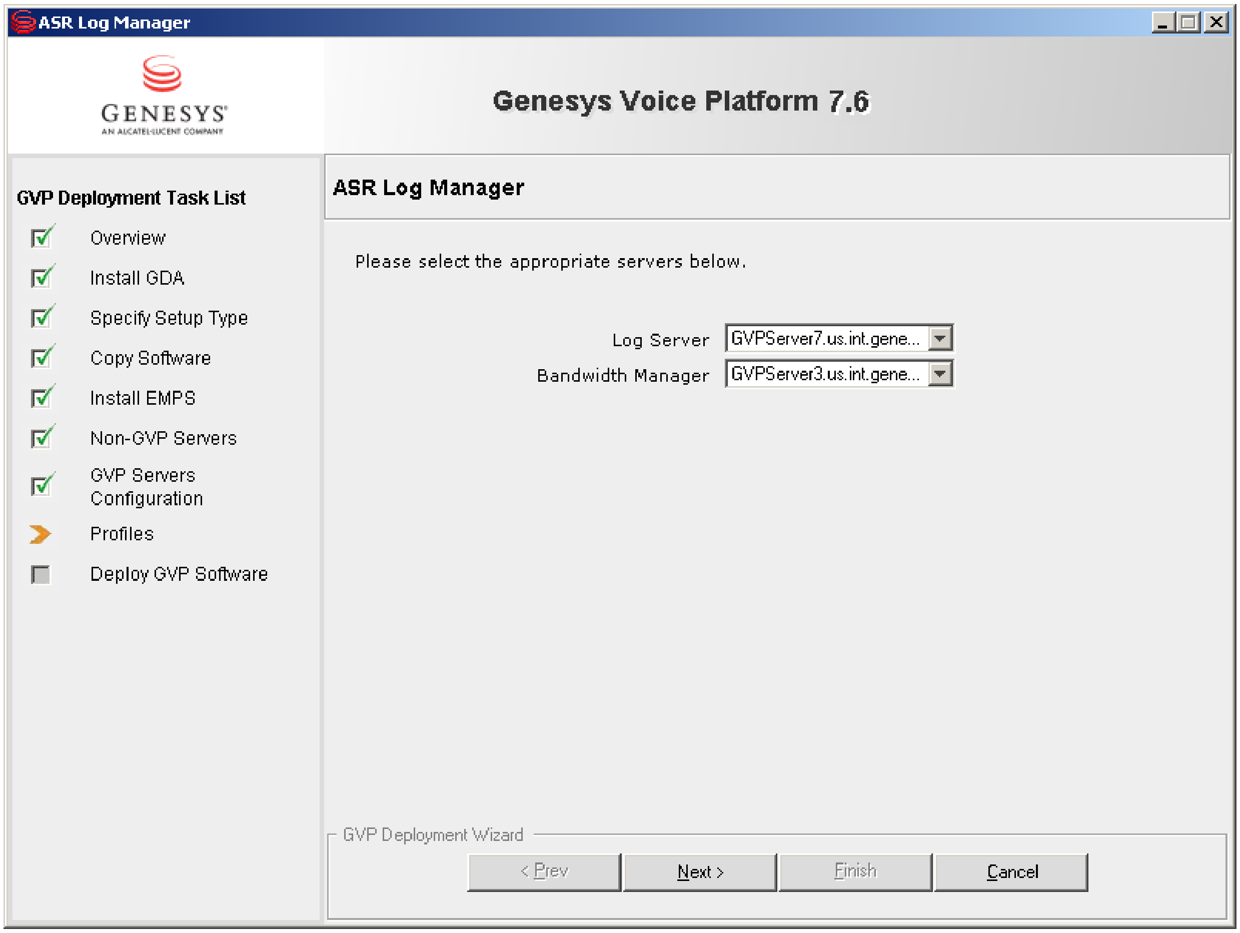
- If you are performing a Custom installation and you selected ASR Log Manager in Step 33 on page 132, the Profiles task page for configuring the ASR Log Manager profile appears. Continue at Step 59.

ASR Log Manager

59. If you selected ASR Log Manager in Step 33 on page 132, the task page for configuring an ASR Log Manager profile appears. (The page is similar to the example shown in Figure 19 on page 139, for IPCS.)

    To create or modify an ASR Log Manager profile, either accept the default name in the Profile Name text box on the Profiles task page, or enter a new name, and then click Next.

    The ASR Log Manager page appears (see Figure 25).



ASR Log Manager

Please select the appropriate servers below.

Log Server GVPServer7.us.int.gene...
Bandwidth Manager GVPServer3.us.int.gene...

Figure 25: ASR Log Manager Profile—ASR Log Manager Page

60. From the drop-down lists on the ASR Log Manager page, select the FQDNs of the following servers, as specified when you selected the GVP server features in Step 33 on page 132:

    - Log Server—The GVP server machine that hosts the ASR Log Server.

- `Bandwidth Manager`—The GVP server machine that hosts the Bandwidth Manager.

Click `Next`.

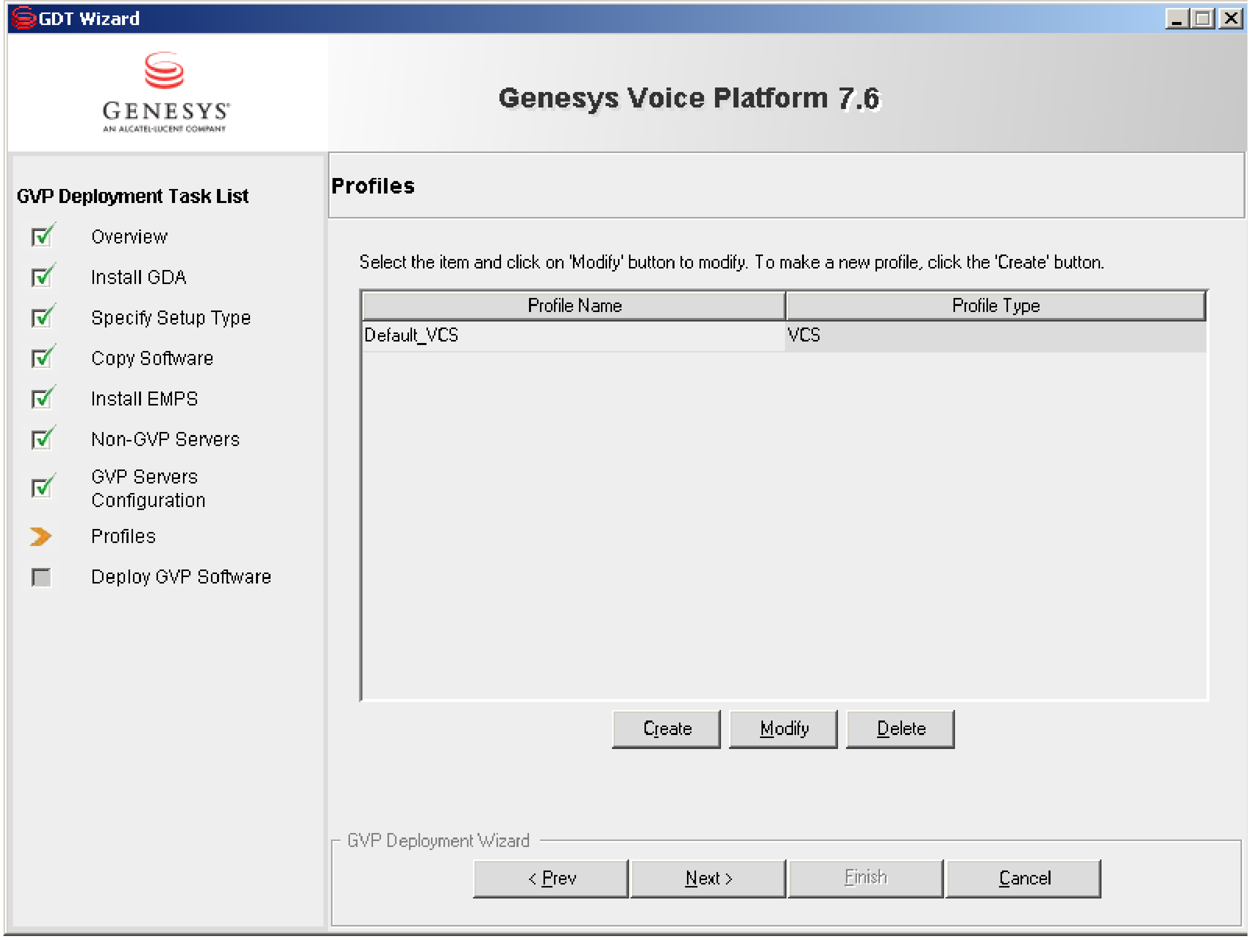
The `Profiles` page for assigning the ASR Log Manager profile appears. (For an example of the profile assignment page, for IPCS, see Figure 23 on page 147).

61. On the `Profiles` assignment page, verify that the list box on the right lists the server(s) to which you want to assign the profile.

- If the list box on the right is empty, or if you want to assign the profile to an additional GVP server, select the appropriate server from the list box on the left, and then click `Add` to move that server to the list box on the right.
- If the list box on the right contains an incorrect server, select the server, and then click `Remove` to move it to the list box on the left. This breaks the profile assignment.

62. After you are satisfied that the ASR Log Manager profile has been assigned to the correct servers on the `Profiles` assignment page, click `Next`.

The `Profiles` task page for managing your profiles appears (see Figure 26).



GVP Deployment Task List

- ☑ Overview
- ☑ Install GDA
- ☑ Specify Setup Type
- ☑ Copy Software
- ☑ Install EMPS
- ☑ Non-GVP Servers
- ☑ GVP Servers Configuration
- ➤ Profiles
- □ Deploy GVP Software

Profiles

Select the item and click on 'Modify' button to modify. To make a new profile, click the 'Create' button.

Profile Name	Profile Type
Default_VCS	VCS

Figure 26: Profiles Task Page—Managing Your Profiles

Managing Profiles

63. On the `Profiles` task page to manage profiles, review your existing profiles.

    Buttons on the task page enable you to do the following:

    - `Create`—Create a new profile.

      To create a new profile, click `Create`. You are presented with the task pages to configure a new profile of a particular type.

    - `Modify`—Modify an existing profile.

      To modify an existing profile, select the profile, and then click `Modify`. You are presented with the task pages to configure that profile.

      For more information about the task pages to configure a new profile or modify an existing one, see:

      — IPCS, Step 50 on page 144

      — VCS, Step 55 on page 148

      — Reporting, Step 41 on page 139

      — OBN Manager, Step 46 on page 143

      — ASR Log Manager, Step 59 on page 150

- `Delete`—Delete an existing profile.

  To delete an existing profile, select the profile, and then click `Delete`.

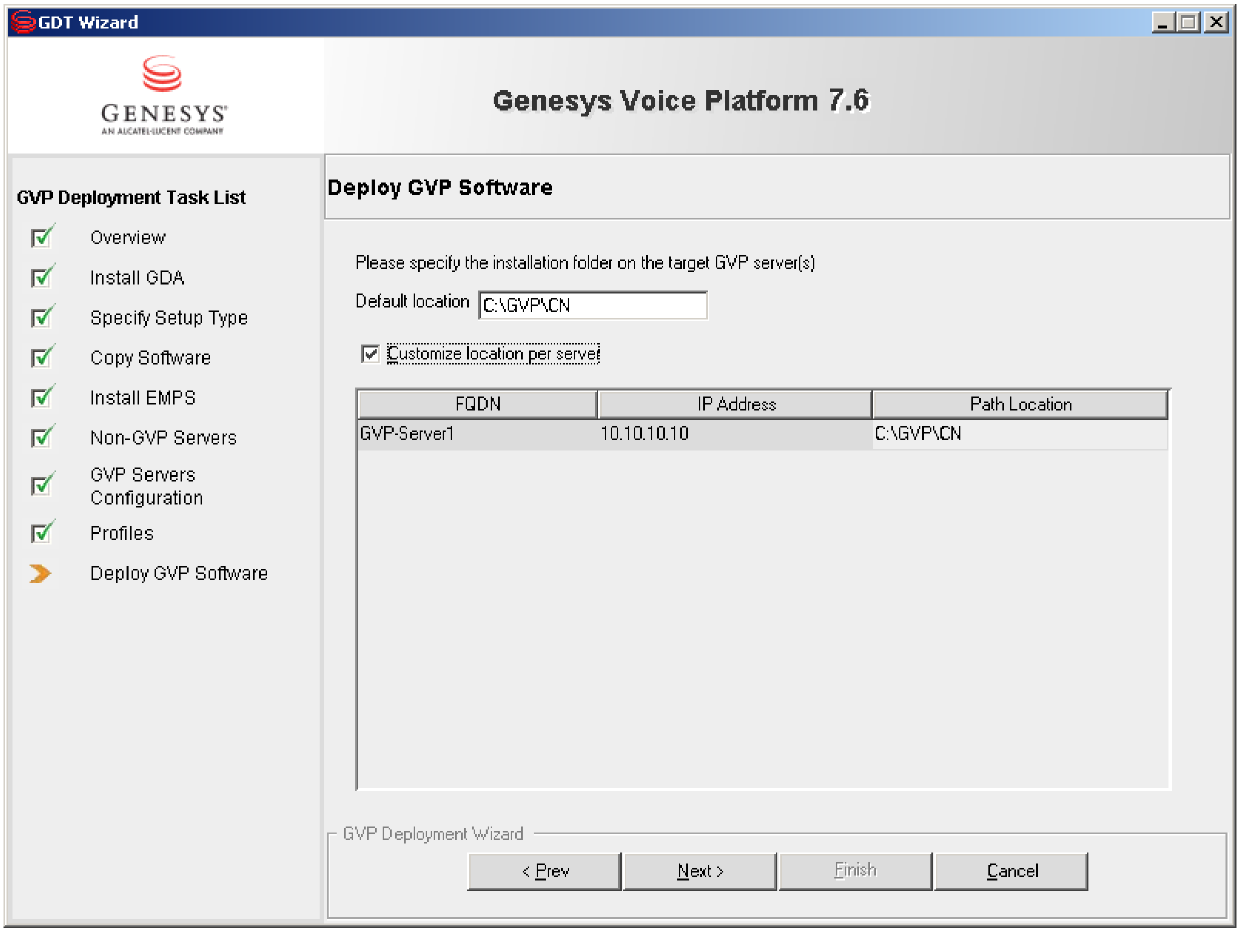
64. After you are satisfied that the correctly configured profiles on the `Profiles` task page to manage profiles have been assigned to the correct GVP servers, click `Next`.

The `Deploy GVP Software` information page appears.

Deploy GVP Software

65. On the `Deploy GVP Software` information page, read the information about the tasks involved with GVP software deployment, and then click `Next`.

The `Deploy GVP Software` task page for specifying the GVP installation folders appears (see Figure 27).



Deploy GVP Software

Please specify the installation folder on the target GVP server(s)

Default location C:\GVP\CN

☑ Customize location per server

FQDN	IP Address	Path Location
GVP-Server1	10.10.10.10	C:\GVP\CN

Figure 27: Deploy GVP Software Page—Specifying the GVP Installation Folders

66. On the Deploy GVP Software page, specify the folder in which GVP software will be installed on the GVP server(s).

a. In the `Default Location` text box, either accept the default value (`C:\GVP\CN`), or enter a new default location that all GVP servers will use.

b. To customize the location for individual GVP servers that host the GVP software:

i. Select the `Customize Locations per server` check box.

ii. For each server whose installation location you want to customize, double-click the `Path Location` box in the row for the server, and specify the custom location.

c. Click `Next`.

The GDT validates the Windows prerequisites for the GVP servers, then displays the results.

- If validation is successful, a `Validation Successful` page appears. Continue at Step 67.
- If any GVP servers fail to meet the software prerequisites, a `Validation Failed` page appears. Click `Finish` to exit the wizard. Before you can install the GVP software, you must either install the required prerequisites on the GVP servers or else reconfigure the deployment model to use other, conforming GVP servers. To resume using the wizard to deploy GVP, do one of the following:
  - — Relaunch the wizard and, on the `Select Activity` page (Step 4 on page 116), select the option to add to an existing deployment. Step through all the remaining sections of the wizard, modifying settings if necessary, until you receive the `Validation Successful` page. Continue at Step 67.
  - — Using commands on the GDT menu, launch portions of the wizard as required to modify settings. Use the GDT `Deploy > Deploy > Selected servers` command to select the target GVP servers and relaunch the `Deploy GVP Software` portion of the wizard. Continue at Step 65 on page 153.

    For more information about the GDT menu commands, see “GDT Menus” on page 102.

For more information about GDT validation of software prerequisites, see “Validating System Requirements” on page 107.

67. On the `Validation Successful` page, click `Next`.

The `Deploy GVP Software` page to install and configure the GVP servers appears.

Note: The GDT automatically saves the deployment model at this time.

68. On the `Deploy GVP Software` page to install and configure the GVP servers, click `Next`.

    The `Installation and Configuration started` page appears. The GDT transfers the installation software from the GDT machine to the target machines, based on the selected components and features, and instructs the GDA to install and configure the GVP components. The `Installation and Configuration started` page is updated with the status of the installation, including errors, as the installation progresses.

69. When the `Installation and Configuration started` page displays the status message that feature configuration has been completed, click `Finish` to exit the wizard.

    You are returned to the GDT.

70. Verify that the GVP installation completed successfully and that the configuration is correct.

    a. Review the GDT logs. For more information about viewing GDT logs, see Viewing log files in the GDT, page 158.

    b. Access the GVP Portal, and confirm that the links to the GVP servers are correct and working.

       To access the GVP Portal, use the following URL:

       `http://<FQDN of EMPS machine>:9810/gvpportal`

End of procedure

Next Steps

- Add the EMPS URL (`http://<EMPS-hostname>:9810`) as a Trusted Site in Internet Explorer, on the `Tools > Internet Options > Security` tab.
- If you included EMS Reporting components or OBN Manager in your deployment, create the databases, set the required file access permissions, and perform other activities to enable EventC reporting, Unified Login, and Network Monitor. For more information, see Chapter 10 on page 181.
- Verify or modify server configurations in the EMPS. For more information, see the chapters about the individual components in Part 3: “GVP Configuration” on page 287.
- If your deployment uses IVR Servers, create and configure the IVR Servers (see “Configuring IVR Server” on page 301).
- Start WatchDog on the GVP servers (see Starting/Restarting GVP in Normal mode (Windows), page 198).

Procedure:
Adding GVP components using the GDT

Purpose: To use the GDT to add GVP components to an existing deployment.

Use this procedure to add GVP features to existing GVP servers, or to add new GVP servers to the deployment.

Prerequisites

- See the Prerequisites items for Using the GVP Deployment Wizard to install GVP components (Windows only), page 113.

Start of procedure

1. Execute the `GVPLaunch.bat` file to launch the GDT and the GVP Deployment Wizard.

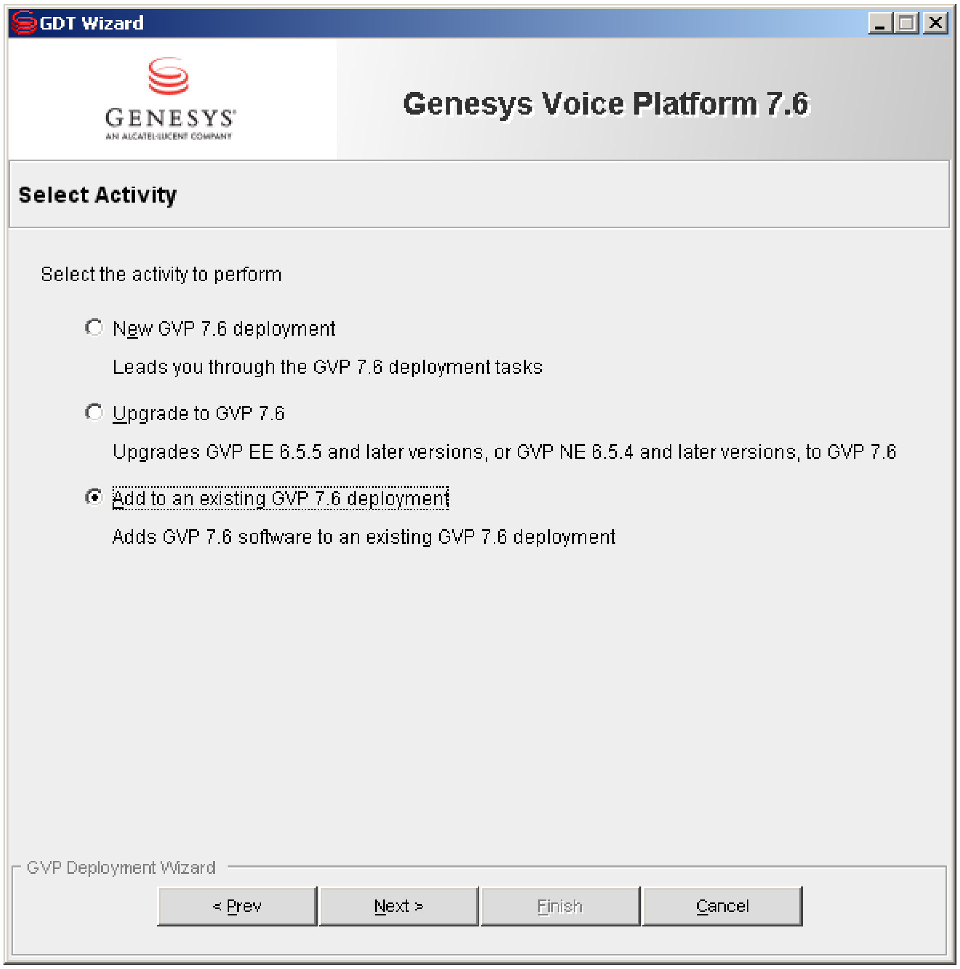
   For more information about launching the GDT and the wizard, see the first steps in the procedure Using the GVP Deployment Wizard to install GVP components (Windows only), page 113.

2. On the `Welcome` page of the wizard, click `Next`.

   The `Genesys License Agreement` page appears.

3. Select the `I accept the above agreement` check box, and then click `Next`.

   The `Select Activity` page appears (see Figure 28).



Select Activity

Select the activity to perform

○ New GVP 7.6 deployment

Leads you through the GVP 7.6 deployment tasks

○ Upgrade to GVP 7.6

Upgrades GVP EE 6.5.5 and later versions, or GVP NE 6.5.4 and later versions, to GVP 7.6

● Add to an existing GVP 7.6 deployment

Adds GVP 7.6 software to an existing GVP 7.6 deployment

Figure 28: Select Activity Page—Add to a Deployment

4. On the `Select Activity` page, select `Add to an existing GVP 7.6 deployment`, then click `Next`.

   The `Overview` page appears.

   To continue stepping through the full wizard, continue as described from Step 5 of Using the GVP Deployment Wizard to install GVP components (Windows only), on page 117.

   To go directly to targeted portions of the wizard, continue at Step 5 of this procedure.

5. To go directly to targeted portions of the wizard:

   a. Cancel out of the wizard, so that the GDT window has focus.

b. Use the commands on the `GVP Deployment`, `Modify`, or `Deploy` menus of the GDT to launch the applicable portions of the wizard, and then follow the instructions that are provided for that part of the wizard in Using the GVP Deployment Wizard to install GVP components (Windows only), page 113.

   For more information about the GDT menu commands, see“GDT Menus” on page 102.

End of procedure

Next Steps

- If you added EMS Reporting components or OBN Manager to your deployment, create the databases, set the required file access permissions, and perform other activities to enable EventC reporting, Unified Login, and Network Monitor. For more information, see Chapter 10 on page 181.
- Verify or modify the new server configurations in the EMPS. For more information, see the chapters about the individual components in Part 3: “GVP Configuration” on page 287.
- Start or restart WatchDog on the GVP servers you added or modified (see Starting/Restarting GVP in Normal mode (Windows), page 198).

Viewing Log Files with the GDT

This section describes how you can use the GDT to view GVP log files during setup or runtime.

Procedure:
Viewing log files in the GDT

Purpose: To use the GDT to display log files for the GDT, the GDA, and GVP processes.

Start of procedure

1. If the GDT is not open, execute the batch file to launch the GDT.
   - If you are using the GVP Base Software CD, double-click `GVPLaunch.bat` in the `<CDImage>\solution_specific\windows\install` folder.

- If the CD Image is on a network drive, copy the `<CDImage>\solution_specific\windows\install` folder to the local machine, and then double-click `GVPLaunch.bat` in the local folder.

The GDT and the GVP Deployment Wizard open simultaneously, in separate windows. Ensure that the `GVP Deployment Tool` window has focus.

2. In the `GVP Deployment Tool` window, select `View > Log Message Viewer.`

   The `GDT Message Viewer` window opens (for an example, see Figure 9 on page 102).

3. From the `View logs for` drop-down list in the `GDT Message Viewer` window, specify the type of log that you want to view. You can select the following log types:

   - `Deployment Tool`—Displays logs relating to GDT activities on the local host. The log files are stored in the following location on the host on which the GDT is running:

     `C:\GDT\logs`

   - `Deployment Agent`—Displays logs relating to GDA activities on a server that you select (see Step 4). The log files are stored in the following location on the applicable server:

     `C:\GDT\logs`

   - `GVP Processes`—Displays logs relating to GVP processes (for example, WatchDog and Scheduler) on a server that you select (see Step 4). The log files are stored in the following location on the applicable server:
     `C:\GVP\CN\log`

4. If you selected the `Deployment Agent` or `GVP Processes` log type in Step 3, also specify the GVP server for which you want to view logs. Select the applicable server from the on `server` drop-down list.

5. Click `Get Logs.`

   The main `Message Viewer` pane is populated with log files that have been generated since you first launched the GDT, with the most recent displaying by default.

   To view a different log file of the specified log type, click the log file in the list in the left-hand pane.

6. If you selected the `Deployment Tool` or `Deployment Agent` log type in Step 3, you can change the level of log messages that display.

   To change the log level, select the log level from the `Show messages of type` drop-down list, and then click `Refresh.`

   The following log levels are available:

   - `Severe`
   - `Warning, Severe`
   - `Info, Warning, Severe`
   - `All types`

7. To exit the GDT Message Viewer, click `Close Window`.

End of procedure

Chapter

7

Installing GVP: DE with the GVP Deployment Tool

This chapter describes how to use the GVP Deployment Tool (GDT) to perform a new installation of the Genesys Voice Platform (GVP): Developers Edition (DE) on windows.

This chapter contains the following sections:

Note: Using the GDT is recommended, but optional. See Appendix B, “Manual Installation on Windows,” on page 505 for instructions on how to install GVP without using the GDT.

Installing GVP Deployment Agent

The following procedure describes the steps to install the GDA.

Procedure: Installing the GDA for GVP:DE

Note: Take note of the fully qualified domain name (FQDN), and IP Address of each GVP server as you will be required to specify this information when using the GDT to install components. In order for the GVP detection software to work properly, FQDNs must not contain special characters such as the underscore (_). Standard characters include letters (A-Z, a-z), digits (0-9), and hyphens (-).

Start of procedure

1. If you are using the GVP Developer's Edition CD, double-click `InstallAgent.bat` from the `<CDImage>/solution_specific/windows/install` folder
   or
   If the CD Image is on a network drive, copy the `<CDImage>/solution_specific/windows/install` folder to the local machine and then double-click `InstallAgent.bat` from the local folder.

   A Disk Operating System (DOS) window will be displayed for approximately 30 seconds showing the progress of the GDA installation. Upon completion of the installation, the DOS window will close.
2. From the Windows `Start` menu, select `Control Panel > Administrative Tools > Services`, and confirm that the GDA service has started.

End of procedure

Installing GVP: DE

The following procedure describes how to use the GDT to perform a new installation of the Genesys Voice Platform: Developer's Edition (GVP: DE) components.

Procedure:
Installing GVP:DE using the GDT

Summary

The GVP: DE deployment process consists of the following tasks:

- Overview
- Install GDA
- Copy Software
- Install EMPS
- Non-GVP Servers
- GVP Servers Configuration
- Profiles
- Deploy GVP Software

Start of procedure

1. On the GVP Developer's Edition CD, navigate to the solution_specific/windows/install folder.
2. Double-click GVPLaunch.bat.

   The GVP Deployment Tool screen appears followed by the Welcome screen of the GVP Deployment Wizard.
3. Click Next.

   The Genesys License Agreement screen appears.
4. Select the I accept the above agreement check box, and then click Next.

   The Select Activity screen appears.
5. Select New GVP 7.6 deployment, and then click Next.

   For information about adding to an existing GVP 7.6 deployment, see Adding GVP components using the GDT, page 156.

   The Overview task screen appears.

Overview

The left pane of the Overview screen, and all subsequent pages of the GVP Deployment Wizard, contains a GVP Deployment Task List that shows your progress through the GVP: DE deployment process.

6. Click Next.
7. The Install GDA task screen appears.

Install GDA

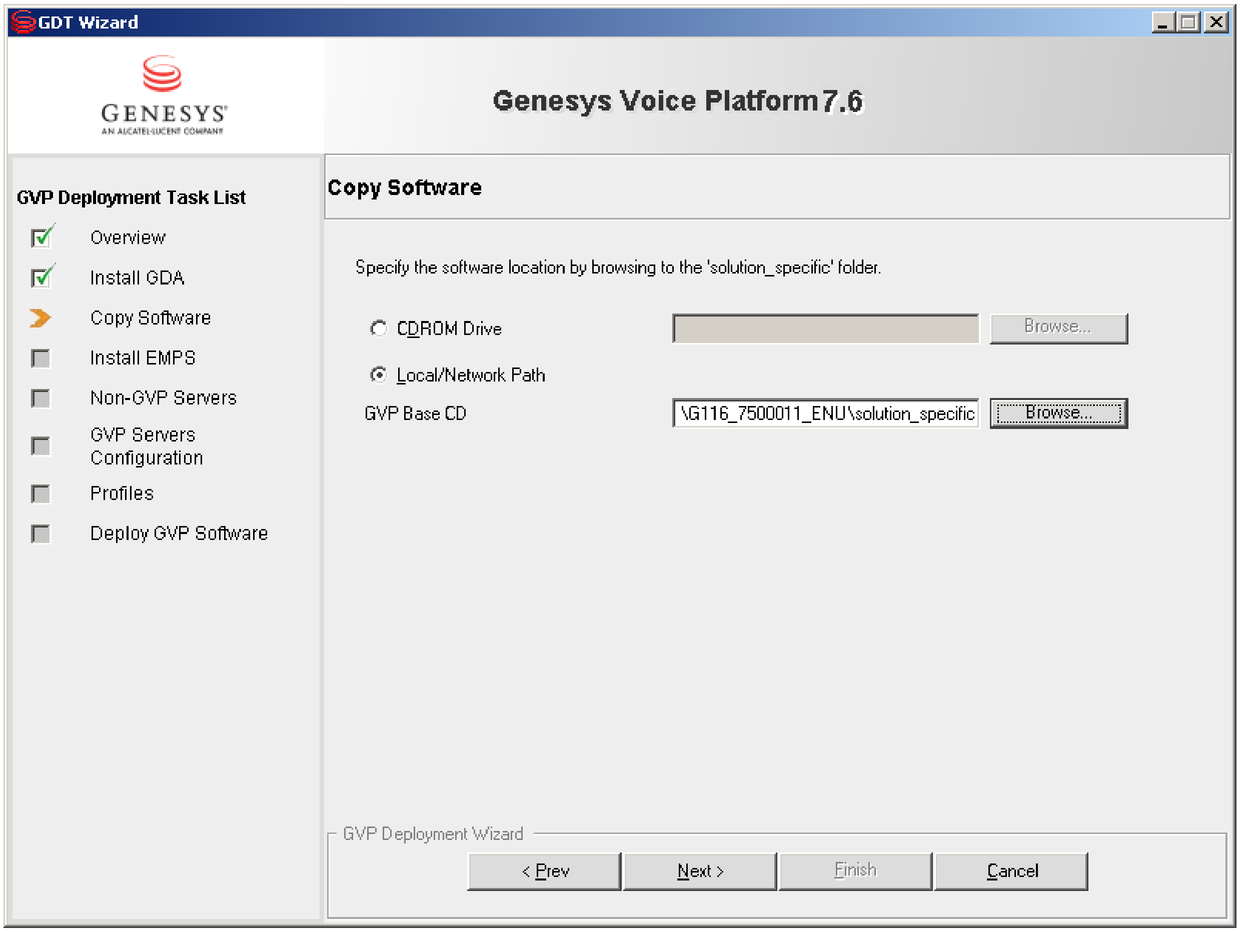
8. Select the GDA is installed and running on all servers on which GVP software will be installed check box, and then click Next.

   The Copy Software information screen appears.

Copy Software

9. Read the information about copying software.

   The GDT will copy the installation software to its working directory (typically at C:\GDT\Media) for later transfer to the GVP server.
10. Click Next.
11. The Copy Software task screen for specifying the GVP software location appears (see Figure 29).



Specify the software location by browsing to the 'solution_specific' folder.

○ CDROM Drive [Browse...]

● Local/Network Path

GVP Base CD: \G116_7500011_ENU\solution_specific [Browse...]

Figure 29: Copy Software Task Screen—Specifying the GVP Software Location

12. Select your Software Location.
    - If the GVP installation software is on CD ROM, select `CDROM Drive`, and then click `Browse` to locate the `solution_specific` folder on the CD drive that contains the GVP software.
    - If the GVP installation software is located on your hard drive, or a mapped network drive, select `Local/Network Path`, and then use the `Browse` button to locate the `solution_specific` folders that contain the GVP software that you want to install.

> `Note:` It can take several minutes for the software to be copied.

13. After the GVP software has been copied, click `Next`.

    The `Install EMPS` information screen appears.

Install EMPS

14. Read the information about installing the EMPS, and then click `Next`.

    The `Install EMPS` task screen appears.

15. In the `EMPS Server FQDN` text box, enter the fully qualified domain name of your EMPS server, and then click `Next`.

    The `Install EMPS` screen for selecting LDAP type appears.

16. Select the LDAP Type:

    - `OpenLDAP`—Recommended for small-sized deployments of GVP.
    - `SunOne`—Recommended for medium-to-large sized deployments of GVP.

17. If you select `SunOne`, enter the LDAP settings in the text boxes, as described in Table 22.

Table 22: Install EMPS—SunOne LDAP Setting Parameters

Parameters	Description
Server Name	Specifies the FQDN of the machine that is hosting the Directory Server.
Server Port	Specifies the listening port of the Directory Server.
Server Root	Specifies the LDAP Root or BaseDN. You must set the value to `o=genesys`.
User Name	Specifies the name that is used to login to SunOne. You must set the value to `cn=Directory Manager`.
Password	Specifies the password that is used to login to SunOne. Use the password you created when setting up your SunOne Directory Server. **Note:** The password is case sensitive.
LDAPPath	Specifies the path to the SunOne installation folder. Typically this is `C:\Sun\MPS`.

18. Click `Next`.

    The `Install EMPS` task screen for specifying the EMPS Installation folder appears.

19. In the `Default Location` text box, either accept the default installation path (`C:\GVP`), or enter a new path for the EMPS installation, and then click `Next`.

20. Read the information about validation, and then click `Next`.

> Note: The GDT validates the Windows prerequisites for the EMPS. After they are validated, the GDT transfers the installation software to the EMPS server.

21. After validation is successful, click `Next`.

    The `Install EMPS` screen appears.

22. On the `Install EMPS` screen, click `Next` to install EMPS.

23. Verify your provisioning information in EMPS. To access EMPS:

    a. In a web browser, access the EMPS login screen by entering the URL `http://<EMPS-hostname>:9810/spm`.

    b. Log in to the EMPS as `Admin`, and enter `password` as your password.

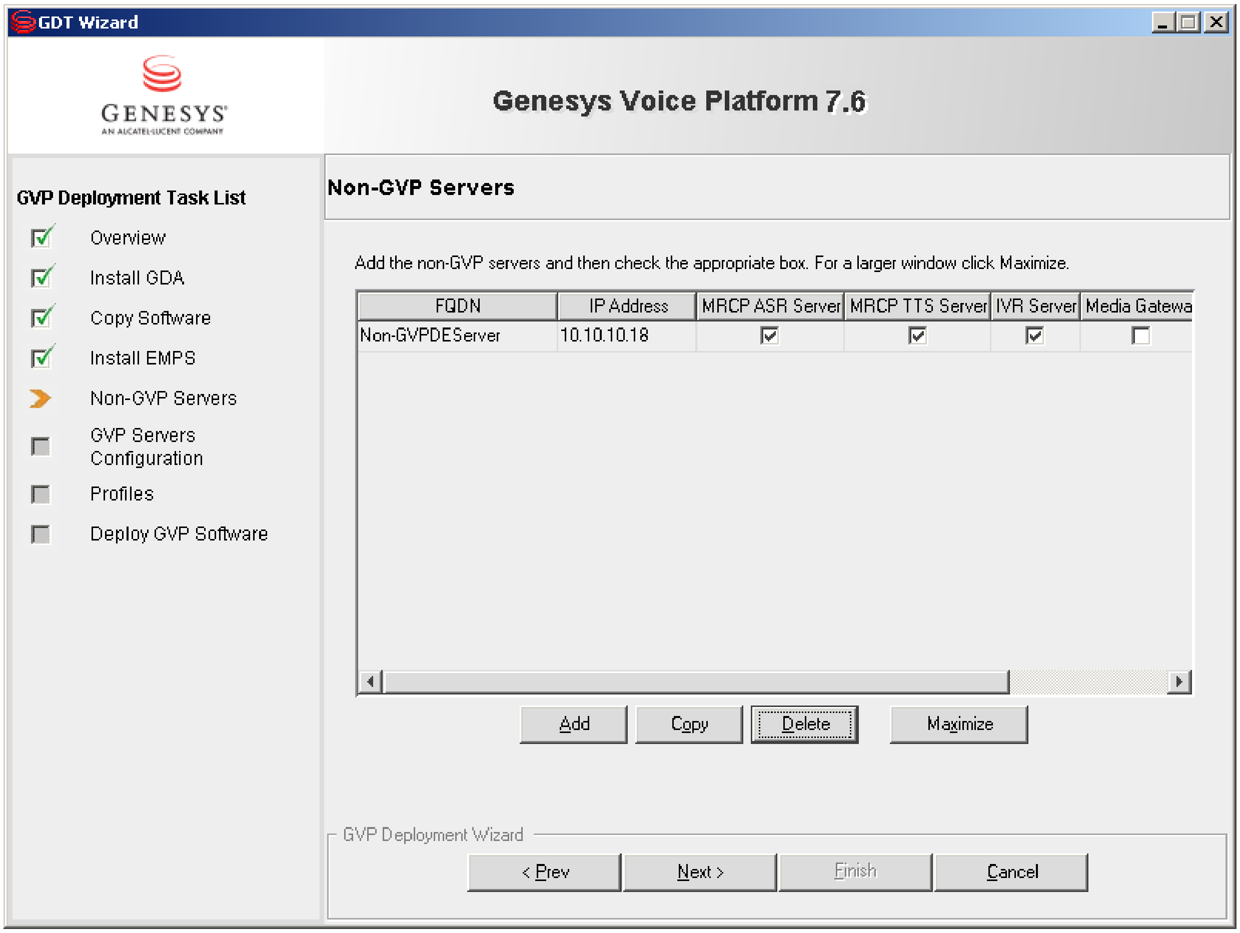
24. After you have verified your provisioning information, click `Next`.

    The `Non-GVP Servers` task screen appears.

Non-GVP Servers

25. Read the information about Non-GVP Servers, and then click `Next`.

26. The `Non-GVP Servers` task screen for adding Non-GVP Servers appears (see Figure 30).



- ☑ Overview
- ☑ Install GDA
- ☑ Copy Software
- ☑ Install EMPS
- ➤ Non-GVP Servers
- □ GVP Servers Configuration
- □ Profiles
- □ Deploy GVP Software

Add the non-GVP servers and then check the appropriate box. For a larger window click Maximize.

FQDN	IP Address	MRCP ASR Server	MRCP TTS Server	IVR Server	Media Gatewa
Non-GVPDEServer	10.10.10.18	☑	☑	☑	□

Figure 30: Non-GVP Servers Task Screen—Adding Non-GVP Servers

Table 23 describes the buttons that appear on this page.

Table 23: Non-GVP Servers—Adding Non-GVP Servers Buttons

Button	Description
Add	Adds a new server.
Copy	Creates a copy of the selected server.
Delete	Removes the selected server.
Maximize	Displays the larger `Advanced Grid` screen which provides a larger working area for selecting features. Click `OK` to return to the previous screen.

27. To add a non-GVP server:

  a. Click `Add`.

  b. Double-click in the `FQDN` box, and add the fully qualified domain name of your non-GVP server.

  c. Double-click in the `IP Address` box, and add the IP address of your non-GVP server.

  d. Use the check boxes to specify the third-party software that you want to configure on this non-GVP server (for example, MRCP ASR Server, MRCP TTS Server, IVR Server, and so on).

28. Click `Next`.

29. For each check box that you selected in Step d, a `Non-GVP Servers` task screen for configuring the corresponding third-party software appears.

Non-GVP Server Features

30. To configure the non-GVP server Features, follow the instruction in Chapter 6, “Non-GVP Servers,” on page 124.

31. After you have finished adding all of your non-GVP servers, click `Next`.

The `GVP Servers Configuration` information screen appears.

GVP Servers Configuration

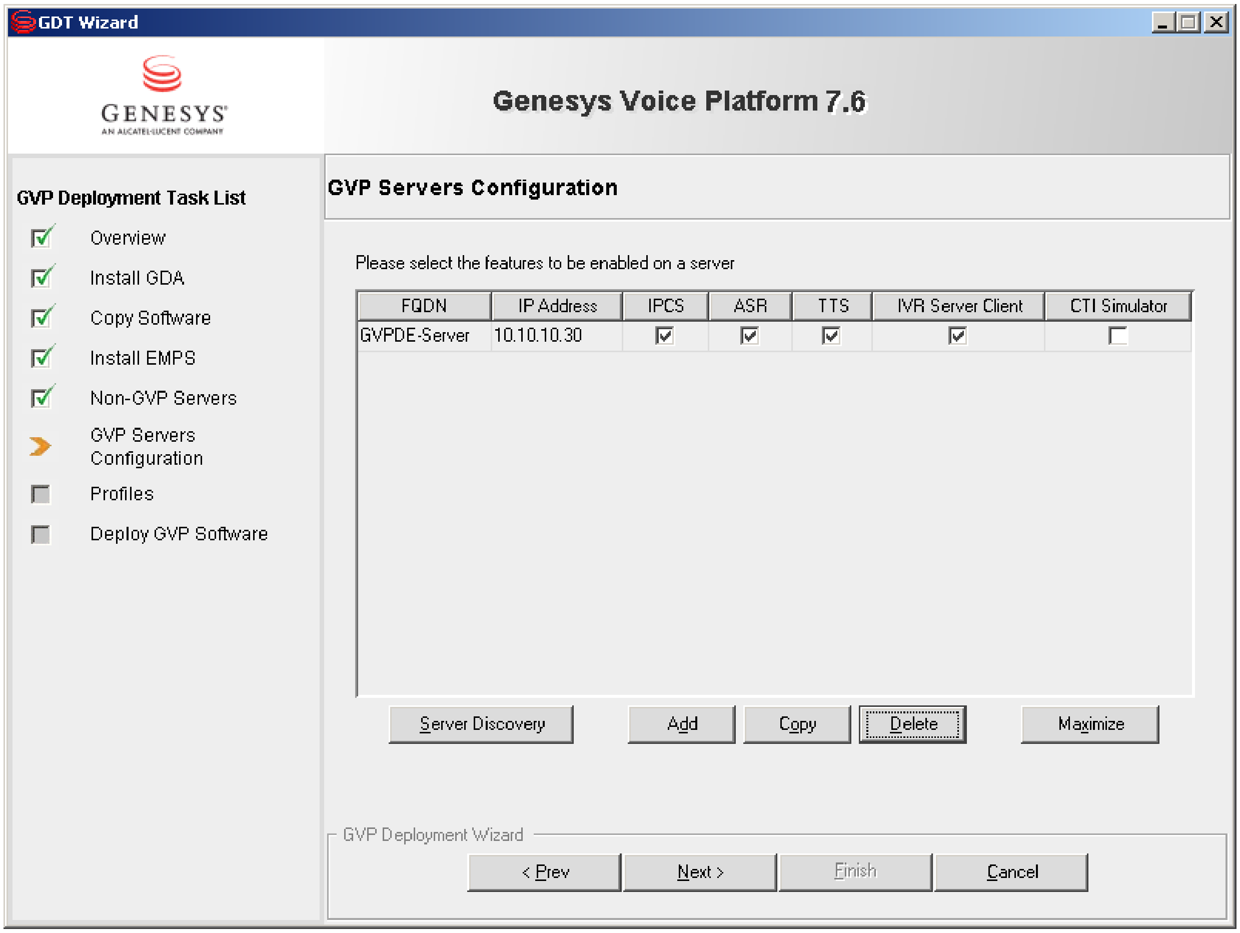
32. Read the information about configuring GVP servers, and then click `Next`.

33. When prompted, `Do you want to discover the GVP servers on which agent is running`, click `Yes`.

After the GVP server has been located, the `GVP Servers Configuration` task screen for selecting features appears (see Figure 31).

Note: The GDT will only discover (display) servers running within the same subnet as the server the GDT is running on. If there are servers in other subnets, and you only want to run the GDT from one central location (recommended), those servers must be added manually in the Discover Servers window. Otherwise, the GDT will have to be run on a server in each subnet.

If GVP: DE is being installed on a machine with no network connection (for example, a laptop), then the machine will not be discovered. You must add it manually, just as if it were in a different subnet.



GVP Deployment Task List

- ☑ Overview
- ☑ Install GDA
- ☑ Copy Software
- ☑ Install EMPS
- ☑ Non-GVP Servers
- › GVP Servers Configuration
- □ Profiles
- □ Deploy GVP Software

GVP Servers Configuration

Please select the features to be enabled on a server

FQDN	IP Address	IPCS	ASR	TTS	IVR Server Client	CTI Simulator
GVPDE-Server	10.10.10.30	☑	☑	☑	☑	□

Figure 31: GVP Servers Configuration Task Screen—Selecting Features

This `GVP Servers Configuration` task screen will be populated with the fully qualified domain name, and IP address of the server in your network that is running the GDA.

34. If the FQDN and IP Address of a server that is running the GDA in your network does not appear on this screen, do the following:

  a. Verify that your GVP server has the GDA installed, and that the GDA is running (started) as a service.

  b. Verify connectivity between the server that is hosting the GDT and the server that is hosting the GDA.

  c. If the GDA is running, and connectivity has been verified, click Server Discovery to detect the GVP server on the same subnet as the GDT.

  After the GDT has finished searching, you are returned to the GVP Servers Configuration task screen for selecting features.

35. If your GVP server was not detected, you can add it manually:

  a. Click Add to add a row.

  b. Double-click in the FQDN and IP Address boxes and update the information in them.

36. After you have added your GVP server, use the check boxes to specify the features that you want to install on it.

Note: You cannot enable the IVR Server Client and the CTI Simulator features on the same server. Because the purpose of the CTI Simulator is to simulate Universal Routing Server (URS) control in the absence of the Genesys call router Framework, there is no role for the IVR Server Client in the simulated deployment.

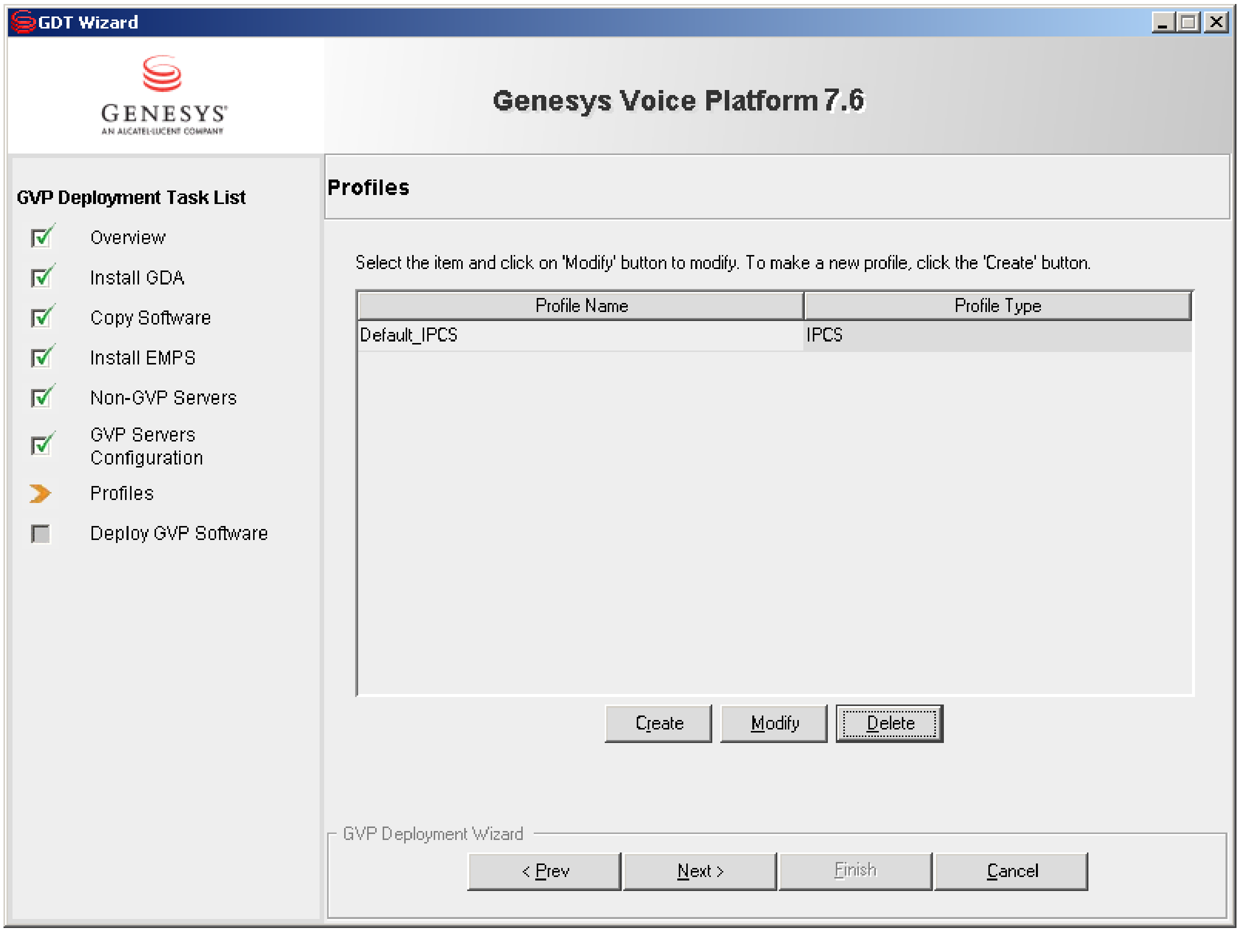
37. Click Next.

  The Profiles task screen appears.

Profiles

38. Read the information about profiles, and how to create them, and then click Next.

  The Profiles task screen for managing your profiles appears (see Figure 32).



GVP Deployment Task List

- ☑ Overview
- ☑ Install GDA
- ☑ Copy Software
- ☑ Install EMPS
- ☑ Non-GVP Servers
- ☑ GVP Servers Configuration
- ➤ Profiles
- □ Deploy GVP Software

Select the item and click on 'Modify' button to modify. To make a new profile, click the 'Create' button.

Profile Name	Profile Type
Default_IPCS	IPCS

Figure 32: Profiles Task Screen—Managing Your Profiles

Table 24 describes the buttons that appear on this page.

Table 24: Profiles Screen Parameters

Parameter	Description
Create	Displays the screen for creating a Profile.
Modify	Displays the screen for configuring the selected profile.
Delete	Removes the selected Profile.

39. Review your existing profiles.

40. Use the `Create`, `Modify`, and `Delete` buttons to manage your profiles.

41. When you are finished, click `Next`.

The `Deploy GVP Software` information screen appears.

Deploy GVP Software

42. Read the information about the tasks involved with GVP software deployment, and then click `Next`.

43. The `Deploy GVP Software` task screen for specifying the GVP installation folder appears.

44. In the `Default Location` text box, either accept the default value (`C:\GVP\CN`), or enter a new default location.

45. Click `Next`.

The `Validation in Progress` screen appears.

46. Click `Next`.

The `Deploy GVP Servers` screen appears.

47. Click `Next` to install, and configure GVP.

After the installation and configuration are complete, you will be returned to the GDT.

48. Review the GDT logs to ensure the GVP installation and configuration is complete.

49. To start GVP:

In Normal Mode:

Go to the GDT menu and select `Deploy > Watchdog > Start`.

In Safe Mode:

`Note:` Watchdog can be started in Safe Mode. Recommended only if the WatchDog cannot be started on the EMPS in Normal mode. For information on Safe Mode, refer to “Safe Mode” on page 39.

a. Go to `Services`, and select the `WatchDog` service.

b. Right-click and select `Properties`.

c. In the `WatchDog Properties` window, enter `-s` in the `Start parameters` text box.

d. Click `Start`.

`Warning!` Do not click `OK`, and try to start the service from the services window as the -s parameter will not have been saved.

End of procedure

Chapter

8 Installing Dialogic

This chapter describes how to install Dialogic on the Voice Communication Server (VCS) host. It contains the following sections:

Note: This chapter is applicable only for VCS.

For a list of supported Dialogic boards, see the *Genesys Supported Media Interfaces Reference Manual*.

Installing Dialogic Software

The VCS supports the Dialogic System Release (SR) 6.0 Service Update (SU) 174 software. Before you install the VCS, you must first install the Dialogic software on the host computer for the VCS.

Notes: You need a minimum of 2 GB (preferably more) of free space on the C: drive in order to install Dialogic software.

You must use the Genesys Dialogic Installation Wizard to install the Dialogic software.

Procedure:
Installing Dialogic software on the VCS host

Purpose: To prepare the VCS host by installing and activating the software that is required to operate the Dialogic boards.

Prerequisites

- Physically install the Dialogic board(s). For information about how to install the Dialogic board, see the vendor documentation that was included with the board, or go to the Dialogic website.
- Ensure that the computer on which you install the Dialogic software has a minimum of 2 GB (preferably more) of free space available for the installation.

Summary

Installing Dialogic on the VCS host is a three-stage process:

- Run the Dialogic Installer to install the software (Steps 1 through 9).
- Run the `Found New Hardware Wizard` to install the driver (Steps 10 through 12).
- Activate the Dialogic boards (Steps 13 through 16).

Start of procedure

Install the Software

1. Insert the Genesys Voice Platform: Dialogic SR 6.0 CD into the computer on which you will be installing the VCS, or copy the Dialogic CD files onto the computer.

   Note: The Dialogic Installer does not support UNC paths.

2. Open the `Genesys\Windows\DialogicInstaller` folder.
3. Double-click `DialogicInstall.bat.`

   If the CD content is on a network, the following error will display:

   ```
   Input Error: Can not find script file C:\WINNT\DialogicInstall.js
   ```

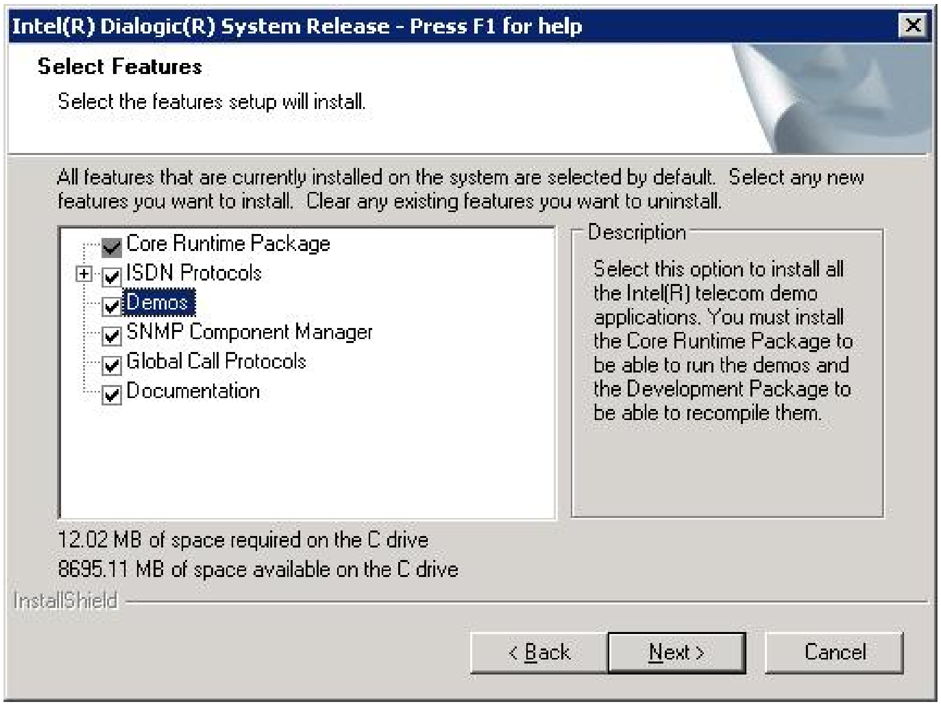
   If you receive the error message, copy the CD content onto the local hard drive, and then rerun `DialogicInstall.bat.`

   The Dialogic Installer `Welcome` screen appears.
4. On the Dialogic Installer `Welcome` screen, click `Next`.

   The `Customer Information` screen appears.
5. Enter your user name and company name, and then click `Next`.

   The `Choose Destination Location` screen appears.
6. Specify the installation directory by doing one of the following:
   - Accept the default destination, then click `Next`.
   - Browse for a new installation path, then click `Next`.

   The `Select Features` screen appears (see Figure 33).



Intel(R) Dialogic(R) System Release - Press F1 for help

Select Features

Select the features setup will install.

All features that are currently installed on the system are selected by default. Select any new features you want to install. Clear any existing features you want to uninstall.

- ☑ Core Runtime Package
- ☑ ISDN Protocols
- ☑ Demos
- ☑ SNMP Component Manager
- ☑ Global Call Protocols
- ☑ Documentation

Description

Select this option to install all the Intel(R) telecom demo applications. You must install the Core Runtime Package to be able to run the demos and the Development Package to be able to recompile them.

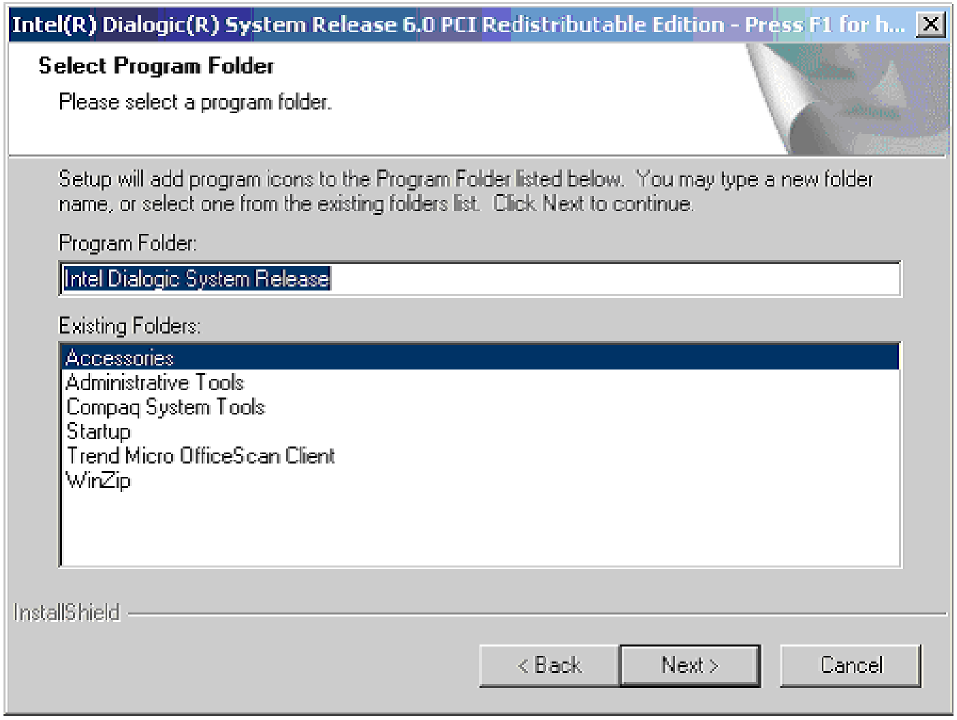
12.02 MB of space required on the C drive
8695.11 MB of space available on the C drive

Figure 33: Select Features Screen

7. Select all of the features, and then click `Next`.
   - If Java Runtime Environment (JRE) 1.4.2 or higher is installed on the system, the `Select Program Folder` screen appears.
   - If JRE 1.4.2 or higher is not installed on the system, a dialog box appears, which requires you to confirm whether you want to install third-party software. Click `Yes`. The `Select Program Folder` screen appears.

> Note: JRE is required only if you plan to run the Dialogic debugging utilities. If you want to install JRE 1.4.2 or higher, go to `java.sun.com`.

8. In the `Select Program Folder` screen, specify the program folder to which you want the installer to add program icons for the Dialogic components (see Figure 34).



Intel(R) Dialogic(R) System Release 6.0 PCI Redistributable Edition - Press F1 for h...

Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

Program Folder:

Intel Dialogic System Release

Existing Folders:

Accessories
Administrative Tools
Compaq System Tools
Startup
Trend Micro OfficeScan Client
WinZip

Figure 34: Select Program Folder Screen

Do one of the following:

- To use the default program folder, make no changes, and click `Next`.

  The default program folder is: `Intel Dialogic System Release`
- To use a different folder, do one of the following:
  - — In the `Program Folder` text box, enter the name of a new folder.
  - — From the `Existing Folders` list, select a folder.

  Then click `Next`.

The `Start Copying Files` screen appears.

9. On the `Start Copying Files` screen, click `Next` to begin copying files.

   The `Setup Status` screen appears, showing the installation progress. When the installation process is complete, the `Setup Complete` screen appears.

Install the Driver

10. Restart the computer.

    When you reboot the system during or after a Dialogic software installation, the `Found New Hardware Wizard` opens after you log in.

11. Run the `Found New Hardware Wizard` to install the required Dialogic driver:

    a. On the `Welcome to the Found New Hardware Wizard` screen, select `Install from a list or a specific location`, and then click `Next`.

b. On the Please choose your search and installation options screen, select Don't search. I will choose the driver to install, and then click Next.

The Hardware Type screen appears.

c. The Hardware Type screen displays all of the available hardware types. The wizard automatically selects the Dialogic hardware that is installed on your machine. Click Next.

d. If you are operating a Windows 2003 system, your system might display the Security Alert - Driver Installation dialog box, which prompts you for digital signing. If you receive this dialog box, click Yes.

e. Allow installation of the driver to complete, and then click Finish.

12. Select Yes, I want to restart my computer now, and then click Finish.

While the computer is restarting, a script appears in a DOS window for a few seconds, and then closes. This indicates the completion of the installation.

Activate the Dialogic Boards

13. Open the Dialogic Configuration Manager (DCM) by selecting Configuration Manager - DCM in the Dialogic program folder on the Windows Start menu. For the default program folder setting (Step 8 on page 175), the path is Start > Programs > Intel Dialogic System Release > Configuration Manager - DCM.

If this is the first time that you are starting the DCM, go to Step 14.

If this is not the first time that you are starting the DCM, the main DCM window appears. Continue at Step 15.

14. The first time that you start the DCM, a dialog box appears, prompting you for the computer connection. Click Connect.

The main DCM window appears.

15. In the main DCM window, activate the Dialogic boards:

a. Right-click each disabled board (that is, each board with an X icon next to it).

b. Select Enable device(s).

16. Close the DCM.

End of procedure

Chapter

9 Installing the Bulk Provisioning Tool

The optional Bulk Provisioning Tool (BPT) enables you to create, regenerate, and reprovision IVR profiles in bulk. This chapter describes how to install the BPT.

It contains the following section:

Note: The BPT is available for Windows only.

Bulk Provisioning Tool Installation

Install the BPT on the host that you will use to access the tool. The following procedure describes how to install the tool.

Procedure: Installing the Bulk Provisioning Tool (Windows)

Start of procedure

1. Insert the Genesys Voice Platform Base CD into the computer, or browse to the folder where you have copied the Base software.
2. Navigate to the `solution_specific\windows\bulkprovtool` folder, and double-click the `setup.exe` file.
3. On the `Welcome` screen, click `Next`.
4. Browse to and select the destination folder to which you want to install the BPT, then click `Next`.

Note: Make sure that the folder name does not contain any spaces in it. Genesys recommends the path `C:\BPT`.

5. When prompted, click `Install` to start the installation process.

The setup program installs the BPT.

6. When prompted, click `Finish` to complete the installation.

End of procedure

Next Steps

- There are no configuration procedures for the BPT. For information about how to launch and use the tool, see the *Genesys Voice Platform 7.6 Reference Manual.*

Chapter

10 Post-Installation Activities on Windows Hosts

For Genesys Voice Platform (GVP) deployments that include Element Management System (EMS) Reporting or Outbound Notification (OBN) Manager, this chapter describes post-installation activities that you must perform on the Element Management Provisioning System (EMPS) server before you install other GVP components, and on the EMS Reporting and OBN Manager server(s) before you can configure them in the EMPS. This chapter also provides information about starting and stopping GVP in all deployments.

This chapter contains the following sections:

Creating the Microsoft SQL Server Databases

This section describes how to set up the databases for the following components:

- EMPS
- EventC
- Login Server (Unified Login)
- Network Monitor
- OBN Manager

The instructions in this section are advanced database procedures. Genesys strongly recommends that your database administrator perform these steps or assist you in performing these steps.

Note: If you are performing a manual installation rather than using the GVP Deployment Tool, you must create the EMPS database before you install other GVP components.

Before You Begin

Ensure that the Microsoft SQL Server and Clients have been prepared, as described in Table 11, "Preparing the Microsoft SQL Server and Clients," on page 94.

The database creation scripts are unpacked during installation of the components. For the script names and post-installation paths on the respective servers, see Table 25.

Setting Up the Databases

This section provides the following generic procedures to create the database schemas:

- Setting up the databases in Microsoft SQL Server 2000
- Setting up the databases in Microsoft SQL Server 2005, page 184

Table 25 summarizes the database names, user names, and user roles that Genesys recommends, as well as the paths to the scripts to create the respective database schemas.

Table 25: Information Summary—GVP Databases

Com-ponent	Database and User Name*	Database Creation Scripts	
		Script Files	Path to Script
EMPS	emps	EMPS_DB_NEW_76SQLServer.SQL	<Installation Drive>\GVP\CN\Config\Database
EventC	collector	Collector_from_scratch_7_6_0.sql	<Installation Drive>\GVP\CN\sqlscripts\mssql\EventC\7.6.0
	peaks	Peaks_from_scratch_7_6_0.sql	
	reporter	Reporter_from_scratch_7_6_0.sql	
	repdwh	RepDWH_from_scratch_7_6_0.sql	
*Genesys recommends that you use the same name for the database and the user, and that you assign the role of db_owner to the user.			

Table 25: Information Summary—GVP Databases (Continued)

Component	Database and User Name*	Database Creation Scripts	
		Script Files	**Path to Script**
Login Server	unifiedlogin	`UnifiedLogin_from_scratch_7_6_0.sql`	`<Installation Drive>\GVP\CN\sqlscripts\mssql\UnifiedLogin\7.6.0`
Network Monitor	netmon	`Netmon_from_scratch_7_6_0.sql`	`<Installation Drive>\GVP\Cn\sqlscripts\mssql\7.6.0`
OBN Manager	obnmanager	`OBN_DB_NEW_76.sql` `OBN_PROC_NEW_76.sql`	`<Installation Drive>\GVP\CN\config\database\sqlserver`
*Genesys recommends that you use the same name for the database and the user, and that you assign the role of `db_owner` to the user.			

Procedure:
Setting up the databases in Microsoft SQL Server 2000

Purpose: To create a required database, user, and schema in Microsoft SQL Server 2000.

Repeat this procedure as required to create the databases for your deployment, using information from Table 25 on page 182.

Start of procedure

1. On the Microsoft SQL Server, open SQL Enterprise Manager.
2. Create the database.
   a. Open SQL Enterprise Manager.
   b. Expand the `SQL Server` group.
   c. Select your local machine.
   d. Expand the `Databases` node.
   e. Right-click `Databases` and select `New Databases`.
   f. In the `Name` field, enter the name of the database to be created. Leave the other fields at the default values.
   g. Click `OK`. The database is created.
3. Create a unique SQL Server user account for the database:
   a. Create the new user.
   b. Assign the role of `db_owner` to the user.

c. Assign the user access privileges to the database.

The user names and passwords can be anything as long as they are unique, but Genesys recommends the following:.

- Use `<dbname>` as the name of the user for each database. For example, `collector` for the `collector` database.

Note: All examples in this guide assume that the database user name follows this convention.

4. Select the database in the navigation tree.
5. From the `Tools` menu, select `SQL Query Analyzer.`
6. Connect to the database as the user you just created.
7. Verify that the correct database is selected in the drop-down list in the center of the `SQL Query Analyzer` toolbar.
8. Run the script(s) to create the database schema:

   a. Open the script file. For the applicable script files and paths, see Table 25 on page 182.

   b. Click anywhere inside the script that opens, to ensure that it has focus.

   c. Do one of the following:

   - Click `Run` (the green triangle).
   - Press `F5.`
   - From the `Query` menu, select `Execute.`

   Ignore any `PRIMARY_KEY_CONSTRAINT violations` error messages.

   After the script has finished running, the following message should appear: `The command completed successfully.`

   Check for any error messages.

9. Close SQL Server Query Analyzer and Enterprise Manager.

End of procedure

Procedure: Setting up the databases in Microsoft SQL Server 2005

Purpose: To create a required database, user, and schema in Microsoft SQL Server 2005.

Repeat this procedure as required to create the databases for your deployment, using information from Table 25 on page 182.

Start of procedure

1. On the Microsoft SQL Server, launch the SQL Server Management Studio (Start > Programs > Microsoft SQL Server 2005 > Management Studio).
2. Click File > Connect Object Explorer.
3. Enter sa as the User Name and Password.
4. Expand the server name on the Object Explorer.
5. Right-click Databases, and then select New Database. The New Database dialog box appears.
6. Enter the Database name.
7. Click OK. The database is created.
8. To verify that the database was created, refresh Object Explorer.
9. Select File > Open > File.
10. Use the FileOpen dialog box to navigate to the required script(s).
11. Connect as the database user when prompted.
12. Change the database in the DB List to the required database.
13. Press F5 to execute the script.

    Ignore any PRIMARY_KEY_CONSTRAINT violations error messages.
14. Close SQL Server Management Studio.

End of procedure

Setting File Permissions for EMS Reporting

EventC, Reporter, and Network Monitor require you to provide the Internet Guest Account with Modify, Read and Execute, and Write access privileges for certain folders. Table 26 identifies the folders for which these permissions are required, by component.

Table 26: Required Internet Guest Account Privileges

Folder	EventC	Reporter	Network Monitor
<installation dir>\data	X	X	X
<Installation Dir>\Log	X	X	X
Legend: X = Internet Guest Account requires Modify, Read and Execute, and Write permissions.			

Table 26: Required Internet Guest Account Privileges (Continued)

Folder	EventC	Reporter	Network Monitor
`<Installation Dir>\php`	X	X	X
`<Installation Dir>\extweb\reporter\download`		X	
Legend: X = Internet Guest Account requires `Modify, Read and Execute`, and `Write` permissions.			

The following procedure describes how to provide the required permissions.

Procedure:
Setting file access permissions for EMS Reporting (Windows)

Purpose: To provide access privileges for the Internet Guest Account user for EventC, Reporter, and Network Monitor.

Repeat this procedure as required to provide access privileges on the folders that are identified in Table 26 on page 185.

Start of procedure

1. On the EMS Reporting server, open Windows Explorer.
2. Right-click the directory for which you want to modify permissions, and select `Properties` from the shortcut menu.

   The `Data Properties` dialog box opens.
3. Click the `Security` tab.
4. Click `Add`
5. Add the Internet Guest Account with `Modify, Read and Execute,` and `Write` permissions.
6. Click `OK`.

End of procedure

Enabling Unified Login

Table 27 summarizes the steps that are required to configure Unified Login for your GVP deployment.

Table 27: Enabling Unified Login for Windows

Objective	Related Procedures and Actions
1. Install and configure Login Server.	**1.** If you are using the GVP Deployment Wizard to install GVP, perform a `Custom` setup, and ensure that you select Login Server as one of the EMS Reporting features that you install. For more information, see Using the GVP Deployment Wizard to install GVP components (Windows only), page 113. **2.** On the EMS Reporting server that hosts Microsoft SQL Server, create the `unifiedlogin` database. For more information, see “Setting Up the Databases” on page 182. **3.** Verify or modify the Login Server configuration in the EMPS. For more information, see Configuring Login Server in the EMPS, page 320.
2. For a multi-tenant deployment, provision the Administrative Customer (Admin Customer or NSP Customer).	See Setting the Admin Customer for Unified Login, page 324.
3. Update the Admin Customer data in the `unifiedlogin` database.	See Updating the Customer ID in the Login Server database (Windows), page 187.
4. Create the website for Unified Login on every host that has EMS Reporting components.	See Creating a website for Unified Login (Windows 2003), page 188. or Creating a website for Unified Login (Windows 2008), page 191.
5. Modify the Unified Login URL to configure the Login Administration service for Reporter and Call Status Monitor.	See Modifying the Unified Login URL for additional services (Windows), page 193.

The following procedures support the deployment of Unified Login in your Windows installation.

Procedure: Updating the Customer ID in the Login Server database (Windows)

Purpose: To update the Admin Customer (NSP customer) information in the `unifiedlogin` database.

You must update the UL_USERS table in the unifiedlogin database every time you modify provisioning for the Admin Customer in the EMPS.

Prerequisites

- If the emps and unifiedlogin databases are on different servers, obtain the Admin Customer's Customer ID from the EMPS (see Setting the Admin Customer for Unified Login, page 324).

Start of procedure

1. Log in to Enterprise Manager (for Microsoft SQL 2000) or Management Studio (for Microsoft SQL 2005), and connect as sa.
2. Open a query window to execute a query against the unifiedlogin database.

   If the emps and unifiedlogin databases are on the same server, go to Step 3, and skip step 4.

   If the emps and unifiedlogin databases are on different servers, skip step 3, and go to Step 4.
3. If the emps and unifiedlogin databases are on the same server, enter the following command to execute the setadminuser stored procedure, and then press F5:

   ```
   exec setadminuser '<EMPS Database Name>'
   ```
4. If the emps and unifiedlogin databases are on different servers, enter the following SQL command to update the UL_USERS table in the unifiedlogin database:

   ```
   update ul_users set customer_id=<ADMIN_CUST_ID> where k_users=1;
   ```

   where <ADMIN_CUST_ID> is the Customer ID for the Admin Customer that you provisioned in the EMPS.

   The default k_users value for the administrator is 1.

   After the script runs, the name of the customer that is set to be the Unified Login administrator is shown in the bottom window pane, and the password (administrator) is shown as well.

End of procedure

Procedure: Creating a website for Unified Login (Windows 2003)

Purpose: To configure the default website in Internet Information Services (IIS). IIS 6 is required for this procedure.

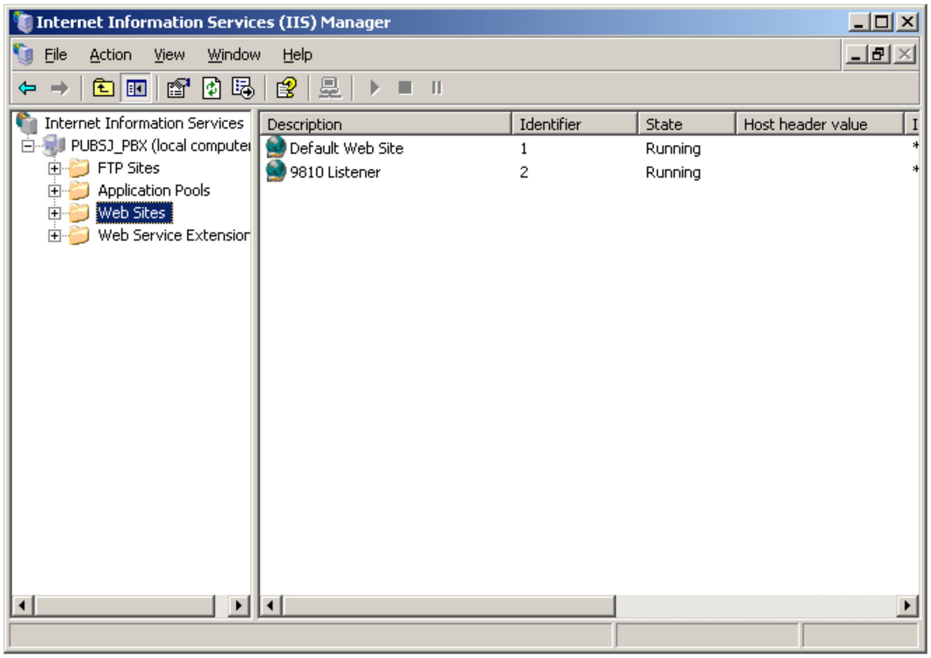
Perform this procedure on every host that has EMS Reporting components.

Note: This procedure creates a website that runs on port 80. The website for Dispenser also runs on port 80. Therefore, if Login Server and Dispenser have been installed on the same machine, do not create a new website. Rather, open the Default website that has been configured for Dispenser, and configure the Home Directory only (see Step 6 on page 189).

Dispenser uses Virtual Directory under the Default website, so the Unified Login Home Directory configuration will not affect Dispenser.

Start of procedure

1. Access IIS Manager from Administrative Tools.
2. Expand and select `Web sites`, as shown in Figure 35 on page 189.



Description	Identifier	State	Host header value
Default Web Site	1	Running	
9810 Listener	2	Running	

Figure 35: Internet Information Services (IIS) Manager

3. Right-click `Web Sites`, and select `New > Website`.

   The Web Site Creation Wizard opens. Click `Next`.
4. For the WebSite description, enter `LoginServer`. Click `Next`.
5. On the `IP Address and Port Settings` page, accept `80` as the TCP port, and then click `Next`.
6. On the `Web Site Home Directory` page, browse to select the `<CN Directory>\extweb` directory as the local path. Click `Next`.
7. On the `Web Site Access Permissions` page, select `Read, Execute, and Write` permissions. Click `Next`.

8. In the warning dialog box that displays, click `Yes`, and then click `Finish`.

The Unified Login website will be created.

9. Update the `.php` extensions:

a. Right-click the `LoginServer` website, and select `Properties`.

b. Click the `Home Directory` tab.

c. In the `Application Settings` section, click `Configuration`.

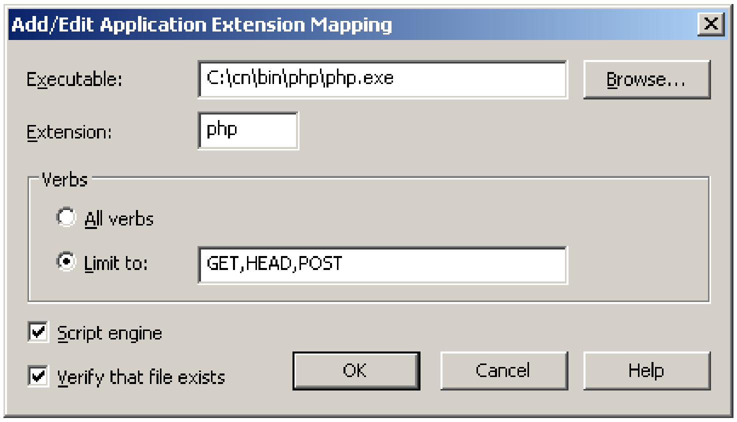
The `Application Configuration` dialog box appears.

d. Click `Add`.

e. In the `Add/Edit Application Extension Mapping` dialog box, specify the following values, and then click `OK` (see Figure 36 on page 190):

- Executable: `<CN Directory>\bin\php\php.exe`
- Extension: `.php`
- Verbs limited to: `GET,HEAD,POST`

Note: Do not use spaces in the Verbs `Limit to` field.



Add/Edit Application Extension Mapping

Executable: C:\cn\bin\php\php.exe

Extension: php

Verbs

○ All verbs

● Limit to: GET,HEAD,POST

☑ Script engine

☑ Verify that file exists

Figure 36: Mapping PHP Extensions

f. Click `OK` to exit the `Application Configuration` and `LoginServer` properties dialog boxes.

10. Stop the default website (because it also runs on port 80).

11. Start the website for Unified Login:

a. In the IIS Manager, right-click the `LoginServer` website.

b. Select `Start`.

The `.php` extensions to the `LoginServer` website will be updated.

12. Log into `http://server.domain/unifiedlogin/login.php` to check the GUIs.

End of procedure

Procedure: Creating a website for Unified Login (Windows 2008)

Purpose: To configure the default website in Internet Information Services (IIS). IIS 7 or IIS 7.5 is required for this procedure.

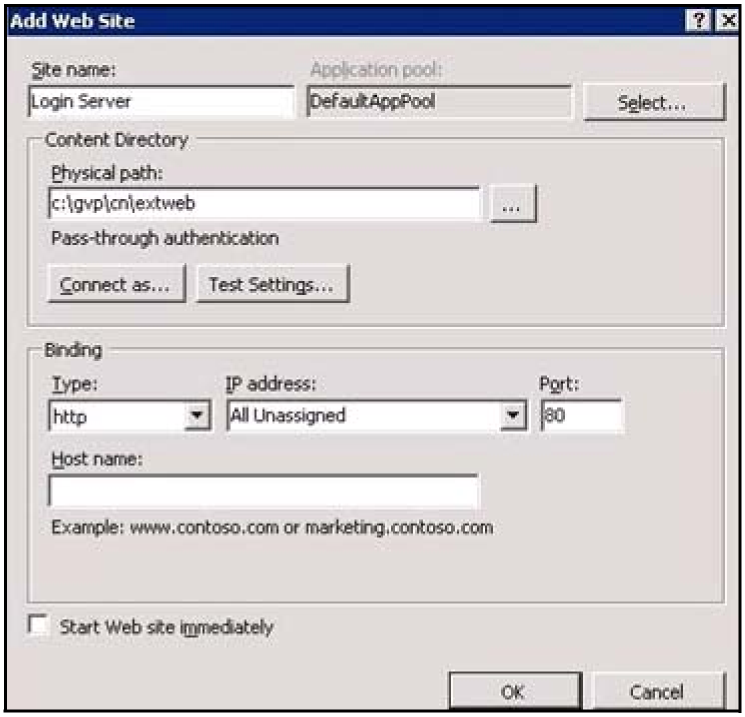
Perform this procedure on every host that has EMS Reporting components.

Start of procedure

1. Launch IIS Manager from Administrative Tools.
2. Stop the `Default` web site if it is not hosting the `Dispenser` web site.
3. In the `Connections` pane, right-click the `Sites` node in the tree, and click `Add Web Site.`

   The `Add Web Site` dialog box opens.
4. In the `Site name` field, type `Login Server.`
5. Click `Select..`

   The `Select Application Pool` dialog box opens.
6. From the `Application Pool` drop down list, select `DefaultAppPool` and click `OK.`
7. In the `Physical path` field, browse to select the `<CN Directory>\extweb` directory.
8. In the Binding section:
   a. From the `Type` drop down list, select `http.`
   b. From the `IP address` drop down list, select `All Unassigned.`
   c. In the `Port` field, enter `80.`
9. Uncheck the `Start Web site immediately` checkbox.



Site name: Login Server

Application pool: DefaultAppPool

Content Directory

Physical path: c:\gvp\cn\extweb

Pass-through authentication

Binding

Type: http

IP address: All Unassigned

Port: 80

Host name:

Example: www.contoso.com or marketing.contoso.com

□ Start Web site immediately

Figure 37: Add Web Site Dialog, IIS Manager (Login Server)

10. From the left pane, click `Website`.

11. In the center pane, double-click `Handler Mappings`.

12. In the `Actions` pane:

a. Click `Edit Feature Permissions...`

The `Edit Feature Permissions` dialog box opens.

b. Select the `Read and Execute privileges` check box and click `OK`.

c. Click `Add Script Map`.

13. In the `Add Script Map` dialog box.

a. In the `Request Path` field, enter `*.php`.

b. In the `Executable` field, enter `<CN Directory>\bin\php\php.exe`

c. In the `Name` field, enter `PHP`.

14. Click `Request Restriction`.

15. On the `Access` tab, ensure `Script` is selected and click `OK`.

16. On the left pane, click on the website and switch to `Features View`.

17. Double-click `Authentication`.

18. In the `Actions` pane, ensure `Anonymous Authentication` is enabled. (If not, click to enable it.)

19. To start the web site:

a. Right-click on the web site.

b. Select `Manage Web Site`.

c. Click `Start`.

End of procedure

Procedure: Modifying the Unified Login URL for additional services (Windows)

Purpose: To configure the Reporter and Call Status Monitor to use the Login Administration service.

Start of procedure

1. Log in to the Unified Login at `http://server.domain/unifiedlogin`.
   - `Login Name` = `Administrator`
   - `Customer Name` = `<name of the NSP Customer>`
   - `Password` = `<password>`

   Notes: Customer Name is required when GVP runs in multi-tenant mode.

   The password that is set by the Unified Login database scripts is `administrator`.

2. Click `Login Administration`.
3. Click `Modify Service`.
4. From the drop-down list, select `RTP1`, and then click `Search`.
5. Modify the `URL` field as follows:

   `http://<reporter server FQDN>/reporter/login.php`
6. If the Reporter is on a VPN in addition to being on the public network, then modify the `VPN URL` field as follows:

   `http://<reporter server name or IP addr on VPN>/reporter/login.php`
7. Click `Save`.
8. Repeat Steps 4 through 7 to add Call Status Monitor, using the following information:

   a. Search for `CSM Call Status Monitor`.

   b. Specify the following URL:
   `http://<CSM Server FQDN>/callstatusmonitor/login.php`

c. Specify the following VPN URL:

```
http://<call status monitor server name or IP addr on VPN>/
callstatusmonitor/login.php
```

d. Click `Save`.

9. Check the GUIs:

a. Log into the following URL:

```
http://<Login Server FQDN>/unifiedlogin
```

b. Click `Historical Reports`.

End of procedure

Enabling Network Monitor

Table 28 summarizes the steps that are required to configure Network Monitor for your GVP deployment.

Table 28: Enabling Network Monitor for Windows

Objective	Related Procedures and Actions
1. Install and configure Network Monitor.	**1.** If you are using the GVP Deployment Wizard to install GVP, perform a `Custom` setup, and ensure that you select Network Monitor as one of the EMS Reporting features that you install. For more information, see Using the GVP Deployment Wizard to install GVP components (Windows only), page 113. **2.** On the EMS Reporting server that hosts Microsoft SQL Server, create the `netmon` database. For more information, see “Setting Up the Databases” on page 182. **3.** Verify or modify the Network Monitor configuration in the EMPS. For more information, see Configuring Network Monitor in the EMPS, page 333.
2. Set the required access privileges for the Internet Guest Account.	See Setting file access permissions for EMS Reporting (Windows), page 186.
3. Create the website for Network Monitor.	See Creating a website for Network Monitor (Windows 2003), page 195 or Creating a website for Network Monitor (Windows 2008), page 196.

The following procedure describes how to create the Network Monitor website.

Procedure: Creating a website for Network Monitor (Windows 2003)

Perform this procedure on the EMS Reporting host on which Network Monitor is installed.

Prerequisites

- IIS 6 is required for this procedure.

Start of procedure

1. Launch IIS Manager from Administrative Tools.
2. Expand and select `Web sites`. (For an illustration of the IIS window, see Figure 35 on page 189.)
3. Right-click `Web Sites`, and select `New > Website`.

   The Web Site Creation Wizard opens. Click `Next`.
4. For the WebSite description, enter `NetMon`. Click `Next`.
5. On the `IP Address and Port Settings` page, enter `9811` as the TCP port. Click `Next`.
6. On the `Web Site Home Directory` page:
   a. Browse to select the `<CN Directory>\NetMon` directory as the local path.
   b. Ensure that the check box to allow anonymous access to the website is selected.
   c. Click `Next`.
7. On the `Web Site Access Permissions` page, select `Read, Execute, and Write` permissions. Click `Next`.
8. In the warning dialog box that displays, click `Yes`, and then click `Finish`.

   The Network Monitor website will be created.
9. Update the `.php` extensions:
   a. Right-click the `NetMon` website, and select `Properties`.
   b. Click the `Home Directory` tab.
   c. In the `Application Settings` section, click `Configuration`.

      The `Application Configuration` dialog box appears.
   d. Click Add.
   e. In the `Add/Edit Application Extension Mapping` dialog box, specify the following values, and then click `OK` (see Figure 36 on page 190):
      - Executable: `<CN Directory>\bin\php\php.exe`
      - Extension: `.php`
      - Verbs limited to: `GET,HEAD,POST`

Note: Do not use spaces in the Verbs `Limit to` field.

f. Click `OK` to exit the `Application Configuration` and `LoginServer` properties dialog boxes.

10. Start the `NetMon` website:
    a. In the IIS Manager, right-click the `NetMon` website.
    b. Select `Start.`

       The `.php` extensions to the `NetMon` website will be updated.
11. Restart the World Wide Web Publishing service.
12. Log into `http://server.domain:9811/` to check the GUIs.

End of procedure

Procedure: Creating a website for Network Monitor (Windows 2008)

Perform this procedure on the EMS Reporting host on which Network Monitor is installed.

Prerequisites

- IIS 7 or IIS 7.5 is required for this procedure.

Start of procedure

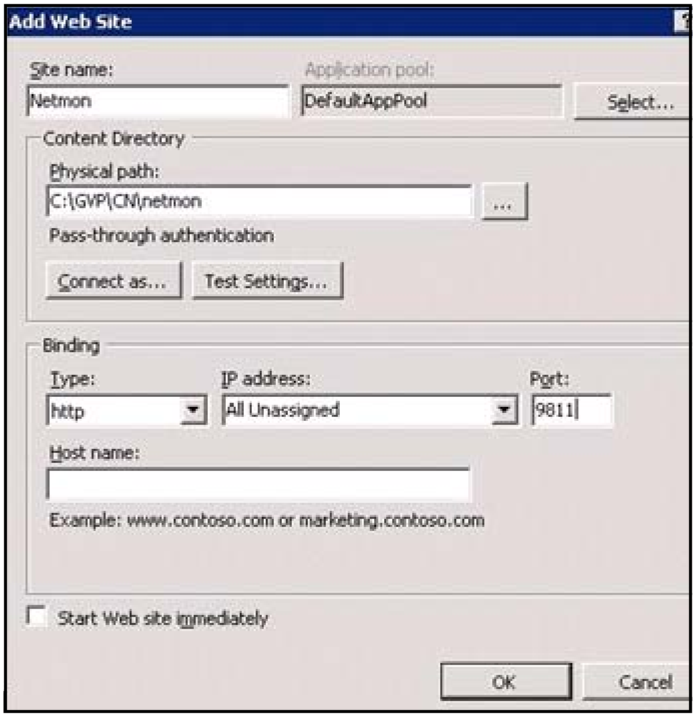
1. Launch IIS Manager from Administrative Tools.
2. In the `Connections` pane, right-click the `Sites` node in the tree, and click `Add Web Site.`

   The `Add Web Site` dialog box opens.
3. In the `Site name` field, type `Netmon.`
4. Click `Select..`

   The `Select Application Pool` dialog box opens.
5. From the `Application Pool` drop down list, select `DefaultAppPool` and click `OK.`
6. In the `Physical path` field, browse to select the `<CN Directory>\NetMon` directory.
7. In the Binding section:
   a. From the `Type` drop down list, select `http.`
   b. From the `IP address` drop down list, select `All Unassigned.`

c. In the Port field, enter 9811.

8. Uncheck the Start Web site immediately checkbox.



Site name: Netmon

Application pool: DefaultAppPool

Physical path: C:\GVP\CN\netmon

Type: http

IP address: All Unassigned

Port: 9811

Host name:

Example: www.contoso.com or marketing.contoso.com

□ Start Web site immediately

Figure 38: Add Web Site Dialog, IIS Manager (Netmon)

9. From the left pane, click Website.

10. In the center pane, double-click Handler Mappings.

11. In the Actions pane:

    a. Click Edit Feature Permissions...

       The Edit Feature Permissions dialog box opens.

    b. Select the Read and Execute privileges check box and click OK.

    c. Click Add Script Map.

12. In the Add Script Map dialog box.

    a. In the Request Path field, enter *.php.

    b. In the Executable field, enter <CN Directory>\bin\php\php.exe

    c. In the Name field, enter PHP.

13. Click Request Restriction.

14. On the Access tab, ensure Script is selected and click OK.

15. On the left pane, click on the website and switch to Features View.

16. Double-click Authentication.

17. In the Actions pane, ensure Anonymous Authentication is enabled. (If not, click to enable it.)

18. To start the web site:
    a. Right-click on the web site.
    b. Select `Manage Web Site`.
    c. Click `Start`.

End of procedure

Starting and Stopping GVP on Windows

Starting or stopping GVP means starting or stopping the WatchDog process on the GVP server.

WatchDog can operate in two modes: normal and safe. For more information about WatchDog and its modes of operation, see "WatchDog" on page 38.

You must start the WatchDog process on all GVP servers after installation. You must also restart the WatchDog process on a GVP server after you make any configuration changes for that component in the EMPS.

Note: The EMPS WatchDog must be running before you install other components. The GVP Deployment Tool (GDT) installation wizard automatically starts the EMPS WatchDog during installation. If you are performing a manual installation, start the EMPS WatchDog in Safe mode before you install other GVP components.

This section provides information about the various ways in which you can start or restart WatchDog on Windows hosts:

- Starting/Restarting GVP in Normal mode (Windows)
- Starting/Restarting GVP in Safe mode (Windows)
- Stopping WatchDog (Windows)

Procedure: Starting/Restarting GVP in Normal mode (Windows)

Purpose: To describe the ways in which you can start or restart WatchDog in Normal mode.

Prerequisites

- The following services are running on the GVP server:
    - Internet Information Services (IIS)
    - World Wide Web Publishing Service

Start of procedure

1. To start or restart WatchDog using the GDT:
   - a. Double-click the `GVPLaunch.bat` file to launch the GDT.

     The `GVPLaunch.bat` file is located in the `<Installation directory>\solution_specific\windows\install` folder (where the GVP Base Software was copied).
   - b. Specify the servers on which you want to start WatchDog:
     - i. From the GDT `Deploy` menu, select `Selected Servers.`
     - ii. On the `Select Servers` page, use the `Add >` button to move the desired servers from the list box on the left to the list box on the right.
   - c. From the GDT `Deploy` menu, select `Watchdog > Start`.
2. To start or restart WatchDog as a Windows Service:
   - a. Go to `Start > Control Panel > Administrative Tools > Services.`
   - b. Select WatchDog, and start or restart the service in the `Services` window.
3. To restart WatchDog from the EMPS:
   - a. In a web browser, access the `EMPS Login Page` by entering the following URL:

     `http://<EMPS-hostname>:9810/spm`
   - b. On the `EMPS Login` page, log in with the following credentials:

     User Name: `Admin`

     Password: `password`
   - c. In the EMPS navigation tree, expand the `Servers` node, and then the component.
   - d. Right-click the server for which you want to start WatchDog, and select `Restart GVP.`L

End of procedure

Procedure: Starting/Restarting GVP in Safe mode (Windows)

Purpose: To start or restart core WatchDog processes even though other GVP processes may not be able to start up.

Prerequisites

- The following services are running on the GVP server:
  - Internet Information Services (IIS)
  - World Wide Web Publishing Service

Start of procedure

1. Go to Start > Control Panel > Administrative Tools > Services.
2. Right-click WatchDog, and select Properties.

   The WatchDog Properties dialog box opens.
3. In the Start parameters text box, enter the following parameter:

   ```
   -s
   ```
4. Click Start.

Warning!	Do not click OK to exit the WatchDog Properties dialog box, and then try to start the service from the Services window, because the -s parameter will not have been saved.

End of procedure

Procedure: Stopping WatchDog (Windows)

Start of procedure

1. Stop WatchDog as a Windows Service:
   a. Go to Start > Control Panel > Administrative Tools > Services.
   b. Select WatchDog, and stop the service in the Services window.

End of procedure

Chapter

11 Maintaining GVP

This chapter describes how to upgrade, repair, or uninstall Genesys Voice Platform (GVP) components on the Windows operating system.

This chapter contains the following sections:

Upgrading GVP Using the GDT

This section describes how to use the GDT to upgrade from earlier GVP releases to GVP release 7.6.

This section includes the following procedures:

- Upgrading the GDA using the GDT, page 202
- Upgrading GVP using the GDT, page 202
- Installing a new EMPS on an existing EMPS server (Windows), page 210

Note: The procedures to upgrade GVP describe only how to use the GDT and the GVP Deployment Wizard to upgrade components. These instructions are **not** an upgrade strategy. For more information about what is supported, about upgrade strategies, and about additional steps that you must perform to upgrade GVP, refer to the chapter about upgrading to GVP 7.6 in the *Genesys Migration Guide*.

Procedure:
Upgrading the GDA using the GDT

Purpose: To upgrade the GDA on multiple GVP servers at the same time.

Start of procedure

1. Execute the `GVPLaunch.bat` file to launch the GDT.

   For more information about launching the GDT, see the first steps in the procedure Using the GVP Deployment Wizard to install GVP components (Windows only), page 113.

2. Cancel the GVP Deployment Wizard, so that the GDT window has focus.

3. From the `Deploy > Maintenance` menu, select `GDA Upgrade`.

   The `Copy Software` task page for specify the GDA software location appears.

4. On the `Copy Software` task page, specify the location of the `solution_specific` folder that contains the `InstallAgent.bat` file, and then click `Next`. (The `InstallAgent.bat` file must be compatible with the version of the `GVPLaunch.bat` file that you are using for the GDT.)

   The GDT copies the software to its working directory for later transfer to the required GVP servers.

   After the software has been copied, the `Select Servers` page appears.

5. On the `Select Servers` page, use the `Add >` button to move the desired servers from the list box on the left to the list box on the right, and then click `Next`.

   The GDA will be upgraded on all the servers that you select.

6. On each applicable GVP server, verify that the GDA service is running:

   a. From the Windows `Start` menu, go to `Control Panel > Administrative Tools > Services`.

   b. If necessary, start or restart the `GVP Deployment Agent` service.

End of procedure

Procedure:
Upgrading GVP using the GDT

Summary

The GDT wizard leads you through the following steps in the upgrade process:

1. Overview, page 205

2. Install GDA, page 206
3. Specify Setup Type, page 206
4. Copy Software, page 206
5. Install EMPS, page 207

Note: The Element Management Provisioning System (EMPS) itself cannot be upgraded—a new EMPS must be installed. The GDT upgrade process provides options to install a new EMPS on a new server, or to upgrade other components in a deployment that already has a 7.6 EMPS. The `Install EMPS` pages do not display if you select the option to upgrade other components with an existing 7.6 EMPS (see Step 5 on page 205).

To install a new EMPS on an existing EMPS host, you must perform a manual workaround to move the EMPS to a new location on the EMPS server. For more information, see Installing a new EMPS on an existing EMPS server (Windows), page 210.

6. Migrate EMPS Data, page 209
7. Upgrade GVP Servers, page 209

Prerequisites

- A version of the GDA that is compatible with the GDT version has been installed and is running on each GVP server on which you want to upgrade GVP software. If necessary, upgrade the GDA (see Upgrading the GDA using the GDT, page 202).
- If you plan to install a new EMPS server, the new EMPS machine conforms to GVP requirements. For more information, see Chapter 4, “Preparing Your Windows Environment,” on page 81.
- If you plan to install a new EMPS on the existing EMPS server, you have performed the manual workaround to remove the old EMPS. For more information, see Installing a new EMPS on an existing EMPS server (Windows), page 210.
- For GVP servers that are not in the same subnet as the GDT, the fully qualified domain names (FQDNs) and IP addresses are available.
- All third-party software, especially antivirus software, has been stopped on the server that is running the GDT and on the servers on which GVP software will be upgraded.

Start of procedure

1. Execute the `GVPLaunch.bat` file to launch the GDT and the GVP Deployment Wizard.

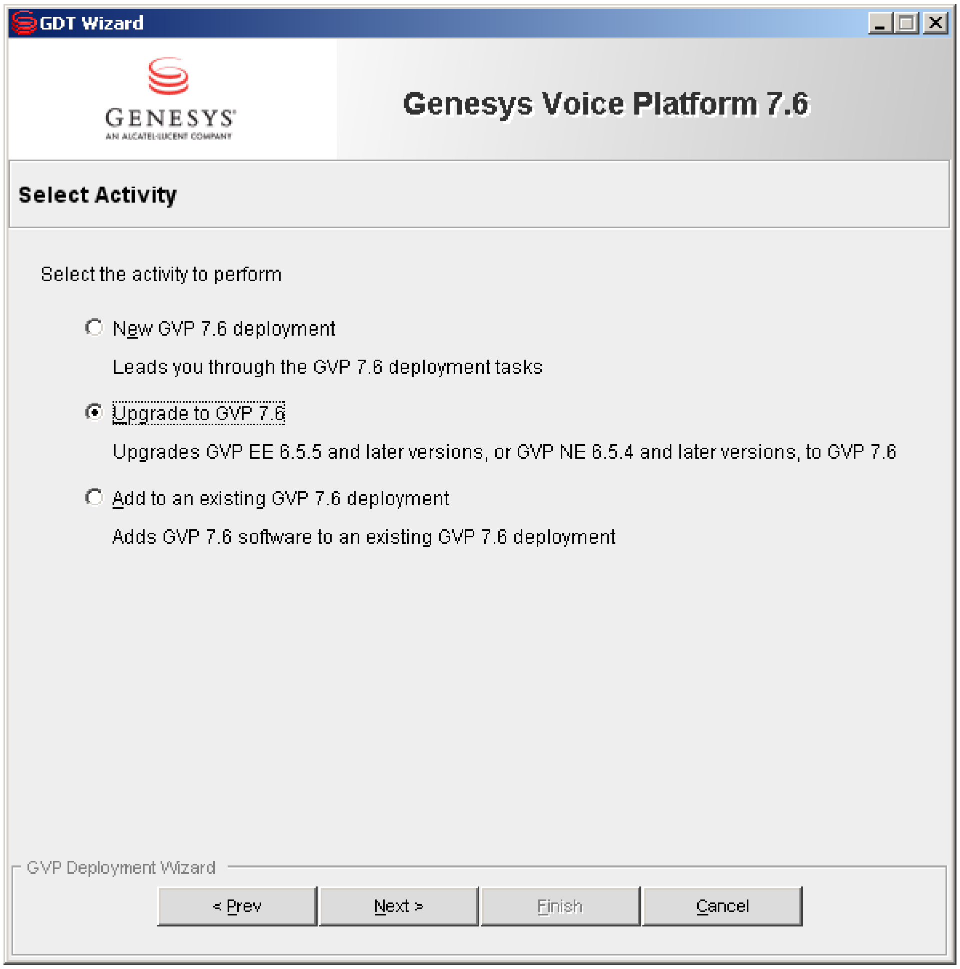
   For more information about launching the GDT and the wizard, see the first steps in the procedure Using the GVP Deployment Wizard to install GVP components (Windows only), page 113.

2. On the `Welcome` page of the wizard, click `Next`.

   The `Genesys License Agreement` page appears.

3. Select the `I accept the above agreement` check box, and then click `Next`.

   The `Select Activity` page appears (see Figure 39).



GDT Wizard

Genesys Voice Platform 7.6

Select Activity

Select the activity to perform

○ New GVP 7.6 deployment

Leads you through the GVP 7.6 deployment tasks

● Upgrade to GVP 7.6

Upgrades GVP EE 6.5.5 and later versions, or GVP NE 6.5.4 and later versions, to GVP 7.6

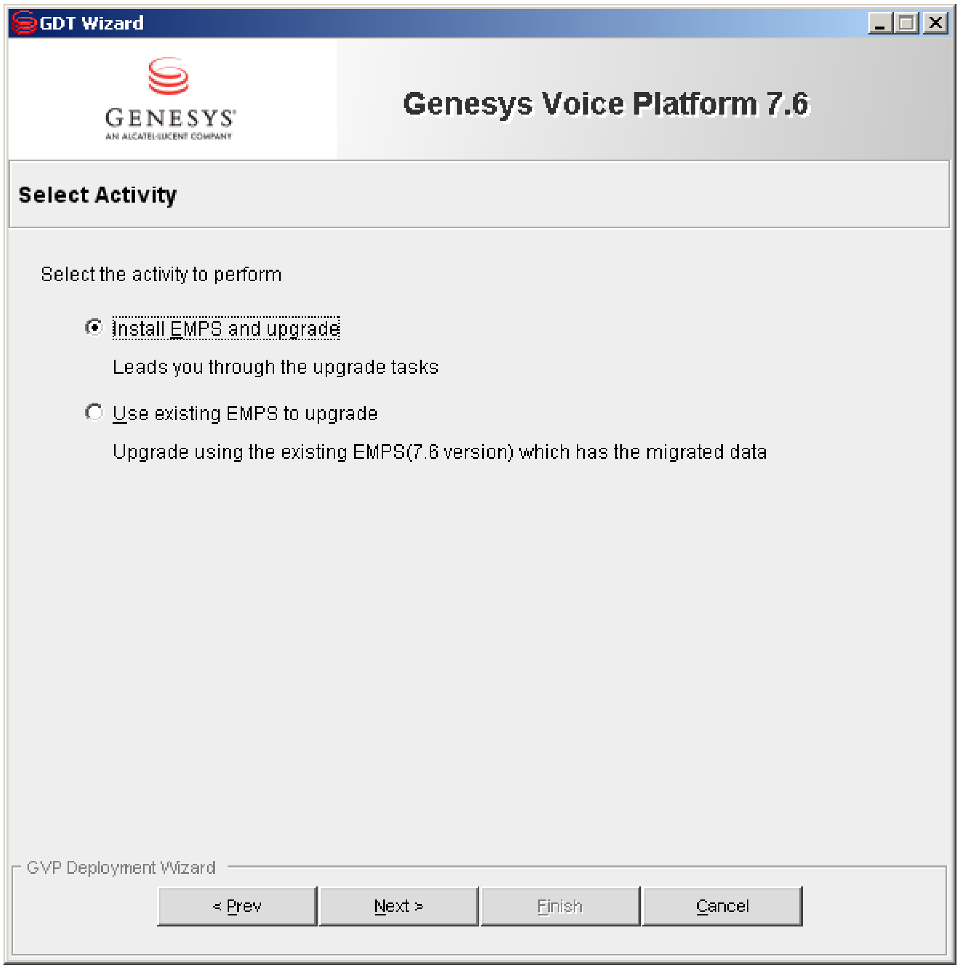
○ Add to an existing GVP 7.6 deployment

Adds GVP 7.6 software to an existing GVP 7.6 deployment

Figure 39: Select Activity Page

4. Select `Upgrade to GVP 7.6`, and then click `Next`.

   Another `Select Activity` page appears (see Figure 40).



Select Activity

Select the activity to perform

● Install EMPS and upgrade

Leads you through the upgrade tasks

○ Use existing EMPS to upgrade

Upgrade using the existing EMPS(7.6 version) which has the migrated data

Figure 40: Select Activity Page

5. On the `Select Activity` page, choose one of the following:
   - `Install EMPS and upgrade`—Select this option if the EMPS in your existing deployment is earlier than release 7.6.
   - `Use existing EMPS to upgrade`—Select this option if your deployment already includes a 7.6 EMPS, and you are running the GDT wizard to upgrade other GVP components.
6. Click `Next`.

   The `Overview` page appears.

Overview

The left pane of the `Overview` page, and all subsequent pages of the wizard, contains a GVP Deployment Task List that shows your progress through the upgrade process.

7. On the `Overview` page, click `Next`.

   The `Install GDA` page appears.

Install GDA

8. On the Install GDA page, select the GDA is installed and running on all servers on which GVP software will be installed check box, and then click Next.

The Specify Setup Type information page appears.

Specify Setup Type

9. On the Specify Setup Type information page, read the information about telephony types, and then click Next.

The Specify Setup Type page appears. (For an example, see Figure 11 on page 118).

10. On the Specify Setup Type task page:

a. Select the Telephony type:

- IP Telephony—Uses IP Communication Server (IPCS) to receive calls.
- TDM Telephony—Uses Dialogic telephony boards on Voice Communication Server (VCS) to receive calls.

b. Select the GVP setup type:

- Typical—Includes IPCS/VCS, ASR, TTS, and IVR Server Client.
- Custom—Includes everything under Typical plus the option to select Reporting, ASR Log Manager, OBN Manager/Policy Manager/ Bandwidth Manager, SIP Call Manager, and H323 Call Manager. Click the Details button to select the Custom components you want to install and configure.

11. Click Next.

The Copy Software information page appears.

Copy Software

12. On the Copy Software information page, read the information about copying software, and then click Next.

The Copy Software task page for specifying the GVP software location appears. (For an example, see Figure 13 on page 120).

13. On the Copy Software task page, specify the location of the installation software, and then click Next.

- If the GVP installation software is on a CD, select CDROM Drive, and then click Browse to locate the solution_specific folder on the CD drive that contains the GVP software.

- If the GVP installation software is located on your hard drive, or on a mapped network drive, select Local/Network Path, and then click the Browse buttons to locate the solution_specific folders that contain the GVP software that you want to install.

The GDT copies the installation software to its working directory.

Note: It can take several minutes for the software to be copied.

After the GVP software has been copied, one of the following pages appears, depending on the option you selected in Step 5 on page 205:

- If you selected the option Install EMPS and upgrade, the Install EMPS information page appears. Continue at Step 15.
- If you selected the option Use existing EMPS to upgrade, the EMPS Connection Settings page appears. Continue at Step 14.

14. On the EMPS Connection Settings page, specify the settings to connect to the EMPS, and then click Next.

- Server Name—The FQDN of the server that is hosting the EMPS.
- User Name—The user name that is used to log in to the EMPS. The default is Admin.
- Password—The password that is used to log in to the EMPS. The default is password.

After you click Next, the Migrate EMPS Data task page appears. Continue at Step 23 on page 209.

Install EMPS

15. On the Install EMPS information page, read the information about installing the EMPS, and then click Next.

The Install EMPS task page appears.

16. On the Install EMPS task page, specify the following:

- In the EMPS Server FQDN text box, enter the FQDN of your EMPS server.
- Select the appropriate tenancy option:
  - — Select Single-tenancy if there is only one reseller.
  - — Select Multi-tenancy if you have purchased the Multi-tenancy option and there is more than one reseller.

Click Next.

The Install EMPS task page for specifying the Lightweight Directory Access Protocol (LDAP) type and settings appears. (For an example, see Figure 14 on page 122.)

17. On the Install EMPS LDAP settings page, specify the LDAP type, and then click Next.

- OpenLDAP—Recommended for small-sized deployments of GVP.

- `SunOne`—Recommended for medium- to large-sized deployments of GVP.

If you select `SunOne`, also specify the following required settings (see Figure 14 on page 122):

- Server Name—The FQDN of the machine that is hosting the Directory Server.
- Server Port—The listening port of the Directory Server. You must set the value to `389`.
- Server Root—The LDAP Root or BaseDN. You must set the value to `o=genesys`.
- User Name—The name that is used to log in to SunOne. You must set the value to `cn=Directory Manager`.
- Password—The password that is used to log in to SunOne. Use the password that you created when you set up your SunOne Directory Server. The password is case sensitive.
- LDAPPath—The path to the SunOne installation folder. Typically, this is `C:\Sun\MPS`.

After you click `Next`, the `Install EMPS` task page for specifying the EMPS installation folder appears.

18. On the `Install EMPS` installation folder page, specify the installation path by accepting the default value or entering a new path in the `Default Location` text box, and then click `Next`. The default path is `C:\GVP\CN`.

An `Install EMPS` information page appears, with information about validation.

19. On the `Install EMPS` information page, read the information about validation, and then click `Next`.

The GDT validates the Windows prerequisites for the EMPS, then displays the results. If validation is successful, a `Validation Successful` page appears.

20. On the `Validation Successful` page, click `Next`.

If you are installing the EMPS on another server (in other words, not the server on which the GDT is running), the GDT transfers the installation software to the EMPS server. The `CD Image Transfer` page appears.

21. On the `CD Image Transfer` page, click `Next`.

After the installation software has been copied to the EMPS server, the `Install EMPS` page appears.

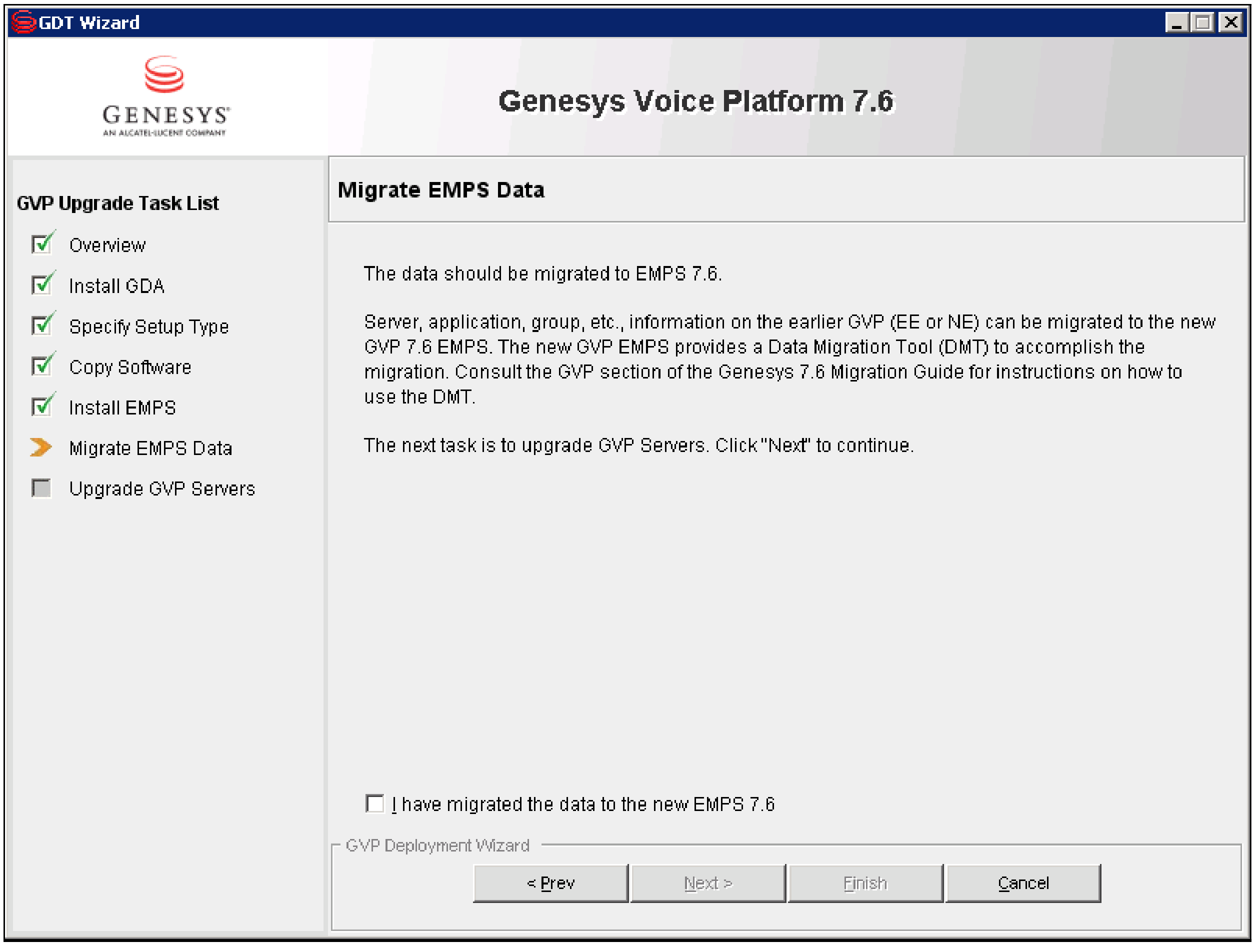
22. On the `Install EMPS` page, click `Next`.

The GDT installs EMPS on the server, then displays the results.

WatchDog automatically restarts.

Click `Next`. The `Migrate EMPS Data` page appears (see Figure 41).

Migrate EMPS Data



The data should be migrated to EMPS 7.6.

Server, application, group, etc., information on the earlier GVP (EE or NE) can be migrated to the new GVP 7.6 EMPS. The new GVP EMPS provides a Data Migration Tool (DMT) to accomplish the migration. Consult the GVP section of the Genesys 7.6 Migration Guide for instructions on how to use the DMT.

The next task is to upgrade GVP Servers. Click "Next" to continue.

□ I have migrated the data to the new EMPS 7.6

Figure 41: Migrate EMPS Data Task Page

23. Use the Data Migration Tool (DMT) to migrate the EMPS data. For more information, see the information about EMPS data migration in the GVP section of the *Genesys Migration Guide*.
24. After the EMPS data has been migrated, select the `I have migrated the data to the new EMPS 7.6` check box on the `Migrate EMPS Data` page, and then click `Next`.

    The `Upgrade GVP Servers` information page appears.

Upgrade GVP Servers

25. On the `Upgrade GVP Servers` information page, read the information about upgrading the GVP servers, and then click `Next`.

    The GDT collects upgrade information.
26. After the upgrade information has been collected, the status bar displays `Completed`. Click `Next`.

    The `Upgrade GVP Servers` task page for selecting the servers appears.

27. Select the server(s) that you want to upgrade from the list box on the left, and click the `Add >` button to move the selected server(s) to the list box on the right.

28. After you have selected the server(s) that you want to upgrade, click `Next`.

29. Click `Next` to upgrade the GVP Servers.

30. Click `Finish` to complete the upgrade.

End of procedure

Next Steps

- Restart WatchDog on the upgraded server(s). For more information, see Starting/Restarting GVP in Normal mode (Windows), page 198.

Procedure: Installing a new EMPS on an existing EMPS server (Windows)

Purpose: To uninstall EMPS and other GVP components on the EMPS host, and then reinstall them in another location, in a way that preserves EMPS data.

Start of procedure

1. Stop the EMPS WatchDog.

   If your EMPS uses OpenLDAP, continue at Step 2.

   If your EMPS uses SunOne Directory Server, continue at Step 5.

2. Unregister the OpenLDAP service.

   a. Stop the OpenLDAP service.

   b. Open a command prompt.

   c. Execute the following command to run the batch file that removes the OpenLDAP registration:

   ```
   <Installation drive>/gvp/cn/openldap/openldap_service.bat slapd
   remove
   ```

3. Uninstall the GVP components on the EMPS host in the following order:

   - EMPS
   - Other GVP components
   - Common

   For information about using the GVP Deployment Tool to uninstall GVP components, see Uninstalling GVP components using the GDT, page 214.

   For information about uninstalling GVP components manually, see “Uninstalling GVP components manually (Windows)” on page 216.

4. If you want to preserve your EMPS data, copy the `<gvp root>/openldap` folder to the new location (for example, `<new gvp root>/openldap`).

   If you do not want to preserve your EMPS data, skip this step.

5. For all installations (Open LDAP or SunOne Directory Server), if the Dispenser was installed on the EMPS host, copy the `<gvp root>/web/dispenser` folder to the new location (for example, `<new gvp root>/web/dispenser`).

6. Delete the old installation folder, to ensure that the former software is completely removed.

7. Install the EMPS and other GVP components in the new location (<new gvp root>). For more information, see Upgrading GVP using the GDT, page 202.

End of procedure

Installing a Hot Fix

This section describes how to use the GDT to install a 7.6.x hot fix for a GVP component.

Note: All GVP components that are running on the same server share Voice Platform Common and must be compatible with it. Be aware that, if you are upgrading one of the components, you may also need to upgrade Voice Platform Common and other components that reside on the same server.

If you are upgrading EMS Reporting components, there may also be database considerations that arise from common database scripts.

For more information, see the applicable release notes and release advisories.

Procedure: Installing a hot fix using the GDT

Purpose: To upgrade a GVP component to a 7.6.x hot fix software release.

Prerequisites

- The hot fix software has been downloaded and is available to the GDT in a path that ends with `ip`.

- A version of the GDA that is compatible with the GDT version is running on the GVP server that hosts the component you want to upgrade. If necessary, upgrade the GDA (see Upgrading the GDA using the GDT, page 202).

Start of procedure

1. Execute the `GVPLaunch.bat` file to launch the GDT.

   For more information about launching the GDT, see the first steps in the procedure Using the GVP Deployment Wizard to install GVP components (Windows only), page 113.
2. Cancel the GVP Deployment Wizard, so that the GDT window has focus.
3. From the `Deploy > Maintenance` menu, select `Hotfix GVP`.

   The `Hotfix GVP` information page appears.
4. On the `Hotfix GVP` information page, click `Next`.

   The `Copy Software` page appears.
5. Browse to the `ip` folder that contains hot fix software, and then click `Next`.

   The GDT copies the installation softwareto its working directory. After the software has been copied, the `Select Servers` page appears.
6. On the `Select Servers` page, use the `Add >` button to move the required server(s) from the list box on the left to the list box on the right, and then click `Next`.
7. Click `Next` to upgrade the GVP server(s).
8. Click `Finish` to complete the hot fix.

End of procedure

Next Steps

- If your hot fix applies to EMS Reporting components or OBN Manager, you may need to update the database schema. See the applicable release note for information about database scripts that you may need to run.
- Restart WatchDog on the upgraded server(s). For more information, see Starting/Restarting GVP in Normal mode (Windows), page 198.

Repairing a GVP Server

To repair a server that has GVP components installed on it, the GDT sends a request to the GDA to uninstall all currently installed components, and then to reinstall the components.

The following procedure describes how to use the GDT to repair a GVP server.

Procedure: Repairing a GVP server using the GDT

Prerequisites

- A version of the GDA that is compatible with the GDT version has been installed and is running on the GVP server that you want to repair. If necessary, upgrade the GDA (see Upgrading the GDA using the GDT, page 202).

Start of procedure

1. Execute the `GVPLaunch.bat` file to launch the GDT.

   For more information about launching the GDT, see the first steps in the procedure Using the GVP Deployment Wizard to install GVP components (Windows only), page 113.
2. Cancel the GVP Deployment Wizard, so that the GDT window has focus.
3. From the `Deploy > Maintenance` menu, select `Repair`.

   The `Select Servers` page appears.
4. On the `Select Servers` page, use the `Add >` button to move the required server(s) from the list box on the left to the list box on the right, and then click `Next`.

   The `Repair started` screen appears.
5. After the repair is completed, click `Next` to return to the GDT.
6. Restart WatchDog.

End of procedure

Uninstalling GVP Components

This section describes how to remove GVP components from a Windows host. It includes the following procedures:

- Uninstalling GVP components using the GDT
- Uninstalling GVP components manually (Windows), page 216
- Uninstalling Dialogic, page 217

Note: WatchDog does not start unless the GVP components that are installed on a server match the configuration shown in the EMPS. When you uninstall a GVP component from a server that has other GVP components on it, the corresponding node in EMPS is not removed. As a result, WatchDog will not start. Contact Genesys Technical Support for assistance if you plan to continue running the remaining software.

Procedure:
Uninstalling GVP components using the GDT

Prerequisites

- A version of the GDA that is compatible with the GDT version has been installed and is running on the GVP server that you want to repair. If necessary, upgrade the GDA (see Upgrading the GDA using the GDT, page 202).

Start of procedure

1. Execute the `GVPLaunch.bat` file to launch the GDT.

   For more information about launching the GDT, see the first steps in the procedure Using the GVP Deployment Wizard to install GVP components (Windows only), page 113.

2. Cancel the GVP Deployment Wizard, so that the GDT window has focus.

3. From the `Deploy > Maintenance > Uninstall` menu, select one of the following menu options, and then click `Next`.
   - `Uninstall All Components`—Uninstalls all the GVP components that are hosted on the server(s) that you specify. The `Select servers` page appears. Continue at Step 4.
   - `Uninstall Selected Components`—Uninstalls only those components (features) that you select on specified servers. The `Uninstall Component Selection` page appears (see Figure 42 on page 215). Continue at Step 5 on page 215.
   - `Uninstall EMPS`—Uninstalls the EMPS. Continue at Step 6 on page 216.

4. If you selected the menu option to uninstall all the GVP components on the specified server(s):

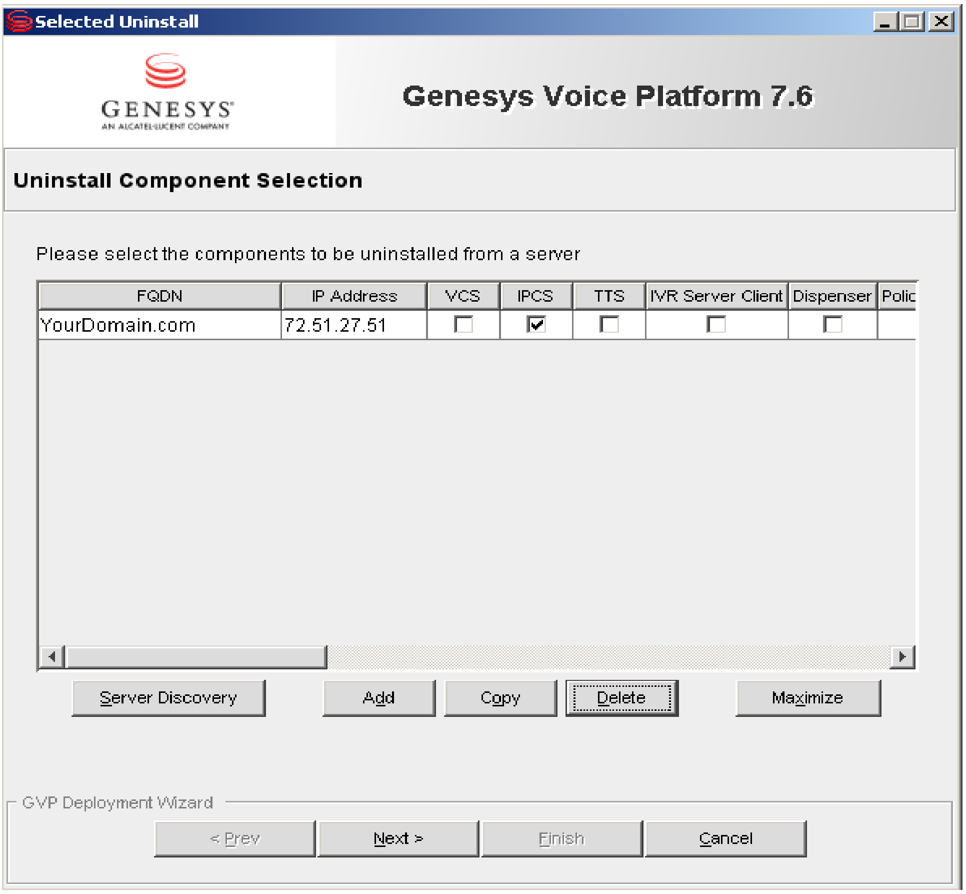
   a. On the `Select Servers` page, use the `Add >` button to move the servers that you want to uninstall from the list box on the left to the list box on the right.

   b. Click `Next`.

      The `Uninstall GVP Components` screen appears.

c. After reading about the uninstall, click `Next` to start the uninstall. Continue at Step 7 on page 216.

5. If you selected the menu option to uninstall selected components, on the `Uninstall Component Selection` page, specify the components that you want to uninstall (see Figure 42).



Uninstall Component Selection

Please select the components to be uninstalled from a server

FQDN	IP Address	VCS	IPCS	TTS	IVR Server Client	Dispenser	Polic
YourDomain.com	72.51.27.51	□	☑	□	□	□	

Figure 42: Uninstall Component Selection Screen

a. The page is populated with the FQDN and IP address of each GVP server in your deployment. In each server row, use the check boxes to specify the features that you want to uninstall on that server (for example, IPCS).

b. Click `Next`.

The `Uninstall GVP Components` screen appears.

c. After reading about the uninstall, click `Next` to start the uninstall.

The wizard validates that the selected components exist on the specified server, and then directs the GDA(s) to uninstall the components.

Continue at Step 7 on page 216.

6. If you selected the menu option to uninstall the EMPS, the `Uninstall EMPS` information page appears. After reading about the uninstall, click `Next` to uninstall the EMPS, Dispenser, and Portal.

   Continue at Step 7.

7. After the uninstall is complete, review the uninstallation messages, and then click `Finish` to return to the GDT.

End of procedure

Next Steps

- Uninstalling the GVP Deployment Agent

Procedure: Uninstalling the GVP Deployment Agent

Perform this procedure on each GVP server from which you want to remove the GDA.

Start of procedure

1. Go to `Add/Remove Programs`.
2. Select the `GVP Deployment Agent` from the list of currently installed programs. Click `Remove`.

   Note: Uninstalling GDA removes the `GDT` folder and all of its contents.L

End of procedure

Procedure: Uninstalling GVP components manually (Windows)

You must uninstall the GVP components one at a time, and in the reverse order of installation. Remove Core Components last.

Note: Uninstalling GVP software does not remove its corresponding entry in LDAP. To remove the entry from LDAP, you must delete the node for the corresponding component in the EMPS.

Start of procedure

1. Go to Add/Remove Programs.
2. Select the appropriate Voice Platform component from the list of currently installed programs. Click Remove.
3. When the uninstall is complete for each of the GVP components, restart the machine.

End of procedure

Procedure: Uninstalling Dialogic

Purpose: To uninstall the software for the Dialogic boards on the Voice Communication Server (VCS).

Start of procedure

1. Go to Add/Remove Programs.
2. Select Intel Dialogic System Release 6.0 PCI Redistributable Edition.
3. Click Remove.
4. When prompted to back up the current configuration, click No unless you expect to reinstall the same version of Dialogic.
5. If the uninstall procedure prompts about specific files to be deleted, click Yes.
6. When prompted, click Yes to restart the machine.
7. After restart, the Dialogic Clean-Up Utility will be displayed briefly, and will delete all Dialogic folders, files, and shortcuts.

End of procedure

Part

3 Solaris Installation

Part Three of this manual describes how to install and set up Genesys Voice Platform (GVP) components on the Solaris operating system. This information appears in the following chapters:

- Chapter 12, “Solaris Deployment Task Summaries,” on page 221
- Chapter 13, “Preparing Your Solaris Environment,” on page 225
- Chapter 14, “Installing GVP on Solaris,” on page 235
- Chapter 15, “Post-Installation Activities on Solaris Hosts,” on page 271
- Chapter 16, “Uninstalling GVP on Solaris,” on page 285

Chapter

12 Solaris Deployment Task Summaries

This chapter describes the installation sequence to deploy Genesys Voice Platform (GVP) on Solaris, and provides links to detailed information about the required tasks.

This chapter contains the following section:

Installing GVP on Solaris

Table 29 summarizes the steps to install GVP in a Solaris environment.

Table 29: Task Summary—Installing GVP on Solaris

Objective	Related Procedures and Actions
1. Plan the deployment.	For specific restrictions and recommendations to consider, see "Host Setup" on page 67.
2. Prepare your environment.	**1.** Install and configure third-party hardware and software: • If you are using Automatic Speech Recognition (ASR) and/or Text-to-Speech (TTS), install the third-party Media Resource Control Protocol (MRCP) speech server host(s). For more information, see your MRCP vendor's documentation. • If your deployment will include EMS Reporting and/or OBN Manager, install the Oracle Server and Oracle Client software and libraries, and prepare tablespaces for the EMPS and EMS Reporting databases. For more information, see "Preparing the Oracle Database Server and Clients" on page 231. • If you are using the SunOne Directory Server for the EMPS, install and configure the directory server on the EMPS host (see "Preparing the SunOne Directory Server" on page 225). For more information about prerequisite software, see "Solaris Prerequisites" on page 63. **2.** Prepare the GVP servers. For more information, see Preparing the GVP servers for software installation (Solaris), page 237. **3.** Stop antivirus software that may be running on systems that will host GVP components.
3. Obtain the GVP software.	For information about the GVP software CDs, see "GVP Software for Solaris" on page 235.
4. Obtain server and database information.	See the Next Steps item on page 238 for details about the information that you must provide during the installation of SNMP, Apache, and Common on all GVP servers.

Table 29: Task Summary—Installing GVP on Solaris (Continued)

Objective	Related Procedures and Actions
5. Install and configure the EMPS.	**1.** Install SNMP, Apache, Common, EMPS, and Dispenser on the EMPS host. • See “Installing SNMP, Apache, and Common on Solaris” on page 238 and “Installing EMPS and Dispenser on Solaris” on page 244. • After installation, check SNMP and modify SNMP configuration as required, as described in the Next Steps item on page 240. **2.** If your deployment will include EMS Reporting and/or OBN Manager, create the EMPS database schema (see “Setting up the EMPS database in Oracle (Solaris).” on page 273). **3.** Verify or modify the EMPS server configuration (see “Configuring EMPS” on page 291). **4.** Start the EMPS WatchDog in safe mode (see Starting/Restarting GVP (Solaris), page 283). **5.** Verify the EMPS installation: • Verifying system connectivity, page 299. • Testing the installation (Solaris), page 248
6. Install the IPCS and other GVP components, as required for your deployment. You must install SNMP, Apache, Common on every GVP server.	See the installation procedures in Chapter 14 on page 235.
7. Verify or modify GVP server configurations in the EMPS.	See the various GVP configuration chapters in Part 4: “GVP Configuration” on page 287.
8. Depending on the features you have installed, perform post-installation activities.	• Configure ASR/TTS (see “Enabling MRCP ASR and TTS” on page 391). • Create the database schemas for EMS Reporting and OBN Manager (see “Setting Up the Databases” on page 272). • For the EMPS and EMS Reporting, modify file permissions as required (see “Setting File Access Permissions” on page 277). • Configure Unified Login (see “Enabling Unified Login” on page 278). • Configure IP Call Manager (IPCM) (see “Enabling IPCM” on page 403).

Table 29: Task Summary—Installing GVP on Solaris (Continued)

Objective	Related Procedures and Actions
9. Start or restart WatchDog on all GVP servers.	See Starting/Restarting GVP (Solaris), page 283.
10. Install the Management Information Base (MIB) files on the SNMP Manager.	See Installing MIB files (Solaris), page 268.

Chapter

13 Preparing Your Solaris Environment

This chapter describes the prerequisites to prepare hardware and software for Genesys Voice Platform (GVP) 7.6 deployments on Solaris hosts.

This chapter contains the following sections:

- Preparing the SunOne Directory Server, page 225
- Preparing the Oracle Database Server and Clients, page 231

For information about all the hardware and software prerequisites for Solaris deployments, see "Solaris Prerequisites" on page 63.

Preparing the SunOne Directory Server

If you plan to use OpenLDAP as the Directory Server for the Element Management Provisioning System (EMPS), no preparation is required.

If you plan to use SunOne/iPlanet Directory Server, you (or your system administrator) must install the software on the EMPS host, and then configure it to set up the appropriate access controls and directory structure elements. The following procedures provide the details:

- Installing SunOne Directory Server (Solaris), page 226
- Creating a root node in SunOne Directory Server 5.1 SP4 (Solaris)
- Creating a root node in SunOne Directory Server 5.2 (Solaris)
- Setting the root node password in SunOne Directory Server 5.1 SP4 or 5.2 (Solaris)

Procedure:
Installing SunOne Directory Server (Solaris)

Start of procedure

1. Follow the instructions from SunOne to set up SunOne Directory Server version 5.1 SP4 or SunOne Directory Server version 5.2.

   During the installation, note all the information that you specify for user names, passwords, administration URLs, and administration ports. (If necessary, obtain this information from your system administrator after installation.)

   Table 30 provides recommendations for the parameters that you must provide during installation.

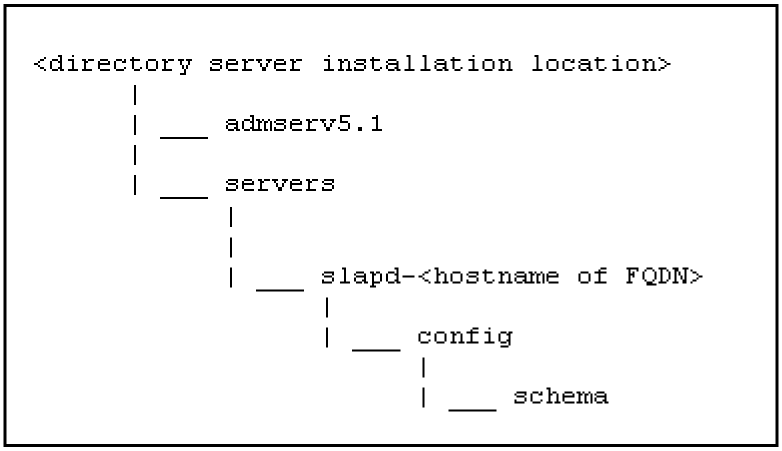
Table 30: SunOne Directory Server Parameter Recommendations

Parameter	Value	Comment
Installation location on hard drive	`/usr/iplanet/servers/`	The last component of the path must be `/servers/`.
LDAP Port	389	GVP requires this value, and you must retain it.
Administration Port	555	The installer suggests random values for administration ports. Genesys recommends that you standardize on one value.
Password for Administrator	`admin123`	
Password for `cn=Directory Manager`	`admin123`	

2. If you are using SunOne Directory Server version 5.2, install Patch 117667-02:
   a. Stop the SNMP service.
   b. Follow the instructions from SunOne to install Patch 117667-02.
   c. Restart the SNMP service.

3. Verify that Directory Server is correctly installed and running:
   a. Telnet to the host on which SunOne/iPlanet Directory Server is installed.
   b. Log in as `root` or obtain root permissions.

c. Verify that the directory structure looks like the structure shown in Figure 43.



```
<directory server installation location>
       |
       | ___ admserv5.1
       |
       | ___ servers
              |
              |
              | ___ slapd-<hostname of FQDN>
                     |
                     | ___ config
                            |
                            | ___ schema
```

Figure 43: Directory Server Structure

d. Restart the Directory Server by entering the following commands:

```
<installation location>/servers/restart-admin
<installation location>/servers/slapd-<hostname>/restart-slapd
```

e. Verify that the system does not report any errors.

End of procedure

Next Steps

- Configure Directory Server:
  - Create a root node. Do one of the following, as applicable:
    - Creating a root node in SunOne Directory Server 5.1 SP4 (Solaris)
    - Creating a root node in SunOne Directory Server 5.2 (Solaris), page 229
  - Set a password for the root node. For more information, see Setting the root node password in SunOne Directory Server 5.1 SP4 or 5.2 (Solaris), page 230.

Procedure: Creating a root node in SunOne Directory Server 5.1 SP4 (Solaris)

Purpose: To create the root node for GVP data (`o=genesys,` or a name that is more suitable for your environment).

The root node is also referred to as the *Root Suffix* or *Root DIT.*

Note: You must use a Sun terminal or, if you want to use a PC, you must be running remote X-server software (for example, Hummingbird's Exceed software).

Start of procedure

1. Log in as `root` or get root permissions.
2. Open the SunOne Server Console by entering the following command:

   `<installation dir>/startconsole`
3. Log in using `cn=Directory Manager` and your password.

   Use the format `AdminURL = http://<host-name>:<Admin-port>`—for example: `http://qa-sun-perf3:555`.
4. In the tree view on the left pane, click the plus sign (+) to expand the server node (for example, `ldap.mycompany.com`).
5. Expand the `Server Group` node, and then select `Directory Server`.

   Verify that the version is correct (5.1 SP4).
6. Right-click `Directory Server`, and then select `Open`.

   The Directory Server Console appears.
7. Create the root suffix:
   a. In the Directory Server Console, click the `Configuration` tab.
   b. Select the `Database` icon, and then expand it.
   c. Select `Object > New Root Suffix`.

      The `Create New Root Suffix` dialog box appears.
   d. In the `New Suffix` field, enter a suffix name of your choice.

   Note: Restrict the values to 8 to 12 lowercase letters.

   The GVP installation uses `o=genesys.net` as the default value.

   e. Select the `Create associated database automatically` check box.
   f. Enter the name of the database—for example, `genesys`.

   Note: Do not use the period (.) character or any other special characters.

   g. Click `OK`.
8. Add the new root object to the directory tree:
   a. In the Directory Server Console, click the `Directory` tab.
   b. Select your local server, and then select `Object > New Root Object > <your newly created root suffix>`.

      A dialog box appears.

c. Select `Organization`, and then click `OK`.

   A dialog box appears.

d. Click `OK` to accept the default values.

The new root node now appears in the directory tree. All data that is relevant to GVP is populated under this node.

End of procedure

Next Steps

- Set the password for the GVP root node. For more information, see Setting the root node password in SunOne Directory Server 5.1 SP4 or 5.2 (Solaris), page 230.

Procedure: Creating a root node in SunOne Directory Server 5.2 (Solaris)

Purpose: To create the root node for GVP data (`o=genesys`, or a name that is more suitable for your environment).

The root node is also referred to as the *Root Suffix* or *Root DIT.*

Note: You must use a Sun terminal or, if you want to use a PC, you must be running remote X-server software (for example, Hummingbird's Exceed software).

Start of procedure

1. Log in as `root` or get root permissions.
2. Open the SunOne Server Console by entering the following command:

   `<installation dir>/startconsole`
3. Log in using `cn=Directory Manager` and your password.

   Use the format `AdminURL = http://<host-name>:<Admin-port>`—for example: `http://qa-sun-perf3:555`.
4. In the tree view on the left pane, click the plus sign (+) to expand the server node (for example, `ldap.mycompany.com`).
5. Expand the `Server Group` node, and then select `Directory Server`.

   Verify that the version is correct.
6. Right-click `Directory Server`, and then select `Open`.

   The Directory Server Console appears.

7. Create the root suffix:
   a. In the Directory Server Console, click the `Configuration` tab.
   b. Select the `Data` icon, and then expand it.
   c. Select `Object > New Suffix.`

      A dialog box appears.
   d. In the `Suffix DN` box, enter a suffix name of your choice (for example, `o=genesys`). Observe the following naming conventions:
      - Format is `o=xyz,` where `o` is lowercase letter *o,* not zero (`0`).
      - Restrict the length to 8 to 12 letters.
      - Use lowercase, without spaces.
   e. Click `OK.`
8. Add the new root object to the directory tree:
   a. In the Directory Server Console, click the `Directory` tab.
   b. Select your local server, and then select `Object > New Root Object > <your newly created root object>.`

      A dialog box appears.
   c. Select `organization,` and then click `OK.`

      A dialog box appears.
   d. Click `OK` to accept the default values.

   The new root node now appears in the directory tree. All data that is relevant to GVP is populated under this node.

End of procedure

Next Steps

- Set the password for the GVP root node. For more information, see Setting the root node password in SunOne Directory Server 5.1 SP4 or 5.2 (Solaris).

Procedure:
Setting the root node password in SunOne Directory Server 5.1 SP4 or 5.2 (Solaris)

Purpose: To provide password-secured access to the root node, which the EMPS uses as a system account for scheduled tasks.

Start of procedure

1. In the Directory Server Console, click the `Directory` tab.
2. Select the root node folder that you created in Creating a root node in SunOne Directory Server 5.1 SP4 (Solaris), page 227 or Creating a root node in SunOne Directory Server 5.2 (Solaris), page 229.
3. Select `Object > Properties`.

   A dialog box appears.
4. Click `Add Attribute`.

   A dialog box appears.
5. Select `userpassword`, and then click `OK`.

   A new attribute, labeled `Password`, appears.
6. Enter a password, and then click `OK`.

   Note: Make note of your password. EMPS uses this password for executing scheduled tasks.

7. Close all SunOne windows.

End of procedure

Next Steps

- Restart the SunOne Directory Server to verify that Directory Server is installed and running. Enter the following commands:

  ```
  <installation location>/servers/restart-admin
  <installation location>/servers/slapd-<hostname>/restart-slapd
  ```

  When all of the services successfully start, the Directory Server configuration is complete.

Preparing the Oracle Database Server and Clients

If your GVP deployment will include Element Management System (EMS) Reporting or Outbound Notification (OBN) Manager, you must install Oracle database server and client software, and prepare tablespaces for the Oracle databases in your environment.

Note: Genesys recommends that you install the Oracle database server on the EMS Reporting/OBN Manager host, and the Oracle client on the

EMPS host. Oracle is required only if EMS Reporting or OBN Manager is installed.

For the supported versions of Oracle, see "Database Server and Client" on page 65.

Table 31 summarizes the steps that you or your database administrator must perform to prepare the Oracle database server and clients.

Table 31: Preparing the Oracle Server and Clients

Objective	Related Procedures and Actions
1. Install the Oracle server software.	**1.** Install Oracle with any database instance name (for example, `GenesysVoicePlatform`). **2.** Configure the database instance to start during system boot.
2. Create the required tablespaces and users.	• For the EMS Reporting components: • `COLLECTOR` • `PEAKS` • `REPORTER` • `REPDWH` • `UNIFIEDLOGIN` • `NETMON` • For OBN Manager, the `obnManager` tablespace and user, with password `obnManager`. A sample script to create the `obnManager` tablespace and user (`OBN_DB_NEW_CREATE_760_oracle.sql`) is available in the installation folder after OBN Manager has been installed. The `obnManager` tablespace script is configured for a specific `DATAFILE` path. Change this path to suit your Oracle installation. • For the EMPS, the `vwps` tablespace and user. For more information, see "Setting up the EMPS database in Oracle (Solaris)." on page 273. **Note:** To enable Reports to be viewed on EMPS and Reporter machines, ensure that all users have rwx permissions to the Oracle directory.

Table 31: Preparing the Oracle Server and Clients (Continued)

Objective	Related Procedures and Actions
3. Install the client software.	• Install and configure the Oracle Client software on the EMPS host and on all other hosts that must access the Oracle server. • Ensure that the SQL Plus utility, which is provided with Oracle, is available. The utility is typically located in `<oracle-installation-dir>/bin`. You must be able to connect to the Oracle server from the client system using the SQL Plus utility.
4. Set environment variables on Oracle clients.	Set the following environment variables on the EMPS host and on all other hosts that must access the Oracle server: • `ORACLE_HOME=<OracleInstallationPath>` • `LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORALCE_HOME/lib32:$LD_LIBRARY_PATH`
5. Record Oracle information.	Ensure that the following information is available during GVP installation and configuration: • `ORACLE_HOME` (for example, `/usr/oracle9iR2` or `/usr/oracle10g`) • `ORACLE_SID` • Password for user `SYSTEM`

Chapter

14 Installing GVP on Solaris

This chapter describes how to install Genesys Voice Platform (GVP) components on the Solaris operating system.

This chapter contains the following sections:

Before You Begin

Before you perform any of the installation procedures in this chapter, review the information in Chapter 13, "Preparing Your Solaris Environment," on page 225, and ensure that you have satisfied all the prerequisites to prepare your environment.

GVP Software for Solaris

Table 32 summarizes the contents of the source software CDs for the GVP components that are supported on Solaris.

Table 32: GVP Source Software CDs for Solaris

CD Name	GVP Components	
Genesys Voice Platform: Base Software (Required)	• Apache • Common • Launcher • SNMP	• BWM (Bandwidth Manager) • Dispenser • EMPS • IPCS • IVR Server Client • MIBs • OBN Manager • Policy Manager • Portal • TTS
Genesys Voice Platform: Reporting and Monitoring (Optional)	• Apache • Common • Launcher • SNMP	• Call Status Monitor • EventC • Login Server • Network Monitor • Reporter • SNMP
Genesys Voice Platform: H.323 Call Manager (Optional)	• Apache • Common • Launcher • SNMP	• H.323 Session Manager • Resource Manager
Genesys Voice Platform: SIP Call Manager (Optional)	• Apache • Common • Launcher • SNMP	• Resource Manager • SIP Session Manager
Genesys Voice Platform: Cisco Queue Adapter (Optional)	• Apache • Common • Launcher • SNMP	• Cisco Queue Adapter
Genesys Voice Platform: MRP SMP Integrator	• Apache • Common • Launcher • SNMP	• MRP SMP Integrator

Preparing the GVP Servers

The following procedure describes the steps that you must perform on each Solaris server that will host a GVP component, before you can install the software on it.

Procedure: Preparing the GVP servers for software installation (Solaris)

Purpose: To create the directory structure and provide the appropriate permissions for the GVP installation software.

Start of procedure

1. On each Solaris GVP server, log in as root or make sure that you have root permissions. You must have root permissions to install and execute all of the GVP components.
2. Create a directory in which you want to install the specific GVP components. Genesys recommends that you use the name `/opt/genesys/gvp.`

   Table 33 lists the paths that Genesys recommends for installing the GVP components. However, you may specify any path that you wish, as long as the paths are different for the SNMP, Apache, and Common components.

Table 33: Solaris Install Paths

GVP Component	Recommended Install Path
SNMP	/opt/genesys/gvp/netsnmp
Apache	/opt/genesys/gvp/www
Common and all other GVP components	/opt/genesys/gvp/cn **Note:** The installation path for Common must end at the `gvp/cn` subdirectory.

3. Create a directory on each host (Genesys recommends `/home/<user_name>/gvpInstallationSW`), and copy the `solution_specific` directory from the required GVP CDs into it.

   For information about locating the source software for the various GVP components, see “GVP Software for Solaris” on page 235.

4. Execute the following commands to add read and execute permissions on all `install.sh` files for each component in the `solaris/solution_specific` directory, for all users:

```
cd <gvpInstallSwDir>/solution_specific/solaris
chmod -R o+rx */install.sh
```

Note: If you did not copy the files directly from the Genesys Voice Platform 7.6 CDs, Genesys strongly recommends that you check the permissions. For example, if you used `File Copy` on a Windows PC to copy the files to a remotely mounted UNIX file system with the `<gvpInstallSwDir>` directory, you should check permissions.

End of procedure

Next Steps

- Ensure that the following information is available, because you must provide it when you install SNMP, Apache, and Common.
  - The e-mail address of the person or administrator responsible for maintaining the SNMP system
  - The physical location of the host server
  - The IP address of your SNMP Manager (for example, HP OpenView)
  - The community name that the SNMP Manager uses

  Note: To ensure security, Genesys strongly recommends that you use a community name other than `public`.

  - The Provisioning Server name
  - The Provisioning Server password
  - The Provisioning user name
- Install the GVP software, starting with the EMPS server (see Installing EMPS (Solaris), page 244).

Installing SNMP, Apache, and Common on Solaris

The SNMP, Apache, and Common components are installed as part of the installation of specific GVP components. The following procedures are referenced during the specific component installation.

Warning! You must install SNMP and Apache components in a different directory from the directory in which you install the GVP component on that host. Otherwise, the installation process overwrites some files, and if you then uninstall the components, the system will be left in an unusable state.

This section provides the following procedures:

- Installing SNMP (Solaris)
- Installing Apache (Solaris), page 240
- Installing Common (Solaris), page 241

Procedure: Installing SNMP (Solaris)

The SNMP installation starts automatically after you select the applicable component (for example, EMPS or IPCS) on the `Main Menu` of the Launcher.

Prerequisites

- For Solaris 10 installations, edit the `/etc/sma/snmp/snmpd.conf` file to disable the SNMP daemon (snmpd) service that is bundled with Solaris. Otherwise, the bundled snmpd starts by default when the system boots, and this prevents the GVP snmpd from starting, because of a possible port conflict.

Start of procedure

1. At each of the following prompts, enter the appropriate information and press `Enter`.

a.
```
Please enter system administrator contact information for this
host (for example hostmaster@yourdomain.com) =>
```

b.
```
Please enter the location of this host (for example "Rack 32")
=>
```

c.
```
Please enter the IP address of your main Network Node Manager
(for example 10.10.0.2) =>
```

d.
```
Please enter the Community Name to be used for SNMP requests and
traps (for example "public"),
please seriously consider using a Community Name other than
"public" for security reasons =>
```

Note: To ensure security, Genesys strongly recommends using a community name other than `public`. The community name you use must match the community name set on the SNMP Manager.

e.
```
Press ENTER to confirm
/opt/genesys/gvp/netsnmp/share/snmp/snmpd.conf as
the destination directory or enter a new one =>
```

2. When you press `Enter` after the last prompt, the installation begins. The system displays the following:

```
Extracting tarfile: data.tar.gz to directory:
/home/<user_name>/opt/genesys/gvp/netsnmp/share/snmp
x bin, 0 bytes, 0 tape blocks
x bin/encode_keychange, 558016 bytes, 1090 tape blocks
x bin/fixproc, 15484 bytes, 31 tape blocks
Installation of Voice Platform 3rd Party SNMP Solaris, version
7.6.xxx.xx completed successfully.
```

End of procedure

Next Steps

- The Launcher automatically begins the installation of Third-Party Apache Solaris (see Installing Apache (Solaris)).
- After the GVP component installation has completed:
  - Verify that SNMP is running. For more information, see Testing, starting, or stopping SNMP (Solaris), page 242.
  - If you have more than one SNMP Manager, edit the `snmpd.conf` file to enter the additional managers. For more information, see Configuring more than one SNMP Manager (Solaris), page 243.
  - Check the SNMP log file to verify the SNMP Multiplexing (SMUX) peer configuration for the SNMP daemon (snmpd). For more information, see Verifying the SNMP log file (Solaris), page 243.

Procedure: Installing Apache (Solaris)

The Apache installation starts automatically after the installation of SNMP.

Start of procedure

1. At the destination prompt, enter the installation directory as `/opt/genesys/gvp/apache` (or any directory different from the GVP install directory), or press `Enter` to select the default.
2. For the Element Management Provisioning System (EMPS) host and the Element Management System (EMS) Reporting or OBN Manager host, type `y` when asked if you want to add Oracle support to PHP, and answer the prompts regarding the version of Oracle. For all other hosts, type `n`.
3. The Launcher verifies that the `ORACLE_HOME` environment variable is set.

- If the `ORACLE_HOME` environment variable is not set, the installation is aborted. You must set this variable, and then re-install Third-Party Apache Solaris.
- If the `ORACLE_HOME` environment variable is set, the Launcher installs Apache. When the installation is complete, the following appears:

  ```
  *** You need to install Voice Platform Common before you can
  start Voice Platform 3rd Party Apache Solaris ***
  Installation of Voice Platform 3rd Party Apache Solaris, version
  7.6.xxx.xx completed successfully.
  ```

End of procedure

Next Steps

- The Launcher automatically begins the installation of Common (see Installing Common (Solaris)).

Procedure:
Installing Common (Solaris)

The Common installation starts automatically after the installation of Apache.

Start of procedure

1. At the destination prompt, enter the installation directory as `/opt/genesys/gvp/cn` or press `Enter` to select the default.

Note: The installation path for Common must end at the `gvp/cn` subdirectory.

2. When prompted, press `Enter` to confirm the default Provisioning Server name. To set a different Provisioning Server name, type the Provisioning server name with domain, and then press `Enter`.
3. When prompted, press `Enter` to confirm the Provisioning user name.
4. Type the Provisioning Password when prompted, and then press `Enter`.

   The Launcher completes the Common component installation. When the installation is complete, the Launcher prompts you to install the selected component.

End of procedure

Next Steps

- The Launcher automatically begins the installation of the required GVP component.

Configuring and Testing SNMP on Solaris

This section describes the steps to test SNMP and to modify the SNMP configuration, if necessary. It contains the following procedures:

- Testing, starting, or stopping SNMP (Solaris), page 242
- Configuring more than one SNMP Manager (Solaris)
- Verifying the SNMP log file (Solaris), page 243

Procedure:
Testing, starting, or stopping SNMP (Solaris)

Prerequisites

- SNMP has been installed (see Installing SNMP (Solaris), page 239).
- For Solaris 10 installations, the bundled `snmpd` service has been disabled in the `/etc/sma/snmp/snmpd.conf` file. For more information, see the Prerequisites item on page 239.

Start of procedure

1. At a command prompt, type the following:

   ```
   ps -ef | grep snmpd
   ```

   The process is running if you receive a system response like the following:

   ```
   qa-sun-perf2# ps -ef|grep snmpd
   root 16347     1  0 10:25:39 ?        0:00
   /home/smith/opt/genesys/gvp/76snmp/sbin/snmpd -c
   /home/smith/opt/genesys
   root 16495 16218  0 10:44:30 pts/2    0:00 grep snmpd
   ```

2. To start SNMP if it is not running, type the following at a command prompt:

   ```
   /etc/init.d/gvpsnmp start
   ```

   Note: The GVP installation script does not start SNMP. SNMP automatically starts when it is installed, or after any reboot of the system.

3. To stop SNMP, type the following at a command prompt:

   ```
   /etc/init.d/gvpsnmp stop
   ```

End of procedure

Procedure: Configuring more than one SNMP Manager (Solaris)

Purpose: To edit the `snmpd.conf` file to enable more than one SNMP Manager in the deployment.

Start of procedure

1. Open the file `/opt/genesys/gvp/netsnmp/share/snmp/snmpd.conf.`
2. For each additional SNMP Manager that will query the GVP Management Information Base (MIB) data, add a `com2sec` line.
3. For each additional SNMP Manager that will receive the GVP traps, add a `trapsink` line.
4. Save the edited `snmpd.conf` file.

   For an example of a GVP `snmpd.conf` file, see "Sample snmpd.conf File" on page 527.
5. Type the following commands to restart the SNMP daemon (snmpd):

   ```
   /etc/init.d/gvpsnmp stop
   /etc/init.d/gvpsnmp start
   ```

Note: Manual pages for SNMP are installed in a subdirectory of the SNMP installation directory. To access the manual pages, use the `-M` flag on the `man` command. For example, to see the documentation about the `snmpd.conf` configuration file, type the following command:

```
man -M /opt/genesys/gvp/76snmp/man snmpd.conf
```

End of procedure

Procedure: Verifying the SNMP log file (Solaris)

Purpose: To verify the SNMP daemon (snmpd) configuration for the SMUX peer.

Start of procedure

1. Open the SNMP log file, `/var/log/snmpd.log,` which snmpd creates after it starts.

   For an example of a GVP SNMP log file, see "Sample SNMP Log File" on page 529.

2. Verify that the log file contains the following line:

   ```
   accepted smux peer: oid SNMPv2-SMI::enterprises.3814, password test,
   descr syslogd
   ```

3. If the log file does not contain the required line, edit the `/opt/genesys/gvp/netsnmp/share/snmp/snmpd.conf` file to ensure that it includes the required `smuxpeer` line.

   For an example of a correctly configured `snmpd.conf` file, see "Sample snmpd.conf File" on page 527.

> Note: You can ignore any timeout lines in the log file, such as `snmpd: send_trap: Timeout`.

End of procedure

Installing EMPS and Dispenser on Solaris

This section describes how to install the Element Management Provisioning System (EMPS) prerequisites and components on a Solaris host.

The section includes the following procedures:

- Installing EMPS (Solaris)
- Installing Dispenser (Solaris), page 247
- Testing the installation (Solaris), page 248

Procedure: Installing EMPS (Solaris)

Summary

Installing EMPS is a multi-stage process. The Launcher guides you through the installation of the following:

- SNMP (Step 5)
- Apache (Step 6)
- Common (Step 7)
- EMPS (Steps 8 through 13)
- Portal (Step 14)

Prerequisites

- Java Runtime Environment (JRE) has been installed on each machine on which the EMPS user interface (SPM) will be accessed with a browser. If Java runtime has not yet been installed on an EMPS server, download JRE from `www.java.com,` and follow the JRE installation instructions that are available on `java.sun.com`.
- The information that you must provide during the installation of SNMP, Apache, and Common is available. For details about the required information, see Next Steps item on page 238.
- All third-party software, especially antivirus software, has been stopped on the server on which you will install EMPS and Dispenser.

Start of procedure

1. On the Solaris host that contains the Sun One Directory Server, log in as `root`.
2. Open a terminal window and navigate to the `solution_specific/solaris/Launcher` directory in the directory that contains the GVP installation software.
3. Type the following command to start the installation:

   ```
   sh install.sh
   ```

   The `Main Menu` appears.
4. Type `4` (EMPS and Portal), and press `Enter`.

Installing SNMP, Apache, and Common

5. The Launcher proceeds to install SNMP. For more information, see Installing SNMP (Solaris), page 239.
6. The Launcher proceeds to install Apache. For more information, see Installing Apache (Solaris), page 240.

   During the installation, when you are asked if you want to add Oracle support to PHP, type `y`. Answer the prompts regarding the version of Oracle.
7. The Launcher proceeds to install Common. For more information, see Installing Common (Solaris), page 241.

   During the installation, when you are prompted to register Common with EMPS, select `n`.

   When the installation of Common is complete, the following appears:

   ```
   Installation of Voice Platform Common, version 7.6.xxx.xx completed
   successfully.
   ```

Installing EMPS

8. After Common has installed successfully, the Launcher proceeds with EMPS installation.

When you are prompted to confirm the destination directory:

- To accept the default selection, type `y`, then press `Enter`.
- To set a different destination directory:
  — Type `n`, then press `Enter`.
  — Type the installation path, then press `Enter`.

The Launcher extracts the required files and places them in the destination directory.

When the Launcher has finished extracting the files, it begins to update the Provisioning schema.

9. When prompted, enter your tenancy choice (`Do you want to install EMPS in Single-Tenanted mode (y) or in Multi-Tenanted mode (n) (y/n)?`).

10. When prompted for DataStore, enter `Y` for `Sun-One` or `N` for `OpenLDAP`.

11. When prompted, provide the following information:

a. Provisioning Server Name (OpenLDAP or Sun-One)

b. Provisioning Username—For OpenLDAP, enter `cn=Manager`. For SunOne, enter `cn=Directory Manager`.

c. LDAP port number—Valid values are `0` and `389`. Enter `389`.

d. Provisioning user password—Enter `admin123`.

e. Root node—Enter `o=genesys`.

Note: The values displayed in the Launcher are not default values.

12. The Launcher verifies that the `ORACLE_HOME` environment variable is set.

- If the `ORACLE_HOME` environment variable is not set, the installation is aborted. You must set this variable, and then reinstall EMPS (starting from Step 3 on page 245).
- If the `ORACLE_HOME` environment variable is set, the Launcher continues with the EMPS installation.

13. When prompted with `Are you using Oracle10g (y/n)?`, type the appropriate answer.

Note: If you are using Oracle 10g and type `n`, EMPS will not work correctly.

The Launcher continues with the installation of EMPS. When the EMPS installation is complete, a message appears, indicating success.

14. The Launcher automatically continues with the Portal installation.

    The portal software is installed under `<CN_ROOT>/web/GVPPortal`.

    When the Portal installation is complete, the `Main Menu` appears.

15. Type `8` to exit the Launcher.

End of procedure

Next Steps

- Verify SNMP. For more information, see the relevant item under Next Steps on page 240.
- Verify that you can access the portal. Use the following URL:

  `http://<FQDN of EMPS machine>:9810/gvpportal`
- Install Dispenser. For more information, see Installing Dispenser (Solaris).

Procedure: Installing Dispenser (Solaris)

The Dispenser is installed in the same path as the Common component on the GVP host.

Start of procedure

1. Open the terminal server, and navigate to the folder where the Dispenser IP is available.
2. Enter `sh install.sh`
3. Confirm that it is acceptable to use `/opt/genesys/gvp/cn` as the destination directory.

   If it is not acceptable, stop setup by entering `n`.
4. When prompted `Do you wish to continue (y/n)?`, enter `y`.
5. Press `Enter` to confirm `<provisioning server>` as the Provisioning Server, or enter a new one.
6. Press `Enter` to confirm `admin` as the Provisioning User, or enter a new one.
7. Enter the Provisioning Server password.
8. Enter `chmod 777 log` from the `CN` directory.

End of procedure

Next Steps

- Before installing other GVP components, you must create the EMPS database and configure the EMPS server in EMPS. For more information, see Setting up the EMPS database in Oracle (Solaris)., page 273 and "Configuring EMPS" on page 291.
- Verify EMPS installation by starting EMPS. For more information, see Starting/Restarting GVP (Solaris), page 283.
- Test the installation (see Testing the installation (Solaris).

Procedure: Testing the installation (Solaris)

Purpose: To provision a voice application to test for the correct creation and FTP transfer of the `did.xml` and `app.xml` files.

Start of procedure

1. Create and provision a VoiceXML application, as described in the *Genesys Voice Platform 7.6 Reference Manual.* The application is for test purposes only, and does not have to be a real application with valid parameters.
2. Check for `did.xml` and `app.xml` files on the EMPS host in the location that you specified in the EMPS host configuration (see the description of the `Local XML Files Folder` parameter on page 294).
3. Check that the `did.xml` and `app.xml` files were sent by FTP to the Dispenser.

End of procedure

Installing EMS Runtime on Solaris

EMS Runtime refers to a number of optional components that provide additional functionality to manage GVP operations. This section provides the procedures to install and test the EMS Runtime components:

- Installing EMS Runtime (Solaris)—to install IVR Server Client, Bandwidth Manager, Policy Manager
- Installing Cisco Queue Adapter (Solaris), page 253
- Installing MRP SMP Integrator (Solaris), page 254

Procedure:
Installing EMS Runtime (Solaris)

Summary

Installing EMS Runtime is a multi-stage process. The Launcher guides you through the installation of the following components:

- SNMP (Step 5)
- Apache (Step 6)
- Common (Step 7)
- IVR Server Client (Steps 8 through 11)
- Bandwidth Manager (Steps 12 through 15)
- Policy Manager (Steps 16 through 19)

If you install EMS Runtime components on different servers, you must install SNMP, Apache, and Common on all the EMS Runtime servers.

Note: Cisco Queue Adapter (CQA) and Media Resource Platform (MRP) System Management Protocol (SMP) Integrator are EMS Runtime components that you must install separately. For more information, see Installing Cisco Queue Adapter (Solaris), page 253 and Installing MRP SMP Integrator (Solaris), page 254.

Prerequisites

- All third-party software, especially antivirus software, has been stopped on the server(s) on which you will install EMS Runtime components.
- The information that you must provide during the installation of SNMP, Apache, and Common is available. For details about the required information, see Next Steps item on page 238.
- The EMPS database has been created, and the EMPS server has been configured in EMPS. For more information, see Setting up the EMPS database in Oracle (Solaris)., page 273 and "Configuring EMPS" on page 291.

Start of procedure

1. On the Solaris host that will be used as the EMS machine, log in as `root`.
2. Open a terminal window and navigate to the `solution_specific/solaris/Launcher` directory in the directory that contains the GVP installation software.

3. Type the following command to start the installation:

   ```
   sh install.sh
   ```

   The `Main Menu` appears.

4. Type `2` (EMS Runtime) and press `Enter`.

Installing SNMP, Apache, and Common

5. The Launcher proceeds to install SNMP. For more information, see Installing SNMP (Solaris), page 239.

6. The Launcher proceeds to install Apache. For more information, see Installing Apache (Solaris), page 240.

   During the installation, when you are asked if you want to add Oracle support to PHP, type `n`.

7. The Launcher proceeds to install Common. For more information, see Installing Common (Solaris), page 241.

   During the installation, when you are prompted to register Common with EMPS, select `y`.

   When the installation of Common is complete, the following appears:

   ```
   Installation of Voice Platform Common, version 7.6.xxx.xx completed
   successfully.
   ```

   After Common has installed successfully, the Launcher proceeds with the IVR Server Client installation.

Installing IVR Server Client

8. The Launcher prompts you for the installation directory:

   ```
   Please confirm that it is acceptable to use /opt/genesys/gvp/cn
   directory as destination directory.
   
   Do you wish to continue (y/n)?
   ```

   Type `y` to accept the selection, and then press `Enter`.

   To set a different destination directory, type `n` and press `Enter`. The Launcher prompts you for a new destination directory. Type the installation path, and then press `Enter`.

9. The Launcher prompts you for the Provisioning server name:

   ```
   Press ENTER to confirm "your_server_hostname.your_server_domain" as
   the Provisioning Server or enter a new one =>
   ```

   Press `Enter` to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press `Enter`.

10. The Launcher prompts you for the Provisioning user name:

    ```
    Press ENTER to confirm "admin" as the Provisioning User or enter a
    new one =>
    ```

    Press `Enter`.

11. The Launcher prompts you to provide a password for Provisioning:

    ```
    Please enter Provisioning password =>
    ```

    Type the Provisioning Password (default is `password`), and then press `Enter`."

    This completes the installation of IVR Server Client. The Launcher now prompts you to install Bandwidth Manager.

Installing Bandwidth Manager

12. The Launcher prompts you for the installation directory:

    ```
    Please confirm that it is acceptable to use /opt/genesys/gvp/cn
    directory as destination directory.
    ```

    ```
    Do you wish to continue (y/n)?
    ```

    Type `y` to accept the selection, and then press `Enter`.

    To set a different destination directory, type `n` and press `Enter`. The Launcher prompts you for a new destination directory. Type the installation path, and then press `Enter`.

13. The Launcher prompts you for the Provisioning server name:

    ```
    Press ENTER to confirm "your_server_hostname.your_server_domain" as
    the Provisioning Server or enter a new one =>
    ```

    Press `Enter` to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press `Enter`.

14. The Launcher prompts you for the Provisioning user name:

    ```
    Press ENTER to confirm "admin" as the Provisioning User or enter a
    new one =>
    ```

    Press `Enter`.

15. The Launcher prompts you to provide a password for Provisioning:

    ```
    Please enter Provisioning password =>
    ```

    Type the Provisioning Password, and then press `Enter`.

    This completes the installation of Bandwidth Manager. The Launcher now prompts you to install Policy Manager.

Installing Policy Manager

16. The Launcher prompts you for the installation directory:

    ```
    Please confirm that it is acceptable to use /opt/genesys/gvp/cn
    directory as destination directory.
    ```

    ```
    Do you wish to continue (y/n)?
    ```

    Type `y` to accept the selection, and then press `Enter`.

    To set a different destination directory, type `n` and press `Enter`. The Launcher prompts you for a new destination directory. Type the installation path, and then press `Enter`.

17. The Launcher prompts you for the Provisioning server name:

    ```
    Press ENTER to confirm "your_server_hostname.your_server_domain" as
    the Provisioning Server or enter a new one =>
    ```

    Press `Enter` to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press `Enter`.

18. The Launcher prompts you for the Provisioning user name:

    ```
    Press ENTER to confirm "admin" as the Provisioning User or enter a
    new one =>
    ```

    Press `Enter`.

19. The Launcher prompts you to provide a password for Provisioning:

    ```
    Please enter Provisioning password =>
    ```

    Type the Provisioning Password, and then press `Enter`.

    When the Policy Manager installation is complete, the `Main Menu` appears.

20. Type `8` to exit the Launcher.

End of procedure

Next Steps

- Verify SNMP. For more information, see the relevant item under Next Steps on page 240.
- If required, install the additional EMS Runtime components:
    - Cisco Queue Adapter (see Installing Cisco Queue Adapter (Solaris))
    - MRP SMP Integrator (see Installing MRP SMP Integrator (Solaris), page 254)
- If your deployment uses IVR Servers, create and configure the IVR Servers (see “Configuring IVR Server” on page 301).
- If your deployment does not use IVR Servers, proceed to test the installation (see Testing the installation (Solaris), page 248).

Procedure: Installing Cisco Queue Adapter (Solaris)

Purpose: To install the component that connects a multi-tenant GVP to Cisco ICM Enterprise Call Routers.

Prerequisites

- All third-party software, especially antivirus software, has been stopped on the server on which you will install Cisco Queue Adapter (CQA).
- The EMPS database has been created, and the EMPS server has been configured in EMPS. For more information, see Setting up the EMPS database in Oracle (Solaris)., page 273 and "Configuring EMPS" on page 291.

Start of procedure

1. From the Genesys Voice Platform Cisco Queue Adapter CD, copy the contents of the `solution_specific` directory to the EMS Runtime server directory on which you wish to install this component.
2. Change the directory to where you placed the installation package for the Cisco Queue Adapter.
3. Log in as root or get root permissions.
4. Type `sh install.sh`.
5. When prompted, enter the following information:
   a. Destination directory for the installation:

      Type `<target directory>`

      For example, `/opt/genesys/gvp/cn`

   b. Provisioning Server:

      Press `Enter` or type `<FQDN of EMPS system>`.

   c. Provisioning User:

      Press `Enter` or type `admin`.

   d. Provisioning User Password:

      Type your password.

      For example, `password`

End of procedure

Procedure: Installing MRP SMP Integrator (Solaris)

Purpose: To install the component that integrates GVP with the Alcatel Open Service Platform Media Extensions (OSPME).

Prerequisites

- GVP Common has been installed on the Solaris machine that will host MRP SMP Integrator. For more information about installing Common, see Installing Common (Solaris), page 241.
- All third-party software, especially antivirus software, has been stopped on the server on which you will install MRP SMP Integrator.

Start of procedure

1. From the Genesys Voice Platform MRP SMP Integrator CD, copy the contents of the `solution_specific/solaris/MRPSMPIntegrator` directory to the directory containing the GVP installation software.
2. Type the following command to start the installation:

   ```
   sh install.sh
   ```
3. When prompted, specify the installation directory:

   ```
   Please confirm that it is acceptable to use /opt/genesys/gvp/cn
   directory as destination directory.
   ```

   ```
   Do you wish to continue (y/n)?
   ```

   Type `y` to accept the selection, and then press `Enter`.

   To set a different destination directory, type `n` and press `Enter`. You will be prompted for a new destination directory. Type the installation path, and then press `Enter`.
4. When prompted, specify the Provisioning Server name:

   ```
   Press ENTER to confirm
   ```

   `"your_server_hostname.your_server_domain" as the Provisioning` Server or enter a new one =>

   Press `Enter` to accept the selection. To set a different Provisioning Server name, type the Provisioning Server name with domain, and then press `Enter`.
5. When prompted, provide a password for Provisioning:

   ```
   Please enter Provisioning password =>
   ```

   Type the Provisioning Password, and then press `Enter`.

End of procedure

Next Steps

- Configure MRP SMP Integrator (see "Configuring MRP SMP Integrator" on page 304).

Installing EMS Reporting and OBN Manager on Solaris

This section describes the procedures to install the EMS Reporting and Outbound Notification (OBN) Manager components on a Solaris host.

Procedure: Installing EMS Reporting (Solaris)

Summary

Installing EMS Reporting is a multi-stage process. The Launcher guides you through the installation of the following components:

- SNMP (Step 5)
- Apache (Step 6)
- Common (Step 7)
- EventC (Steps 8 through 11)
- Reporter (Steps 12 through 16)
- Login Server (Steps 17 through 21)
- Call Status Monitor (Steps 22 through 26)
- Network Monitor (Steps 27 through 31)

Prerequisites

- Oracle server software for the Reporting databases has been installed and configured as described in "Preparing the Oracle Database Server and Clients" on page 231.
- All third-party software, especially antivirus software, has been stopped on the server on which you will install EMS Reporting components.
- The information that you must provide during the installation of SNMP, Apache, and Common is available. For details about the required information, see Next Steps item on page 238.
- The EMPS database has been created, and the EMPS server has been configured in EMPS. For more information, see "Setting up the EMPS database in Oracle (Solaris)." on page 273 and "Configuring EMPS" on page 291.

Start of procedure

1. On the Solaris host that will be used as the EMS machine, log in as `root`.
2. Open a terminal window and navigate to the `solution_specific/solaris/Launcher` directory in the directory that contains the GVP installation software.
3. Type the following command to start the installation:

   ```
   sh install.sh
   ```

   The `Main Menu` appears.
4. Type `1` (EMSREPORTING), and then press `Enter`.

Installing SNMP, Apache, and Common

5. The Launcher proceeds to install SNMP. For more information, see Installing SNMP (Solaris), page 239.
6. The Launcher proceeds to install Apache. For more information, see Installing Apache (Solaris), page 240.

   During the installation, when you are asked if you want to add Oracle support to PHP, type `y`. Answer the prompts regarding the version of Oracle.K.
7. The Launcher proceeds to install Common. For more information, see Installing Common (Solaris), page 241.

   During the installation, when you are prompted to register Common with EMPS, select `y`.

   When the installation of Common is complete, the following appears:

   ```
   Installation of Voice Platform Common, version 7.6.xxx.xx completed
   successfully.
   ```

   After Common has installed successfully, the Launcher proceeds to the EventC installation.

Installing EventC

8. The Launcher prompts you for the installation directory:

   ```
   Please confirm that it is acceptable to use /opt/genesys/gvp/cn
   directory as destination directory.
   ```

   ```
   Do you wish to continue (y/n)?
   ```

   Type `y` to accept the selection, and then press `Enter`.

   To set a different destination directory, type `n` and press `Enter`. The Launcher prompts you for a new destination directory. Type the installation path, and then press `Enter`.

9. The Launcher prompts you for the Provisioning server name:

   ```
   Press ENTER to confirm "your_server_hostname.your_server_domain" as
   the Provisioning Server or enter a new one =>
   ```

   Press `Enter` to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press `Enter`.

10. The Launcher prompts you for the Provisioning user name:

    ```
    Press ENTER to confirm "admin" as the Provisioning User or enter a
    new one =>
    ```

    Press `Enter`.

11. The Launcher prompts you to provide a password for Provisioning:

    ```
    Please enter Provisioning password =>
    ```

    Type the Provisioning Password, and then press `Enter`.

    The installation process continues, and when it is complete, a message appears, indicating successful completion.

    The Launcher now prompts you to install the Reporter component.

Installing Reporter

12. Stop Apache and WatchDog if they are running by typing:

    ```
    /etc/init.d/gvpapache stop
    /etc/init.d/gvp stop
    ```

13. The Launcher prompts you for the installation directory:

    ```
    Please confirm that it is acceptable to use /opt/genesys/gvp/cn
    directory as destination directory.
    ```

    ```
    Do you wish to continue (y/n)?
    ```

    Type `y` to accept the selection, and then press `Enter`.

    To set a different destination directory, type `n` and press `Enter`. The Launcher prompts you for a new destination directory. Type the installation path, and then press `Enter`.

14. The Launcher prompts you for the Provisioning server name:

    ```
    Press ENTER to confirm "your_server_hostname.your_server_domain" as
    the Provisioning Server or enter a new one =>
    ```

    Press `Enter` to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press `Enter`.

15. The Launcher prompts you for the Provisioning user name:

    ```
    Press ENTER to confirm "admin" as the Provisioning User or enter a
    new one =>
    ```

    Press `Enter`.

16. The Launcher prompts you to provide a password for Provisioning:

```
Please enter Provisioning password =>
```

Type the Provisioning Password, and then press `Enter`.

The installation process continues, and when it is complete, the following message appears:

```
Installation of Voice Platform Reporter completed successfully.
```

The Launcher now prompts you to install the Login Server component.

Installing Login Server

17. Stop Apache and WatchDog if they are running by typing:

```
/etc/init.d/gvpapache stop
/etc/init.d/gvp stop
```

18. The Launcher prompts you for the installation directory:

```
Please confirm that it is acceptable to use /opt/genesys/gvp/cn
directory as destination directory.
```

```
Do you wish to continue (y/n)?
```

Type `y` to accept the selection, and then press `Enter`.

To set a different destination directory, type `n` and press `Enter`. The Launcher prompts you for a new destination directory. Type the installation path, and then press `Enter`.

19. The Launcher prompts you for the Provisioning server name:

```
Press ENTER to confirm "your_server_hostname.your_server_domain" as
the Provisioning Server or enter a new one =>
```

Press `Enter` to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press `Enter`.

20. The Launcher prompts you for the Provisioning user name:

```
Press ENTER to confirm "admin" as the Provisioning User or enter a
new one =>
```

Press `Enter`.

21. The Launcher prompts you to provide a password for Provisioning:

```
Please enter Provisioning password =>
```

Type the Provisioning Password, and then press `Enter`.

The Login Server installation continues, and when it is complete, the following message appears:

```
Installation of Voice Platform Login Server completed successfully.
```

The Launcher now prompts you to install the Call Status Monitor component.

Installing Call Status Monitor

22. Stop Apache and WatchDog if they are running by typing:

```
/etc/init.d/gvpapache stop
/etc/init.d/gvp stop
```

23. The Launcher prompts you for the installation directory:

```
Please confirm that it is acceptable to use /opt/genesys/gvp/cn
directory as destination directory.
```

```
Do you wish to continue (y/n)?
```

Type `y` to accept the selection, and then press `Enter`.

To set a different destination directory, type `n` and press `Enter`. The Launcher prompts you for a new destination directory. Type the installation path, and then press `Enter`.

24. The Launcher prompts you for the Provisioning server name:

```
Press ENTER to confirm "your_server_hostname.your_server_domain" as
the Provisioning Server or enter a new one =>
```

Press `Enter` to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press `Enter`.

25. The Launcher prompts you for the Provisioning user name:

```
Press ENTER to confirm "admin" as the Provisioning User or enter a
new one =>
```

Press `Enter`.

26. The Launcher prompts you to provide a password for Provisioning:

```
Please enter Provisioning password =>
```

Type the Provisioning Password, and then press `Enter`.

The installation continues, and when it is complete, the following message appears:

```
Installation of Voice Platform Call Status Monitor completed
successfully.
```

The Launcher now prompts you to install the Network Monitor component.

Installing Network Monitor

27. Stop Apache and WatchDog if they are running by typing:

```
/etc/init.d/gvpapache stop
/etc/init.d/gvp stop
```

28. The Launcher prompts you for the installation directory:

    ```
    Please confirm that it is acceptable to use /opt/genesys/gvp/cn
    directory as destination directory.
    ```

    ```
    Do you wish to continue (y/n)?
    ```

    Type `y` to accept the selection, and then press `Enter`.

    To set a different destination directory, type `n` and press `Enter`. The Launcher prompts you for a new destination directory. Type the installation path, and then press `Enter`.

29. The Launcher prompts you for the Provisioning server name:

    ```
    Press ENTER to confirm "your_server_hostname.your_server_domain" as
    the Provisioning Server or enter a new one =>
    ```

    Press `Enter` to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press `Enter`.

30. The Launcher prompts you for the Provisioning user name:

    ```
    Press ENTER to confirm "admin" as the Provisioning User or enter a
    new one =>
    ```

    Press `Enter`.

31. The Launcher prompts you to provide a password for Provisioning:

    ```
    Please enter Provisioning password =>
    ```

    Type the Provisioning Password, and then press `Enter`.

    The installation continues, and when it is complete, the following message appears:

    ```
    Installation of Voice Platform Network Monitor completed
    successfully.
    ```

    The installation of the EMS Reporting host server is complete. The `Main Menu` appears.

32. If your deployment includes Outbound Notification (OBN), continue with installing OBN Manager (see Installing OBN Manager (Solaris)).

    If your deployment does not include OBN, type `3` to exit the Launcher.

End of procedure

Next Steps

- If your deployment includes Outbound Notification (OBN), install OBN Manager (see Installing OBN Manager (Solaris)).
- Verify SNMP. For more information, see the relevant item under Next Steps on page 240.

- Create the required databases and then configure the EMS Reporting components in EMPS. For more information, see “Creating the Oracle Databases” on page 271 and Chapter 19 on page 309.

Procedure: Installing OBN Manager (Solaris)

Prerequisites

- Oracle server software for the OBN database has been installed and configured as described in “Preparing the Oracle Database Server and Clients” on page 231.
- The EMPS database has been created, and the EMPS server has been configured in EMPS. For more information, see Setting up the EMPS database in Oracle (Solaris)., page 273 and “Configuring EMPS” on page 291.
- SNMP, Apache, and Common have been installed on the OBN Manager server. If they have not, start the installation of OBN Manager as described in Installing EMS Reporting (Solaris), Step 1 on page 256 through Step 7, until you are returned to the `Main Menu`.

Start of procedure

1. At the `Main Menu` of the Launcher, type `4` (`OBN Manager`), and then press `Enter`.
2. The Launcher prompts you for the installation directory:

   ```
   Please confirm that it is acceptable to use /opt/genesys/gvp/cn
   directory as destination directory.
   ```

   ```
   Do you wish to continue (y/n)?
   ```

   Type `y` to accept the selection, and then press `Enter`.

   To set a different destination directory, type `n` and press `Enter`. The Launcher prompts you for a new destination directory. Type the installation path, and then press `Enter`.
3. When prompted `Will you use Oracle10g (y/n)?`, type the appropriate answer.
4. The Launcher verifies that the `ORACLE_HOME` environment variable is set. If it is not set, the installation is aborted, and you must set this variable, and re-install OBN Manager.

5. The Launcher prompts you for the Provisioning server name:

   ```
   Press ENTER to confirm "your_server_hostname.your_server_domain" as
   the Provisioning Server or enter a new one =>
   ```

   Press `Enter` to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press `Enter`.

6. The Launcher prompts you for the Provisioning user name:

   ```
   Press ENTER to confirm "admin" as the Provisioning User or enter a
   new one =>
   ```

   Press `Enter`.

7. The Launcher prompts you to provide a password for Provisioning:

   ```
   Please enter Provisioning password =>
   ```

   Type the Provisioning Password, and then press `Enter`.

   When the OBN Manager installation is complete, the `Main Menu` appears.

8. Type `6` to exit the Launcher.

End of procedure

Next Steps

- Verify SNMP. For more information, see the relevant item under Next Steps on page 240.
- Create the OBN database, and then configure the OBN Manager in EMPS. For more information, see "Setting up the OBN Manager database in Oracle (Solaris)" on page 276 and "Configuring OBN Manager" on page 335.

Installing IPCS on Solaris

This section describes how to install the IP Communication Server (IPCS) components.

Procedure: Installing IPCS (Solaris)

Summary

Installing IPCS is a multi-stage process. The Launcher guides you through the installation of the following components:

- SNMP (Step 5)
- Apache (Step 6)

- Common (Step 7)
- IPCS (Steps 8 through 12)

Prerequisites

- All third-party software, especially antivirus software, has been stopped on the server on which you will install IPCS.
- The information that you must provide during the installation of SNMP, Apache, and Common is available. For details about the required information, see Next Steps item on page 238.
- The EMPS database has been created, and the EMPS server has been configured in EMPS. For more information, see Setting up the EMPS database in Oracle (Solaris)., page 273 and “Configuring EMPS” on page 291.

Start of procedure

1. On the Solaris host that will be used as the IPCS machine, log in as `root`.
2. Open a terminal window and navigate to the `solution_specific/solaris/Launcher` directory in the directory that contains the GVP installation software.
3. Type the following command to start the installation:

   ```
   sh install.sh
   ```

   The `Main Menu` appears.
4. Type `1` to install IPCS, and then press `Enter`.

Installing SNMP, Apache, and Common

5. The Launcher proceeds to install SNMP. For more information, see Installing SNMP (Solaris), page 239.
6. The Launcher proceeds to install Apache. For more information, see Installing Apache (Solaris), page 240.

   During the installation, when you are asked if you want to add Oracle support to PHP, type `n` for no.
7. The Launcher proceeds to install Common. For more information, see Installing Common (Solaris), page 241.

   During the installation, when you are prompted to register Common with EMPS, select `y`.

   When the installation of Common is complete, the following appears:

   ```
   Installation of Voice Platform Common, version 7.6.xxx.xx completed
   successfully.
   ```

   After Common has installed successfully, the Launcher proceeds to the IPCS installation.

Installing IPCS

8. The Launcher prompts you for the installation directory:

   ```
   Please confirm that it is acceptable to use /opt/genesys/gvp/cn
   directory as destination directory.
   ```

   ```
   Do you wish to continue (y/n)?
   ```

   Type `y` to accept the selection, and then press `Enter`.

   To set a different destination directory, type `n` and press `Enter`. The Launcher prompts you for a new destination directory. Type the installation path, and then press `Enter`.

9. The Launcher prompts you for the Provisioning server name:

   ```
   Press ENTER to confirm "your_server_hostname.your_server_domain" as
   the Provisioning Server or enter a new one =>
   ```

   Press `Enter` to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press `Enter`.

10. The Launcher prompts you for the Provisioning user name:

    ```
    Press ENTER to confirm "admin" as the Provisioning User or enter a
    new one =>
    ```

    Press `Enter`.

11. The Launcher prompts you to provide a password for Provisioning:

    ```
    Please enter Provisioning password =>
    ```

    Type the Provisioning Password, and then press `Enter`.

    The Launcher finishes installing the IPCS and registers it with Provisioning.

    TTS is installed as part of IPCS. The Launcher registers MRCP TTS and MRCP ASR Server with the EMPS.

    When the IPCS installation is complete, the `Main Menu` appears.

12. Type `6` to exit the Launcher.

End of procedure

Next Steps

- Configure the IPCS in EMPS. For more information, see Chapter 20 on page 341.

Installing IP Call Manager on Solaris

This section describes how to install the IP Call Manager (IPCM) components:

- For SIP: Resource Manager and SIP Session Manager

- For H.323: Resource Manager and H.323 Session Manager

Note: If you are using the Genesys SIP Server, you do not need to install the SIP Session Manager.

Procedure: Installing Call Manager (Solaris)

Summary

Installing IPCM is a multi-stage process. The Launcher guides you through the installation of the following components:

- SNMP (Step 5)
- Apache (Step 6)
- Common (Step 7)
- Resource Manager (Steps 8 through 11)
- SIP Session Manager or H.323 Session Manager (Steps 12 through 15)

Prerequisites

- All third-party software, especially antivirus software, has been stopped on the server on which you will install IPCM components.
- The information that you must provide during the installation of SNMP, Apache, and Common is available. For details about the required information, see Next Steps item on page 238.
- The EMPS database has been created, and the EMPS server has been configured in EMPS. For more information, see Setting up the EMPS database in Oracle (Solaris)., page 273 and “Configuring EMPS” on page 291.

Start of procedure

1. On the Solaris host that will be used as the IPCM machine, log in as `root`.
2. Open a terminal window and navigate to the `solution_specific/solaris/Launcher` directory in the directory that contains the GVP installation software.
   - For SIP, obtain the software from the Genesys Voice Platform: SIP Call Manager 7.6 CD.
   - For H.323, obtain the software from the Genesys Voice Platform: H.323 Call Manager 7.6 CD.

3. Type the following command to start the installation:

   ```
   sh install.sh
   ```

   The Main Menu appears.

4. Type 1 to install CM (SIPCM or H323CM).

Installing SNMP, Apache, and Common

5. The Launcher proceeds to install SNMP. For more information, see Installing SNMP (Solaris), page 239.

6. The Launcher proceeds to install Apache. For more information, see Installing Apache (Solaris), page 240.

   During the installation, when you are asked if you want to add Oracle support to PHP, type n for no.

7. The Launcher proceeds to install Common. For more information, see Installing Common (Solaris), page 241.

   During the installation, when you are prompted to register Common with EMPS, select y.

   When the installation of Common is complete, the following appears:

   ```
   Installation of Voice Platform Common, version 7.6.xxx.xx completed
   successfully.
   ```

   After Common has installed successfully, the Launcher prompts you to install Voice Platform Resource Manager.

Installing Resource Manager

8. The Launcher prompts you for the installation directory:

   ```
   Please confirm that it is acceptable to use /opt/genesys/gvp/cn
   directory as destination directory.
   ```

   ```
   Do you wish to continue (y/n)?
   ```

   Type y to accept the selection, and then press Enter.

   To set a different destination directory, type n and press Enter. The Launcher prompts you for a new destination directory. Type the installation path, and then press Enter.

9. The Launcher prompts you for the Provisioning server name:

   ```
   Press ENTER to confirm
   ```

   "your_server_hostname.your_server_domain" as the Provisioning Server or enter a new one =>

   Press Enter to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press Enter.

10. The Launcher prompts you for the Provisioning user name:

    ```
    Press ENTER to confirm "admin" as the Provisioning User or enter a
    new one =>
    ```

11. Press `Enter`.The Launcher prompts you to provide a password for Provisioning:

    ```
    Please enter Provisioning password =>
    ```

    Type the Provisioning Password, and then press `Enter`.

    When the Launcher completes the Resource Manager installation, it prompts you to install the Session Manager (either SIP Session Manager or H.323 Session Manager, depending on the source of your installation software (see Step 2 on page 265).

Installing the Session Manager (SIP or H.323)

12. The Launcher prompts you for the installation directory:

    ```
    Please confirm that it is acceptable to use /opt/genesys/gvp/cn
    directory as destination directory.
    ```

    ```
    Do you wish to continue (y/n)?
    ```

    Type `y` to accept the selection, and then press `Enter`.

    To set a different destination directory, type `n` and press `Enter`. The Launcher prompts you for a new destination directory. Type the installation path, and then press `Enter`.

13. The Launcher prompts you for the Provisioning server name:

    ```
    Press ENTER to confirm
    ```

    `"your_server_hostname.your_server_domain" as the Provisioning` Server or enter a new one =>

    Press `Enter` to accept the selection. To set a different Provisioning server name, type the Provisioning server name with domain, and then press `Enter`.

14. The Launcher prompts you for the Provisioning user name:

    ```
    Press ENTER to confirm "admin" as the Provisioning User or enter a
    new one =>
    ```

    Press `Enter`.

15. The Launcher prompts you to provide a password for Provisioning:

    ```
    Please enter Provisioning password =>
    ```

    Type the Provisioning Password, and then press `Enter`.

    When the IPCM installation is complete, the `Main Menu` appears.

16. Type `3` to exit the Launcher.

End of procedure

Next Steps

- Configure the IPCM server in EMPS. For more information, see Chapter 23 on page 403.

Installing MIBs on Solaris

This section describes how to install the Management Information Base (MIB) files for GVP.

The MIBs component contains the `.mib` files that enable an SNMP Manager (for example, HP OpenView) to provide a user-friendly display of the SNMP traps generated by GVP. Do not install the MIBs component on any of the GVP hosts.

Procedure:
Installing MIB files (Solaris)

Start of procedure

1. From the Genesys Voice Platform CD, copy the contents of the `solution_specific/solaris/MIBS` directory to the directory on the SNMP Manager where all the `.mib` files are stored.
2. If there is a `.tar` file, extract the files using `tar xvf <MIBs IP file>`.

> Note: There is no loading sequence for the MIB files if you are copying all of the MIB files into the third-party SNMP Manager.
>
> If you are loading only one or just a few of the GVP MIB files, you must first load the `CallNet.mib` and `CallNetTrap.mib` files.

3. After you copy the MIB files to your SNMP Manager, your Manager may require additional steps, such as compiling the MIBs. Genesys recommends that you check the instructions for your SNMP Manager to see if any additional steps are required.

End of procedure

Locating Components After Installation

All UNIX IPs include an `ip_description.xml` file that is copied into the target directory or, in cases where several IPs share a common parent target, into a subdirectory of the target directory.

For each IP, the `ip_description.xml` file lists the unique IP nickname for the particular component. To locate a particular IP, execute the `grep` command to search for the `ip_description.xml` file in combination with the IP nickname.

Locating Dispenser

You may need to find the physical location of Dispenser, in order to verify whether it is installed or uninstalled, or to debug problems with posting `XML` files to Dispenser.

The Dispenser is installed in the same path as the Common component on the GVP host. To search for Dispenser, execute the following command:

```
grep VoPlDispenser ip_description.xml
```

To verify whether Dispenser has been uninstalled, use the following procedure.

Procedure:
Verifying Dispenser installation or uninstallation on Solaris

Purpose: To verify whether Dispenser is installed or uninstalled.

Start of procedure

1. Navigate to the installation directory, and verify whether the Dispenser IP exists.

   To find the installation path, use the following command:

   ```
   grep VoPlDispenser ip_description.xml
   ```

2. To verify that Dispenser has been fully uninstalled if the IP has been deleted, search for the following file:

   ```
   <CN_ROOT>\web\dispenser\spd_manager.php
   ```

   The `spd_manager.php` file is deleted during uninstallation.

End of procedure

Chapter

15 Post-Installation Activities on Solaris Hosts

For Genesys Voice Platform (GVP) deployments that include Element Management System (EMS) Reporting or Outbound Notification (OBN) Manager, this chapter describes post-installation activities that you must perform on the Element Management Provisioning System (EMPS) server before you install other GVP components, and on the EMS Reporting and OBN Manager server(s) before you can configure them in the EMPS. This chapter also provides information about starting and stopping GVP in all deployments.

This chapter contains the following sections:

Creating the Oracle Databases

This section describes how to set up the databases for the following components:

- EMPS
- EventC
- Login Server (Unified Login)
- Network Monitor
- OBN Manager

The instructions in this section are advanced database procedures. Genesys strongly recommends that your database administrator perform these steps or assist you in performing these steps.

Note: You must create the EMPS database before you install other GVP components.

Before You Begin

Ensure that the Oracle Server and Clients have been prepared, as described in Table 31, "Preparing the Oracle Server and Clients," on page 232.

The database creation scripts are unpacked during installation of the components.

Setting Up the Databases

This section provides the following procedures to set up the database schemas:

- Starting SQL Plus on the Oracle Client (Solaris)
- Setting up the EMPS database in Oracle (Solaris)., page 273
- Setting up the EMS Reporting databases in Oracle (Solaris), page 275
- Setting up the OBN Manager database in Oracle (Solaris), page 276

Procedure:
Starting SQL Plus on the Oracle Client (Solaris)

Purpose: To start the SQL Plus utility to connect from the Oracle Client to the Oracle server.

Start of procedure

1. Telnet into the Oracle Client (for example, the EMPS system).

   Warning! Do not use `Exceed`. If you do, only some of the queries copy successfully into `SQL Plus`.

2. Log in as `root` or get root permissions.
3. Type `cd $ORACLE_HOME/bin`, or type the path to where the Oracle Client is installed.
4. Type `sqlplus`.

5. Type `<system-username>/ <system-password>@<first line entry in /usr/<Oracle installation folder>/network/admin/tnsnames.ora>`

   For example, `username=system/manager@perf1.us.int.genesyslab.com`

End of procedure

Procedure:
Setting up the EMPS database in Oracle (Solaris).

Start of procedure

1. Telnet into the EMPS system, and log in to SQL Plus (see Starting SQL Plus on the Oracle Client (Solaris), page 272).
2. Create a tablespace `vwps`.

   > Note: This step must be performed by your Oracle database administrator.

   The command to create the tablespace looks similar to the following:

   ```
   CREATE TABLESPACE vwps DATAFILE '$ORACLE_HOME/oradata/vwps/' SIZE
   5M;
   ```

3. Create user `vwps` with password `vwps` by running the following query:

   ```
   CREATE USER VWPS IDENTIFIED BY VALUES DEFAULT

   TABLESPACE VWPS TEMPORARY TABLESPACE TEMP PROFILE DEFAULT ACCOUNT
   UNLOCK;

   GRANT CONNECT TO VWPS;

   GRANT RESOURCE TO VWPS;

   ALTER USER VWPS DEFAULT ROLE ALL;

   GRANT UNLIMITED TABLESPACE TO VWPS;
   ```

   > Note: Enter the query as one continuous entry.

4. Connect as `vwps` in SQL Plus:

   ```
   CONNECT  vwps/vwps@<value supplied by your database administrator>
   ```

5. Run all queries in the bundled script `<gvp installation folder>/config/database/EMPS_DB_NEW_76_Oracle.sql`, to create the following tables:
   - `APPLICATIONS`
   - `CUSTOMERS`
   - `RESELLERS`
   - `DIDGROUPS`
   - `DIDS`

- `GROUPS`
- `SERVERS`

6. Execute the `INSERT` statement to create a default Direct Inward Dialing (DID) Group entry in the DID `Groups` table. This statement begins with `INSERT` and ends with a semicolon.
7. Set permissions for the `Oracle` folder:
   a. Go to the folder where the Oracle client is installed. For example, `/usr/oracle10g`.
   b. From the `ORACLE_HOME` directory, execute the following command for all folders and subfolders:

   ```
   chmod -R 777*
   ```

   For example:

   ```
   dev-sun-vwm9# pwd
   /usr/oracle10g
   dev-sun-vwm9# chmod -R 777
   ```
8. Set permissions for the `log` folder.
   a. Navigate to `<GVP installation location>/web/spm`. For example, `/opt/genesys/gvp/cn/web/spm`.
   b. In this folder, set all permissions for root as well as any users, by executing the following:

   ```
   chmod 777 log
   ```

   For example:

   ```
   dev-sun-vwm9# pwd
   /opt/genesys/gvp/cn/web/spm
   dev-sun-vwm9# chmod 777 log
   ```

Note: To enable EMPS Reports to be viewed on Solaris, provide `rwx` permissions on the `/opt/genesys/gvp/cn/web/spm/log` directory.

9. Set permissions for the `temp` folder.
   a. Navigate to `<GVP installation location>/temp` (for example, `/opt/genesys/gvp/cn/temp`).
   b. In this folder, set all permissions for root as well as any users, by executing the following:

   ```
   chmod 777 temp
   ```

   For example:

   ```
   dev-sun-vwm9# pwd
   /opt/genesys/gvp/cn
   dev-sun-vwm9# chmod 777 temp
   ```

End of procedure

Procedure: Setting up the EMS Reporting databases in Oracle (Solaris)

Purpose: To create the required users and database schemas for the EMS Reporting databases.

The Oracle scripts are located in the following directories:

- For EMS Reporting: `<CN Dir>/sqlscripts/oracle/EventC/7.6.0`
- For Login Server: `<CN Dir>/sqlscripts/oracle/UnifiedLogin/7.6.0`
- For Network Monitor: `<CN Dir>/sqlscripts/oracle/7.6.0`

Prerequisites

- The required tablespaces have been created (see Table 31 on page 232).

Start of procedure

1. Create the EMS Reporting users:
   a. Change the directory to `<CN Dir>/sqlscripts/oracle/EventC/7.6.0/`.
   b. Log in to SQL Plus, and connect as `system user`.
   c. Run the script `create_all_users.sql`.
2. Change the directory to `<CN Dir>/sqlscripts/oracle/UnifiedLogin/7.6.0`.
3. Execute the script `vwps_grant.sql` as the system user. This will be used later to grant permission to the Unified Login for the parent NSP customer.
4. Change the directory to `<CN Dir>/sqlscripts/oracle/EventC/7.6.0/`.
5. Create the `collector` database:
   a. Log in to SQL Plus and connect as `collector/collector`.
   b. Run the script `collector_from_scratch_7_6_0.sql`.
6. Create the `peaks` database:
   a. Log in to SQL Plus and connect as `peaks/peaks`.
   b. Run the script `peaks_from_scratch_7_6_0.sql`.
7. Create the `reporter` database:
   a. Log in to SQL Plus and connect as `reporter/reporter`.
   b. Run the script `reporter_from_scratch_7_6_0.sql`.
8. Create the `repdwh` database:
   a. Log in to SQL Plus and connect as `repdwh/repdwh`.
   b. Run the script `repdwh_from_scratch_7_6_0.sql`.
9. Exit SQL Plus

10. Create the `unifiedlogin` database:
    a. Change the directory to `<CN Dir>/sqlscripts/oracle/UnifiedLogin/7.6.0/`.
    b. Log in to SQL Plus, and connect as `unifiedlogin/unifiedlogin`.
    c. Run the following scripts in the order listed:
       - `unifiedlogin_from_scratch_7_6_0.sql`
       - `setadminuser.sql`
11. Exit SQL Plus
12. Create the `netmon` database:
    a. Change the directory to `<CN Dir>/sqlscripts/oracle/7.6.0/`.
    b. Log in to SQL Plus and connect as `netmon/netmon`.
    c. Run the following script:
       `netmon_from_scratch_7_6_0.sql`

End of procedure

Procedure: Setting up the OBN Manager database in Oracle (Solaris)

Purpose: To create the `obnmanager` database.

The Oracle scripts for OBN Manager are located in the following directory:

`<CN Dir>/config/database/oracle`

Prerequisites

- The `obnManager` tablespace and the `obnManager` user have been created (see Table 31 on page 232).

Start of procedure

1. Change the directory to `<CN Dir>/config/database/oracle`.
2. Log in to SQL Plus, and connect as the `obnManager` user.
3. Execute the following scripts:
   - `OBN_DB_NEW_760_oracle.sql`
   - `OBN_DB_NEW_OBN_PKG_760_oracle.sql`
   - `OBN_DB_NEW_OBN_PKG_BODY_760_oracle.sql`

End of procedure

Setting File Access Permissions

This section provides information about the file access privileges you must provide on the EMPS and EMS Reporting hosts.

PHP Settings

For PHP functionality, EventC, Reporter, and EMPS require you to assign read and execute permissions to the `nobody` account for the following folders:

- `$ORACLE_HOME`
- Subdirectories of `$ORACLE_HOME`

Permissions for EMS Reporting

EventC, Reporter, and Network Monitor require you to grant read, write, and execute permissions to the owner, group, and others for certain folders.

The following procedure provide details about how to provide the required permissions.

Procedure:
Setting file access permissions for EMS Reporting (Solaris)

Purpose: To grant read, write, and execute permissions for the EventC, Reporter, and Network Monitor users.

Start of procedure

1. Set file access permissions for EventC:

   a. Change the directory to `<Cn Directory>`.

   For example, execute the following command:

   ```
   cd /opt/genesys/gvp/cn
   ```

   b. Grant read, write, and execute permissions to the owner, group, and others for the `log, php,` and `data` directories.

   For example, execute the following command:

   ```
   chmod -R 777 php log data
   ```

   c. Within the `<Cn Directory>` directory, create a link that points to `<Apache Directory>`. The Apache directory is typically `/opt/genesys/gvp/apache`.

   For example, execute the following command:

   ```
   ln -s <Apache Dir> apdir
   ```

2. Set file access permissions for Reporter:
   a. Grant read, write, and execute permissions to the owner, group, and others for the `<Cn Directory>/extweb/reporter/download` directory.
   b. Grant read, write, and execute permissions to the owner, group, and others for the `<Cn Directory>/php` directory.

      For example, execute the following commands:

      ```
      chmod -R 777 <Cn Directory>/extweb/reporter/download
      chmod -R 777 <Cn Directory>/php
      ```
   c. In the `<Cn Directory>`, create a link to the `<Apache Directory>`.

      For example, execute the following command:

      ```
      In -s <Apache Dir> apdir
      ```
3. Set file access permissions for Network Monitor:
   a. Grant `read, write,` and `execute` permissions to owner, group, and others for `<Cn Directory>/php/*.`

      For example, execute the following command:

      ```
      chmod -R 777 <Cn Directory>/php
      ```
   b. In the `<Cn Directory>`, create a link to the `<Apache Directory>`.

      For example, execute the following command:

      ```
      In -s <Apache Dir> apdir
      ```
4. Make sure that the 32-bit Oracle 9i R2 or 10g client libraries are available through `LD_LIBRARY_PATH` in the environment you are using.
5. Restart the Apache and WatchDog services by typing:

   ```
   /etc/init.d/gvpapache start
   /etc/init.d/gvp restart
   ```

   Note: Do not start WatchDog from the `log, temp,` or `data` directory under CN. Always start WatchDog from `bin` or any other folder.

6. Open the EMPS GUI. The menu tree now displays the `EventC` node.
7. View the Network Monitor from the following URL:

   ```
   http://<Server Name>.<Domain Name>:9811/
   ```

End of procedure

Enabling Unified Login

Table 34 summarizes the steps that are required to configure Unified Login for your GVP deployment.

Table 34: Enabling Unified Login for Solaris

Objective	Related Procedures and Actions
1. Install and configure Login Server.	**1.** Install the Login Server component (see Installing EMS Reporting (Solaris), page 255). **2.** Create the `unifiedlogin` database (as well as other required databases, such as `vwps`). For more information, see Setting up the EMS Reporting databases in Oracle (Solaris), page 275. **3.** Verify or modify the Login Server configuration in the EMPS. For more information, see Configuring Login Server in the EMPS, page 320.
2. For a multi-tenant deployment, provision the Administrative Customer (Admin Customer or NSP Customer).	See Setting the Admin Customer for Unified Login, page 324.
3. Update the Admin Customer data in the `unifiedlogin` database.	See Updating the Customer ID in the Login Server database (Solaris), page 279.
4. Modify the Unified Login URL to configure the Login Administration service for Reporter and Call Status Monitor.	See Modifying the Unified Login URL for additional services (Solaris), page 281.

The following procedures support the deployment of Unified Login in your Solaris installation.

Procedure: Updating the Customer ID in the Login Server database (Solaris)

Purpose: To update the Admin Customer (NSP customer) information in the `unifiedlogin` database.

You must update the `UL_USERS` table in the `unifiedlogin` database every time you modify provisioning for the Admin Customer in the EMPS.

Prerequisites

- If the EMPS and Unified Login databases are on the same server, ensure that the `unifiedlogin` user has select privileges to tables in the `vwps` schema. If necessary, log in to SQL Plus, and execute the following script to grant the required privileges to the `unifiedlogin` user:

```
<CN Dir>/CN/sqlscripts/oracle/UnifiedLogin/7.6.0/vwps_grant.sql
```

- If the EMPS and Unified Login databases are on different servers, obtain the Admin Customer's Customer ID from the EMPS (see Setting the Admin Customer for Unified Login, page 324).

Start of procedure

1. Open an SQL Plus session, and connect to the database server as the `unifiedlogin` user.

   If the EMPS and Unified Login databases are on the same server, go to Step 2.

   If the EMPS and Unified Login databases are on different servers, go to Step 3.

2. If the EMPS and Unified Login databases are on the same server:

   a. Enter the following command to execute the `setadminuser` stored procedure:

      ```
      exec unifiedlogin.setadminuser('vwps');
      ```

      If your deployment uses different schema names, replace `unifiedlogin` with the name of your Unified Login schema, and replace `vwps` with the provisioning schema name.

   b. Execute the following command to save the changes:

      ```
      commit;
      ```

3. If the EMPS and Unified Login databases are on different servers, enter the following SQL Plus command to update the `UL_USERS` table in the `unifiedlogin` database:

   ```
   update ul_users set customer_id=<ADMIN_CUST_ID> where k_users=1;
   ```

   where `<ADMIN_CUST_ID>` is the Customer ID for the Admin Customer that you provisioned in the EMPS.

   The default `k_users` value for the administrator is `1`.

4. Make sure that the 32-bit Oracle 9iR2 or 10g client libraries are available through `LD_LIBRARY_PATH` in the environment you are using.

5. Check the GUI:

   a. Access the Unified Login home page at `http://<fully qualified server name>/unifiedlogin`.

   b. Log in as Administrator:

      - `Login Name` = `Administrator`
      - `Customer Name` = `<name of the NSP Customer>`
      - `Password` = `<password>`

Notes: Customer Name is required when GVP runs in multi-tenant mode.

The password that is set by the Unified Login database scripts is `administrator`.

End of procedure

Procedure: Modifying the Unified Login URL for additional services (Solaris)

Purpose: To configure the Reporter and Call Status Monitor to use the Login Administration service.

Prerequisites

- Make sure that the 32-bit Oracle 9iR2 or 10g client libraries are available through `LD_LIBRARY_PATH` in your environment.
- Type the following commands to restart the Apache and WatchDog services on the EMS Reporting host:

```
/etc/init.d/gvpapache start
/etc/init.d/gvp start
```

Start of procedure

1. Log in to the Unified Login at `http://server.domain/unifiedlogin`.
   - `Login Name` = `Administrator`
   - `Customer Name` = `<name of the NSP Customer>`
   - `Password` = `<password>`

Notes: Customer Name is required when GVP runs in multi-tenant mode.

The password that is set by the Unified Login database scripts is `administrator`.

2. Click `Login Administration`.
3. Click `Modify Service`.
4. From the drop-down list, select `RPT1-Network Reports`, and then click `Search`.
5. Modify the `URL` field as follows:

```
http://<reporter server name>/reporter/login.php
```

6. If the Reporter is on a VPN in addition to being on the public network, then enter the VPN URL in the `VPN URL` field as follows:

   `http://<reporter server name or IP addr on VPN>/reporter/login.php`

7. Click `Save`.

8. Repeat Steps 4 through 7 to add Call Status Monitor, using the following information:

   a. Search for `CSM1-Network Call Status Monitor`.

   b. Specify the following URL:
   `http://<call status monitor server name>/callstatusmonitor/login.php`

   c. Specify the following VPN URL:
   `http://<call status monitor server name or IP addr on VPN>/callstatusmonitor/login.php`

   d. Click `Save`.

9. Check the GUIs:

   a. Log into the following URL:

   `http://server.domain/unifiedlogin`

   b. Click `Historical Reports`.

End of procedure

Special Setting for Enhanced Media Services

If IPCS is using Intel HMP Enhanced Media Services or Alcatel MRF Enhanced Media Services with SpeechWorks MediaServer 3.1.13 as the Media Resource Control Protocol (MRCP) Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) server, you must set the following parameters in the `OSSserver.cfg` file:

```
# The audio sending rate samples per second
server.realspeak4.rtpSendRate VXIInteger 8000

# The size of rtp packet in sample
server.realspeak4.rtpPacketSamples VXIInteger 160
```

Starting and Stopping GVP on Solaris

Starting or stopping GVP means starting or stopping the WatchDog process on the GVP server.

WatchDog can operate in two modes: normal and safe. For more information about WatchDog and its modes of operation, see “WatchDog” on page 38.

You must start the WatchDog process on the EMPS before you install other GVP components, and you must start the WatchDog process on the other GVP servers after you have installed the components. You must also restart the WatchDog process on a GVP server after you make any configuration changes for that component in the EMPS.

Starting WatchDog

The following procedure describes how to start or restart WatchDog on Solaris hosts.

Procedure: Starting/Restarting GVP (Solaris)

Prerequisites

- The following environment variables have been set:
  - `ORACLE_HOME=<OracleInstallationPath>`
  - `LD_LIBRARY_PATH=$ORACLE_HOME:$LD_LIBRARY_PATH`
- Ensure that the following Oracle client libraries are available through `LD_LIBRARY_PATH` in the EMPS environment that you are using:
  - For Oracle 10g, the 32-bit Oracle 10g Standard Edition client libraries. EMPS needs `libclntsh.so.9.0,` which should be a link pointing to `libclntsh.so.10.1.`
  - For Oracle 9i, the 32-bit Oracle 9i Standard Edition client libraries (specifically, `libclntsh.so.9.0).`

  Without this library, the EMPS process will not start, and the error will be written to the `daemon.log` file.

  To check whether the library files are available after you set the `LD_LIBRARY_PATH,` type the following command from `<GVP Installation Folder>/bin:`

  ```
  ldd SPS | grep libclntsh
  ```

  If the output states not found, correct the `LD_LIBRARY_PATH.`

Start of procedure

1. Start Apache by entering the following command:

   ```
   /etc/init.d/gvpapache start
   ```

2. Start WatchDog by entering one of the following commands:
   - **For Normal mode:**
     ```
     /etc/init.d/gvp start
     ```
   - **For Safe mode:**
     ```
     /etc/init.d/gvp -s
     ```

Note: Do not start WatchDog from the `log`, `temp`, or `data` directory under `CN`. Always start it from `bin` or any other folder.

End of procedure

Stopping WatchDog

The following procedure describes how to stop WatchDog on Solaris hosts.

Procedure: Stopping WatchDog on Solaris Hosts

Start of procedure

1. Change the directory by entering the following command:
   ```
   cd /etc/init.d/
   ```
2. Stop WatchDog by entering the following command
   ```
   gvp stop
   ```

End of procedure

Chapter

16 Uninstalling GVP on Solaris

This chapter describes how to uninstall Genesys Voice Platform (GVP) components in a Solaris deployment. It contains the following sections:

Uninstalling GVP Components

This section describes how to uninstall the GVP components on a Solaris host.

You must uninstall the GVP components one at a time and in the reverse order of installation.

Note: WatchDog does not start unless the GVP components that are installed on a server match the configuration shown in the EMPS. When you uninstall a GVP component from a server that has other GVP components on it, the corresponding node in EMPS is not removed. As a result, WatchDog will not start. Contact Genesys Technical Support for assistance if you plan to continue running the remaining software.

Procedure: Uninstalling GVP components (Solaris)

Start of procedure

1. Login as root or get root permissions.
2. Type `source ~/.cshrc`.
3. Go to the directory that contains the installation software (the installation directory) for each component.
4. Type `sh install.sh -uninstall`.

This removes all of the installed files and folders for the component and modifies the `/etc/cn_info` file to indicate that the component is no longer installed.

End of procedure

Example

To uninstall the GVP components from an IPCS host:

1. Go to the installation directory for TTS and type:
   ```
   sh install.sh -uninstall
   ```
2. Go to the installation directory for IPCS and type:
   ```
   sh install.sh -uninstall
   ```
3. Go to the installation directory for Common and type:
   ```
   sh install.sh -uninstall
   ```
4. Go to the installation directory for Apache and type:
   ```
   sh install.sh -uninstall
   ```
5. Go to the installation directory for SNMP and type:
   ```
   sh install.sh -uninstall
   ```
6. Go to the installation directory for MRP SMP Integrator and type:
   ```
   sh install.sh -uninstall
   ```

Part

4 GVP Configuration

This part of the manual provides details about how to configure Genesys Voice Platform (GVP) components in the Element Management Provisioning System (EMPS).

If you used the GVP Deployment Tool to install GVP in a Windows environment, you do not need to manually configure GVP.

This part contains the following chapters:

- Chapter 17, “Configuring EMPS in the EMPS,” on page 289
- Chapter 18, “Configuring EMS Runtime in the EMPS,” on page 301
- Chapter 19, “Configuring EMS Reporting and OBN Manager in the EMPS,” on page 309
- Chapter 20, “Configuring IPCS in the EMPS,” on page 341
- Chapter 21, “Configuring VCS in the EMPS,” on page 363
- Chapter 22, “Configuring MRCP ASR and TTS in the EMPS,” on page 391
- Chapter 23, “Configuring IP Call Manager in the EMPS,” on page 403
- Chapter 24, “ASR Log Manager System,” on page 421

Chapter

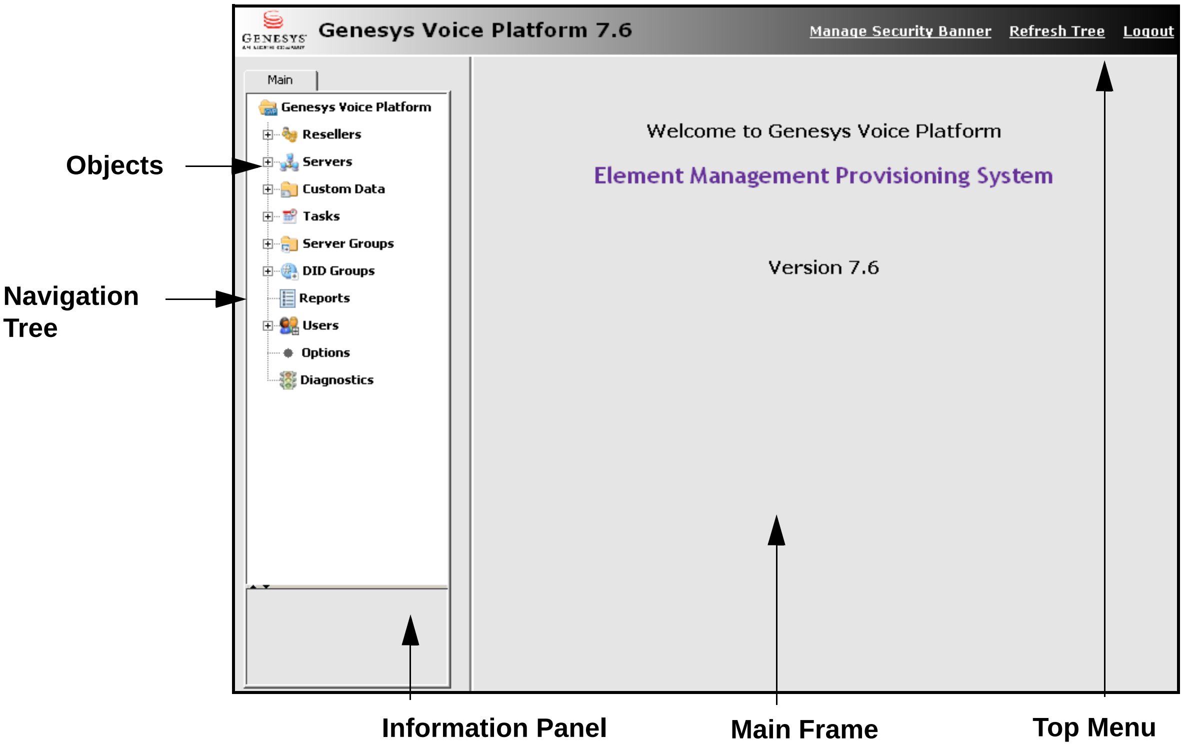
17 Configuring EMPS in the EMPS

This chapter describes how to configure the Genesys Voice Platform (GVP) Element Management Provisioning System (EMPS) component. It contains the following sections:

About the EMPS GUI

The EMPS is a repository for GVP configuration information. It provides a graphical user interface (GUI) for configuring GVP components.

Figure 44 shows the layout of the EMPS GUI.



Welcome to Genesys Voice Platform

Element Management Provisioning System

Version 7.6

Figure 44: EMPS Welcome Page

Click objects in the navigation tree to expand them so that you can view or edit the properties of their child nodes. The property pages for the selected node display in the main frame. The property pages for the root servers in the `Servers` hierarchy are read-only.

The property pages (tabs) that display for each node depend on the component.

System Tab All components have a `System` property tab, which displays read-only system attributes such as Template Link and Server Version.

Additional Tab If you configure additional attributes that are not included as part of the standard template, the attributes appear on a tab called `Additional`. An icon appears next to the attribute to flag it as non-standard. The text that identifies the attribute is configurable.

Help Context-sensitive (tooltip) help is available for all attributes on the properties tabs. To display the tooltip help, clear the `Disable Help` check box at the bottom of the property page (or select it to hide the help).

For more information about using the EMPS GUI, see the chapter about the Element Management Provisioning System in the *Genesys Voice Platform 7.6 Reference Manual.*

Configuring EMPS

This section includes the following procedures to configure the EMPS server:

- Configuring the EMPS server in the EMPS
- Verifying system connectivity, page 299

Procedure: Configuring the EMPS server in the EMPS

Purpose: To configure the Element Management Provisioning System (EMPS) on both Solaris and Windows hosts.

Prerequisites

- The required permissions have been set, and the EMPS database has been set up. For more information, see: “Creating the Microsoft SQL Server Databases” on page 181 or “Creating the Oracle Databases” on page 271.
- For Windows deployments, the EMPS URL (`http://<EMPS-hostname>:9810`) has been added as a Trusted Site in Internet Explorer, on the `Tools > Internet Options > Security` tab.

Start of procedure

1. In a web browser, access the `EMPS Login` page in one of the following ways:
   - Through the Element Management System (EMS) GUI:
     - **i.** Enter the following URL:

       `http://<EMPS-hostname>:9810`

       The EMS GUI opens.
     - **ii.** In the left pane of the EMS GUI, click `EMPS`. The login page for the EMPS opens.
   - Directly, by entering the following URL:

     `http://<EMPS-hostname>:9810/spm`
2. On the `EMPS Login` page, log in with the following credentials:

   User Name: `Admin`

   Password: `password`
3. In the EMPS navigation tree, expand the `Servers` > `EMPS > <host-name>` nodes.
4. Right-click the `SPS` node, and then select `Edit`.
5. On each tab, enter or verify the values for the parameters listed in Table 35.

Note: The values that you enter might not match the example values shown in Table 35.

Table 35: EMPS Parameters

Tab	Parameter	Description	Example Value
Data Store	Datastore Type	Specifies the DataSource that the EMPS uses for storing provisioning information.	`OpenLDAP (bundled)`
	LDAP Port	Specifies the port used to communicate with Lightweight Directory Access Protocol (LDAP).	`389`
	LDAP Root	Specifies the root node of the datastore (OpenLDAP or SunOne).	`o=genesys`
	LDAP Password	Specifies the LDAP server account (the account specified for the LDAP user) password used for connecting to LDAP.	For OpenLDAP: `admin123` For SunOne: Use the password created for the `cn=Directory Manager` account.

	LDAP User	Specifies the LDAP server user name to be used for connecting to LDAP.	For OpenLDAP:
			`cn=Manager`
			For SunOne:
			`cn=Directory Manager`

	LDAP Machine	Specifies the fully qualified domain name (FQDN) of the machine on which the LDAP is installed.	`emps.yourcompany.com`

Table 35: EMPS Parameters (Continued)

Tab	Parameter	Description	Example Value
EMPS	EMPS View	(Mandatory) Specifies the view of the EMPS UI. Options are `Standard` or `Advanced.` If you select `Standard,` the custom data UI is not available. To enable advanced operations, select `Advanced,` and then click `Save.` In order for this to take effect, you must notify the EMPS server, log out of the EMPS, and then log back in.	`Standard`
	HTTP Safe AppXML Folders	(Optional) If you select this check box, the EMPS generates AppXML in URLScan safe folders. For example, the EMPS generates AppXML 2.0 in a `0200` folder (note that the name does not contain a period) in addition to the `2.0` folder.	Selected
	EMPS Operating Mode	Specifies the EMPS operating mode.	`Standalone (No Genesys Framework)`
System	GVP Options Flag	Enables the options functionality in EMPS.	Selected

Table 35: EMPS Parameters (Continued)

Tab	Parameter	Description	Example Value
Dispenser	HTTP Port to use	(Optional) Specifies the HTTP port that the EMPS uses to communicate with other servers.	`9810`

	Local XML Files Folder	(Mandatory) Specifies the local folder in which the EMPS generates `.xml` files.
		Note: The value for this parameter is set atinstallation (the default value is `<CN_INSTALL_PATH>/web/did_url_mappings`). You can change the parameter value if you want to generate the files in a different location. After Server Notification or Server Restart, the `.xml` files will be generated in the new location. The new path is preserved if you reinstall EMPS. However, be aware that any `App.xml` files that were generated before you changed the default `Local XML Files Folder` path are not carried over to the new location. You must regenerate old `App.xml` files in the new location.
			Solaris:
			`/opt/genesys/gvp/cn/web/did_url_mappings/`
			Windows:
			`c:\gvp\cn\web\did_url_mappings\`

DBBridge **Note:** This tab is visible only if you installed EMS Reporting.	Database Password	Specifies the database server account password for the account specified in `Database Username`. **Note**: If no password was set up on the database, leave this field empty	`<password>`

Table 35: EMPS Parameters (Continued)

Tab	Parameter	Description	Example Value
DBBridge (continued)	Populate Adjunct Database	Specifies whether the EMPS replicates specific data from the Directory Server to the EMPS database. EMS Reporting and the Events subsystem use this data. To enable this feature, select this check box. **Note:** If you clear this check box, data will not be replicated, and Reporter will not work correctly.	Selected
	Servers IP Lookup	Specifies whether IP addresses are looked up from the Domain Name System (DNS) for servers that are registered with the EMPS. This is needed for Reporter. **Note:** If several servers in the EMPS do not have a DNS entry, selecting this check box might cause the EMPS to intermittently freeze.	Selected
	DB Initial Catalog (Database) **Note:** Windows-based EMPS only	Specifies the name of the database or SID (Oracle) that is used for storing information. This database should exist in the indicated database server machine. You can also enter the value of the database machine name.	`emps`
	Update Frequency in seconds	Specifies the frequency (in seconds) with which data is copied to the `emps` database from the Directory Server. Range: `60`–`10800` seconds. Default: `600` seconds.	`600`

Table 35: EMPS Parameters (Continued)

Tab	Parameter	Description	Example Value
DBBridge (continued)	Purge Interval (days)	Specifies the number of days after which the EMPS deletes from the adjunct database, entries that have been deleted from the Directory Server. When entries are deleted from the Directory Server, they are kept in the adjunct database for reporting and billing purposes. If you enter a value of 0, entries are deleted immediately. Valid values: 0–750 days. Default value: 45 days.	45
	Database Machine Name	Specifies the fully qualified domain name (FQDN) of the machine where the database is located.	emsreporting.yourcompany.com
	Database Username	Specifies the database server user name to be used for connecting to the database. This is the database user name that you specify when you create the database schema (see “Setting Up the Databases” on page 182 or Setting up the EMPS database in Oracle (Solaris)., page 273).	emps
Cache	Purge Cache	Specifies whether the EMPS purges older cached .xml files from CacheServers defined in the EMPS. To enable this feature, select this check box. **Note:** The EMPS currently supports only BlueCoat cache boxes.	Cleared

Table 35: EMPS Parameters (Continued)

Tab	Parameter	Description	Example Value
Tasks	System Account Password	(Optional) Specifies the password for the EMPS system account. This account is used only for scheduled tasks. **Note:** This is the password that you added in Creating a root node in SunOne Directory Server 5.2 (Windows), page 91 (for Windows) or Creating a root node in SunOne Directory Server 5.1 SP4 (Solaris), page 227 (for Solaris).	<password>
	Enable Scheduled Tasks	(Mandatory) Enables and disables scheduled tasks. If you select this check box, scheduled tasks will be executed. If you clear this check box, you can still create and save scheduled tasks, but they will not be executed.	Selected
	Scheduled Tasks Interval	(Optional) Specifies the frequency (in seconds) with which the EMPS checks for pending scheduled tasks and executes them. Valid values: `180·10800` (seconds). Default value: `180`.	`180`

Table 35: EMPS Parameters (Continued)

Tab	Parameter	Description	Example Value
Logging	Log Levels	(Optional) Specifies the level of detail when debugging information is written to process log files.	`*:0x03`
	Log File Size	Specifies the size of the log file in bytes.	`262144`
CTI	Default to CTI Simulator	If checked, the EMPS will point the QAdapter URLs in the `ivrprofile` xml file to the CTI Simulator. This occurs only if the IVR Profile does not use IVR Server Client or Cisco CTI. **Note:** This parameter is for GVP: DE only and does not have to be set manually, it will be enabled automatically during installation of the CTISimulator.	

6. Click `Save`.

   For Windows installations, continue at Step 7.

   For Solaris installations, continue at Step 8.

7. To complete EMPS configuration on Windows:

   a. Start or restart the EMPS WatchDog (see Starting/Restarting GVP in Normal mode (Windows), page 198).

   b. Navigate to the `<EMPS Installation drive>:\CN\Config` folder, and verify that the `gvp.ini.tds` file is not present.

   If it is present, there is a problem with the new information. Use `watchdog.log` to start debugging.

8. To complete EMPS configuration on Solaris:

   a. Start or restart the EMPS WatchDog by entering the following commands:

```
/etc/init.d/gvp stop
/etc/init.d/gvp start
```

Note: Do not start WatchDog from the `log`, `temp`, or `data` directory under `CN`. Always start it from `bin` or any other folder.

b. Restart Apache on the EMPS host, by entering the following command:

```
/etc/init.d/gvpapache start
```

c. Restart SNMP on the EMPS host, but entering the following command:

```
/etc/init.d/gvpsnmp start
```

When WatchDog restarts, the EMPS configuration is complete.

End of procedure

Next Steps

- Verify connectivity (see Verifying system connectivity).

Procedure: Verifying system connectivity

Start of procedure

1. In a web browser, access the EMPS login page by entering the URL `http://<EMPS-hostname>:9810/spm.`
2. Log in to the EMPS as `Admin,` and enter your password.
3. In the EMPS navigation tree, click `Diagnostics.`

   The `Diagnostics` property page opens, and displays the results of the following tests:

   - EMPS Server connectivity
   - Directory Server connectivity
   - Database Server connectivity

   A check mark in a green circle indicates successful connectivity. Do not proceed with additional GVP configuration if you do not receive a successful result.

End of procedure

Next Steps

- **For Solaris:**

  Install additional components. For more information, see Chapter 14 on page 235.

- **For Windows (GVP installed with the GVP Deployment Tool):**
  - If your deployment includes EventC, Login Server, Reporter, Call Status Monitor, Network Monitor, or OBN Manager, create the required databases (see “Creating the Microsoft SQL Server Databases” on page 181).
  - To modify configuration parameters in the EMPS, configure the following as required:
    - EMS Reporting servers (see Chapter 19 on page 309)
    - IP Communication Server (IPCS) (see Chapter 20 on page 341)
    - Voice Communication Server (VCS) (see Chapter 21 on page 363)
- **For Windows (manual installation)**
  - Install additional components. For more information, see “Manual Installation on Windows” on page 505.

Chapter

18 Configuring EMS Runtime in the EMPS

This chapter describes how to configure the IVR Server and Media Resource Platform (MRP) System Management Protocol (SMP) Integrator components on the Element Management System (EMS) Runtime host.

This chapter contains the following sections:

Note: The other EMS Runtime components (IVR Server Client, Policy Manager, Bandwidth Manager, and Cisco Queue Adapter [CQA]) do not require server configuration.

Configuring IVR Server

This section describes how to create and configure the Interactive Voice Response (IVR) Server for both Solaris and Windows hosts.

Procedure: Creating IVR Server in the EMPS

Purpose: To create the IVR Server object in the EMPS, because the IVR Server Client must have an IVR Server with which to communicate.

Prerequisites

- The EMPS database has been created, and the EMPS server has been configured in the EMPS. For more information, see “Creating the Microsoft SQL Server Databases” on page 181 or Setting up the EMPS database in Oracle (Solaris)., page 273, and “Configuring EMPS” on page 291.

Start of procedure

1. In a web browser, access the EMPS login page by entering the URL `http://<EMPS-hostname>:9810/spm`.
2. Log in to the EMPS as `Admin`, and enter your password.
3. In the EMPS navigation tree, expand the `Servers` > `ISVR` nodes.
4. Right-click the `IServer_Sample` node, and then select `Create a Copy`.

   The `Server Configuration` property page appears.
5. Click `Copy`.
6. In the `To Node` text box, enter a new IVR Server node name, and then click `Copy`.

   A confirmation dialog box appears.
7. Click `OK`.

End of procedure

Next Steps

- Configure the IVR Server (see Configuring IVR Server).

Procedure:
Configuring IVR Server

Start of procedure

1. In the EMPS navigation tree, expand the `Servers > ISVR > <newly created node>` nodes.
2. Right-click `IServerInfo`, and then select `Edit`.
3. On the `General` tab, verify or enter the values for the parameters listed in Table 36.

Table 36: IVR Server Parameters

Tab	Parameter	Description	Example Value
General	KeepAlive Response Timeout	Specifies the amount of time, in seconds, that the IVR Server Client waits for the KeepAlive Response from the IVR Server. Valid values: 2–5 (seconds) Default value: 3	3
	IServer Host IP Address	Specifies the IP address of the IVR Server. The value that you enter must match the IP address that is configured in the gli-server-address option in the Genesys Configuration Layer—For example, if gli-server-address = 10.10.23.126:7080, you must set IServer Host ip address to 10.10.23.126. The gli-server-address option is located in the gli_server_group_[x] section (typically gli_server_group_1) of the application that represents the virtual TServer. The application resides in the Applications folder under Environment in the Configuration Layer.	10.10.30.90
	IServer Communication Port	Specifies the listening port of the IVR Server. The value that you enter must match the port number that is configured in the gli-server-address option in the Configuration Layer—For example, if gli-server-address = 10.10.23.126:7080, you must set the IServer Communication Port to 7080. The gli-server-address option is located under the gli_server_group_[x] section (typically gli_server_group_1) of the application that represents the virtual TServer. The application resides in the Applications folder under Environment in the Configuration Layer.	9090
Note: For more information about the KeepAlive options for the IVR Server Client, see the *Genesys Voice Platform 7.6 Reference Manual.*			

Table 36: IVR Server Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	CME IVR Client Name	Specifies the name of the IVR object, exactly as it is configured in the Configuration Layer. In a multi-tenant environment, the IVR object is located in the IVRs folder for your tenant; in a single-tenant environment, it is in the Resources folder. This value is case-sensitive and it must exactly match the name of the IVR object.	GVP_IVR
	Enable KeepAlive Request	Check box that enables or disables the KeepAlive Request option from the IVR Server Client to the IVR Server.	Cleared
	Number of KeepAlive Request	Specifies the number of requests that are sent to the IVR Server before it is marked as unavailable. Valid values: 2–5 Default value: 3	3
	KeepAlive Request Interval	Specifies the interval, in seconds, at which the IVR Server Client sends KeepAlive requests to the IVR Server. Valid values: 2–3600 (seconds) Default value: 5	5
Note: For more information about the KeepAlive options for the IVR Server Client, see the *Genesys Voice Platform 7.6 Reference Manual.*			

4. Click Save.
5. Start the EMS WatchDog. Refer to Starting/Restarting GVP in Normal mode (Windows), page 198 or Starting/Restarting GVP (Solaris), page 283 for details.

End of procedure

Configuring MRP SMP Integrator

This section describes how to configure the MRP SMP Integrator (for the Solaris operating system only):

- Configuring SnmpSmpConverter
- Configuring StatHandler, page 306

Procedure: Configuring SnmpSmpConverter

Start of procedure

1. In the EMPS navigation tree, expand the `Servers > SMPInteg > <servername>` node.
2. Right-click `SnmpSmpConverter`, and then select `Edit`.
3. On the `General` and `GM` tabs, verify or enter the values for the parameters listed in Table 37.

Table 37: SnmpSmpConverter Parameters

Tab	Parameter	Description	Example Value
General	Default Alarm Code	Specifies the alarm code that is used if the code is not defined.	`777`
	Trap Severity 0	Specifies the severity mapping for the GVP alarms to the Media Resource Function (MRF) alarms.	`3`
	Trap Severity 1	Specifies the severity mapping for the GVP alarms to the MRF alarms.	`4`
	Trap Severity 2	Specifies the severity mapping for the GVP alarms to the MRF alarms	`5`
	Trap Severity 3	Specifies the severity mapping for the GVP alarms to the MRF alarms	`6`
	Trap Severity 4	Specifies the severity mapping for the GVP alarms to the MRF alarms	`7`
	LM UDP Port	Specifies the Local Manager’s UDP port number.	`20700`
	Ack Timer	Specifies the acknowledge time from the Global Manager.	`60`
	Locate Period	Specifies the keep alive timer between the MRP SMP Integrator components and the Global Manager.	`60`

Table 37: SnmpSmpConverter Parameters (Continued)

Tab	Parameter	Description	Example Value
GM	GM Alarm Port	Specifies the listening port for traps of the Global Manager.	`20710`
	GM Statistics Port	Specifies the listening port for statistics of the Global Manager.	`20730`
	GM Host Name	Specifies the host name of the Global Manager.	`123.456.789.00`

4. Click `Save`.
5. Set the `MIBDIRS` variable to the path where the MIBs are stored. For example, if SNMP is installed in `/opt/genesys/gvp/netsnmp`, the `MIBDIRS` variable must be set to `/opt/genesys/gvp/netsnmp/share/snmp/mibs`.

   Make sure that the MIB files (with the `.txt` extension) for both the IPCM and the IPCS are located in this directory.
6. Start the EMS Runtime WatchDog. Refer to Starting/Restarting GVP (Solaris), page 283 for details.

End of procedure

Next Steps

- Configuring StatHandler

Procedure: Configuring StatHandler

Start of procedure

1. In the EMPS navigation tree, expand the `Servers > SMPInteg> <servername>` node.
2. Right-click `StatHandler,` and then select `Edit.`
3. On the `General` tab, verify or enter the values for the parameters listed in Table 38 on page 307.

Table 38: StatHandler Parameters

Tab	Parameter	Description	Example Value
General	Statistics Polling Timer	Specifies the time interval (in seconds) that the StatHandler process collects the GVP agent statistics and sends them to the MRF.	`1`
	Enable Archive File	Flag that manages the size of the archive files. `0`–disables the archive files. `1`–enables the archive files.	`1`
	Archive File Name	Specifies the name and relative path of the archive file.	`/tmp/stat.arc`
	Local Server Port	Specifies the listening port of the local server.	`7110`
	Local Time Out	Specifies the time out interval (in seconds) of the local server.	`10`
	Counter Mode	Specifies the statistic message type sent by the StatHandler. The value must always be set to 4.	`4`

4. Click `Save`.
5. Start the WatchDog service on the EMS Runtime host. Refer to Starting/Restarting GVP (Solaris), page 283 for details.
6. Change the directory to `<GVP Installation>\cn\`.
7. Grant read, write, and execute permissions to the owner, group, and others on the `config` directory, by executing the following command:

```
chmod -R 777 config
```

End of procedure

Chapter

19 Configuring EMS Reporting and OBN Manager in the EMPS

This chapter describes how to configure the Element Management System (EMS) Reporting and OBN Manager components in the Element Management Provisioning System (EMPS).

This chapter contains the following sections:

Configuring EventC

This section describes how to configure EventC for both Solaris and Windows.

Note: Genesys recommends that you run the EventC Server on the Greenwich Mean Time (GMT) time zone.

This section includes the following procedures:

- Configuring the Events Collector (EventC) in the EMPS
- Disabling Peaks in a multiple EventC setup, page 319

Procedure:
Configuring the Events Collector (EventC) in the EMPS

Summary

To update provisioning for EventC, you must configure parameters for the following nodes:

- EventC (`ConfigEventC`)—see Step 3
- Call Records Generator (`CallRecsGenerator`)—see Step 6 on page 315
- EventC Manager (`EventCManager`)—see Step 9 on page 316
- Events Loader (`EventsLoader`)—see Step 12 on page 317
- Peaks NSP (`PeaksNSP1`)—see Step 15 on page 317

Prerequisites

- The EventC database schema has been created. For more information, see “Creating the Microsoft SQL Server Databases” on page 181 or “Creating the Oracle Databases” on page 271.

Start of procedure

1. In a web browser, access the EMPS login page by entering the URL `http://<EMPS-hostname>:9810/spm/login.php`.
2. Log in to the EMPS as `Admin`, and enter your password.

EventC Parameters

3. On the EMPS navigation tree, expand the nodes `Servers > Events Collector > <ServerName>`, and then right-click `ConfigEventC`.
4. From the shortcut menu, select `Edit`.
5. Verify or enter values for the parameters under each tab listed in Table 39, and then click `Save`.

> Note: Only one Peaks process can run for an EventC setup. In the case where EventC processes run on multiple machines, you must disable Peaks on those machines (see Disabling Peaks in a multiple EventC setup, page 319).

Table 39: ConfigEventC Parameters

Tab	Parameter	Description	Example Value
Options	Type of Database	Specifies the Oracle database server.	For Solaris: `oracle` For Windows: `mssql`
	Load All Events	Specifies whether to load all events, or events relevant to reporting only.	No
	Create call records in billing DB?	Specifies whether to create call records in the billing database (RepDWH).	No
	Create call phase records in billing DB?	Specifies whether to create call phase records in the billing database. (RepDWH).	No
	Peaks Wait Time	Specifies the delay, in hours, before the first peak process starts.	`6`
	Peaks Addl Delay	Specifies, in seconds, an additional delay for subsequent processes.	`30`
	Peak Execution Sequence	Specifies the sequence of peak process execution.	`PeaksNSP`
	Maximum Call Duration (hours)	Specifies the maximum duration, in hours, for a call.	`6`
	Database Cleanup Interval (mins)	Specifies the intervals, in minutes, in which the EventCManager attempts to clean the database.	`60`
	Reset peaks automatically if problems found?	Specifies whether to reset peaks automatically if the peaks accuracy check fails.	Yes
	Port for GVP	Specifies the port on which Genesys Voice Platform interaction occurs.	`9810`

Table 39: ConfigEventC Parameters (Continued)

Tab	Parameter	Description	Example Value

EventFiles	Source Directory	Specifies the path to the current directory.	Solaris:
			`/opt/genesys/gvp/cn/data/current`
			Windows:
			`c:\gvp\cn\data\current`

	Archive Directory	Specifies the path to the archive directory.	Solaris:
			`/opt/genesys/gvp/cn/data/archives`
			Windows:
			`c:\gvp\cn\data\archives`

	Exceptions Directory	Specifies the directory that stores event files containing errors.	Solaris:
			`/opt/genesys/gvp/cn/data/exceptions`
			Windows:
			`c:\gvp\cn\data\exceptions`

CollectorDB	Collector - DB Server Name (Oracle Net Service Name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the Collector database. Usually, this is the combination of the Oracle Service ID and the database service IP.
		Windows—Specifies the fully qualified domain name of the server that has the Collector database.
			Oracle:
			`GENGRP_172.24.129.52`
			MSSQL:
			`172.24.129.52`

	Collector - Database / Schema Name	Specifies the name of the Collector database.	`collector`
	Collector - DB User Name	Specifies the User ID for the Collector database.	`collector`
	Collector - DB Password	Specifies the password for the Collector database.	`collector`

Table 39: ConfigEventC Parameters (Continued)

Tab	Parameter	Description	Example Value

ReporterDB	Reporter - DB Server Name (Oracle Net Service Name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the Reporter database. Usually, this is the combination of the Oracle Service ID and the database service IP.
		Windows—Specifies the fully qualified domain name of the server that has the Reporter database.
			Oracle:
			`GENGRP_172.24.129.52`
			MSSQL:
			`172.24.129.52`

	Reporter - Database / Schema Name	Specifies the name of Reporter database.	`reporter`
	Reporter - DB User Name	Specifies the User ID for the Reporter database.	`reporter`
	Reporter - DB Password	Specifies the password for the Reporter database.	`reporter`

Datawarehouse DB	DataWareHouse - DB Server Name (Oracle Net Service Name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the Data Warehouse database. Usually, this is the combination of the Oracle Service ID and the database service IP.
		Windows—Specifies the fully qualified domain name of the server that has the Data Warehouse database.
			Oracle:
			`GENGRP_172.24.129.52`
			MSSQL:
			`172.24.129.52`

	DataWareHouse - Database / Schema Name	Specifies the name of the Data Warehouse database.	`repdwh`
	DataWareHouse - DB User Name	Specifies the User ID for the Data Warehouse database.	`repdwh`
	DataWareHouse - Password	Specifies the password for the Data Warehouse database.	`repdwh`

Table 39: ConfigEventC Parameters (Continued)

Tab	Parameter	Description	Example Value
ProvisioningDB	EMPS - Server Name (Oracle Net Service name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the EMPS database. Usually, this is the combination of the Oracle Service ID and the database service IP. Windows—Specifies the fully qualified domain name of the server that has the EMPS database.	Oracle: `GENGRP_172.24.129.52` MSSQL: `172.24.129.52`
	EMPS - Database / Schema Name	Specifies the name of the Events EMPS database.	`emps`
	EMPS - DB User Name	Specifies the User ID for the Events EMPS database.	`emps`
	EMPS - Password	Specifies the password for the Events EMPS database.	`emps`
PeaksDB	Peaks - DB Server Name (Oracle Net Service Name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the Peaks database. Usually, this is the combination of the Oracle Service ID and the database service IP. Windows—Specifies the fully qualified domain name of the server that has the Peaks database.	Oracle: `GENGRP_172.24.129.52` MSSQL: `172.24.129.52`
	Peaks - Database / Schema Name	Specifies the name of the Peaks database.	`peaks`
	Peaks - DB User Name	Specifies the User ID for the Peaks database.	`peaks`
	Peaks - Password	Specifies the password for the Peaks database.	`peaks`

Table 39: ConfigEventC Parameters (Continued)

Tab	Parameter	Description	Example Value
Management	Save Event Files For (Days)	Specifies the period, in days, for which event files are archived before being deleted.	7
	Save Raw Events For (Days)	Specifies the period, in days, for which raw events in the Collector are archived before being deleted.	14
	Save Reporter Data For (Days)	Specifies the period, in days, for which data in the Reporter database is archived before being deleted.	365
	Save Billing Data For (Days)	Specifies the period, in days, for which data is archived in the RepDWH before being deleted.	45
	Load Balancing Interval (Days)	Specifies the intervals, in days, that the EventCManager performs load balancing.	1
DaylightSavings	DLS Period Start Date (GMT)	Specifies the start date of daylight savings time.	YYYY-MM-DD HH:MM:SS
	DLS Period End Date (GMT)	Specifies the end date of daylight savings time.	YYYY-MM-DD HH:MM:SS

CallRecsGenerator Parameters

6. On the EMPS navigation tree, right-click `Servers > Events Collector > <ServerName> > CallRecsGenerator1`.
7. From the shortcut menu, select `Edit`.
8. Verify or enter values for the parameters under each tab listed in Table 40, and then click `Save`.

Table 40: CallRecsGenerator Parameters

Tab	Parameter	Description	Example Value

Startup	Directory to execute php script	Specifies the location of the PHP script files to be executed.	Solaris:
			`/opt/genesys/gvp/cn/php/eventc`
			Windows:
			`c:\gvp\cn\php\eventc`

	Cycle Interval	Specifies the interval, in seconds, for the repeated invocation of the Call Records Generator process.	`180`
Advanced	SOAP Port	The port used for Simple Object Access Protocol (SOAP) communication.	`21006`

EventCManager Parameters

9. On the EMPS navigation tree, right-click `Servers > Events Collector > <ServerName> > EventCManager1`.

10. From the shortcut menu, select `Edit`.

11. Verify or enter values for the parameters under each tab listed in Table 41, and then click `Save`.

Table 41: EventCManager Parameters

Tab	Parameter	Description	Example Value

Startup	Directory to execute php script	Specifies the location of the PHP script files to be executed.	Solaris:
			`/opt/genesys/gvp/cn/php/eventc`
			Windows:
			`c:\gvp\cn\php\eventc`

	Cycle Interval	Specifies the interval, in seconds, for the repeated invocation of the EventC Manager process.	`180`
Advanced	SOAP Port	The port used for SOAP communication.	`21700`

EventsLoader Parameters

12. On the EMPS navigation tree, right-click `Servers > Events Collector > <ServerName> > EventsLoader1`
13. From the shortcut menu, select `Edit`.
14. Verify or enter values for the parameters under each tab listed in Table 42, and then click `Save`.

Table 42: EventsLoader Parameters

Tab	Parameter	Description	Example Value

Startup	Directory to execute php script	Specifies the location of the PHP script files to be executed.	Solaris:
			`/opt/genesys/gvp/cn/php/eventc`
			Windows:
			`c:\gvp\cn\php\eventc`

	Cycle Interval	Specifies the interval, in seconds, for the repeated invocation of the Events Loader process.	`180`
Advanced	SOAP Port	The port used for SOAP communication.	`21005`
	Delimiter in Event File	Specifies the character used to delimit the file.	`&`

PeaksNSP1 Parameters

15. On the EMPS navigation tree, right-click `Servers > Events Collector > <ServerName> >PeaksNSP1`.
16. From the shortcut menu, select `Edit`.
17. Verify or enter values for the parameters under each tab listed in Table 43, and then click `Save`.

Table 43: PeaksNSP Parameters

Tab	Parameter	Description	Example Value

Startup	Directory to execute php script	Specifies the location of the PHP script files to be executed.	Solaris:
			`/opt/genesys/gvp/cn/php/eventc`
			Windows:
			`c:\gvp\cn\php\eventc`

	Cycle Interval	Specifies the interval, in seconds, for the repeated invocation of the Peaks process.	`180`
Logging	Log File	Specifies the log file name for the Peaks process.	`PeaksNSP.log`
	Log Levels	Specifies the log levels for the Peaks process.	`*:0x3`
	Log Max Size	Specifies the maximum size limit (in bytes) of the log file. Range is `1 to 2147483647`.	`1073741824`
	Log ULIDs	Specifies the unique log identifier. This parameter has not been implemented.	
Advanced	SOAP Port	The port used for SOAP communication.	`21008`

Note: EventC expects one reseller to be a Parent NSP, a customer under the Parent NSP to be Admin customer, and an IVR Profile under the Admin customer. These must to be configured before starting EventC.

End of procedure

Next Steps

- If you have not already done so, set the required permissions for the `log`, `php`, and `data` directories on the EMS Reporting host. For more information, see Setting file access permissions for EMS Reporting (Windows), page 186 or Setting file access permissions for EMS Reporting (Solaris), page 277.

- If there is more than one EventC machine in your deployment, disable the Peaks process on the other EventC machines. For more information, see Disabling Peaks in a multiple EventC setup, page 319.

Procedure:
Disabling Peaks in a multiple EventC setup

Purpose: To disable the Peaks process on an EMS Reporting host in a multiple EventC setup if a Peaks process is already running on another server.

Start of procedure

1. On the EMPS navigation tree, right-click `Servers > Events Collector > <ServerName> > ConfigEventC`.
2. From the shortcut menu, select `Edit`.
3. On the `Options` tab, clear the attribute `Peak Execution Sequence`.
4. Click `Save`.
5. On the EMPS navigation tree, right-click `Servers > Events Collector > <ServerName> > PeaksNSP1`.
6. From the shortcut menu, select `Edit`.
7. Add a new attribute with the parameter name `php_directory`. Do not assign any value to it.

End of procedure

Configuring Login Server

This section describes how to configure the Login Server and Reseller for Unified Login for both Solaris and Windows.

This section includes the following procedures:

- Configuring Login Server in the EMPS
- Setting the Admin Customer for Unified Login, page 324

Procedure:
Configuring Login Server in the EMPS

Summary

To configure the Login Server for Unified Login, you must configure parameters for the following nodes:

- Login Server (`UnifiedLogin`)—see Step 3 on page 320
- User Administration (`UserConfig`)—see Step 6 on page 322

Prerequisites

- The Unified Login database schema has been created. For more information, see “Creating the Microsoft SQL Server Databases” on page 181 or “Creating the Oracle Databases” on page 271.

Start of procedure

1. In a web browser, access the EMPS login page by entering the URL `http://<EMPS-hostname>:9810/spm/login.php`.
2. Log in to the EMPS as `Admin`, and enter your password.

UnifiedLogin Parameters

3. On the EMPS navigation tree, expand the nodes `Servers > Unified Login Server > <ServerName>`, and then right-click `UnifiedLogin`.
4. From the shortcut menu, select `Edit`.
5. Verify or enter values for the parameters under each tab listed in Table 44, and then click `Save`.

Table 44: UnifiedLogin Parameters

Tab	Parameter	Description	Example Value
Options	Type of Database	Specifies the type of database server.	For Solaris: `oracle` For Windows: `mssql`
	VPN Addresses Start With	Specifies that the IP addresses that begin with this value are identified as VPN addresses.	`10`
	Public Domain Name for Services	Specifies the domain name for the Login Server and other services for public access.	`.domain.com`
	VPN Domain Name for Services	Specifies the domain name for the Login Server and other services for VPN access.	`.vpndomain.com`

LoginServerDB	Login Database Server Name (Oracle Net Service Name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the Login Server database. Usually, this is the combination of the Oracle Service ID and the database service IP.
		Windows—Specifies the fully qualified domain name of the server that has the Login Server database.
			Oracle:
			`GENGRP_172.24.129.52`
			MSSQL:
			`emsreporting.yourdomain.com`

	Login Database / Schema Name	Specifies the name of the Login database.	`unifiedlogin`
	Login Database Server User Name	Specifies the user name to access the Login database.	`unifiedlogin`
	Login Database Server Password	Specifies the password to access the Login database.	`unifiedlogin`

Table 44: UnifiedLogin Parameters (Continued)

Tab	Parameter	Description	Example Value
ProvisioningDB	EMPS Database Server Name (Oracle Net Service name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the EMPS database. Usually, this is the combination of the Oracle Service ID and the database service IP. Windows—Specifies the fully qualified domain name of the server that has the EMPS database.	Oracle: `GENGRP_172.24.129.52` MSSQL: `emsreporting.yourdomain.com`
	EMPS Database / Schema Name	Specifies the database/schema name for the EMPS.	`emps`
	EMPS Database User Name	Specifies the user name of the EMPS database.	`emps`
	EMPS Database Password	Specifies the password of the EMPS database.	`emps`
Advanced	Unified Login Service ID	Specifies the service ID for the Login Server.	`UL1`

UserConfig Parameters

6. On the EMPS navigation tree, right-click the `Servers > Unified Login Server > <ServerName> > UserConfig` node.
7. From the shortcut menu, select `Edit`.
8. Verify or enter values for the parameters under each tab listed in Table 45, and then click `Save`.

Table 45: UserConfig Parameters

Tab	Parameter	Description	Example Value
Options	Type of Database	Specifies the Oracle database server.	`oracle`
LoginServerDB	Login Database Server Name (Oracle Net Service Name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the Login database. Usually, this is the combination of the Oracle Service ID and the database service IP. Windows—Specifies the fully qualified domain name of the server that has the Login database.	Oracle: `GENGRP_172.24.129.52` MSSQL: `emsreporting.yourdomain.com`
	Login Database / Schema Name	Specifies the database name of the Login server database.	`unifiedlogin`
	Login Database Server User Name	Specifies the user ID for the Login server user.	`unifiedlogin`
	Login Database Server Password	Specifies the password for the Login server user.	`unifiedlogin`
ProvisioningDB	EMPS Database Server Name (Oracle Net Service name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the EMPS database. Usually, this is the combination of the Oracle Service ID and the database service IP. Windows—Specifies the fully qualified domain name of the server that has the EMPS database.	Oracle: `GENGRP_172.24.129.52` MSSQL: `emsreporting.yourdomain.com`
	EMPS Database / Schema Name	Specifies the database name of the EMPS database.	`emps`
	EMPS Database User Name	Specifies the User ID for the EMPS user.	`emps`
	EMPS Database Password	Specifies the password for the EMPS user.	`emps`

Table 45: UserConfig Parameters (Continued)

Tab	Parameter	Description	Example Value
Advanced	User Config Service ID	Specifies the service ID for the User Config.	`CONFIG1`
	Service ID for Administration Utility	Specifies the service ID for the administration utility.	`CONFIG1`

End of procedure

Next Steps

- For a multi-tenant deployment, specify the Administrative Customer (Admin Customer). For more information, see Setting the Admin Customer for Unified Login.
- In Windows deployments, set up the Unified Login website. For more information, see Creating a website for Unified Login (Windows 2003), page 188.L

Procedure:
Setting the Admin Customer for Unified Login

Purpose: To designate the Customer who will be the administrator user.

If your deployment is multi-tenant, you must perform this procedure.

If your deployment is single-tenant, perform this procedure if you want to change the default Reseller and Admin Customer. In single-tenant mode, you can have only one Reseller. The default Reseller is `GVPOwner`, and the default Customer is `Admin`.

The Admin Customer is also referred to as the NSP Customer.

For more information about provisioning Resellers and Customers, see the chapter about EMPS in the *Genesys Voice Platform 7.6 Reference Manual.*

Start of procedure

1. Specify the parent Network Service Provider (NSP) Reseller:
   a. In the EMPS, create or select the Reseller to designate as the parent NSP.
   b. On the properties page for that Reseller, select the `Reseller is Parent NSP` check box.
2. Specify the NSP Customer:
   a. Create or select the Customer of the parent NSP that you want to designate as the NSP Customer.

   b. On the properties page for that Customer, select the `NSP Customer` check box.

3. Note the Customer ID for the NSP Customer, because you need it for Unified Login configuration.

End of procedure

Next Steps

- Update the UnifiedLogin database. For more information, see Updating the Customer ID in the Login Server database (Windows), page 187 or Updating the Customer ID in the Login Server database (Solaris), page 279.

  Note: Whenever you change the NSP Customer in the EMPS, you must update the UnifiedLogin database.

- If you have not already done so, set up the Unified Login website. For more information, see Creating a website for Unified Login (Windows 2003), page 188.

Configuring Reporter

This section describes how to configure Reporter for both Solaris and Windows.

This section includes the following procedures:

- Configuring Reporter in the EMPS
- Changing the Regional Settings for Reporter, page 330

Procedure:
Configuring Reporter in the EMPS

Summary

To update provisioning for Reporter, you must configure parameters for the following nodes:

- Reporter server (`Reporter`)—see Step 3
- Reporter Download (`ReporterDownload`)—see Step 6 on page 328

Prerequisites

- The Reporter database schema has been created. For more information, see "Creating the Microsoft SQL Server Databases" on page 181 or "Creating the Oracle Databases" on page 271.

Start of procedure

1. In a web browser, access the EMPS login screen by entering the URL `http://<EMPS-hostname>:9810/spm/login.php`.
2. Log in to the EMPS as `Admin`, and enter your password.

Reporter Parameters

3. On the EMPS navigation tree, expand the nodes `Servers > Reporter > <ServerName>`, and then right-click `Reporter`.
4. From the shortcut menu, select `Edit`.
5. Verify or enter values for the parameters under each tab listed in Table 46, and then click `Save`.

Table 46: Reporter Parameters

Tab	Parameter	Description	Example Value
Options	Type of Database	Specifies the type of database server.	For Solaris: `oracle` For Windows: `mssql`
	SSL Enabled on the Web Server	Check box that specifies whether SSL certificates are installed and enabled on the web server.	Cleared
	Name of NSP to Show in Reports	Specifies the network service provider name shown in the Reporter.	`NSP`
	Download Files Directory	Specifies the directory where the Reporter stores the download files.	`/download`
	Downloadable Reports Cleanup Interval	Specifies the number of days to retain the downloadable reports files, before the reports are cleaned up. Range is: `1–1000`	`7`

Table 46: Reporter Parameters (Continued)

Tab	Parameter	Description	Example Value
Options (continued)	Locale Setting	Specifies the UTF-8 locale setting that determines the way dates and numbers display on the Reporter screens. For more information about locale settings for Reporter, see "Locale Setting" on page 329.	`en-us`

ReporterDB	Reporter Database Server Name (Oracle Net Service Name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the Reporter database. Usually, this is the combination of the Oracle Service ID and the database service IP.
		Windows—Specifies the fully qualified domain name of the server that has the Reporter database.
			Oracle:
			`GENGRP_172.24.129.52`
			MSSQL:
			`emsreporting.yourdomain.com`

	Reporter Database / Schema Name	Specifies the Reporter database name.	`reporter`
	Reporter Database User Name	Specifies the Reporter Server user name.	`reporter`
	Reporter Database Password	Specifies the Reporter Server password.	`reporter`

ProvisioningDB	EMPS Database Server Name (Oracle Net Service name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the EMPS database. Usually, this is the combination of the Oracle Service ID and the database service IP.
		Windows—Specifies the fully qualified domain name of the server that has the EMPS database.
			Oracle:
			`GENGRP_172.24.129.52`
			MSSQL:
			`emsreporting.yourdomain.com`

	EMPS Database / Schema Name	Specifies the EMPS database name.	`emps`

Table 46: Reporter Parameters (Continued)

Tab	Parameter	Description	Example Value
ProvisioningDB (continued)	EMPS Database User Name	Specifies the user name to access the EMPS database.	`emps`
	EMPS Database Password	Specifies the password to access the EMPS database.	`emps`
Advanced	Instance Identifier	Specifies the Reporter instance identifier on the machine.	`Reporter1`

ReporterDownload Parameters

6. On the EMPS navigation tree, right-click the `Servers > Reporter > <ServerName> > ReporterDownload` node.
7. From the shortcut menu, select `Edit`.
8. Verify or enter values for the parameters under each tab listed in Table 47, and then click `Save`.

Table 47: Reporter Download Parameters

Tab	Parameter	Description	Example Value

Startup	Directory to Execute php Script	Specifies the location of the `.php` script files to be executed.	Solaris:
			`/opt/genesys/gvp/cn/php/reporter`
			Windows:
			`c:\gvp\cn\php\reporter`

	Cycle Interval	Specifies, in seconds, the interval for the repeated invocation of the Reporter backend process. Range is: `10–360`	`180`
Advanced	SOAP Port	Specifies the port used for SOAP communication.	`21010`

End of procedure

Next Steps

- If you have not already done so, set the required permissions for the `log`, `php`, and `extweb/reporter/download` directories on the EMS Reporting host. For more information, see "Setting File Permissions for EMS Reporting" on page 185 or "Setting File Access Permissions" on page 277.
- Modify the Unified Login URL to add the Reporter service (see Modifying the Unified Login URL for additional services (Windows), page 193 or Modifying the Unified Login URL for additional services (Solaris), page 281).

Locale Setting

The Reporter supports different regional settings. UTF-8 locales are supported.

By default, the Reporter is set to the US locale. Ensure that the US regional settings are available in the installed operating system before using the Reporter screens.

You can change the regional setting for Reporter to any UTF-8 locale. For more information, see Changing the Regional Settings for Reporter, page 330.

locale.xml File

Locale information (in other words, regional settings for various languages) is specified in the `locale.xml` file. The following regional setting specifications are included by default:

- `en_us`—English US
- `en_uk`—English UK
- `fr`—French Standard
- `de`—German Standard
- `pt`—Portuguese (Brazil)

Table 48 describes the attributes that are specified in a regional settings node in the `locale.xml` file.

Table 48: Regional Settings Attributes in the locale.xml File

Attribute Name	Description	Format
id	The name of the regional setting that is referenced in the `Locale` attribute in the EMPS Reporter node.	Any alphanumeric name (English alphabet only) with no special characters or spaces.
decimalpt	The decimal point indicator that the Reporter will use.	Any single character—for example, comma (`,`) or period (`.`).
thousandgrp	The thousand grouping indicator that the Reporter will use.	Any single character—for example, comma (`,`) or period (`.`).

Table 48: Regional Settings Attributes in the locale.xml File (Continued)

Attribute Name	Description	Format

dtformat	The date format that the Reporter will use.	`DD/MM/YYYY`
		or
		`MM/DD/YYYY`

UNIX	The non-Windows operating system locale string regional setting.	As suggested in the Solaris documentation. For more information, see: • developers.sun.com • docs.sun.com
win	Specifies the Microsoft locale string regional setting.	As suggested in the Microsoft documentation. For more information, see: • msdn.microsoft.com • microsoft.com
Text between the node strings	A user-referenced value to identify the regional setting.	Any alphanumeric name (English alphabet only).

To change the locale for Reporter, use the following procedure.

Procedure:
Changing the Regional Settings for Reporter

Start of procedure

1. Verify that the required regional setting is available on the operating system.
2. Open the `<CN Dir>/extweb/reporter/locale.xml` file in a text editor.
3. Locate the regional setting that you want to use.

   If necessary, modify or add the specification for the regional setting that you require. You may specify any number of nodes. If you make any changes, save the file.

   For more information about the attributes in a regional settings node, see Table 48 on page 329.

4. Make note of the string value of the `id` attribute of the node.

   For example, in the following sample specification of the French Standard regional setting, the value of the `id` attribute is `fr`.

   ```
   <locale id="fr">
   <strings decimalpt="," thousandgrp=""
   dtformat="DD/MM/YYYY" unix="fr_FR.UTF-8" win="fra">French
   Standard</strings>
   </locale>
   ```

5. Close the `locale.xml` file.
6. In the EMPS, under the `Reporter` object, set the `Locale` string parameter to the regional setting value that you noted in Step 4. For more information about the required parameter, see Locale Setting on page 327.

End of procedure

Configuring Call Status Monitor

This section describes how to configure Call Status Monitor for both Solaris and Windows.

Procedure: Configuring Call Status Monitor in the EMPS

Summary

To update provisioning for Call Status Monitor, you must configure parameters for the `CallStatusMonitor` node.

Start of procedure

1. In a web browser, access the EMPS login screen by entering the URL `http://<EMPS-hostname>:9810/spm/login.php`.
2. Log in to the EMPS as `Admin`, and enter your password.
3. On the EMPS navigation tree, expand the nodes `Servers > Call Status Monitor > <ServerName>`, and then right-click `Call Status Monitor`.
4. From the shortcut menu, select `Edit`.
5. Verify or enter values for the parameters under each tab listed in Table 49, and then click `Save`.

Table 49: Call Status Monitor Parameters

Tab	Parameter	Description	Example Value
Options	Type of Database	Specifies the type of database server.	For Solaris: `oracle` For Windows: `mssql`
	PM Web Server Port	Specifies the port on which the Policy Manager process listens.	`9810`
	Name of NSP to Show in Reports	Specifies the network service provider name shown in the Call Status Monitor reports.	`NSP`
ProvisioningDB	EMPS Database Server Name (Oracle Net Service name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the EMPS database. Usually, this is the combination of the Oracle Service ID and the database service IP. Windows—Specifies the fully qualified domain name of the server that has the EMPS database.	Oracle: `GENGRP_172.24.129.52` MSSQL: `emsreporting.yourdomain.com`
	EMPS Database / Schema Name	Specifies the EMPS database name.	`emps`
	EMPS Database User Name	Specifies the EMPS Server user name.	`emps`
	EMPS Database Password	Specifies the EMPS Server password.	`emps`
Advanced	Service ID for Call Status Monitor	Specifies the service ID for the Call Status Monitor.	`CSM1`

End of procedure

Next Steps

- Configure the Call Status Monitor services in the Login Administration service (see Modifying the Unified Login URL for additional services (Windows), page 193 or Modifying the Unified Login URL for additional services (Solaris), page 281).

Configuring Network Monitor

This section describes how to configure Network Monitor for both Solaris and Windows.

Procedure:
Configuring Network Monitor in the EMPS

Summary

To update provisioning for Network Monitor, you must configure parameters for the NetworkMonitor node.

Prerequisites

- The Network Monitor database schema has been created. For more information, see "Creating the Microsoft SQL Server Databases" on page 181 or "Creating the Oracle Databases" on page 271.

Start of procedure

1. In a web browser, access the EMPS login screen by entering the URL `http://<EMPS-hostname>:9810/spm/login.php`.
2. Log in to the EMPS as `Admin`, and enter your password.
3. On the EMPS navigation tree, expand the nodes `Servers > Network Monitor > <ServerName>`, and then right-click `NetworkMonitor`.
4. From the shortcut menu, select `Edit`.
5. Verify or enter values for the parameters under each tab listed in Table 50, and then click `Save`.

Table 50: Network Monitor Parameters

Tab	Parameter	Description	Example Value

Startup	PHP Executable Directory	Specifies the name of the directory where the PHP files exist.	Solaris:
			`/opt/genesys/gvp/cn/php/netmon`
			Windows:
			`c:\gvp\cn\php\netmon`

	PHP Script Interval	Specifies the interval (in seconds) between executions.	`180`
Options	Type of Database	Specifies the type of database server.	For Solaris: `oracle` For Windows: `mssql`

Table 50: Network Monitor Parameters (Continued)

Tab	Parameter	Description	Example Value

NetmonDB	Netmon -DB Server Name (Oracle Net Service name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the Network Monitor database. Usually, this is the combination of the Oracle Service ID and the database service IP.
		Windows—Specifies the fully qualified domain name of the server that has the Network Monitor database.
			Oracle:
			`GENGRP_172.24.129.52`
			MSSQL:
			`emsreporting.yourdomain.com`

	Netmon Database Name / Schema name	Specifies the name of the Network Monitor database.	`netmon`
	Netmon - DB User Name	Specifies the user name to access the Network Monitor database.	`netmon`
	Netmon - DB Password	Specifies the password to access the Network Monitor database.	`netmon`

ProvisioningDB	EMPS Database Server Name (Oracle Net Service name in case of Oracle)	Solaris—Specifies the Net Service name of the server that has the EMPS database. Usually, this is the combination of the Oracle Service ID and the database service IP.
		Windows—Specifies the fully qualified domain name of the server that has the EMPS database.
			Oracle:
			`GENGRP_172.24.129.52`
			MSSQL:
			`emsreporting.yourdomain.com`

	EMPS Database Name / Schema name	Specifies the name of the EMPS database.	`emps`
	EMPS Database Server User Name	Specifies the user name to access the EMPS database.	`emps`
	EMPS Database Server Password	Specifies the password to access the EMPS database.	`emps`

Table 50: Network Monitor Parameters (Continued)

Tab	Parameter	Description	Example Value
Advanced	SOAP Port	Specifies the port used for SOAP communication.	`21015`
	PM Web Server Port	Specifies the port on which the Policy Manager process listens.	`9810`

End of procedure

Next Steps

- If you have not already done so, set the required permissions for the `php` directory on the EMS Reporting host. For more information, see Setting file access permissions for EMS Reporting (Windows), page 186 or Setting file access permissions for EMS Reporting (Solaris), page 277.
- For Windows deployments, set up the Network Monitor website. For more information, see Creating a website for Network Monitor (Windows 2003), page 195.

Configuring OBN Manager

This section describes how to configure OBN Manager for both Solaris and Windows.

This section includes the following procedures:

- Configuring OBN Manager in the EMPS
- Creating groups for OBN Manager in the EMPS, page 339

For more information about the OBN Manager, see the *Genesys Voice Platform 7.6 Reference Manual.*

Procedure:
Configuring OBN Manager in the EMPS

Summary

To update provisioning for OBN Manager, you must configure parameters for the `OBNManager` node.

Prerequisites

- The OBN database schema has been created. For more information, see “Creating the Microsoft SQL Server Databases” on page 181 or “Creating the Oracle Databases” on page 271.

Start of procedure

1. In a web browser, access the EMPS login screen by entering the URL `http://<EMPS-hostname>:9810/spm/login.php`.
2. Log in to the EMPS as `Admin`, and enter your password.
3. On the EMPS navigation tree, expand the nodes `Servers > Outbound Notification Manager > <ServerName>`, and then right-click `OBNManager`.
4. From the shortcut menu, select `Edit`.
5. Verify or enter values for the parameters under each tab listed in Table 51, and then click `Save`.

Table 51: OBN Manager Configuration Parameters

Tab	Parameter	Description	Example Values
Data Store	Database Server (Service Name for Oracle)	Solaris—Specifies the Net Service name of the server that has the OBN Manager database. Usually, this is the combination of the Oracle Service ID and the database service IP. Windows—Specifies the fully qualified domain name of the server that has the OBN Manager database.	Oracle: `GENGRP_172.24.129.52` MSSQL: `emsreporting.yourdomain.com`
	Database Username	Username for database user account.	`obnmanager`
	Database Password	Password for database user account.	`obnmanager`
	Database Catalog **Note:** There is no database catalog for Solaris hosts, and therefore this parameter will not be displayed.	The OBN Manager Database Name.	`obnmanager`

Table 51: OBN Manager Configuration Parameters (Continued)

Tab	Parameter	Description	Example Values
Advanced Configuration	Min DB Pool Size	Minimum number of database connections kept alive for use in QManager.	`5`
	Max DB Pool Size	Maximum number of database connections kept alive for use in QManager.	`20`
	OCS Retransmit Timeout	Interval, in seconds, during which OBN Manager will try to retransmit GVP responses to OCS, if the socket connection between OCS and OBN Manager has gone down. OBN Manager regularly scans the OBN database to detect responses that have not been transmitted to OCS. (The interval at which OBN Manager scans the database is configurable—see the `Retransmit Interval` parameter.) For each response that has failed to transmit, the `OCS Retransmit Timeout` interval starts when the failure first occurs and is recorded in the OBN database. If OBN Manager has not succeeded in transmitting the response by the time that the `OCS Retransmit Timeout` interval expires for that response, OBN Manager flushes the response from its storage and does not attempt to retransmit it again.	`18000`
	ORP Threads	Number of Outbound Request Processor (ORP) threads that should process requests prepared by QManager.	`10`

Table 51: OBN Manager Configuration Parameters (Continued)

Tab	Parameter	Description	Example Values
Advanced Configuration (continued)	Queue Batch Size	Number of entries that QManager adds to the queue at one time for ORP to pick up and process.	`200`
	Clean Interval	Interval, in seconds, at which QManager removes expired or completed requests from the database.	`300`
	QCheck Interval	Interval, in milliseconds, at which QManager removes expired requests from the prepared queue, so that ORP does not that pick up.	`3000`
	Queue Interval	Interval, in milliseconds, at which QManager populates the internal queue.	`2000`
	VCS/IPCS Inactive Interval.	Interval, in seconds, after OBN Manager receives a `NO_PORTS` message in a failure URL from Call Flow Assistant (CFA), for which OBN Manager will not send any requests to the VCS or IPCS that sent the message. The applicable VCS or IPCS is marked as `stale` for the duration of the inactivity interval. If the applicable VCS or IPCS is the only communication server that has been configured for OBN Manager, requests to the stale server will fail and will be treated as failed attempts. If the applicable VCS or IPCS is not the only communication server that has been configured for OBN Manager, requests will be sent to the other active servers, in round-robin fashion.	`60`

Table 51: OBN Manager Configuration Parameters (Continued)

Tab	Parameter	Description	Example Values
Advanced Configuration (continued)	Retransmit Interval	Frequency, in seconds, with which OBN Manager scans the OBN database for failed GVP responses, to retransmit to OCS. See also the `OCS Retransmit Timeout` parameter.	`180`
	Max Active Requests	Maximum number of requests that are prepared for processing by ORP. Genesys recommends that you set this to about at least 5 times the size of the `Queue Batch Size` parameter.	`1000`
OCS Configuration	OCS Configured	Select this check box for integration of OBN with Outbound Contact Server (OCS).	Selected
	OCS Listener Port	Port used to establish a connection with OCS. The port is set to `2355`.	`2355`
System	Log Levels	Logging setting, to control the amount of information that is written to the log file.	`*:0x3`

End of procedure

Next Steps

- Create the groups of IPCS/VCS servers that OBN Manager will use for Outbound Applications (see Creating groups for OBN Manager in the EMPS).
- Restart the OBN WatchDog after you complete the EMPS configuration changes. For information about starting WatchDog, see Starting/Restarting GVP in Normal mode (Windows), page 198 or Starting/Restarting GVP (Solaris), page 283.

Procedure: Creating groups for OBN Manager in the EMPS

Purpose: To create the IPCS/VCS server groups for Outbound Applications.

Prerequisites

- Outbound ports have been configured on the IPCS or VCS servers that you want to include in the groups.

Start of procedure

1. On the EMPS navigation tree, right-click `Server Groups,` and select `Add New Group.`
2. In the `Group Name` field, enter the name of the group.
3. From the `Server Group Type` drop-down list, select `OBNCS.`

   The `Available` list in the `Servers Selection` section is populated with all of the IPCS and VCS servers that have been provisioned.
4. For each IPCS or VCS server that you want to use for an Outbound Application, click the server in the `Available` list, and then click `>>` to move it to the `Selection` list.
   - For VCS, ensure that you select only servers that have provisioned Outbound ports (the `Route Type` of the `Route1` node has been set to either `Inbound & Outbound` or `Outbound`).
   - For IPCS, you can select any server, because the ports are universal.

   To remove a server from the `Selection` list, click the server, and then click `<<`.
5. Click `Save.`

End of procedure

Next Steps

- Create applications for OBN Manager. For more information, see the chapter about Outbound Notification Manager in the *Genesys Voice Platform 7.6 Reference Manual.*

Chapter

20 Configuring IPCS in the EMPS

This chapter describes how to configure the Genesys Voice Platform (GVP) IP Communication Server (IPCS) in the Element Management Provisioning System (EMPS).

This chapter contains the following sections:

Configuring IPCS

This section describes how to configure the IPCS for both Solaris and Windows.

Procedure: Configuring IPCS in the EMPS

Summary

To configure the IPCS, you must configure parameters for the following nodes:

- PopGateway process (`PopGateway1`)—see Step 3 on page 342
- PopGateway Route (`Route`)—see Step 6 on page 350
- Call Flow Assistant (`CFA`)—see Step 9 on page 351
- Media Control Unit process (`mcu`)—see Step 12 on page 354
- Mcu Media Controller (`MediaController`)—see Step 15 on page 354
- Page Collector (`PageCollector`)—see Step 18 on page 355

Start of procedure

1. In a web browser, access the EMPS login page by entering the URL `http://<EMPS-hostname>:9810/spm/login.php`.
2. Log in to the EMPS as `Admin`, and enter your password.

PopGateway Parameters

3. On the EMPS navigation tree, expand the nodes `Servers > IP Communication Server > <ServerName>`, and then right-click `PopGateway1`.
4. From the shortcut menu, select `Edit`.
5. Verify or enter values for the parameters under each tab listed in Table 52, and then click `Save`.

> Note: When configuring PopGateway parameters, be aware that, by default, each PopGateway has 200 logical ports. This means that each PopGateway can have a maximum of 200 concurrent calls. To bridge both inbound and outbound legs, both legs must be from the same PopGateway.
>
> To create the nodes for additional PopGateway processes, copy an existing `PopGateway` node and reconfigure its parameters as required.

For more information, see the chapter about multiple PopGateways and MCUs in the *Genesys Voice Platform 7.6 Reference Manual*.

Table 52: IPCS PopGateway Parameters

Tab	Parameter	Description	Example Value
General	Log File	Specifies the log file for the PopGateway process.	`PopGateway1.log`
	Outbound Default ANI	Specifies the default Automatic Number Identification (ANI) that is used for outbound calls when no ANI is available.	`8880000000`
IVR	Primary DID Mapper	(Mandatory) Specifies the fully qualified domain name (FQDN) of the `Dispenser/did_url_mappings/$did$.xml`.	`http://<FQDN of Dispenser>/did_url_mappings/$did$.xml`

Table 52: IPCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
IVR (continued)	Backup DID Mapper	Specifies the backup FQDN of the `Dispenser/did_url_mappings/$did$.xml`.	`http://<FQDN of Dispenser>/did_url_mappings/$did$.xml`
	Primary Outbound DID Mapper	(Mandatory) Specifies the FQDN of the `<EMPS machine>/did_url_mappings/$reseller-name$_$customer-name$_$application-name$_outbounddid.xml`. **Note:** For Solaris, this value is case sensitive, and you must use all lowercase.	`http://<FQDN of EMPS machine>:9810/did_url_mappings/$reseller-name$_$customer-name$_$application-name$_OutboundDID.xml`
	Backup Outbound DID Mapper	Specifies the backup FQDN of the `<EMPS machine>/did_url_mappings/$reseller-name$_$customer-name$_$application-name$_outbounddid.xml`. **Note:** For Solaris, this value is case sensitive, and you must use all lowercase.	`http://<FQDN of EMPS machine>:9810/did_url_mappings/$reseller-name$_$customer-name$_$application-name$_OutboundDID.xml`
	Dispenser URL Fetch Timer (secs)	(Mandatory) Specifies the length, in seconds, of the fetch timeout that the PopGateway gives to the Dispenser URL.	`3`
	Billing Server URL	(Mandatory) Specifies the Billing URL to which billing records should be posted. The format is: `http://<Fully Qualified Name of EventC machine>:9810/billing/events.php`	`http://<FQDN of EventC>:9810/billing/events.php`

Table 52: IPCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
IVR (continued)	Primary Generic URL Mapper	Used instead of `Primary DID Mapper` when the Interactive Voice Response (IVR) application URL is given in the signaling message (for example, Session Initiation Protocol [SIP] Network Announcement). Configure this parameter in one of the following ways, depending on the scenario and requirements: • To point to a `did.xml` file (for example, `http://<dispenser>/did_url_mappings/$did$.xml`). This assumes that the signaling message contains a valid Dialed Number Identification Service (DNIS). The DNIS must already have been associated with the Network Announcement application during application provisioning. • To point to an `appid.xml` file (for example, `http://<dispenser>/did_url_mappings/0200/<appname>.xml`). This assumes either that the signaling message does not contain a valid DNIS (it might contain a dummy DNIS, for example) or that it contains a large range of DNISs (which makes it impractical to provision). The `<appname>` must already have been provisioned as an application of `Network Announcement` type. Note that the Genesys Voice Platform (GVP) system will not be multi-tenant in this scenario.	`http://machine/path/genericdid.xml`

Table 52: IPCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
IVR (continued)	Backup Generic URL Mapper	Used instead of `Backup DID Mapper` when the IVR application URL is given in the signaling message (for example, SIP Network Announcement). Configure this parameter in one of the following ways, depending on the scenario and requirements: • To point to a `did.xml` file (for example, `http://<dispenser>/did_url_mappings/$did$.xml`). This assumes that the signaling message contains a valid DNIS. The DNIS must already have been associated with the Network Announcement application during application provisioning. • To point to an `appid.xml` file (for example, `http://<dispenser>/did_url_mappings/0200/<appname>.xml`). This assumes that either the signaling message does not contain a valid DNIS (it might contain a dummy DNIS, for example) or that it contains a large range of DNISs (which makes it impractical to provision). The `<appname>` must already have been provisioned as an application of `Network Announcement` type. Note that the Genesys Voice Platform (GVP) system will not be multi-tenant in this scenario.	`http://machine/path/genericdid2.xml`
	ASR Result Properties Access	Check box that specifies whether Automatic Speech Recognition (ASR) result properties can be accessed by the voice application.	Cleared

Table 52: IPCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
SIP	Local SIP Port	Specifies the port used for SIP communications.	`5060`
	Primary Call Manager IP Address	Specifies the IP address of the primary Call Manager.	`10.10.10.10`
	Backup Call Manager IP Address	Specifies the IP address of the backup Call Manager.	`10.10.10.11`
	Primary Call Manager SIP Port	Specifies the User Datagram Protocol (UDP) port that the primary Call Manager uses for SIP communications.	`5060`
	Backup Call Manager SIP Port	Specifies the UDP port that the backup Call Manager uses for SIP communications.	`5060`
	Resource Manager	Specifies the Resource Manager IP address/host name and port, in the following format: `<ip address:port>` **Note:** You must set this parameter when integrating with the Genesys SIP Server.	`10.10.10.10:1234`
	Back Up Resource Manager	Specifies the Backup Resource Manager IP address/hostname and port, in the following format: `<ip address:port>` **Note:** You must set this parameter when integrating with the Genesys SIP Server.	`10.10.10.10:1234`

Table 52: IPCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
SIP (continued)	SIP Registrar	Specifies whether SIP registration is enabled. To enable this feature, specify an IP address and port, in the following format: `<ip address>:port` If this parameter is left empty, no registration requests will be sent.	`10.10.10.10:5060`
	SIP Registration Refresh Interval	Specifies the interval, in seconds, at which IPCS sends registration requests to the SIP server. The minimum value is `3600` seconds. Valid values: `3600–31536000` Default value: `604800` (one week)	`604800`
	Default Media/Signalling Gateway IP Address	Specifies the IP address of the IP/Time-division Multiplexing (TDM) media gateway.	`10.10.10.10`
	SIP Inbound Call Responses	Specifies, as a comma-separated list, the SIP `1xx` responses that will be sent for all new inbound call `INVITE` messages. **Note:** Currently only `100, 180 and 183` responses are supported.	`100,180,183`
	Starting Number for Port IDs / Channel IDs	Specifies the start of unique channel/port numbering. You should enter a minimum value of `1,` which ensures that the channels have unique numbers across the PopGateway processes.	`1`
	Enable Reliable Provisional Messages	Check box that specifies whether the application supports sending provisional responses to SIP messages in a reliable way.	Cleared

Table 52: IPCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
SIP (continued)	SIP Header for DID	Specifies where IPCS looks to retrieve the Direct Inward Dial (DID). Valid values: • `History-Info` • `<empty>` Default value: `<empty>` If you leave this parameter empty, IPCS uses the `To` Header for DID lookup.	
	SIP Header for IVR Port	Specifies the SIP header from which IPCS obtains the IVR port value and sends it to Genesys Framework. Valid values: • `To` • `<empty>` The default value is <empty>. If you leave this parameter empty, or if IPCS cannot obtain the port number from the SIP header, IPCS reports the telephony port as the IVR port.	
	Local IP Address	Specifies the Internet Protocol (IP) address of the PopGateway. **Note:** You must set this parameter for systems with multiple Network Interface Cards (NIC).)	`10.10.10.10`

Table 52: IPCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
Hangup	Hangup Cause Fetch Error	Specifies the hangup response message if any VoiceXML file download fails at any time during call setup.	503
	Hangup Cause Internal Error	Specifies the hangup response message for any application error.	500
	Hangup Cause Parse Error	Specifies the hangup response message for an application parsing error.	500
	Hangup Cause Resource Unavailable	Specifies the hangup response message when IPCS does not have the necessary resources to answer a call.	480
	Hangup Cause SDP Error	Specifies the hangup response message when IPCS is unable to parse the Session Description Protocol (SDP).	400
Media	Media Server Process	Specifies the name of the Media Server process to use. Valid value: `mcu`	mcu
	Media Server Address	Specifies the IP address of the Media Server. The default value is the IP address of the local machine.	10.10.10.10

Table 52: IPCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
Session	Enable Session Timers	Specifies whether Session Timer support is enabled for a call session. Select to enable Session Timer support.	Cleared
	Session Timer Refresher	Specifies which user agent initiates refreshing of a call session. If you select `Local,` IPCS refreshes the session. If you select `Remote,` the far-end refreshes the session. If the refresher is already specified by the far end for inbound calls, this parameter is ignored.	`Local,0;Remote,1`
	Session Timer Interval (secs)	Specifies the time interval, in seconds, at which a call session must be refreshed; otherwise the session expires. **Note:** The minimum value must be no lower than 90 (seconds).	`1800`

Route Parameters

6. On the EMPS navigation tree, expand the `Servers > IP Communication Server > <ServerName> > Popgateway` node, and then right-click `Route`.
7. From the shortcut menu, select `Edit`.
8. Verify or enter values on the `General` tab for the parameters listed in Table 53, and then click `Save`.

Table 53: IPCS Route Parameters

Tab	Parameter	Description	Example Value
General	Route Description	Specifies the description of this route.	Route1
	Route ID Number	Specifies the unique number that identifies this route.	1
	Call Direction	Specifies the direction of the call. Valid values: • In—Inbound ports; can only accept inbound calls. • Out—Outbound ports; can only make outbound calls. • InOut—Inbound/Outbound ports; can both accept inbound calls and make outbound calls.	InOut
	Licensed Channels	Specifies an encrypted number of licensed channels for calls that this route can use. This is a read-only parameter.	
	Max Channels	Specifies the maximum number of channels that this route can use.	100

CFA Parameters

9. On the EMPS navigation tree, right-click `Servers > IP Communication Server > <ServerName> > CFA`.

10. From the shortcut menu, select `Edit`.

11. Verify or enter values on the `General` tab for the parameters listed in Table 54, and then click `Save`.

Table 54: IPCS CFA Parameters

Tab	Parameter	Description	Example Value
General	Primary CTA URL	Specifies the URL to use if transfers are to be performed through an external gateway. If the `Transfer Type` parameter is set to `External Transfer`, then, when it is time to perform a transfer, GVP contacts the `Primary CTA URL` to complete the transfer. **Note:** This parameter is used only if the `Transfer Type` is set to `External Transfer`.	`http://<CTA Server>/webnotify.asp?notifyprocess=CTA`
	DID.xml URL in case of failures	Specifies the URL to use if the Framework provides a DNIS that has not been provisioned on the GVP.	`http://qadid.qa.genesyslab.com/did_url_mappings/Windows/$did$.xml`
	Transfer Type	Specifies the type of transfer on the platform. Valid values: • `Transfer on platform` • `Transfer through CTI` • `External Transfer`	`Transfer on platform`
	Application URL in case of failures	Specifies the URL to use if the Call Flow Assistant (CFA) fails to contact the IVR Server Client to fetch the DNIS at call setup time. This URL will also be used if the IVR Server Client is not accessible to perform a computer telephony integration (CTI) transfer.	`http://$empsservername$/emps/database/dids/$did$.xml`
	Backup CTA URL	Specifies the URL that GVP uses if it fails to contact the Primary CTA URL at call setup time.	`http://<CTA Server>/webnotify.asp?notifyprocess=CTA`
	URL for $did$.xml file	Specifies the URL that is used to fetch the `$did$.xml` file.	`http://(Ini Dispenser Machine)/$did$.xml`

Table 54: IPCS CFA Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	I-Server Client URL	Specifies the IVR Server Client URL that is used to fetch the ANI/DNIS from the IVR Server in a behind-the-switch configuration. This URL is also used for performing CTI transfers if the `Transfer Type` parameter is set to `Transfer through CTI`. **Note:** This parameter applies only to the primary IVR Server Client. A backup IVR Server Client URL applies only to an IVR Server that is running in either `InFront` mode or `Network` mode, and it is set during customer provisioning.	`http://localhost/WebNotify.asp?NotifyProcess=ISvrClient`
	Default DNIS	Specifies the default DNIS that will be used if the DNIS from CTI is not received.	`1234`
	GVP Success URL	Specifies the URL that is used to fetch the actual `did.xml` file in a behind-the-switch configuration. This URL should point to the Dispenser directory in which the actual `.did` files are stored.	`http://$empsservername$/emps/database/dids/$did$.xml`
	Use SCP Gateway For ANI & DNIS	Reserved for future use.	NO
	Use CTI Client For ANI & DNIS	Specifies whether to fetch the ANI and DNIS from the CTI client. Valid values: • `0`—Disable • 1—Enable **Note:** This parameter is typically enabled when GVP is configured in the behind-the-switch mode.	`0`
	ReRoute Wait Timeout (in sec)	Specifies the amount of time, in seconds, that the platform waits before ending the call if the agent leg drops without initiating a reroute. This parameter is valid only for applications that have rerouting enabled. Valid values: `1–10000` (seconds) Default value is `5`.	`5`

Mcu Parameters

12. On the EMPS navigation tree, right-click `Servers > IP Communication Server > <ServerName> > Mcu`.
13. From the shortcut menu, select `Edit`.
14. Verify or enter values for the parameters under each tab listed in Table 55, and then click `Save`.

Table 55: Mcu Parameters

Tab	Parameter	Description	Example Value
General	Log File	Specifies the log file for the `mcu` process.	`mcu.log`
DTMF	Fallback DTMF Mode	Specifies the type of DTMF used if RFC 2833 cannot be negotiated. DTMFs generated will fall back to this type. DTMF detection will always recognize both RFC 2833 and SIP INFO. If inband is selected, Inband DTMF will also be detected as a fallback. Valid values are: • Digitized Inband RTP • SIP INFO Msg	`SIP INFO Msg`

Media Controller Parameters

15. On the EMPS navigation tree, expand the `Servers > IP Communication Server > <ServerName> > Mcu > MediaController` node.
16. If required, specify the media control that IPCS uses for Real-time Transport Protocol (RTP) streaming:
    - The default value is `NativeRTP`. If your deployment uses IPCS with Native RTP, continue at Step 17.

      For information about the codecs that the native IPCS supports, see the *Genesys Voice Platform 7.6 Reference Manual*.
    - If your deployment uses IPCS with a Convedia Media Sessions Markup Language (MSML)/Media Object Markup Language (MOML) media server, see Configuring IPCS for MxML servers in the EMPS, page 361.
    - If your deployment uses IPCS with Dialogic HMP, open the `MediaController` node for editing and, from the drop-down list, select `HMP Intel`. Skip the next step.

17. For a NativeRTP IPCS, configure the Servers > IP Communication Server > <ServerName> > Mcu > MediaController > NativeRTP node:
    a. Right-click the node and, from the shortcut menu, select Edit.
    b. Verify or enter values on the DTMF tab for the parameters listed in Table 56, and then click Save.

Table 56: NativeRTP Parameters

Tab	Parameter	Description	Example Value
DTMF	Inband DTMF Edge Detection	Specifies the edge on which dual-tone multi-frequency (DTMF) is to be detected. Valid values: • Leading Edge • Falling Edge	Leading Edge
	Inband DTMF Interdigit Silence	Specifies the minimum silence time, in milliseconds, between tones.	40
	Inband DTMF Minimum Duration	Specifies the minimum tone start time, in milliseconds, for detecting DTMF tones.	60

Note: You must perform additional configuration of the Mcu process to enable communication with Media Resource Control Protocol (MRCP) and MxML servers. For more information see “Enabling MRCP ASR and TTS” on page 391 and “Enabling MxML Servers” on page 358.

For more information about advanced Mcu configuration, see the chapter about IPCS in the *Genesys Voice Platform 7.6 Reference Manual*.

PageCollector Parameters

18. On the EMPS navigation tree, right-click Servers > IP Communication Server > <ServerName> > PageCollector.
19. From the shortcut menu, select Edit.
20. Verify or enter values on the General tab for the parameters listed in Table 57 on page 356, and then click Save.

Table 57: IPCS Page Collector Parameters

Tab	Parameter	Description	Example Value
General	Host Cache List	A comma-separated list of host names from which all static responses are cached at Page Collector. The cached files are used only if the network fetch fails.	`localhost`
	Proxy Server List	A comma-separated list of the URLs of proxy servers that are used to fetch or post a page. The format is: `http://<hostname>:<port>` Where: • `hostname`—Either the IP address or the FQDN of the proxy server. • `port`—(Optional) The port on which the proxy server listens.The default port number is `80`.	`http://<hostname>:<port>`
	Proxy Bypass List	A comma-separated list of host names or IP addresses for the web servers that will be contacted directly, bypassing the proxy server.	`dev.emps.adcc.alcatel.be, 10.10.10.200`

Table 57: IPCS Page Collector Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	HTTP Caching	Specifies the Hypertext Transfer Protocol (HTTP) caching behavior for CnInet. Valid values: • `Off`—Disables caching. • `On`—Enables caching. When enabled, caching is limited to maximum thresholds of 4096 MB and 16384 files. All of the CnInet cache-related files are stored under the `cn\data\CnCache` folder. There are two types of files: • **Index File**—There is only one index file, which is created at `cn\data\CnCache\index.dat.` The index file stores thumbnail data about the actual cached files, to enable a fast search. The data in the index file is stored in binary format. For each cached file, the corresponding thumbnail data in the index file consists of the URL, local file location, response headers, last access time, and so on. The index file is read into memory at the time of process startup. Thereafter, at periodic intervals and during shutdown, the in-memory image persists to the index file. During an HTTP operation, the index file is searched for the entry. If the entry is not found, the request is sent to the web server. If the entry is found, validation is performed according to the *RFC 2616 HTTP 1.1 specification,* to determine whether the cached entry should be returned to the client, or whether it should be sent to the web server. • **Cache Files**—Each response that is cachable is stored in a local file. The file location is `cn\data\CnCache\<server>\CACxx.tmp,` where `<server>` is the name of the web server (as it appears in the URL) from which the response was received, and `xx` is a random number. Each time a response is cached, the corresponding thumbnail entry is created in the index file.	`Off`

21. To verify that you can see and monitor the system processes from the Element Management System (EMS) GUI, enter the following URL in a web browser:

```
http://<VCS-hostname>:9810
```

End of procedure

Next Steps

- If your deployment includes Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) features, configure the `mcu > ASR` and `mcu > TTS` nodes. For more information, see Configuring IPCS or VCS for MRCP ASR in the EMPS, page 396 and Configuring IPCS or VCS for MRCP TTS in the EMPS, page 400.
- If your deployment uses MxML (Convedia) servers for enhanced media functionality, configure the `mcu > MediaController` node. For more information, see Configuring IPCS for MxML servers in the EMPS, page 361.
- After you have completed all the required IPCS configuration, start or restart the IPCS WatchDog. For information about starting WatchDog, see Starting/Restarting GVP in Normal mode (Windows), page 198 or Starting/Restarting GVP (Solaris), page 283.

Enabling MxML Servers

The IPCS integrates with Convedia servers through Media Sessions Markup Language (MSML) over Session Initiation Protocol (SIP) to provide enhanced media functionality. In the EMPS, Convedia servers are media controllers of the `MxML` type.

Table 58 summarizes the steps that are required to enable the use of MxML (Convedia) servers to communicate with other GVP components.

Table 58: Configuring MxML Servers

Objective	Related Procedures and Actions
1. Configure the media servers in the EMPS.	Configuring an MxML media server in the EMPS, page 359
2. Configure the media server groups.	Creating media server groups in the EMPS, page 360
3. Configure the IPCS `Mcu` process.	1. Configuring IPCS for MxML servers in the EMPS, page 361). 2. If all IPCS configuration has been completed, restart WatchDog on the IPCS host.

The following procedures provide detailed information about the steps to enable MxML media servers in your GVP deployment.

Procedure: Configuring an MxML media server in the EMPS

Start of procedure

1. Create the Media Server node:
   a. On the EMPS navigation tree, expand the Servers > Media Server node.
   b. Right-click SampleMediaSvr, and select Create a Copy.
   c. Click Copy.
   d. Enter the name of the new server node in the To Node text box—for example, Convedia.
2. Refresh the EMPS window to display the new node.
3. Expand the new node.
4. Right-click MediaSvrInfo, and then select Edit.
5. Verify or enter values on the General tab for the parameters listed in Table 59, and then click Save.

Table 59: Media Server Info Parameters

Tab	Parameter	Description	Example Value
General	Media Server URL	Specifies the URL to the Media Server machine. For example: hostname:port	MediaServerHost:1234
	Media Server Type	Specifies the Media Server type. Valid values: • Convedia • MRF	MRF

Table 59: Media Server Info Parameters (Continued)

Tab	Parameter	Description	Example Value

General (continued)	Features List	Specifies the features that the media server supports, separated by semicolons.	`pcma:8;pcmu:0;g723:4;g729:18`
			Note: If configured to use the Alcatel Media Resource Function (MRF) as the MxML server, IPCS will not support enhanced RTP codecs. The `Features List` parameter must be configured as:
			`pcmu:0;pcma:8;cpa;localbridge`

Warning! If you are integrating with Media Resource Point (MRP), IPCS must be configured work with the Alcatel Media Resource Function (MRF). The MRF does not support transcoding from one codec to another. In this setup, the g729, g723, and other enhanced RTP codecs are not supported unless the ASR or TTS servers and the MRF have the same common enhanced RTP codecs. The current MRCP ASR/TTS servers used in MRP support only g711 mu-law and g711a-law. Therefore, the MRP platform will support only the g711 mu-law and a-law.

End of procedure

Next Steps

- Add the server to a server group (see Creating media server groups in the EMPS).

Procedure: Creating media server groups in the EMPS

Purpose: To create the resource groups that the IPCS will use for enhanced media services through Convedia.

Prerequisites

- The individual servers have been created and configured in the EMPS (see Configuring an MxML media server in the EMPS, page 359).

Start of procedure

1. Create the server group node:
   a. On the EMPS navigation tree, right-click `Server Groups`, and then select `Add New Group`.
   b. In the `Group Name` field, enter the name of the new group—for example, `MediaServer_Grp1`.
   c. From the `Server Group Type` drop-down list, select `MEDIASVRGRP`.

   The `Available` list in the `Servers Selection` section is populated with the media servers that you configured previously (see Configuring an MxML media server in the EMPS, page 359).
2. Select the required media servers from the `Available` list, and move them to the `Selection` list box on the right.
3. Click `Save`.

End of procedure

Next Steps

- Configure the `Mcu` process in the IPCS. For more information, see Configuring IPCS for MxML servers in the EMPS.

Procedure: Configuring IPCS for MxML servers in the EMPS

Purpose: To configure the IPCS `Mcu` process to communicate with the MxML server(s) for media port allocation and de-allocation.

Prerequisites

- The media server group has been created in the EMPS. For more information, see Creating media server groups in the EMPS, page 360.
- WatchDog has been stopped on the IPCS host.

Start of procedure

1. On the EMPS navigation tree, right-click `Servers > IPCS > <ServerName> > Mcu > MediaController`.
2. From the `MediaController` drop-down list, select `MxML`.
3. Right-click `Servers > IPCS > <ServerName> > Mcu > MediaController > MxML`, and then select `Edit`.
4. Verify or enter values on the `General` tab for the parameters listed in Table 60, and then click `Save`.

Table 60: MxML Parameters

Tab	Parameter	Description	Example Value
General	Local SIP Port	Specifies the UDP port that will be used to listen for SIP messages.	`5070`
	Primary Media Server Group(s)	Specifies one or more Media Server group(s) that will be the primary resource used for any RTP media streaming. For more information about creating the groups, see Creating media server groups in the EMPS, page 360.	`Mediaserver_group1`
	Backup Media Server Group(s)	Specifies one or more Media Server group(s) that will be used if the resources from the primary group are unavailable.	`Mediaserver_group2`
	Out of Service Ping Interval (seconds)	Specifies the interval, in seconds, between pings to out-of-service servers. Valid values: `30-300` (seconds) Default value: `30` **Note:** For more information, see the *Genesys Voice Platform 7.6 Reference Manual*.	`30`

End of procedure

Next Steps

- If all IPCS configuration has been completed, start or restart WatchDog on the IPCS host.

Chapter

21 Configuring VCS in the EMPS

This chapter describes how to configure the Genesys Voice Platform (GVP) Voice Communication Server (VCS) component in the Element Management Provisioning System (EMPS).

Note: The VCS is available only for Windows installations.

This chapter contains the following sections:

Configuring VCS

This section describes how to configure the Voice Communication Server.

Procedure: Configuring VCS in the EMPS (Windows)

Summary

To configure the VCS, you must configure parameters for the following nodes:

- PopGateway process (`PopGateway1`)—see Step 3 on page 364
- PopGateway Route (`Route`)—see Step 6 on page 372
- PopGateway Call Progress Detection (`CPD`)—see Step 9 on page 379
- Call Progress Analysis (`CPA`)—see Step 12 on page 381
- Page Collector (`PageCollector`)—see Step 15 on page 384

Start of procedure

1. In a web browser, access the EMPS login page by entering the URL `http://<EMPS-hostname>:9810/spm/login.php`.
2. Log in to the EMPS as `Admin`, and enter your password.

PopGateway Parameters

3. On the EMPS navigation tree, expand the nodes `Servers > Voice Communication Server > <ServerName>`, and then right-click `PopGateway1`.
4. From the shortcut menu, select `Edit`.
5. Verify or enter values for the parameters under each tab listed in Table 61, and then click `Save`.

> Note: When configuring PopGateway parameters, be aware that, by default, each PopGateway has 100 physical threads. This means that each PopGateway can have a maximum of 100 concurrent calls. To bridge both inbound and outbound legs, both legs must be from the same PopGateway.
>
> To create the nodes for additional PopGateway processes, copy an existing `PopGateway` node and reconfigure its parameters as required.

Table 61: VCS PopGateway Parameters

Tab	Parameter	Description	Example Value
General	Log File	Specifies the log file for the PopGateway process.	`PopGateway1.log`
	Outbound Default ANI	Specifies the default Automatic Number Identification (ANI) that is used for outbound calls when no ANI is available.	`8880000000`
Telephony	Recording Clipped on DTMF	Specifies the number of bytes to clip when a recording is terminated on a dual-tone multi-frequency (DTMF) tone. Valid values: `0–32000` (bytes)	`0`

Table 61: VCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
Telephony (continued)	Ringback Filename	Specifies the file that is used instead of `Index File Name` to play the ringback tone. The file format is 8Khz PCM, and either MuLaw or ALaw depending on the region. The file must contain a single ring with the desired trailing silence, and it must be located in the `%CN_ROOT%\resources` directory. You can use this parameter to provide a customized ringback tone to the VCS. When a call lands on the VCS, the VCS plays this file to the caller while the call is in the alerting/proceeding state (that is, before the call is answered). If this parameter is undefined, the VCS plays the default ringback tone to the customer. **Notes:** You should record this file using ALaw for E1 and MuLaw for T1, with a sampling rate of 8KHz/s. The switch and the telephony signaling will determine whether the caller hears this ringback (some switches disable the outbound voice channel until the call is answered).	

Table 61: VCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
Telephony (continued)	Transaction Recording Resources	Specifies which Dialogic transaction recording resources are being used. The format is: `x:y-z [ x1:y1-z1,...]` Where: `x` = board number `y` = starting channel number `z` = ending channel number **Note:** If you are specifying channels in this parameter, you must not use these channels in the `Route > Channels` parameter. For more information about configuring the VCS for transactional recording, see the *Genesys Voice Platform 7.6 Reference Manual*.	`1:1-32,2:2-16`
	Number of retries on glare	Specifies the number of times that an outbound call will be re-attempted if it fails because of a glare condition (when both an incoming and an outgoing call request the same timeslot). When a glare condition occurs, the inbound call is given preference, and the outbound call is dropped.	1

Table 61: VCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
Telephony (continued)	Hangup Code	Specifies the hangup code to use whenever the call must be ended because of an error. Valid values: • Normal Unspecified (ISDN=31) • Unassigned Number (ISDN=01) • Normal Clearing (ISDN=16) • Channel Unacceptable (ISDN=06) • User Busy (ISDN=17) • Call Rejected (ISDN=21) • Destination Out of Order (ISDN=27) • Network Congestion (ISDN=42) • Requested Circuit/Channel Unavailable (ISDN=44)	Normal Unspecified (ISDN=31)
IVR	Primary DID Mapper	(Mandatory) Specifies the URL to the Dispenser mapping of DIDs to IVR Profiles (did.xml).	http://<FQDN of Dispenser>:9810/did_url_mappings/did.xml
	Backup DID Mapper	Specifies the backup URL to the Dispenser did.xml.	http://<FQDN of backup Dispenser>:9810/did_url_mappings/did.xml
	Primary Outbound DID Mapper	(Mandatory) Specifies the URL to the Dispenser mapping of DIDs to IVR Profiles for outbound calls ($reseller-name$_$customer-name$_$application-name$_OutboundDID.xml).	http://<FQDN of Dispenser>:9810/did_url_mappings/$reseller-name$_$customer-name$_$application-name$_OutboundDID.xml

Table 61: VCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
IVR (continued)	Backup Outbound DID Mapper	Specifies the backup URL to the Dispenser for outbound calls (`$reseller-name$_$customer-name$_$application-name$_OutboundDID.xml`).	`http://<FQDN of Dispenser>:9810/did_url_mappings/$reseller-name$_$customer-name$_$application-name$_OutboundDID.xml`
	Dispenser URL Fetch Timer (secs)	(Mandatory) Specifies the length, in seconds, of the fetch timeout that the PopGateway gives to the Dispenser URL. Valid values: `3–10` (seconds)	`3`
	Billing Server URL	(Mandatory) Specifies the Billing URL to which billing records should be posted. The format is: `http://<FQDN of EventC machine>/<path>/<script file>`.	`http://EMSRep_EventC.yourdomain.com:9810/billing/events.php`
	ASR Result Properties Access	Check box that specifies whether Automatic Speech Recognition (ASR) result properties can be accessed by the voice application.	Cleared
	TTS Fetch	The TTS fetch hint setting, which specifies whether TTS grammars are loaded as needed or in advance. Valid values: • `safe` (as needed) • `prefetch` (all are preloaded) Default value: `safe`	`safe`

Table 61: VCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
CPA	CPA Option	Enables or disables customized CPA values on the DM/V and JCT board. Valid values: • `EnableCpaDetectionDefault`—Enables CPA detection • `EnableCustomCpaDetectionSpringware`—Enables CPA detection for JCT boards • `EnableCustomCpaDetectionDMV`—Enables CPA detection for DM/V boards For more information about the CPA option, see the *Genesys Voice Platform 7.6 Reference Manual*. **Note:** For accurate tuning of CPA parameters, Genesys recommends that you also consult with Dialogic.	`EnableCpaDetectionDefault`
	CpaPamdOption	Specifies the desired speed and accuracy of answering machine detection. Valid values: • `AMDetectionQuick`—Quick look at connect circumstances. • `AMDetectionFull`—Quick and full evaluation of response. • `AMDetectionAccurate`—Slow and complete evaluation to calculate positive answering machine detection (PAMD). You can use this parameter with DM/V and JCT boards. **Note:** For accurate tuning of CPA parameters, Genesys recommends that you also consult with Dialogic.	`AMDetectionAccurate`

Table 61: VCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
CPA (continued)	Cpa Continuous No Signal	Specifies the maximum amount of silence, in milliseconds (ms), after cadence detection before NO_RINGBACK is returned. Valid values: 250–8000 (ms) Default value: 4000 You can use this parameter with DM/V and JCT boards. **Note:** For accurate tuning of call progress analysis (CPA) parameters, Genesys recommends that you also consult with Dialogic.	4000
	CpaFailTime	Specifies the maximum time to wait for positive answering machine detection (PAMD). Valid values: 100–800 (ms) Default value: 400 You can use this parameter with DM/V and JCT boards. **Note:** For accurate tuning of CPA parameters, Genesys recommends that you also consult with Dialogic.	400
	CpaMaxInterRing	Specifies the maximum amount of time, in milliseconds, to wait between consecutive ringback signals before determining that the call has been connected. Valid values: 250–2000 (ms) Default value: 800 You can use this parameter with JCT boards. **Note:** For accurate tuning of CPA parameters, Genesys recommends that you also consult with Dialogic.	800

Table 61: VCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
CPA (continued)	CpaMinRing	Specifies the minimum ring duration, in milliseconds, for PAMD. Valid values: `100–800` (ms) Default value: `190` You can use this parameter with JCT boards. **Note:** For accurate tuning of CPA parameters, Genesys recommends that you also consult with Dialogic.	`190`
	Cpa Qualification Template	Specifies the qualification template that is used for PAMD. Default value: `PAMD_QUALITMP` You can use this parameter with JCT boards. **Note:** For accurate tuning of CPA parameters, Genesys recommends that you also consult with Dialogic.	`PAMD_QUALITMP`

Table 61: VCS PopGateway Parameters (Continued)

Tab	Parameter	Description	Example Value
CPA (continued)	CpaStartDelay	Specifies the amount of time, in milliseconds, to wait after dialing, before starting cadence, frequency, or positive voice detection. Valid values: `2–300 (ms)` Default value: `25` You can use this parameter with JCT boards. **Note:** For accurate tuning of CPA parameters, Genesys recommends that you also consult with Dialogic.	`25`
	Disable Custom Tones before CPA	Specifies whether custom tones will be deleted unconditionally before Call Progress Analysis (CPA) is performed. You can use this parameter with JCT boards. **Note:** For accurate tuning of CPA parameters, Genesys recommends that you also consult with Dialogic.	Cleared

PopGateway Route Parameters

6. On the EMPS navigation tree, right-click the `Servers > Voice Communication Server > <ServerName> > PopGateway > Route1` node, and then select `Edit`.
7. Verify or enter values for the parameters on each tab listed in Table 62, and then click `Save`.

   For a summary of the essential parameters that you must configure for your switch configuration, see “Configuring Route Protocols” on page 387.

Table 62: VCS PopGateway Route Parameters

Tab	Parameter	Description	Example Value
General	Route Type	(Mandatory) Specifies the call direction of the route. Valid values: • `Inbound`—Handles only inbound calls. • `Outbound`—Handles only outbound calls. • `Inbound & Outbound`—Handles both inbound and outbound calls. If both an incoming call and an outgoing call request the same port (resulting in a glare condition), the incoming call is given preference. **Note:** The `Inbound & Outbound` route type is supported only on Integrated Digital Services Network [ISDN]. If you set the `Route Type` to `Inbound & Outbound`, ensure that you select a compatible `Signaling Type`.	`Inbound`
	Signaling Type	(Mandatory) Specifies the signaling type. Valid values: • `T1-ISDN (PRI)` • `Analog` • `E1-ISDN (PRI)` • `T1-RobbedBit` • `E1-CAS`	`T1-ISDN (PRI)`

Table 62: VCS PopGateway Route Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	Channels	(Mandatory) Specifies the ports for this route. The format is `Span:PortRange`. **Notes:** • If you specified channels in the `Transaction Recording Resources` parameter, you must not use those same channels in this parameter. • Do not add extra spaces in the middle of the parameter value. Empty spaces are allowed only in the leading and trailing portions. • EMPS validates the value of this parameter to ensure that the range of channels is unique and that channels do not overlap within the same span. Validation occurs if the node name starts with *Route* and ends with a number—for example, `Route 1`, `Route2` (but not `Route_1`, `PGRoute1`).	`1:1-23`
	Network Type	(Mandatory) Specifies the type of telephony network to which the route is connected. Valid values: • `PSTN` • `Enterprise (PBX/ACD)`	`PSTN`
	Max Digits to Dial	(Mandatory) Specifies the number of digits that should be dialed out. • If the `Network Type` parameter is set to `PSTN`, this parameter must be set to `7`, `10`, or `11`. • If `Network Type` is set to `Enterprise (PBX/ACD)`, this parameter can have any value. • If the value of this parameter is `0`, then there is no maximum. • If the value of this parameter is missing or invalid, the default value `7` is used. **Note:** for more information, see the *Genesys Voice Platform 7.6 Reference Manual*.	`7`

Table 62: VCS PopGateway Route Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	ISDN Numbering Type	Used for outbound ISDN routes to determine the encoding of the Calling/Called Party Information Element (IE) Numbering Type in the outgoing setup. Valid values: • 0x00—Unknown (Dialogic EN_BLOC_NUMBER) • 0x01—International Number (Dialogic INTL_NUMBER) • 0x02—National Number (Dialogic NAT_NUMBER) • 0x04—Subscriber Number (Dialogic LOC_NUMBER)	0x02
	ISDN Table	Specifies the URL containing ISDN table data.	
	ISDN Numbering Plan	Used for outbound ISDN routes, to determine the encoding of the Calling/Called Party IE Numbering Plan in the outgoing setup. Valid values: • 0x00—Unknown (Dialogic UNKNOWN_NUMB_PLAN) • 0x01—ISDN E.164 (Dialogic ISDN_NUMB_PLAN) • 0x02—Telephony E.163 (Dialogic TELEPHONY_NUMB_PLAN) • 0x09—Private (Dialogic PRIVATE_NUMB_PLAN)	0x01
	Route Description	Specifies the user name for this route.	Inbound Route
	Enable Transaction Record	Specifies whether transaction recording is enabled. **Note:** For more information about configuring the VCS for transactional recording, see the *Genesys Voice Platform 7.6 Reference Manual*.	Cleared

Table 62: VCS PopGateway Route Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	For CSP: Media Resource Board to use	Specifies, for Continuous Speech Processing (CSP), which route number the Automatic Speech Recognition (ASR) engine uses. If no value is specified, this parameter defaults to the same board as the network port. Any other value indicates the board number to use for CSP resources. For ISDN JCT boards, the board that you configure for CSP must be different than the board for the network port. **Note:** The value should be a single value, not a comma-separated list. Routes with this parameter should be on a single board—for example, do not use Ports=`1:1-4, 2:3-5`.	`2`
	Area Code of the Trunk	Specifies the area code of the trunk. Default value: `000`. If the `Network Type` is set to `PSTN,` the system administrator must provide a value; otherwise all outbound calls will be considered long distance. If `Network Type` is set to `Enterprise,` this value is ignored.	`000`
	Network Specific Facility Service	Used for outbound ISDN routes, to determine the encoding of the network-specific facility IE in the outgoing setup. If the value is `0xFF,` the network-specific facility service IE is not encoded. Otherwise, the value is used to encode the IE with the specified server. The values are specific to your service provider—for example, `3 - Megacom.` For more information, see the ISDN specifications.	`0xFF`

Table 62: VCS PopGateway Route Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	Type of Two Channel Transfer	Specifies the two-channel transfer type. Valid values: • None • nortelRLT • ECTexplicit • ECTexplicit_nz • ECTexplicit_UK	None
	Dial Prefix	Specifies the dial prefix. If the call is not in the home Numbering Plan Area (NPA), or area code, the VCS prepends this to the number that is to be dialed. This parameter is used only when the Network Type parameter is set to PSTN.	1
	One Channel Transfer Type	Specifies the One Channel Transfer Types supported. Valid values: • None • DialogicBlindXfer—invokes a Dialogic blind transfer. Dialogic performs a hookflash, dials out the dialed number identification service (DNIS), and hangs up the call. This is currently supported on both DMV and JCT boards. Default value: None	None
CPD	Enable Genesys CPD Library	Specifies whether to make outgoing calls by using Genesys Call Progress Detection (CPD) library.	Cleared
	Range of Directory Numbers	Specifies the directory number range for the route. Separate the directory numbers with dashes or commas. **Note:** The directory number must equal the number of ports in the route. For example, if you have 23 ports in the route, you must have 23 directory numbers.	101-110, 115, 120-130

Table 62: VCS PopGateway Route Parameters (Continued)

Tab	Parameter	Description	Example Value
Robbed bit T1	Max Digits to Receive in Overlap Receive Mode	Specifies the maximum number of digits to receive in overlap receive mode (ANI + DNIS + delimiters).	`0`
	T1rb ANI/DNIS Order	Specifies how T1 gives ANI/DNIS. This is valid only when the signaling protocol is T1 Robbed Bit. Valid values: • `No ANI or DNIS` • `DNIS only` • `DNIS followed by ANI` • `ANI followed by DNIS` **Note:** When set to `No ANI or DNIS`, the `gc_getDNIS` function is not called.	1
	T1rb Protocol File	Specifies which Dialogic T1 configuration file to use. This field is mandatory for T1-Robbed Bit signaling. Valid options vary according to board type: **DM/V:** • `dmv`—For all DM/V-A boards. **JCT:** • `us_mf_io`—For generic US T1 Robbed Bit. Make sure that you are using a T1 trunk that is directly connected to a North American carrier (not through a lab tandem system). • `us_mf_loop_io`—For lab loopback testing. For additional available protocols, see the *GlobalCall Country Dependent Parameters Reference* document, which is provided with the Dialogic GlobalCall installation.	`dmv`
	T1rb Remove ANI/DNIS Delimiter	Specifies whether ANI/DNIS delimiters should be removed. This is valid only when the signaling protocol is T1 Robbed Bit.	Selected

Table 62: VCS PopGateway Route Parameters (Continued)

Tab	Parameter	Description	Example Value
Robbed bit T1 (continued)	ANI DNIS Delimiter	Specifies the character that separates ANI from DNIS in the incoming call data—for example, # or *.	#
	Confirmation with CC	Specifies when GVP confirms the call with CC. Choices are: • BeforeAnswer • AfterAnswer **Note:** Select AfterAnswer when using groundstart protocol, otherwise select the default value BeforeAnswer.	BeforeAnswer

8. Create additional routes if required.

   a. Copy an existing Route node.

      When you name the new route, observe the following rules:

      - The format of the name is Route*n,* where *n* is the sequential route number. Follow the spelling exactly.
      - Routes must be numbered sequentially. For example, Route1 must be followed by Route2, and then Route3, and so on.

      Any misspelled or out-of-sequence routes will not be saved.

   b. Configure the new route node (see Step 7 on page 372).

   c. Repeat as necessary to create multiple routes.

PopGateway CPD Parameters

9. On the EMPS navigation tree, right-click Servers > Voice Communication Server > <ServerName> > PopGateway > CPD.

10. From the shortcut menu, select Edit.

11. Verify or enter values on the General tab for the parameters listed in Table 63, and then click Save.

Table 63: VCS PopGateway CPD Parameters

Tab	Parameter	Description	Example Value
General	Name of CPD DLL	Specifies the name of the CPD dynamic link library (DLL).	cpdlib_MD.dll
	IP Address of Primary TServer	Specifies the IP address of the primary TServer.	10.10.10.10

Table 63: VCS PopGateway CPD Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	Primary TServer Listening Port	Specifies the port at which the primary TServer accepts requests.	5678
	IP Address of Backup TServer	Specifies the IP address of the backup TServer.	10.10.10.10
	Backup TServer Listening Port	Specifies the port at which the backup TServer accepts requests.	1234
	CPD Reconnect Timeout for TServer	Specifies the reconnect timeout for TServer, in milliseconds. Default value: 20000	20000
	CPD Calls Made by TServer	When the Genesys CPD library is used, specifies whether TServer makes outgoing calls.	Cleared
	FAX2 Tone as Answering Machine	Specifies whether the CPD library should accept the FAX2 tone as answering machine.	Cleared
	CPD Off-hook Delay	When the Genesys CPD library is used, specifies the length of the off-hook delay, in milliseconds. This is the absolute value of the timeout between going off-hook and making a call by TServer. A negative value specifies to set the channel off-hook first, and then dial a number. A positive value specifies to dial a number first, and then set the channel off-hook. Default value: 0 (ms) **Note:** Used only if the CPD Calls Made by TServer parameter is checked.	0

Table 63: VCS PopGateway CPD Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	CPD Postconnect Priority	Specifies whether priority should be given to TServer or Dialogic in case of conflicting CPD results. Values are: • `TServer` • `Dialogic`	`TServer`
	CPD Preconnect Priority	Specifies whether priority is given to TServer or Dialogic in the event of conflicting CPD results. Valid values: • `TServer` • `Dialogic`	`TServer`
	CPD Calls Cleared by TServer	When the Genesys CPD library is used, specifies whether TServer clears outgoing calls.	Cleared
	Wait for Offhook Confirmation	If checked, the CPD Library waits for an offhook confirmation event from TServer before dialing. **Note:** Used only if the `CPD Off-hook Delay` parameter is set to a negative value.	Cleared

CFA Parameters

12. On the EMPS navigation tree, right-click `Servers > Voice Communication Server > <ServerName> > CFA`.
13. From the shortcut menu, select `Edit`.
14. Verify or enter values on the `General` tab for the parameters listed in Table 64, and then click `Save`.

Table 64: VCS CFA Parameters

Tab	Parameter	Description	Example Value
General	Primary CTA URL	Specifies the URL to use if transfers are to be performed through an external gateway. If the `Transfer Type` parameter is set to `External Transfer`, then, when it is time to perform a transfer, GVP contacts the Primary CTA URL to complete the transfer. **Note:** This parameter is used only if the `Transfer Type` is set to `External Transfer`.	`http://<CTA Server>/webnotify.asp?notifyprocess=CTA`
	DID.xml URL in case of failures	Specifies the URL to use if the Genesys Framework provides a DNIS that has not been provisioned on the GVP.	`http://qadid.qa.genesyslab.com/did_url_mappings/Windows/$did$.xml`
	Transfer Type	Specifies the type of transfer on the platform. Valid values: • `Transfer on platform` • `Transfer through CTI` • `External Transfer`	`Transfer on platform`
	Application URL in case of failures	Specifies the URL to use if the Call Flow Assistant (CFA) fails to contact the IVR Server Client to fetch the DNIS at call setup time. This URL will also be used when the IVR Server Client is not accessible to perform a computer telephony integration (CTI) transfer.	`http://$empsservername$/emps/database/dids/$did$.xml`
	Backup CTA URL	Specifies the URL that GVP uses if it fails to contact the Primary CTA URL at call setup time.	`http://<CTA Server>/webnotify.asp?notifyprocess=CTA`
	URL for $did$.xml file	Specifies the URL that is used to fetch the `$did$.xml` file.	`http://(Ini Dispenser Machine)/$did$.xml`

Table 64: VCS CFA Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	I-Server Client URL	Specifies the IVR Server Client URL that is used to fetch the ANI/DNIS from the IVR Server in a behind-the-switch configuration. This URL is also used for performing CTI transfers if the `Transfer Type` is set to `Transfer through CTI`. **Note:** This parameter applies only to the primary IVR Server Client. A backup IVR Server Client URL applies only to an IVR Server that is running in either `InFront` mode or `Network` mode, and it is set during customer provisioning.	`http://localhost/WebNotify.asp?NotifyProcess=ISvrClient`
	Default DNIS	Specifies the default DNIS that will be used if the DNIS from CTI is not received.	`1234`
	GVP Success URL	Specifies the URL used to fetch the actual `did.xml` file in a behind-the-switch mode. This URL should point to the Dispenser directory where the actual `did` files are stored.	`http://$empsservername$/emps/database/dids/$did$.xml`
	Use SCP Gateway For ANI & DNIS	Reserved for future use.	NO

Table 64: VCS CFA Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	Use CTI Client For ANI & DNIS	Specifies whether to fetch the ANI and DNIS from the CTI client. Valid values: • 0—Disable • 1—Enable **Note:** This parameter is typically enabled when GVP is configured in the behind-the-switch mode.	0
	ReRoute Wait Timeout (in sec)	Specifies the amount of time, in seconds, that the platform waits before ending the call if the agent leg drops without initiating a reroute. This parameter is valid only for applications that have rerouting enabled. Valid values: 1–10000 Default value: 5.	5

Page Collector Parameters

15. On the EMPS navigation tree, right-click Servers > Voice Communication Server > <ServerName> > PageCollector.
16. From the shortcut menu, select Edit.
17. Verify or enter values on the General tab for the parameters listed in Table 65, and then click Save.

Table 65: VCS Page Collector Parameters

Tab	Parameter	Description	Example Value
General	Host Cache List	A comma-separated list of host names from which all static responses are cached at Page Collector. The cached files are used only if the network fetch fails.	`localhost`
	ProxyServer List	A comma-separated list of the URLs of proxy servers that are used to fetch or post a page. The format is: `http://<hostname>:<port>` Where: • `hostname`—Either the IP address or the FQDN of the proxy server. • `port`—(Optional) The port on which the proxy server listens.The default port number is `80`.	`http://<hostname>:<port>`

Table 65: VCS Page Collector Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	Proxy Bypass List	A comma-separated list of host names or IP addresses for the web servers that will be contacted directly, bypassing the proxy server.	`10.10.10.10,10.10.10.11`
	HTTP Caching	Specifies the Hypertext Transfer Protocol (HTTP) caching behavior for CnInet. Valid values: • `Off`—Disables caching. • `On`—Enables caching. When enabled, caching is limited to maximum thresholds of 4096 MB and 16384 files. All of the CnInet cache-related files are stored under the `cn\data\CnCache` folder. There are two types of files: • **Index File**—There is only one index file, which is created at `cn\data\CnCache\index.dat.` The index file stores thumbnail data about the actual cached files, to enable a fast search. The data in the index file is stored in binary format. For each cached file, the corresponding thumbnail data in the index file consists of the URL, local file location, response headers, last access time, and so on. The index file is read into memory at the time of process startup. Thereafter, at periodic intervals and during shutdown, the in-memory image persists to the index file. During an HTTP operation, the index file is searched for the entry. If the entry is not found, the request is sent to the web server. If the entry is found, validation is performed according to the *RFC 2616 HTTP 1.1 specification,* to determine whether the cached entry should be returned to the client, or whether it should be sent to the web server. • **Cache Files**—Each response that is cachable is stored in a local file. The file location is `cn\data\CnCache\<server>\CACxx.tmp,` where `<server>` is the name of the web server (as it appears in the URL) from which the response was received, and `xx` is a random number. Each time a response is cached, the corresponding thumbnail entry is created in the index file.	`Off`

18. To verify that you can see and monitor the system processes from the Element Management System (EMS) GUI, enter the following URL in a web browser:

```
http://<VCS-hostname>:9810
```

End of procedure

Next Steps

- Perform additional configuration on the routes as required. For more information, see "Configuring Route Protocols".
- If your deployment includes Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) features, configure the `PopGateway > ASR` and the `TTS_MRCP` nodes. For more information, see Configuring IPCS or VCS for MRCP ASR in the EMPS, page 396 and Configuring IPCS or VCS for MRCP TTS in the EMPS, page 400.
- After you have completed all the required VCS configuration, restart the VCS WatchDog. For information about starting WatchDog, see Starting/Restarting GVP in Normal mode (Windows), page 198 or Starting/Restarting GVP (Solaris), page 283.

Configuring Route Protocols

This section describes the EMPS parameters and Dialogic configuration files that you must configure for the following signaling protocols, as required for your switch configuration:

- ISDN
- T1-Robbed Bit/E1-CAS/R2MFC (see page 388)
- T1/E1 Answer Supervision (see page 388)
- Groundstart protocol for T1-Robbed Bit (see page 389)

Configuring ISDN

For each ISDN route, make sure that you set the following parameters in the EMPS on the `Servers > Voice Communication Server > <servername> > PopGateway > Route` node:

- `Signaling Type`
- `Network Specific Facility Service`
- `ISDN Numbering Type`
- `ISDN Numbering Plan`

Obtain the values for the parameters from either your carrier or your telecom division.

For more information about the parameters, see Table 62 on page 373.

Configuring T1-Robbed Bit/E1-CAS/R2MFC

For each T1-Robbed Bit, E1-CAS, or R2MFC route, make sure that you set the following parameters in the EMPS on the Servers > Voice Communication Server > <servername> > PopGateway > Route node:

- Signaling Type
- T1rb Protocol File
- T1rb ANI/DNIS Order
- T1rb Remove ANI/DNIS Delimiter

For more information about the required parameters, see Table 62 on page 373.

For T1-Robbed Bit routes on which you want to use groundstart protocol, see also “Configuring Groundstart Protocol for T1-Robbed Bit” on page 389.

For information about additional changes you may need to make to the Dialogic configuration files, see “Additional Configuration for Non-ISDN” on page 493

Configuring T1/E1 Answer Supervision

For each T1-Robbed Bit or E1-CAS route that you want to configure for Answer Supervision, configure the AnswerSupervisionType parameter in the EMPS on the Servers > Voice Communication Server > <servername> > PopGateway > Route node, as described in Configuring the VCS for T1/E1 Answer Supervision in the EMPS.

Procedure:
Configuring the VCS for T1/E1 Answer Supervision in the EMPS

Prerequisites

- The other required parameters for a T1-Robbed Bit or E1-CAS route have been configured (see Configuring T1-Robbed Bit/E1-CAS/R2MFC).

Start of procedure

1. On the EMPS navigation tree, right-click the Servers > Voice Communication Server > <servername> > PopGateway > Route node, and select Edit.
2. Click Add New Attribute.

3. Enter the following values in the text boxes that appear:
   - Parameter Name: `AnswerSupervisionType`
   - Parameter Value: `Default` or `CPA`
     - — `Default` = Normal signaling information is to be used while making an outbound call.
     - — `CPA` = CPA is to be done by analyzing the audio on the line while making an outbound call.

End of procedure

Configuring Groundstart Protocol for T1-Robbed Bit

To use groundstart protocol on T1-Robbed Bit, modify the PDK configuration files on the VCS on which the route is configured.

pdk.cfg File

On each VCS that uses groundstart protocol on T1-Robbed Bit, ensure that the `pdk.cfg` file includes the following line:

```
board 0 fcdfile ml2_dsa_cas.fcd pcdfile ml2_dsa_cas.pcd variant
pdk_us_ls_fxs_io.cdp
```

pdk_us_ls_fxs_io.cdp File

On each VCS that uses groundstart protocol on T1-Robbed Bit, ensure that the `pdk_us_ls_fxs_io.cdp` file is configured with the feature parameters that are required for your configuration and environment.

GVP supports the following features:

- DNIS and ANI after start
- CPA after answer for Network Announcements
- CPA after answer for Busy
- CPA after answer for Ring No Answer
- CPA after answer for voice
- Label Routing

For an example of a file that illustrates the use of various feature parameters, see “Sample CDP File for US Loopstart FXS Protocol Variant” on page 497.

Chapter

22 Configuring MRCP ASR and TTS in the EMPS

This chapter describes the configuration steps that you must perform in the Element Management Provisioning System (EMPS) to enable the Media Resource Control Protocol (MRCP) Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) features in Genesys Voice Platform (GVP).

This chapter contains the following section:

Enabling MRCP ASR and TTS

This section describes how to configure MRCP ASR and TTS, for both Solaris and Windows.

Table 66 summarizes the steps that are required to enable the MRCP servers to communicate with other GVP components.

Table 66: Configuring MRCP ASR and TTS

Objective	Related Procedures and Actions
1. Configure the speech servers in the EMPS.	• For MRCP ASR: Configuring an MRCP ASR server in the EMPS, page 392 • For MRCP TTS: Configuring an MRCP TTS server in the EMPS, page 394
2. Configure the speech server groups.	Configuring speech server groups in the EMPS, page 395

Table 66: Configuring MRCP ASR and TTS (Continued)

Objective	Related Procedures and Actions
3. Configure the IPCS or VCS for ASR and TTS.	**1.** Stop WatchDog on the IPCS or VCS host. **2.** Configure the IPCS or the VCS for ASR (see Configuring IPCS or VCS for MRCP ASR in the EMPS, page 396). **3.** Configure the IPCS or the VCS for TTS (see Configuring IPCS or VCS for MRCP TTS in the EMPS, page 400). **4.** If all IPCS or VCS configuration has been completed, restart WatchDog on the IPCS or VCS host.
4. Verify that you can see and monitor the system processes from the Element Management System (EMS) GUI.	Enter the following URL in a web browser: `http://<VCS-hostname>:9810`

The following procedures provide detailed information about the steps to enable MRCP ASR and TTS in your GVP deployment.

Procedure:
Configuring an MRCP ASR server in the EMPS

Start of procedure

1. Create the MRCP ASR server node:
   a. On the EMPS navigation tree, expand the `Servers > MRCP ASR Server` node.
   b. Right-click one of the following sample servers, and select `Create a Copy`:
      - For a SpeechWorks Media Server (SWMS), select `SampleASRServerSWMS`.
      - For a Nuance Speech Server, select `Sample ASRServerNSS`.
      - For any other supported speech server, select `Sample ASRServer`.

      The sample servers are partially preconfigured, for convenience.
   c. Click `Copy`.
   d. Enter the name of the new server node—for example, `ASR_Server1`.
2. Refresh the EMPS window to display the new node.
3. Expand the new node.
4. Right-click `ASRInfo`, and then select `Edit`.
5. Verify or enter values on the `General` tab for the parameters listed in Table 67, and then click `Save`.

Table 67: MRCP ASR Server Parameters

Tab	Parameter	Description	Example Value
General	Vendor Specific Parameters	A comma-separated list of key-value pairs that specify the vendor-specific parameters that will be sent to this MRCP server.	`swi.rec.applicationName=$Reseller$_$Customer$_$Application$`
	Hotword Support	Specifies whether your server supports Hotword. The default is set to `None`. Choices are: • `Vendor Specific Parameters`—Applies only to servers that support Hot Word through vendor specific parameter Recognition-Mode on MRCPv1. For example, SWMS supports this parameter. • `None`—Applies to all other servers that do not support Hot Word.	`Vendor Specific Parameters`
	MRCP ASR Server Vendor Name	Specifies the name of the MRCP ASR Vendor **Note:** For more information about configuring additional ASR vendor names, see the *Genesys Voice Platform 7.6 Reference Manual*.	`MRCP`
	Grammar Caching Flag	Specifies whether the underlying MRCP server supports grammar caching.	Cleared
	MRCP ASR Server URL	Specifies the URL to the MRCP ASR Server machine.	`rtsp://<MRCP ASR Server host name>:4900/media/speechrecognizer/`

End of procedure

Next Steps

- Add the server to a server group. For more information, see Configuring speech server groups in the EMPS.

Procedure: Configuring an MRCP TTS server in the EMPS

Start of procedure

1. Create the MRCP TTS server node:
   a. On the EMPS navigation tree, expand the `Servers > MRCP TTS Server` node.
   b. Right-click `SampleTTSServer`, and select `Create a Copy`.
   c. Click `Copy`.
   d. Enter the name of the new node—for example, `TTS_Server1`.
2. Refresh the EMPS window to display the new node.
3. Expand the new node.
4. Right-click `TTSInfo`, and then select `Edit`.
5. Verify or enter values on the `General` tab for the parameters listed in Table 68, and then click `Save`.

Table 68: MRCP TTS Server Parameters

Tab	Parameter	Description	Example Value
General	MRCP TTS Server URL	Specifies the URL to the MRCP TTS Server machine.	`rtsp://<MRCP TTS Server host name>:4900/media/speechsynthesizer/` **Note:** This example is specific to SWMS.
	MRCP TTS Server Vendor Name	Specifies the name of the MRCP TTS Server vendor. **Note:** For information about how to configure additional TTS vendor names, see the *Genesys Voice Platform 7.6 Reference Manual*.	`MRCP`

End of procedure

Next Steps

- Add the server to a server group. For more information, see Configuring speech server groups in the EMPS.

Procedure: Configuring speech server groups in the EMPS

Purpose: To create the resource groups that the IPCS or VCS will use for MRCP ASR and TTS services.

You must create separate groups of MRCP ASR and TTS resources. Repeat this procedure as needed to create the groups that are required in your deployment.

Prerequisites

- The individual servers have been created and configured in the EMPS. For more information, see:
  - Configuring an MRCP ASR server in the EMPS, page 392
  - Configuring an MRCP TTS server in the EMPS, page 394

Start of procedure

1. Create the server group node:
   a. On the EMPS navigation tree, right-click `Server Groups`, and then select `Add New Group`.
   b. In the `Group Name` field, enter the name of the new group—for example, `ASR_Grp1` or `TTS_Grp1`.
   c. From the `Server Group Type` drop-down list, select the type of server:
      - For MRCP ASR, select `MRCPASR`.
      - For MRCP TTS, select `MRCPTTS`.

      The `Available` list in the `Servers Selection` section is populated with the servers of that type that you configured previously (see Prerequisites).
2. Select the required speech servers from the `Available` list, and move them to the `Selection` list box on the right.
3. Click `Save`.

End of procedure

Next Steps

- Configure the IPCS or the VCS. For more information, see Configuring IPCS or VCS for MRCP ASR in the EMPS, page 396 and Configuring IPCS or VCS for MRCP TTS in the EMPS, page 400.

Procedure: Configuring IPCS or VCS for MRCP ASR in the EMPS

Purpose: To configure the IPCS Mcu process or VCS PopGateway process to communicate with the MRCP ASR server(s).

Prerequisites

- The ASR server groups have been created in the EMPS. For more information, see Configuring speech server groups in the EMPS, page 395.

Start of procedure

1. On the EMPS navigation tree, access the ASR node for editing:
   - For IPCS, right-click Servers > IPCS > <ServerName> > Mcu > ASR, and then select Edit.
   - For VCS, right-click Servers > Voice Communication Server > <ServerName> > PopGateway> ASR, and then select Edit.
2. From the ASR Platform drop-down list, select MRCP.
3. Expand the ASR node.
4. Right-click the ASR > MRCP node, and then select Edit.
5. Verify or enter values for the parameters under each tab listed in Table 69, and then click Save.

Table 69: MRCP ASR Server Configuration Parameters

Tab	Parameter	Description	Example Value
General	Primary MRCP ASR Server Group(s)	Specifies the primary group of ASR servers for this IPCS or VCS. For more information about creating the groups, see Configuring speech server groups in the EMPS, page 395.	MRCPASR_GRP1
	Backup MRCP ASR Server Group(s)	Specifies the backup group of ASR Servers for this IPCS or VCS.	MRCPASR_GRP2
	DEFINE GRAMMAR Response Timeout	Specifies the amount of time, in milliseconds, that the platform waits for a DEFINE-GRAMMAR response from the MRCP server before timing out. Valid values: 1000-86400000 Default value: 5000	5000
	RTP port range	Specifies the port range for Real-time Transport Protocol (RTP). (Applicable only for Windows deployments with VCS.)	500000-510000
	Enable Utterance Capture Parameter	Specifies the string containing the vendor-specific parameter that is sent to the server in order to enable utterance capturing. (Required only for the ASR Log Manager system.)	swirec_suppress_waveform_logging=0 (utterance capture enabled for the supported speech servers)

Table 69: MRCP ASR Server Configuration Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	Disable Utterance Capture Parameter	Specifies the string containing the vendor-specific parameter that is sent to the server to disable utterance capturing. (Required only for the ASR Log Manager system.)	`swirec_suppress_waveform_logging=1` (utterance capture disabled for the supported speech servers)
	Out of Service Ping Interval (seconds)	Specifies the interval, in seconds, between pings to out-of-service servers. Valid values: `30-300` (seconds) Default value: `30` **Note:** For more information, see the *Genesys Voice Platform 7.6 Reference Manual*.	`30`
Traps	MRCP Error Response Traps	Specifies the MRCP error responses that result in a trap, provided the originating request is enabled to send traps. Enter a comma-separated list of values and/or ranges. Valid values: `401-499,201` Default value: `405,407`	`405,407`
	MRCP Error Event Traps	Specifies the completion causes for `RECOGNITION-COMPLETE` MRCP events that will result in a trap. Enter a comma-separated list of values and/or ranges. Valid values: `001-010` Default value: `004-006,009,010`	`004-006,009,010`
	DEFINE GRAMMAR Request Failure Trap	Check box that specifies whether a `DEFINE-GRAMMAR` request timeout/connection failure results in a trap.	Selected

Table 69: MRCP ASR Server Configuration Parameters (Continued)

Tab	Parameter	Description	Example Value
Traps (continued)	DEFINE GRAMMAR Error Response Trap	Check box that specifies whether an error response to a `DEFINE-GRAMMAR` request results in a trap, provided that the corresponding `MRCP Error Response Trap` is enabled.	Selected
	SET PARAMS Request Failure Trap	Check box that specifies whether a `SETPARAMS` request timeout/connection failure results in a trap.	Cleared
	SET PARAMS Error Response Trap	Check box that specifies whether an error response to a `SET-PARAMS` request results in a trap, provided the corresponding `MRCP Error Response Trap` is enabled.	Cleared
	RECOGNIZE Request Failure Trap	Check box that specifies whether a `RECOGNIZE` request timeout/connection failure results in a trap.	Selected
	RECOGNIZE Error Response Trap	Check box that specifies whether an error response to a `RECOGNIZE` request results in a trap, provided the corresponding `MRCP Error Response Trap` is enabled.	Selected
	RECOGNITION START TIMERS Request Failure Trap	Check box that specifies whether a `RECOGNITION-START-TIMERS` request timeout/connection failure results in a trap.	Cleared
	RECOGNITION START TIMERS Error Response Trap	Check box that specifies whether an error response to a `RECOGNITION-START-TIMERS` request results in a trap, provided the corresponding `MRCP Error Response Trap` is enabled.	Cleared

Table 69: MRCP ASR Server Configuration Parameters (Continued)

Tab	Parameter	Description	Example Value
Traps (continued)	STOP Request Failure Trap	Check box that specifies whether a `STOP` request timeout/connection failure results in a trap.	Cleared
	STOP Error Response Trap	Check box that specifies whether an error response to a `STOP` request results in a trap, provided the corresponding `MRCP Error Response Trap` is enabled.	Cleared

End of procedure

Next Steps

- If required, configure the IPCS or the VCS for TTS. For more information, see Configuring IPCS or VCS for MRCP TTS in the EMPS, page 400.
- If all IPCS or VCS configuration has been completed, restart WatchDog on the IPCS or VCS host.

Procedure: Configuring IPCS or VCS for MRCP TTS in the EMPS

Prerequisites

- The TTS server groups have been created in the EMPS. For more information, see Configuring speech server groups in the EMPS, page 395.

Start of procedure

1. On the EMPS navigation tree, access the `TTS MRCP` node for editing:
   - **For IPCS:**
     i. Right-click `Servers > IPCS > <ServerName> > Mcu > TTS`.
     ii. From the `Platform` drop-down list, select `MRCP`.
     iii. Specify the `Max Text Size per request in Bytes`. For more information about this parameter, see the description in Table 70 on page 401.
     iv. Right-click `Servers > IPCS > <ServerName> > Mcu > TTS > MRCP`, and then select `Edit`.

- **For VCS:**
  - **i.** Right-click `Servers > Voice Communication Server > <ServerName> > TTS MRCP`.
  - **ii.** Select `Edit`.

2. Verify or enter values for the parameters under each tab listed in Table 70, and then click `Save`.

Table 70: TTS Server Configuration Parameters

Tab	Parameter	Description	Example Value
General	Primary MRCP TTS Server Group(s)	Specifies the primary group of TTS servers for this IPCS.	`MRCPTTS_SWMS_GRP1`
	Backup MRCP TTS Server Group(s)	Specifies the backup group of TTS Servers for this IPCS.	`MRCPTTS_SWMS_GRP2`
	Out of Service Ping Interval (seconds)	Specifies the interval, in seconds between pings to out-of-service servers. Valid values: `30-300` (seconds) Default value: `30` **Note:** For more information, see the *Genesys Voice Platform 7.6 Reference Manual*.	`30`
	Max Text Size per request in Bytes	Specifies the maximum text size (in bytes) per request.	`10000`
Traps	MRCP Error Response Traps	Specifies the MRCP error responses that result in a trap, provided the originating request is enabled to send traps. Enter a comma separated list of values and/or ranges. Valid values: `401-499,201` Default value: `405,407`	`405,407`

Table 70: TTS Server Configuration Parameters (Continued)

Tab	Parameter	Description	Example Value
Traps (continued)	MRCP Error Event Traps	Specifies the completion causes for `SPEAK-COMPLETE` MRCP events that will result in a trap. Enter a comma-separated list of values and/or ranges. Valid values: `001-005` Default value: `002-005`	`002-005`
	SET-PARAMS Request Failure Trap	Check box that specifies whether a `SETPARAMS` request timeout/connection failure results in a trap.	Cleared
	SET-PARAMS Error Response Trap	Check box that specifies whether an error response to a `SET-PARAMS` request results in a trap, provided the corresponding MRCP Error Response Trap is enabled.	Cleared
	SPEAK Request Failure Trap	Check box that specifies whether a `SPEAK` request timeout/connection failure results in a trap.	Selected
	SPEAK Error Response Trap	Check box that specifies whether an error response to a `SPEAK` request results in a trap, provided the corresponding MRCP Error Response Trap is enabled.	Selected

End of procedure

Next Steps

- If required, configure the IPCS or the VCS for ASR. For more information, see Configuring IPCS or VCS for MRCP ASR in the EMPS, page 396.
- If all IPCS or VCS configuration has been completed, restart WatchDog on the IPCS or VCS host.

Chapter

23 Configuring IP Call Manager in the EMPS

This chapter describes how to configure IPCM in the Genesys Voice Platform (GVP) Element Management Provisioning System (EMPS) for both Solaris and Windows, in deployments that include more than one IP Communication Server (IPCS).

This chapter contains the following sections:

Enabling IPCM

IPCM consists of Resource Manager (RM) with SIP Session Manager (SSM), or RM with H.323 Session Manager (HSM).

You must configure IPCM before you start the IPCM WatchDog.

Table 71 summarizes the steps that are required to enable the IPCM components to communicate with other GVP components.

Table 71: Configuring IPCM

Objective	Related Procedures and Actions
1. Provision the Media Gateway resources. **Note:** Skip this step if the proxy routing policy in your deployment uses a softswitch to handle both inbound and outbound calls, and to manage Media Gateway resources.	**1.** Configuring the Media Gateway in the EMPS, page 405. **2.** Configuring a Media Gateway group in the EMPS, page 406.
2. Configure the resource manager.	Configuring Resource Manager in the EMPS, page 407.
3. Configure the session manager(s).	• For SIP: Configuring SIP Session Manager in the EMPS, page 412. • For H.323: Configuring H.323 Session Manager in the EMPS, page 417.
4. Start or restart the IPCM WatchDog.	See Starting/Restarting GVP in Safe mode (Windows), page 199 or Starting/Restarting GVP (Solaris), page 283.
5. Verify that you can see and monitor the system processes from the Element Management System (EMS) GUI.	Enter the following URL in a web browser: `http://<hostname>:9810`

Note: If you plan on using Call Manager in a setup which uses both NativeRTP IPCS and Enhanced Media IPCS, all calls that arrive with a preferred codec of G711 will always be routed to NativeRTP, even if Enhanced Media IPCS has free G711 ports. This is because RM always selects IPCS as it has the lowest cost factor. If you need calls with the preferred G711 codec to be routed to the Enhanced Media IPCS, then it can only be achieved through application control. This is done by configuring either the `IPCSFeatrueList` or the `Preferred-Destination` parameters when provisioning your application. For more information, see the section about configuring media support for the IPCS in the *Genesys Voice Platform 7.6 Reference Manual.*

Warning! A single inbound call to IPCS witha G.711 codec will occupy more than one G.711 port on the Enhance Media IPCS, if Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) is used in the application.This in turn, uses the higher cost factor involved with a g711 media call when routed to the Enhanced Media IPCS instead of the Native RTP IPCS.

The following sections provide detailed information about the steps to enable IPCM in your GVP deployment.

Provisioning Media Gateway Resources

This section provides the procedures to configure the Media Gateway resources in the EMPS.

Procedure: Configuring the Media Gateway in the EMPS

Purpose: To create and configure the node for the Media Gateway with which the IPCS must communicate.

Repeat this procedure as required to create EMPS nodes for the Media Gateways in your deployment.

Start of procedure

1. Create the Media Gateway node:

   a. On the EMPS navigation tree, expand the `Servers > Media Gateways` node.

   b. Right-click `SampleMediaGateway`, and then select `Create a Copy`.

   A dialog box appears.

   c. Click `Copy`.

   d. In the `To Node` text box, enter a name for your Media Gateway, and then click `Copy`.

   e. Refresh the EMPS tree.

2. On the EMPS navigation tree, expand the Media Gateway node that you created.

3. Right-click `Device`, and then select `Edit`.

4. Verify or enter values on the `General` tab for the parameters listed in Table 72, and then click `Save`.

Table 72: Media Gateway Parameters

Tab	Parameter	Description	Example Value
General	Port Type	Specifies whether this device is capable of accepting inbound calls, making outbound calls, or both. Valid values: • `Inbound` • `Outbound` • `InOut`	`Inbound`
	Number of Ports	Specifies the number of ports for this device.	`23`
	IP Address for this Device	Specifies the IP address for this device.	`10.10.30.5`
	Signaling Network Port for this Device	Specifies the signaling network port for this device.	`5091`
	Description for this Device	Specifies the description for this device.	`Media Gateway simulator`
	Provider	Specifies the carrier to which the T1 lines belong.	`AT&T, MCI, Sprint`, and so on.
	Name of the Media Gateway	Specifies the name for this device	`Media Gateway Inbound`

End of procedure

Next Steps

- Add the Media Gateway to a resource group (see Configuring a Media Gateway group in the EMPS).

Procedure: Configuring a Media Gateway group in the EMPS

Purpose: To create the pool of Media Gateway resources for IPCM.

Prerequisites

- The individual Media Gateways have been created and configured in the EMPS (see Configuring the Media Gateway in the EMPS, page 405).

Start of procedure

1. Create the server group node:
   a. On the EMPS navigation tree, right-click `Server Groups`, and then select `Add New Group`.
   b. In the `Group Name` field, enter the name of the new group—for example, `MG_Grp1`.
   c. From the `Server Group Type` drop-down list, select `MG`.

      The `Available` list in the `Servers Selection` section is populated with the Media Gateways that you created.
2. Select the required Media Gateways from the `Available` list, and move them to the `Selection` list box on the right.
3. Click `Save`.

End of procedure

Next Steps

- Add the group to the RM resource pool by configuring the `Media Gateway Server Group` parameter on the `Resource Config` tab of the `Servers > Resource Manager > <RM ServerName> ResourceManager` node. For more information, see Configuring Resource Manager in the EMPS.

Configuring IPCM Components

This section provides the procedures to configure the resource and session managers in the EMPS.

Procedure: Configuring Resource Manager in the EMPS

Start of procedure

1. On the EMPS navigation tree, right-click `Servers > Resource Manager > <RM ServerName> ResourceManager`, and then select `Edit`.
2. Verify or enter values for the parameters under each tab listed in Table 73, and then click `Save`.

Table 73: Resource Manager Parameters

Tab	Parameter	Description	Example Value
General	resourcefeaturelist	Specifies the feature list for static payload types. Default value:pcmu:0;pcma:8;g723:4;g729:18;h261:31;h263:34;gsm:3	pcmu:0;pcma:8;g723:4;g729:18;h261:31;h263:34;gsm:3
SIP Config	SIP listening IP address	Specifies the IP address that RM uses to listen to SIP messages. You do not need to change this default value unless you wish to use a specific IP address (NIC).	10.10.10.10
	SIP listening port	Specifies the network port that RM uses to listen to SIP messages. You do not need to change the default value unless you want to use a specific port number.	5070
	Backup UA Address and Port	Specifies the IP address and port of the backup SIP Server. Required when the RM works as a SIP Redirect Server, configured with SIP Server. Format is: <IP address>:<port>	10.10.10.14:1234
	Primary UA Address and Port	Specifies the IP address and port of the primary SIP Server. Required when the RM works as a SIP Redirect Server, configured with SIP Server. Format is: <IP address>:<port>	10.10.10.15:1234

Table 73: Resource Manager Parameters (Continued)

Tab	Parameter	Description	Example Value
SIP Config (continued)	Subscription Refresh Interval	Specifies the interval, in seconds, at which the RM, when it is working with SIP Server, sends subscribe requests to SIP Server. Default value: `60`. **Note:** The recommended value is `600`.	`600`
Database	Primary Database IP address and port	Specifies the IP address and port of the primary (in-memory) database. Format is: `<IP address>:<port>` **Note:** If there is only one IPCM in the setup, this value is the IP address of the IPCM.	`10.10.10.10:16500`
	Backup Database IP address and port	Specifies the IP address and port of the backup database. Format is: `<IP address>:<port>` **Note:** This parameter is applicable only if the IPCM is running in High Availability mode.	`10.10.10.11:16500`

Table 73: Resource Manager Parameters (Continued)

Tab	Parameter	Description	Example Value
Resource Config	Mask for Polling SIP Devices	Specifies whether the RM will poll IPCS and Media Gateway (MG) devices for periodic health checks. Valid values: • `0` = Polling disabled • `1` = Polling enabled for IPCS device only • `2` = Polling enabled for MG device only • `3` = Polling enabled for MG and IPCS Default value: 0 (polling disabled) If enabled for the type of device, the IPCM periodically sends a SIP `OPTIONS` message to each IPCS and MG (SIP only), with a timeout value. Based on the response, the IPCM marks the status of each device as either available or unavailable. The RM will not reserve resources from an unavailable device. Do not enable this option if the SIP Server in use does not support the `OPTIONS` method.	`0`
	Primary DID URL Location	Specifies the URL to the primary Dispenser `did.xml` file.	`http://10.10.10.10:9810/did_url_mappings/$did$.xml`
	Backup DID URL Location	Specifies the backup URL to the `did.xml` file in the following format: `http://<EMPS system FQDN or ip addr>:9810/did_url_mappings/$did$.xml.`	`http://10.10.10.11:9810/did_url_mappings/$did$.xml`

Table 73: Resource Manager Parameters (Continued)

Tab	Parameter	Description	Example Value
Resource Config (continued)	Media Gateway Server Group	Specifies the group(s) of Media Gateway resources that this RM manages. The Available list in the Server Group Selection section is populated with the Media Gateway group(s) that you create (see Configuring a Media Gateway group in the EMPS, page 406). Select the required server group from the Available list, and move it to the Selection list. **Note:** Do not provision MG resources if your deployment uses a softswitch to handle both inbound and outbound calls (see the SSM ProxyRoutingPolicy parameter on page 416).	
	Default Media Codec	Specifies the media codec to use for handling pre-GVP 7.5 IPCS devices. Valid values: • G.711-mulaw • G.711-alaw If you are using a pre-GVP 7.5 IPCS, you must specify a default codec, because the pre-GVP 7.5 IPCS does not pass codec information to the RM when it registers with the RM. The pre-GVP 7.5 IPCS supports only G.711 mu-law or G.711 a-law.	G.711 mu-law

Table 73: Resource Manager Parameters (Continued)

Tab	Parameter	Description	Example Value
Process Control	Monitor Process	Specifies whether WatchDog controls the restart of the RM process. Valid values: • `0` = WatchDog does not control restart. • 1 = WatchDog does control restart. Default value: 1 (WatchDog does control restart) **Notes:** • When IPCM is used in cluster mode, set the value to `0` so that Cluster Manager, not WatchDog, controls the restart of the RM process. • This parameter is applicable only for Windows.	1

End of procedure

Next Steps

- Configure the session manager (see Configuring SIP Session Manager in the EMPS or Configuring H.323 Session Manager in the EMPS, page 417).

Procedure:
Configuring SIP Session Manager in the EMPS

Start of procedure

1. On the EMPS navigation tree, expand the nodes `Servers > SIP Session Manager > <SSM ServerName>`, and then right-click `SIPSessionManager`.
2. From the shortcut menu, select `Edit`.
3. Verify or enter values for the parameters under each tab listed in Table 74, and then click `Save`.

Table 74: SIP Session Manager Parameters

Tab	Parameter	Description	Example Value
General	Primary database IP address and port	(Mandatory) Specifies the IP address and port of the primary (in-memory) database. Format is: `<port>:16500` **Note**: If there is only one IPCM in the setup, this value is the IP address of the IPCM.	`10.10.10.10:16500`
	Backup database IP address and port	Specifies the IP address and port of the backup database. Format is: `<IP address>:16500` **Note:** This parameter is applicable only if the IPCM is running in High Availability mode.	`10.10.10.11:16500`
	Primary DID URL	(Mandatory) Specifies the primary URL to the `did.xml` file.	`http://<EMPS system FQDN or ip addr>:9810/did_url_mappings/$did$.xml`
	Backup DID URL	Specifies the backup URL to the `did.xml` file.	`http://<EMPS system FQDN or ip addr>:9810/did_url_mappings/$did$.xml`

Table 74: SIP Session Manager Parameters (Continued)

Tab	Parameter	Description	Example Value
General (continued)	Monitor Process	Specifies whether WatchDog controls the restart of the SSM process. Valid values: • `0` = WatchDog does not control restart. • 1 = WatchDog does control restart. Default value: 1 (WatchDog does control restart) **Notes:** • When IPCM is used in cluster mode, set the value to `0,` so that Cluster Manager, not WatchDog, controls the restart of the SSM process. Otherwise, you should not change the default value. • This parameter is applicable only for Windows.	1
SIP Configuration	SIP listening IP address	Specifies the IP address that SSM uses to listen to SIP messages. You do not need to change the default value unless you want to use a specific IP address (NIC).	`10.10.10.10`

Table 74: SIP Session Manager Parameters (Continued)

Tab	Parameter	Description	Example Value
SIP Configuration (continued)	SIP Header for DID	Specifies the SIP header for Direct Inward Dial (DID) lookup. Valid values: • `History-Info` • `<None>` Default Value: `<None>`	`<None>`
	Resource Manager IP address and port	(Mandatory) Specifies the IP address and port of the RM. Format is: `<RM IP address>:5070` **Note:** Make sure the port number is same as the one configured for RM in the RM configuration section. Leave it to `5070` if the RM configuration for the port has not changed.	`10.10.10.10:5070`
	Backup Softswitch SIP IP address and port	Specifies the SIP IP address and signaling port of the backup softswitch. **Note:** This parameter is required only if the proxy routing policy indicates the use of a softswitch for inbound, outbound, or both.	`10.10.10.11:1234`
	Primary Softswitch SIP IP address and port	Specifies the primary SIP IP address and signaling port of the softswitch. **Note:** This parameter is required only if the proxy routing policy indicates the use of a softswitch for inbound, outbound, or both.	`10.10.10.10.1234`
	SIP listening port	(Mandatory) Specifies the network port that SSM uses to listen to SIP messages. You do not need to change the default value unless you want to use a specific port number.	`5060`

Table 74: SIP Session Manager Parameters (Continued)

Tab	Parameter	Description	Example Value
SIP Configuration (continued)	ProxyRoutingPolicy	(Mandatory) Specifies the SIP device configurations to be used with SSM. Valid values: • `MG for both Inbound and Outbound`—The Media Gateway (MG) is used for inbound and outbound calls, and the IPCM handles resource management. You do not need to configure the primary and backup softswitch when you are using this configuration. • `MG for Inbound and SoftSwitch for Outbound call`—The MG is used for inbound calls, and the softswitch is used for outbound calls. The IPCM manages resources only for inbound calls, and the softswitch manages resources for outbound calls. • `Softswitch for Inbound and Outbound call`—The softswitch is used for both inbound and outbound calls, and it also manages MG resources. Do not provision the MG if you use this configuration.	`MG for both Inbound and Outbound`
	To process SIP error codes for INVITE response.	Specifies the `INVITE` message error code responses that will cause SSM to try a different IPCS. Use a semi-colon as separator. Default values: `480;503`	`480;503`
	ResourceFeatureList	Specifies the feature list for static payload types. Default value:`pcmu:0;pcma:8;g723:4;g729:18;h261:31;h263:34;gsm:3`	`pcmu:0;pcma:8;g723:4;g729:18;h261:31;h263:34;gsm:3`

End of procedure

Next Steps

- If you have not already done so, configure the other IPCM components that are required in your deployment (see Configuring Resource Manager in the EMPS, page 407 and Configuring H.323 Session Manager in the EMPS, page 417).
- If all the required IPCM components have been configured, start the IPCM WatchDog (see Starting/Restarting GVP in Normal mode (Windows), page 198 or Starting/Restarting GVP (Solaris), page 283).

Procedure:
Configuring H.323 Session Manager in the EMPS

Start of procedure

1. On the EMPS navigation tree, expand the nodes `Servers > Core Services > <HSM ServerName>`, and then right-click `H323SessionManager`.
2. From the shortcut menu, select `Edit`.
3. Verify or enter values for the parameters under each tab listed in Table 75, and then click `Save`.

Table 75: H.323 Session Manager Parameters

Tab	Parameter	Description	Example Value
General	Resource Manager IP address & port	Specifies the IP address and port of the Resource Manager (RM).	`<CM IP address>:5070`
	Primary DID URL	Specifies the primary URL to the `did.xml` file.	`http://<EMPS system Fully Qualified Domain Name (FQDN) or ip addr>:9810/did_url_mappings/$did$.xml`
	Backup DID URL	Specifies the backup URL to the `did.xml` file.	`http://<EMPS system FQDN or ip addr>:9810/did_url_mappings/$did$.xml`
	Local Tone Rendering	Specifies the method of Dual-tone Multi-frequency (DTMF) detection/generation. Valid values: • `alphanumeric & signal`—If you select this option, you must configure the `Local Tone Rendering` parameter in *all* IPCSs with the value `SIP INFO Msg.` • `RFC2833`—if you select this option, you must configure the `Local Tone Rendering` parameter in *all* IPCSs with the value `RTP using RFC-2833.`	`RFC2833`
SIP	SIP Listening IP Address	Specifies the IP address that the HSM uses to listen to SIP messages. You do not need to change the default value unless you want to use a specific IP address (Network Interface Card [NIC]).	`10.10.10.10`
	SIP Listening Port	Specifies the network port that HSM uses to listen to SIP messages. You do not need to change the default value unless you want to use a specific port number.	`5060`

Table 75: H.323 Session Manager Parameters (Continued)

Tab	Parameter	Description	Example Value
H323	ISDN Numbering Type	Specifies the Integrated Digital Services Network (ISDN) numbering type. Valid values: • `Unknown` • `International` • `National` • `Subscriber` **Note:** The numbering type is used for outbound calls from GVP.	`International`
	Primary Gatekeeper IP Address	Specifies the IP address and port of the primary Gatekeeper.	`10.10.10.10:1234`
	H.323 Listening Port	Specifies the network port that is used to listen to H.323 messages.	`5678`
	H.245 Tunneling	Enables H.245 tunneling.	Cleared
	Call Transfer Method	Specifies the type of H.323 protocol that is used to perform transfers. Valid values: • `H.450.2` • `H.225 Facility`	`H.450.2`
	Backup Gatekeeper IP Address	Specifies the IP address and port of the backup Gatekeeper (only in semi-routed mode). The HSM contacts the backup Gatekeeper if it fails to contact the primary Gatekeeper.	`10.10.10.11:8888`
	H.323 Listening IP Address	Specifies the IP address that is used to listen to H.323 messages.	`10.10.10.12`

Table 75: H.323 Session Manager Parameters (Continued)

Tab	Parameter	Description	Example Value
H323 (continued)	Alias Address	Specifies the alias address of the endpoint. You must specify this address when the `Enable RAS Messages` check box is selected.	`1234`
	Enable RAS Messages	Specifies whether Registration Admission Status (RAS) messages are required in order to communicate with the Gatekeeper. **Note:** This parameter works in conjunction with the `Primary Gatekeeper IP Address`.	Cleared

End of procedure

Next Steps

- If you have not already done so, configure the other IPCM components that are required in your deployment (see Configuring Resource Manager in the EMPS, page 407 and Configuring SIP Session Manager in the EMPS, page 412).
- If all the required IPCM components have been configured, start the IPCM WatchDog (see Starting/Restarting GVP in Normal mode (Windows), page 198 or Starting/Restarting GVP (Solaris), page 283).

Chapter

24 ASR Log Manager System

This chapter describes the Automatic Speech Recognition (ASR) Log Manager system, its architecture, and configuration requirements.

This chapter contains the following sections:

Note: The ASR Log Manager system is available only for Windows installations.

Overview

Companies deploying Genesys Voice Platform (GVP) are interested in having all of their callers' speech utterances available when the call ends. These utterances can be used to confirm the customer's choices, identify the customer, or tune the speech recognition application.

For ASR that is provided by the supported Nuance speech servers (see "Supported Speech Servers for ASR Log Manager" on page 422), the GVP ASR Log Manager system provides a way for you to manage the ASR logs and utterances. GVP provides the functionality to archive the utterances along with the speech server log files, and to make those archives available through the Login Server. Archives are sorted by customer first, and then by voice application. All utterances in the archive are marked with the Session ID of the call where they were captured, so that they can be easily associated with that particular call.

As part of the ASR Log Manager system, the GVP Policy Manager performs the following functions:

- Enables and disables ASR wave capture per voice application.

- Enables your administrator to configure the number of ASR samples per voice application.
- Controls whether the Voice Communication Server/IP Communication Server (VCS/IPCS) enables the ASR server to capture logs for a given call.

You can then view and download the ASR logs through the Login Server. The Login Server contains two graphical user interfaces (GUIs): one for operators, and one for customers. The customer GUI enables customers to view and download their ASR logs and wave captures. The operator GUI enables operators to monitor the status of the various log transfers. For more information about the Login Server, refer to the Login Server chapter in the *Genesys Voice Platform 7.6 Reference Manual*.

Supported Speech Servers for ASR Log Manager

GVP 7.6 ASR Log Manager supports the following speech servers and recognition software:

- Nuance SpeechWorks Media Server (SWMS) 3.1.x with Nuance OpenSpeech Recognizer (OSR) 3.0.x
- Nuance 5.0 Speech Server with Nuance Recognizer 9.0

Architecture

Figure 45 depicts a high-level overview of the ASR Log Manager system.

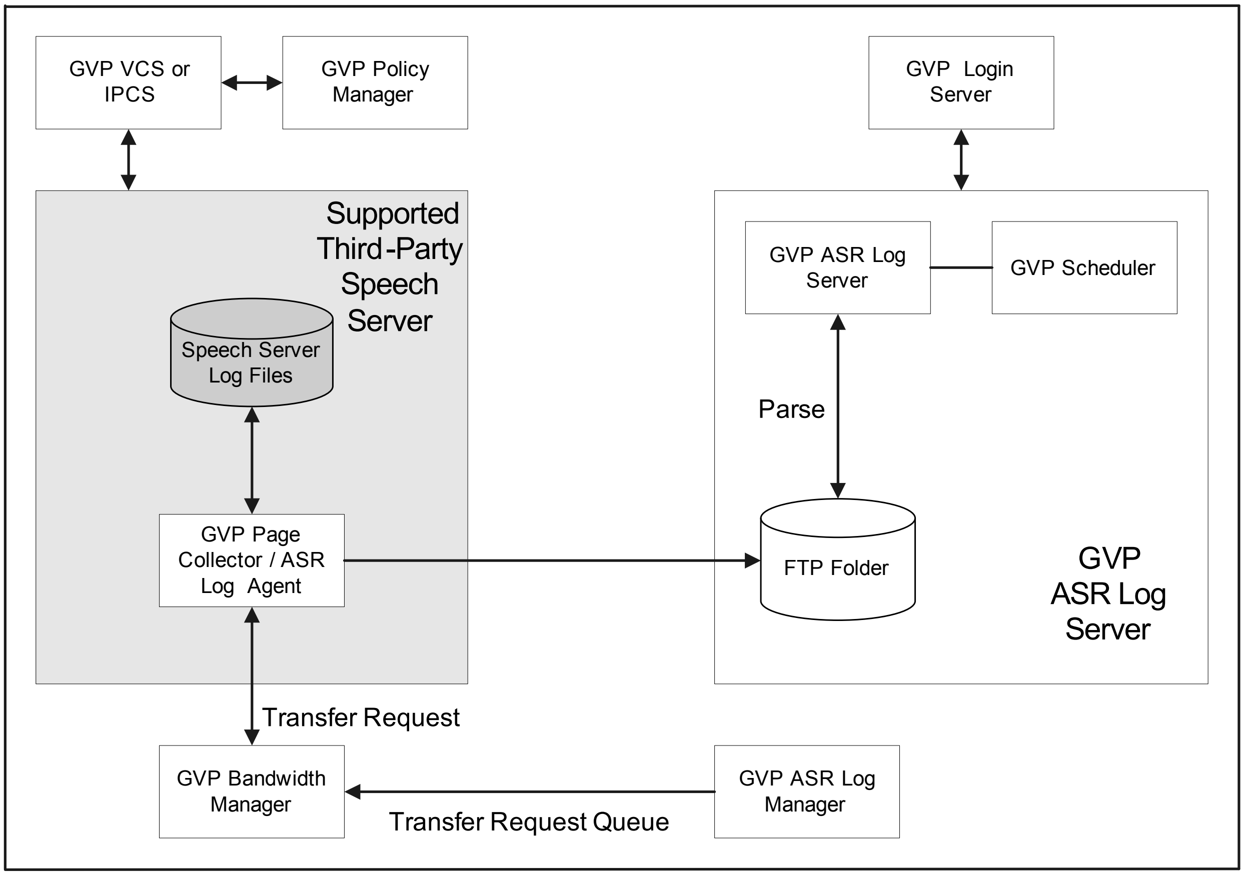


Figure 45: ASR Log Manager System

GVP Components of the ASR Log Manager System

The main GVP components of the ASR Log Manager system are:

- **ASR Log Manager**—GVP software that initiates and monitors the ASR log and utterance transfers from the various supported speech servers to the ASR Log Server.
- **ASR Log Server**—GVP software that parses the transferred ASR log utterances files and organizes them according to customers. The ASR Log Server Web Interface, which is provided by the Login Server, enables the customer and administrator to view and download the logs and utterances. The GVP 7.6 ASR Log Server is able to parse the new format of Nuance Recognizer 9.0 log files.
- **ASR Log Agent**—Resides on the speech server. It uses Page Collector to transfer ASR logs, along with utterances, to the ASR Log Server machine when initiated by ASR Log Manager. The ASR Log Agent is a GVP component that you must install on the supported speech server.

- **Bandwidth Manager**—Manages the rate of transfer between the IPCS/VCS and the ASR Log Server, and provides feedback to the ASR Log Manager about the status of the transfer. It also performs retries in the event of failures.
- **Policy Manager**—Enables and disables ASR wave capture (utterance capture) per voice application. It also enables the administrator to configure the number of ASR samples per application.
- **Voice Communication Server/IP Communication Server**—Provides trunk interfaces/media gateway to receive calls that are processed according to interpretation of voice applications. The VCS/IPCS processes speech-enabled applications through integration with the speech servers via Media Resouce Control Protocol (MRCP). Together with the speech server, VCS/IPCS provides the logs and utterances required by the ASR Log Server.

  The VCS/IPCS passes an MRCP logging tag for all MRCP ASR calls, in the following format:

  ```
  GenesysLab_<ResellerName>_<CustomerName>_<AppName>_<SessionID>
  ```

  The speech server, in turn, produces an OSLE token in the recognition software event logs with the logging tag.

  For example:

  ```
  TIME=20051121151918678|CHAN=298022|EVNT=OSCL|OSLE=GenesysLab_resell
  er2_cust1_asrdtmf_462EDB45-EFA7-4A90-BBB9-
  F12174EC1D5F|UCPU=73703|SCPU=17406
  ```

  The ASR Log Server uses this token to parse the recognition software event logs and sort them by application.
- **Login Server**—Provides an interface to view and download the ASR logs and utterances.

For more information about how the GVP and non-GVP components of the ASR Log Manager system process ASR information, see “ASR Information Processing” on page 435.

Host Setup for the ASR Log Manager System

The ASR Log Manager and ASR Log Server can co-reside on the same host, but Genesys recommends that you install them on separate servers if possible. The ASR Log Agent must reside on the speech server host.

For security reasons, Genesys recommends that the Login Server (for Unified Login) and the ASR Log Server do not reside on the same server.

For more information about software distribution and host considerations in your GVP deployment, see “Host Setup” on page 67.

Enabling the ASR Log Manager System

Table 76 summarizes the steps that are required to configure and use the ASR Log Manager system.

Table 76: Setting Up the ASR Log Manager System

Objective	Related Procedures and Actions
1. Install the components for the GVP ASR Log Manager system: ASR Log Manager; ASR Log Server; ASR Log Agent; Policy Manager; Bandwidth Manager; Login Server.	• If you are using the GVP Deployment Wizard to install GVP, ensure that you include the following steps: a. In the `Specify Setup Type` section, select the option for a `Custom` setup, and then select the following GVP options: `Reporting` (for Login Server); `ASR Log Manager;` the group that includes `Policy Manager` and `Bandwidth Manager`. For more information, see "Specify Setup Type" on page 117. b. In the `GVP Servers Configuration` section, assign the ASR Log Manager system components to the appropriate GVP servers. For more information, see "GVP Servers Configuration" on page 129. c. In the `Profiles` section, configure the `Reporting` profile and the `ASR Log Manager` profile. For more information, see "Reporting" on page 139 and "ASR Log Manager" on page 150. • If you are installing GVP components manually, see "Manually installing the ASR Log Manager System (Windows)" on page 521.
2. On the ASR Log Manager server, specify the database connection to the log manager data source.	Create the Data Source Name (DSN) that specifies the Open Database Connectivity (ODBC) connection to `logmgr.mdb`. For more information, see Creating the System DSN for ASR Log Manager, page 426.
3. Prepare the ASR Log Server for FTP.	Enable anonymous FTP access for the ASR Log Server. For more information, see Configuring FTP for the ASR Log Server, page 427.

Table 76: Setting Up the ASR Log Manager System (Continued)

Objective	Related Procedures and Actions
4. Configure GVP components in the Element Management Provisioning System (EMPS).	**1.** Configure the speech server group (ASRTeleServers). For more information, see Configuring the speech servers group for ASR Log Manager in the EMPS, page 428. **2.** Configure ASR Log Manager. For more information, see Configuring GVP components for the ASR Log Manager system, Step 2 on page 429. **3.** Configure ASR Log Server. For more information, see Configuring GVP components for the ASR Log Manager system, Step 3 on page 430. **4.** Provision the IVR profile to perform ASR logging through the Policy Manager. For more information, see Configuring GVP components for the ASR Log Manager system, Step 5 on page 431. **5.** Configure VCS/IPCS to send the required vendor-specific parameters to enable or disable utterances correctly for each call. For more information, see Configuring GVP components for the ASR Log Manager system, Step 6 on page 432.
5. Specify the baseline speech server setting for logging waveforms.	On the speech server, configure the `baseline.xml` file, to specify the value of the `swirec_suppress_waveform_logging` parameter. For more information, see Configuring the speech server baseline.xml file, page 432.
6. Configure the Login Server interface.	Configure the `ASR Files Download` service for Unified Login. For more information, see Configuring Unified Login for the ASR Log Manager system, page 433.
7. Configure the settings for deleting old ASR Log Server log files.	Configure the Garbage Collector settings for ASR Log Server log files. For more information, see Cleaning the ASR Log Server yesterday.log file, page 433.

The following procedures provide detailed information about the steps to set up the ASR Log Manager system.

Procedure: Creating the System DSN for ASR Log Manager

Purpose: To create the Data Source Name (DSN) that Open Database Connectivity (ODBC) requires to access data.

Prerequisites

- The ASR Log Manager component has been installed on the server.

Start of procedure

1. On the server that hosts ASR Log Manager, go to `Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC) > System DSN`.
2. Click `Add`.

   The `Create New Data Source` dialog box displays.
3. Select `Microsoft Access Driver` from the list of driver names.
4. Click `Finish`.

   The `ODBC Microsoft Access Setup` dialog box displays.
5. Specify the data source:
   a. In the `Data Source Name` text box, enter `logmgr`.
   b. In the `Description` text box, enter `Log Manager Database`.
   c. Click `Select` to access the `Select Database` dialog box.
6. Select the log manager database, which was automatically created when you installed ASR Log Manager:
   a. In the `Directories` panel, navigate to `<GVP installation directory>\cn\data`.
   b. In the `Database Name` list, select `logmgr.mdb`.
   c. Click `OK`.
7. Click `OK` in the next two dialog boxes, to save the DSN and exit.

End of procedure

Procedure:
Configuring FTP for the ASR Log Server

Purpose: To enable anonymous access for FTP on the ASR Log Server.

Start of procedure

1. On the ASR Log Server host, go to `Start > Settings > Control Panel > Administrative Tools > Internet Services Manager`.
2. Configure the `Default FTP Site`:
   a. Right-click `Default FTP Site`, and select `Properties`.
   b. On the `Home Directory` tab, ensure that the `Local path` is set to `c:\inetpub\ftproot`.

   c. Select the Write check box.
   d. Click OK.

3. Create the ASR Log Server website. When configuring the information for the website home directory:
   a. Set the path to the c:\gvp\cn\extweb directory.
   b. Select the check box to allow anonymous access.

End of procedure

Procedure: Configuring the speech servers group for ASR Log Manager in the EMPS

Prerequisites

- The required speech servers have been configured in the EMPS Servers > MRCPASR node. For more information, see Configuring an MRCP ASR server in the EMPS, page 392.

Start of procedure

1. Access the EMPS:
   a. In a web browser, go to http://<EMPS-hostname>:9810/spm.
   b. On the EMPS login page, log in as Admin, and enter your password.
2. In the EMPS navigation pane, go to the Server Groups node.
   - If the ASRTeleServers group is not displayed in the navigation tree, go to Step 3.
   - If the ASRTeleServers group is displayed in the navigation tree, go to Step 4.
3. Create the ASRTeleServers group:
   a. Right-click Servers Group, and select Add New Group.
   b. In the Group Name box, enter ASRTeleServers.
   c. Click Save.

      The new group is added to the Servers Group list in the navigation tree.
4. Configure the ASRTeleServers group:
   a. In the navigation tree, right-click the ASRTeleServers group to edit the node.
   b. From the Server Group Type drop-down list, select MRCPASR.
   c. Select an available speech server from the Available drop-down box, and move it to the Selection list box on the right.

d. Click `Save`.

End of procedure

Procedure: Configuring GVP components for the ASR Log Manager system

Purpose: To configure the EMPS attributes for ASR Log Manager, ASR Log Server, IVR profile, and VCS/IPCS that are required for the ASR Log Manager system.

Prerequisites

- Configuring the speech servers group for ASR Log Manager in the EMPS, page 428

Start of procedure

1. Access the EMPS:
   a. In a web browser, go to `http://<EMPS-hostname>:9810/spm`.
   b. On the EMPS login page, log in as `Admin`, and enter your password.
2. Configure ASR Log Manager:
   a. Go to the `Servers > ASR Log Manager > <Server Name> > LogMgr` node.
   b. Configure the attributes that are listed in Table 77.
   c. Add `Read`, `Write`, and `Delete` permissions to the local IIS user for the `C:\GVP\CN\data\` directory.

Table 77: ASR Log Manager Attributes

Attribute	Description	Example Value
Start Time for Data Transfer (HH:MM)	Specifies the time of day that the ASR Log Manager initiates transfers.	`16:55`
Log Server URL	Specifies the FTP address of the ASR Log Server machine.	`ftp://asrls.company.com`
BWM URL	Specifies the fully qualified name of the Bandwidth Manager machine, which runs on port 9810. **Note:** Except for the computer name, do not change the default URL.	`http://bwm.company.com:9810/webnotify.asp?notifyprocess=bwm1&customer=ASRLogManager`

Table 77: ASR Log Manager Attributes (Continued)

Attribute	Description	Example Value
Duration Between Consecutive Transfers	Specifies how often the ASR Log Manager initiates transfers.	`86400`
Group List	Specifies the names of the groups containing the supported speech servers. Separate the group names with a semicolon. For information about creating the groups, see Configuring the speech servers group for ASR Log Manager in the EMPS, page 428.	`ASRTeleServers`

3. Configure ASR Log Server:
   a. Go to the `Servers > ASR Log Server > <ASR Log Server Name> > Scheduler > ASRLogServer` node.
   b. Configure the attributes that are listed in Table 78.
   c. Go to the `Servers > ASR Log Server > <ASR Log Server Name> > ASRLogServer` node.
   d. On the `ProvisioningDB` tab, configure the attributes that are listed in Table 78.
   e. Add `Read`, `Write`, and `Delete` permissions to the local IIS user for the `C:\GVP\CN\extweb\ASRLogs\` directory.

Table 78: ASR Log Server Attributes

Tab	Attribute	Description	Example Value
Servers > ASR Log Server > `<ASR Log Server Name>` > Scheduler > ASRLogServer > General	Task Start Time (hr:min:sec)	Specifies the time of day that the ASR Log Server initiates parsing. **Note:** In order for all `.wav` files to be transferred successfully, Genesys recommends having a time difference of at least eight hours between the ASR Log Manager `Start Time for Data Transfer` and the ASR Log Server `Task Start Time`. Also note that these two attributes are in different time units.	`15:30:00`
	Task Frequency (hr:min:sec)	Specifies how often the ASR Log Server parses the logs and utterances.	`24:00:00`

Table 78: ASR Log Server Attributes (Continued)

Tab	Attribute	Description	Example Value
Servers > ASR Log Server > <ASR Log Server Name> > Scheduler > ASRLogServer > General (continued)	Task Priority	Specifies the priority at which GVP Scheduler runs this task. **Note:** If you set this attribute to High, the GVP Scheduler processes this request higher than Normal and Low. Genesys recommends using the default value of Normal.	Normal
	Audiofiletype	Specifies the type of audio file.	wav
	EMPS URL	Specifies the fully qualified name of the EMPS machine. **Note:** Replace the computer name only in the default URL.	http://emps.company.com:9810/webnotify.php?notifyprocess=sps
Servers > ASR Log Server > <ASR Log Server Name> > ASRLogServer > ProvisioningDB	EMPS Database Server Name (Oracle Net Service name in case of Oracle)	Specifies the fully qualified domain name of the server that has the EMPS database.	MSSQL: 172.24.129.52
	EMPS Database / Schema Name	Specifies the database/schema name for the EMPS.	emps
	EMPS Database User Name	Specifies the user name of the EMPS database.	emps
	EMPS Database Password	Specifies the password of the EMPS database.	emps

4. Enable ASR Log Server to fetch the RCA information from EMPS:
   a. On the General tab, click Add New Attribute to manually add the following parameter:

      tdsgenerated = 1

   b. Restart Watchdog.
5. Provision the IVR profile to perform ASR logging through the Policy Manager.
   a. In the Resellers > <Customer> navigation tree, access the provisioning property pages of the IVR profile.
   b. On the Provision ASR tab, select the Enable ASR Logging check box, and enter the number of ASR samples (for example, 10).
   c. Click Save.

6. Configure the VCS/IPCS to send the required vendor-specific parameters to enable proper integration to the ASR Log Manager, so that utterances are enabled or disabled correctly for each call:
   a. Access the `ASR > MRCP` node:
      - For VCS, go to `Servers > <VCS Server Name> > VCS > PopGateway > ASR > MRCP`.
      - For IPCS, go to `Servers > IPCS > <IPCS Server Name> > Mcu > ASR > MRCP`.
   b. On the `General` tab,
      i. To enable utterance capture, set the `Enable Utterance Capture Parameter` to the following value:

         ```
         swirec_suppress_waveform_logging=0
         ```
      ii. To disable utterance capture, set the `Disable Utterance Capture Parameter` to the following value:

         ```
         swirec_suppress_waveform_logging=1
         ```
      iii. To enable the maximum number of simultaneous `.wav` file captures, click `Add New Attribute` to manually add the following parameter:

         ```
         maxchannelwavcapture=10
         ```
   c. Restart Watchdog.

   For more information about the utterance capture parameters, see Table 69 on page 397.

End of procedure

Procedure: Configuring the speech server baseline.xml file

Purpose: To set the baseline value of the parameter that specifies whether waveforms are logged for the current recognition.

Start of procedure

1. Go to `Program Files\SpeechWorks\OpenSpeech Recognizer\config\baseline.xml`.
2. Set the following parameter values:

```
<param name="swiep_suppress_waveform_logging">
<value>1</value>
</param>
```

```
<param name="swirec_suppress_waveform_logging">
<value>1</value>
</param>
```

Note: Genesys recommends that you set the value of the `swirec_suppress_waveform_logging` parameter to `1` (waveforms are not logged for the current recognition). If you want waveforms to be logged for the current recognition, set this parameter to `0`. For more information, refer to the Nuance documentation.

End of procedure

Procedure: Configuring Unified Login for the ASR Log Manager system

Purpose: To provide the Login Server interface, to view and download ASR logs.

Start of procedure

1. Log in to the Unified Login at `http://<Login Server>/unifiedlogin`.
2. Click `Login Administration`.
3. Click `Modify Service`.
4. From the drop-down list, select `ASRLS1 - ASR Files Download`, and then click `Search`.
5. Modify the `URL` field as follows:

   `http://<FQDN of ASR Log Server>/asrls/login.php`

   If ASR Log Server is on a VPN in addition to being on the public network, then enter the VPN URL in the `VPN URL` field as follows:

   `http://<VPN URL of ASR Log Server>/asrls/login.php`
6. Click `Save`.
7. Verify the GUIs:
   a. Log in to `http://<ASR Log Server FQDN>/unifiedlogin`.
   b. Click `ASR Files Download`.

End of procedure

Procedure: Cleaning the ASR Log Server yesterday.log file

Purpose: To specify the settings for deleting old ASR Log Server log files.

Start of procedure

1. In the EMPS, go to `Servers > ASR Log Server > <ASR Log Server Name> Scheduler > GarbageCollector > CNASRLogs`.
2. Create a new node:
   a. In the main frame, click the `Copy Node` link.
   b. On the `Server Configuration` property page, click `Copy Node`.
   c. In the `To Node` text box, enter the new node name (for example, `CNASRYesterdayLog`).
   d. Click `Copy`.
3. Edit the new node to point the path to the location of the `Yesterday.log` file:
   a. On the main frame for the newly created node, click the `Edit Node` link.
   b. On the `Server Configuration` property page, click `Add New Attribute`.
   c. Specify the attribute name and value:
      - In the `Attribute Name` text box, specify `path`.
      - In the `Attribute Value` text box, specify the path of the `yesterday.log` file (for example, `C:\Inetpub\ftproot\che026.adcc.alcatel.be\SpeechworksOSR\Wav Files)`
   d. Click `Submit`.
4. Edit the new node to specify the file to delete:
   a. On the main frame for the newly created node, click the `Edit Node` link.
   b. On the `Server Configuration` property page, click `Add New Attribute`.
   c. Specify the attribute name and value:
      - In the `Attribute Name` text box, specify `filestodelete`.
      - In the `Attribute Value` text box, specify `Yesterday.log`.
   d. Click `Submit`.
5. Edit the new node to specify the inactivity interval after which a file will be deleted.
   a. On the main frame for the newly created node, click the `Edit Node` link.
   b. On the `Server Configuration` property page, change the value of the `File Unused Time` parameter as required. (For example, a value of `1:00:00` means that the file would be deleted after one day.)
   c. Click `Submit`.

End of procedure

ASR Information Processing

ASR information processing can be divided into the following stages:

Stage 1—The Policy Manager Controls the Utterance Capture

When a call is made to the VCS/IPCS, the Policy Manager verifies the provisioning attributes of that application, and enables the utterance capture only if ASR Logging is enabled.

The Policy Manager also controls the number of ASR samples, as provisioned by the voice application.

Stage 2—The VCS/IPCS, Through the Speech Server, Captures the Utterances

The VCS/IPCS streams the user audio to the speech server via RTP during recognitions.

Note: The VCS/IPCS enables utterances for a call on the speech server only if the following criteria are met:

- Policy Manager grants permission for capturing utterances for a call.
- The PopGateway has not exceeded the maximum number of simultaneous ports enabled for utterance capture.

Stage 3—The Speech Server Transfers the Utterance to the ASR Recognition Software Server

The speech server delivers the utterance to the ASR recognition software server for the recognition.

Stage 4—The Speech Server Generates an Utterance File and Updates the Speech Server Event Log

The speech server receives an utterance, saves it into the voice file, and updates the corresponding event log. The files are stored in the `DataCapture` directory that is configured as one of the speech server parameters in the Registry.

The directory should be set as follows:

```
.\CN\ASR\Log\SpeechworksOSR\WavFiles
```

The full path to the ASR log files looks like the following:

Where

```
.\CN\ASR\Log\SpeechworksOSR\WavFiles\<timestamp>\
```

- `<timestamp>` has format `YYYYMMDDHHMMSS`

For example, it could be `20031007085623`, which means 08:56:23 AM on October 7, 2003.

This directory contains one speech server event file (for example, for SWMS, `SWIevent*.log`) and several voice files. The speech server event file provides information about the call flow for several calls and the references to the utterances captured in these calls. All of the utterances referred to in the event log are stored in the same directory in the voice files.

The Recognizer analyzes the utterances stored on the speech server and sends the recognition result back to the VCS/IPCS. Once utterances are used, they should be sent to the ASR Log Server to be archived and stored.

Note: The transfer occurs if the utterance capture is enabled for the application.

Stage 5—The ASR Log Manager Transfers the Utterance Files and Logs to the ASR Log Server

The ASR Log Manager controls the transfer of the utterance voice files and speech server event logs from the speech server to the ASR Log Server. All transfer parameters are configured in the `Servers > ASR Log Manager > <Server Name> > LogMgr` section in the EMPS. For more information about the transfer parameters, see Table 77 on page 429.

The ASR Log Manager sends the transfer request to the BWM at the configured time. The BWM, in turn, sends the transfer request to the Page Collector that is running on the speech server machine. The Page Collector transfers all of the files from the `\<VCS/IPCS Installation folder>\ASR\Log` directory on the speech server to the `\ftproot\` directory. The following subdirectory structure is created:

```
\ftproot\<ASR server>\SpeechworksOSR\WavFiles\<timestamp>\
```

Stage 6—The ASR Log Server Parses, Archives, and Stores the Files

In the final stage of the process, the transferred files are processed by the ASR Log Server:

1. The ASR Log Server parses the speech server event log files. Parsing is a scheduled process that is configured in the EMPS at `ASR Log Server > <host> > Scheduler > ASRLogServer`.
2. If the event logs are parsed successfully, the files are zipped and moved to the `\<ASR Log Server Installation folder>\ExtWeb\` directory on the same host. The following subdirectory structure is created:

   ```
   \<ASR Log Server Installation folder>\ExtWeb\<customer>\
   <application>
   ```

   The Login Server assumes that this directory tree is used when it displays the archives through the GUI.

The ASR Log Server gets the information about the customers and their applications by using the `EMPS URL` parameter that is configured in the `ASRLogServer` section in the EMPS (see page 431).

Part

5 GVP Integrations

This part of the manual provides information about integrating Genesys Voice Platform (GVP) with Genesys Management Framework and SIP Server.

This part contains the following chapters:

- Chapter 25, "Integrating GVP with Management Framework," on page 441
- Chapter 26, "SIP Server Integration," on page 451

For information about integrating GVP with Outbound Contact for proactive notification, see the *Genesys 7.6 Proactive Contact Solution Guide.*

Chapter

25 Integrating GVP with Management Framework

This chapter provides instructions for integrating the Genesys Voice Platform (GVP) IP Communication Server (IPCS) or Voice Communication Server (VCS) with Genesys Management Framework. It contains the following sections:

Overview

To integrate the IPCS/VCS into a Framework environment, follow this broad outline:

1. Configure the IPCS/VCS in Configuration Manager.
2. Install the Local Control Agent (LCA) on the same machine as the IPCS/VCS. Make sure this machine can connect to the machine on which you have installed Configuration Server.

   Refer to the *Genesys Framework 7.6 Deployment Guide* for information on installing the Local Control Agent.
3. Install the IPCS/VCS.
   - For information about installing the IPCS/VCS on Windows, see "Installing GVP Components with the GDT" on page 111 or "Manual Installation on Windows" on page 505.
   - For information about installing the IPCS on Solaris, see "Installing IPCS on Solaris" on page 262.

Configuring IPCS/VCS in Configuration Manager

The IPCS/VCS configuration involves:

- Creating a new Host configuration object (see Creating the GVP Host object in Configuration Manager).
- Creating a new Application Template object (Creating the GVP Application template in Configuration Manager, page 445).
- Creating a new Application object (Creating the GVP Application object in Configuration Manager, page 446).

Procedure:
Creating the GVP Host object in Configuration Manager

Purpose: To create the Configuration Manager Host object for the GVP server.

Start of procedure

1. Open Configuration Manager.
2. Expand the Configuration menu on the left side of the dialog box (see Figure 46).

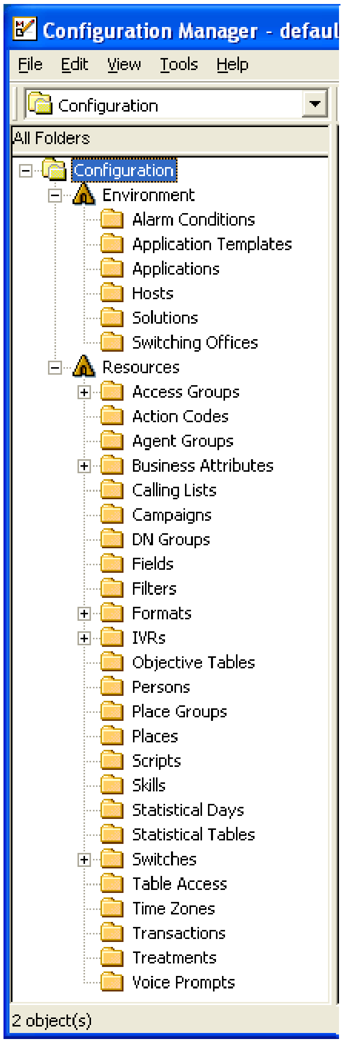
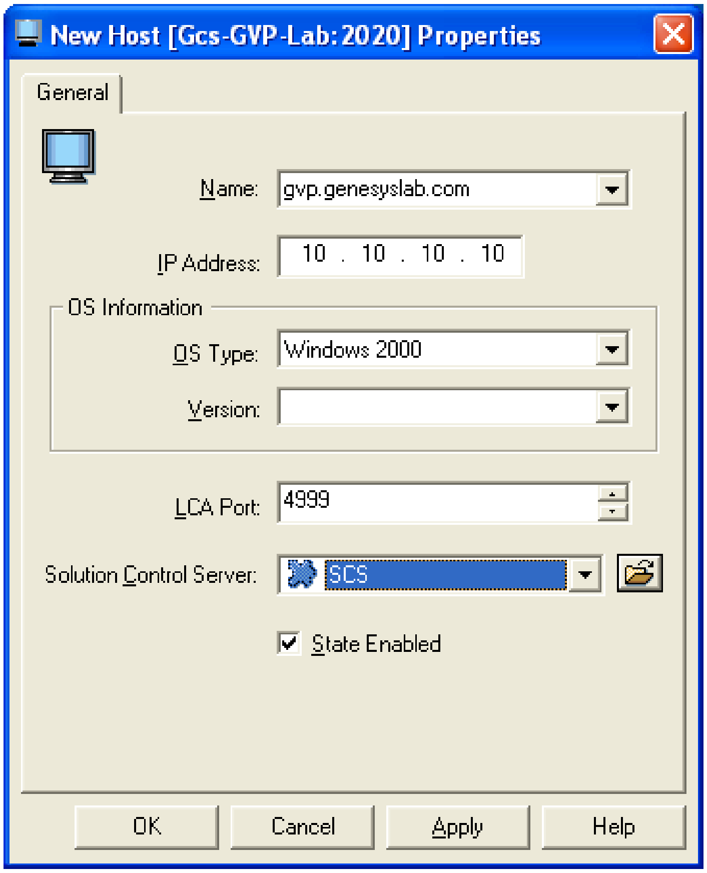


Figure 46: Configuration Manager Dialog Box

3. Click `Environment`, and then click `Hosts`.
4. Right-click the right side of the dialog box, and select `New > Host` from the shortcut menu. The `Host Properties` dialog box opens (see Figure 47).



New Host [Gcs-GVP-Lab:2020] Properties

General

Name: gvp.genesyslab.com

IP Address: 10 . 10 . 10 . 10

OS Information

OS Type: Windows 2000

Version:

LCA Port: 4999

Solution Control Server: SCS

☑ State Enabled

Figure 47: Host Properties Dialog Box—General Tab

5. In the `Name` box, enter the name of the new host. The name should be the fully qualified hostname of the GVP machine.
6. Enter the `IP address`, `OS Type`, `Version`, `LCA port` number, and `Solution Control Server` name in the appropriate fields.
7. Click `OK`. This creates the new `Host` object.

End of procedure

Next Steps

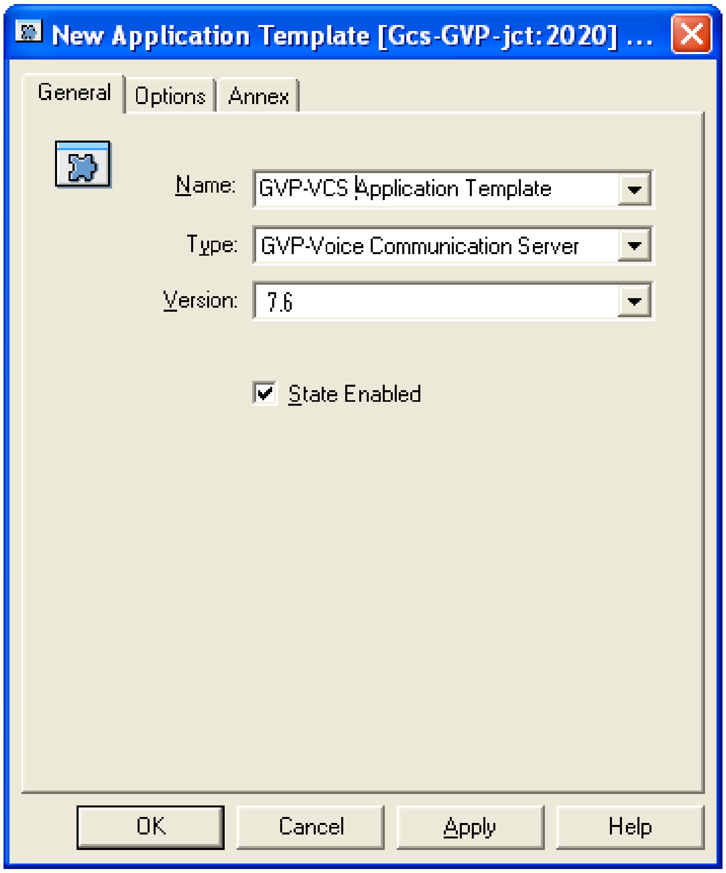
- Creating the GVP Application template in Configuration Manager

Procedure: Creating the GVP Application template in Configuration Manager

Purpose: To provide the template for the GVP-Voice Communication Server Application object.

Start of procedure

1. Open Configuration Manager.
2. Expand the Configuration menu on the left side of the Configuration Manager dialog box.
3. Click Environment, and then click Application Templates.
4. Right-click the right side of the dialog box, and select New > Application Template from the shortcut menu. The Application Template Properties dialog box opens (see Figure 48).



Name: GVP-VCS Application Template

Type: GVP-Voice Communication Server

Version: 7.6

☑ State Enabled

Figure 48: Application Template Properties Dialog Box

5. In the Name box, enter a name for the new application template:

- For IPCS, enter GVP-IPCS Application Template
- For VCS, enter GVP-VCS Application Template

6. For both IPCS and VCS, select GVP-Voice Communication Server from the Type drop-down list.
7. Specify the Version.
8. Click Apply.
9. On the Options tab, right-click in the white space and select New. In the Section Name box, enter Log.Click OK.
10. Double-click the Log section that you just created. Use the Create New Section/Option icon to create the name-value pairs under the Log section, as shown in Table 79. When you are finished, click OK.

Table 79: Name Value Pairs

Name	Value
all	.\log\ipcsinterface
buffering	true
standard	network
trace	network
verbose	all

End of procedure

Procedure: Creating the GVP Application object in Configuration Manager

Prerequisites

- The Application Template exists. For information about creating the required Application Template, see Creating the GVP Application template in Configuration Manager, page 445).

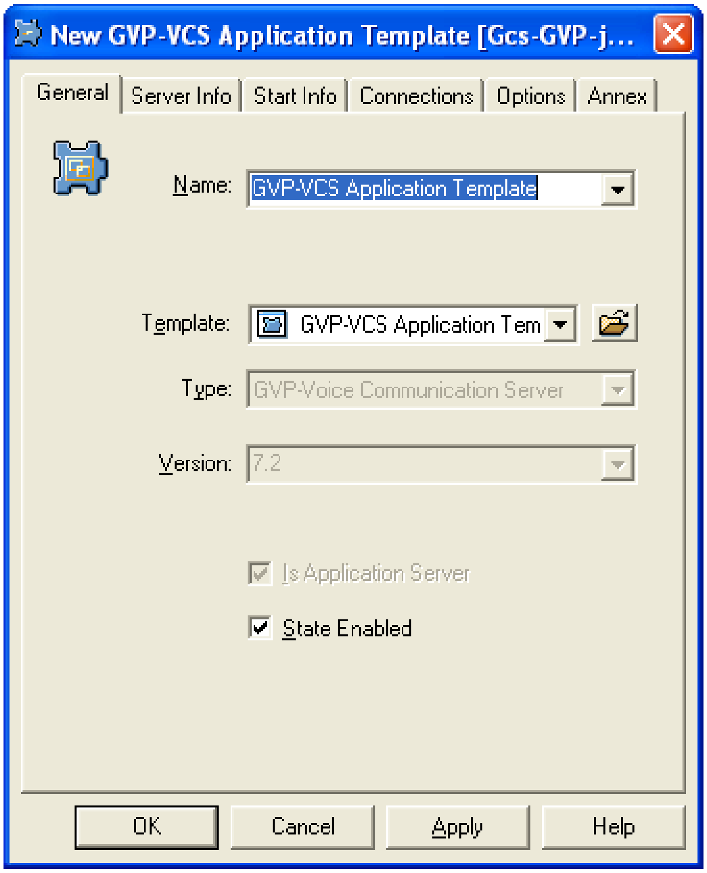
Start of procedure

1. Open Configuration Manager.
2. Expand the Configuration menu on the left side of the Configuration Manager dialog box.
3. Click Environment, and then click Applications.

4. Right-click the right side of the dialog box, and select `New > Application` from the shortcut menu.

5. In the `Browse` dialog box that displays, select the `GVP-Voice Communication Server` application template, and then click `OK`.

   The dialog box to configure the `Application` displays (see Figure 49).



Name: GVP-VCS Application Template

Template: GVP-VCS Application Tem

Type: GVP-Voice Communication Server

Version: 7.2

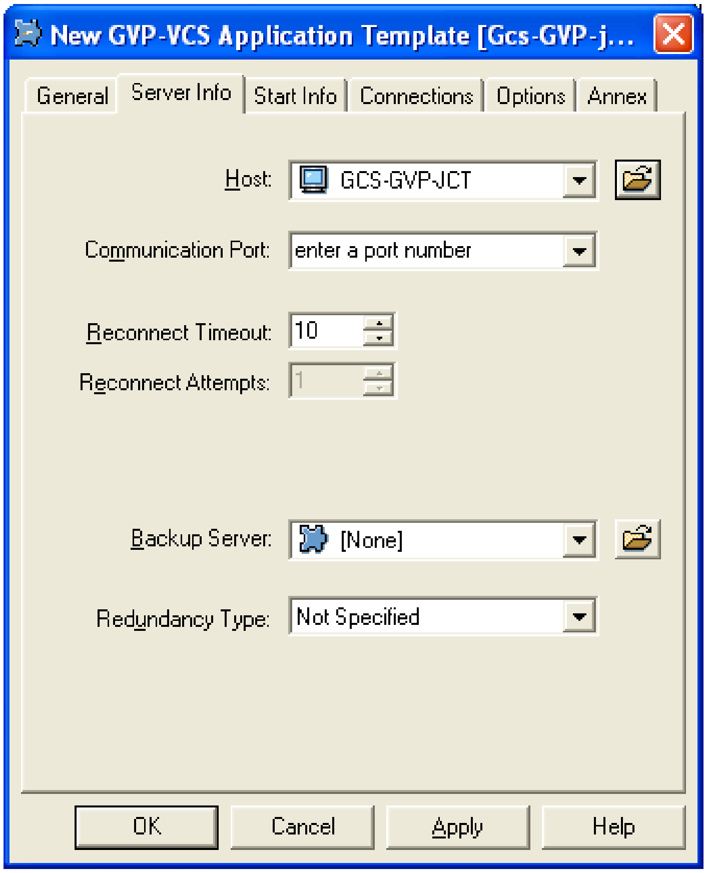
☑ Is Application Server

☑ State Enabled

Figure 49: GVP Application Properties Dialog Box

6. On the `General` tab, enter a name for the `Application` object in the `Name` box:
   - For IPCS, enter `ipcs-<ipcs_host_name>`, where `<ipcs_host_name>` is the fully qualified domain name of the machine on which you have installed the IPCS.
   - For VCS enter, `vcs-<vcs_host_name>`, where `<vcs_host_name>` is the fully qualified domain name of the machine on which you have installed the VCS.

7. Configure the `Server Info` tab (see Figure 50).



Host: GCS-GVP-JCT

Communication Port: enter a port number

Reconnect Timeout: 10

Reconnect Attempts: 1

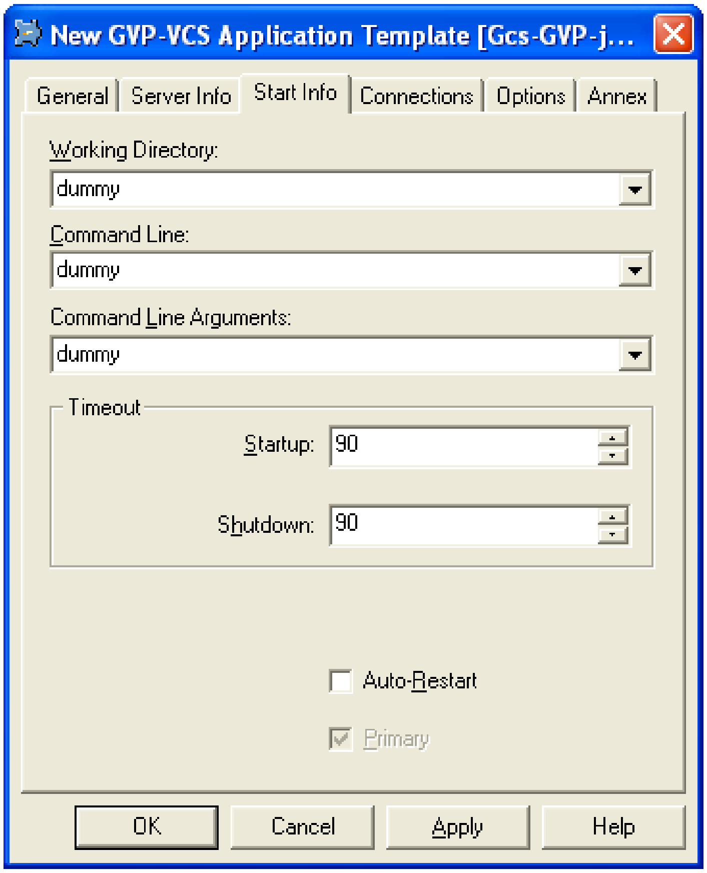
Backup Server: [None]

Redundancy Type: Not Specified

Figure 50: Application Properties Dialog Box —Server Info Tab

- **a.** From the `Host` drop-down list, select the `Host` configuration object that you created (see Creating the GVP Host object in Configuration Manager, page 442).
- **b.** Enter a unique port for the `Communication Port`, and then enter the `Reconnect Timeout`.
- **c.** Leave the `Backup Server` set to `None`, and the `Redundancy Type` set to `Not Specified`.

8. Configure the `Start Info` tab (see Figure 51).



Working Directory: dummy

Command Line: dummy

Command Line Arguments: dummy

Timeout

Startup: 90

Shutdown: 90

☐ Auto-Restart

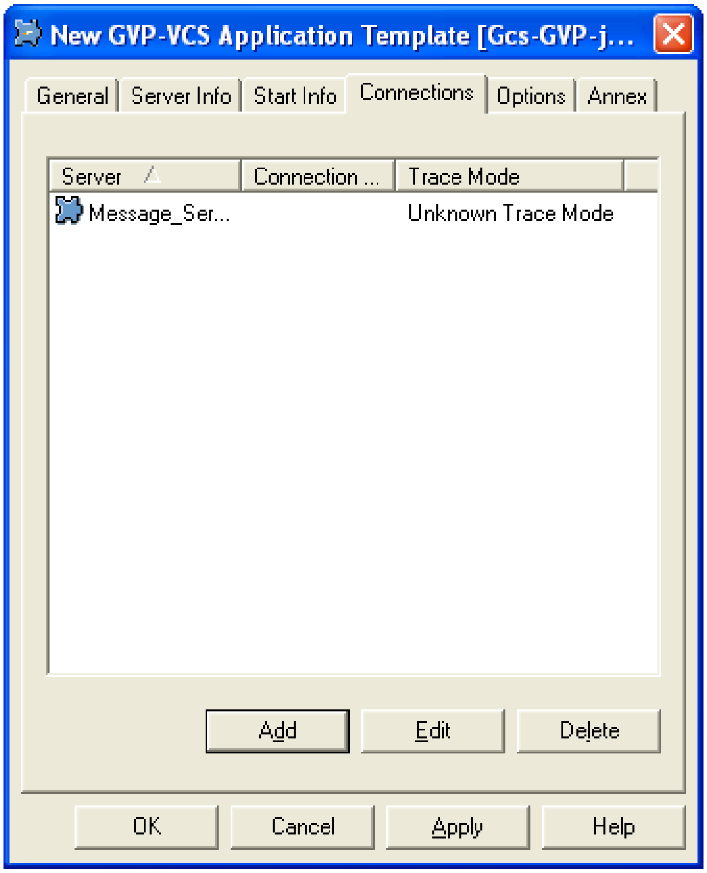
☑ Primary

Figure 51: Application Properties Dialog Box—Start Info Tab

a. Set the `Working Directory`, `Command Line`, and `Command-Line Arguments` fields to dummy values. When you install the IPCS/VCS, it automatically connects to the Configuration Server and updates these parameters to the correct values.

b. Clear the `Auto-Restart` check box.

9. Configure the `Connections` tab, to add a connection to Message Server (see Figure 52).



New GVP-VCS Application Template [Gcs-GVP-j...

Server	Connection ...	Trace Mode
Message_Ser...		Unknown Trace Mode

Figure 52: Application Properties Dialog Box—Connections Tab

a. Click `Add`.

b. Use the `Browse` button in the `Connection Info Properties` dialog box to browse for the Message Server to which you would like to connect.

c. Select `Message Server`, and click `OK`.

d. The `Trace Mode` box is set automatically to `Unknown Trace Mode`. Do not change this.

10. Click `OK`.

End of procedure

Chapter

26 SIP Server Integration

This chapter describes how to install and configure Genesys Voice Platform (GVP) for integration with the Genesys SIP Server. It contains the following sections:

Overview

Genesys Voice Platform (GVP) supports Session Initiation Protocol (SIP) Server integration through the GVP Resource Manager (RM). In addition to managing resources, the RM is enhanced to perform as a SIP Redirect Server in order to integrate with SIP Server. In this scenario, SIP Server will send a new call to RM and RM will provide the appropriate IP Communication Server (IPCS) resource based on it's application features.

The IPCS is enhanced to send Registration/Un-registration requests to RM. The RM address information is obtained from the advanced parameter in the Element Management Provisioning System (EMPS) for the PopGateway process.

The Genesys SIP Server is a SIP T-Server that has soft switch capabilities.

Operating Modes

There are three modes in which a GVP/SIP solution may be deployed:

- `GVP Stand Alone` mode—In this mode, GVP uses SIP Server as its SIP proxy instead of the GVP SIP Session Manager (SSM) component. This mode is intended for self service usage.

- `GVP Behind-the-Switch` mode—Involves the configuration of IVR Server with SIP Server. In this mode, SIP Server acts as SIP TServer. The IVR Server communicates with SIP Server as a TServer client. SIP Server can also act like a softswitch and have agents registered directly with it.
- `GVP In-Front-of-the-Switch` mode—In this mode, the SIP Server replaces the SIP Session Manager and the dialed number identification service (DNIS) is received in the initial message from SIP Server rather than from the Genesys Framework.

When discussing GVP operation modes, the terms `In-Front-of-the-Switch` and `Behind-the-Switch` are in context to the IVR Server configuration. SIP Server is always in front of GVP, and provides an interface for GVP to other external SIP platforms. At a minimum, SIP Server acts as a SIP proxy for GVP, but it could also be used as a SIP T-Server, or a SIP soft-switch for GVP.

High Availability

High Availability ensures that a service is not interrupted in the event of a failure or a process restart. Genesys SIP Server and the GVP Resource Manager currently support High Availability through the Microsoft Windows Cluster Service.

The High Availability feature for GVP Resource Manager is available when both primary and backup Resource Manager hosts are deployed with Microsoft Windows Cluster Service.

The High Availability feature for SIP Server hosts is available when both primary and backup SIP Server hosts are deployed with Microsoft Windows Cluster Service.

It is important to ensure that for the combined integrated solution to utilize the High Availability feature, that the GVP Resource Manager and the SIP Server are installed on separate hosts, with both the GVP Resource Manager and the SIP Server independently deployed in a manner to support the High Availability feature.

When deployed in a High Availability configuration, the virtual IP address is provided by the associated Cluster Service for both the GVP Resource Manager and the SIP Server.

Deploying GVP to Use the Genesys SIP Server

Install GVP using the Genesys Deployment Tool.

Note: On the IP Call Manager host machine, install Voice Platform Common, and Resource Manager components only. The Voice Platform SIP Session Manager component does not need to be installed as it is replaced by the Genesys SIP Server in this integration.

Configuring GVP to Use the Genesys SIP Server

This section describes the steps required to configure the GVP solution with the Genesys SIP Server.

Configuring Resource Manager

Consider the following when configuring Resource Manager:

- The Primary User Agent (UA) address and port both reference the primary SIP Server address and port in the network. This information will be used to validate incoming requests. RM will also send subscription information to this address.
- The Backup UA address and port are not required and can contain null values.
- The `Primary DID URL` location references the actual path to the primary direct inward dial (DID) Uniform Resource Locator (URL) location. This information is used to retrieve the application profile. This is a mandatory parameter.
- The `Backup DID URL` location references the actual path to the backup DID URL location. This information is used to retrieve the application profile. This parameter is optional.
- The `subscription refresh interval` value is used in the `Expires` header information in the `SUBSCRIBE` message. The default value is `60` seconds. Genesys recommends that you set the value between `40` and `600`.

Configuring IPCS

Consider the following when configuring IPCS:

- The Resource Manager references the Primary RM address and port in the format `IP address:Port`. The `Resource Manager` parameter is under the `PopGateway1` node for IPCS in the EMPS.
- The Backup RM references the Backup RM address and port. The `Backup Resource Manager` parameter is under the `PopGateway1` node for IPCS in the EMPS.
- The `Primary Call Manager IP Address`, and the `Primary Call Manager SIP Port` parameters under the `Popgateway1` section must reference the SIP Server IP address and port.
- The `Backup Call Manager IP Address` and the `Backup Call Manager SIP Port` parameters under the `Popgateway1` section are not required, and can contain null values.
- The port range of the IPCS must match the corresponding range of the Voice Treatment Ports defined in the Configuration Layer. The Voice Treatment port range must be contiguous. Configure the `Starting Number for PortIDs/ChannelIDs` parameter in the `SIP` tab of the `PopGateway` node in EMPS to start with the same starting number as the first Voice Treatment Port.

Configuring for GVP Deployment—Stand Alone Mode

Perform the following steps when deploying GVP in Stand Alone mode:

- Configure the Media Gateway that is the source of the inbound calls to SIP Server as a `Trunk` object in Configuration Manager. For more information about this option, see the *Framework 7.6 SIP Server Deployment Guide*.
- Configure separate inbound trunks that reference the RM.
- Configure separate trunk(s) that reference the IPCS. The `straight-forward` option enables this functionality. For more information, see the*Framework 7.6 SIP Server Deployment Guide*.

Configuring for GVP Deployment—Behind-the-Switch Mode

GVP Behind-the-Switch mode allows SIP extensions to be controlled directly by SIP Server.

The following provides an overview of the steps to perform in Configuration Manager in order to deploy this solution in GVP Behind-the-Switch mode. For more information about these steps, see the *Framework 7.6 SIP Server Deployment Guide*. Contact your regional Genesys Technical Support office for additional support and questions about specific switch-related configurations.

1. On the SIP Server Application property page, under the `Options` tab:
   a. `TServer` section:
      - Create the `override-to-on-divert` option, and set the value to `false`. See the *Framework 7.6 SIP Server Deployment Guide* for more information about this option.

> Note: Ensure the `INVITE` message sent to GVP contains the same `TO` header user name as the original `INVITE` message. The number originally dialed (Route Point) must exist on GVP as a direct inward dialing (DID) number.

      - Create the `event-ringing-on-100trying` option, and set the value to `true`. This option forces `EventRinging` generation without waiting for `180` Ringing from IPCS. See the *Framework 7.6 SIP Server Deployment Guide* for more information about this option.
      - Create the `sip-treatments-enabled` option, and set the value to `true`. If call queuing happens on Stream Manager, it is recommended to make usage of the SIP protocol between SIP Server and Stream Manager. See the *Framework 7.6 SIP Server Deployment Guide* for more information about this option.

   b. Add the following option to the `extrouter` section:
      - Create the `handle-vsp` option, and set the value to `all`. If agents can be located on another TServer than SIP Server, and if call queuing happens on GVP, then this option insures that ISCC messages will properly flow between SIP Server, and the remote TServer. See the *Framework 7.6 SIP Server Deployment Guide* for more information about this option.

2. Configure a DN of type `Voice Treatment Port` for every virtual IPCS port.

   On the DNs property page, under the `Annex` tab, add the following configuration options to the `TServer` section:

> Note: If the `TServer` section does not exist, you must create it.

   a. Create the `contact` option, and set the value to the applicable IPCS SIP address and port. For example:

      `sip:172.21.11.15:5088`

   b. Create the `subscription-id` option and set the value to `GVP`.

> Note: The `subscription-id` option must have the same value (`GVP`) for every IPCS port.

   This activity will uniquely identify each of the IPCS ports for subscription.

3. Configure a `Place` for every DN previously configured.

This step enables Stat Server to monitor each port's status.

4. Configure Place Groups for every IPCS instance. Distribute the Places into Place Groups according to the IPCS port capacity.
5. Create a virtual switch.
6. Create an access code on the switch object for which SIP Server has a connection to.
7. Create an IVR Server application that references the SIP Server application as it's T-Server on the IVR Server application Connections tab.
8. Create a Virtual T-Server application that refers to the IVR Server application. Associate the Virtual T-Server application to the Virtual Switch object. Refer to the IVR Server documentation for more details.
9. Create an IVR object. This object contains IVR ports that are mapped to real DNs that were configured above.
10. Configure a Routing Point, and a strategy that will route a call to IPCS using RM. Refer to the *Framework 7.6 SIP Server Deployment Guide* for detailed information about the Play Application step portion of this strategy.
11. Configure Routing Points, and a strategy that will be used by GVP to find an available agent.
12. For call queuing on GVP, at least one Virtual Route Point (VRP) is required. Add your VRP(s) to the VirtualRoutePoints section of the I-Server application options.
13. Configure GVP.

Note: IPCS enables you to override the randomly-selected IVR port with a number obtained from the SIP header message if you set the SIP Header for IVR Port parameter in the EMPS application to RequestURI.

Configuring for GVP Deployment—In-Front-of-the-Switch Mode

GVP In-Front-of-the-Switch mode specifies that SIP end points are controlled by a separate T-Server that is different than SIP Server. IVR Server contains an Inter-server Call Control (ISCC) connection to that particular T-Server. The attached data is passed using ISCC, while the call is transferred from GVP to the external route point using SIP Server.

Steps 2, 3, 4, and 10 for GVP Behind-the-Switch mode deployment are similar for GVP In-Front-of-the-Switch mode. The call is still routed from the SIP Server that uses RM to IPCS. However, the IVR Server configuration, and processing are different. In this scenario, IVR Server starts a strategy itself because it functions like a T-Server. It can use ISCC to pass attached data to the T-Server that is monitoring the DNs. The destination T-Server will provide the external route point for call routing purposes. Refer to the *Framework 7.6 SIP Server Deployment Guide* for detailed information about configuring In-Front-of-the-Switch mode.

Additional References

For additional information about integrating GVP and SIP Server, refer to the following White Papers, which are available from Genesys Technical Support or from Genesys Professional Services:

- SIP Server 7.2.1 GVP Integration—Behind Mode.
- SIP Server 7.2.1 GVP Integration—Standalone Mode.
- SIP Server 7.2.1 GVP Integration—Avaya S8X00.

Note: The preceding white papers are also relevant for the 7.6 release.

Limitations

- When using SIP Server, GVP, and Outbound Contact Server to perform outbound calls, the following limitations occur:
  - GVP attempts to use a busy DN.
  - SIP Server reports that an outbound call is not valid, but GVP reports that the same call is valid.

  These limitations occur because SIP Server physically maps available DNs to a GVP virtual ports group. GVP can assign the DNs to these virtual ports, but cannot send any DN information back to SIP Server in an outbound call scenario.
- GVP currently does not support an incoming `SIP RE-INVITE` message in the following scenario:
  - SIP Server performs a mute transfer call to an agent using the `REFER` method.
  - The agent attempts to bridge GVP with the call.
  - SIP Server uses Stream Manager to initiate a conference call with GVP.
- GVP will release a call when an agent places a call on hold, or attempts to perform a bridged transfer call.

Part

6 Appendixes

This part of the manual contains miscellaneous information in the following appendixes:

- Appendix A, “Configuring Dialogic,” on page 461
- Appendix B, “Manual Installation on Windows,” on page 505
- Appendix C, “Behind-the-Switch,” on page 523
- Appendix D, “Sample SNMP Configuration and Log Files (Solaris),” on page 527

Appendix

A Configuring Dialogic

This appendix describes how to manually configure the Dialogic software and troubleshoot the Dialogic Driver.

This appendix contains the following sections:

Configuring the Dialogic Software

This section describes how to configure your Dialogic Software for the appropriate signaling protocol after you manually install Genesys Voice Platform (GVP).

This section does not apply to GVP installations that were performed using the GVP Deployment Tool (GDT).

Note: Using Terminal Services might cause a failure to detect Dialogic boards after a restart. If this failure occurs, log off Terminal Service, and then log back on. If the board remains undetectable, contact Dialogic technical support.

This section includes the following information:

- "Configuring JCT Boards" on page 462
- "Configuring Dialogic DM/V-A Boards" on page 469
- "Configuring Dialogic DM/V-B Boards" on page 477
- "Additional Configuration for Non-ISDN" on page 493
- "Configuring Dialogic for Two B-Channel Transfer" on page 496

Configuring JCT Boards

This section describes how to configure JCT boards. It applies to the following JCT boards:

- D240JCT
- D480JCT
- D300JCT
- D600JCT

This section contains the following information:

- Required Configuration for All Signaling Protocols on JCT Boards
- Additional Configuration for JCT Boards Using T1/E1 ISDN (see page 464)
- Additional Configuration for JCT Boards Using T1/E1 Non-ISDN (see page 465)
  - Additional Configuration to use DTMF for ANI/DNIS for JCT T1/E1 (see page 466)
  - Additional Configuration to use MF for ANI/DNIS for JCT T1/E1 (see page 467)
  - Additional Configuration for E1-CAS. (see page 468)

Required Configuration for All Signaling Protocols on JCT Boards

You must complete the following procedure for all JCT boards, regardless of the signaling protocol that they require:

Procedure:
Configuring Signaling Protocols on JCT Boards

Start of procedure

1. In the Dialogic installation directory, edit the `<DialogicInstallDir>\CFG\icapi.cfg` configuration file as follows:

   In the section named `Parameter 14`, set the following parameter

   ```
   $14 Use of DTI Wait call function ( 0=auto detect, 1=disabled ) : 0
   ```

   equal to `1` for disabled, so that it looks like this:

   ```
   $14 Use of DTI Wait call function ( 0=auto detect, 1=disabled ) : 1
   ```

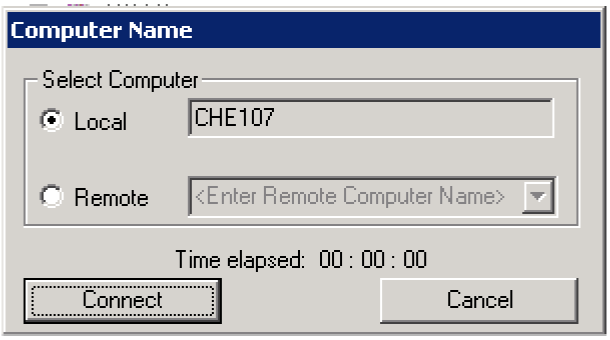
2. Set the T1 Framing and Suppression mode.

   Depending on your specific trunk configuration, you might need to make the following changes in the `<DialogicInstallDir>\Data\SpanDti.prm` file. Check with your trunk carrier for your particular settings.

- The default T1 framing is D4. If you need to use ESF, remove the semicolon from the beginning of the line `;0014 00` and change the `00` value to `01`, so that the line looks like this:
  `0014 01`
- By default, the Zero Code Suppression mode is `none`. If you need to use B8ZS, remove the semicolon from the beginning of the line `;0020 00` and change the value `00` to `01`, so that the line looks like this:
  `0020 01`

Note: If you make any changes to the `SpanDti.prm` file, you must restart the Dialogic Service either through Dialogic Configuration Manager (DCM), or Windows Services.

3. Start the DCM by selecting `Start > Program Files > Intel Dialogic System Release > Configuration Manager - DCM`. The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 53).



Computer Name

Select Computer

● Local CHE107

○ Remote <Enter Remote Computer Name>

Time elapsed: 00 : 00 : 00

Figure 53: Dialogic Configuration Manager Dialog Box

To connect:

- Select the `Local` radio button, and then click `Connect`.

4. In the main DCM window, right-click `Bus 0`, and then select `Configure Device` from the shortcut menu.
5. Click the `TDM Bus Configuration` tab, and configure the following parameters:
   - Set `TDM Bus Type (User Defined)` to `H.100`.
   - Set `Media Type (User Defined)` to `Alaw` for E1 boards, and `Mulaw` for T1 boards.

End of procedure

Additional Configuration for JCT Boards Using T1/E1 ISDN

Complete the following procedure for each JCT board that requires Integrated Services Digital Network (ISDN):

Procedure: Configuring JCT Boards Using T1/E1 ISDN

Start of procedure

1. From the Dialogic installation directory, edit the appropriate protocol file located in the `\Dialogic\Data\` directory.

   For T1 boards:

   - `NT1.prm`
   - `NI2.prm`
   - `DMS.prm`
   - `4ESS.prm`
   - `5ESS.prm`

   For E1 boards:

   - `NE1.prm`
   - `CTR4.prm`

   For the preceding file, complete the following steps:

   a. Open the file in a text editor.

   b. Locate the `0024` parameter near the end of the file. Remove the semicolon from the beginning of the line, and set the parameter to `10`, so that it looks as follows:
   `0024 10`

   c. For E1 protocol files, set the `CRC ENABLE SWITCH` parameter to `OFF` by setting the `000F` parameter to `00`.

   d. Save and close the file.

2. Start the DCM.

   The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 53 on page 463).

   Select the `Local` radio button, and then click `Connect`.

3. Double-click the board that you want to configure.

4. Click the `Interface` tab, and select the appropriate ISDN protocol for each span. Select `none` if that span is used for Continuous Speech Processing (CSP).

5. Click `OK`.

6. Right-click the board and select `Enable Device` from the shortcut menu.

7. Click the `Misc` tab.
8. Set the span to act as the CSP. The CSP enables the Automatic Speech Recognition (ASR) resource.
   a. Set `FirmwareFile` to `Default.`
   b. Set `FirmwareFile2` to `spcsp.fwl` (for a T1 configuration) or to `spe1csp.fwl` (for an E1 configuration).
9. Start the Dialogic Service by clicking the green button on the DCM toolbar.

End of procedure

Additional Configuration for JCT Boards Using T1/E1 Non-ISDN

Unless specifically stated, this section applies to all T1/E1 non-ISDN protocols, including:

- WinkStart
- GroundStart
- Channel Associated Signaling (CAS)
- R2MF

Procedure: Configuring JCT Boards Using T1/E1 ISDN

Start of procedure

1. Start the DCM.

   The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 53 on page 463).

   Select the `Local` radio button, and then click `Connect.`
2. Click `OK.` The DCM autodetects all of the boards.
3. Double-click `TDM Bus Configuration.`
4. Make sure that the `Media Type` parameter is set to `ALaw` for E1 protocols or `MuLaw` for T1 protocols, and the `TDM Bus Type` is set to `H.100.`
5. For each JCT board, make sure that the interface protocol is not set. Double-click the board.
6. Click the `Misc` tab.
7. To enable the Automatic Speech Recognition (ASR) resource, set the span to be used for Continuous Speech Processing (CSP).
   a. Set `FirmwareFile` to `Default.`

b. Set `FirmwareFile2` to `spcsp.fwl` (for a T1 configuration) or to `spe1csp.fwl` (for an E1 configuration).

8. If you are using T1-LoopStart signaling, set the `ParameterFile` parameter to `spandti.prm`.

9. Start the Dialogic Service by clicking the green button on the DCM toolbar.

End of procedure

Additional Configuration to use DTMF for ANI/DNIS for JCT T1/E1

If Automatic Number Identification (ANI)/Dialed Number Identification Service (DNIS) are generated using Dual-Tone Multi-Frequency (DTMF) tones, you must complete the following procedures for all non-ISDN T1/E1 protocols:

Procedure: Configuring DTMF for ANI/DNIS for JCT T1/E1

Start of procedure

1. In the Dialogic installation directory, edit the `..\Dialogic\CFG\us_mf_io.cdp` configuration file by setting the following parameters:

> Note: For loopback lab testing, also set these parameters in the `us_mf_loop_io.cdp` file.

- `$6 inter digit timeout (s) : 1`
- `$7 maximum number of DDI digits (excluded KP and ST) (inbound) : ZZZ`
- where `ZZZ` is the number of ANI digits, plus the number of DNIS digits, plus all separators. For example, if your carrier gives ANI/DNIS in the format `*4081234567*8005551111*` then set `ZZZ` to `23`.
- Check with your trunk carrier to find out the format in which ANI/DNIS are presented. If you are unsure of what value to enter for `ZZZ,` then try `30,` which is the maximum allowed.
- `$8 maximum number of ANI digits (excluded KP and ST) (inbound) : 0`
- `$9 Number of ring before speech (inbound) : 0`
- `$21 set to one if GCEV_ALERTING should be sent after : 0`
- `$16 collect/Send ANI after DDI (1=YES, 0=NO) : 1`
- `$41 return to idle after caller disconnection (outbound) (1=YES, 0=NO) : 1`

- `$47 T1 MF protocol option mask : 00`

Note: For each route, only one `.cdp` file can be used; you will specify this during VCS configuration.

End of procedure

Additional Configuration to use MF for ANI/DNIS for JCT T1/E1

If ANI/DNIS are generated using Multi Frequency (MF) tones, you must complete the following procedures for all non-ISDN T1/E1 protocols:

Procedure: Configuring MF for ANI/DNIS for JCT T1/E1

Start of procedure

1. In the Dialogic installation directory, edit the `..\Dialogic\CFG\us_mf_io.cdp` configuration file by setting the following parameters:

Note: For loopback lab testing, also set these parameters in `us_mf_loop_io.cdp` file.

- `$6 inter digit timeout (s) : 1`
- `$7 maximum number of DDI digits (excluded KP and ST) (inbound) : ZZZ`
- Where `ZZZ` is the number of ANI digits, plus the number of DNIS digits, plus all separators. For example, if your carrier gives ANI/DNIS in the format `*4081234567*8005551111*` then set `ZZZ` to `23`.
- Check with your trunk carrier to find out the format in which ANI/DNIS are presented. If you are unsure of what value to enter for `ZZZ`, then try `30`, which is the maximum allowed.
- `$8 maximum number of ANI digits (excluded KP and ST) (inbound) : 0`
- `$9 Number of ring before speech (inbound) : 0`
- `$21 set to one if GCEV_ALERTING should be sent after : 0`
- `$16 collect/Send ANI after DDI (1=YES, 0=NO) : 1`
- `$41 return to idle after caller disconnection (outbound) (1=YES, 0=NO) : 1`
- `$47 T1 MF protocol option mask : 02`

> Note: For each route, only one `.cdp` file can be used; you will specify this during VCS configuration.

End of procedure

Procedure: Configuring JCT for E1/CAS

Purpose: Additional Configuration for E1-CAS.

Start of procedure

1. Start the DCM.

   The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (See Figure 53 on page 463).

   Select the `Local` radio button, and then click `Connect`.
2. In the main DCM window, verify that the first parameter, `TDM Bus Type (User Defined)`, is set to `Default`.
3. Set the `Media Type` parameter to `Alaw` for E1 protocols, and then click `OK`.
4. Click on the `Interface` tab, and make sure that the interface protocol is not set for each JCT board.

> Note: You must verify that the file exists in the `bin\` directory. Also note that this is the general file naming convention; it might differ based on Intel/Dialogic requirements.

5. Run the DCM; it autodetects the JCT boards.
6. Modify the ANI digits and DNIS digits in the `pdk_in_r2_io.cdp` file, as follows:
   - `CDP_ANI_ENABLED :` (To enable ANI, set to `1;` to disable ANI, set to `0`)
   - `CDP_NO_OF_DNIS_BEFORE_CAT : 0`
   - `CDP_NUM_OF_DNIS_DIGITS : 10`
   - `CDP_NUM_OF_ANI_DIGITS : 10` (if ANI is enabled)
   - `CDP_DNIS_MaxDigits : 10`
   - `CDP_ANI_MaxDigits : 10` (if ANI is enabled)
7. Start the Dialogic system services.

End of procedure

Configuring Dialogic DM/V-A Boards

This section provides instructions for configuring the DM/V-A boards for the following protocols:

- Configuring DM/V-A Boards for T1-ISDN
- Configuring DM/V-A Boards for E1-ISDN (see page 471)
- Configuring DM/V-A Boards for T1/E1 Non-ISDN (see page 473)

  For additional configuration steps for non-ISDN, see “Additional Configuration for Non-ISDN” on page 493.
- Configuring Dialogic DM/V-A Boards for R2-MFC (see page 475)

Configuring DM/V-A Boards for T1-ISDN

If you are using ISDN call control signaling, you must complete the following configuration procedure:

Procedure: Configuring DM/V-A Boards for T1-ISDN

Start of procedure

1. Navigate to the directory in which `Dialogic\Data` is installed (typically `C:\Program Files\Dialogic\Data\`).
2. In a text editor, open the appropriate configuration file for your installed board:
   - For DM/V480A-2T1 board: `ml2_dsa_<xxx>.config`
   - For DM/V960A-4T1 board: `ml2_qsa_<xxx>.config`

   Where `<xxx>` is the ISDN protocol being used by the trunk—for example, `4ESS, 5ESS, DMS,` or `net5.`
3. Set T1 Framing by setting `LineType` to either `D4` or `ESF:`

   Each trunk has a `[LineAdmin.x]` section, where `x` is the physical trunk ID.

   In each of the `[LineAdmin.x]` sections, change `Setparm=0x1601.`
   - For D4: `Setparm=0x1601,0`
   - For ESF: `Setparm=0x1601,1`
4. Set Coding to either `B8ZS` or `AMI`:

   In each of the `[LineAdmin.x]` sections, change `Setparm=0x1603.`
   - For B8ZS: `Setparm=0x1603,7`
   - For AMI: `Setparm=0x1603,8`
5. Change the trunk to user-side:

   Each trunk has a `[CCS.x]` section, where `x` is the physical trunk ID.

In each `[CCS.x]` section, change `Setparm=0x17` to `Setparm=0x17,0`.

For loopback lab testing, one side must be user-side, and the other must be network-side. To configure the network side, set this line to `Setparm=0x17,1`.

6. Set the default port startup mode to `InService`:

   In the `[CHP]` section, change `Setparm=0x1311` to `Setparm=0x1311,1`.

7. Enable sending of B-channel maintenance messages:

   In the `[CHP]` section, change `Setparm=0x1312` to `Setparm=0x1312,0`.

> Note: Not all switches may use or require this parameter. Check with your switch vendor.

8. Save and close the file.
9. Open an MS-DOS command prompt and change the current directory to the `<Dialogic>\Data\` directory (typically `C:\Program Files\Dialogic\Data\`).
10. Run the following commands:
    - For DM/V480A-2T1 boards:

      ```
      ..\bin\fcdgen  ..\data\ml2_dsa_<xxx>.config
      ```

      This command should return the following line:

      ```
      Building ml2_dsa_<xxx>.fcd from ml2_dsa_<xxx>.config
      ```

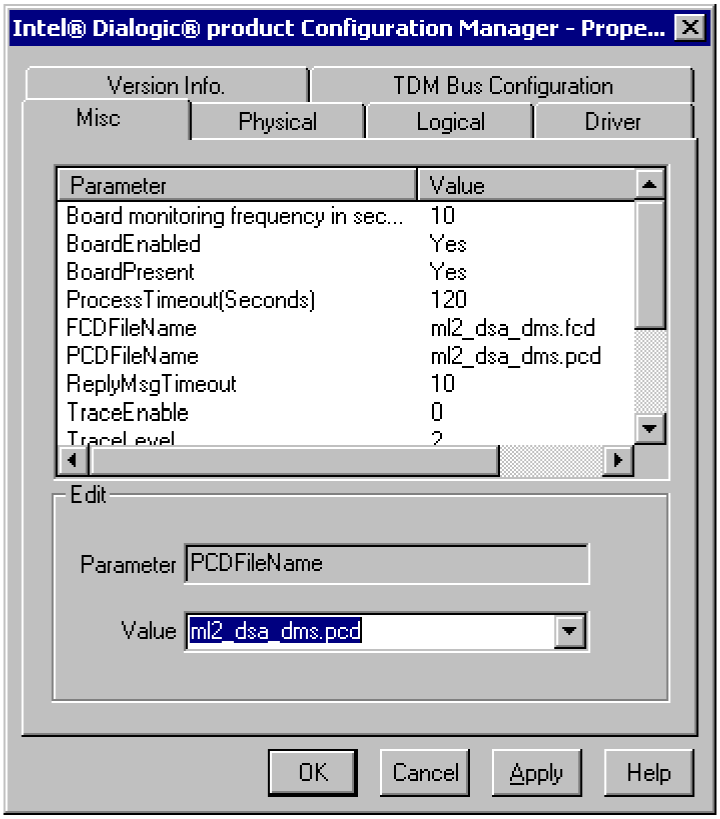
    - For DM/V960A-4T1 boards:

      ```
      ..\bin\fcdgen  ..\data\ml2_qsa_<xxx>.config
      ```

      This command should return the following line:

      ```
      Building ml2_qsa_<xxx>.fcd from ml2_qsa_<xxx>.config
      ```

11. Close the command prompt.
12. Start the DCM. A dialog box appears, prompting you for the computer connection (see Figure 53 on page 463).
13. Select the `Local` radio button, and then click `Connect`. Dialogic autodetects all of the boards.
14. Double-click on the board for which the firmware files are to be set.
15. Select the `Misc` tab and configure the correct firmware file (see Figure 54 on page 471).
    - For a DM/V480A-2T1 board: `ml2_dsa_<xxx>.pcd`.
    - For a DM/V960A-4T1 board: `ml2_qsa_<xxx>.pcd`.



Parameter	Value
Board monitoring frequency in sec...	10
BoardEnabled	Yes
BoardPresent	Yes
ProcessTimeout(Seconds)	120
FCDFileName	ml2_dsa_dms.fcd
PCDFileName	ml2_dsa_dms.pcd
ReplyMsgTimeout	10
TraceEnable	0
TraceLevel	2

Parameter PCDFileName

Value ml2_dsa_dms.pcd

Figure 54: Properties Dialog Box

16. Click `OK`.
17. Click the `TDM Bus Configuration` tab, and then right-click `TDM Bus`.
18. Ensure that the `Media Type` parameter is set to `MuLaw` for T1 protocols and that the `TDM Bus Type` is set to `H.100`.
19. Right-click the Dialogic board in the `DM3` node, and then select `Enable Device` from the shortcut menu.

    Configuration of the DM/V board is now complete.
20. Start the Dialogic Service by clicking the green button on the DCM toolbar.

End of procedure

Configuring DM/V-A Boards for E1-ISDN

If you are using ISDN call control signaling, you must complete the following configuration procedure:

Procedure: Configuring DM/NV-A Boards for E1-ISDN

Start of procedure

1. Navigate to the directory in which `Dialogic\Data` is installed (typically `C:\Program Files\Dialogic\Data`).
2. In a text editor, open the appropriate configuration file for your installed board:
   - For DM/V600A-2E1: `ml2_dsa_<xxx>.config`
   - For DM/V1200A-4E1: `ml2_qsa_<xxx>.config`

   Where `<xxx>` is the ISDN protocol being used by the trunk—for example, qsige1, net5, and so on.
3. Disable CRC by setting `LineType` to either `E1` or `E1_CRC`:

   Each trunk has a `[lineAdmin.x]` section, where `x` is the physical trunk ID. In each of the `[lineAdmin.x]` sections, change `Setparm=0x1601`.
   - To disable CRC: `Setparm=0x1601,2`
   - To enable CRC: `Setparm=0x1601,3`
4. Set `Coding` to either `AMI` or `HDB3`:

   In each of the `[lineAdmin.x]` sections, change `Setparm=0x1603`.
   - For AMI: `Setparm=0x1603,8`
   - For HDB3: `Setparm=0x1603,9`
5. Change the trunk to user-side:

   Each trunk has a `[CCS.x]` section, where `x` is the physical trunk ID. In each `[CCS.x]` section, change `Setparm=0x17` to `Setparm=0x17,0`.

   For loopback lab testing, one side must be user-side, and the other must be network-side. To configure the network side, set this line to `Setparm=0x17,1`.
6. Set the default port startup mode to `InService`:
   - In the `[CHP]` section, change `Setparm=0x1311` to `Setparm=0x1311,1`.
7. Enable sending of B-channel maintenance messages:
   - In the `[CHP]` section, change `Setparm=0x1312` to `Setparm=0x1312,0`.
8. Save and close the file.
9. Open an MS-DOS command prompt and change the current directory to the `<Dialogic>\Data\` directory (typically `C:\Program Files\Dialogic\Data\`).
10. Run the following commands:
    - `..\bin\fcdgen  ml2_dsa_<xxx>.config`

      This command should return the following line:

```
Building ml2_dsa_<xxx>.fcd from ml2_dsa_<xxx>.config
```

- `..\bin\fcdgen  ml2_qsa_<xxx>.config`

  This command should return the following line:

  ```
  Building ml2_qsa_<xxx>.fcd from ml2_qsa_<xxx>.config
  ```

11. Close the command prompt.
12. Start the DCM.

    The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (See Figure 53 on page 463).

    Select the `Local` radio button, and then click `Connect`.

    Dialogic autodetects all of the boards.
13. Select the board, right-click it, and select `Configure Device` from the shortcut menu.
14. Click the `Misc` tab, and select the appropriate firmware file for your installed board:
    - For a DM/V600A-2E1 board: `ml2_dsa_<xxx>.pcd`
    - For a DM/V1200A-4E1 board,: `ml2_qsa_<xxx>.pcd`

    Click `OK`.
15. Click the `TDM Bus Configuration` tab, and then right-click `TDM Bus`.
16. Make sure that the `Media Type` parameter is set to `ALaw` for E1 protocols or `MuLaw` for T1 protocols, and that the `TDM Bus Type` is set to `H.100`.
17. Right-click the Dialogic board in the `DM3` node, and then select `Enable Device` from the shortcut menu.

    Configuration of the DM/V board is now complete.
18. Start the Dialogic Service by clicking the green button on the DCM toolbar.

End of procedure

Configuring DM/V-A Boards for T1/E1 Non-ISDN

Note: Before you can configure these boards, you must download the Global Call (PDK) protocol module and the country dependent parameters (CDP) to the DM3 boards. For more information, see the “Downloading the Protocol and CDP File on DM3 Boards” section of the *Global Call Country Dependent Parameters (CDP) for PDK Protocols Configuration Guide* by Intel.

Unless specifically stated, this section applies to all T1/E1 non-ISDN protocols, including:

- WinkStart

- CAS

Procedure: Configuring DM/V-A Boards for T1/E1 Non-ISDN

Start of procedure

1. Navigate to the directory in which `Dialogic\Data` is installed (typically `C:\Program Files\Dialogic\Data\`).
2. In a text editor, open the appropriate configuration file for your installed board:
   - For DM/V480A-2T1: `ml2_dsa_cas.config`
   - For DM/V960A-4T1: `ml2_qsa_cas.config`
3. Set T1 Framing by setting `LineType` to either `D4` or `ESF`:

   Each trunk has a `[lineAdmin.x]` section, where `x` is the physical trunk ID. In each of the `[lineAdmin.x]` sections, change `Setparm=0x1601`.
   - For D4: `Setparm=0x1601,0`
   - For ESF: `Setparm=0x1601,1`
4. Set `Coding` to either `B8ZS` or `AMI`:

   In each of the `[lineAdmin.x]` sections, change `Setparm=0x1603`.
   - For B8ZS: `Setparm=0x1603,7`
   - For AMI: `Setparm=0x1603,8`
5. Save and close the file.
6. Open an MS-DOS command prompt and change the current directory to the `<Dialogic>\Data\` directory (typically `C:\Program Files\Dialogic\Data\`).
7. Run the following commands:
   - `..\bin\fcdgen ml2_dsa_cas.config`

     This should return the following line:

     ```
     Building ml2_dsa_cas.fcd from ml2_dsa_cas.config
     ```
   - `..\bin\fcdgen ml2_qsa_cas.config`

     This should return the following line:

     ```
     Building ml2_qsa_cas.fcd from ml2_qsa_cas.config
     ```
8. If you are using a protocol variant (for example, `pdk_us_mf_io.cdp`) other than the Dialogic default, edit the `pdk.cfg` file to specify the protocol variant. For more information, see Configuring T1/E1 Non-ISDN to Use Specific Protocol Variants, page 494.

9. You may need to change the ANI configuration in the *.cdp file to match the far end. For more information, see "Additional Configuration for ANI/DNIS for T1/E1 Non-ISDN" on page 493. See also Step 6 in the section, Configuring T1/E1 Non-ISDN to Use Specific Protocol Variants, page 494.

   If the far end does not send ANI, disable ANI in the *.cdp file as well (set CDP_IN_ANI_Enabled and CDP_OUT_ANI_Enabled to 0). Also modify SYS_FEATURES to remove FEATURE_ANI from the features. For example, to disable ANI, change pdk_us_mf_io.cdp as follows:

   - All BOOLEAN_t CDP_IN_ANI_Enabled:0
   - All BOOLEAN_t CDP_OUT_ANI_Enabled:0
   - All CHARSTRING_t SYS_FEATURES:feature_outbound, feature_inbound, feature_DNIS,feature_transfer, feature_hold

10. Start the DCM.

    The first time you start the DCM, a dialog box appears, prompting you for the computer connection (seeFigure 53 on page 463).

11. Select the Local radio button, and then click Connect. Dialogic autodetects all of the boards.
12. Double-click on the board for which the firmware files are to be set.
13. Select the Misc tab and configure the correct firmware file (see Figure 54 on page 471).
    - For a DM/V480A-2T1 board: ml2_dsa_cas.pcd and ml2_dsa_cas.fcd
    - For a DM/V960A-4T1 board: ml2_qsa_cas.pcd and ml2_qsa_cas.fcd
14. Click OK.Configuration of the DM/V board is now complete.
15. Click the green button on the DCM toolbar to start the Dialogic Service.

End of procedure

Configuring Dialogic DM/V-A Boards for R2-MFC

To configure Dialogic for DM/V-A boards for R2-MFC complete the following procedure:

Procedure: Configuring Dialogic DM/V-A Boards for R2-MFC

Start of procedure

1. Start the DCM.

   The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 53 on page 463). Select the Local radio button, and then click Connect.

Dialogic autodetects all of the boards.

2. Double-click on the board for which the firmware files are to be set.
3. Select the `Misc` tab and configure the correct firmware file (see Figure 54 on page 471).
   - For a DM/V600A-2E1 board: `ml2_dsa_r2mf.pcd`
   - For a DM/V1200A-4E1 board: `ml2_qsa_r2mf.pcd`
4. Click `OK`.
5. For each configuration file created by the above procedure, perform the following:

   a. Open the file in a text editor such as Notepad.

   b. Set the CRC Framing.

   This is done by setting the `LineType` to `E1_CRC`. Each trunk has a `[lineAdmin.x]` section, where `x` is the physical trunk ID.

   - In the `gul1_dsb_2_r2mf.config` file (used by DMV600B-2T1 boards), you will have `[lineAdmin.1]` and `[lineAdmin.2]` sections.
   - In the `gul1_dsb_4_r2mf.config` file (used by DMV1200B-4T1 boards), you will have `[lineAdmin.1]`, `[lineAdmin.2]`, `[lineAdmin.3]`, and `[lineAdmin.4]` sections.

   In each of the `[lineAdmin.x]` sections, change `Setparm=0x1601`:

   - For CRC OFF: `Setparm=0x1601,2`
   - For CRC ON: `Setparm=0x1601,3`

   c. Set Coding to either B8ZS, AMI, or HDB3.

   In each of the `[lineAdmin.x]` sections, change `Setparm=0x1603`:

   - For B8ZS: `Setparm=0x1603,7`
   - For AMI: `Setparm=0x1603,8`
   - For HDB3: `Setparm=0x1603,9`

   d. Save and close the file.
6. Open an MS-DOS command prompt and change the current directory to `<Dialogic>\Data` (typically `c:\program files\dialogic\data`).

   Execute the following commands:

   - `..\bin\fcdgen gul1_dsb_<n>_<trunk type>.config`

     This command returns you to the command prompt.
   - `..\bin\fcdgen gul1_qsb_<n>_<trunk type>.config`

     This command returns you to the command prompt.
7. If you are using a protocol variant (for example, `pdk_us_mf_io.cdp`) other than the Dialogic default, edit the `pdk.cfg` file to specify the protocol variant. For more information, see Configuring T1/E1 Non-ISDN to Use Specific Protocol Variants, page 494.

8. You may need to change the ANI configuration in the `*.cdp` file to match the far end. For more information, see "Additional Configuration for ANI/DNIS for T1/E1 Non-ISDN" on page 493. See also Step 6 in the section, Configuring T1/E1 Non-ISDN to Use Specific Protocol Variants, page 494.
9. Select `TDM Bus`, and set `Media Type (User Defined)` to `Alaw`.

   Configuration of the DM/V board is now complete.
10. Start the Dialogic Service by clicking the green button on the DCM toolbar.

End of procedure

Configuring Dialogic DM/V-B Boards

This section provides instructions for configuring the DM/V-B boards for the following protocols:

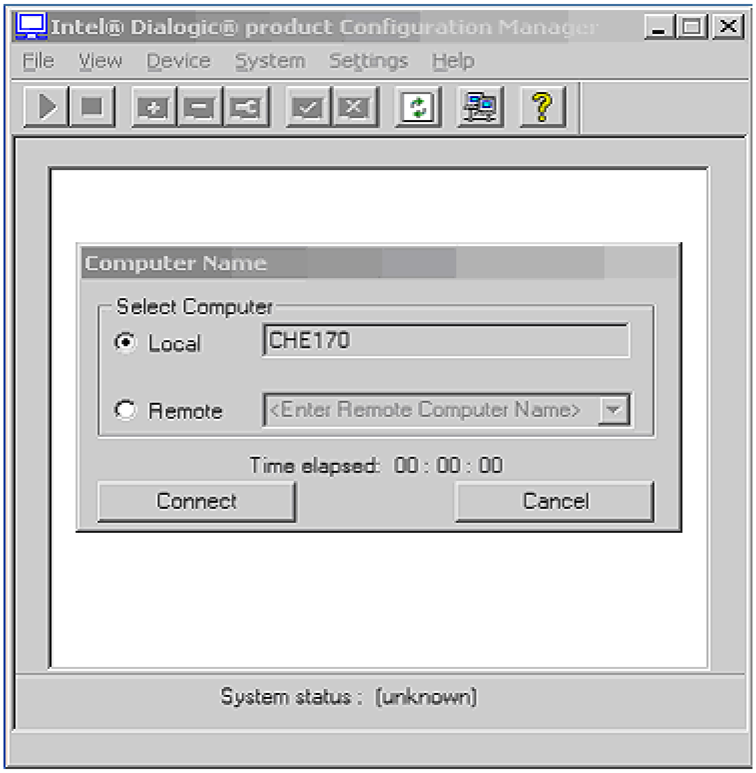
- Configuring Dialogic DM/V-B Boards for T1-ISDN
- Configuring Dialogic DM/V-B Boards for E1-ISDN (see page 483)
- Configuring Dialogic DM/V-B Boards for T1-RobbedBit (see page 486)
- Configuring Dialogic DM/V-B Boards for E1-CAS (see page 489)

In addition, there are special configuration steps for non-ISDN. For more information, see page 483.

Procedure: Configuring Dialogic DM/V-B Boards for T1-ISDN

Start of procedure

1. Start the DCM by selecting `Start > Program Files > Intel Dialogic System Release > Configuration Manager - DCM`. The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 55).



Select Computer

● Local CHE170

○ Remote <Enter Remote Computer Name>

Time elapsed: 00 : 00 : 00

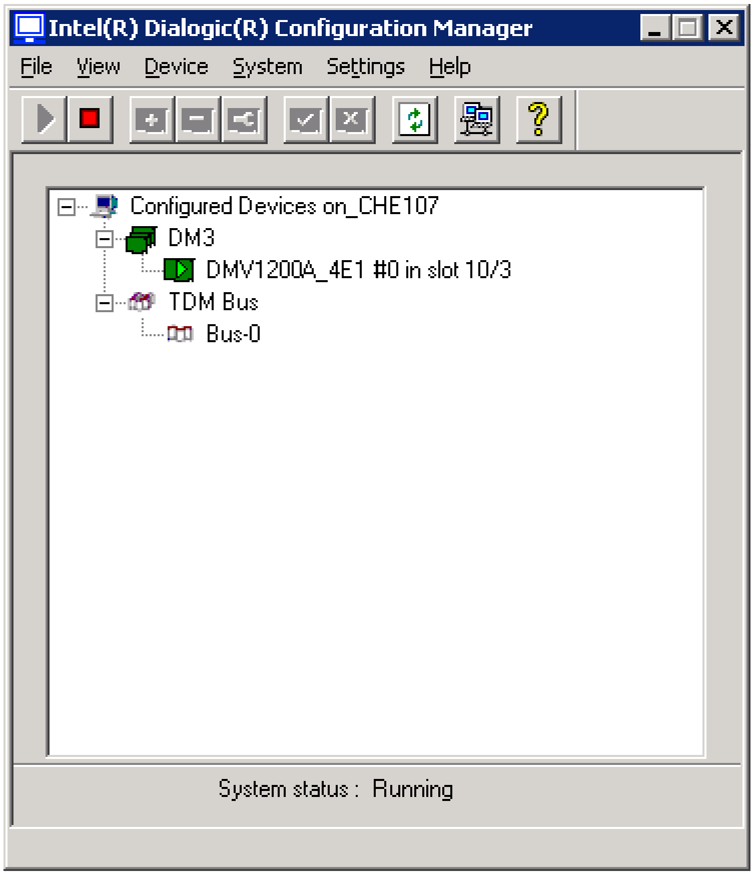
System status : (unknown)

Figure 55: Computer Name Screen

> Note: If you have started DCM before, you will not get the above prompt.

2. To connect:
   - Select the `Local` radio button, and then click `Connect`.

   Dialogic autodetects all the boards, and then displays the main DCM window (see Figure 56).

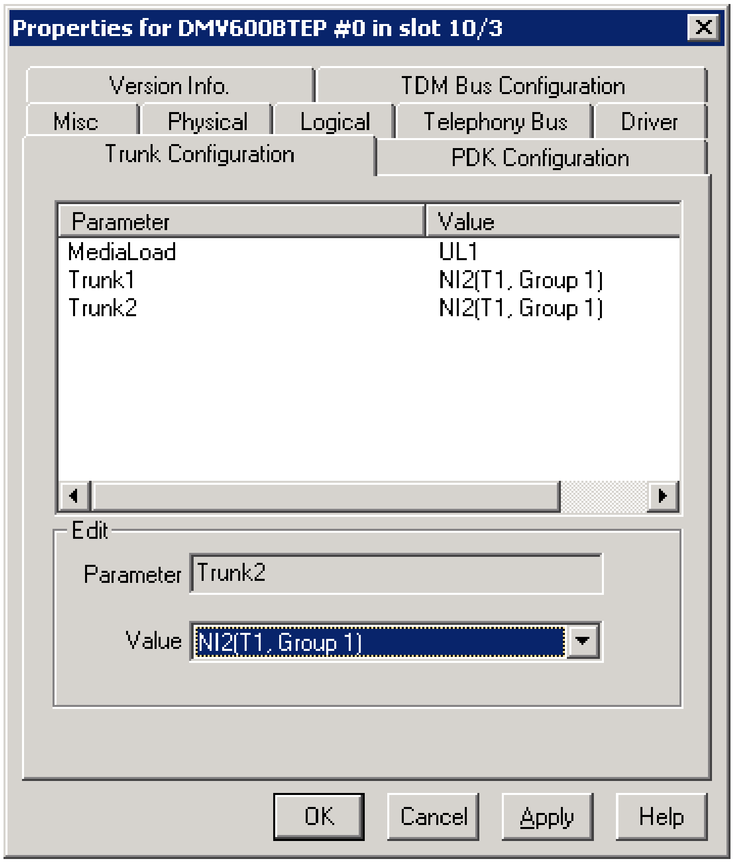

Intel(R) Dialogic(R) Configuration Manager
File View Device System Settings Help

Configured Devices on_CHE107
DM3
DMV1200A_4E1 #0 in slot 10/3
TDM Bus
Bus-0

System status : Running

Figure 56: Dialogic product Configuration Manager

3. Double-click the board model name in the main DCM window to display the property sheet for the board.
4. Click the `Trunk Configuration` tab (see Figure 57).



Properties for DMV600BTEP #0 in slot 10/3

Parameter	Value
MediaLoad	UL1
Trunk1	NI2(T1, Group 1)
Trunk2	NI2(T1, Group 1)

Parameter: Trunk2

Value: NI2(T1, Group 1)

Figure 57: Trunk Configuration

5. To configure a DMV600BTEP or DMV1200BTEP board:
   a. Click the `Trunk1` parameter.
   b. In the `Value` text box, select the protocol to be assigned to this board.

Note: E1 and T1 protocol Groups cannot be configured together. For example, a single DMV600BTEP card cannot be configured with one T1 ISDN protocol, and one E1 ISDN protocol.

Table 80 on page 481 shows the protocol groups.

Table 80: Trunk Protocols

Protocol Group	Protocols
ISDN T1	• 4ESS • 5ESS • NTT • NI2 • DMS • QSIGT1
ISDN E1	• NET5 • QSIGE1
ISDN British Telecom	• DPNSS • DASS2
T1 CAS	• CAS • T1 CLEAR CHANNEL
E1 CAS	• R2MF • E1 CLEAR CHANNEL

c. Configure each trunk as specified in step a and b above.

d. Click `Apply` to save the configuration. DCM will display a message indicating that the new configuration file will be created.

e. Click `OK`. A `.config` file and the related `.fcd` and `.pcd` files will be written to the `c:\program files\dialogic\data` directory.

The configuration fileset will have the following format for DMV600B boards:

- `g<media load>_dsb_<n>_<trunk type 1>_<m>_<Trunk Type 2>`

Example:

If you have a media load ULI, trunk type 1 as ni2 (E1), and trunk type 2 as ni2 (E1), then the configuration file created will be:
`gul1_dsb_2_ni2.config`

Also, `gul1_dsb_2_ni2.pcd` and `gul1_dsb_2_ni2.fcd` files will be created for a DM/V480B-2T1 board.

6. For each configuration file created by the above procedure, do the following:

a. Open the file in a text editor such as Notepad.

b. Set the `default port startup mode` to `InService`:

- In the `[CHP]` section, change `Setparm=0x1311` to `Setparm=0x1311, 1`.

c. Enable the sending of B-channel maintenance messages:

- In the `[CHP]` section, change `Setparm=0x1312` to `Setparm=0x1312,0`.

d. Change the trunk to be user-side.

Each trunk has a `[CCS.x]` section, where `x` is the physical trunk ID.

In the `gul1_dsb_2_ni2.config` file (used by the DMV600BTEP boards), you will have `[CCS.1]` and `[CCS.2]` sections.

In the `gul2_dsb_4_ni2.config` file (used by the DMV1200BTEP boards), you will have `[CCS.1]`, `[CCS.2]`, `[CCS.3]`, and `[CCS.4]` sections.

In each of these `[CCS.x]` sections, change `Setparm=0x17` to `Setparm=0x17,0` to indicate that the trunk is user-side.

For lab loopback testing, one side must be user-side, and the other must be network-side. To configure it as network-side, set it as `Setparm=0x17,1`.

e. Set the `T1 Framing`. This is done by setting the `LineType` to either `D4` or `ESF`.

Each trunk has a `[LineAdmin.x]` section, where x is the physical trunk ID.

In the `gul1_dsb_2_ni2.config` file (used by the DMV600B-2T1 boards), you will have `[LineAdmin.1]` and `[LineAdmin.2]` sections.

In the `gul1_dsb_4_ni2.config` file (used by the DMV1200B-4T1 boards), you will have `[LineAdmin.1]`, `[LineAdmin.2]`, `[LineAdmin.3]`, and `[LineAdmin.4]` sections.

In each of the `[LineAdmin.x]` sections, change `Setparm=0x1601`.

- For D4: `Setparm=0x1601,0`
- For ESF: `Setparm=0x1601,1`

f. Set `Coding` to either `B8ZS` or `AMI`.

In each of the `[LineAdmin.x]` sections, change `Setparm=0x1603`.

- For B8ZS: `Setparm=0x1603,7`
- For AMI: `Setparm=0x1603,8`

g. Save the file and close it.

7. Open a MS-DOS command prompt, and change the current directory to `<Dialogic>\Data` (typically `c:\program files\dialogic\data`). Execute the following commands:

- `..\bin\fcdgen gul1_dsb_<n>_<trunk type>.config`

  This command should return to the command prompt.

- `..\bin\fcdgen gul1_qsb_<n>_<trunk type>.config`

  This command should return to the command prompt.

The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 55).

Note: If you have started DCM before, you will not get the above prompt.

8. To connect:

- Select the `Local` radio button, and then click `Connect`.

End of procedure

Procedure:
Configuring Dialogic DM/V-B Boards for E1-ISDN

Start of procedure

1. Start the DCM by selecting `Start > Program Files > Intel Dialogic System Release > Configuration Manager - DCM`.

The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 55).

Note: If you have started DCM before, you will not get the above prompt.

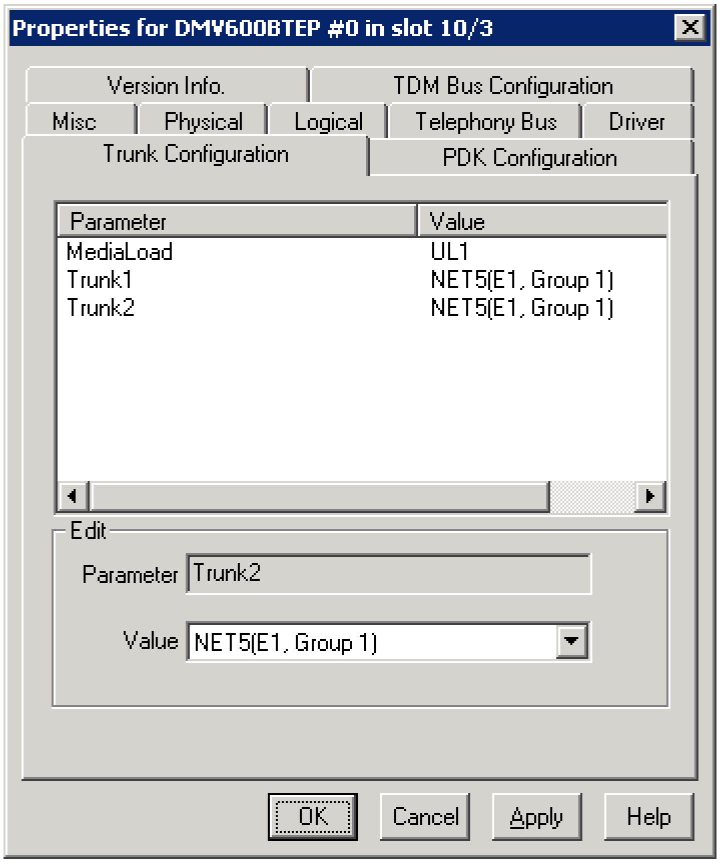
2. To connect:

- Select the `Local` radio button, and then click `Connect`.

Dialogic autodetects all the boards, and then displays the main DCM window (see Figure 56).

3. Double-click the board model name in the main DCM window to display the property sheet for the board.

Click the `Trunk Configuration` tab (see Figure 58 on page 484).



Properties for DMV600BTEP #0 in slot 10/3

Parameter	Value
MediaLoad	UL1
Trunk1	NET5(E1, Group 1)
Trunk2	NET5(E1, Group 1)

Edit

Parameter: Trunk2

Value: NET5(E1, Group 1)

Figure 58: Trunk Configuration

4. To configure a DMV600BTEP or DMV1200BTEP board:

a. Click the `Trunk1` parameter.

b. In the `Value` text box, select the protocol to be assigned to this board.

> `Note:` E1 and T1 protocol Groups cannot be configured together. For example, a single DMV600BTEP card cannot be configured with one T1 ISDN protocol and one E1 ISDN protocol.

The protocol groups are shown in Table 80 on page 481.

c. Configure each trunk as specified in step a and b above.

d. Click `Apply` to save the configuration. DCM will display a message indicating that the new configuration file will be created.

e. Click `OK`. A `.config` file and the related `.fcd` and `.pcd` files will be written to the `c:\program files\dialogic\data` directory.

The configuration fileset will have the following format for DMV600B boards:

- `g<media load>_dsb_<n>_<trunk type 1>_<m>_<Trunk Type 2>`

Example:

If you have a media load ULI, trunk type 1 as net5 (E1), and trunk type 2 as net5 (E1), then the configuration file created will be: gul1_dsb_2_net5.config

Also, gul1_dsb_2_net5.pcd and gul1_dsb_2_net5.fcd files will be created for a DMV600BTEP board.

5. For each configuration file created by the above procedure, do the following:
   a. Open the file in a text editor such as Notepad.
   b. Set the default port startup mode to InService:
      - In the [CHP] section, change Setparm=0x1311 to Setparm=0x1311,1.
   c. Enable the sending of B-channel maintenance messages:
      - In the [CHP] section, change Setparm=0x1312 to Setparm=0x1312,0.
   d. Change the trunk to be user-side.

      Each trunk has a [CCS.x] section, where x is the physical trunk ID.

      In the gul1_dsb_2_net5.config file (used by the DMV600BTEP boards), you will have [CCS.1] and [CCS.2] sections.

      In the gul2_dsb_4_net5.config file (used by the DMV1200BTEP boards), you will have [CCS.1], [CCS.2], [CCS.3], and [CCS.4] sections.

      In each of these [CCS.x] sections, change Setparm=0x17 to Setparm=0x17,0 to indicate that the trunk is user-side.

      For lab loopback testing, one side must be user-side, and the other must be network-side. To configure it as network-side, set it as Setparm=0x17,1.
   e. Set the Framing CRC. This is done by setting the LineType to either CRC ON or CRC OFF.

      Each trunk has a [lineAdmin.x] section, where x is the physical trunk ID.

      In the gul1_dsb_2_net5.config file (used by the DMV600B-2T1 boards), you will have [lineAdmin.1] and [lineAdmin.2] sections.

      In the gul1_dsb_4_net5.config file (used by the DMV1200B-4T1 boards), you will have [lineAdmin.1], [lineAdmin.2], [lineAdmin.3], and [lineAdmin.4] sections.

      In each of the [lineAdmin.x] sections, change Setparm=0x1601.
      - For CRC OFF: Setparm=0x1601,2
      - For CRC ON: Setparm=0x1601,3
   f. Set Coding to either B8ZS, AMI, or HDB3.

      In each of the [lineAdmin.x] sections, change Setparm=0x1603.
      - For B8ZS: Setparm=0x1603,7
      - For AMI: Setparm=0x1603,8
      - For HDB3: Setparm=0x1603,9
   g. Save the file and close it.

6. Open an MS-DOS command prompt, and change the current directory to `<Dialogic>\Data` (typically `c:\program files\dialogic\data`). Execute the following commands:

   a. `..\bin\fcdgen gul1_dsb_<n>_<trunk type>.config.`

      This command should return to the command prompt.

   b. `..\bin\fcdgen gul1_qsb_<n>_<trunk type>.config.`

      This command should return to the command prompt.

7. Start the DCM by selecting `Start > Program Files > Intel Dialogic System Release > Configuration Manager - DCM.`

   The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 55).

   Note: If you have started DCM before, you will not get the above prompt.

8. To connect:

   - Select the `Local` radio button, and then click `Connect.`

End of procedure

Procedure:
Configuring Dialogic DM/V-B Boards for T1-RobbedBit

Start of procedure

1. Start the DCM by selecting `Start > Program Files > Intel Dialogic System Release > Configuration Manager - DCM.`

   The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 55).

   Note: If you have started DCM before, you will not get the above prompt.

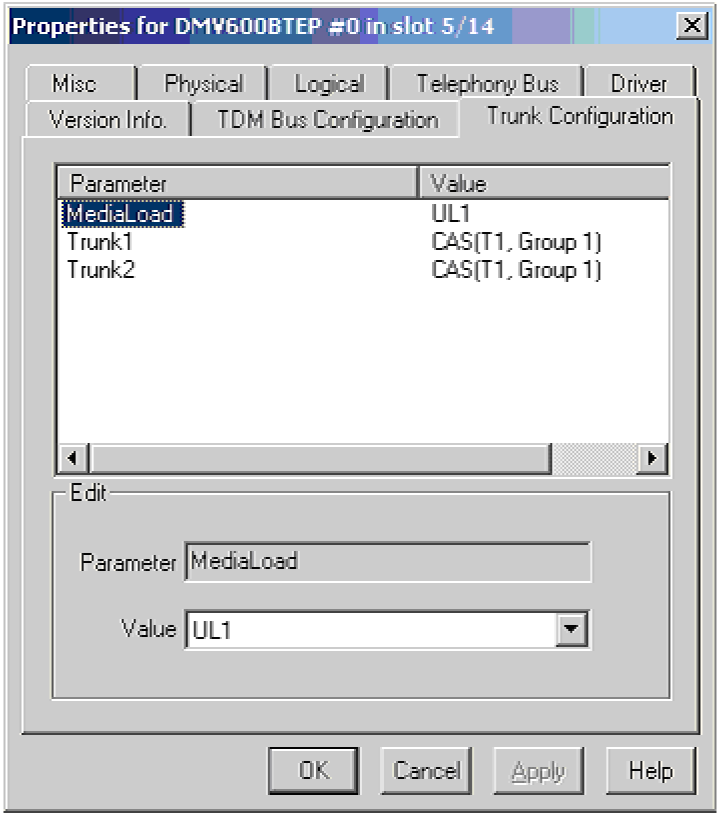
2. To connect:

   - Select the `Local` radio button, and then click `Connect.`

   Dialogic autodetects all the boards, and then displays the main DCM window (see Figure 56).

3. Double-click the board model name in the main DCM window to display the property sheet for the board.

4. Click the `Trunk Configuration` tab (see Figure 59).



Parameter	Value
MediaLoad	UL1
Trunk1	CAS(T1, Group 1)
Trunk2	CAS(T1, Group 1)

Parameter: MediaLoad

Value: UL1

Figure 59: Trunk Configuration

5. To configure a DMV600BTEP or DMV1200BTEP board:

a. Click the `Trunk1` parameter.

b. In the `Value` text box, select the protocol to be assigned to this board.

`Note:` E1 and T1 protocol Groups cannot be configured together. For example, a single DMV600BTEP card cannot be configured with one T1 non-ISDN protocol and one E1 non-ISDN protocol.

The protocol groups are shown in Table 80 on page 481.

c. Configure each trunk as specified in step a and b above.

d. Click `Apply` to save the configuration. DCM will display a message indicating that the new configuration file will be created.

e. Click `OK`. A `.config` file and the related `.fcd` and `.pcd` files will be written to the `c:\program files\dialogic\data` directory.

The configuration fileset will have the following format for DMV600B boards:

- `g<media load>_dsb_<n>_<trunk type 1>_<m>_<Trunk Type 2>`

Example:

If you have a media load ULI, trunk type 1 as cas (E1), and trunk type 2 as cas (E1), then the configuration file created will be: `gul1_dsb_2_cas.config`

Also, `gul1_dsb_2_cas.pcd` and `gul1_dsb_2_cas.fcd` files will be created.

6. For each configuration file created by the above procedure, do the following:
   a. Open the file in a text editor such as Notepad.
   b. Set the `T1 Framing`. This is done by setting the `LineType` to either `D4`, or `ESF`.

      Each trunk has a `[lineAdmin.x]` section, where x is the physical trunk ID.

      In the `gul1_dsb_2_cas.config` file (used by the DMV600B-TEB boards), you will have `[lineAdmin.1]` and `[lineAdmin.2]` sections.

      In the `gul1_dsb_4_cas.config` file (used by the DMV1200B-TEB boards), you will have `[lineAdmin.1]`, `[lineAdmin.2]`, `[lineAdmin.3]`, and `[lineAdmin.4]` sections.

      In each of the `[lineAdmin.x]` sections, change `Setparm=0x1601`.
      - For D4: `Setparm=0x1601,0`
      - For ESF: `Setparm=0x1601,1`
   c. Set `Coding` to either `B8ZS`, or `AMI`.

      In each of the `[lineAdmin.x]` sections, change `Setparm=0x1603`.
      - For B8ZS: `Setparm=0x1603,7`
      - For AMI: `Setparm=0x1603,8`
   d. Save the file and close it.
7. Open an MS-DOS command prompt, and change the current directory to `<Dialogic>\Data` (typically `c:\program files\dialogic\data`). Execute the following commands:
   - `..\bin\fcdgen gul1_dsb_<n>_<trunk type>.config`

     This command should return to the command prompt.
   - `..\bin\fcdgen gul1_qsb_<n>_<trunk type>.config`

     This command should return to the command prompt.
8. If you are using a protocol variant (for example, `pdk_us_mf_io.cdp`) other than the Dialogic default, edit the `pdk.cfg` file to specify the protocol variant. For more information, see Configuring T1/E1 Non-ISDN to Use Specific Protocol Variants, page 494.
9. You may need to change the ANI configuration in the `*.cdp` file to match the far end. For more information, see “Additional Configuration for ANI/DNIS for T1/E1 Non-ISDN” on page 493. See also Step 6 in the section, Configuring T1/E1 Non-ISDN to Use Specific Protocol Variants, page 494.

If the far end does not send ANI, disable ANI in the `*.cdp` file as well (set `CDP_IN_ANI_Enabled` and `CDP_OUT_ANI_Enabled` to `0`). Also modify `SYS_FEATURES` to remove `FEATURE_ANI` from the features. For example, to disable ANI, change `pdk_us_mf_io.cdp` as follows:

- `All BOOLEAN_t CDP_IN_ANI_Enabled:0`
- `All BOOLEAN_t CDP_OUT_ANI_Enabled:0`
- `All CHARSTRING_t SYS_FEATURES:feature_outbound, feature_inbound, feature_DNIS,feature_transfer, feature_hold`

10. Start the DCM by selecting `Start > Program Files > Intel Dialogic System Release > Configuration Manager - DCM`.

The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 55).

Note: If you have started DCM before, you will not get the above prompt.

11. To connect:

- Select the `Local` radio button, and then click `Connect`.

End of procedure

Procedure: Configuring Dialogic DM/V-B Boards for E1-CAS

Start of procedure

1. Start the DCM by selecting `Start > Program Files > Intel Dialogic System Release > Configuration Manager - DCM`. The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 55).

Note: If you have started DCM before, you will not get the above prompt.

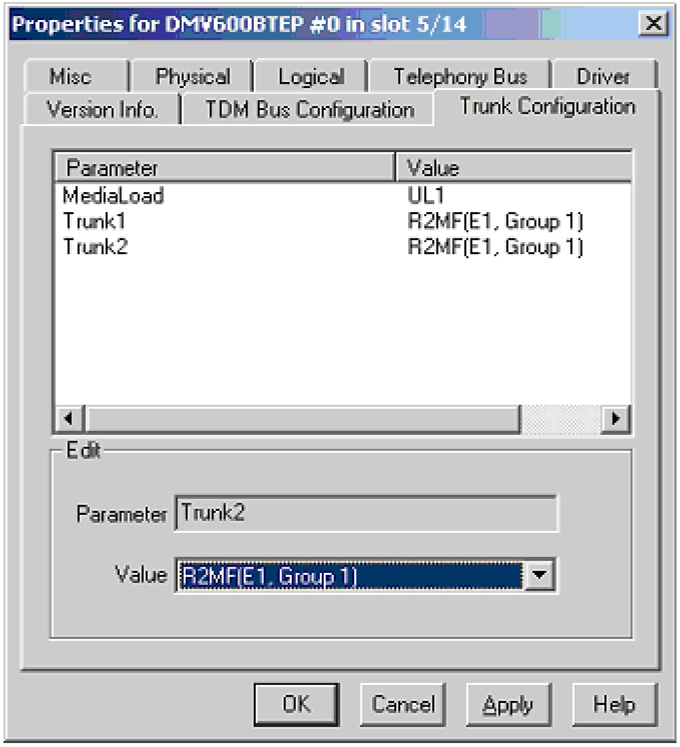
2. To connect:

- Select the `Local` radio button, and then click `Connect`.

Dialogic autodetects all the boards, and then displays the main DCM window (see Figure 56).

3. Double-click the board model name in the main DCM window to display the property sheet for the board.

4. Click the `Trunk Configuration` tab (see Figure 60).



Properties for DMV600BTEP #0 in slot 5/14

Parameter	Value
MediaLoad	UL1
Trunk1	R2MF(E1, Group 1)
Trunk2	R2MF(E1, Group 1)

Parameter: Trunk2

Value: R2MF(E1, Group 1)

Figure 60: Trunk Configuration

5. To configure a DMV600BTEP or DMV1200BTEP board:

a. Click the `Trunk1` parameter.

b. In the `Value` text box, select the protocol to be assigned to this board.

> Note: E1 and T1 protocol Groups cannot be configured together. For example, a single DMV600BTEP card cannot be configured with one T1 non-ISDN protocol and one E1 non-ISDN protocol.

The protocol groups are shown in Table 80 on page 481.

c. Configure each trunk as specified in step a and b above.

d. Click `Apply` to save the configuration. DCM will display a message indicating that the new configuration file will be created.

e. Click `OK`. A `.config` file and the related `.fcd` and `.pcd` files will be written to the `c:\program files\dialogic\data` directory.

The configuration fileset will have the following format for DMV600B boards:

- `g<media load>_dsb_<n>_<trunk type 1>_<m>_<Trunk Type 2>`

Example:

If you have a media load ULI, trunk type 1 as r2mf (E1), and trunk type 2 as r2mf (E1), then the configuration file created will be: `gul1_dsb_2_r2mf.config`

Also, `gul1_dsb_2_r2mf.pcd` and `gul1_dsb_2_r2mf.fcd` files will be created.

6. For each configuration file created by the above procedure, do the following:

a. Open the file in a text editor such as Notepad.

b. Set the `CRC Framing`. This is done by setting the `LineType` to `E1_CRC` or not.

Each trunk has a `[LineAdmin.x]` section, where `x` is the physical trunk ID.

In the `gul1_dsb_2_r2mf.config` file (used by the DMV600B-2T1 boards), you will have `[LineAdmin.1]` and `[LineAdmin.2]` sections.

In the `gul1_dsb_4_r2mf.config` file (used by the DMV1200B-4T1 boards), you will have `[LineAdmin.1], [LineAdmin.2], [LineAdmin.3],` and `[LineAdmin.4]` sections.

In each of the `[LineAdmin.x]` sections, change `Setparm=0x1601`.

- For CRC OFF: `Setparm=0x1601,2`
- For CRC ON: `Setparm=0x1601,3`

c. Set `Coding` to either `B8ZS`, `AMI, or HDB3`.

In each of the `[LineAdmin.x]` sections, change `Setparm=0x1603`.

- For B8ZS: `Setparm=0x1603,7`
- For AMI: `Setparm=0x1603,8`
- For HDB3: `Setparm=0x1603,9`

d. Save the file and close it.

7. Open an MS-DOS command prompt, and change the current directory to `<Dialogic>\Data` (typically `c:\program files\dialogic\data`). Execute the following commands:

- `..\bin\fcdgen gul1_dsb_<n>_<trunk type>.config.`

  This command should return to the command prompt.
- `..\bin\fcdgen gul1_qsb_<n>_<trunk type>.config.`

  This command should return to the command prompt.

8. Open an MS-DOS command prompt, and change the current directory to `<Dialogic>\bin.`

9. At the dos prompt, type `PdkManagerRegsetup add`.

10. Using Windows Explorer, navigate to `<Dialogic>\cfg`.

11. Look for the `pdk.cfg` file.

- If the `pdk.cfg` does not exist, create an empty file by this name using Notepad.

- If the pdk.cfg file does exist, open the file in Notepad and delete the contents.

12. Using Notepad, edit the pdk.cfg file, and add a line for each T1-RobbedBit/E1-CAS based DM3 board in the following format:

```
board <b> fcdfile <f> pcdfile <p> variant <v> mlmfile
universal_pdk_qfc3_xscale.mlm.sym
```

where:

<b> is the logical board number. To get the logical board number, use the listboards utility located in <dialogic>\bin.

<f> is the .fcd file assigned to that board in the DCM.

<p> is the .pcd file assigned to that board in the DCM.

<v> is the name of the CDP file for the protocol to be used. For example, pdk_ar_r2_io.cdp.

Note: The variant field is needed only for the T1-RobbedBit/E1-CAS based protocols.

A sample line in this file for a E1-CAS protocol would be:

```
board 1 fcdfile gul1_dsh_r2mf.fcd pcdfile gul1_dsh_r2mf.pcd
variant pdk_us_mf_io.cdp.
```

13. Modify the ANI and DNIS parameters in the pdk_in_r2_io.cdp file as follows:

- CDP_ANI_ENABLED—For enabling set to 1. For disabling, set to 0.
- CDP_NO_OF_DNIS_BEFORE_CAT—0
- CDP_NUM_OF_DNIS_DIGITS—10
- CDP_NUM_OF_ANI_DIGITS—10 (if ANI is enabled)
- CDP_DNIS_MaxDigits—10
- CDP_ANI_MaxDigits—10 (if ANI is enabled)

14. Start the DCM by selecting Start > Program Files > Intel Dialogic System Release > Configuration Manager - DCM.

The first time that you start the DCM, a dialog box appears, prompting you for the computer connection (see Figure 55).

Note: If you have started DCM before, you will not get the above prompt.

15. To connect:

- Select the Local radio button, and then click Connect.

End of procedure

Additional Configuration for Non-ISDN

This section contains information about additional configuration requirements for Dialogic DM/V cards for non-ISDN protocols:

- Additional Configuration for ANI/DNIS for T1/E1 Non-ISDN
- Configuring T1/E1 Non-ISDN to Use Specific Protocol Variants (see page 494)

Additional Configuration for ANI/DNIS for T1/E1 Non-ISDN

This information applies to Global Call 4.0 and later releases that use the Dialogic PDK libraries for call control of T1/E1 protocols.

Dialogic can be configured to separate the ANI and DNIS during call setup for T1/E1 protocol variants, but this configuration is complicated. To avoid the complications, you can configure Dialogic to give GVP all the digits as the DNIS in a single string (including delimiters). GVP software then parses the tones that are given during call setup.

To enable correct parsing, you must set certain parameters in your protocol variant `*.cdp` file so that they match the far end. The `*.cdp` file resides in the `<Dialogic>\cfg\` directory, and its name should contain `pdk`—for example, `pdk_us_mf_io.cdp`.

For example, if your carrier gives ANI/DNIS in the format `*4081234567*650987654321*,` set the parameters in the `*.cpd` file as follows:

- `All BOOLEAN_t CDP_IN_WinkStart:1`
- `All BOOLEAN_t CDP_OUT_WinkStart:1`
- `All BOOLEAN_t CDP_IN_DNIS_Enabled:1`
- `All BOOLEAN_t CDP_OUT_DNIS_Enabled:1`
- `All BOOLEAN_t CDP_IN_DNIS_ST_Needed:0`
- `All BOOLEAN_t CDP_OUT_DNIS_ST_Needed:0`
- `All INTEGER_t CDP_IN_DNIS_MaxDigits:22`
- `All BOOLEAN_t CDP_IN_DNIS_WINK_Needed:0`
- `All BOOLEAN_t CDP_OUT_DNIS_WINK_Needed:0`
- `All BOOLEAN_t CDP_IN_DNIS_KP_Needed:0`
- `All BOOLEAN_t CDP_OUT_DNIS_KP_Needed:0`
- `All BOOLEAN_t CDP_IN_ANI_Enabled:0`
- `All BOOLEAN_t CDP_OUT_ANI_Enabled:1`
- `All BOOLEAN_t CDP_IN_ANI_ST_Needed:0`
- `All BOOLEAN_t CDP_OUT_ANI_ST_Needed:0`
- `All INTEGER_t CDP_IN_ANI_MaxDigits:12`
- `All BOOLEAN_t CDP_IN_ANI_WINK_Needed:0`
- `All BOOLEAN_t CDP_OUT_ANI_WINK_Needed:0`
- `All BOOLEAN_t CDP_IN_ANI_KP_Needed:0`
- `All BOOLEAN_t CDP_OUT_ANI_KP_Needed:0`

Note: `CDP_IN_DNIS_MaxDigits` is the default number of digits that combines the DNIS, ANI, and any delimiter. You might need to change the value, depending on the trunk service provider; otherwise, GVP will not obtain the correct DNIS and ANI number.

For more information, see “Additional Configuration to use DTMF for ANI/DNIS for JCT T1/E1” on page 466 and “Additional Configuration to use MF for ANI/DNIS for JCT T1/E1” on page 467.

Procedure: Configuring T1/E1 Non-ISDN to Use Specific Protocol Variants

Purpose: To configure a DM/V-A or DM/V-B board to use a protocol variant:

Summary

Follow the instructions in this section only if the following conditions are met:

- DM3 boards are being used with T1/E1 non-ISDN protocols such as CAS.
- A protocol variant (for example, `pdk_us_mf_io.cdp`) other than the Dialogic default is being used.

Start of procedure

1. Stop the Dialogic Service if it is running.
2. Open a command prompt and do the following:
   a. Change the directory to `<Dialogic>\bin`.
   b. Execute the following command:
   ```
   PdkManagerRegSetup add
   ```
3. Using Windows Explorer, navigate to `<Dialogic>\cfg`.
4. Check if a file called `pdk.cfg` exists in this directory.
   - If the file does not exist, create an empty file with this name (`pdk.cfg`).
   - If the file does exist, open the file in Notepad and delete the contents.
5. Using Notepad, edit the `pdk.cfg` file to add a line for each DM3 board that is based on T1-RobbedBit or E1-CAS protocols, in the following format:
   ```
   board <b> fcdfile <f> pcdfile <p> variant <v> mlmfile
   universal_pdk_qfc3_xscale.mlm.sym
   ```
   where:
   - `<b>` is the logical board number. To get the logical board number, use the `listboards` utility located in `<dialogic>\bin`.
   - `<f>` is the `.fcd` file assigned to that board in the DCM.
   - `<p>` is the `.pcd` file assigned to that board in the DCM.

- `<v>` is the name of the `.cdp` file for the protocol to be used (for example, `pdk_ar_r2_io.cdp`).

> Note: The variant field is needed only for T1-RobbedBit/E1-CAS based protocols.

The following are sample lines for various non-ISDN protocols:

- For E1-CAS:

  ```
  board 1 fcdfile ml2_dsa_cas.fcd pcdfile ml2_dsa_cas.pcd variant
  pdk_us_mf_io.cdp
  ```

- For T1-RobbedBit:

  ```
  board 1 fcdfile gul1_dsh_cas.fcd pcdfile gul1_dsh_cas.pcd
  variant pdk_ar_r2_io.cdp
  ```

- For R2-MFC:

  ```
  board 1 fcdfile gul1_dsh_r2mf.fcd pcdfile gul1_dsh_r2mf.pcd
  variant pdk_us_mf_io.cdp
  ```

6. If necessary, change the following parameters in the `*.cdp` file to match the far end:

- `CDP_IS_CALLING_LINE_IDENTIFICATION_PERMITTED` (not applicable to T1 Robbed Bit)
- `CDP_OVERLAP_SENDING_ENABLED` (not applicable to T1 Robbed Bit)
- `SYS_FEATURES`—Because of an Intel bug, this parameter must be set to the following:

  ```
  feature_outbound,feature_inbound,feature_DNIS,feature_hold,
  feature_transfer
  ```

> Note: If you need to change the parameters to match the far end, you must perform this step regardless of the version of GlobalCall that is being used.

End of procedure

Next Steps

- For more information, see the *GlobalCall 4.3 Release Notes*.
- For an example of a `.cdp` file for loopstart, see “Sample CDP File for US Loopstart FXS Protocol Variant” on page 497.

Configuring Dialogic for Two B-Channel Transfer

Procedure: Configuring Dialogic for Two B-Channel Transfer

Purpose: To configure all machines that are going to support Two B-Channel Transfer (TBCT) functionality.

Start of procedure

1. Open the registry editor, `regedit`.
2. In the registry, navigate to the node: `HKEY_LOCAL_MACHINE\SOFTWARE\Dialogic\Cheetah\CC\` node.
3. Double-click the `NetCRV Support` key.
4. In the `Value Data` field, enter `1`, and then click `OK`.
5. Close the registry editor.

   Dialogic configuration to support TBCT functionality is now complete.

End of procedure

Troubleshooting the Dialogic Driver

Use the following procedure to troubleshoot when using T1-Robbed Bit:

Procedure: Troubleshooting the Dialogic Driver when T1-Robbed Bit is Used

Purpose:

Start of procedure

1. In the Dialogic installation directory, edit or copy the ...`\Dialogic\CFG\us_mf_io.cdp` configuration file by setting the following parameters:
   a. `$6-inter-digit timeout (s): 1`

b. `$7-maximum number of DDI digits (excluded KP and ST) (inbound): ZZZ`

   `ZZZ` is the number of ANI digits, plus the number DNIS digits, plus all separators. For example, if your carrier gives ANI/DNIS in the format: `*4081234567*8005551111*` then set `ZZZ` to `23`.

   Check with your trunk carrier to see the format in which ANI/DNIS are presented. If you can not determine the appropriate `ZZZ` settings, then try `30`, which is the maximum allowed.

c. `$8-maximum number of ANI digits (excluded KP and ST) (inbound): 0`

d. `$9-number of rings before speech (inbound): 0`

e. `$21-set to 1, if GCEV_ALERTING should be sent after: 0`

f. `$16-collect/send ANI after DDI (1=YES, 0=NO): 1`

g. `$41-return to IDLE after caller disconnection (outbound) (1=YES, 0=N-): 1`

h. `$47·T1 MF protocol option mask: 00`

End of procedure

Next Steps

- If you make any changes to `us_mf_io.cdp` (or any other `*.cdp` file), you only need to restart WatchDog. Refer to Starting/Restarting GVP in Normal mode (Windows), page 198 for details.

Sample CDP File for US Loopstart FXS Protocol Variant

The following is an example of apdk_us_ls_fxs_io.cdp file, which is used for the US loopstart Foreign Exchange Subscriber (FXS) protocol variant. The file illustrates the use of various feature parameters, such as Call Progress Analysis (CPA) behavior after answer for voice.

This example is provided for reference purposes only. Be sure to use the feature parameters that apply to your configuration and environment. Consult the Dialogic Product Manuals for additional information.

pdk_us_ls_fxs_io.cdp

```
/**
%full_filespec: pdk_us_ls_fxs_io.cdp-10:ascii:gc#1 %
*****************************************************
FILE    : PDK_US_LS_FXS_IO.CDP
USES    : PDK_US_LS_FXS_IO.PSI
```

```
COUNTRY : T1 FXS
PROTOCOL: Inbound + Outbound
*******************************************************
This is a CDP file is to be used with the US loop-start FXS
protocol. It provides only the voice mail side execution of the
protocol. The FXO-FXS protocol is asymmetrical, and may only
interface with a line running an FXO (PBX) side of the protocol.
ALL CAS_SIGNAL_TRANS_t  CDP_TRANS =  ABCD, ABCD,
PreInterval,PostInterval,
PreIntervalNominal,PostIntervalNominal
ALL PATTERN_PULSE  CDP_PULSE =  OffCode<ABCD>,
OnCode<ABCD>,
PreInterval,PostInterval,
PreIntervalNominal,PostIntervalNominal,
m_PulseIntervalMin,m_PulseIntervalNominal,
m_PulseIntervalMax
*/
/* FXS protocol supports and requires following features:*/
ALL Charstring_t Sys_features = "Feature_Inbound, Feature_Outbound,
Feature_Transfer,Feature_Hold, Feature_Drop_On_Hold"
DM3 INTEGER_t SYS_LineTypeT1 = 1
/*
This PSL parameter informs the PDK engine that protocol requires
call progress (pre-connect call analysis).
Possible values:
0 = ALWAYS-OFF (disable)
1 = PREFERRED (always use - protocol requires)
2 = PASS-THROUGH (use if requested by application, i.e., control is
passed-through to application)
*/
R4 INTEGER_t PSL_MakeCall_CallProgress = 1
DM3 INTEGER_t PSL_CACallProgressOverride = 1
/*
This PSL parameter informs the PDK engine that protocol requires
media detection (post-connect call analysis).
Possible values:
1 = PREFERRED (always use - protocol requires)
2 = PASS-THROUGH (use if requested by application, i.e., control is
passed-through to application)
*/
R4 INTEGER_t PSL_MakeCall_MediaDetect = 2
DM3 INTEGER_t PSL_CAMediaDetectOverride = 2
/*
Set this value to true(1) to have the FXS transition to Accepted
state immediately upon receiving an accept call command and thus
ignore the number of rings parameter. The current default is false
(0) to be consistent with ICAPI, thereby waiting for the specified
number of rings before transitioning to Accepted state.
*/
ALL BOOLEAN_t CDP_IMMEDIATE_ACCEPTSTATE = 0
```

```
/*
This parameter controls when the protocol will send up
GCEV_ALERTING/GCEV_CONNECTED event to the application. If set to 0,
GCEV_ALERTING is sent, when ring back is detected, and
GCEV_CONNECTED is sent when the call is connected. If set to 1,
GCEV_ALERTING is sent when
•  After dialing is completed if CPA is disabled, or
•  After dialing is initiated if CPA is enabled.
However, if CPA is disabled and CDP_PBXAnswerEnabled is also
disabled, then GCEV_CONNECTED will be sent after dialing instead of
GCEV_ALERTING, for the protocol would not be able to reach the
connected state otherwise.
All BOOLEAN_t CDP_Send_Alerting_Or_Connected_After_Dial = 1
/*
Set this value to true (1) to have the FXS wait for dial tone prior
to dialing.
Note this parameter does NOT apply to supervised transfers
(consultation calls) in which case dial tone is not verified.
*/
ALL BOOLEAN_t CDP_WaitDialToneEnabled = 1
/* Set this value to true (1) to have the FXS connect on positive
media detection, i.e., voice, fax, modem, etc. */
ALL BOOLEAN_t CDP_CONNECT_UPON_MEDIA = 1
/* Set this value to true (1) to have the FXS connects on call
analysis result of no ringback (remote collision). */
ALL BOOLEAN_t CDP_ConnectOnNoRingBack = 1
/* Set this value to true (1) to have the FXS connects on call
analysis result of no dialtone (local collision). */
ALL BOOLEAN_t CDP_ConnectOnNoDialTone = 1
/*
Define the dial tone detection for a dual-tone of 440Hz+480Hz on for
at least 1 sec.
Dial tone detection is only active if the prior parameter is
enabled.
TONE_t format = Freq 1, Freq 1 Dev, Freq 2, Freq 2 Dev, Amp 1, Amp
2, On Time,
On Time Dev, Off Time, Off Time Dev, Mode (1 for Edge Detection, 0
for Cadence Detection), Repeat Count
*/
ALL TONE_t TONE_DIAL = 350,50,440,50,0,0,0,0,0,0,1,1
/* Define the ring tone detection */
ALL TONE_t TONE_RINGBACK = 440,65,480,65,0,0,1000,100,0,0,1,1
/* Define the dial tone timeout (msec). Used only when
CDP_WaitForDialTone is enabled. */
ALL INTEGER_t CDP_DialToneWaitTime = 5000
/*
Define the intentional delay (msec) for going onhook prior to making
a call before gc_WaitCall is ever called.
*/
ALL INTEGER_t CDP_OnhookDuration = 2000
```

```
/*
Define the intentional delay (msec) after the offhook prior to
dialing digits.
This is used primarily in scenarios when CDP_WaitDialToneEnabled is
disabled (zero).
*/
ALL INTEGER_t CDP_PostOffhookDelay = 0
/* Define timeout (msec) to determine whether PBX has hung-up. */
ALL INTEGER_t CDP_MinPBXHangupTime = 6000
/*
Define the intentional delay (msec) after the blind transfer
hookflash and the start of dialing. Note this should not be
necessary assuming the wait for dialtone parameter,
CDP_WaitDialToneEnabled, is enabled.
*/
ALL INTEGER_t CDP_BTPreDialDelay = 1000
/* Define the intentional delay (msec) before hanging up after
dialing on a blind transfer. */
ALL INTEGER_t CDP_BTPostDialDelay = 500
/* This parameter sets the hookswitch state upon opening the device:
0:= ONHOOK, 1:= OFF_HOOK */
ALL BOOLEAN_t CDP_ProtocolStartsOffhook = 1
/* This parameter sets the hookswitch state on protocol completion:
0:= ONHOOK, 1:= OFF_HOOK */
ALL BOOLEAN_t CDP_ProtocolStopsOffhook = 0
/* This parameter indicates an off-hook (outbound seize) from the
voicemail side (local) on the line. */
ALL CAS_SIGNAL_TRANS_t CAS_OFFHOOK = xxxx,11xx,50,50,0,80
/* This parameter indicates an on-hook (idle) from the voicemail
side (local) on the line. */
ALL CAS_SIGNAL_TRANS_t CAS_ONHOOK = xxxx,01xx,50,50,0,80
/* This parameter identifies the CAS pattern that indicates the PBX
applied a ring signal (inbound seize) on the line. */
ALL CAS_SIGNAL_TRANS_t CAS_RING_APPLIED = 01xx,00xx,50,50,80,80
/* This parameter identifies the CAS pattern that indicates the PBX
applied a ring signal (inbound seize) on the line. */
ALL CAS_SIGNAL_TRANS_t CAS_RING_STOPPED = 00xx,01xx,50,50,80,80
/* This parameter identifies the CAS pattern for a hookflash on the
line. */
ALL CAS_SIGNAL_PULSE_t CAS_HOOKFLASH =
11xx,01xx,50,50,80,80,450,500,550
/*
This parameter permits the remote PBX to initiate transitioning to
the connected state with an answer signal. However, any PBX answer
signal is ignored if call progress is mandated in the make call.
*/
ALL BOOLEAN_t CDP_PBXAnswerEnabled = 1
/* This pattern indicates that the remote PBX has answered. */
ALL CAS_SIGNAL_TRANS_t CAS_PBX_ANSWER = 11xx,01xx,50,50,80,80
```

```
/* Enabling this parameter permits the remote PBX to initiate
disconnects. */
ALL BOOLEAN_t CDP_PBXDiscEnabled = 1
/* This pattern indicates that the remote PBX has disconnected. */
ALL CAS_SIGNAL_TRANS_t CAS_PBX_DISC = 0xxx,1xxx,50,600,0,80
/*
This parameter permits the protocol to bypass signaling a hookflash
when dropping a consultation call. It should be enabled only in the
case when all consultation calls are assumed to initiate the
disconnect. When enabled, no hookflash CAS signaling is sent and
only state changes are delivered to the application. (Normally this
parameter should be disabled and set to zero.)
*/
ALL BOOLEAN_t CDP_BypassHookflashOnConsultationDrop = 0
/*
This parameter permits the protocol to bypass signaling a hookflash
when initiating either a supervised or unsupervised transfer via
gc_SetupTransfer( ) or gc_BlindTransfer( ) respectively. It is
currently a temporary customized feature and should be normally
disabled and set to zero. When enabled, no hookflash CAS signaling
is issued and only applicable state changes are delivered to the
application.
*/
ALL BOOLEAN_t CDP_BypassHookflashOnTransfer = 0
/* These three tone templates define the DTMF tones used for support
of disconnect supervision:  */
ALL TONE_t TONE_DISCONNECTDIAL = 350,50,440,50,0,0,1000,-
1000,0,0,1,0
ALL TONE_t TONE_DISCONNECTREORDER =
480,50,620,50,0,0,250,50,250,50,1,4
ALL TONE_t TONE_DISCONNECTBUSY = 480,50,620,50,0,0,500,50,500,50,1,4
/*
Following tone templates define the default Call Progress tones
used:
Note: Do not uncomment unless non-US call progress tones are used by
switch (FXO).
R4 TONE_t PSL_TONE_CP_DIAL_LCL = 350,50,440,50,0,0,0,0,0,0,1,0
R4 TONE_t PSL_TONE_CP_RNGBK1 =
440,65,480,65,0,0,1000,100,3000,300,1,0
R4 TONE_t PSL_TONE_CP_BUSY1 = 480,50,620,60,0,0,500,50,500,50,1,4
*/
/*
***********************************************
DM3 Parameters
***********************************************
*/
DM3 INTEGER_t PSL_VariantId = 9
/* PSL_VendorId: (REQUIRED) Identifies the vendor of the protocol,
this Id is assigned by Dialogic to the vendor */
DM3 INTEGER_t PSL_VendorId = 0x10001
```

```
/* PSL_ProtocolId: (REQUIRED) Vendor assigned Id, which identifies a
vendors protocol. */
DM3 INTEGER_t PSL_ProtocolId = 0x1001d
/* PSL_Version: (REQUIRED) Identifies version of the protocol.
Maintained by vendor but must be in the standard Dialogic versioning
format.
The combination of VendorId, ProtocolId, and Version uniquely
identifies a protocol.
The following describes the format.
*/
/*                             ---Type: 0=Prod, 1=Beta, 2=Alpha,
3=Exp
 *                            | -----Major Number
 *                            ||  -----Minor Number
 *                            || |  -----Beta Number
 *                            || | |  -----Alpha Number
 *                            || | | |
 *                            vv v v v */
DM3 INTEGER_t PSL_Version = 0x00300000
/*
PSL_CompatibilityMask: A bit mask of the Version value it determines
compatibility between protocol and cdp files. The value used when
building the protocol will determine which cdp variant are
considered to be compatible. The value supplied by the variant will
determine which protocol build is acceptable. The combination of the
stored and supplied masks will determine if a match is found */
/*                                       ---Type: 0=Prod, 1=Beta,
2=Alpha, 3=Exp
 *                                      | -----Major Number
 *                                      ||  -----Minor Number
 *                                      || |  -----Beta Number
 *                                      || | |  -----Alpha Number
 *                                      || | | |
 *                                      vv v v v */
DM3 INTEGER_t PSL_CompatibilityMask = 0xfffff000
/* sys_ProtocolName (REQUIRED) Vendor assigned Id that identifies
auxiliary files. */
DM3 CHARSTRING_t SYS_ProtocolName = pdk_us_ls_fxs_io
/* sys_VariantName (OPTIONAL) Differentiates between variants using
the same base protocol. */
DM3 CHARSTRING_t SYS_VariantName = t1_fx_io
/* sys_i960HotFile (REQUIRED) Protocol object file to use with this
CDP file. */
DM3 CHARSTRING_t sys_i960HotFile = pdk_us_ls_fxs_io.hot
/*
*******************************************************************
*
```

```
              END OF FILE
********************************************************************
*
*/
```

Appendix

B Manual Installation on Windows

This appendix describes how to manually install each Genesys Voice Platform (GVP) component on the Windows operating system. It contains the following sections:

- Before You Begin, page 505
- Installing GVP Components Manually, page 505

Before You Begin

Before you perform any of the installation procedures in this chapter, review the information in Chapter 4, “Preparing Your Windows Environment,” on page 81, and ensure that you have satisfied all the prerequisites to prepare your environment. Genesys also recommends that you review the information in “Host Setup” on page 67 and “Windows Deployment Task Summaries” on page 75 before you install any software.

Antivirus software may interfere with the GVP installation. Make sure that the server is not running antivirus software, or any other third-party software, during installation.

After you have installed and configured the components, start or restart WatchDog on the GVP servers. For more information, see “Starting and Stopping GVP on Windows” on page 198.

Installing GVP Components Manually

This section describes the steps to install GVP components, if you are not using the GVP Deployment Tool (GDT):

- Manually installing Common (Windows)

- Manually installing EMPS (Windows), page 508
- Manually installing Dispenser (Windows), page 512
- Manually installing EMS Runtime components (Windows), page 513
- Manually installing Cisco Queue Adapter (Windows), page 513
- Manually installing EMS Reporting components (Windows), page 514
- Manually installing OBN Manager (Windows), page 516
- Manually installing IPCS (Windows), page 517
- Manually installing VCS (Windows), page 517
- Manually installing TTS (Windows), page 518
- Manually installing IP Call Manager (Windows), page 519
- Manually installing Portal (Windows), page 520
- Manually installing the ASR Log Manager System (Windows), page 521
- Manually installing MIBs (Windows), page 521

See also Chapter 9 on page 179 for information about installing the optional Bulk Provisioning Tool.

Procedure:
Manually installing Common (Windows)

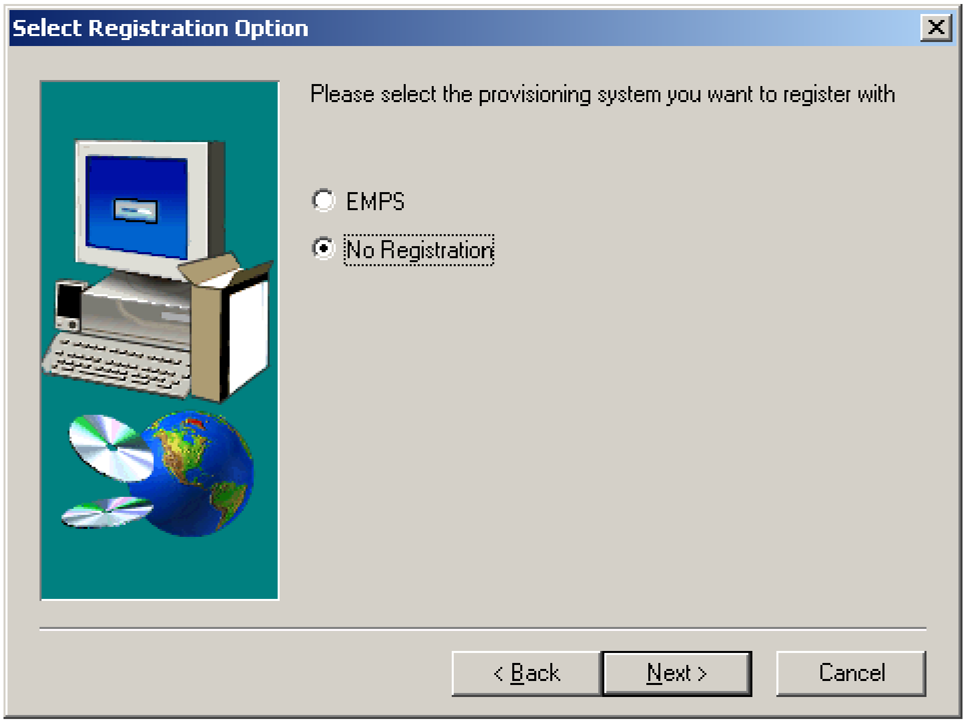
You must install Common on each server that will host GVP components.

Start of procedure

1. Insert the Genesys Voice Platform Base CD into the computer, or browse to the folder where you have copied the Base components.
2. Go to the `solution_specific > windows > Common` folder, and double-click `CoreSetupRelease.exe`.
3. On the `Welcome` screen, click `Next` to open the `Software License Agreement` screen.
4. On the `Software License Agreement` screen, click `Yes` to open the `Choose Destination Location` screen.
5. On the `Choose Destination Location` screen, accept `C:\GVP\CN` as the default location, or click `Browse` to choose another destination, and then click `Next` to start the installation.

Note: EMPS installs in the same directory as Common. If this is an EMPS upgrade or re-installation and the Open LDAP data from the previous EMPS installation is to be preserved, Common should be installed in the same directory as its previous installation. The new EMPS will be unable to access earlier Open LDAP data unless it installs in the same directory as the previous EMPS.

6. After the Core components have been installed, the `Select Registration Option` screen appears (see Figure 61).



Select Registration Option

Please select the provisioning system you want to register with

○ EMPS

● No Registration

Figure 61: Select Registration Option Screen

7. Select the provisioning system with which you want to register, and then click `Next`.
   - If you are installing Common for the EMPS server, select `No Registration` (because there is no EMPS with which to register yet). Continue at Step 9.
   - For all other servers, select `EMPS`.

     The `Directory Server Information` screen appears. Continue at Step 8.

Register with EMPS

8. On the `Directory Server Information` screen, verify or enter the following information to register with EMPS:
   - EMPS Fully Qualified Domain Name or IP Address—for example, `servername.yourcompany.com`
   - EMPS User Name—for example, `admin`
   - EMPS Password

   Click `Next`. The `Setup Complete` screen appears.

9. On the `Setup Complete` screen, click `Finish` to complete the GVP Core Components setup.

Note: If you install the Core Components in the incorrect location for your setup, uninstall them before you reinstall them to the correct location.

End of procedure

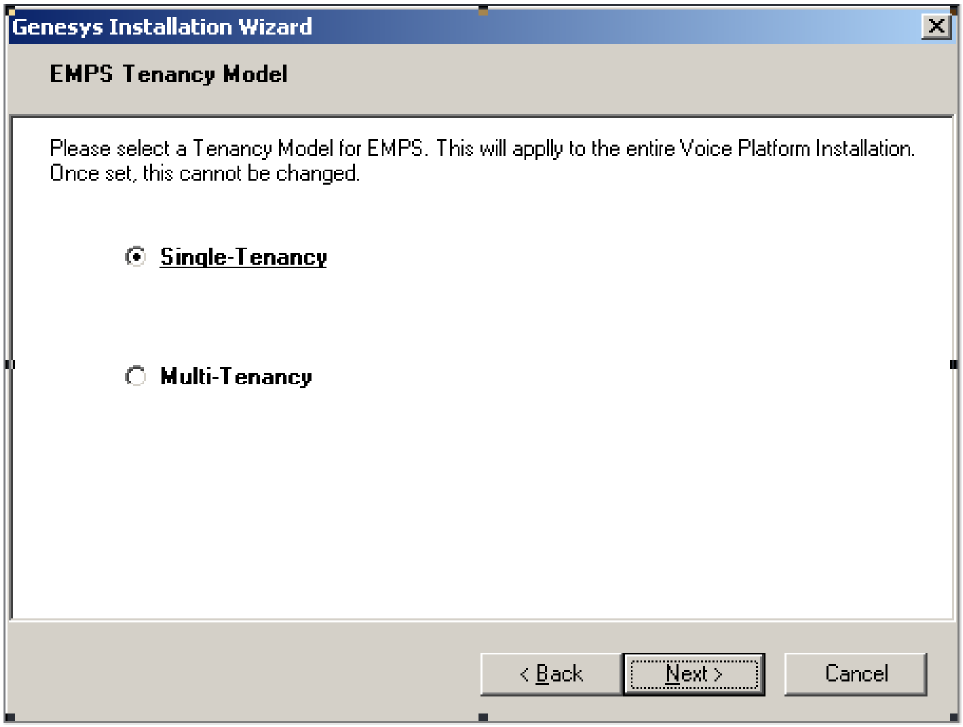
Procedure: Manually installing EMPS (Windows)

Prerequisites

- Java Runtime Environment (JRE) has been installed on each machine on which the EMPS user interface (SPM) will be accessed with a browser. JRE is required to run Browser28, which is a free utility to work with LDAP V3compliant directory servers. If Java runtime has not yet been installed on the EMPS server, download JRE from `www.java.com`, and follow the JRE installation instructions that are available on `java.sun.com`.

Start of procedure

1. Install Common. For more information, see Manually installing Common (Windows), page 506.
2. Insert the Genesys Voice Platform Base CD into the computer, or browse to the folder where you have copied the Base software.
3. From the `solution_specific\windows\EMPS` folder, double-click `setup.exe`. The InstallShield starts.
4. On the `Welcome` screen, click `Next` to open the `EMPS Tenancy Model` screen (see Figure 62).



EMPS Tenancy Model

Please select a Tenancy Model for EMPS. This will applly to the entire Voice Platform Installation. Once set, this cannot be changed.

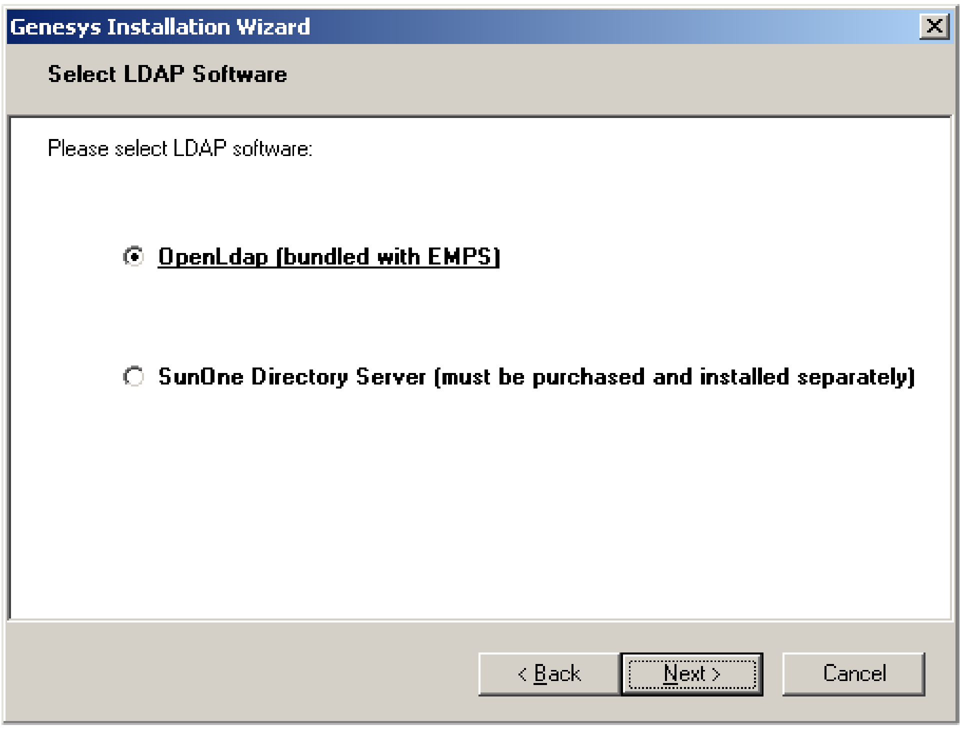
● Single-Tenancy

○ Multi-Tenancy

Figure 62: EMPS Tenancy Model Screen

5. Select a Tenancy model, and then click `Next`.

   The `Select LDAP Software` screen appears (see Figure 63)



Select LDAP Software

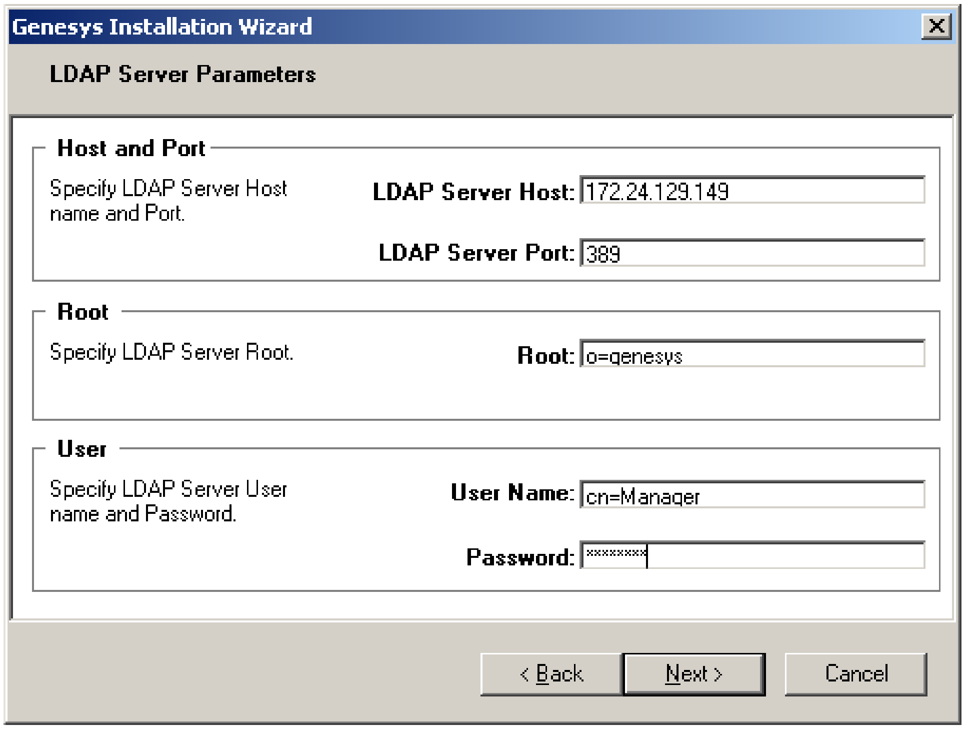
Please select LDAP software:

● OpenLdap (bundled with EMPS)

○ SunOne Directory Server (must be purchased and installed separately)

Figure 63: Select LDAP Software Screen

6. Select the LDAP software, and then click `Next` to open the `LDAP Server Parameters` screen (see Figure 64).



Genesys Installation Wizard

LDAP Server Parameters

Host and Port

Specify LDAP Server Host name and Port.

LDAP Server Host: 172.24.129.149

LDAP Server Port: 389

Root

Specify LDAP Server Root.

Root: o=genesys

User

Specify LDAP Server User name and Password.

User Name: cn=Manager

Password: ********

Figure 64: LDAP Server Parameters Screen

7. Enter the LDAP Settings as described in Table 81.

Table 81: LDAP Server parameters

Parameters	Description
LDAP Server Host	Specifies the IP address of the machine hosting the Directory Server.
LDAP Server Port	Specifies the listening port of the Directory Server. Port `389` must be used.
Root	Specifies the LDAP Root or BaseDN. The valid value is `o=genesys`.
User Name	Specifies the name used to login to the Directory Server. For SunOne, the valid value is `cn= Directory Manager`. For OpenLDAP, the valid value is `cn=Manager`.
Password	Specifies the password used to login to the Directory Server. For SunOne, use the password you created when setting up your SunOne Directory Server. For OpenLDAP, enter `admin123`. **Note**: The password is case sensitive.

Click `Next` to open the `Ready to Install` screen.

8. At the `Ready to Install` screen, click `Install`.
9. At the `Installation Complete` screen, click `Finish` to complete the EMPS installation.

End of procedure

Next Steps

- Add the EMPS URL (`http://<EMPS-hostname>:9810`) as a Trusted Site in Internet Explorer, on the `Tools > Internet Options > Security` tab.
- Install Dispenser (see Manually installing Dispenser (Windows)) and Portal (see Manually installing Portal (Windows), page 520).
- If you included EMS Reporting components or OBN Manager in your deployment, create the EMPS database. For more information, see “Creating the Microsoft SQL Server Databases” on page 181.

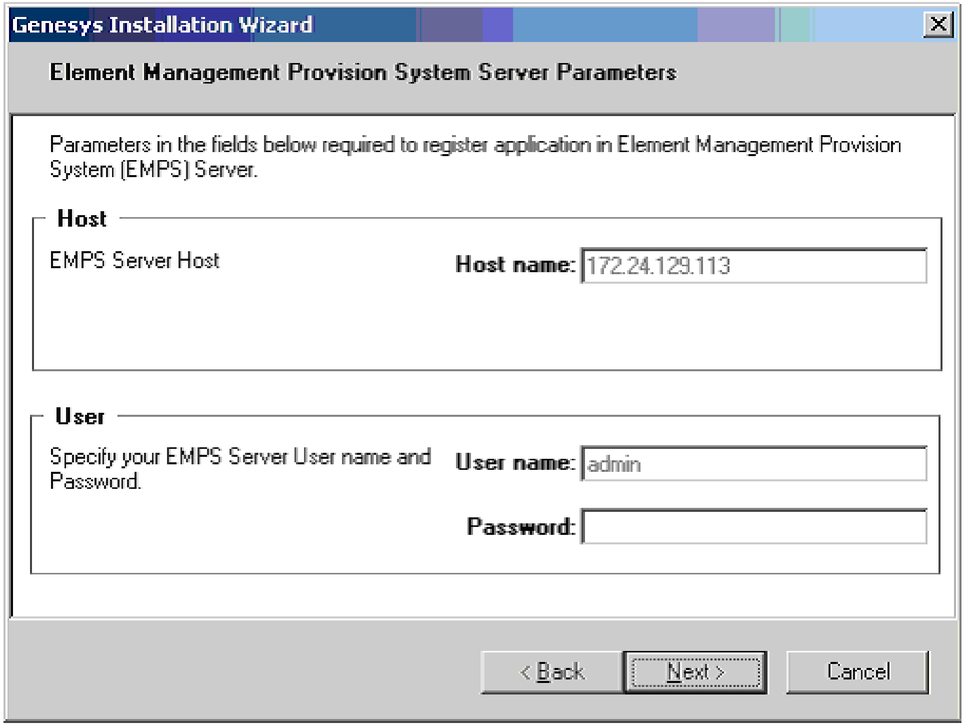
- Verify or modify EMPS server configuration in the EMPS. For more information, see Chapter 17 on page 289.

Procedure: Manually installing Dispenser (Windows)

Start of procedure

1. Go to the solution_specific > windows > Dispenser folder, and double-click setup.exe.
2. On the Welcome screen, click Next.

   The Element Management Provision System Server Parameters screen appears (see Figure 65).



Genesys Installation Wizard

Element Management Provision System Server Parameters

Parameters in the fields below required to register application in Element Management Provision System (EMPS) Server.

Host

EMPS Server Host

Host name: 172.24.129.113

User

Specify your EMPS Server User name and Password.

User name: admin

Password:

Figure 65: Element Management Provision System Server Parameters

3. Enter password in the Password textbox.
4. Click Next to install the Dispenser in the same folder as the Common components.

End of procedure

Procedure: Manually installing EMS Runtime components (Windows)

The optional EMS Runtime components are:

- Policy Manager
- Bandwidth Manager
- IVR Server Client

Start of procedure

1. Install Common. For more information, see Manually installing Common (Windows), page 506.
2. Insert the Genesys Voice Platform Base CD into the computer, or browse to the folder where you have copied the Base components.
3. Go to the `solution_specific > windows > <component>` directory where the installer for the component you want to install is located.

   For example, to install Bandwidth Manager, browse to the `<CD Image>\solution_specific\windows\BWM` directory.
4. Double-click `Setup.exe`.
5. Follow the on-screen prompts to install the EMS Runtime component.
6. At the `Setup Complete` prompt for each component, click `Finish`.
7. Repeat the above steps for each EMS Runtime component that you want to install.

End of procedure

Next Steps

- Verify or modify server configurations in the EMPS. For more information, see Chapter 18 on page 301.
- If your deployment uses IVR Servers, create and configure the IVR Servers (see “Configuring IVR Server” on page 301).

Procedure: Manually installing Cisco Queue Adapter (Windows)

The Cisco Queue Adapter (CQA) is an optional component.

Start of procedure

1. If it is not already installed on the server, install Common. For more information, see Manually installing Common (Windows), page 506.
2. Insert the Genesys Voice Platform Cisco Queue Adapter CD into the computer, or browse to the `solution_specific\windows\CiscoQueueAdapter` folder where you have copied the Cisco Queue adapter software.
3. Double-click `Setup.exe`.
4. Follow the on-screen prompts to install the Cisco Queue Adapter.
5. On the `Directory Server Information` screen, enter the following information to register with the EMPS/LDAP Server:
   - EMPS Fully Qualified Domain Name or IP Address—for example, `servername.yourcompany.com`
   - EMPS User Name—for example, `admin`
   - EMPS Password
6. At the `Setup Complete` prompt, click `Finish` to complete the Cisco Queue Adapter setup.

End of procedure

Procedure: Manually installing EMS Reporting components (Windows)

The optional EMS Reporting components are:

- EventC
- Network Monitor
- Call Status Monitor
- Login Server
- Reporter

Repeat this procedure for each EMS Reporting component that you want to install.

Prerequisites

- The database server and clients have been prepared. The scripts to create the database schemas are unpacked during the installation, and you create the actual database schemas after the InstallShield wizard has completed. For more information, see “Preparing Database Connectivity for Windows” on page 93.

Start of procedure

1. If it is not already installed on the server, install Common. For more information, see Manually installing Common (Windows), page 506.
2. Insert the Genesys Voice Platform Reporting and Monitoring CD into the computer, or browse to the folder where you have copied the Reporting and Monitoring software.
3. For each component, navigate to the `solution_specific\windows\<componentname>` folder and double-click `setup.exe`.

   The Genesys Installation Wizard `Welcome` screen appears.
4. Click `Next`.

   The `Element Management Provision System Server Parameters` screen appears.
5. Enter the EMPS `Password`, and then click `Next`.

   The `Ready to Install` screen appears.
6. Click `Install` to proceed with the installation.

   The `Installation Complete` screen appears.
7. Click `Finish`.

   The `After Installation` screen appears.
8. Click `Next`.

   The `Finish Admin Install` screen appears.
9. Once the installation has completed, click `Finish`.

End of procedure

Next Steps

- Create the databases, set the required file access permissions, and perform other activities to enable EventC reporting, Unified Login, and Network Monitor. For more information, see Chapter 10 on page 181.
- Configure the EMPS Reporting components in the EMPS. For more information, see Chapter 19 on page 309.

Procedure:
Manually installing OBN Manager (Windows)

Prerequisites

- The database server and client have been prepared. The scripts to create the database schema are unpacked during the installation, and you create the actual database schema after the InstallShield wizard has completed. For more information, see "Preparing Database Connectivity for Windows" on page 93.

Start of procedure

1. If it is not already installed on the server, install Common. For more information, see Manually installing Common (Windows), page 506.
2. Insert the Genesys Voice Platform Base CD into the computer, or browse to the folder where you have copied the Base software.
3. From the `solution_specific\windows\OBNManager` folder, double-click `Setup.exe`.
4. Follow the on screen prompts to install the OBN Manager.
5. On the `Directory Server Information` screen, enter the following information to register with the SunOne Directory Server:
   - EMPS Fully Qualified Domain Name or IP Address—for example, `servername.yourcompany.com`
   - EMPS User Name—for example, `admin`
   - EMPS Password
6. Click `Next`.

   The `Setup Complete` prompt appears.
7. Click `Finish` to complete the OBN Manager setup.

End of procedure

Next Steps

- Create the database schema. For more information, see "Creating the Microsoft SQL Server Databases" on page 181.
- Configure the component in the EMPS. For more information, see Chapter 19 on page 309.

Procedure:
Manually installing IPCS (Windows)

Start of procedure

1. Install Common. For more information, see Manually installing Common (Windows), page 506.
2. Insert the Genesys Voice Platform Base CD into the computer, or browse to the folder where you have copied the Base software.
3. From the `solution_specific\windows\IPCS` folder, double-click `IPCSSetupRelease.exe.`
4. On the `Directory Server Information` screen, verify or enter the following information to register with EMPS:
   - EMPS Fully Qualified Domain Name or IP Address—for example, `servername.yourcompany.com`
   - EMPS User Name—for example, `admin`
   - EMPS Password
5. At the `Setup Complete` prompt, click `Finish` to complete the IPCS setup.

Note: TTS is automatically installed with IPCS.

End of procedure

Next Steps

- Configure the IPCS in the EMPS. For more information, see Chapter 20 on page 341.

  Note: If your deployment will use Dialogic HMP or Convedia, ensure that you configure the Media Controller parameters for these enhanced media services.

Procedure:
Manually installing VCS (Windows)

Prerequisites

- Dialogic telephony boards have been installed and configured on the Voice Communication Server (VCS) host. For more information, see “Installing Dialogic Software” on page 173.

Start of procedure

1. Install Common. For more information, see Manually installing Common (Windows), page 506.
2. Insert the Genesys Voice Platform Base CD into the computer, or browse to the folder where you have copied the Base software.
3. From the `solution_specific\windows\VCS` folder, double-click `VCSSetupRelease.exe`.
4. Follow the on-screen prompts to install VCS.
5. On the `Directory Server Information` screen, verify or enter the following information to register with EMPS:
   - EMPS Fully Qualified Domain Name or IP Address—for example, `servername.yourcompany.com`
   - EMPS User Name—for example, `admin`
   - EMPS Password
6. At the `Setup Complete` prompt, click `Finish` to complete the VCS setup.

End of procedure

Next Steps

- If your deployment includes Media Resource Control Protocol (MRCP) Text-to-Speech (TTS), install TTS (see Manually installing TTS (Windows)).

Procedure: Manually installing TTS (Windows)

Install this component on the VCS host only if you are using MRCP TTS.

Start of procedure

1. Insert the Genesys Voice Platform Base CD into the computer, or browse to the folder where you have copied the Base software.
2. From the `solution_specific\windows\TTS` folder, double-click `TTSSetupRelease.exe`.
3. Follow the on-screen prompts to install the TTS server.
4. On the `Select Components` screen, select MRCP or the desired TTS vendor, and then click `Next`.
5. On the `Directory Server Information` screen, verify or enter the following information to register with EMPS:
   - EMPS Fully Qualified Domain Name or IP Address—for example, `servername.yourcompany.com`

- EMPS User Name—for example, admin
- EMPS Password

6. At the Setup Complete prompt, click Finish to complete the TTS server setup.

End of procedure

Procedure: Manually installing IP Call Manager (Windows)

IP Call Manager (IPCM) consists of one of the following:

- Resource Manager (RM) and Session Initiation Protocol (SIP) Session Manager (SSM)
- RM and H.323 Session Manager (HSM)

Note: If you plan to use both SIP and H.323 in your setup, you must install these components on separate hosts. SSM and HSM do not share IPCS and Media Gateway resources.

Start of procedure

1. If it is not already installed on the server, install Common. For more information, see Manually installing Common (Windows), page 506.
2. Install Resource Manager:
   a. Insert the software CD into the computer, or browse to the folder where you have copied the software.
      - If you are using RM with SSM, use software from the Genesys Voice Platform SIP Call Manager CD.
      - If you are using RM with HSM, use software from the Genesys Voice Platform H.323 Call Manager CD.

   b. From the solution_specific\windows\ResourceManager folder, double-click setup.exe.

      The Welcome dialog box appears.

   c. Click Next.

      The Element Management Provisioning System Server Parameters dialog box appears.

   d. Enter the password, and then click Next.

      The Ready to Install dialog box appears.

   e. Click Install.

      The Installation Complete dialog box appears.

   f. Click Finish to complete the installation.

3. Install the session manager:
   a. Insert the software CD into the computer, or browse to the folder where you have copied the software.
      - For SSM, use software from the Genesys Voice Platform SIP Call Manager CD.
      - For HSM, use software from the Genesys Voice Platform H.323 Call Manager CD.

   b. From the `solution_specific\windows\<SessionManager>` folder, double-click `setup.exe`.

      The `Welcome` dialog box appears.

   c. Click `Next`.

      The `Element Management Provisioning System Server Parameters` dialog box appears.

   d. Enter the password, and then click `Next`.

      The `Ready to Install` dialog box appears.

   e. Click `Install`.

      The `Installation Complete` dialog box appears.

   f. Click `Finish` to complete the installation.

End of procedure

Next Steps

- Configure the IPCM server in EMPS. For more information, see Chapter 23 on page 403.

Procedure: Manually installing Portal (Windows)

Install GVP Portal on the EMPS host only. For more information about GVP Portal, see “Portal” on page 51.

Start of procedure

1. On the Windows machine that hosts the EMPS, navigate to the `solution_specific/windows/Portal` directory containing the GVP installation software.
2. Double-click `setup.exe`.
3. After the installation completes, the portal software will be installed under `<CN_ROOT>/web/GVPPortal`.

4. Use the following URL to access GVP Portal:
   `http://<FQDN of EMPS machine>:9810/gvpportal`

End of procedure

Procedure: Manually installing the ASR Log Manager System (Windows)

Purpose: To install the ASR Log Manager, ASR Log Server, and ASR Log Agent components of the ASR Log Manager system.

Repeat this procedure to install each component of the ASR Log Manager system in your deployment.

For information about how to distribute the components on the GVP servers, see "Host Setup for the ASR Log Manager System" on page 424.

Start of procedure

1. For the ASR Log Manager and ASR Log Server components, if Common has not yet been installed on the host, install Common. For more information, see Manually installing Common (Windows), page 506.
2. Insert the Genesys Voice Platform ASR Log Manager CD into the computer, or browse to the folder where you have copied the ASR Log Manager software.
3. From the `solution_specific\windows\<ASR Log Manager system component>` folder, double-click `Setup.exe`.
4. Follow the on-screen prompt to install the component.

End of procedure

Next Steps

- For additional steps that you must perform to set up the ASR Log Manager system, see "Enabling the ASR Log Manager System" on page 425.

Procedure: Manually installing MIBs (Windows)

Purpose: To extract the Windows MIBs and copy them to the Network Management System (NMS).

The MIBs component contains the `.mib` files that enable a Simple Network Management Protocol (SNMP) Manager (for example, HP OpenView) to provide a user-friendly display of the SNMP traps generated by GVP.

The MIBs component is not meant to be installed on any of the GVP hosts.

Start of procedure

1. From `<Base Software Installation CD>\solution_specific\windows\MIBS`, run `setup.exe`.
2. Accept the default installation directory.
3. Copy the contents of the installation directory to the directory on the SNMP Manager where all the other `.mib` files are stored.

> Note: There is no loading sequence for the MIB files if you are copying **all** of the MIB files into the third-party SNMP Manager.
>
> If you are loading only one or just a few of the GVP MIB files, you must first load the `CallNet.mib` and `CallNetTrap.mib` files.

4. After copying the MIB files to your SNMP Manager, some Managers may require additional steps, such as compiling the MIBs. Genesys recommends that you check the instructions for your SNMP Manager to see if any additional steps are required.

End of procedure

Appendix

C Behind-the-Switch

This appendix provides information about configuring Genesys Voice Platform (GVP) for Behind-the-Switch operation. It contains the following sections:

Configuring EMPS for Behind-the-Switch

This section describes how to configure Genesys Voice Platform (GVP) using the Element Management Provisioning System (EMPS) for operating behind-the-switch.

PopGateway Section

1. Log into the EMPS.
2. Click `Servers` on the top menu.
3. If IPCS was installed, expand the nodes `IPCS > <IPCS host>`, and then click `Popgateway1`.

   If VCS was installed, expand the nodes `VCS > <VCS host>`, and then click `Popgateway1`.
4. Click `Edit Node`.
5. Select the `IVR` tab.
6. Set the `Primary DID Mapper` attribute with the value `http://localhost:9810/did_url_mappings/GenericDID.xml`.
7. Click `Submit`.

CFA Section

1. Log into the EMPS.
2. Click `Servers` on the top menu.
3. If IPCS was installed, select the nodes `IPCS > <IPCS host>`, and then click `CFA`.

   If VCS was installed, select the node `VCS > <VCS host>`, and then click `CFA`.
4. Click `Edit Node`.
5. Select the `General` tab.
6. Set the attributes and values listed in Table 82, and then click `Submit`.

Table 82: CFA Parameters

Parameter	Description
Use CTI Client For ANI & DNIS	1
Transfer Type	`Transfer Through CTI`
(Optional) Default DNIS	`<default did>` **Note:** This direct inward dial (DID) should be available in the .ini dispenser location

I-Server Client Url	**Windows:**
	`http://<IVR Server Client Host name or IP address>:9810/WebNotify.asp?NotifyProcess=<reseller>_<customer>_GQA`
	Solaris:
	`http://<IVR Server Client Host name or IP address>:9810/WebNotify.php?NotifyProcess=<reseller>_<customer>_GQA`

GVP Success URL	`http://<ini Dispenser Machine>/$did$.xml`
Application URL in case of failures	`http://(Ini Dispenser Machine)/$did$.xml`

IVR Server Client Section

1. Log into the EMPS.
2. On the left pane, right-click the Reseller you created, and select `Add new Customer`.

3. On the right pane, under the Main tab, specify values for the following parameters:
   - Customer ID
   - Customer Name
   - Customer Display Name
   - Active

   Click Save.
4. On the left pane, right-click the Customer that will use the IVR Server Client, and select Provision.
5. On the right-pane, click the GenesysCTI tab.
6. Set the attributes and values listed in Table 83.

Table 83: IVR Server Client Settings

Parameter	Description
IVR Svr Client Active	Select to enable the IVR Svr Client.
Primary IVR Svr Client Machine	Specifies the IVR Server Client Machine.
Primary IVR Svr Client URL	**Note:** This attribute will be populated once the value is set for Primary IVR Svr Client Machine. The IVR Server Client machine and the process to contact should be the same as configured in CFA > I-Server Client URL.
Customer IServers	Select the appropriate customer IServer.
IVR Server Mode	Behind the Switch

7. Click Save.

Note: If you are prompted to enter information contained under the Policy tab, refer to the *Genesys Voice Platform 7.6 Reference Manual* for information about the Policy Manager parameters.

If you are using OBN, perform the following steps:

8. From the navigation tree on the left pane, expand Servers > GQA > <server host name>, and then click on the <customer process name> node.
9. Click Edit Node.
10. Click Add New Attribute.

11. Enter the following values in the text boxes that appear:
    - Parameter Name: `PrependHostIPToCalledNum`
    - Parameter Value: `0`

    This parameter removes an IP address from the `New Call` request that the IVR Server Client sends to the IVR Server.
12. Click Save.

Genesys Framework Application Selection

1. Perform all of the steps in the section "Configuring EMPS for Behind-the-Switch" on page 523.
2. Log into the EMPS.
3. Expand `Resellers` from the navigation tree on the left pane.
4. Select the required reseller, and then select the required customer.
5. Right-click your customer and select `Provision`.
6. Select `Provision IVR Server Client`.
7. Select the `GenesysCTI` tab.
8. Verify that the `IVR Server Mode` is set to `Behind the Switch`.
9. Select the `Fetch Script ID from URS` check box.
10. By default, the `Script ID Key Name` is set to `scriptname`. Change this value to the appropriate user data key name, which is configured in Genesys Framework. This user data key value will be retrieved by GVP and will be used as DNIS to fetch the voice application.
11. By default, the `Script ID Fetch Timeout` is set to `5000` msec. This timeout is used during the fetching of the Script ID key value. The range is `500-5000` msec. Set this value to the desired timeout.

Appendix

D Sample SNMP Configuration and Log Files (Solaris)

This appendix provides examples of Genesys Voice Platform (GVP) Simple Network Management Protocol (SNMP) configuration and log files for Solaris. It contains the following sections:

Sample snmpd.conf File

The following is an example of the `snmpd.conf` file, which is located in the `/opt/genesys/gvp/netsnmp/share/snmp/` directory.

```
###############################################################################
#
# snmpd.conf: This is a "minimal" configuration file for the 'snmpd' daemon for
#             GVP.
# .NOTE:-
# 1. '$node-manager' should be replaced with the IP address of your respective
#    SNMP Node Manager, e.g. HP OpenView.  A possible value is 10.10.0.2.
# 2. '$sys-contact' may be replaced by the contact information
#    of the snmp administrator, e.g. hostmaster@yourdomain.com.
# 3. '$sys-location' may be replaced with the physical location information of
#    the machine, e.g. Rack 32.
###############################################################################
#
# When the snmpd agent starts up, it reads this file.
# All lines beginning with a '#' are comments and are intended for user
# to read.  All other lines are configuration commands for the agent.
# System contact information
#syslocation $sys-location
#syscontact $sys-contact
syslocation US,CA
syscontact hostmaster@genesyslab.com
rocommunity public


# Access Control
#---------------
#1. Map the community name to a security name.
#   You can have more than one com2sec line and
#   may use the same sec.name for all such lines.
#   Add one line for each Network Manager that
#   may request MIB data.
#-----------------------------------------
#       sec.name   source        community
#-----------------------------------------
#com2sec mynetwork  $node-manager   public
com2sec mynetwork  10.10.10.156   public
#-----------------------------------------
#
#
#
#
#2. Second, map the security names into group names:
#------------------------------------
#             sec.model  sec.name
#------------------------------------
group MyROGroup v1         mynetwork
#------------------------------------
#
#
# 3. Create a view to let the groups have rights
#-----------------------------------------------------------
#           incl/excl subtree                          mask
#-----------------------------------------------------------
view all    included  .1                               80
#-----------------------------------------------------------
#
#
#
#
# 4. Grant the 2 groups access to the 1 view with different
# write permissions.
#----------------------------------------------------------------------
#                context sec.model sec.level match  read   write  notif
#----------------------------------------------------------------------
access MyROGroup ""      any       noauth    exact  all    none   none
# -----------------------------------------------------------------------------
```

```
##############################################################################
# Subagent control
smuxpeer  .1.3.6.1.4.1.3814 test


##############################################################################
# Trap Host information
authtrapenable 1
trapcommunity public

# You can have more than one trapsink line.
# Add one line for each device to which traps
# should be sent.
#-----------------------------------------
#         target        community
#-----------------------------------------
#trapsink $node-manager public
trapsink 10.10.10.156 public
```

Sample SNMP Log File

The following is an example of the `snmpd.log` file, which is located in the `/var/log/` directory.

```
$ cat /var/log/snmpd.log
snmpd: send_trap: Timeout
NET-SNMP version 5.1.1
[smux_accept] accepted fd 20 from 127.0.0.1:59813
accepted smux peer: oid SNMPv2-SMI::enterprises.3814, password test, descr syslogd
smux_accept: setsockopt SO_RCVTIMEO: Option not supported by protocol
```

Index