Performance Management Advisors 8.1.1

Deployment Guide

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

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

About Genesys

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

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

Notice

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

Your Responsibility for Your System's Security

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

Trademarks

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

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 regional numbers provided on page 11. For complete contact information and procedures, refer to the ***Genesys Technical Support Guide***.

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: 811pma_dep_11-2011_v8.1.101.00

Table of Contents

List of Procedures 7

Preface 9

About Advisors 9
Intended Audience 10
Making Comments on This Document 10
Contacting Genesys Technical Support 11
Document History 11
Release 8.1.101.00 11

Part 1 **Creating the Databases 13**

Chapter 1 **Deployment Overview 15**

Deployment Prerequisites 15
Deployment Process Overview 16
Software Distribution Contents 18
Deployment Notes 21

Chapter 2 **Creating a SQL Server Database 23**

Creating a SQL Server Database 23
Assigning Additional User Permissions 35
Database Migration Scripts 35

Chapter 3 **Creating an Oracle 11g Database 37**

Creating an Oracle Database 37

Chapter 4 **Oracle 11g: Configuring Metrics Data Sources 43**

AGA Metrics on Same Oracle Instance as PLT Database 43
AGA Metrics on Different Oracle Instance From PLT Database 46
Cisco ICM Datasource or AGA Metrics on MSSQL Instance 47

Chapter 5 **Oracle Secure Deployment 49**

Secure Deployment for Oracle 11g 49
List of Function-Based Indexes 50

Part 2 **Deploying Advisor Components 53**

Chapter 6 **Deploying Advisors Platform 55**

Deploying Advisors Platform 55
User Authentication 56
Installation Process 60
Deploying Platform 60
Troubleshooting Installation Errors 72
Changing Memory Allocations 74
Configuring Access to External Websites 75
Changing the Mail Server Configuration After Server Installation 76
Changing Encrypted Passwords After Installation 76
Adding a Text Message on the Login Page 77
Customizing the Logo and Colors in the Advisors Browser 77
Customizing the Colors for Alert Management 77
Deploying and Configuring Apache 78
Using a Second Instance of Apache 81
Configuring Apache to Support HTTPS 82
Latency Getting to the Login page 83

Chapter 7 **Deploying Genesys Adapter 85**

Prerequisites 85
Installation Overview 86
Introduction 86
Dependencies and Issues 86
Support for LoggedIn Scripts 88
Deploying Genesys Adapter Manually 88
Deploying the Adapter Core Service Component 89
Operation of Stat Server Redundant Pairs 103
Modifying the XMLGen Configuration 104
Deploying the SDS Service 105
Deploying Resource Management Console 114
Deploying Multiple Instances of the Genesys Adapter Core Service on a Single Server 116
Installation Notes 116
Troubleshooting Installation Errors 118

Chapter 8 **Deploying Cisco Adapter 119**

Prerequisites 119
Installation Summary 119
Installation Contents 120
Deploying the Cisco Adapter 121
Deploying Multiple Instances of the Cisco Adapter on a Single Server 131
Troubleshooting Installation Errors 133

Chapter 9 **Deploying Contact Center Advisor and Workforce Advisor 135**

Deployment Notes 135
Prerequisites 136
Deploying CCAdv/WA Modules 136
Configuring Metric Graphing Properties 143
Deploying XML Generator Service 147
Deploying the XML Generator 147
Notes for the Data Source Database Name 152
Custom Time Zones 153
Workforce Advisor Web Service Option 154
Deploying the Genesys Advisors Browser 158
Deploying the Genesys Advisors Browser 158
Uninstalling the Genesys Advisors Browser 159
Formatting Alert Messages Sent by Advisors 160
Changing the XML Generator Connection after Installation 162
Deploying the XML Generator as a Service 163
Disabling Performance Monitor and the Workforce What-If Tool 164
Configuring Contact Groups 164
Contact Groups' Filename 164
Contact Group File's Header 164
Troubleshooting Installation Errors 165

Chapter 10 **Deploying Frontline Advisor 167**

Prerequisites 167
Installation Overview 168
Installation Contents 168
FA Hierarchy and Configuration Server 168
Deploying Frontline Advisor 169
Troubleshooting Installation Errors 177
Starting the Frontline Advisor Service 178
Verifying Server Connections 178
Verifying the Frontline Advisor Server Connection 178

Verifying Apache Routing 178
Verifying the Genesys Advisor Browser Connection 179
Integrating External Links 179
Changing the Values at the Enterprise Node 180

Chapter 11 **Deployment Generics 181**

Automated Installation Options 181
Specifying Input Properties 181
Performing a Semi-Silent Installation 182
Performing a Silent Installation 182
Advisor Component Names 183
Installing Services under Windows 2008 Server 183
Adjusting the Log File Roll and Retention Settings 184

Supplements **Related Documentation Resources 187**

Document Conventions 189

Index **..... 191**

List of Procedures

Creating the database 23
Creating a login to be used by the database 26
Creating linked servers for the database 29
Creating objects in the database 34
Creating an Oracle 11g database. 38
Configuring AGA metrics on same Oracle instance as PLT Database. 44
Configuring AGA metrics on different Oracle instance from PLT database 46
Configuring Cisco ICM or AGA metrics on MSSQL instance 48
Uninstalling Windows services 60
Deploying Platform 61
Changing the Mail Server configuration after Platform server is installed. 76
Changing an encrypted password 76
Customizing the logo 77
Deploying and configuring Apache. 78
Generating the SSL security certificate and private key. 82
Reconfiguring Apache to support HTTPS 83
Deploying Stat Server and MCR extensions 86
Deploying Genesys Adapter manually 88
Deploying the Core Service component. 89
Modifying the XMLGen Configuration. 104
Deploying the SDS service. 105
Deploying Resource Management console 114
Deploying the Cisco Adapter 121
Deploying multiple instances of Cisco Adapter on a single server. . . . 131
Deploying CCAdv/WA Modules 136
Changing the time period of graphed values 144
Changing the duration of values retained for graphing. 144

Changing the interval in seconds between values 145
Changing whether graphed values start at midnight 146
Deploying the XML Generator 148
Reviewing JDBC data source error logs. 153
Configuring custom time zones 153
Deploying Workforce Advisor Web service 154
Deploying the Genesys Advisors Browser 158
Uninstalling the Genesys Advisors Browser. 159
Deploying XML Generator as a service 163
Removing XMLGen as a service 163
Deploying Frontline Advisor 169
Starting the Frontline Advisor Service 178
Adjusting the log file roll & retention settings 184

Preface

Welcome to the Genesys *Performance Management Advisors 8.1 Deployment Guide.* This document describes how to deploy all Advisors components for a full implementation.

This document is valid only for 8.1.x releases of this product.

Note: For versions of this document created for other releases of this product, 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 contains the following sections:

- About Advisors, page 9
- Intended Audience, page 10
- Making Comments on This Document, page 10
- Contacting Genesys Technical Support, page 11
- Document History, page 11

For information about related resources and about the conventions that are used in this document, see the supplementary material starting on page 187.

About Advisors

The Genesys Performance Management Advisors product family enables contact center business and operations managers and key users to see real-time graphical metrics and Key Performance Indicators based on their role. This enables them to quickly identify developing service and performance issues and take corrective action before customers and revenues are affected. With Genesys Advisors, agents can also manage their own performance in real time, correlate performance with supervisors and receive the information they need.

Genesys Contact Center Advisor creates visibility into real-time operations, allowing users to quickly determine the root cause of problems and collaborate to resolve them.

Genesys Workforce Advisor consolidates data from multiple switches and workforce management applications to help organizations more effectively manage the supply of agents against the ever-changing call demand in the contact center.

Genesys Frontline Advisor monitors contact center agent performance metrics and behavioral rules, alerting managers when business objectives are not being met and if calls are being handled outside of contact center performance guidelines. This breakthrough contact center performance monitoring allows supervisors to effectively coach-in-the-moment to improve agent performance and reduce turnover.

Genesys Agent Advisor allows contact center agents to self-manage their performance. Genesys Agent Advisor provides the agents with the same performance information the supervisor has and gives them the opportunity to proactively manage their own performance in real time.

Intended Audience

This document is primarily intended for system implementers and system administrators. It has been written with the assumption that you have a basic understanding of:

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

Making Comments on This Document

If you especially like or dislike anything about this document, 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 scope of this document only and to the way in which the information is presented. Contact your Genesys Account Representative or 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.

Contacting Genesys Technical Support

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

Region	Telephone	E-Mail
North and Latin America	+888-369-5555 (toll-free) +506-674-6767	support@genesyslab.com
Europe, Middle East, and Africa	+44-(0)-1276-45-7002	support@genesyslab.co.uk
Asia Pacific	+61-7-3368-6868 (international)	support@genesyslab.com.au
Malaysia	1-800-814-472 (toll-free) +61-7-3368-6868 (international)	support@genesyslab.com.au
India	000-800-100-7136 (toll-free) +61-7-3368-6868 (international)	support@genesyslab.com.au
Japan	+81-3-6361-8950	support@genesyslab.co.jp
Before contacting technical support, refer to the *Genesys Technical Support Guide* for complete contact information and procedures.		

Document History

This section describes information that has been added or substantially changed since the first release of this document.

Release 8.1.101.00

- Installation process changes related to integration with Genesys Management Framework
- Installation process changes related to the hierarchy database for Frontline Advisor, which is now resides in the Genesys Configuration Server
- New optional configuration parameters for the processing and display of metrics and metric graphing

Part

1 Creating the Databases

Part 1 of this document describes the generic creation of both a Microsoft SQL Server database and an Oracle database. These two creation processes will be repeated with specific variations for each Advisors component being deployed.

This information appears in the following chapters:

- Deployment Overview, page 15
- Creating a SQL Server Database, page 23
- Creating an Oracle 11g Database, page 37
- Oracle 11g: Configuring Metrics Data Sources, page 43
- Oracle Secure Deployment, page 49

Chapter

1 Deployment Overview

This chapter gives an overview of deployment of an Advisors 8.1 solution:

- Deployment Prerequisites, page 15
- Deployment Process Overview, page 16
- Software Distribution Contents, page 18
- Deployment Notes, page 21

Deployment Prerequisites

Networks Advisors components and all related components (Stat Server, Configuration Server) must be installed on the same network.

Software Before commencing Advisors deployment, ensure that the following external software is installed on the appropriate physical computer involved in Advisors installation:

- Java Development Kit Installation, version JDK 1.6.
- Flash Player 10.x for non-IE browsers (such as Firefox).
- Install Apache HTTP Server 2.2.6.

  If the Apache server is installed on the same machine as Advisors Platform, the Apache server must use aport other than 8080 (which is used by Advisors Platform). In most cases, Apache will be able to use port 80.
- One of:
  - Microsoft SQL Server 2005
  - Microsoft SQL Server 2008
  - Oracle 11g

- If using Oracle 10g or 11g, the appropriate Oracle JDBC driver is also required. You can obtain the driver from Oracle's website, www.oracle.com. Advisors requires versions compatible with JDK 1.6. (Drivers containing tracing code or compiled with `-g` option are not necessary.)

  Note: The following Oracle JDBC drivers can used:
  - Oracle database 10g release 2 (10.2.0.4). The download file is `ojdbc14.jar`.
  - Oracle database 11g release 2 (11.2.0.2.0). The download file is `ojdbc6.jar`.

System Clocks All physical servers used in a given Advisors installation must have their system clocks synchronized with a central time server.

Deployment Process Overview

The high-level deployment process for an Advisors solution is described in Task Summary: Deploying an Advisors 8.1 Solution.

Task Summary: Deploying an Advisors 8.1 Solution

Step	Task	Notes & References
1	Ensure that all the external prerequisites are in place.	See "Deployment Prerequisites" on page 15.
2	Create the Platform database.	See either: • Chapter 2, "Creating a SQL Server Database," on page 23, or; • Chapter 3, "Creating an Oracle 11g Database," on page 37.
3	Install the Platform service, including Geronimo.	Unzip `advisors-platform-distribution-<version>.zip` into a temporary directory and check that all the build artifacts are present. See Chapter 6, "Deploying Advisors Platform," on page 55.
4	Optionally, create either the Genesys Adapter or Cisco Adapter database.	See either: • Chapter 2, "Creating a SQL Server Database," on page 23, or; • Chapter 3, "Creating an Oracle 11g Database," on page 37.

Task Summary: Deploying an Advisors 8.1 Solution (Continued)

Step	Task	Notes & References
5	Install the core service for the Adapter(s) you have installed.	Unzip `the relevant <component-name>-distribution-<version>.zip` into a temporary directory and check that all the build artifacts are present. • Chapter 7, "Deploying Genesys Adapter," on page 85 • Chapter 8, "Deploying Cisco Adapter," on page 119 If your installation will use a Genesys data source, you must deploy the Genesys Adapter. If a CCAdv/WA installation uses a Cisco data source, no adapter is required, but if FA/AA is installed, the Cisco Adapter must be present. Note that CCAdv/WA and FA cannot share Genesys Adapter instances.
6	Optionally install Contact Center Advisor, Workforce Advisor, XML Generator, Resource Management and Supervisor Desktop Service. **Note**: Resource Management is not available in a Cisco-only configuration.	See Chapter 9, "Deploying Contact Center Advisor and Workforce Advisor," on page 135. Platform must have been pre-installed on each physical server on which you install a Web application (such as Contact Center Advisor or Workforce Advisor). Servers running XMLGen require Advisors Platform to be installed.
7	Optionally, create the Frontline Advisor database.	See either: • Chapter 2, "Creating a SQL Server Database," on page 23, or; • Chapter 3, "Creating an Oracle 11g Database," on page 37.
8	Optionally, install Frontline Advisor/Agent Advisor.	See Chapter 10, "Deploying Frontline Advisor," on page 167.
9	Make any additional configuration changes required.	See the relevant component chapters.

Please also refer to the information that applies across multiple components, which you can find in the following chapter:

- Chapter 11, "Deployment Generics," on page 181.

Software Distribution Contents

Table 1 lists the contents of the Advisors software distribution.

Table 1: Distribution Artifacts

Advisors Component	Distribution Artifacts	Contents	Notes
Platform	advisors-platform-installer-<version>.jar		The installer for the Platform.
	baseweb-<version>-static-web.zip		A copy of the static files that can be served by Apache
	SQL Server platform-new-database-<version>.sql		The creation and migration script for the Platform database for MSSQL. This script is located in the `sql\mssql` directory.
	Oracle plt-<version>_TBS.sql plt-<version>_Schema.sql plt-<version>_DDL.sql plt-<version>_CUSTOM_ROUTINE.sql plt-<version>-InitialUpload.sql plt-8.1-SNAPSHOT_ROUTINE.sql		The creation scripts for the Platform database for Oracle. These scripts are located in the `sql\oracle` directory.
CCAdv/WA	ccadv-wa-server-installer-<version>.jar		The installer for CCAdv/WA.
	SQL Server mg-new-database-<version>.sql		The creation and migration database script for Metric Graphing for MS SQL. This script is located in the `sql\mssql` directory.
	Oracle mg-<version>_TBS.sql mg-<version>_Schema.sql mg-<version>_DDL.sql mg-<version>_ROUTINE.sql		The creation database scripts for Metric Graphing for Oracle. These scripts are located in the `sql\oracle` directory.

Table 1: Distribution Artifacts (Continued)

Advisors Component	Distribution Artifacts	Contents	Notes
FA/AA	fa-server-installer-<version>.jar		The installer for FA/AA.
	SQL Server fa-new-database-<version>.sql fa-database-migration-3.1-to-3.3.sql fa-database-migration-3.3-to-8.0.sql fa-database-migration-8.0-to-8.1.sql fa-database-migration-8.1-to-8.1.1.sql		The creation and migration scripts for the FA/AA database for MSSQL. These scripts are located in the `mssql` and `mssql\migrations` directories.
	Oracle fa_<version>_TBS.sql fa_<version>_Schema.sql fa-new-database-<version>.sql		The creation scripts for the FA/AA database for Oracle. The first 3 scripts are located in the `oracle` directory.
	SQL Server fa-hierarchy-mssql-<version>.sql hierarchy-migration-3.1-to-3.3.sql hierarchy-migration-3.3-to-8.0.sql hierarchy-migration-8.0-to-8.1.sql hierarchy-migration-8.1-to-8.1.1 sql		The creation and migration scripts for the FA/AA Hierarchy database for MSSQL. These scripts are located in the `mssql` and `mssql\migrations` directories.
	Oracle Not applicable.		

Table 1: Distribution Artifacts (Continued)

Advisors Component	Distribution Artifacts	Contents	Notes
AGA	aga-installer-<version >.jar	Platform	The installer for Genesys Adapter.
	SQL Server gc_core_newdb_<version>.sql gc_core_migrate_<old_version>_<version>.sql gc_metrics_newdb_<version>.sql		The creation and migration scripts for the Genesys Adapter databases for MSSQL. These scripts are located in the `configuration-schema\mssql` directory.
	Oracle gc_cfg_new_<version>_TBS.sql gc_cfg_new_<version>_Schema.sql gc_cfg_new_<version>_DDL.sql gc_metrics_new_<version>_TBS.sql gc_metrics_new_<version>_Schema.sql gc_metrics_new_<version>_DDL. sql		The creation scripts for the Genesys Adapter databases for Oracle. These scripts are located in the `configuration-schema\oracle` directory.
ACA	aca-installer-<version>.jar		The installer for Cisco Adapter
	SQL aca-new-database-<version>.sql aca-migration-3.3-to-8.0.sql aca-migration-8.0-to-8.1.sql aca-migration-8.1-to-8.1.1.sql GeneratePermsStatements.sql		The creation and migration scripts for the Cisco Adapter databases for MSSQL. These scripts are located in the `mssql` directory.
	Oracle aca-<version>_TBS.sql aca-<version>_Schema.sql aca-new-database-<version>.sql		The creation scripts for the Cisco Adapter databases for Oracle. These scripts are located in the `oracle` directory.
SDS	sds-installer-<version >.jar		The installer for Supervisor Desktop Service

Note: In 8.1.x releases, the Oracle scripts are creation scripts. Any existing schema with the same name must be dropped prior to running the scripts.

Deployment Notes

- Alert e-mail templates are located in the `<install dir>\conf\templates` directory.
- An 8.x version of the Advisors Browser can co-reside with a 3.x version on the same box; however, both versions cannot run on the same box simultaneously. Attempts to launch a second browser will only open another window for the running instance: for example, launching 3.3 and then 8.x will result in two 3.3 windows. For 8.x to co-reside with 3.X, you must do the following:
  - Agree to upgrade your browser to the later version found on the 8.x server, and
  - Agree not to remove the older version of the browser on your machine.
- The installation process has several distinct sections in order to accommodate different stages of system preparation. If some or all of the infrastructure software systems are already installed, various steps can be bypassed. It is important to get specific information about the location of these components from the original installer or the package manager.
- You cannot mix database types within an Advisors installation. Each installation must be either wholly MSSQL or wholly Oracle.

Chapter

2 Creating a SQL Server Database

This chapter describes how to create a SQL Server database. It contains the following section:

- Creating a SQL Server Database, page 23
- Database Migration Scripts, page 35

Creating a SQL Server Database

Procedure: Creating the database

Note: If due to security restrictions administrator or security administrator access cannot be granted, the local DBA should implement the steps described in this section.

Start of procedure

1. Connect to the SQL Server 2005 instance using Microsoft SQL Server Management Studio with the `LoginID` assigned to the SQL Server `sysadmin` server role. It can be `sa` or any other login assigned to the `sysadmin` server role and created for you for temporary use during the deployment.
2. In the object explorer right-click on `Databases` and choose `New Database`. Open the `General` screen (Figure 1 on page 24).

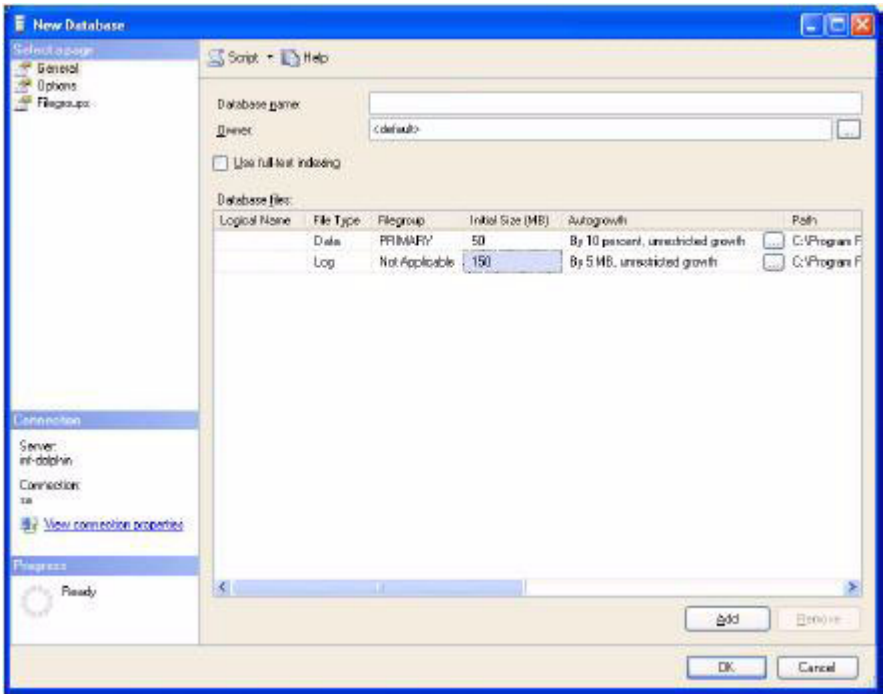


Figure 1: Database Properties—General

a. Specify the database name. See Table 2 for details.

b. Leave the owner as `<default>`.

c. Specify `50` Mb as the initial data file size with `Autogrowth` set to `By 10%, unrestricted file growth`.

d. Specify `150` Mb as the initial log file size with `Autogrowth` set to `By 5MB, unrestricted file growth`.

e. Change the pathnames to the data and log files if necessary.

Table 2: SQL Database Recommended Names

Advisors Component	Recommended Database Name	Notes
Platform	advisors_platformdb	Required for Advisors implementations.
CCAdv/WA		Required for the CCAdv/WA modules. Uses the Platform database.
Metric Graphing	advisors_mgdb	Required for running Dashboards and XML Gen.
FA/AA	advisors_fadb	Required for the FA/AA modules.

Table 2: SQL Database Recommended Names (Continued)

Advisors Component	Recommended Database Name	Notes
Genesys Adapter	advisors_genadptdb	Required for Genesys Adapter.
	advisors_gametricsdb	Used by AGA to transfer Genesys configuration and statistics values to XML Generator. Only required for CCAdv/WA installations.
Cisco Adapter	cisco_adapterdb	Required for Cisco Adapter.

3. Open the `Options` screen. See Figure 2 on page 25.

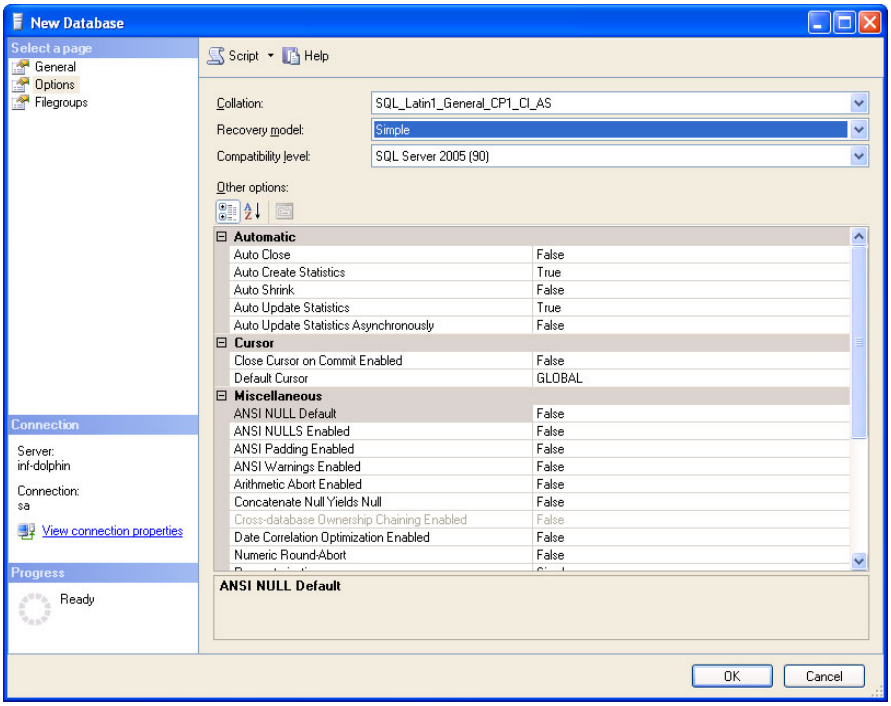


Figure 2: Database Properties, Options

   a. In the `Collation` field, select `SQL_Latin1_General_CP1_CI_AS`.
   b. In the `Recovery model` field, select `Simple`.
   c. Set `Auto Create Statistics` and `Auto Update Statistics` to the value `true`.

4. Click `OK`.
5. If you want to use a separate schema as a container for the database objects related to the Advisors applications, implement steps 6 and 7. Otherwise proceed to "Creating a login to be used by the database" on page 26.

6. In the `Object Explorer`, expand `Databases`, <*databasename*_db>, `Security`, and `Schemas`.

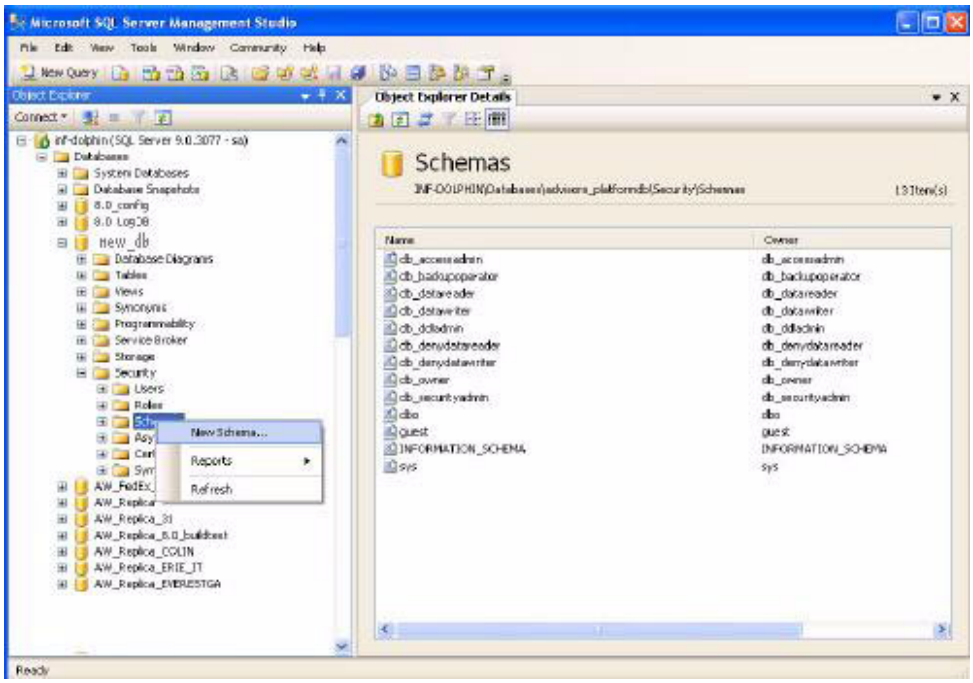


Figure 3: Database Security—Schemas

7. Right-click on `Schemas`, choose `New Schema`, then specify the schema name. You can choose any schema name that corresponds to your company and SQL Server naming conventions; for example, `callcenter01`.
8. Click `OK`. The database is created and properties are configured.

End of procedure

Procedure: Creating a login to be used by the database

`Note:` If due to security restrictions administrator or security administrator access cannot be granted, have the customer's DBA implement the steps described in this section.

Start of procedure

1. In the Microsoft SQL Server Management Studio object explorer, select `Server` and then `Security`.

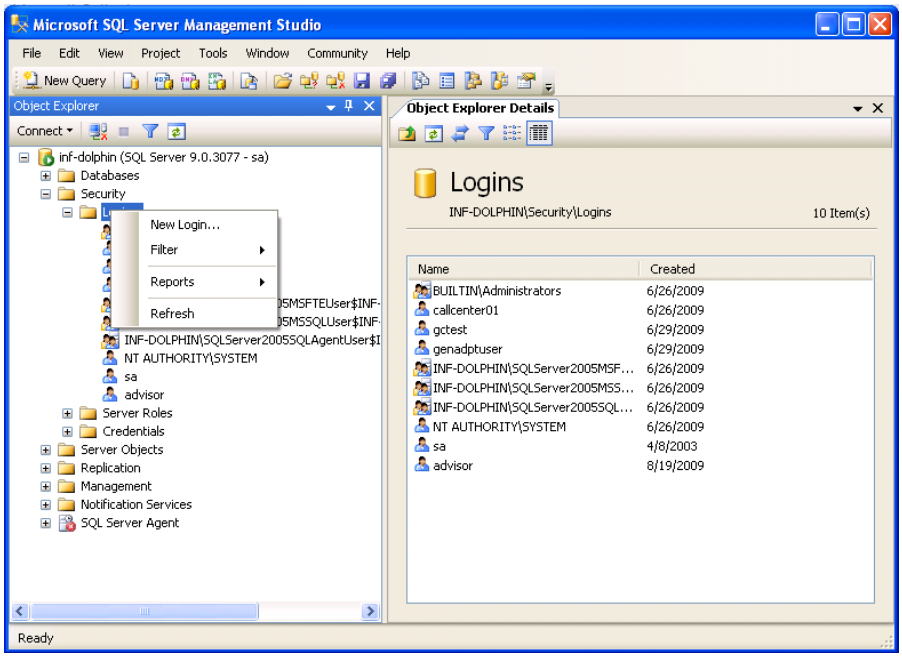


Figure 4: Server-Level Security

2. Right-click `Logins` and choose `New login`.
   a. Specify the login name (in this example, `callcenter01`).
   b. Click `SQL Server Authentication`.
   c. Specify a password that complies with the organization's security policy.
   d. If strong passwords are part of the security policy, check the `Enforce password policy` check box.
3. Open the `Login Properties - User Mapping` screen (Figure 5).

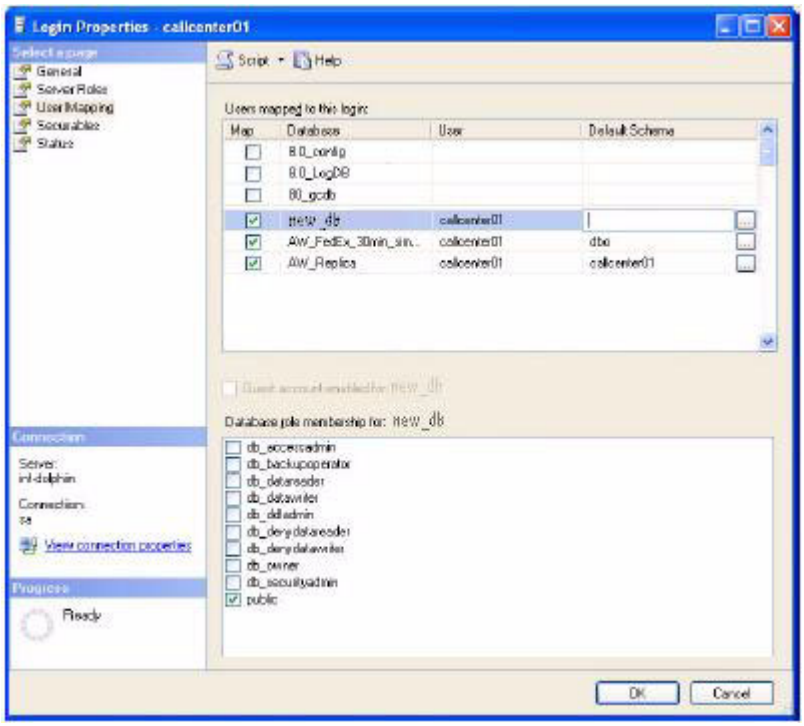


Figure 5: Login Properties—User Mapping

a. Map the user (`callcenter01` in this example) to the newly created database by checking the appropriate check box.

b. Choose `dbo` as a default schema if you skipped steps 5 and 6 in the procedure "Creating the database" on page 23. Otherwise select the name of the created schema.

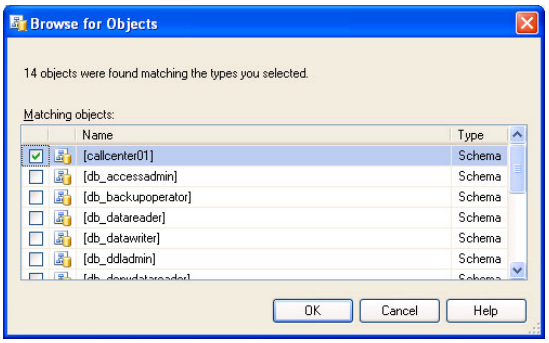


Figure 6: Browse for Objects

c. Click `OK`, then confirm your selection by highlighting it and clicking `OK` again in the `Select Schema` dialog. This returns you to the `User Mapping` screen.

d. Add the user to one or more database roles by checking the relevant check box in the lower panel of Figure 5. Select either:

- The db_owner database role
- All three of the db_datareader, db_datawriter, and db_ddladmin roles

Note: If you choose db_datareader, db_datawriter, db_ddladmin option, ensure that, after you create all of the database objects, you then complete the step described in "Assigning Additional User Permissions" on page 35.

The login to be used by database is now created and configured.

End of procedure

Procedure: Creating linked servers for the database

Note: If, due to security restrictions, administrator or security administrator access cannot be granted, the local DBA should implement the steps described in this section.

Prerequisites

Before you start the procedure, identify the data sources that must be accessed. If the customer uses a Cisco environment, then an ICM DBA must create an MSSQL Server login in all ICM databases that must be accessed.

Each login must have the master database as its default database.

The ICM AWDB database must have a user mapped to the above SQL Server login. The minimum requirement is that the user has permissions to select the data from the following AWDB views:

- Agent_Skill_Group_Real_Time
- Call_Type
- Call_Type_Real_Time
- Logical_Interface_Controller
- Peripheral
- Peripheral_Real_Time
- Service
- Service_Real_Time
- Skill_Group
- Skill_Group_Real_Time
- Service_Member

- `Controller_Time` table

The user can be given the above object-level permissions or assigned to an equivalent user-defined database role. If it is allowed by the customer security policy, the user can be assigned to any database standard role that includes the above minimum permissions. As an example the user can be assigned to the standard `db_datareader` role.

Each view in the Genesys Adapter metrics database must be accessible by the user defined in the Advisors Platform database.

Start of procedure

1. In the Microsoft SQL Server Management Studio object explorer, click `Server Objects`.

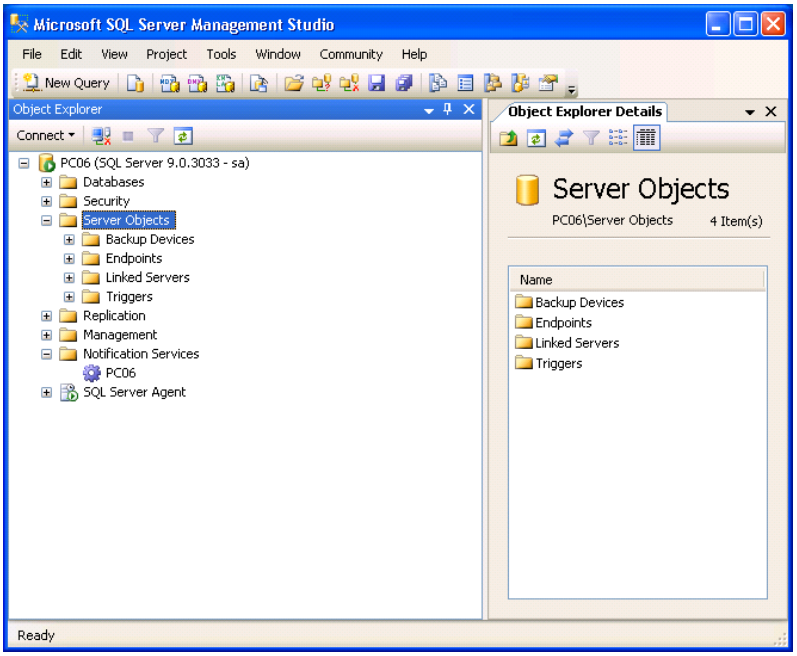


Figure 7: Server Objects

2. Right-click on `Linked Servers` and choose `New Linked Server...`The `New Linked Servers` screen displays (Figure 8 on page 31).

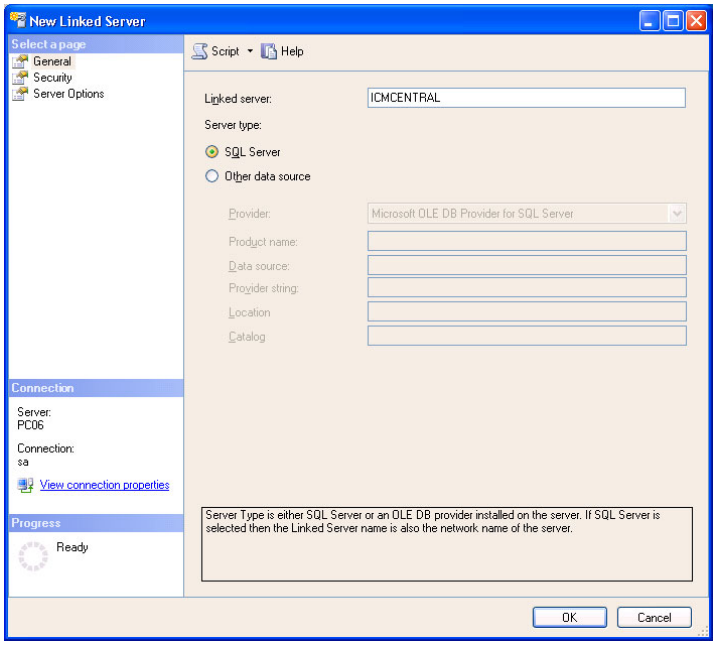


Figure 8: New Linked Server Screen

3. For the `Server` type, select `SQL Server`.
4. Specify the name of the external SQL database server to be accessed. Click `OK`. The `New Linked Server—Security Screen` displays.

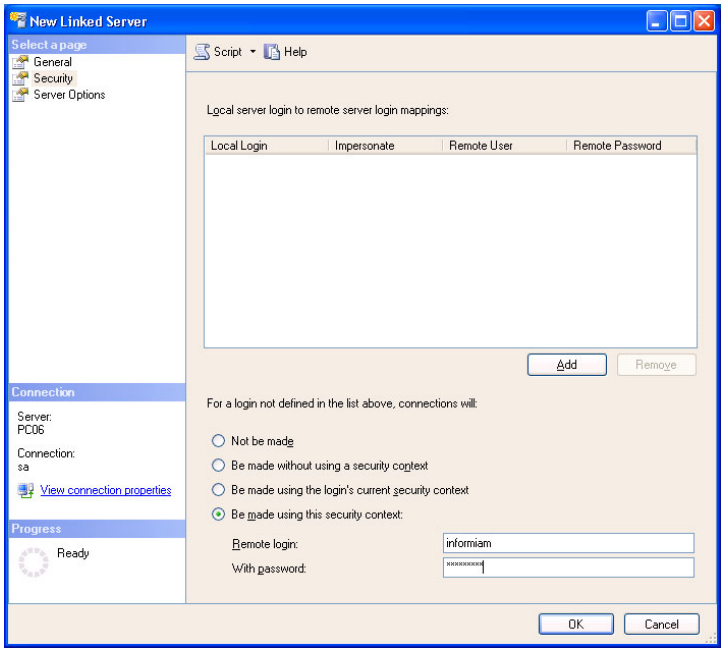


Figure 9: New Linked Server—Security Screen

5. On the `Security` screen:
   a. Select `Be made using this security context`.
   b. Specify the remote login and password created by the external administrator for access to the external database

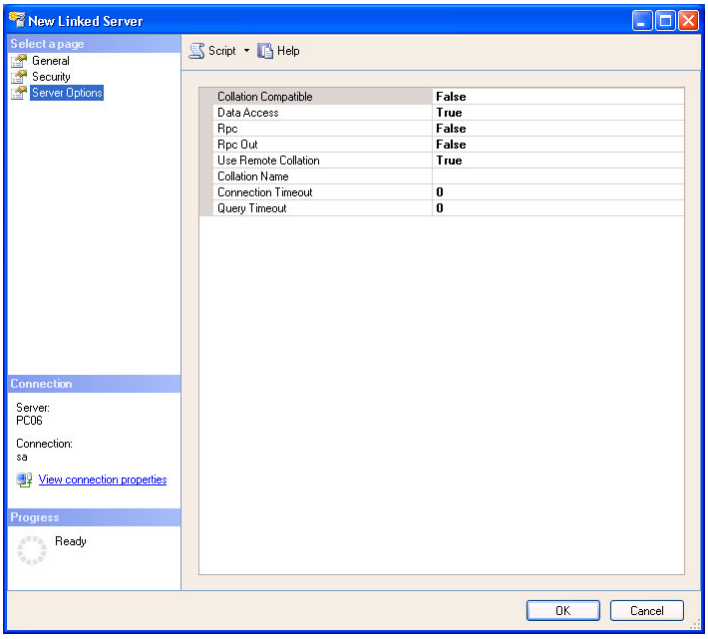


Figure 10: New Linked Server—Server Options

6. On the `Server Options` screen:
   a. Check the `Data Access` check box and `User Remote Collation` check box.
   b. Click `OK`.
7. To test the linked server connectivity run some SQL statements from the Microsoft SQL Server Management Studio.

Figure 11: Connecting to Database Engine

8. Enter the correct connection details and click `Connect`. The New Query screen displays (Figure 9 on page 31).
9. Click `New Query`
10. Type a query using the following notation:
    - Select `<...>` from `<Linked Server Name>.<Remote Database Name>.<Remote Database Owner>.<Remote Table Name>`

    Or:

    - Select `<...>` from `openquery( <Linked Server Name>, 'select <...> from >.<Remote Database Name>.<Remote Database Owner>.<Remote Table Name> [with (<locking hint>)]`

      Example–Cisco

      Select `* from ICM_AWDB1.company_awdb.dbo.Controller_Time`

      Or:

      Select `* from OpenQuery([ICM_AWDB1],'select * from company_awdb.dbo.Controller_Time (nolock)')`

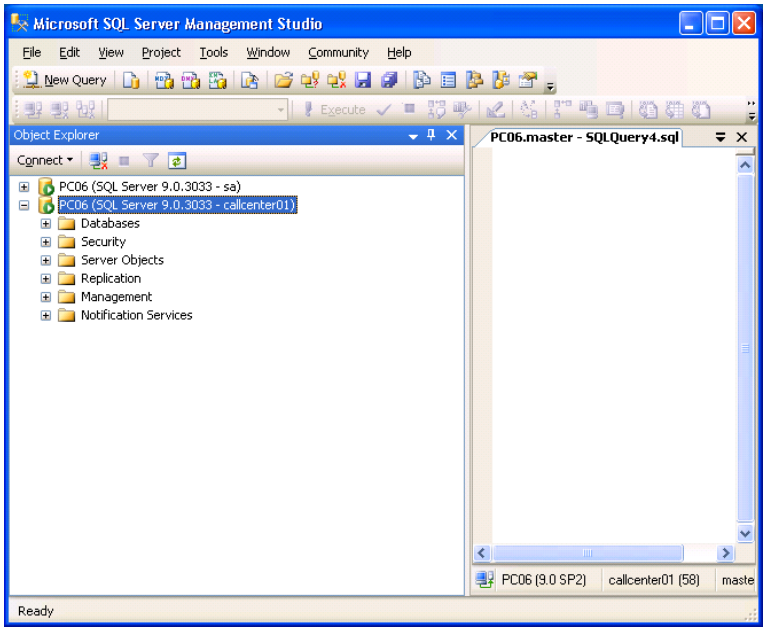


Figure 12: Microsoft SQL Management Studio—New Query

11. For each external data source, repeat this procedure.

End of procedure

Procedure: Creating objects in the database

Prerequisites

This step must be run either with the system administrator account or with a user having `db_owner` permissions to the database. In addition, the user must have the same default schema as that assigned to the Advisors user (created in the "Creating a login to be used by the database" section).

The `db_owner` can be given temporarily to the Advisors user for the purpose of running these steps.

Start of procedure

1. From Microsoft SQL Server Management Studio click `File`. Connect to the database engine as a user meeting the criteria above.
2. Make sure that you choose the correct database from the list of available databases.

3. From the `../sql_files` folder in the distribution folder, run the SQL script `[databasename]-new-database-<version>.sql` against the newly created database. This script creates the database user objects and populates some tables with default configuration data.
4. Scroll down the query results tab and check for errors. Ignore warnings.The objects are created.

End of procedure

Assigning Additional User Permissions

Assigning additional user permissions is necessary if the created database user is assigned to `db_datareader, db_datawriter` and `ddl_admin` roles but is not assigned to the `db_owner` role.

The user assigned to `db_datareader, db_datawriter` and `ddl_admin` roles must be granted execute permissions only, on all user stored procedures that exist in the database after the objects are created.

You can use the SQL Server interface to assign the permissions or create a grant permissions script and execute it against the newly created database. The following statement when executed against the newly created database will produce a set of grant permission statements.

To run the script press CTRL/T, then CTRL/E.

Copy the result from the result pane. That is, click on the `Result` pane, then click CTRL/A then CTRL/C. Paste the content (CTRL/V) into the query pane and execute the following:

```
select 'grant execute on
['+ routine_catalog+'].['+routine_schema+'].['+routine_name+'] to
<database user>' from INFORMATION_SCHEMA.ROUTINES where
ROUTINE_TYPE='PROCEDURE'
```

Note: Before executing the script, please change `<database user>` to the ID for your database user.

Database Migration Scripts

Platform database deployment/migration in MSSQL is performed by executing the `platform-new-database-<version>.sql` script supplied in the distribution. The same script can be applied to a new empty database or a database of any previous version.

Migration for other databases is performed by executing migration scripts supplied in the distribution.

These follow this pattern:

```
<database-name>-migration-<old-version>-to-<new-version>.sql
```

The example below is for the FA database:

```
fa-database-migration-3.1-to-3.3.sql
fa-database-migration-3.3-to-8.0.sql
fa-database-migration-8.0-to-8.1.sql
fa-database-migration-8.1-to-8.1.1.sql
```

To migrate a database across more than one update, run, the scripts in sequence from earliest to latest.

Chapter

3 Creating an Oracle 11g Database

This chapter describes how to create a generic Oracle 11g database. Each individual Oracle database in an Advisors implementation has its own creation script in the 8.1 release.

This chapter contains the following section:

- Creating an Oracle Database, page 37

Creating an Oracle Database

You must perform all the steps below on a machine where you have Oracle client installed. The installation scripts require SQLPlus which is installed as part of Oracle client installation.

Please verify that you have your `ORACLE_HOME` environment variable and `tnsnames.ora` content set properly. Verify the connectivity to the instance by running the following command line:

`tnsping <alias to the oracle instance contained in the local tnsnames.ora file>`.

Example:

Your `tnsnames.ora` contains the following entry:

```
wolf =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = inf-wolf.qalab.com)(PORT =
1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
```

```
      (SERVICE_NAME = orcl.qalab.com)
    )
  )
```

To check the connectivity type:

```
C:>tnsping wolf
```

The successful message will look as follows:

```
Used TNSNAMES adapter to resolve the alias
Attempting to contact (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST =
inf-wolf.qaslab.com)(PORT = 1521)) (CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = orcl.qalab.com)))
OK (0 msec)
```

.

Note: For the 8.1.000 release, the Oracle scripts are creation scripts. Any existing schema with the same name must be dropped prior to running the scripts.

Procedure: Creating an Oracle 11g database

Note: If due to security restrictions administrator or security administrator access cannot be granted, the local DBA should implement the steps described in this section.

Start of procedure

1. In the base data files directory on the Oracle server, for example `$ORACLE_BASE/ORADATA/` , create the required subdirectories:
   - `platform`
   - `ccawa`
   - `genadapt`
   - `frontline`
   - `aca`
2. Copy all of your Oracle database scripts to the machine where you have Oracle client installed.
3. On the machine where you have the Oracle client installed, start SQLPlus by entering `sqlplus /nolog` at the command prompt. You should see the prompt change to `SQL>`.

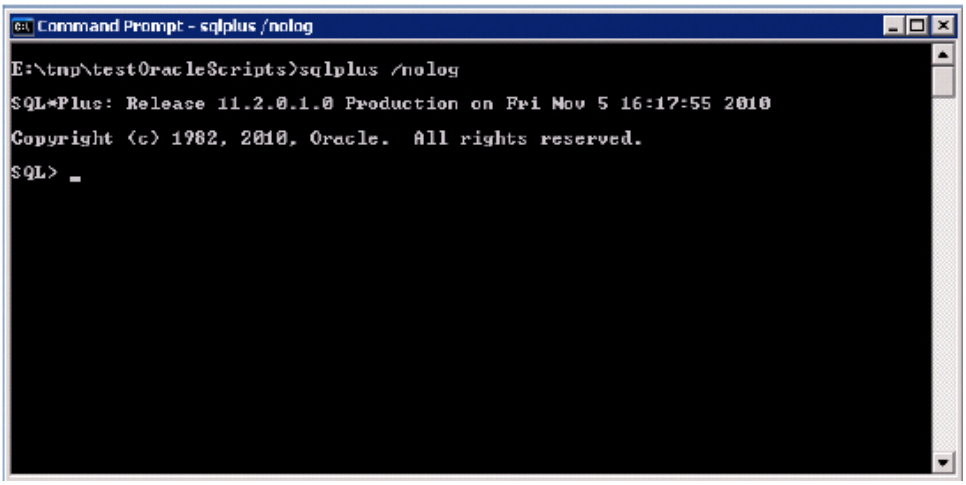


Figure 13: SQL Command Prompt

4. Using a user account that has DBA privileges (for example, `SYSTEM`), connect to the Oracle instance by entering:

   `conn {User}/{Password}@<alias to the Oracle instance contained in the local your tnsnames.ora file>`

   at the prompt.

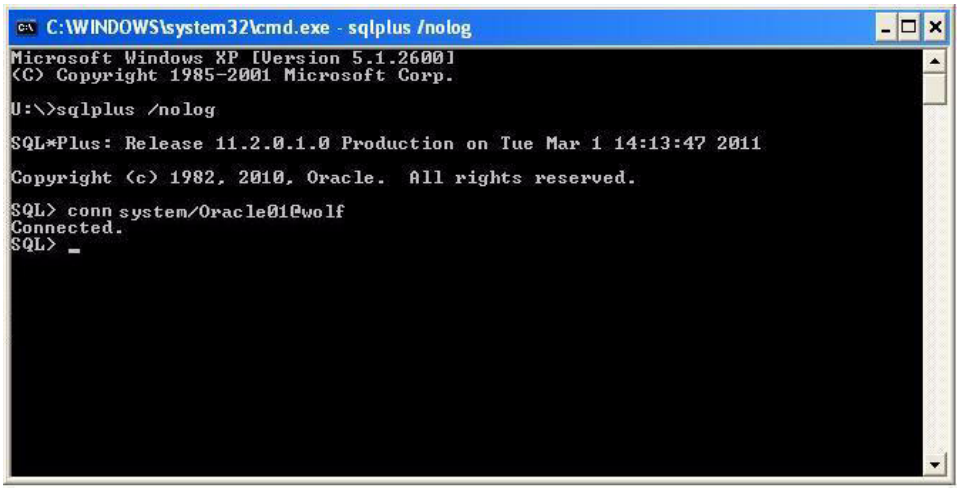


Figure 14: SQL Command Prompt 2

5. (Optional: perform Steps 8 through 10 only if the required tablespaces do not yet exist.

   If table spaces are already present, skip to Step 11.)

   If table spaces are not present, run the tablespace script by entering

   `@<script name>`

   at the prompt (where "<script name>" is the name of your tablespace script—`@plt-8.1-TBS.sql` in the example in Figure 15).

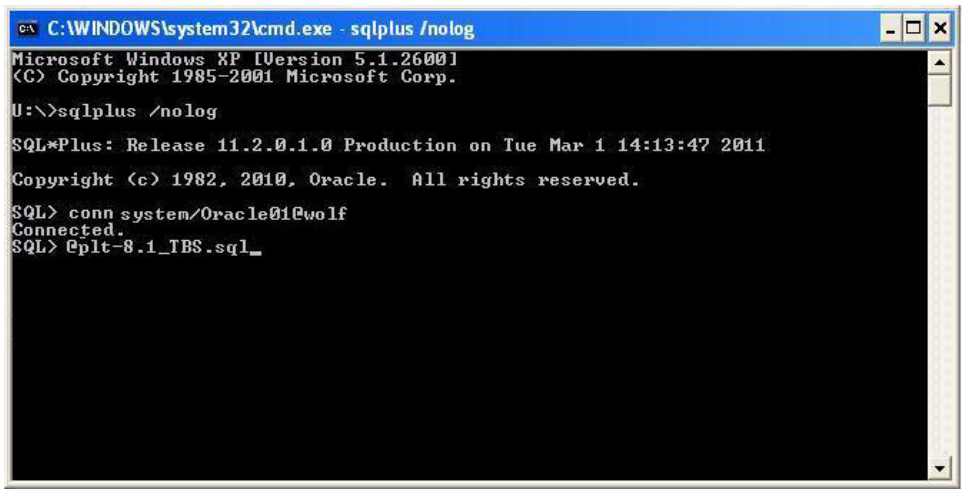


Figure 15: SQL Command Prompt 3

Note: See Table 1, "Distribution Artifacts," on page 18 for details of script names supplied in the distribution.

6. When prompted, enter the full path to your base data file directory (from Step 2), including the trailing slash.

   The script will either:

   - Create the tablespaces if they do not yet exist, or;
   - Skip the creation if the tablespaces are already present.

   Note that the script will preserve your SQLPlus connection, which you will reuse later in this procedure.

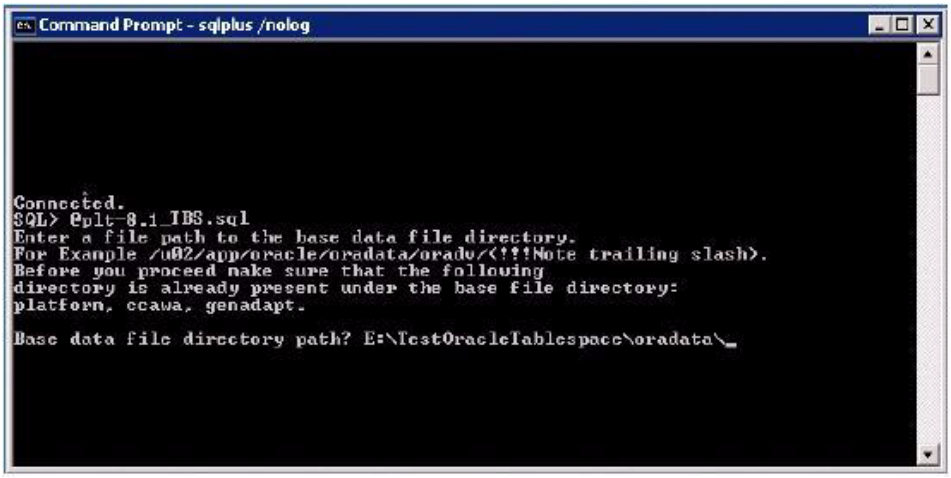


Figure 16: SQL Command Prompt 4

7. Verify the results of your script execution:
   a. Using a separate command prompt / terminal session, examine the `runTbsCre.log` file. You can find this log file in the same directory as your installation scripts.
   b. Browse your data file location to ensure that the files were created. Alternately, you can run the following query from any Oracle client connected as the system user:

      ```
      SELECT * FROM dba_data_files
      ```

8. To create the database schema and objects, and to load initial data, connect as a user with database administrator privileges (such as, system), and run the schema script by entering

   @plt-<version>_Schema.sql

   at the prompt.

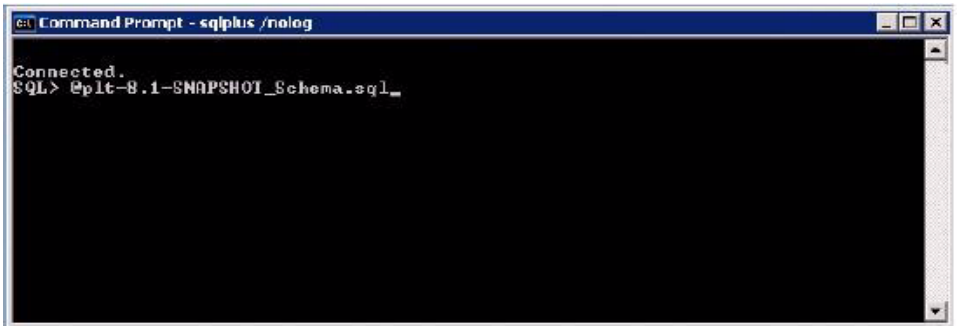


Figure 17: SQL Command Prompt 5

Note: See Table 1, “Distribution Artifacts,” on page 18 for details of script names supplied in the distribution.

9. When prompted, enter your schema name for the database objects. (The screens following use the example `AdvPlatform`.)

Figure 18: SQL Command Prompt 6

10. When prompted, enter the schema password.

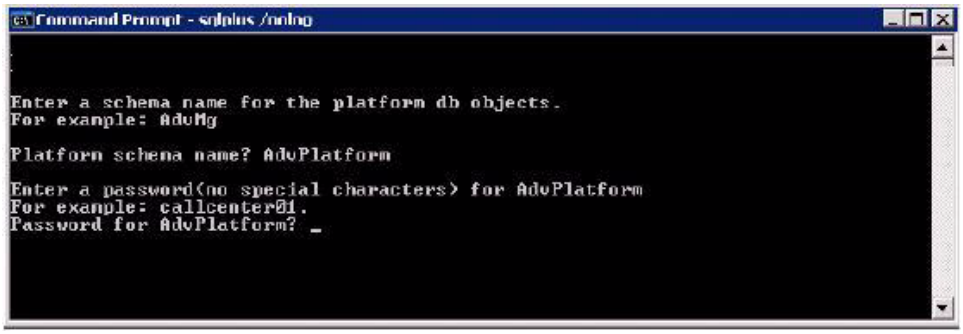


Figure 19: SQL Command Prompt 7

11. On SID prompt enter the alias to the Oracle instance contained in the local `tnsnames.ora`.

Figure 20: SQL Command Prompt 8

12. Once the script completes and SQLPlus exits, verify the results by examining the `runUsrCre.log` file, located in the same directory as your installation scripts.

End of procedure

The `DDL, ROUTINE` and `InitialUpload` scripts are executed automatically as part of the schema scripts. Do not run them separately.

Chapter

4 Oracle 11g: Configuring Metrics Data Sources

This chapter describes how to configure Oracle metrics datasources. This chapter contains the following sections:

- AGA Metrics on Same Oracle Instance as PLT Database, page 43
- AGA Metrics on Different Oracle Instance From PLT Database, page 46
- Cisco ICM Datasource or AGA Metrics on MSSQL Instance, page 47

AGA Metrics on Same Oracle Instance as PLT Database

This section describes how to configure AGA metrics where the AGA datasource is on the same Oracle instance as the Platform database.

Procedure: Configuring AGA metrics on same Oracle instance as PLT Database

Start of procedure

1. Either:
   - Connect as a privileged user (such as `system`) and grant the following select permissions to the platform user:

     ```
     GRANT SELECT ON <ga metrics schema>.AGENT_SKILL_GROUP_REAL_TIME TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.CALL_TYPE TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.CALL_TYPE_REAL_TIME TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.CONTROLLER_TIME TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.INTERACTION_QUEUE TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.INTERACTION_QUEUE_REAL_TIME TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.LOGICAL_INTERFACE_CONTROLLER TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.PERIPHERAL TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.PERIPHERAL_REAL_TIME TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.SERVICE TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.SERVICE_MEMBER TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.SERVICE_REAL_TIME TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.SKILL_GROUP TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.SKILL_GROUP_REAL_TIME TO <platform user>;
     GRANT SELECT ON <ga metrics schema>.CONTROLLER_TIME TO <platform user>;
     ```

   Or;

- Connect to the GA metrics schema as its owner and execute the following statements:

```
GRANT SELECT ON AGENT_SKILL_GROUP_REAL_TIME TO <platform user>;
GRANT SELECT ON CALL_TYPE TO <platform user>;
GRANT SELECT ON CALL_TYPE_REAL_TIME TO <platform user>;
GRANT SELECT ON CONTROLLER_TIME TO <platform user>;
GRANT SELECT ON INTERACTION_QUEUE TO <platform user>;
GRANT SELECT ON INTERACTION_QUEUE_REAL_TIME TO <platform user>;
GRANT SELECT ON LOGICAL_INTERFACE_CONTROLLER TO <platform user>;
GRANT SELECT ON PERIPHERAL TO <platform user>;
GRANT SELECT ON PERIPHERAL_REAL_TIME TO <platform user>;
GRANT SELECT ON SERVICE TO <platform user>;
GRANT SELECT ON SERVICE_MEMBER TO <platform user>;
GRANT SELECT ON SERVICE_REAL_TIME TO <platform user>;
GRANT SELECT ON SKILL_GROUP TO <platform user>;
GRANT SELECT ON SKILL_GROUP_REAL_TIME TO <platform user>;
GRANT SELECT ON CONTROLLER_TIME TO <platform user>;
```

2. Test the connectivity by verifying that the following select statements return 0 or more rows if run as Platform user:

```
SELECT * FROM "<ga metrics schema>.AGENT_SKILL_GROUP_REAL_TIME;
SELECT * FROM "<ga metrics schema>.CALL_TYPE;
SELECT * FROM "<ga metrics schema>.CALL_TYPE_REAL_TIME;
SELECT * FROM "<ga metrics schema>.CONTROLLER_TIME;
SELECT * FROM "<ga metrics schema>.INTERACTION_QUEUE;
SELECT * FROM "<ga metrics schema>.INTERACTION_QUEUE_REAL_TIME;
SELECT * FROM "<ga metrics schema>.LOGICAL_INTERFACE_CONTROLLER;
SELECT * FROM "<ga metrics schema>.PERIPHERAL;
SELECT * FROM "<ga metrics schema>.PERIPHERAL_REAL_TIME;
SELECT * FROM "<ga metrics schema>.SERVICE;
SELECT * FROM "<ga metrics schema>.SERVICE_MEMBER;
SELECT * FROM "<ga metrics schema>.SERVICE_REAL_TIME;
SELECT * FROM "<ga metrics schema>.SKILL_GROUP;
SELECT * FROM "<ga metrics schema>.SKILL_GROUP_REAL_TIME;
```

End of procedure

AGA Metrics on Different Oracle Instance From PLT Database

This section describes how to configure AGA metrics where the AGA datasource is on the same MSSQL instance as the Platform database.

Prerequisites

- The Platform user must be granted the following permission:

  ```
  GRANT CREATE DATABASE LINK TO <platform user>
  ```

- The `tnsnames.ora` file, located on the Oracle instance where the Platform schema resides, must contain a SID entry for the Oracle instance where the AGA metrics schema is located.

  Example:

  ```
  atlanta12 =
     (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST =p3458atl12
  .us.prod.company.com)(PORT = 1521))
      (CONNECT_DATA =
        (SERVER = DEDICATED)
        (SERVICE_NAME = orcl12. us.prod.company.com)))
  ```

  You can locate your `tnsnames.ora` file in the `$ORACLE_HOME/network/admin` directory.

Procedure: Configuring AGA metrics on different Oracle instance from PLT database

Start of procedure

1. Create the actual database or the public database link. For example;

   ```
   CREATE DATABASE LINK atl12.gcmdb81 CONNECT TO
                    "<ga metrics schema> IDENTIFIED BY "<ga metrics
   schema owner pwd> USING ' atlanta12';
   ```

2. Test the links from SqlDeveloper or run a select statement as a Platform user. For example;

   ```
   SELECT * FROM Controller_Time@atl12.gcmdb81;
   ```

End of procedure

Cisco ICM Datasource or AGA Metrics on MSSQL Instance

This section describes how to configure datasource metrics where either a Cisco ICM datasource or the AGA datasource is on the same Oracle instance as the Platform database.

Prerequisites

- Identify the databases that must be accessed.
- Ensure that a MSSQL Server login in all ICM and Genesys metrics source databases that must be accessed by Contact Center Advisor and Workforce Manager is created.
- Ensure that each login has the master database as a default database.
- Ensure that the ICM AWDB database has a user mapped to the above SQL Server login. The minimum requirement is that the user has permissions to select the data from:

CISCO source AWDB views

```
Agent_Skill_Group_Real_Time
Call_Type
Call_Type_Real_Time
Logical_Interface_Controller
Peripheral
Peripheral_Real_Time
Service
Service_Real_Time
Skill_Group
Skill_Group_Real_Time
Service_Member
```

and

```
AWDB Controller_Time table.
```

Genesys source metrics DB views

```
Agent_Skill_Group_Real_Time
Call_Type
Call_Type_Real_Time
Logical_Interface_Controller
Peripheral
Peripheral_Real_Time
Service
Service_Real_Time
```

```
Skill_Group
Skill_Group_Real_Time
Service_Member
Interaction_Queue
Interaction_Queue_Real_Time
Controller_Time.
```

- The user can be given the above object-level permissions or assigned to an equivalent user-defined database role. If it is allowed by the customer security policy, the user can be assigned to any database standard role that includes the above minimum permissions. As an example the user can be assigned to the standard `db_datareader` role.

Procedure: Configuring Cisco ICM or AGA metrics on MSSQL instance

Start of procedure

1. Ensure that the Oracle gateway for MSSQL is installed and configure the initialization parameter file(s) and Oracle Net for the gateway for each Cisco ICM data source or Genesys metrics database.
2. Ensure that a separate database link in the platform schema for each ICM or Genesys metrics data source is created. For this the user must be granted the following permission:

   ```
   GRANT CREATE DATABASE LINK TO < user>;
   ```

3. Create links using the following pattern:

   ```
   CREATE DATABASE LINK <arbitrary mssql database link name> CONNECT TO
   "<MSSQL username created for you in ICM awdb>" IDENTIFIED BY "<
   MSSQL password created for you in ICM awdb >" USING '<gateway_sid>';
   ```

   where `gateway_sid` is the name of the non-Oracle SID created by the DBA in the `tnsnames.ora` file.

   You can locate your `tnsnames.ora` file in `$ORACLE_HOME/network/admin` directory. For example;

   ```
   CREATE DATABASE LINK "prod67543.icm1" CONNECT TO
   "user1" IDENTIFIED BY "password1" USING 'dg4msql2';
   ```

4. Test the links from SqlDeveloper or run a select statement against the whole set of views as a Platform user. For example:

   ```
   SELECT * FROM  "Controller_Time"@prod67543.icm1;
   ```

End of procedure

The configuration of ICM data sources is now complete.

Chapter

5 Oracle Secure Deployment

This chapter describes how to deploy Oracle securely. This chapter contains the following section:

- Secure Deployment for Oracle 11g, page 49

Secure Deployment for Oracle 11g

Oracle 11g offers:

- Transparent Database Encryption (TDE) introduced in Oracle 10g which allows the encryption of individual column content on the data file level.
- Tablespace encryption introduced in Oracle11g which allows the encryption of the entire content of a tablespace.

The following specifics of Advisors database deployment must be considered if the above Oracle features are used:

- All tables and indexes are distributed among different tablespaces with specific names, properties and sizing. The tablespace create statements are contained in `xxx_TBS.sql` deployment scripts supplied per each schema.
- There are no ready-to-use scripts for encrypted tablespace creation. The existing scripts must be modified by the DBA before the actual database deployment based on the local security policies and the encryption scope.
- Each tablespace is created in a specific folder located inside the base data files directory specified as a parameter of the script. The different location for the encrypted tablespaces must be considered during the script modification.
- The names of the tablespaces are included into the create object statements. If the customer chooses to encrypt only selected tables, a new encrypted tablespace must be created and the tablespace property must be changed in the related ddl statements contained in the `<version>_DDL` script.

- TDE limitations related to function-based indexes are applicable to Advisor Suite. There are a number of function-based indexes that need to be modified or dropped if the column-based encryption of the related columns is chosen. Another option is to encrypt the entire content of the tables that contain the chosen columns by placing these tables into an encrypted tablespace.

List of Function-Based Indexes

Platform Schema

Index: `IX_APPLICATION_NAME`

Table: `APPLICATION`–Contains application group metadata

Column expression: `UPPER("NAME")`

Index: `IX_CALL_APP_UP`

Table: `CALL_APPLICATION`–Contains metadata for queues, call types, services, interaction queues

Column expression: `UPPER("NAME")`

Index: `IX_CALL_CENTER_NAME`

Table: `CALL_CENTER` –Contains contact center metadata

Column expression: `UPPER("NAME")`

Index: `IX_CALL_CREGION_NAME ON REGION`

Table: `REGIONS`–Contains metadata for geographic regions, reporting regions and operating units

Column expression: `UPPER("NAME"), UPPER("TYPE")`

Index: `IX_CG_UP`

Table: `CONTACT_GROUP`–Contains metadata for workforce contact groups

Column expression: `UPPER("NAME")`

Index: `IX_CONTACT`

Table: `CONTACT`–Contains Advisors users contact data

Column expression: `UPPER("EMAIL")`

Index: `IX_PG_NAME`

Table: `PG`–Contains metadata for peripheral gateways

Column expression: `UPPER("PG_NAME")`

Index: `IX_USERS_USERNAME`

Table: `USERS`–Contains the list of Advisor users

Column expression: `UPPER("USERNAME")`

Frontline Advisor Schema:

Index: `UK_UNIQUERULE`

Table: `FA_RULES`–Contains rules

Column expression: `COALESCE("SUPVRID","AGENTID","TEAMID",0)`

Index: `UK_UNIQUETHRESHOLD`

Table: `FA_THRESHOLDS`

Column expression: `COALESCE("SUPVRID","AGENTID","TEAMID",0)`

Part

2 Deploying Advisor Components

Part 2 of this document describes the deployment of all Advisor components.This information appears in the following chapters:

- Deploying Advisors Platform, page 55
- Deploying Genesys Adapter, page 85
- Deploying Cisco Adapter, page 119
- Deploying Contact Center Advisor and Workforce Advisor, page 135
- Deploying Frontline Advisor, page 167
- Deployment Generics, page 181

Chapter

6 Deploying Advisors Platform

This chapter describes how to deploy the Advisors Platform component. It contains the following sections:

- Deploying Advisors Platform, page 55
- Troubleshooting Installation Errors, page 72
- Changing Memory Allocations, page 74
- Configuring Access to External Websites, page 75
- Changing the Mail Server Configuration After Server Installation, page 76
- Changing Encrypted Passwords After Installation, page 76
- Adding a Text Message on the Login Page, page 77
- Customizing the Logo and Colors in the Advisors Browser, page 77
- Deploying and Configuring Apache, page 78
- Latency Getting to the Login page, page 83

Deploying Advisors Platform

The installer will not upgrade an existing installation. The old installation must be completely removed by deleting its installation directory.

If you plan to do this, uninstall the Windows services for the Contact Center Advisor, XMLGen Application and the Genesys Advisors Server before you delete the installation directory. You must do this if you are going to re-install Genesys Advisors in a different directory from the one in which it is currently installed. This is because uninstalling the Windows services requires files that are in the installation directories you are going to delete. Once you delete them you cannot uninstall the Windows services.

User Authentication

In release 8.1.1, all user authentication is performed by Genesys Configuration Server. The Advisors Platform module, which is responsible for handling user authentication for all other modules (Contact Center Advisor, Workforce Advisor, and Frontline Advisor) now connects to the Configuration Server via the PSDK using a Super Administrator account. When a user tries to log in, the credentials are passed to the Configuration Server for validation.

This change means that where previously customers need to maintain two sets of Genesys accounts, one for the Genesys platform and one for Advisors, this duplication is now removed and a single authentication mechanism replaces it.

Configuration Requirements in Configuration Server

The information in the Advisors database and the Configuration Server must always be synchronized. The Configuration Server is now designated as the master record keeper.

The only user accounts that should be maintained in the Advisors database are those that need access to the Advisor modules. However, the Configuration Server can have thousands of persons, including all the agents in the environment. In order to limit the number of accounts that are synchronized with the Advisors database, you must created access groups in the Configuration Server.

Three access groups need to be created in each tenant that has users that need access to Advisors:

- Advisors Users—List of persons/users that are dashboard users only.
- Advisors Super Administrators—List of persons/users that are Super Administrators for Advisors.
- Advisors Partition Administrators—List of persons/users that are partition Administrators for Advisors

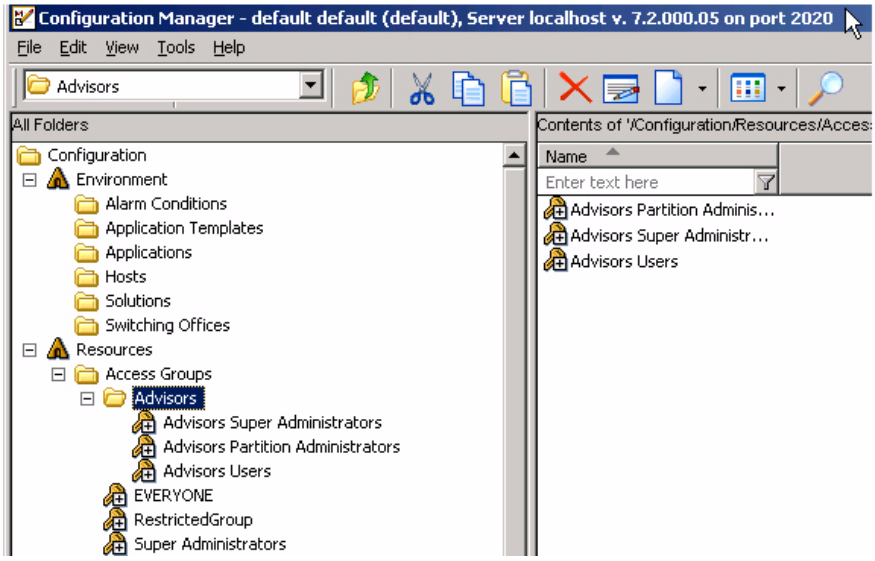


Figure 21: Configuration Server Access Groups

Only user accounts belonging to one of these access groups are synchronized with the Platform database. Users can belong to one and only one access group. If they belong to multiple access groups, their roles will be overwritten in the Advisors database and the final role assigned to the user is undetermined.

If a user is present in the Configuration Server but not part of one of the Advisors access groups, they would not be allowed to access any modules within Advisors even if they are successfully authenticated (since there would be no active account for the user in the Advisors database).

Genesys Impact

No migration procedures are required for Genesys customers as long as the existing user accounts in the Advisors database have the same user name as their corresponding `Person` accounts in the Configuration Server.

If the user names are different, then a system administrator will need to go through the user accounts once the start-up import process is complete to configure the module access for the users. Note that in such a scenario, the user accounts with the Configuration Server user name will be marked as `Active` ones and the previously configured user accounts in the Advisors database will be marked as `Inactive`.

Allowing User Creation

The ability to create users in the Administration user interface is governed by the setting you choose for the parameter `Allow User Creation?` in the Platform installer. The default value is `No`.

After installation, you can change this setting by editing the file `conf/GenesysConfig.properties`. In this file, change the value of `genesys.configServer.allowUserCreate`.

Then restart the Geronimo application server.

Allowing Password Modification

The ability to modify users' passwords in the Administration user interface is governed by the setting you choose for the parameter `Allow Password Modification?` in the Platform installer. The default value is `No`.

After installation, you can change this setting by editing the file `conf/GenesysConfig.properties`. In this file, change the value of `genesys.configServer.allowPasswordChange` to `true`.

Then restart the Geronimo application server.

Cisco Impact

A migration tool is provided for Cisco customers to import the user accounts from the Advisors database to the Configuration Server. This tool provides a simple bulk push of all existing user accounts in the Advisors database to the Configuration Server under the `Resources` tenant. The access groups in the Configuration Server are also set up under the `Resources` tenant, and the user accounts are added to the appropriate access groups based on their role.

In pure Cisco environments, creating, copying and deleting users as well as password management are enabled in the Administration module if the `Allow User Creation?` and `Allow Password Modification?` options are checked during installation (see Figure 29 on page 67).

User Access to Modules

From the administrator's perspective, user access to Advisors modules is managed in the same way through the Administration Workbench. However, the authoritative source for module access exists in the Configuration Server. This configuration is stored in the `AdvisorModules` section of each user's `Annex` tab (see Figure 22 on page 59).

For each module the user has access to, an entry is added in this annex section with a key corresponding to the module's code (as per the Platform database's `Modules` table), and a value of `1` (this can be a numeric or string value type).

Changes to a users's module access through the Administration Workbench are propagated to the Configuration Server, and similarly changes to the `AdvisorModules` section of the user's `Annex` tab (for example, during a bulk import operation) are reflected in Advisors when the user logs in.

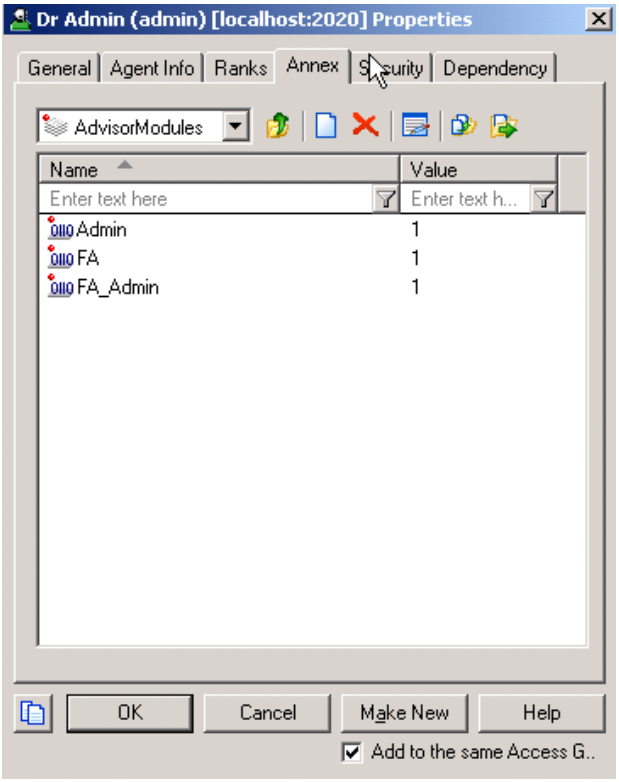


Figure 22: User Annex Tab with Advisor Module Access

Module Codes

- Contact Center Advisor—`CCAdv`
- Workforce Advisor—`WA`
- Frontline Advisor—`FA`
- Administration—`Admin`
- FA Administration—`FA_Admin`
- Resource Management Console—`RMC`
- Alert Management—`AlertMgt`

Installation Process

Procedure: Uninstalling Windows services

Start of procedure

1. Stop the Windows services for Advisor's components.
2. Close the `Services` window.
3. Open a command prompt window.
4. Change directory to the Advisors base directory (the one in which you installed Genesys Advisors), and then change it to `bin\windows-x86`.
5. Run the command: `UninstallAdvisorsServer.bat`.
6. Change the directory to the one in which XMLGen is installed.
7. Run the command `UninstallXmlgen.bat`.
8. If Genesys Adapter is installed, change the directory to the one in which the Genesys Adapter is installed, then change it to `bin`.
9. Run the command `Uninstall-Adapter-NT.bat`.

> Note: Repeat Steps 8 and 9 if Cisco Adapter is installed.

10. Close the command prompt window.
11. Delete all contents from the Advisors base directory.

> Note: Do NOT delete all the contents of the GCTI directory, because this may contain non-Advisors Genesys components.

End of procedure

Deploying Platform

If the Advisors Browser is installed in the installation directory, uninstall it before deleting the directory. Then reinstall the Advisors Browser again after you have installed Genesys Advisors components. (See "Deploying the Genesys Advisors Browser" on page 158.)

Each Web-based application (such as Dashboards, System Administration module, Workforce Web Service and the XMLGen application) requires the installation of the Advisors Platform. The Platform installer installs the base services:

- Geronimo

- Base web
- Navigation service
- Mail-Delivery service
- Preferences service
- Cache service
- Security Realm
- The data source
- Cluster Manager

Note: The Platform JMS URL configuration is named Cluster Node configuration.

Procedure: Deploying Platform

Start of procedure

1. Run the installation jar file by either;
   - Using the command `java -jar advisors-platform-installer-<version>.jar`; or,

- Double-clicking the `advisors-platform-installer-<version>.jar` in the release bundle.

Note: Double-click does not work if only JDK is installed (that is, JRE is not present).

Figure 23: Installer Screen

2. Click `Next`. The `Module to Install` screen displays (see Figure 24 on page 63).

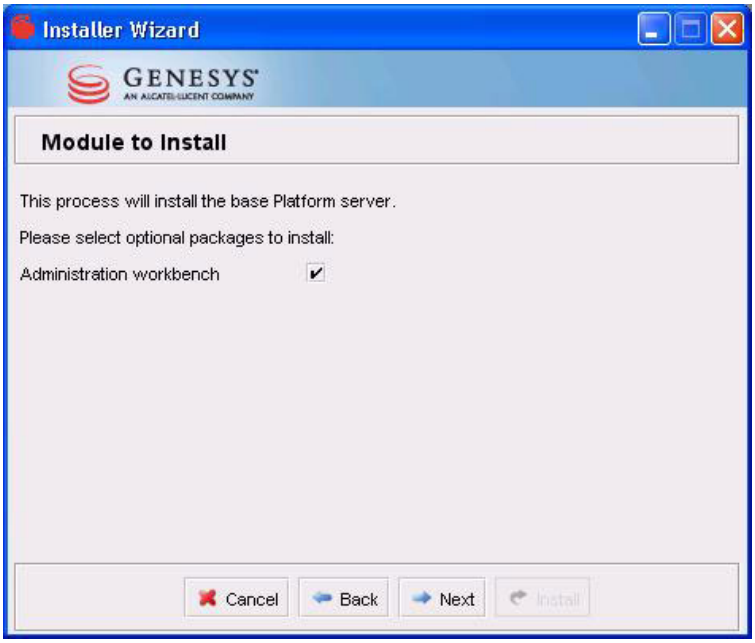


Figure 24: Module to Install Screen

3. If the administration workbench is not already installed, check the `Administration workbench` checkbox.
4. Click `Next`. The `Destination Directory` screen displays.

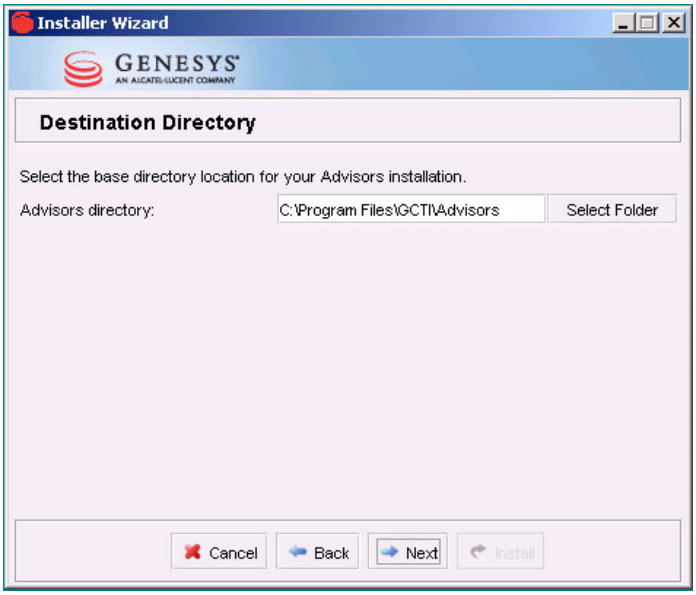


Figure 25: Destination Directory Screen

5. Select the destination directory in which the files will be installed (the Advisors base directory).

   The default directory is ..\GCTI\Advisors. If this directory does not yet exist, you will be prompted to create it.

   Click Next.

6. The Java Development Kit screen displays (Figure 26 on page 64).

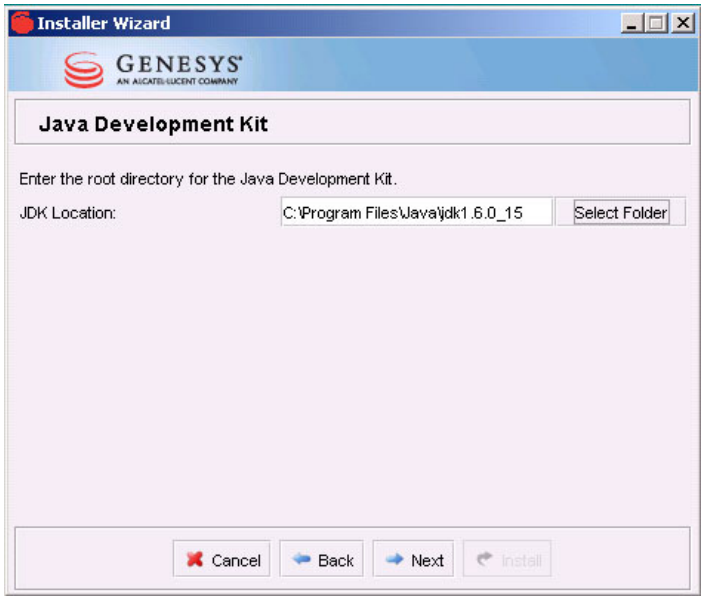


Figure 26: Java Development Kit Screen

7. Enter or select the JDK folder location for the Java Development Kit and click Next.The Cluster Node Configuration screen displays (Figure 27).

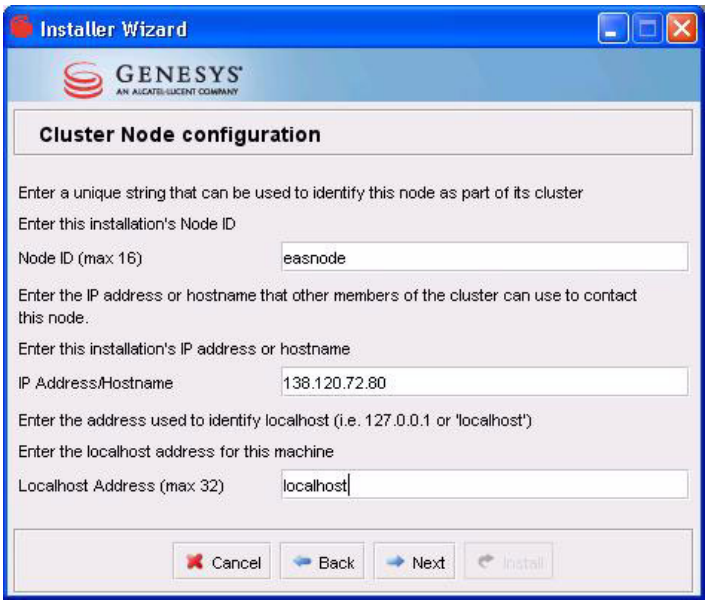


Figure 27: Cluster Node Configuration Screen

8. Each server that installs Platform requires a unique cluster node. Configure the node with the following information:
   - `Node ID`—A unique ID across all Platform installations. Must not contain spaces or any special characters, must be only alpha numeric. For example; `node1; node2`.
   - `IP Address/Hostname`—The IP address or host name that other cluster members will use to contact this node, not `localhost` nor `127.0.0.1`, for example, `192.168.100.1`.
   - `Localhost address`—The local host address, `localhost` or `127.0.0.1`.

   Note: When using numerical IP v6 addresses, please enclose the literal in brackets.

   Click `Next`.
9. The `Genesys Configuration Server Connection Details` page displays. See Figure 28 on page 66.

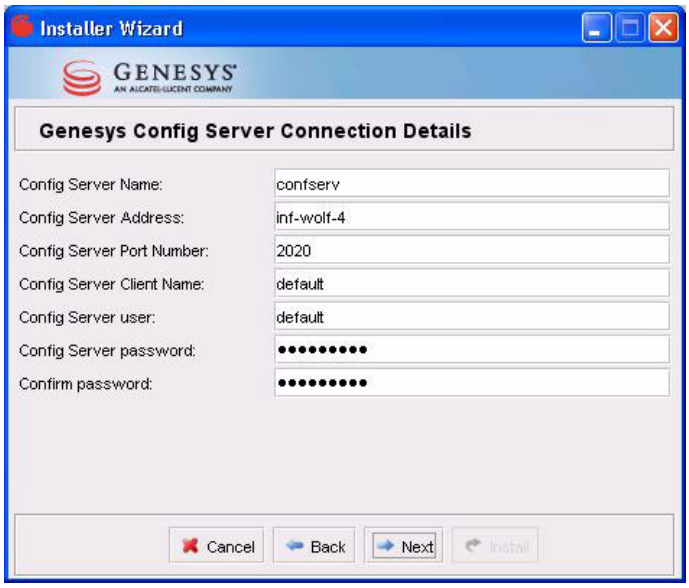


Figure 28: Genesys Configuration Server Connection Details page

10. Complete the details of the Genesys Configuration Server to which this instance of Platform will connect.

> Note: The Genesys Configuration Server password is encrypted and saved in the `..\GCTI\Advisors\conf\GenesysConfig.properties` file by default (unless altered in Step 4). To change the password see "Changing Encrypted Passwords After Installation" on page 76.

11. Click `Next`. The `User Management Options` page displays.

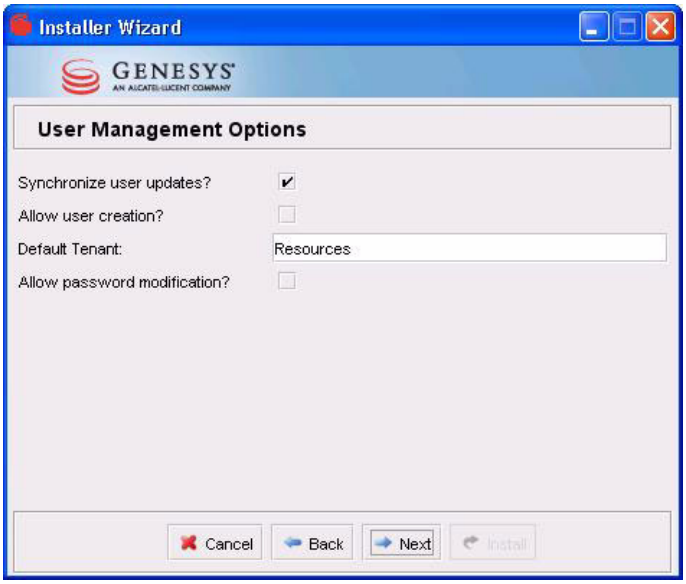


Figure 29: User Management Option page

12. To synchronize user updates, check the check box.

> Note: Selecting this option controls whether update events from the Configuration Server result in updating the Advisors database with the new information.
>
> In a clustered environment, a single Platform instance must be designated as responsible for maintaining the user account synchronization. Other Platform instances in the cluster will continue to provide PSDK access to Advisors modules, so for them, this configuration option can be deselected.
>
> Enabling this option on multiple clustered instances of Platform will result in redundant updates to the database.

13. Select the `Allow User Creation?` check box to enable the `Copy`, `Create` and `Delete` buttons in the `Administration | Users` section of the Administration UI.
14. Add the name of the default Genesys tenant to which new users will be added if they are created through the `Administration | Users` section of the Administration UI.
15. Select `Allow Password Modification?` to make the `Password` field editable via the `Administration | Users` section of the Administration UI.
16. Click `Next`. The `Database Type` screen displays.

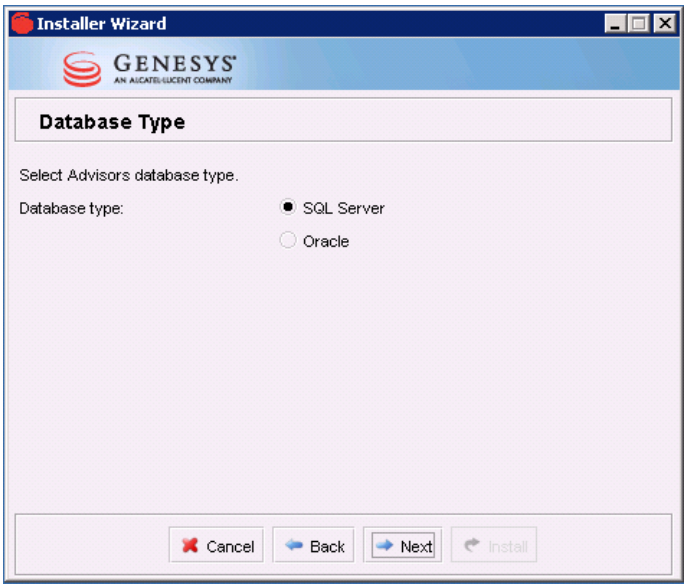


Figure 30: Database Type Screen

17. Select the database type for this installation:
    - Microsoft SQL Server
      Click `Next` and go to Step 18.
    - Oracle
      Click `Next` and go to Step 20

18. The `Genesys Advisor Platform Database` screen for MSSQL is displayed.

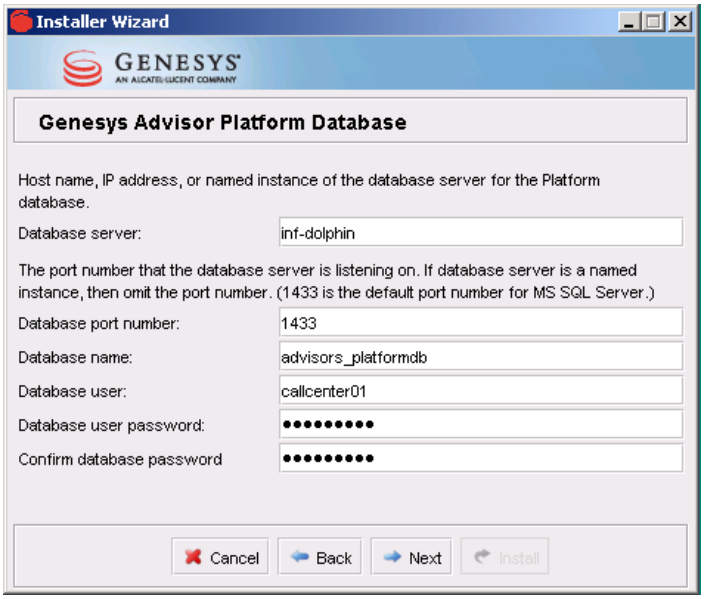


Figure 31: Genesys Advisor Database Screen for MSSQL

19. Enter the database connectivity parameters for the already created or upgraded database (that is, the database must be present and at the current version prior to running the installer). These parameters are server (machine), port number, name, user, and password.

    Note: When using numerical IP v6 addresses, please enclose the literal in brackets.

    If the database server is a named instance, then omit the port number. Click Next. The Mail Service Configuration screen is displayed (Figure 34 on page 71). Go to Step 25.

20. The Genesys Advisor Platform Database screen for Oracle is displayed.

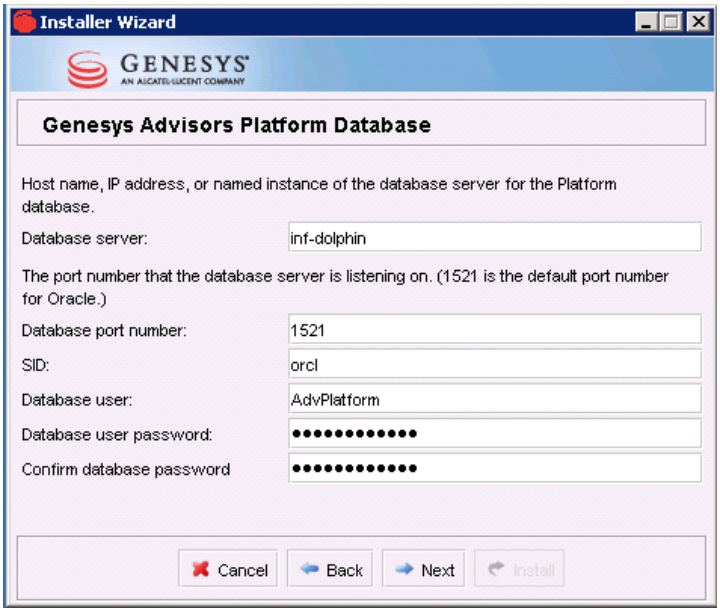


Figure 32: Genesys Advisors Platform Database Screen for Oracle

21. Specify the parameters for the Platform Oracle database:
    - Database Server—The host name where the database server is running
    - Database port number—The database server's port number
    - SID—The database instance alias.
    - Database user and password—The database schema created / used for the Platform database.

    Note: When using numerical IP v6 addresses, please enclose the literal in brackets.

22. Click Next. For Oracle only go to Step 23. Otherwise go to Step 24.
23. Locate the Oracle JBDC driver, then click Next.

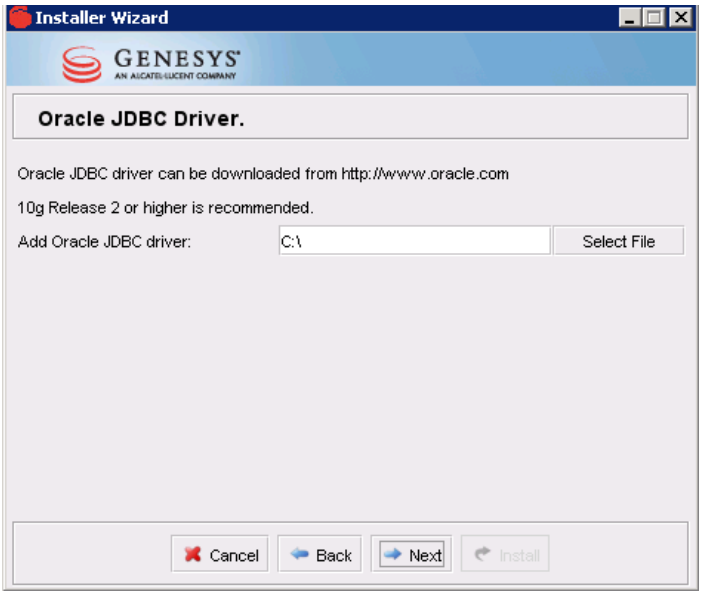


Figure 33: Oracle JBDC Driver Screen

Note: The following Oracle JDBC drivers can be used:

- Oracle database 10g release 2 (10.2.0.4). The download file is `ojdbc14.jar`.
- Oracle database 11g release 2 (11.2.0.2.0). The download file is `ojdbc6.jar`.

24. The `Mail Service Configuration` screen is displayed (Figure 34 on page 71). Go to Step 26.

Figure 34: Mail Service Configuration Screen

25. Enter the SMTP and e-mail parameters.
26. Click `Next`. The `Installation Progress` screen is displayed.
27. Click `Install`.

    The progress displays on the `Output` tab. Any errors display in the `Errors` tab.
28. If no errors display, dismiss the `Finished` popup. The `Output` tab displays the message `Build Successful` and the total time taken for the deployment.
29. If errors display, diagnose them in the `Errors` tab, or refer to "Troubleshooting Installation Errors" on page 72.
30. Install the Advisors windows service:
    a. Open a command prompt, and change directory first to your Advisors base directory (for example, `Program Files\GCTI\Advisors`), then to `bin\windows-x86`.
    b. Run `InstallAdvisorsServer.bat`.

End of procedure

Next Steps

- If you are running Platform with a 64-bit JVM, Genesys recommends that you increase your Geronimo PermGen memory settings.

Troubleshooting Installation Errors

The following are parameter validation errors that you may encounter at the end of installation:

Table 3: Installation Error Messages

Error Message	Cause
[echo] Setting up cluster member configuration for this node [java] Connecting to database: inf-wolf.us.int.genesyslab.com;oracle:1521;DatabaseName=orcl;user=yevgeny_plt_81 ... [java] updating node: KoolNode ipAddress: 138.120.xx.xx localhost: localhost [java] java.sql.SQLException: ORA-01013: user requested cancel of current operation [java] at oracle.jdbc.driver.Database Error.throwSqlException(DatabaseError.java:112) [java] at oracle.jdbc.driver.T4CTTIoer.process Error(T4CTTIoer.java:331) [java] at oracle.jdbc.driver.T4CTTIoer.process Error(T4CTTIoer.java:288) [java] at oracle.jdbc.driver.T4C8Oall.receive(T4C8Oall.java:745) [java] at oracle.jdbc.driver.T4CPreparedStatement. doOall8(T4CPreparedStatement.java:219) [java] at oracle.jdbc.driver.T4CPreparedStatement. executeForRows(T4CPreparedStatement.java:970) [java] at oracle.jdbc.driver.OracleStatement. doExecuteWithTimeout(OracleStatement.java:1190) [java] at oracle.jdbc.driver.OraclePreparedStatement. executeInternal(OraclePreparedStatement.java:3370) [java] at oracle.jdbc.driver.OraclePreparedStatement. executeUpdate(OraclePreparedStatement.java:3454) [java] at com.informiam.installer.DAO.executeTimedOutUpdate (DAO.java:214) [java] at com.informiam.installer.ConfigureClusterMember. performActivities(ConfigureClusterMember.java:60) [java] at com.informiam.installer.AbstractDatabaseUtility. doMain(AbstractDatabaseUtility.java:56) [java] at com.informiam.installer.ConfigureClusterMember. main(ConfigureClusterMember.java:34)	This type of error may happen when the installer attempts to update a table which is locked by a not-committed transaction (usually with Oracle database). The wording of the error may differ, but the key phrase to look for is "ORA-01013: user requested cancel of current operation". Typically this could happen with Oracle database when someone runs a query like DELETE FROM <TABLE_NAME> without then executing COMMIT; and the installer tries to update the same table. In this case, the installer will wait for 20 seconds and fail with an error similar to the above. To correct this, execute COMMIT; after the DELETE statement and re-run the installer. To prevent this situation, always run COMMIT; when manually updating tables in Oracle.
[java] Failed to connect to the database using connection URL: [java] jdbc:sqlserver://192.168.xx.yy:nnn;DatabaseName=ys_pldb;user=sa;password=very_secure_pwd;selectMethod=cursor [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnn has failed. Error: "Connection refused. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port.	Wrong database server name / IP address or port number

Table 3: Installation Error Messages (Continued)

Error Message	Cause
[java] Failed to connect to the database using connection URL: [java] jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=NotAPlatformDB;selectMethod=cursor;user=sa;password=very_secure_pwd [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnnn has failed. Error: "connect timed out. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port."	Wrong database name
[java] Exception while connecting: Login failed for user 'badUserId'. [java] url used: jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=ys_pldb;selectMethod=cursor;user=badUserId;password=very_secure_password	Wrong database user name or password
[echo] pinging cluster node IP address 138.120.yy.zz... [java] WARNING! Host 138.120.yy.zz is unknown - java.net.UnknownHostException: 138.120.yy.zz. This may be due to a firewall blocking requests or a specific server configuration, e.g.: permissions. [java] ERROR! Host 138.120.yy.zz is unknown - java.net.UnknownHostException: 138.120.yy.zz. This may be due to a firewall blocking requests or a specific server configuration, e.g.: permissions. [java] Exception in thread "main" java.security.InvalidParameterException: Host 138.120.yy.zz is unknown - java.net.UnknownHostException: 138.120.yy.zz. This may be due to a firewall blocking requests or a specific server configuration, e.g.: permissions.	The cluster member node identified by the IP address specified is not reachable. This may be for one of the following reasons: • The host is not online • A firewall is blocking access to the host • The IP address of the host is incorrect • The host is configured not to respond to ICMP ping requests

Table 3: Installation Error Messages (Continued)

Error Message	Cause
Apr 11, 2011 3:53:46 PM oracle.jdbc.driver.OracleDriver registerMBeans WARNING: Error while registering Oracle JDBC Diagnosability MBean. java.security.AccessControlException: access denied (javax.management.MBeanTrustPermission register) at java.security.AccessControlContext.checkPermission(Unknown Source) at java.lang.SecurityManager.checkPermission(Unknown Source) at com.sun.jmx.interceptor.DefaultMBeanServerInterceptor.checkMBeanTrustPermission(Unknown Source) at com.sun.jmx.interceptor.DefaultMBeanServerInterceptor.registerMBean(Unknown Source) at com.sun.jmx.mbeanserver.JmxMBeanServer.registerMBean(Unknown Source) at oracle.jdbc.driver.OracleDriver.registerMBeans(OracleDriver.java:360) at oracle.jdbc.driver.OracleDriver$1.run(OracleDriver.java:199) at java.security.AccessController.doPrivileged(Native Method) at oracle.jdbc.driver.OracleDriver.<clinit>(OracleDriver.java:195)	Produced in error and can be ignored. Displays in the Errors tab when installing Platform with Oracle JDBC driver ojdbc6-11.2.0.2.0, and accurately reports that installation was successful.
Exception in thread "AWT-EventQueue-0" java.lang.ArrayIndexOutOfBoundsException: 32 at sun.font.FontDesignMetrics.charsWidth(Unknown Source) at javax.swing.text.Utilities.getTabbedTextOffset(Unknown Source) at javax.swing.text.Utilities.getTabbedTextOffset(Unknown Source) at javax.swing.text.Utilities.getTabbedTextOffset(Unknown Source) at javax.swing.text.PlainView.viewToModel(Unknown Source) at javax.swing.text.FieldView.viewToModel(Unknown Source) at javax.swing.plaf.basic.BasicTextUI$RootView.viewToModel(Unknown Source) at javax.swing.plaf.basic.BasicTextUI.viewToModel(Unknown Source)	Produced in error and can be ignored.

Changing Memory Allocations

If the log is reporting an out of memory error, set the heap size higher by editing the <install dir>/conf'/advisors-server-wrapper.conf file. About a third down the file, change the following lines:

```
# Initial Java Heap Size (in MB)
wrapper.java.initmemory=128

# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=1024
```

to

```
# Initial Java Heap Size (in MB)
```

```
wrapper.java.initmemory=800

# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=1200
```

If the log is reporting a PermGen out of memory error, increase the permanent generation memory by editing the following line in the same file:

```
wrapper.java.additional.13=-XX:MaxPermSize=128m
```

to

```
wrapper.java.additional.13=-XX:MaxPermSize=256m
```

This increase in PermGen memory is normally required only when Platform uses a 64-bit JVM. The most memory you can allocate to `wrapper.java.maxmemory` under 32-bit windows is 1600MB but with 64-bit Windows much larger values can be used.

If the problem persists, experiment with higher values; however, the service may fail to start if it is unable to allocate all of the memory requested from the operating system. This will be noticeable if the server fails to start (reports an error during start). Turn various log settings to DEBUG in the conf file to help diagnose problems.

Configuring Access to External Websites

If you want access external websites via the Genesys Browser, you need to add an extra entry in the `MODULE` tables in the Platform database.

Below is a sample `INSERT` statement:

```
insert into Module (NAME,APP_DEPLOY_URL, VISIBLE,
CODE,HELP_URL,MODULE_VERSION ,  ISEXTERNAL) values ('APEX',
'http://www.informiam.com', 'Y', 'APX', '','','Y')
```

Changing the Mail Server Configuration After Server Installation

Procedure: Changing the Mail Server configuration after Platform server is installed

Start of procedure

1. In the `conf` directory, locate the `MailService.properties`.
2. Edit the settings.
3. For the new settings to take effect, restart the server.

End of procedure

Changing Encrypted Passwords After Installation

The passwords provided during installation are encrypted. The Advisors password encryption utility can be used to change passwords after installation.

Procedure: Changing an encrypted password

Start of procedure

1. Open the `Command` prompt and navigate to the `..\GCTI\Advisors\bin` directory.
2. Run the command `encrypt-password`.
3. When prompted, enter the new password and press `Enter`.
4. Copy the resulted encrypted password and replace the old password in the configuration file.

End of procedure

Adding a Text Message on the Login Page

To add a message on the `Login` page, you must have administrative privileges on the machine where the Web components of Genesys Advisors offering reside. Once logged in, locate the `baseweb\custom\browser` directory in the Advisors installation. Modify the `remote-message.txt` file using a text editor.

Customizing the Logo and Colors in the Advisors Browser

You can change the logo and background on the Advisors Browser to display your company's logo and background. The dimensions of the new logo must be the same as the dimensions of the Genesys logo (maximum `210*52` pixels).

Procedure: Customizing the logo

Start of procedure

1. In the `deploy` directory, navigate to the folder: `C:\informiam\custom\browser`.
2. Replace the existing logo file with the custom logo. The logo filename must be `remote-logo.png`. The logo file should have the same dimensions as `/chrome/skin/ea/ent-images/logo.png` (210 x 52 pixels)
3. Replace the existing background file with the custom background. The background filename must be `remote-background.jpg`. The background file should have the same dimensions as `/chrome/skin/ea/ent-images/login-bkgnd.jpg`.
4. Change `informiam.js` and `skin.js` under the `Apache Server` directory to:

```
informiamCustom =
{ mainColor: '#0288D7',
secondaryColor: '#59B1E4',
thirdColor: '#BDE7FF',
accentColor: '#024B7D',
textColor: '#023E67',
```

End of procedure

Customizing the Colors for Alert Management

```
toolBarColor: '#6893cc',
```

```
borderColor: '#3b5984',
backGroundColor: '#d2e3f8' };
```

All properties from the skin object must be propagated out to Contact Center Advisor and Workforce Advisor.

```
setMainColor(informiamCustom.mainColor);
setSecondaryColor(informiamCustom.secondaryColor);
setThirdColor(informiamCustom.thirdColor);
setAccentColor(informiamCustom.accentColor);
setTextColor(informiamCustom.textColor);

setToolBarColor(informiamCustom.toolBarColor);
setBorderColor(informiamCustom.borderColor);
setBackGroundColor(informiamCustom.backGroundColor);
```

Deploying and Configuring Apache

Procedure: Deploying and configuring Apache

Purpose: To install an Apache Web Server 2.2+ instance to direct http requests to the appropriate server. It is recommended to install Apache Web Server on a separate box.

Start of procedure

1. To enable Apache Web Server serving different modules in the Advisors Browser (for example, Administration, Contact Center Advisor, Workforce Advisor), edit the `httpd.conf` file located in the `conf` folder of the Apache Web Server installation as outlined below.
   a. Locate the following lines in the `httpd.conf` file:
   - `#LoadModule headers_module modules/mod_headers.so`
   - `#LoadModule proxy_module modules/mod_proxy.so`
   - `#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so`
   - `#LoadModule proxy_http_module modules/mod_proxy_http.so`

   b. Remove the hash mark (`#`) from the beginning of each line, so that these four lines appear like this:
   - `LoadModule headers_module modules/mod_headers.so`
   - `LoadModule proxy_module modules/mod_proxy.so`
   - `LoadModule proxy_ajp_module modules/mod_proxy_ajp.so`
   - `LoadModule proxy_http_module modules/mod_proxy_http.so`

c. Locate the following entry and add a `#` to comment out `Deny` from all and to add `Allow` from all:

```
<Directory />
 Options FollowSymLinks
 AllowOverride None
 Order deny,allow
 #Deny from all
 Allow from all
 Satisfy all
</Directory>
```

d. Locate the following entry near line 133 and add a `#` to comment it out:

```
#ServerAdmin
```

e. Add the following line:

```
ProxyRequests off
```

f. Add the following lines to the bottom of the file and change the IP addresses as necessary:

```
# Platform and Advisors Modules
ProxyPass /am/ ajp://192.168.40.234:8009/am/
ProxyPass /admin/ ajp://192.168.40.234:8009/admin/
ProxyPass /am-admin/ ajp://192.168.40.234:8009/am-admin/
ProxyPass /ca/ ajp://192.168.40.234:8009/ca/
ProxyPass /ca-ws/ ajp://192.168.40.234:8009/ca-ws/
ProxyPass /ea-ws/ ajp://192.168.40.234:8009/ea-ws/
ProxyPass /dashboard/ ajp://192.168.40.234:8009/dashboard/
ProxyPass /nav-service/ ajp://192.168.40.234:8009/nav-service/
ProxyPass /prefs-service/
ajp://192.168.40.234:8009/prefs-service/
ProxyPass /wu/ ajp://192.168.40.235:8009/wu/

# Genesys Resource Management Console Web Application
ProxyPass /rmc/ ajp://192.168.40.235:8009/rmc/

# Genesys Adapter Admin Web Application
ProxyPass /gc-admin/ ajp://192.168.40.235:8009/gc-admin/

# FA
ProxyPass /fa/ ajp://192.168.40.234:8009/fa/

## Note that a second copy of Apache must go on the XMLGen
server and serve /ca-xml/ "locally"
```

```
ProxyPass /ca-xml/ http://192.168.40.234/ca-xml/
```

Note: If you need to access external applications via the Genesys Browser should have lines for each of those applications.

For example:

```
ProxyPass /APEX/
http://www.cra-arc.gc.ca/formspubs/menu-eng.html
```

You can comment out or exclude lines to proxy passes that are not installed.

Note: The trailing slash must appear at the end of the line. If it is omitted, users might see `404` or `Not Found` error, or simply get no response when clicking, or see empty white screens in the Advisor browser. Errors can typically be seen in the Geronimo log if DEBUG is enabled.

The solution is to fix the `httpd.conf` and restart Apache.

Example:

`ProxyPass /gc-admin/ ajp://server:8009/gc-admin` would generate an error.

2. Copy the contents of the `baseweb-<version>-static-web.zip` from the Advisors Platform distribution (the directories within the `static-web-content`) into the Apache `htdocs` directory.
3. Install another instance of Apache Web Server 2.2+ onto the same box where the CCAdv application server and XMLGen have been installed. This instance of Apache Web Server will be used to serve XML content produced by XMLGen.
   a. Locate the following entry in the `httpd.conf` and add a `#` to comment out `Deny from all`, and add `Allow from all`:

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Order deny,allow
    #Deny from all
    Allow from all
    Satisfy all
</Directory>
```

   b. Locate the following entry near line 133 and add a `#` to comment it out:

```
#ServerAdmin
```

   c. Locate the following line and remove the `#` from the beginning of the line:

```
#LoadModule headers_module modules/mod_headers.so
```

so that this line appears like this:

```
LoadModule headers_module modules/mod_headers.so
```

d. Point the Apache Web Server to the XMLGen output directory provided in Section 'XMLGen Services Option' above. Add the following line to the end of `httpd.conf` file:

```
Alias /ca-xml/ "D:/Program Files/genesys/ca-xml/"
```

Note: The directory `D:/Program Files/genesys/ca-xml/` is an example. This directory must be exactly the same as provided during XMLGen installation.

e. Add the following lines to the bottom of the file:

```
<Location /ca-xml/>
   Header add "Cache-control" "no-cache"
   Header add "Pragma" "no-cache"
   Header add "Expires" "Thu, 01 Jan 1970 00:00:00 GMT"
</Location>
```

End of procedure

Using a Second Instance of Apache

In some cases, more than one instance of Apache httpd is deployed for a single Advisor system. In environments where no application software can deployed on Web servers, or in cases where it is better to have a Web server with no instance of Geronimo on it, two instances of Apache will be required.

One instance of Apache must always be installed on the server running XML Gen in order to serve the XML files to the Dashboard client. That instance will have a line like this in the `httpd.conf` file:

```
Alias /ca-xml/ "D:/Program Files/GCTI/Advisors/ca-xml/
```

With this configuration, any time a file beginning with `/ca-xml/` is requested from this Apache instance, the files are served directly from the Advisors `ca-xml` directory where XMLGen writes them. If a second copy of Apache is needed on another server that will handle all the Advisor traffic, a line needs to exist that looks similar to this:

```
ProxyPass /ca-xml/ http://servername/ca-xml/
```

With this configuration, when clients request XML files (starting with `/ca-xml/`), those requests are reverse-proxied to the instance of Apache running on the XMLGen server. This ensures that Geronimo is not used to

serve static files, because that will tend to use application server threads unnecessarily and inefficiently.

Configuring Apache to Support HTTPS

To configure Apache to support HTTPS you must:

1. Generate the SSL security certificate and private key.
2. Reconfigure Apache.

Procedure: Generating the SSL security certificate and private key

Start of procedure

1. If not already installed, download and install the C++ redistributables frames official Microsoft downloads site.I
2. If not already installed, download and install OpenSSL from an official SSL download site.
3. Add the OpenSSL bin directory (by default `C:\OpenSSL-Win32\bin`) to your Windows PATH.
4. From the `Start` menu, enter `Run > mmc`.
5. From the `File` menu select `Add/Remove Snap-In`.
6. Execute the following: `Add > Certificates > Add > Computer Account > Local Computer`
7. Expand `Console Root > Certificates > Personal > Certificates.`
8. Right-click `> All Tasks> Export.`
9. Select `Yes` to export the private key.
10. Deselect `Enable strong protection`.
11. Extract the certificate and key using the following command from the directory where the certificate was exported:

    ```
    openssl pkcs12 -in inf-koi.pfx -out inf-koi.crt -nodes
    ```

End of procedure

Procedure:
Reconfiguring Apache to support HTTPS

Start of procedure

1. Copy the certificate/key (`inf-koy.crt`) to the Apache `conf` directory (by default `C:\Program Files\Apache Software Foundation\Apache2.2\conf`).
2. Edit `{Apache conf}\httpd.conf`.
3. Uncomment `LoadModule ssl_module modules/mod_ssl.so` (line 120).
4. Uncomment `Include conf/extra/httpd-ssl.conf` (line 474).
5. Comment out `Listen 80` (line 46).
6. Edit `{Apache conf}\extra\httpd-ssl.conf` and point `SSLCertificateFile` and `SSLCertificateKeyFile` to the certificate.
7. Restart Apache.
8. Verify the configuration by browsing to `https://inf-koi`. This will require accepting a certificate warning unless the client has added the server's certificate.

End of procedure

Latency Getting to the Login page

Consider raising the `ThreadsPerChild` setting to `1024` if Apache log files on the Web server show:

- `[warn] Server ran out of threads to serve requests.` Consider raising the `ThreadsPerChild` setting
- `[notice] Child 5068: All worker threads have exited.`
- `[notice] Child 5068: Child process is exiting`

Chapter

7 Deploying Genesys Adapter

This chapter describes how to install and configure the Genesys Adapter. It contains the following sections:

- Prerequisites, page 85
- Installation Overview, page 86
- Deploying Genesys Adapter Manually, page 88
- Deploying the Adapter Core Service Component, page 89
- Modifying the XMLGen Configuration, page 104
- Deploying the SDS Service, page 105
- Deploying Resource Management Console, page 114
- Deploying Multiple Instances of the Genesys Adapter Core Service on a Single Server, page 116
- Troubleshooting Installation Errors, page 118

Prerequisites

See “Deployment Prerequisites” on page 15.

Before deploying Genesys Adapter, you must have created a Genesys Adapter database. To do this, please see either:

- Chapter 2, “Creating a SQL Server Database,” on page 23, or;
- Chapter 3, “Creating an Oracle Database,” on page 37.

A verified Genesys environment must be ready and available. Credentials with read access to the HDS and AW databases must be available when the Advisors Genesys Adapter Installer is run.

Installation Overview

Introduction

There are two parts to the Genesys Adapter:

- A server component.
  The server component is the main engine of the Genesys Adapter.

Dependencies and Issues

Dependencies

- Use Apache Server 2.2.6 or later. If the Apache server is installed on the same machine as Geronimo, it must use a port other than 8080, such as 80.
- If the T-Server is the Avaya Communication Manager, make sure that the T-Server option `query-agent-work-mode` is set to `on-restart`. This is the default option. To set this option, go to `TServer`, then `Option Tab`, then `T-Server Option` and locate `query-agent-work-mode`. This setting is required for the `AfterCallWork` state changes to be visible.
- Genesys Adapter 8.x requires Genesys Statistics Server 8.0.000.40 and the MCR extension package.

Procedure: Deploying Stat Server and MCR extensions

Start of procedure

1. Install Stat Server 8.0.000.40.
2. Install the MCR extension package. The MCR version corresponding to the most recent GA Stat server version can be obtained from the Genesys installation CD image.
3. Configure the JVM path options for the Stat Server in Configuration Manager.
   a. Right-click on the Stat Server `Application` object.
   b. Select `Wizard`, then `Configure`, then `Java Options`.
   c. Check the `Load Java at startup` checkbox.
   d. Set the JVM Path to the `jvm.dll` file (for example: `C:\Program Files\Java\jre6\bin\client\jvm.dll`).
   e. Set the `ext` directory to the relative path of the extensions directory under the Stat Server installation (the default is `./java/ext`).

   f. Set the `lib` directory to the relative path of the library directory under the Stat Server installation (the default is `./java/lib`).

   g. Select the `eServiceContactStat.jar` and `eServiceInteractionStat.jar` Java Extension jars to be loaded.

   h. Click `OK` to close the `Wizard properties` popup.

4. Ensure that the Stat Server has a connection to the Interaction Server. Double-click the Stat Server application, and add this connection on the `Connections` tab if it is not already present.
5. Under the Stat Server application `Options` tab, create a new section named `common`. Set the value of option `rebind-delay` to `0` (zero).
6. Ensure that the corresponding connection from the Interaction Server back to the Stat Server is also present. Double-click the `Interaction Server Application`, and add the connection on the `Connections` tab if it is not already present.
7. Restart both the Interaction Server and the Stat Server.

End of procedure

Issues

- There are no filters included with the installation of AGA. Configure the required filters through the Configuration Manager on the `Options` tab of the Stat Server(s) that the Adapter is going to use. a sample format for these filters is:

  Name: `Informiam.Regular`

  Value: `PairExists("AppCallType", "Reg")`

  Filters are only required if the customer's Genesys routing uses them, in which case all filters must be present in each Stat Server connected to the AGA. AGA only loads filters that appear on all of its associated Stat Servers.

  If there are any changes made to the filters stored in Configuration Server, after starting AGA, those changes will not be reflected until the next overnight full re-issue of statistics.
- Before Genesys Adapter will report metrics back to Contact Center Advisor, objects must be selected. Refer to the procedure “Editing the associations” in the *Performance Management Advisors 8.1 Contact Center Advisor & Workforce Advisor Administrator User’s Guide*, which can be accessed via the Help button at the top right of the screen within the `Administration` tab of the application.

Support for LoggedIn Scripts

In releases prior to 8.0, the Genesys Adapter was aware of the virtual agent group (VAG) membership only when the VAG script was based on agent skills—for example, skills-based VAGs. In this case, the Configuration Server is aware of the agents who are part of the virtual agent group, and the Genesys Adapter obtains this membership information from the Configuration Server.

In release 8.x, the Adapter has been enhanced so that agent group membership information for VAGs that are defined using the `LoggedIn` script is retrieved from the Stat Server, rather than from the Configuration Server.

Deploying Genesys Adapter Manually

This section describes manual installation steps for Genesys Adapter.

Procedure: Deploying Genesys Adapter manually

Prerequisites

- See "Deployment Prerequisites" on page 15.

Start of procedure

1. Verify the Genesys environment.

   Verify that a Genesys Platform environment is ready and available. This includes (but is not limited to) Configuration Server, Stat Server, and the T-Server(s) and/or Interaction Servers. All of these services must be running prior to deploying the Genesys Adapter.

   Genesys Adapter 8.x requires Genesys Statistics Server 8.0, as well as some extensions. See "Deploying the Adapter Core Service Component" on page 89.

2. Create the Genesys Adapter database. See either:
   - Chapter 2, "Creating a SQL Server Database," on page 23, or;
   - Chapter 3, "Creating an Oracle 11g Database," on page 37.
3. Locate the build files. Unzip the files into a temporary directory. The following files should be present:
   - MS SQL
     - `aga-installer-<version>.jar`
     - `gc_core_newdb_<current version>.sql`
     - `gc_core_migrate_<starting version>_<current version #>.sql`
     - `gc_metrics_newdb_<current version>.sql`

    - GeneratePermsStatements.sql
  - Oracle
    - gc_cfg_new_DDL_<version>.sql
    - gc_cfg_new_Schema_<version>.sql
    - gc_cfg_new_TBS_<version>.sql
    - gc_metrics_new_DDL_<version>.sql
    - gc_metrics_new_Schema_<version>.sql
    - gc_metrics_new_TBS_<version>.sql

4. If you intend to deploy the Genesys Adapter administration module or Resource Management module on a server other than your CCAdv/WA server, install an instance of the Platform Service on that server (see Chapter 6, "Deploying Advisors Platform," on page 55).

   Continue with this installation process after an instance of Platform is installed.
5. Install the Genesys Adapter Core Service. See "Deploying the Adapter Core Service Component" on page 89
6. Optionally configure XMLGen. See "Modifying the XMLGen Configuration" on page 104.
7. Optionally, install the Resource Management Console (RMC) module. See "Deploying Resource Management Console" on page 114. If you install RMC, you must install SDS also.
8. If you have installed RMC, install the SDS service on a separate server from Genesys Adapter and the Resource Management module. See "Deploying the SDS Service" on page 105.

End of procedure

Deploying the Adapter Core Service Component

Procedure: Deploying the Core Service component

Start of procedure

1. Run the installation jar file by either;
   - Using the command `java -jar aga-installer-<version>.jar;` or,

- Double-clicking the `aga-installer-<version>.jar` in the release bundle.

Notes: 1. Double-click does not work if only JDK is installed (that is, JRE is not present).

2. For 64-bit systems, if double-clicking to launch the installer, please ensure that the Java instance associated with the `jar` file type is 64-bit. Running the installer with a 32-bit Java instance will create a Windows service with the wrong executable.

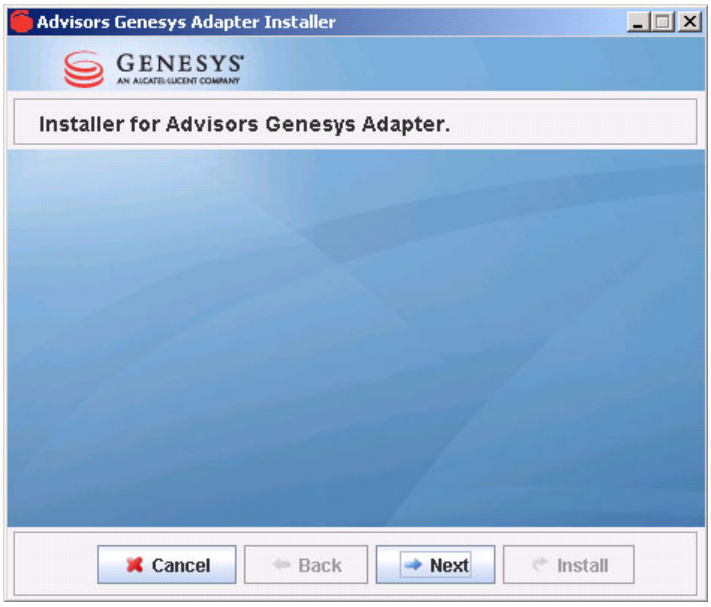


Figure 35: Installer for Genesys Adapter

2. Click `Next`.The `Install Type` screen displays (Figure 36 on page 91).

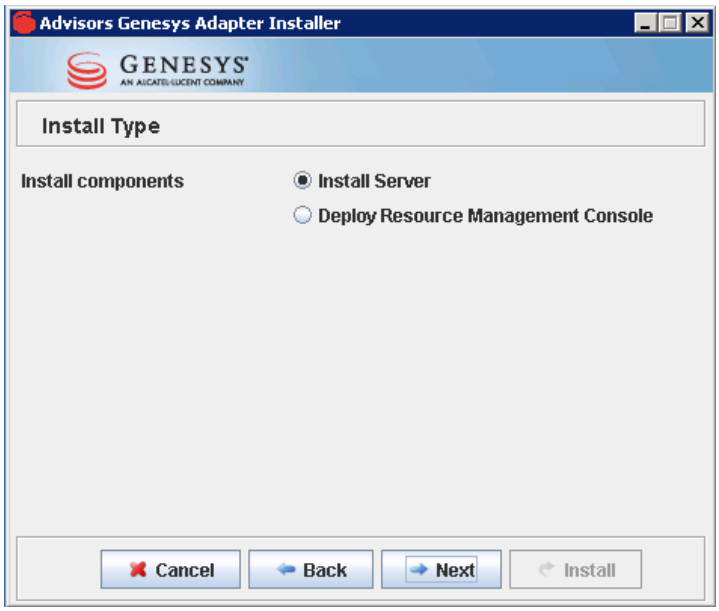


Figure 36: Install Type

3. To install the server, click `Install Server` and click `Next`. The `Server Install Type` screen displays.

   If deploying the Resource Management Console, go to "Deploying Resource Management Console" on page 114.

> `Note:` You can only install a single component (either the core service, or RMC) during a single installer run.

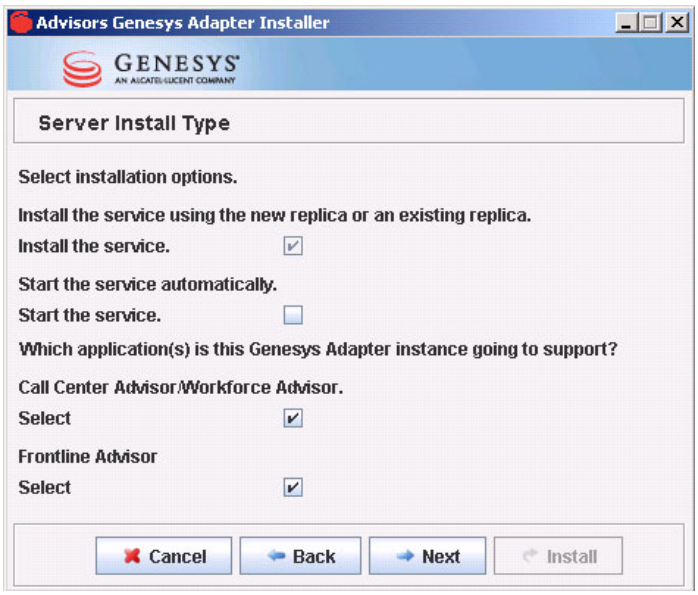


Figure 37: Server Install Type

4. Select whether you want this Adapter instance to serve Contact Center Advisor/Workforce Advisor (CCAdv/WA), Frontline Advisor (FA), or both. Serving both FA and CCAdv/WA is not recommended for performance reasons.
5. Click `Next`. The `Installation Details` screen displays.

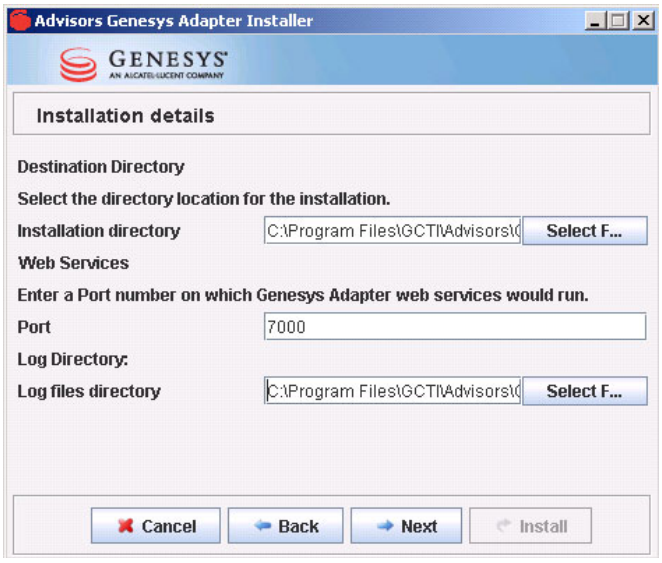


Figure 38: Installation Details

6. Specify the installation directory. The default installation directory is `C:\Program Files\GCTI\Advisors\Genesys\Adapter`.
7. Enter the port number that the Genesys Adapter web services will run on. You can use the default port, `7000`, if no other application is using that port.
8. Specify the directory in which the log files will appear.
9. Click `Next`. `The Java Development Kit` screen is displayed (Figure 39 on page 93).

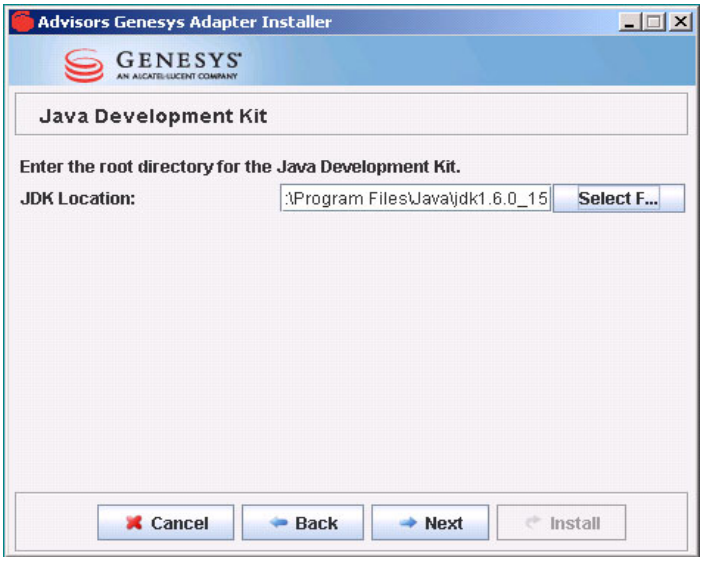


Figure 39: Java Development Kit Screen

10. Add the location of the root directory of the Java installation. Click `Next`. The `Database Type` screen displays.

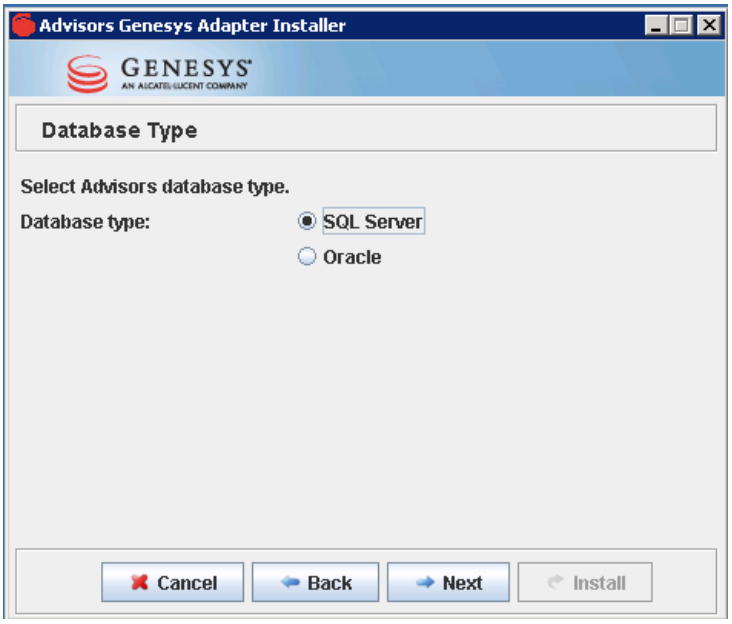


Figure 40: Database Type Screen

11. Select the relevant database type and click `Next`. For Oracle only, go to Step 12. Otherwise go to Step 13.
12. Locate the Oracle JDBC driver. Click `Next`.

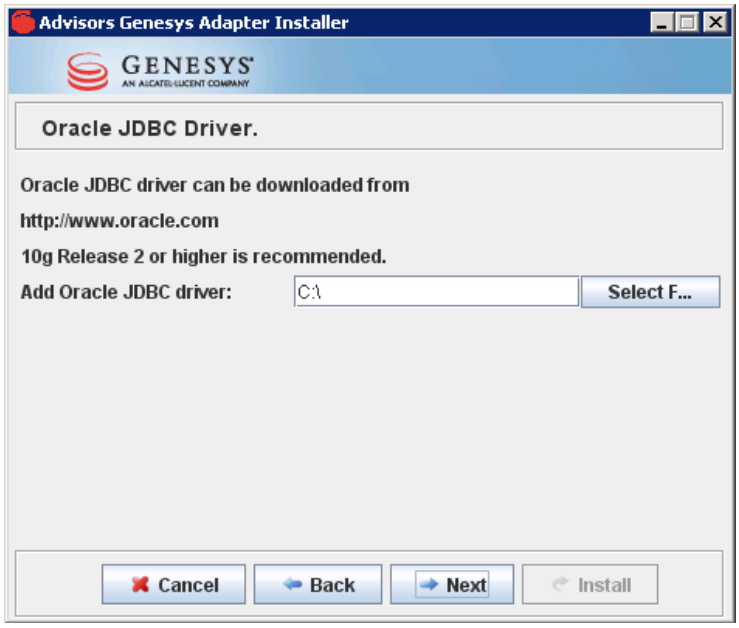


Figure 41: Oracle JDBC Driver Screen

Note: The following Oracle JDBC drivers can be used:

- Oracle database 10g release 2 (10.2.0.4). The download file is `ojdbc14.jar`.
- Oracle database 11g release 2 (11.2.0.2.0). The download file is `ojdbc6.jar`.

13. If this Adapter instance supports Contact Center Advisor (CCAdv), the CCAdv/WA Metrics Database Configuration screen displays.

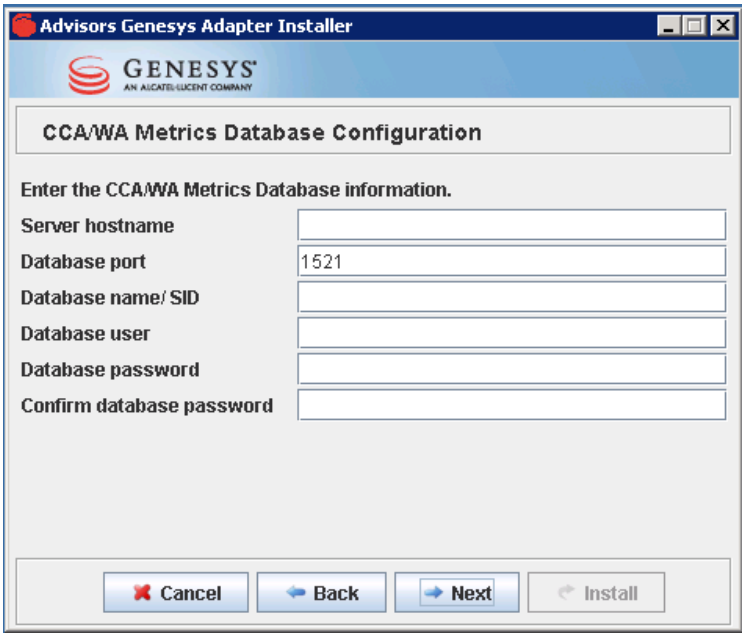


Figure 42: CCAdv/WA Metrics Database Configuration

14. Enter the host name or IP address of the machine where the CCAdv/WA metrics database is installed.

    Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

15. Enter the database name—for example, `advisors_gametricsdb`.
16. Enter the user name and password of a user that will be used by the Adapter to access the database.

    Note: The CCAdv/WA Metrics Database password is encrypted and saved in the `...\GCTI\Advisors\Genesys\Adapter\conf\inf_genesys_importer.properties` file by default. To change the password see "Changing Encrypted Passwords After Installation" on page 76.

17. Click `Next`. If this Adapter instance supports Frontline Advisor, the `FA Database Configuration` screen displays.

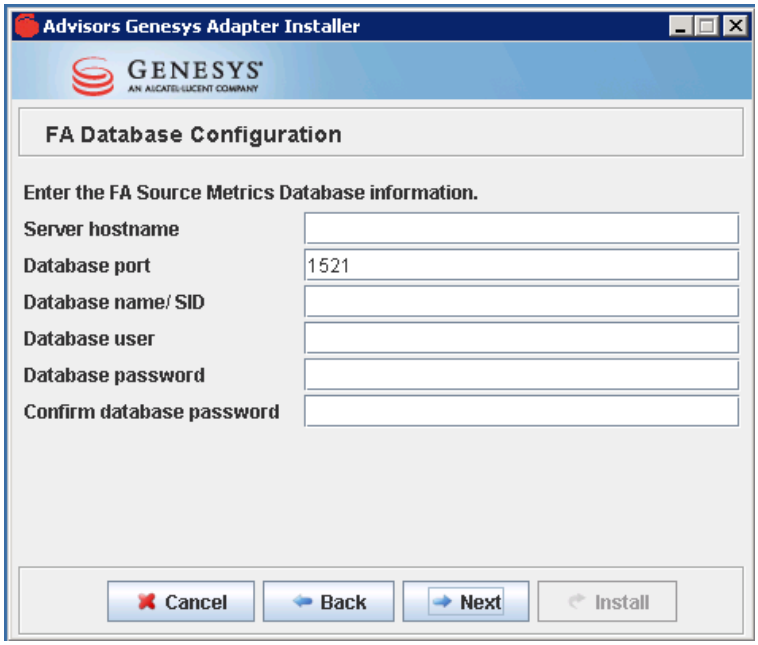


Figure 43: FA Database Configuration

18. Enter the host name or IP address of the machine where the FA Source Metrics database is installed.

> Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

19. Enter the database name.
20. Enter the user name and password of a user that will be used by the connector to access the database.

> Note: The FA Database password is encrypted and saved in the `...\GCTI\Advisors\Genesys\Adapter\conf\inf_genesys_importer.properties` file by default. To change the password see "Changing Encrypted Passwords After Installation" on page 76.

21. Click `Next`. The `Advisors Genesys Adapter Database Configuration` screen is displayed (Figure 44 on page 97).

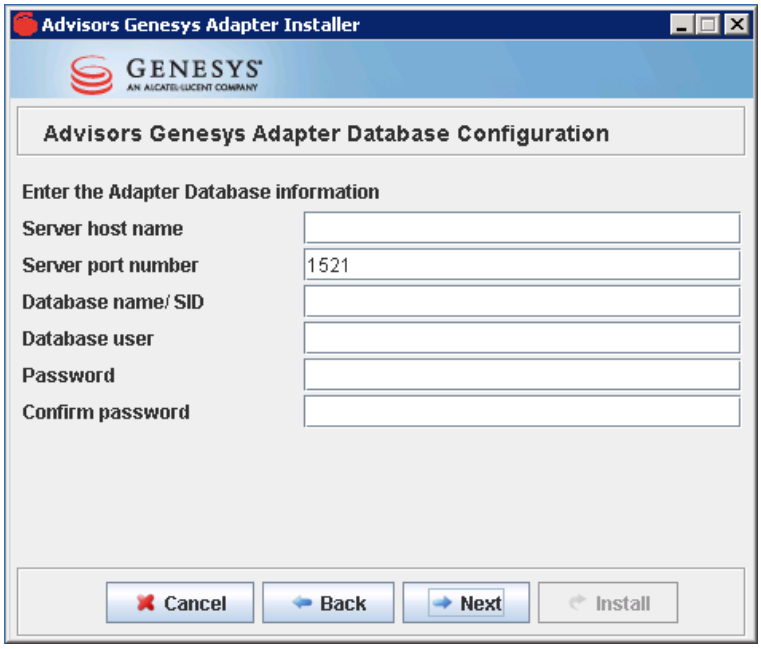


Figure 44: Adapter Database Configuration Screen

22. Enter the host name or IP address of the machine where the Genesys Adapter database is installed, along with the port number and database name.

    Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

23. Enter the user name and password for the user that will be used by the Adapter to access the Genesys Adapter database. This should match the user created earlier.

    Note: The Genesys Adapter Database password is encrypted and saved in the `...\GCTI\Advisors\Genesys\Adapter\conf\inf_genesys_importer.properties` file by default. To change the password see "Changing Encrypted Passwords After Installation" on page 76.

24. Click `Next`. The `Genesys Data Source Configuration` screen displays (see Figure 45 on page 98).

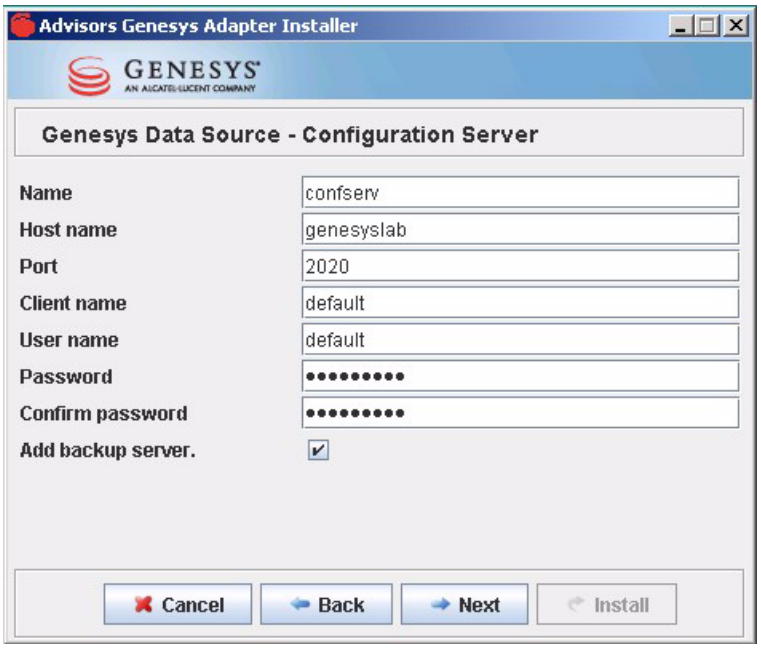


Figure 45: Genesys Data Source—Primary Configuration Server

25. Enter the information required for connecting to the primary (mandatory) Configuration Server in the Genesys environment.
    - `Name`—The name of the primary configuration server. The name is obtained from the Configuration Manager (CM) and is case sensitive.
    - `Host Name`—The name or IP address of the machine hosting the Configuration Server.

    Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

    - `Port`—The port that the configuration server is listening on.
    - `Client Name`—Enter the login credentials of the user account assigned for use by the Genesys Adapter to access the Configuration Server.
    - `User name`—The user name of the account the Adapter will use to connect to the Configuration Server.
    - `Password`—The password of the account the Adapter will use to connect to the Configuration Server.

    Note: The Genesys Configuration Server password is encrypted and saved in the `..\GCTI\Advisors\conf\GenesysConfig.properties` file by default. To change the password see “Changing Encrypted Passwords After Installation” on page 76.

- `Add backup server`—Optionally, select this checkbox to add and configure a backup Configuration Server.

> **Note:** The backup Configuration Server can be, but does not need to be, configured in a high-availability pair in Genesys.

26. Click `Next`. If you opted to configure a backup Configuration Server, the configuration screen for the backup now displays.

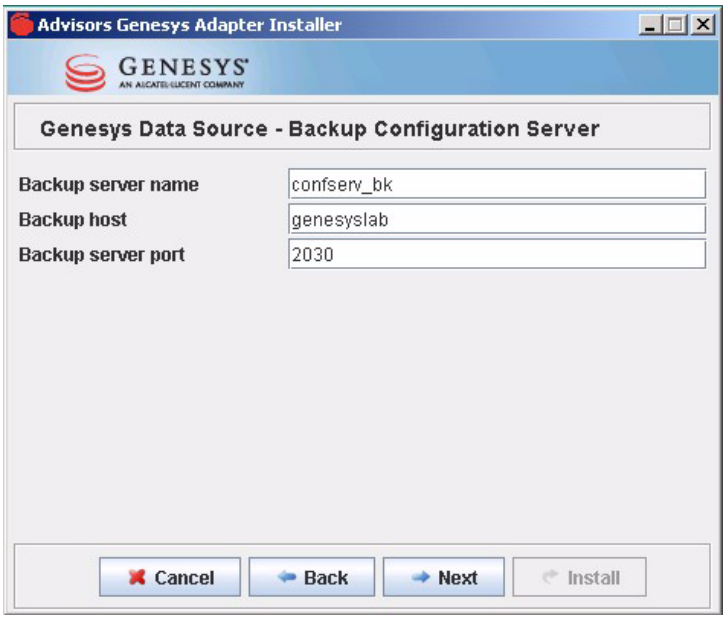


Figure 46: Genesys Data Source—Backup Configuration Server

27. Enter the information required for connecting to the backup Configuration Server in the Genesys environment.

- `Backup server name`—The name of the backup configuration server. The name is obtained from the Configuration Manager (CM) and is case sensitive.
- `Backup host`—The name or IP address of the machine hosting the backup Configuration Server.

> **Note:** When using numerical IPv6 addresses, please enclose the literal in brackets.

- `Backup server port`—The port that the backup Configuration Server is listening on.

28. Click `Next`. The Genesys Data Source Stat Server screen displays.

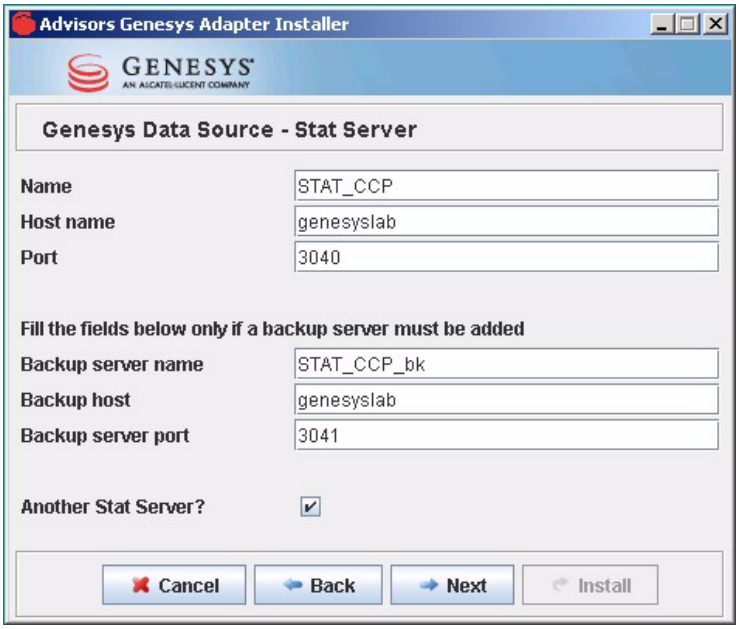


Figure 47: Genesys Data Source—Stat Server Configuration

29. Enter the information required for connecting to the first (mandatory) Stat Server in the Genesys environment.

For the first Stat Server:

- `Name`—The name of the Stat Server server. The name is obtained from the Configuration Manager and is case sensitive.
- `Host Name`—The name or IP address of the machine hosting the Stat Server.

Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

- `Port`— The port that the Stat Server is listening on.

Optionally, specify the backup server parameters for the first Stat Server:

- `Backup server name`—Name of the backup Stat Server. This is obtained from the Configuration Manager.
- `Backup host`—Name or IP address of the machine hosting the backup Stat Server.

Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

- `Backup server port`—The port on which the backup Stat Server listens.

To configure a second or subsequent Stat Server (or Stat Server pair), check the `Another Stat Server?` check box. Repeat this step for each Stat Server (pair) you want to add.

`Note:` Up to four additional Stat Server pairs can optionally be configured—that is, a total of 10 Stat Servers can be configured.

---

30. Click `Next`.

The `Periodic Statistics Reissue Scheduling` screen is displayed (Figure 48 on page 101).

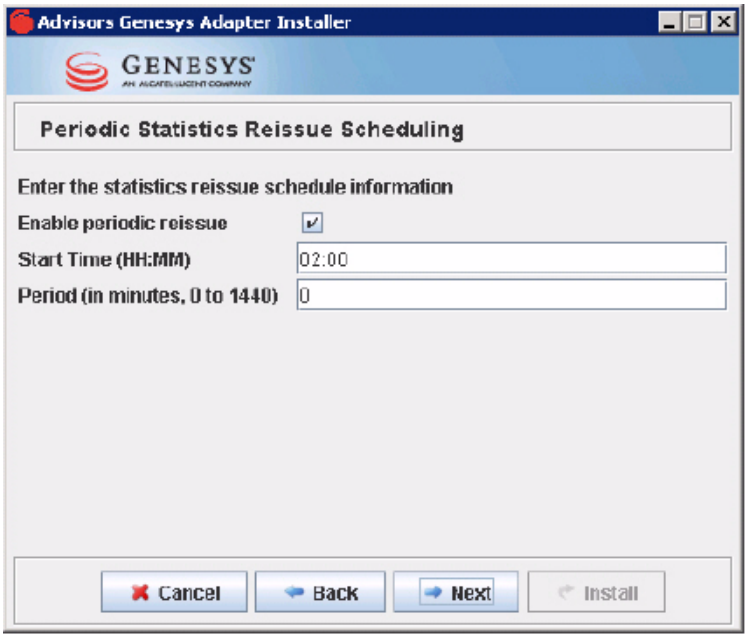


Figure 48: Periodic Statistics Reissue Scheduling Screen

31. If you want the Genesys Adapter to periodically reissue the Genesys statistics from the Genesys Configuration Server, check the `Enable` checkbox, then enter the 24-hour start time and period for the reissue schedule.

`Notes:`
1. Periodic reissue will not occur until after the initial reissue has been performed at the selected start time.
2. If the start time has already passed at the time of Genesys Adapter startup, the initial reissue will occur on the following day.
3. A period of `0` (zero) results in a period of `1440` minutes. Both values result in a once-per-day reissue.
4. The scheduling for overnight reissue of statistics does not take into account any local Daylight savings time changes.
   After the initial scheduling, even if the server local time is adjusted for Daylight savings, the reissue of statistics will continue to take place at the unadjusted time.
   If the Genesys Adapter is restarted after the Daylight time saving is executed, the reissue of statistics will resume at the scheduled time.

---

32. Click `Next`.

    If installing the server, the `Installation Progress` screen displays (Figure 49 on page 102)

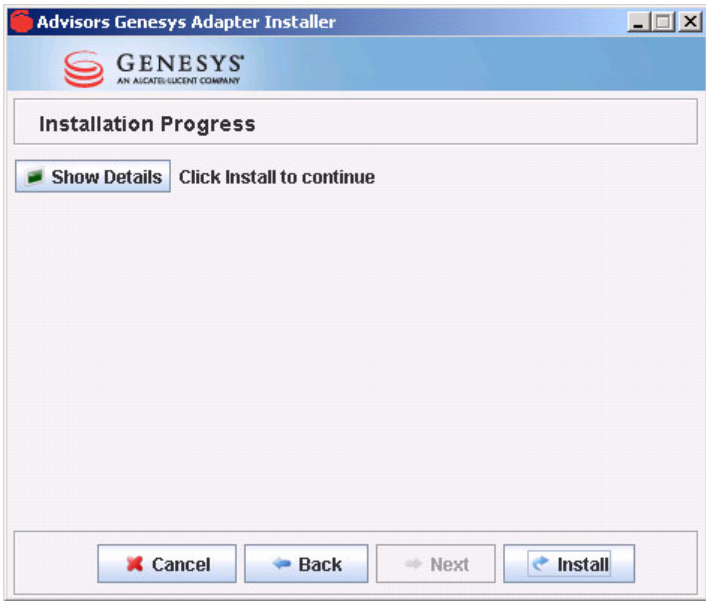


Figure 49: Installation Progress

33. Click `Show Details` then click `Install` and verify that there are no errors during installation.

34. For every Stat Server that you specified above (primary and backup), open the Stat Server configuration through the Configuration Manager and import the Advisor metrics on the `Options` tab. The metrics are stored in a file named `StatServerEntries.cfg`, and the file is located in `C:\Program Files\GCTI\advisors\Genesys\Adapter\CONF` (or wherever you selected to install the Genesys Adapter).

    This configuration file also contains settings for the Stat Server logging. The location of the log file can be changed by changing the following options in the Stat Server `Options` tab under the `Log` section:

    ```
    all=statserver.log
    standard=statserver.log
    ```

End of procedure

Operation of Stat Server Redundant Pairs

Genesys Adapter maintains connections to both the primary and the backup Stat Servers as long as they are available, but also requests the historical statistics from both the Stat Servers of the pair at the same time.

So, when connection to the primary is lost, Genesys Adapter switches over transparently to receiving Stat Server updates from the backup Stat Server. The historical counts therefore remain the same even after the switchover.

After the first switchover, the configured backup Stat Server is now treated as the new primary Stat Server, but when the old primary server comes back online, no automatic switchover takes place. Instead, all the historical statistics are now requested from the old primary Stat Server.

Because this Stat Server has just come back online, it needs to be given sufficient time to accumulate historical aggregated statistic counts. Because in CCAdv, one-day metrics are used, there should be at least a day before the next switchover happens. If the switchover happens sooner, then those statistic values would be shown as aggregated from the time when the Stat Server came back online.

Modifying the XMLGen Configuration

Procedure: Modifying the XMLGen Configuration

Start of procedure

1. After installation of XMLGen, there should be a row in the Platform database in the `ICM_DATABASE` table corresponding to the CCAdv/WA Metrics database created in the previous steps. If not, add this row. This row is needed to ensure that XMLGen works properly with the metrics database.
2. Once the row is inserted, or if there is already an existing row for the metrics database, then update the source column for that row to read `GENESYS` (all upper-case) by executing the following command:

   ```
   UPDATE <ccawa_dbname>.<schema_name>.ICM_DATABASE SET
   SOURCE_NAME='GENESYS' WHERE LINKED_SERVER_NAME IN
   ('<metrics_db_1>','<metrics_db_2.>'..,'<metrics_db_n>')
   ```

   Note: `(<metrics_db_1>,<metrics_db_2...,<metrics_db_n>)` - is a list of Metrics database destinations for the Genesys Adapter.

   The ICM database should then look like Figure 50 on page 104.

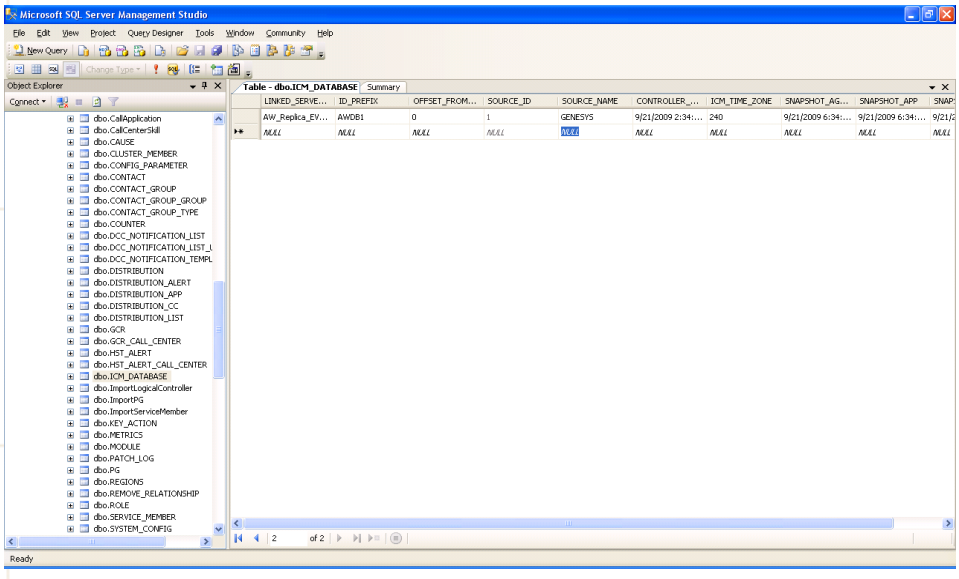


Figure 50: ICM_DATABASE Screen

End of procedure

Deploying the SDS Service

Note: SDS requires a 32-bit Java installation (JVM). SDS will run on a 64-bit operating system, including both Win2K8 and Win2K3 Server —but attempting to run the SDS startup executable against a 64-bit Java causes it to immediately shut down. SDS can be started and run from its batch file using 64-bit Java, but this requires a session to be always open on its server and is therefore not recommended. Java 32-bit can be run on 64-bit Windows operating systems.

Procedure: Deploying the SDS service

Start of procedure

1. If an older version of SDS is already installed, uninstall it:
   a. Shut down the SDS service.
   b. In a command prompt, navigate to the `bin` subdirectory for the SDS installation.
   c. Run `service.bat uninstall SupervisorDesktopService`.
   d. Delete all files and subdirectories in the root SDS directory.
2. Ensure that you have either a `JAVA_HOME` or `JRE_HOME` environment variable set, pointing to the `JDK` or `JRE` root directory respectively
3. Choose a location on the server, and unzip the Supervisor Desktop Service zip file.
4. On the Genesys server, launch the Configuration Manager and go to the `Hosts` folder under the `Environment` tenant. Create a host object for the machine on which the SDS is going to be deployed, if one does not already exist. The IP address configured in this host object should be the actual IP address of the server, not a loopback address.
5. Go to the `Application Templates` folder and import the application template called `Genesys_Supervisor_Desktop_Service_763.adp`. This template is located with the SDS installation files.
6. Go to the `Applications` folder, then right click and select `New` in the right pane, and then select `Application`.
7. Select the `Genesys_Supervisor_Desktop_Service_763.adp` application template and a new window should open showing the new application.
   a. On the `General` tab, set the name of the application to Genesys Supervisor Desktop.

b. (Multi-tenant environments only) On the `Tenants` tab, add the non-Environment tenant that SDS will monitor.

c. On the `Server Info` tab, select the host object configured in the step above (that is, the server that the SDS is going to be deployed on). If necessary, change the port number to `8080`.

d. On the `Start Info` tab, enter a single period (.) for the `Working Directory`, `Command Line` and `Command Line` arguments.

e. On the `Options` tab:

- Under the `License` section, change the value for `license-file` to the port and host name of the server hosting the license server. This value should be in the format `Port@Hostname` (for example, `7260@inf-devlab`).
- Update the following options under the `supervisor` section:
  - `calculated-statistics-enable` with value `true`.
  - `stat-on-request` with value `true`
  - `stat-threads` with value `-1`
  - `stat-peeking` with value `false`
  - `show-env-tenant` with value `false` for multi-tenant configurations, or value `true` for single-tenant configurations

Note: The following setting:

`stat-threads= -1`

can be used to indicate “use all available processors”.

For smaller customers the following settings:

```
stat-peeking=false
stat-refresh-rate=30
```

can be used to create periodic SDS statistics polling at 30-second intervals.

The refresh rate can be increased for more frequent updates, at the cost of increased SDS and Stat Server load.

For larger customers the following setting:

`stat-peeking=true`

can be used to define on-demand statistics retrieval.

f. On the `Connections` tab, add connections to the T-Servers, Interaction Servers, and the Stat Server that the SDS will connect to.

Note: SDS can be connected to one primary/backup Stat Server pair.

g. Save the application.

8. Open the SDS application properties through the Configuration Manager again.

9. Go to the `Security` tab. In the `Log On As` section, select the `This Account` option, and set the value to `default` or set it to the name or any other account that has full control privileges.
10. Go to the `Options` tab and double-click the `Supervisor` option. Add the properties in Table 4 for your e-mail messaging system.

Table 4: E-mail Properties

Property Name	Example Property Value	Description
email-sender-address	<adminaccount@email-server.com>	The `From` address used for all Resource Management notification e-mail messages
email-server	<email-server@domainname.com>	The mail server name
email-server-port	25	Default SMTP port
email-user	sds.email.account	The user account for the e-mail server. Ignored if `email-authenticate` is set to `off`.
email-authenticate		Does the e-mail server require authentication? Valid values: • `on` • `off`
email-use-SSL		Does the e-mail server use SSL? Valid values: • `on` • `off`
password		The password for the e-mail server. Ignored if `email-authenticate` is set to `off`.

11. Verify that the T-Server(s), Interaction Server(s), and Stat Server(s) are configured with a correct host, that is, not with `localhost`.

    Note: The SDS uses the hosts that are configured in the Configuration Server for the T-Servers, Interaction Servers, and the Stat Servers to determine where they are installed and how to reach them. If these servers are configured with the host `localhost`, the SDS will try to connect to the server on which it is installed. This will not work if the SDS and the other servers are installed on different machines.

12. If the user that the SDS will use has already been configured, skip this step. In the Configuration Manager, create a new person in your SDS-monitored tenant. (For single-tenant installations, create the person in the `Environment` tenant.) The person object should have the following attributes:
    - `First Name: Spv`
    - `Last Name: Spv_Last`
    - `Employee ID: Spv`
    - `User Name: Spv`

    Leave the password fields blank and ensure that the `IsAgent` checkbox is checked.

13. Go to the `Annex` tab, and add a new section named `security`. Open this section and add the following properties:
    - `Supervisor = 1`
    - `SupervisorAdhoc = 2`
    - `SupervisorExtended = 10`
    - `SupervisorMonitoring = 1`

14. Save the user. Open the user properties again and go to the `Security` tab. In the `Permissions` pop-up, add the `default` user to the list and select `Full Control` as the type of access (if this does not already exist). Click `OK` and save the user.

15. Add permissions as follows:
    - For single tenant installations, add `Spv` to the Administrators group for the Environment:
      i. Under `AccessGroups`, select `Administrators`, then right-click.
      ii. Select `New --> Shortcut to Person`. Locate and add `Spv`.

- For multiple tenant installations, to enable agent maintenance, the `Spv` user requires the same subset of permissions as given tenant Administrators, but also requires change permission to `Person` objects (in order to manage agent skills).

  You might want to create a separate access group for the `Spv` user that contains these required permissions. If you do not wish to create a separate access group, please add the `Spv` user to the existing tenant's Administrators Access Group, and grant the group change permission to `Person` objects.

16. In the folder containing the Supervisor Desktop Service installation package, run `setup.exe`. The SDS Installation screen displays.

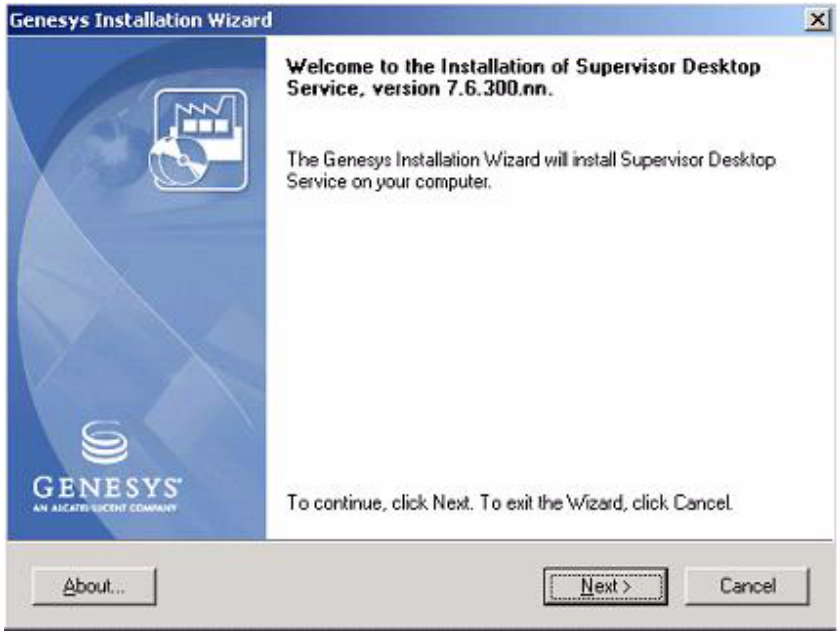


Figure 51: SDS Installation Screen

17. Click `Next`.The `Connection Parameters` screen is displayed.

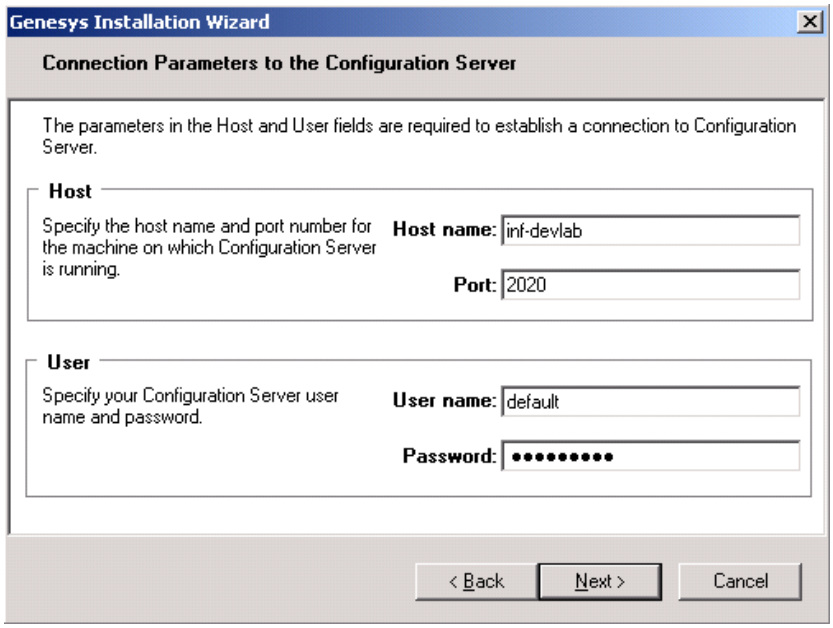


Figure 52: Connection Parameters Screen

18. Enter the host name and port number for your Configuration Server, then enter the Configuration Server user name and password, and click `Next`. The `Select Application` screen is displayed.

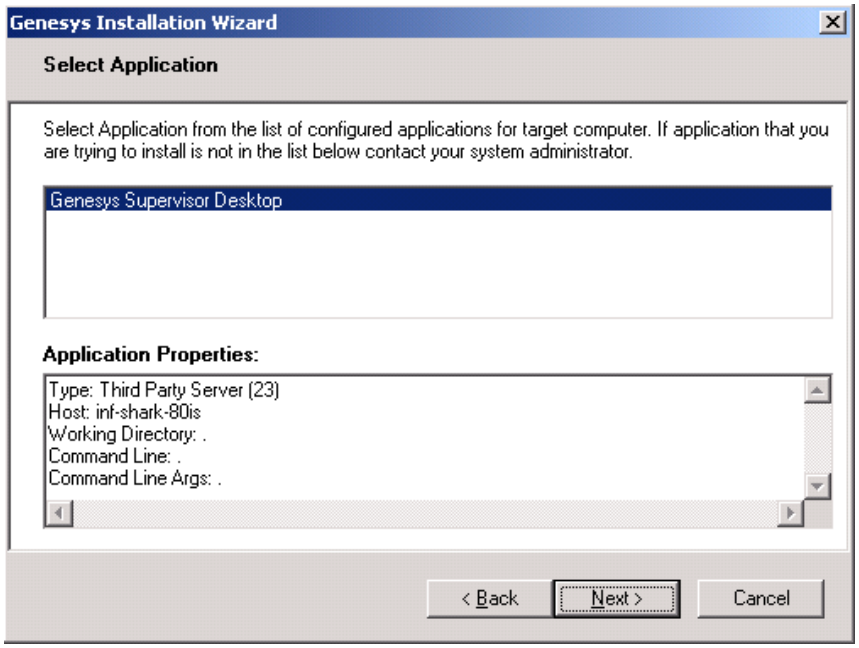


Figure 53: Select Application Screen

19. Select the application you created earlier (in Step 6) and click `Next`. The `Choose Destination Location` screen is displayed.

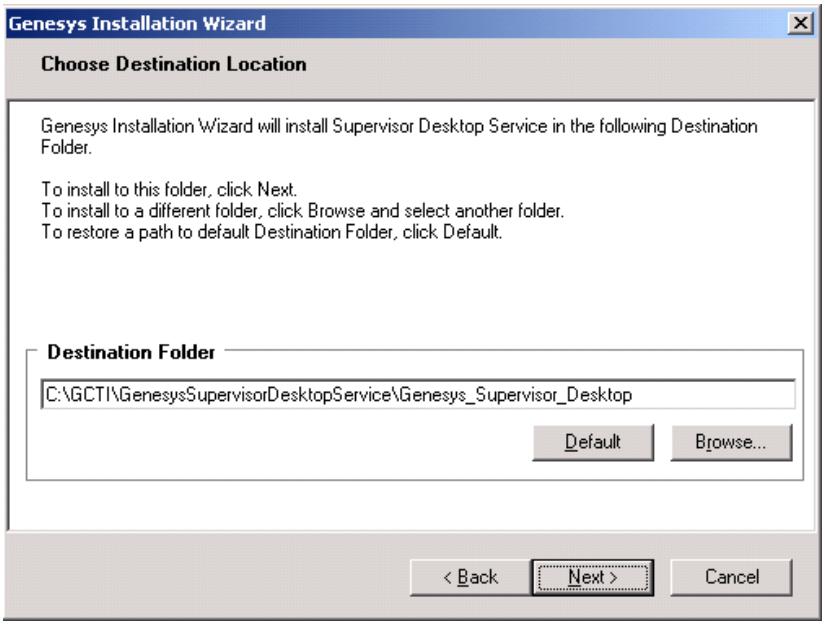


Figure 54: Choose Destination Location Screen

20. Choose the destination folder where the SDS files will be installed and click `Next`. The `Connection Parameters to Backup Configuration Server` screen is displayed.

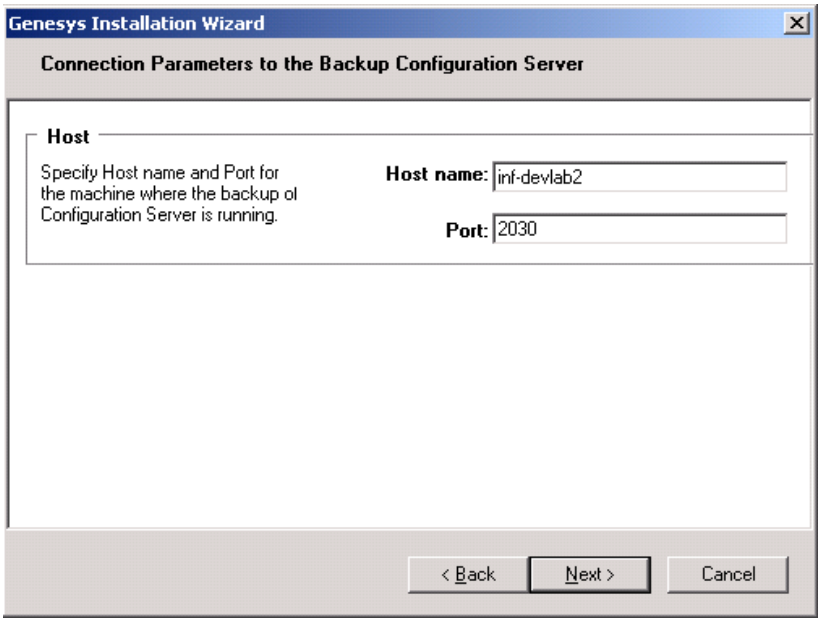


Figure 55: Connection Parameters to Backup Configuration Server

21. If a backup Configuration Server is present, enter the associated host name and port number and click `Next`. The `Configuration Parameters` screen is displayed.

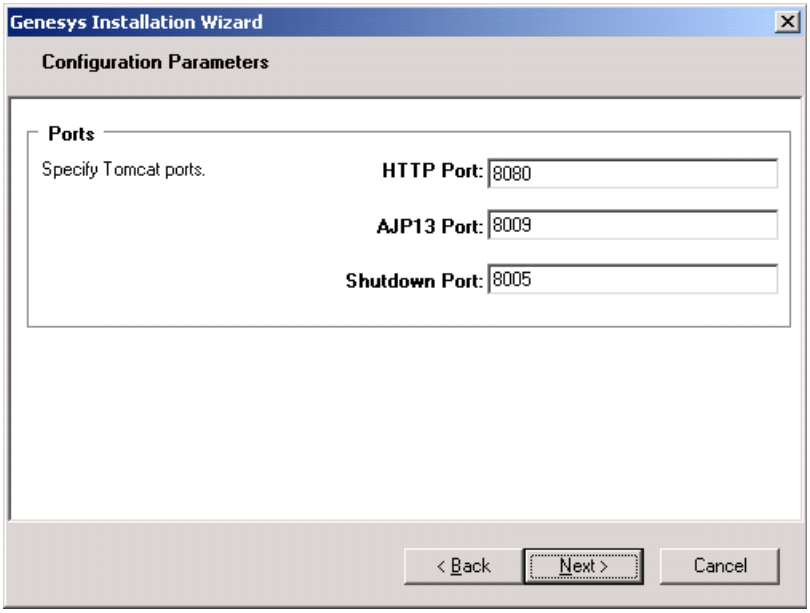


Figure 56: Configuration Parameters

22. Enter the port numbers to be used by Tomcat for HTTP, AJP13, and Shutdown and click `Next`.

    The `Ready to Install` screen is displayed.

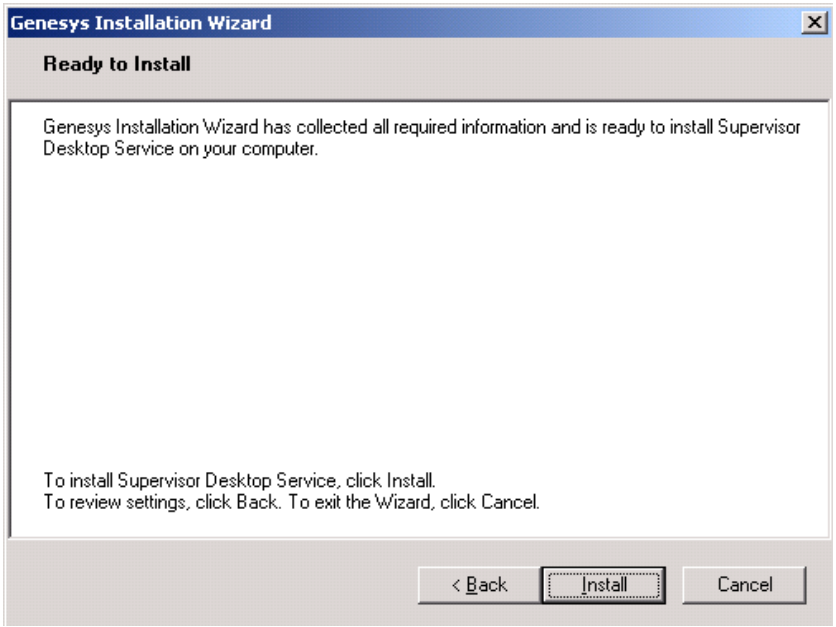


Figure 57: Ready to Install Screen

23. Click `Install`.
24. When the `Installation Complete` screen is shown, click `Finish`.
25. In the Configuration Manager, edit the options for your Stat Server application:
    a. Import the file `GSupervisorDesktopServiceStats.cfg` (found under the `Genesys_Supervisor_Desktop` folder of your installation directory) into the Stat Server application options. Do not overwrite or reload the existing options.
    b. When prompted, choose to overwrite the `Objects` fields for two statistics.
26. In the Configuration Manager, browse to the scripts for the tenant(s) that you use for the SDS installation

    In a pre-7.6 Configuration Manager installation, these would appear under `Resources/Scripts`.

    In a 7.6+ Configuration Manager installation, these would appear under `Tenant/Scripts`.

    Delete all scripts named `User Stat.Spv*`.
27. Restart Stat Server.
28. On the server containing your SDS service, navigate to directory `bin`, and edit the batch file `GDesktopStarter.ini`. Find the line starting with `echo JavaArgs`:
    - Change the value of setting "`--JvmMs`" to `512`.
    - Change the value of setting "`--JvmMx`" to `1024`.
    - Append the following to the end of the line:

      `-XX:+UseConcMarkSweepGC`
    - If SDS is being installed in a multiprocessor environment, add the following to the end of the line:

      `-XX:+UseParNewGC`
29. Open the Windows Services control panel, and start the new Genesys Supervisor Desktop Service.

End of procedure

Deploying Resource Management Console

Procedure:
Deploying Resource Management console

Start of procedure

1. On the machine with the Geronimo instance, run the installer. Click `Next` at the installation screen (see Figure 35 on page 90).
   The `Installation Type` screen is displayed (Figure 36 on page 91).
2. Select `Deploy Resource Management Console` and click `Next`.
   The Database Type screen displays.

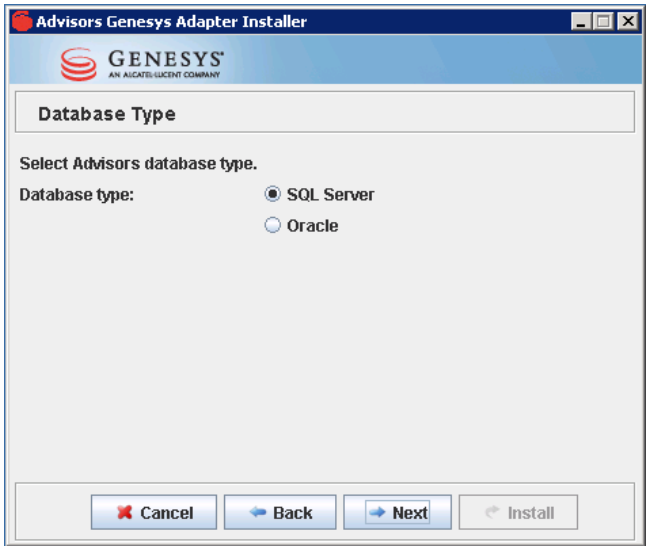


Figure 58: Database Type Screen

3. Select the database type for this installation and click `Next`.
4. Select the base location of the Advisors installation (that, the base directory where the Platform components and Geronimo are installed). In most cases, this is `C:\Program Files\GCTI\Advisors`.

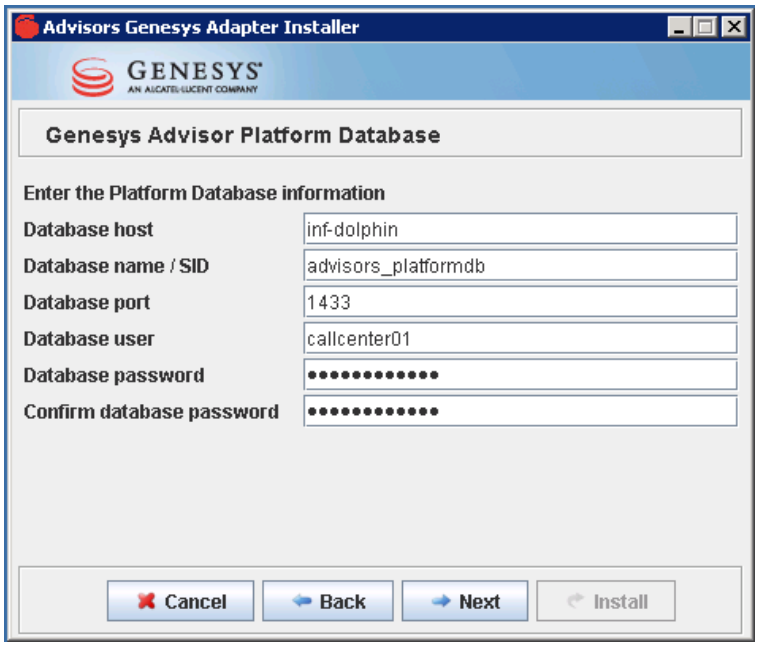


Figure 59: Genesys Advisor Platform Database

5. Type the host name or IP address of the machine where the Genesys Advisor database is installed.

   Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

6. Type the database name.
7. Type the user name and password of a user that will be used by the Adapter to access the database.
8. Click `Next`. The `Installation Progress` screen displays.
9. Click `Show Details then Install`.
10. Edit the `RMCInfo.xml` configuration file, found in:

    ```
    Advisors\geronimo-tomcat6-minimal-2.1.3\repository\com\informiam\genesys\rmc-web\<version> \rmc-web-8.x.xxx_<version>.war
    \WEB-INF\classes
    ```

    (All SDS-prefixed properties refer to the SDS Service, installed earlier. All CCAdv/WA-prefixed properties refer to the CCAdv/WA installation host.) Use the following values:

    a. `SDS_IP`—The IP address for the SDS Service host
    b. `SDS_Port`—The port number for the SDS path (default `8080`)
    c. Do not change `SDS_DeployPath`, `SDS_UserName` or `SDS_Password`.

d. `CCAWA_IP`—The IP address for the CCAdv/WA server host.

> Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

e. `CCAWA_Port`—The port number for the CCAdv/WA server (default `8080`).

11. In order to access the Resource Management Notification administration pages through the Advisors browser (Contact Center Advisor Administration module), the following entry needs to be added to the Apache `httpd.conf` file on the web server:

```
ProxyPass /rmc/ ajp://<rmc host>:<rmc port>/rmc/
```

where <`rmc host`> is the host name or IP address for the machine on which the RMC module is installed, and where <`rmc port`> is the corresponding port number (default: `8009`).

12. Open the services windows and restart the Geronimo server.

End of procedure

Deploying Multiple Instances of the Genesys Adapter Core Service on a Single Server

It is possible to deploy multiple instances of the Genesys Adapter core service on a single server. You must decide whether to use the same metrics database for both Adapters. Note that if you do this, each Adapter must monitor a completely distinct set of objects. Each installation should:

- Create the Genesys Adapter database (see Part 1 on page 13.)
- Install and configure the Genesys Adapter Core Service.
- Configure XMLGen with a few variations.

Installation Notes

Each Genesys Adapter instance must have its own core database. Therefore, when creating the Genesys Adapter database, a unique name is required for each database instance

1. Run the installer jar, then select `Install Server`.

2. On `Server Install Type` screen:

a. Select `Install the service`.

   b. Make sure that `Start the Service` is not selected.
   c. Select the application(s) to be supported.

3. Each Genesys Adapter instance must be installed in a different directory. For example, the first instance could use the following location:

   `C:\Program Files\GCTI\Advisors\Genesys\Adapter`

   and the second instance could be located at:

   `C:\Program Files\GCTI\Advisors\Genesys\Adapter2.`

   This includes the log directory as well. Each Genesys Adapter instance on the same machine must use a different port number.

   The same CCAdv/WA metrics database can be used by other Adapter instances. Alternatively, a new metrics database can be created.

4. During the install, ignore this error if it occurs:

   `[exec] wrapper | CreateService failed – the specified service already exists. (0x431)`

5. Once the adapter has been installed, navigate to the `conf` folder for the second installation:

6. Locate the file `wrapper.conf` and edit it as follows:
   a. Search for the string `# Name of service.`
   b. Edit the parameter below it (`wrapper.ntservice.name=`) so that the service name is different from the original instance—for example, `Advisors Genesys Adapter 2`.
   c. Edit the next parameter (`wrapper.ntservice.displayname=`) so that it differs from the original instance. This is the name that will appear in the `NT Services` dialog. It need not match the name used in `wrapper.ntservice.name=` above, but it can.

7. Save and close the file.

8. Navigate to the `bin` folder for the second installation, and execute the file `Install-Adapter-NT.bat`. This installs the renamed service. After the installation is complete, you can then locate and start the service in the `Services Control Panel` applet.

Troubleshooting Installation Errors

Table 5 lists parameter validation errors that you may encounter at the end of installation.

Table 5: Installation Error Messages

Error Message	Cause
[java] Failed to connect to the database using connection URL: [java] jdbc:sqlserver://192.168.xx.yy:nnn;DatabaseName=ys_gadb;user=sa;password=very_secure_pwd;selectMethod=cursor [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnn has failed. Error: "Connection refused. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port.	Wrong database server name / IP address or port number
[java] Failed to connect to the database using connection URL: [java] jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=NotAPlatformDB;selectMethod=cursor;user=sa;password=very_secure_pwd [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnnn has failed. Error: "connect timed out. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port."	Wrong database name
[java] Exception while connecting: Login failed for user 'badUserId'. [java] url used: jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=ys_gadb;selectMethod=cursor;user=badUserId;password=very_secure_password	Wrong database user name or password

Chapter

8 Deploying Cisco Adapter

This chapter gives an overview of the installation of Cisco Adapter. It contains the following section:

- Prerequisites, page 119
- Deploying the Cisco Adapter, page 121
- Deploying Multiple Instances of the Cisco Adapter on a Single Server, page 131
- Troubleshooting Installation Errors, page 133

Prerequisites

See "Deployment Prerequisites" on page 15.

Before deploying Cisco Adapter, you must have created the following two databases that Cisco Adapter communicates with and set up admin accounts for them:

- FA database
- ACA database

To create the Cisco Adapter databases, see either:

- Chapter 2, "Creating a SQL Server Database," on page 23, or;
- Chapter 3, "Creating an Oracle Database," on page 37.

Installation Summary

In release 8.1.x, Cisco Adapter only works with Frontline Advisor.

An instance of Cisco Adapter will talk to only one instance of Frontline Advisor. For this reason, every Cisco Adapter requires a corresponding, independent Frontline Advisor.

A verified Cisco environment must be ready and available. Credentials with read access to the HDS and AW databases must be available when the Advisors Cisco Adapter Installer is run.

Note: Resource Management is not available for Cisco-only implementations.

Installation Contents

The following files are shipped with the Cisco Adapter:

MS SQL Server

`aca-installer-<version>.jar`

Files in the `mssql` folder:

- `aca-new-database-<version>.sql`

Files in the `mssql\migrations` folder:

- `aca-migration-3.3-to-8.0.sql`
- `aca-migration-8.0-to-8.1.sql`
- `aca-migration-8.1-to-8.1.1.sql`

Files in the `mssql\supplemental` folder:

- `GeneratePermsStatements.sql`

Oracle

Files in the `oracle` folder:

- `aca-<version>_Schema.sql`
- `aca-<version>_TBS.sql`
- `aca-new-database-<version>.sql`

Files in the `oracle\migrations` folder:

- `aca-migration-8.1-to-8.1.1.sql`

Deploying the Cisco Adapter

Procedure:
Deploying the Cisco Adapter

Start of procedure

1. Run the installation jar file by either;
   - Using the command `java -jar aca-installer-<version>.jar`; or,
   - Double-clicking the `aca-installer-<version>.jar` in the release bundle.

Notes: 1. Double-click does not work if only JDK is installed (that is, JRE is not present).

2. For 64-bit systems, if double-clicking to launch the installer, please ensure that the Java instance associated with the `jar` file type is 64-bit. Running the installer with a 32-bit Java instance will create a Windows service with the wrong executable.

The `Installer for Advisors Cisco Adapter` screen displays.

Figure 60: Installer for Cisco Adapter

2. Click `Next`.
   The `Install Type` screen displays (see Figure 61 on page 122).

Figure 61: Install Type

3. Choose an installation option and click `Next`. The `Installation Details` screen displays.

Figure 62: Installation Details

4. Specify the installation directory. The default installation directory is `C:\Program Files\GCTI\Advisors\CiscoAdapter`.

5. Enter the port number that the Cisco Adapter Web services will run on. You can use the default port, `7000`, if no other application is using that port.
6. Specify the directory in which the log files will appear.
7. Click `Next`. If the directory does not yet exist, click `Yes` on the subsequent popup. The Java Development Kit installation screen displays.

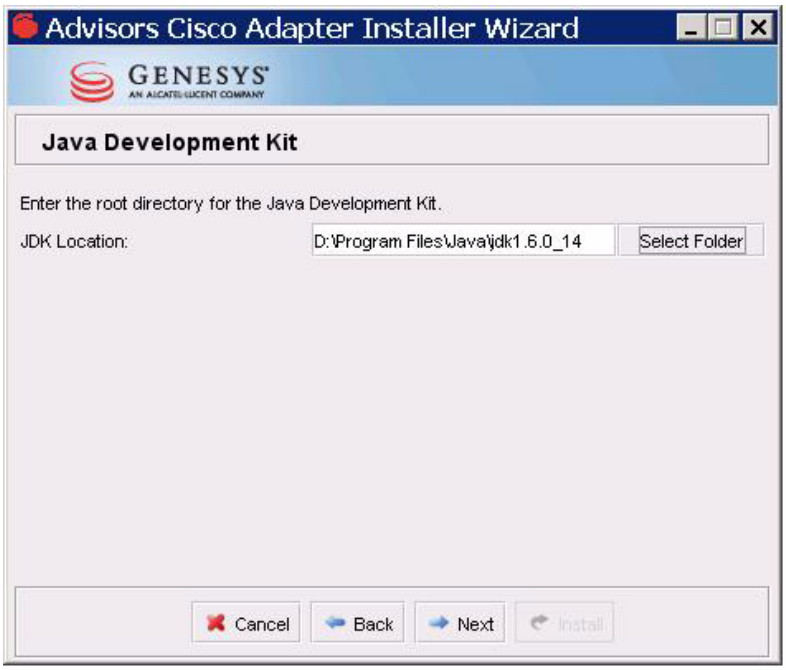


Figure 63: Java Development Kit Screen

8. Specify the root directory for the JDK 1.6 installation by either entering it or by browsing to it with the `Select Folder` button, then click `Next`. The `Cisco Database Configuration` screen displays (see Figure 64 on page 124.)

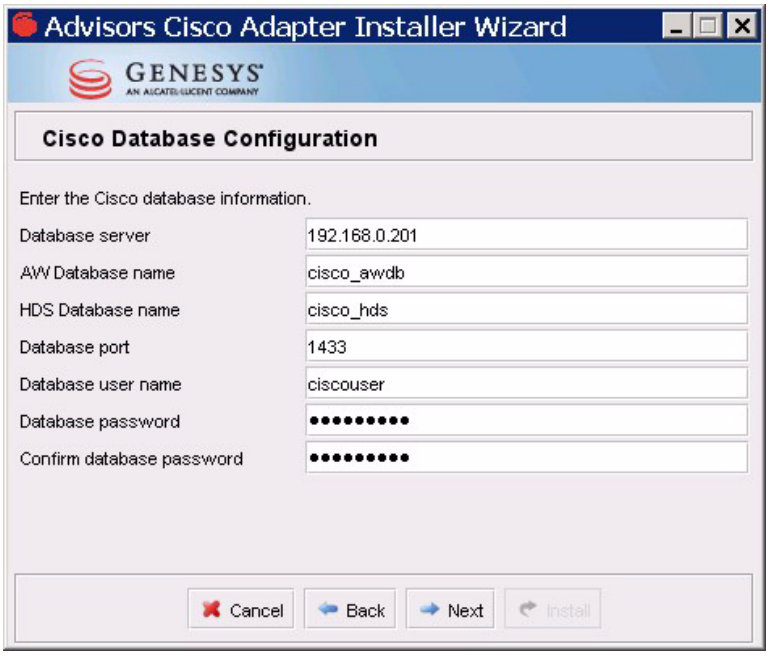


Figure 64: Cisco Database Configuration

9. Enter the information required for connecting to the databases in the Cisco environment.

> Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

10. Click `Next`. The `Cisco Adapter Database Configuration` screen displays.

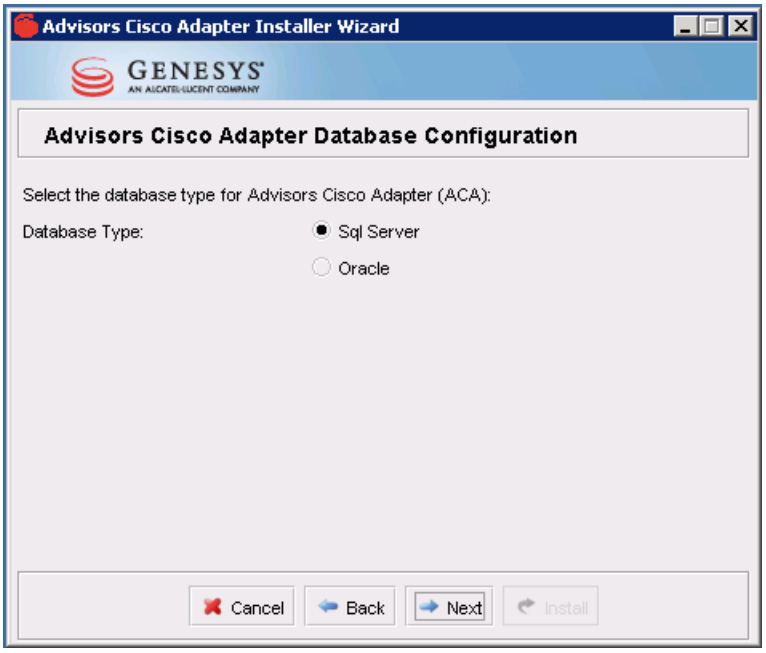


Figure 65: Advisors Cisco Adapter Database Type Screen

11. Select the database type for this installation:

- Microsoft SQL Server
  Click `Next` and go to Step 12.
- Oracle
  Click `Next` and go to Step 19.

12. The Advisors Cisco Adapter Database Configuration Screen displays (see Figure 66, "Advisors Cisco Adapter Database Configuration Screen for SQL Server," on page 126).

Figure 66: Advisors Cisco Adapter Database Configuration Screen for SQL Server

13. Enter the host name or IP address of the machine where the Cisco Adapter database is installed.

> Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

14. Enter the database name.
15. Enter the port number.
16. Enter and confirm the user name and password for the database login created / used for the Cisco Adapter database.
17. Click Next. Go to Step 21.
18. (From Step 11). Locate the Oracle JDBC driver and click Next.

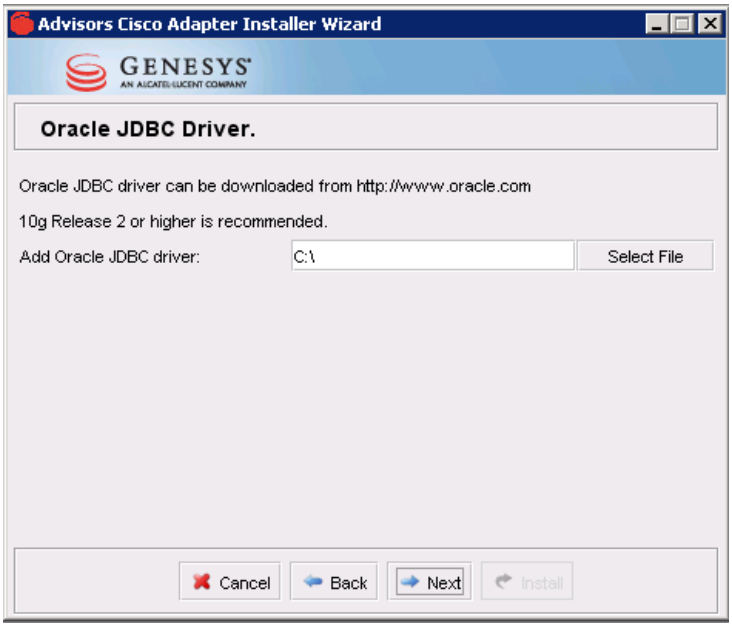


Figure 67: Oracle JDBC Driver Screen

Note: The following Oracle JDBC drivers can be used:

- Oracle database 10g release 2 (10.2.0.4). The download file is `ojdbc14.jar`.
- Oracle database 11g release 2 (11.2.0.2.0). The download file is `ojdbc6.jar`.

19. The `Advisors Cisco Adapter Database Configuration` screen for Oracle is displayed.

Figure 68: Advisors Cisco Database Configuration Screen for Oracle

20. Specify the parameters for the Cisco Adapter Oracle database:

- `Database Server`—The host name or IP address where the database server is running.

> Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

- `Database SID`—The database instance alias.
- `Database port`—The database server's port number
- `Database schema`—The database schema
- `Database schema password`—The database schema created / used for the Cisco Adapter.

21. Click `Next`. The `FA Database Configuration` screen for either MS SQL Server or Oracle displays.

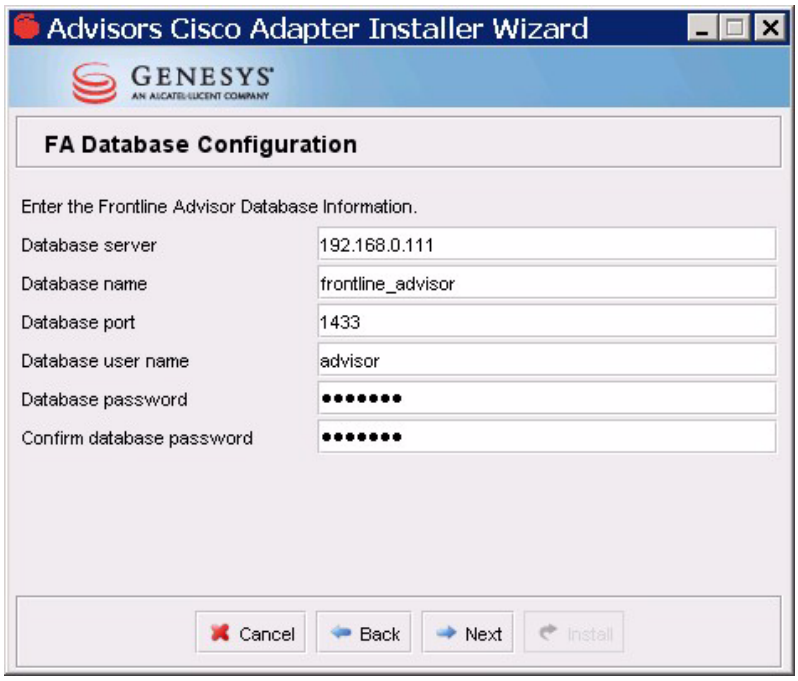


Figure 69: FA Database Configuration for SQL Server

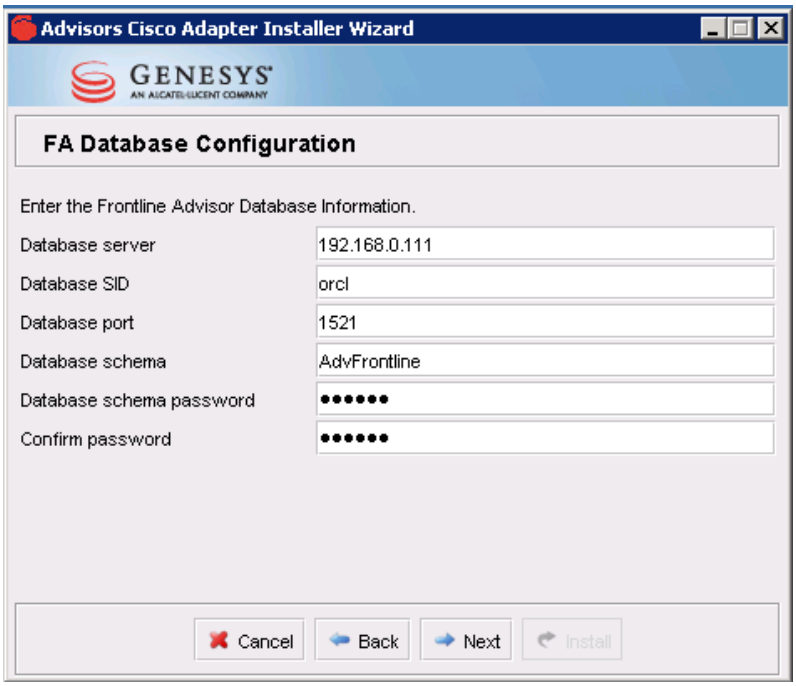


Figure 70: FA Database Configuration for Oracle

22. Complete the required database configuration parameters.

> Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

23. Click Next. Go to Step 24.

Figure 71: Installation Progress

24. Click Show Details then Install.
25. Verify that there are no errors during installation.
26. In the Services Control Panel applet, verify that an Advisors Cisco Adapter service is installed. If the option to start the service was selected earlier, the service's status should be Started. See Figure 72 on page 131.

> Note: All database passwords used by the Cisco Adapter application are encrypted and saved inthe ..GCTI\Advisors\CiscoConnector\conf\cisco_connector.properties file.
>
> To change the password see "Changing Encrypted Passwords After Installation" on page 76.

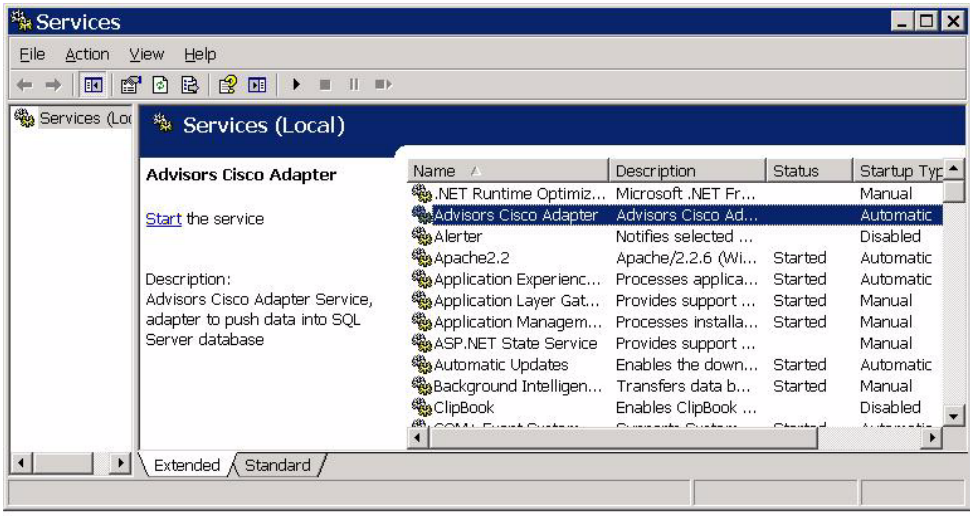


Figure 72: Services (Local) Screen

End of procedure

Deploying Multiple Instances of the Cisco Adapter on a Single Server

You can deploy multiple instances of the Cisco Adapter on a single server.

Procedure: Deploying multiple instances of Cisco Adapter on a single server

Prerequisites

It is recommended that each Cisco Adapter instance have its own database. Therefore, when creating the Cisco Adapter database in step 10, you should use different names for each database instance.

Start of procedure

1. Run the `aca-installer-<version>.jar` file.
2. In the `Server Install Type` screen (Figure 61 on page 122);
   a. Check that `Install the service` is preselected.
   b. Ensure that the `Start the Service` check box is unchecked.

3. Each Cisco Adapter instance must be installed in a different directory. For example, the first instance could be located at:

   `C:\Program Files\GCTI\Advisors\CiscoAdapter`

   and the second instance could be located at:

   `C:\Program Files\GCTI\Advisors\CiscoAdapter2`.

   This includes the log and data directories as well. The Cisco Adapter instance must also use a different port number than the other instances installed on the machine.

   The same Cisco AW and HDS Metrics Database being used by other instances can be used here. Alternatively, different set of Cisco databases can be used.

4. During the install, the following error will come up:

   `[exec] wrapper | CreateService failed – the specified service already exists. (0x431)`

   Ignore this error: the missing service will be installed in step 5.

5. Once the adapter has been installed, navigate to the `\conf` folder.
   a. Locate and edit the file `wrapper.conf`.
      i. Search for the string `# Name of service`.
      ii. Edit the parameter below it (`wrapper.ntservice.name=`) so that the service name is different from the original instance. For example, ‘Advisors Cisco Adapter 2.
      iii. Edit the next parameter (`wrapper.ntservice.displayname=`), so that the display name differs from the original instance. This is the name that will appear in the NT Services dialog. There’s no need for it to match the name above.
      iv. Save and close the file.
   b. Navigate to the `/bin` folder of the second installation, and execute the file `Install-Adapter-NT.bat`. This installs the renamed service. You can then locate and start the service in the `Services Control Panel` applet.

End of procedure

Troubleshooting Installation Errors

The following are parameter validation errors that you may encounter at the end of installation:

Table 6: Installation Error Messages

Error Message	Cause
[java] Failed to connect to the database using connection URL: [java] jdbc:sqlserver://192.168.xx.yy:nnn;DatabaseName=ys_cadb;user=sa;password=very_secure_pwd;selectMethod=cursor [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnn has failed. Error: "Connection refused. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port.	Wrong database server name / IP address or port number
[java] Failed to connect to the database using connection URL: [java] jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=NotAPlatformDB;selectMethod=cursor;user=sa;password=very_secure_pwd [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnnn has failed. Error: "connect timed out. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port."	Wrong database name
[java] Exception while connecting: Login failed for user 'badUserId'. [java] url used: jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=ys_cadb;selectMethod=cursor;user=badUserId;password=very_secure_password	Wrong database user name or password

Table 6: Installation Error Messages (Continued)

Error Message	Cause
[java] Exception in thread "main" java.security.InvalidParameterException: ERROR: Failed to verify validity of the JDK 1.6 located at /home/yevgeny/dev/java/j2sdk1.4.2_08. [java] ERROR: Invalid JDK version found at /home/yevgeny/dev/java/j2sdk1.4.2_08, the version must be at least 1.6, but was 1.4 [java] at com.informiam.installer.jdk.JdkVersionChecker.checkJdk (JdkVersionChecker.java:66) [java] ERROR: Failed to verify validity of the JDK 1.6 located at /home/yevgeny/dev/java/j2sdk1.4.2_08. [java] at com.informiam.installer.jdk.JdkVersionChecker.main (JdkVersionChecker.java:81)	Wrong path to JDK or wrong version of the JDK specified.
Apr 11, 2011 3:53:46 PM oracle.jdbc.driver.OracleDriver registerMBeans WARNING: Error while registering Oracle JDBC Diagnosability MBean. java.security.AccessControlException: access denied (javax.management.MBeanTrustPermission register) at java.security.AccessControlContext.checkPermission(Unknown Source) at java.lang.SecurityManager.checkPermission(Unknown Source)at com.sun.jmx.interceptor.DefaultMBeanServerInterceptor.checkMBeanTrustPermission(Unknown Source) at com.sun.jmx.interceptor.DefaultMBeanServerInterceptor.registerMBean(Unknown Source) at com.sun.jmx.mbeanserver.JmxMBeanServer.registerMBean(Unknown Source) at oracle.jdbc.driver.OracleDriver.registerMBeans(OracleDriver.java:360) at oracle.jdbc.driver.OracleDriver$1.run(OracleDriver.java:199) at java.security.AccessController.doPrivileged(Native Method) at oracle.jdbc.driver.OracleDriver.<clinit>(OracleDriver.java:195)	Produced in error and can be ignored. Displays in the Errors tab when installing Cisco Adapter with Oracle JDBC driver ojdbc6-11.2.0.2.0, and accurately reports that installation was successful.
Exception in thread "AWT-EventQueue-0" java.lang.ArrayIndexOutOfBoundsException: 32 at sun.font.FontDesignMetrics.charsWidth(Unknown Source) at javax.swing.text.Utilities.getTabbedTextOffset(Unknown Source) at javax.swing.text.Utilities.getTabbedTextOffset(Unknown Source) at javax.swing.text.Utilities.getTabbedTextOffset(Unknown Source) at javax.swing.text.PlainView.viewToModel(Unknown Source) at javax.swing.text.FieldView.viewToModel(Unknown Source) at javax.swing.plaf.basic.BasicTextUI$RootView.viewToModel(Unknown Source) at javax.swing.plaf.basic.BasicTextUI.viewToModel(Unknown Source)	Produced in error and can be ignored.

Chapter

9 Deploying Contact Center Advisor and Workforce Advisor

This section describes how to install Contact Center Advisor, Workforce Advisor and the Genesys Advisor browser. It contains the following sections:

- Deployment Notes, page 135
- Prerequisites, page 136
- Deploying CCAdv/WA Modules, page 136
- Deploying XML Generator Service, page 147
- Custom Time Zones, page 153
- Workforce Advisor Web Service Option, page 154
- Deploying the Genesys Advisors Browser, page 158
- Formatting Alert Messages Sent by Advisors, page 160
- Changing the XML Generator Connection after Installation, page 162
- Deploying the XML Generator as a Service, page 163
- Disabling Performance Monitor and the Workforce What-If Tool, page 164
- Configuring Contact Groups, page 164
- Formatting Alert Messages Sent by Advisors, page 160

Deployment Notes

- Install Genesys Adapter if you are using a Genesys CTI installation. For Cisco installations, no adapter is required.

Prerequisites

- Please see "Deployment Prerequisites" on page 15.
- For each physical server on which you install a Web application (such as Contact Center Advisor or Workforce Advisor), you must install Platform.
- XMLGen requires Advisors Platform to be installed.
- A Metrics Graphing database must be installed if either XMLGen or Dashboard is installed. To create this database, see either:
  - Chapter 2, "Creating a SQL Server Database," on page 23, or;
  - Chapter 3, "Creating an Oracle 11g Database," on page 37.
- Contact Center Advisor and Workforce Advisor require database-level connectivity between the Advisors Platform database and the datasource database—a Genesys metrics database and/or a Cisco ICM AWDB database. To configure the connectivity see Chapter 4 on page 43.

Deploying CCAdv/WA Modules

Procedure: Deploying CCAdv/WA Modules

Start of procedure

1. Run the installation jar file by either;
   - Using the command `java -jar ccawa-installer-<version>.jar;` or,
   - Double-clicking the `ccawa-installer-<version>.jar` in the release bundle.

Notes: 1. Double-click does not work if only JDK is installed (that is, JRE is not present).

2. For 64-bit systems, if double-clicking to launch the installer, please ensure that the Java instance associated with the `jar` file type is 64-bit. Running the installer with a 32-bit Java instance will create a Windows service with the wrong executable.

2. Click `Next`.
   The `Module to Install` screen displays (Figure 73 on page 137).

Figure 73: Module to Install Screen

3. Each of the module sets can be installed on a different machine; however, Advisors Platform must be installed on each server where a module is installed. When installing multiple modules on the same machine, the underlying components, such as Geronimo, are installed only once.

   The module sets are:

   - Dashboards:
     - Contact Center Advisor dashboard
     - Workforce Advisor dashboard—Disabled for the user until the Workforce Advisor module is installed.
   - XML Generator application—See “Deploying the XML Generator” on page 147.
   - Workforce Advisor Web service—Workforce Advisor Web server only (not the Dashboard).
   - Alert Management administration—No additional configuration required.

For all options, the installation process prompts for the location of the installation directory and Advisors Platform database. Use the same directory and database configuration that was specified when the Advisors Platform database was configured.

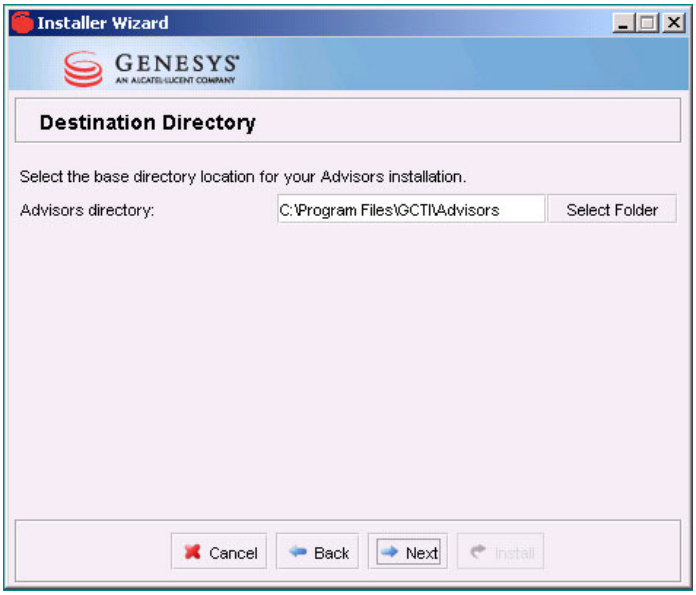


Figure 74: Destination Directory Screen

4. Select the destination directory in which the files will be installed (the Advisors base directory).

   The default directory is `Program Files\GCTI\Advisors`. Click `Next`.

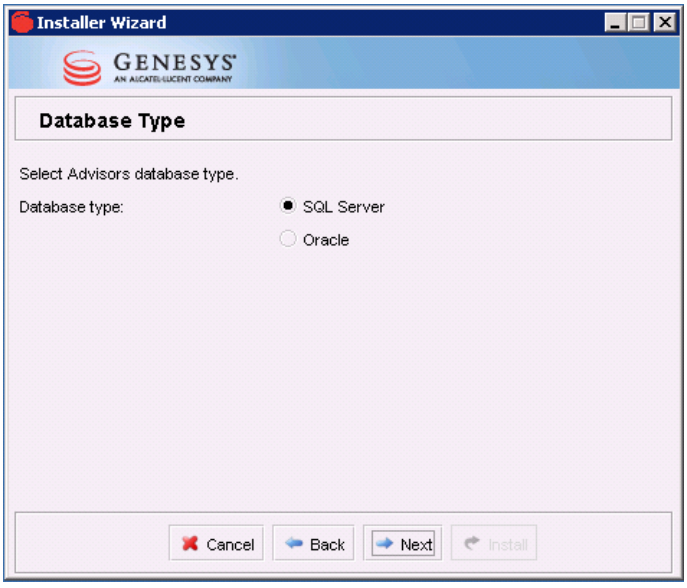


Figure 75: Database Type Screen

5. Select the database type for this installation:
   - SQL Server
     Click `Next` and go to Step 6.

- Oracle
  Click `Next` and go to Step 13.

6. The `Genesys Advisor Platform Database` screen for MSSQL is displayed.

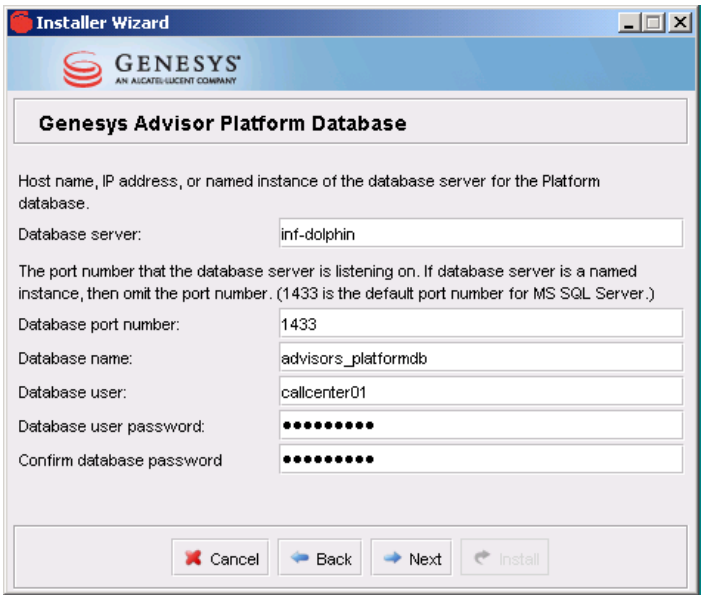


Figure 76: Genesys Advisor Database Screen for MSSQL

7. Enter the database connectivity parameters for the already created or upgraded database (that is, the database must be present and at the current version prior to running the installer). These parameters are server (machine), port number, name, user, and password.

   Note: When using numerical IP v6 addresses, please enclose the literal in brackets.

   If the database server is a named instance, then omit the port number. Click `Next`. Go to Step 15.

8. For the Dashboard and XML Generator options, the installation process prompts for the location of the Metric Graphing database.

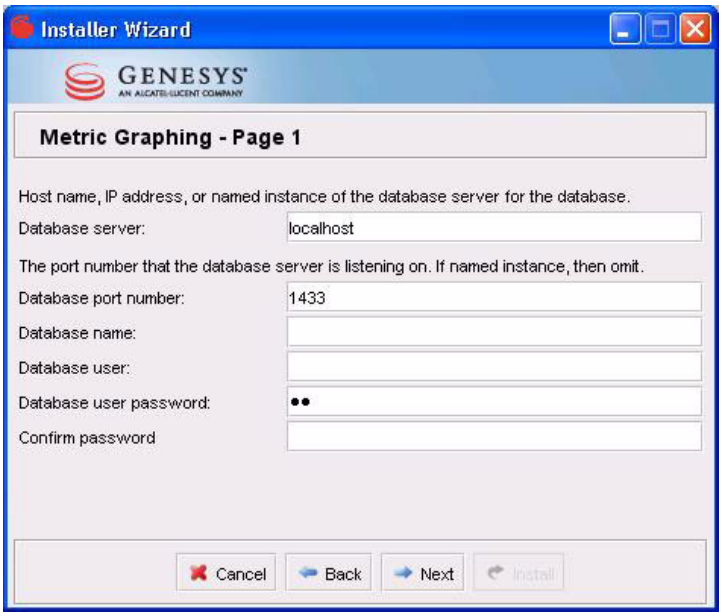
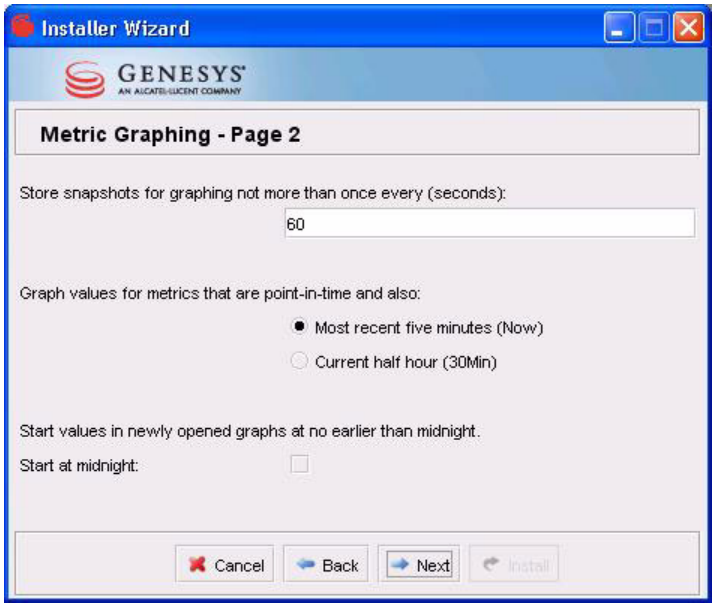


Figure 77: Metric Graphing Screen 1 (MSSQL)—Dashboards and XMLGen

9. Specify the connection parameters for the Metric Graphing database, following the onscreen instructions.

Note: When using numerical IP v6 addresses, please enclose the literal in brackets.

Click Next to display the second Metrics Graphing screen.



10. Enter the interval in seconds that controls how frequently snapshots are stored in the metric graphing database. For example, if this parameter is set to 60 seconds, then XML Generator will store graphable snapshots no more often than that. However, XML Generator may store the snapshots less frequently depending upon load and the complexity of the configuration.
11. Select the time interval to be used for values in the Metric Graphing display; either `Now` or `30 Min`. This is a system-wide setting that will determine the time period of values displayed in graphs. If you choose `Now`, then the values are those in the dashboard columns titled `Now`, from the most recent five minutes. If you choose `30 Min`, then the values are those in the dashboard columns titled `30 Min`, from the current half hour. The values graphed for point-in-time metrics, that do not have a duration, are not affected by this setting.
12. Select whether graphs should display values from the previous day. If you check the `Start at midnight` checkbox, then graphs will not display values from the previous day. Also, an open graph will delete values from the previous day as it reaches midnight.
13. The `Genesys Advisor Platform Database` screen for Oracle is displayed.

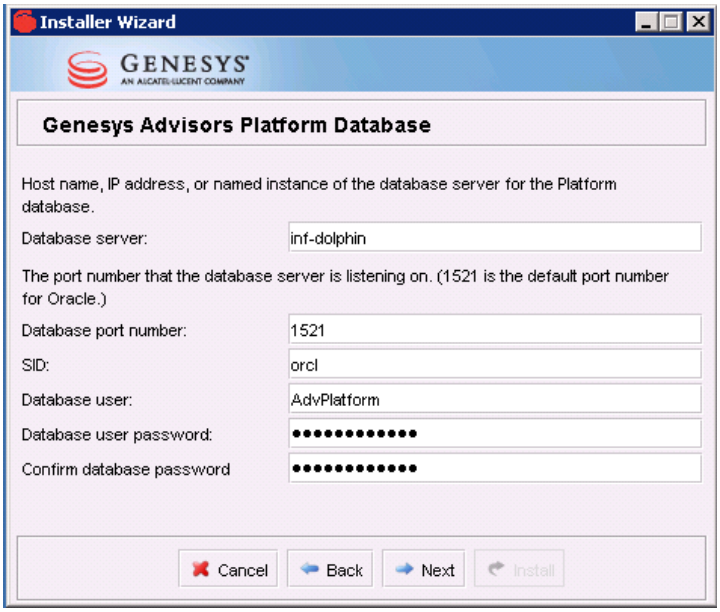


Figure 78: Genesys Advisors Platform Database Screen for Oracle

14. Specify the parameters for the Platform Oracle database:
    - `Database Server`—The host name or IP address where the database server is running

> Note: When using numerical IP v6 addresses, please enclose the literal in brackets.

- Database port number—The database server's port number
- SID—The database instance alias.
- Database user and password—The database schema created / used for the Platform database.

Click Next.

15. For the Dashboard and XML Generator options, the installation process prompts for the location of the Metric Graphing database.

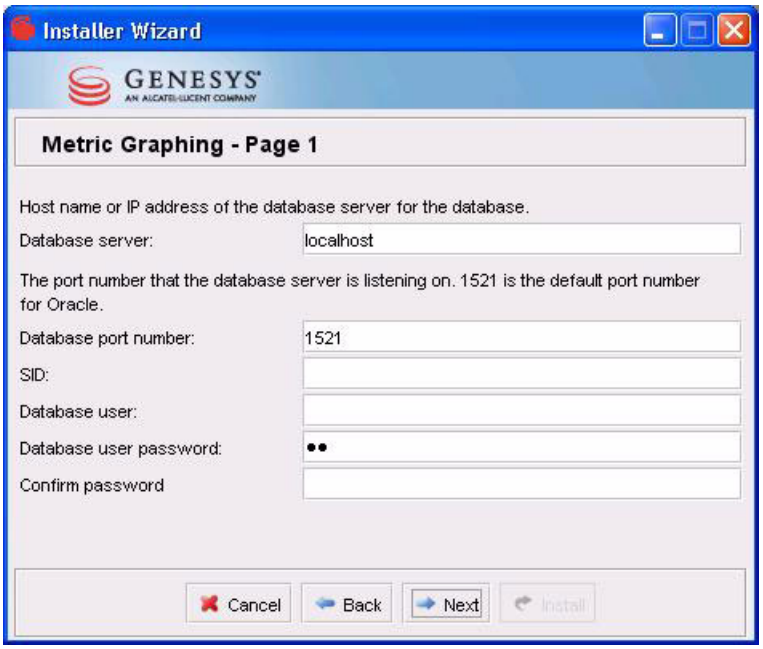


Figure 79: Metric Graphing Screen1 (Oracle)—Dashboards and XMLGen

16. Specify the connection parameters for the Metric Graphing database, following the onscreen instructions.

> Note: When using numerical IP v6 addresses, please enclose the literal in brackets.

17. Click Next to continue.
The Java Development Kit screen displays.

Figure 80: Java Development Kit page

18. Enter or select the folder location for the Java Development Kit.
19. Click `Next`.

End of procedure

Next Steps

- "Deploying XML Generator Service" on page 147

Configuring Metric Graphing Properties

The following list describes the properties that govern metric graphing, in the `CONFIG_PARAMETER` table in the Advisors database:

- The time period of graphed values.
  The default is to show values from the `Now` period, and from point-in-time metrics. You can change this to show values from the `30 Min` period, and from point-in-time metrics. "Changing the time period of graphed values" on page 144.
- The duration of the values retained for graphing on first display of a graph. The default number is 120 minutes, or 2 hours. Changing this number will increase or decrease the number of minutes on the complete X axis of a graph when you first display it. See "Changing the duration of values retained for graphing" on page 144.

- The interval in seconds between graphed values in all graphs for points stored after the change. See “Changing the interval in seconds between values” on page 145.
- Whether graphed values display from midnight.
  The default value is `true`. Changing this to false mean that a graph will not show values with times from the previous day. “Changing whether graphed values start at midnight” on page 146.

Procedure:
Changing the time period of graphed values

Purpose: To change the setting that determines the time period of values in graphs.

Start of procedure

1. In the Advisors database, execute

   ```
   UPDATE CONFIG_PARAMETER SET PARAM_VALUE = 'n'
   ```

   Where

   ```
   PARAM_NAME = warehoused.metrics.period.type
   ```

   For *n*, substitute your desired value. Legal values are `FiveMin` and `ThirtyMin`. `FiveMin` chooses the values from the dashboard columns titled `Now` from the most recent five minutes. `ThirtyMin` chooses values from the dashboard columns titled `30 Min`, from the current half-hour.
2. Wait at least five minutes until the configuration parameter cache expires, and the value you set is loaded into the cache again.
3. From this point on, XML Generator stores the values for graphing from the time period you chose. Previously stored values will still be from the previously chosen time period.

End of procedure

Procedure:
Changing the duration of values retained for graphing

Purpose: To change the duration, in minutes, of the values that are retained for graphing on first display of a graph.

Note that XML Generator is optimized with the graphing parameters of 120 minutes of graphable values that are no closer than 60 seconds apart.

If you decrease the interval in seconds between values, you must decrease the duration of values stored, so that only approximately 120 values are stored for graphing. See “Changing the interval in seconds between values” on page 145.

Start of procedure

1. In the Advisors database, execute:

   ```
   UPDATE CONFIG_PARAMETER SET PARAM_VALUE = 'n'
   ```

   Where

   ```
   PARAM_NAME = warehoused.metrics.max.minutes.kept
   ```

   For *n*, substitute your desired value. Note that the value is entered as a character string, surrounded by single quotes.
2. Wait at least five minutes until the configuration parameter cache expires, and the value you set is loaded into the cache.
3. From this point on, XML Generator will store up to *n* minutes of values for each metric in the metric graphing database. The graphing service will return *n* minutes of values for each graph when you first open it.

End of procedure

Procedure: Changing the interval in seconds between values

The supported amount of historical data that XML Generator stores for one graphed metric is 120 values. By default, XML Generator keeps 120 values that are not closer than one minute apart.

Note that XML Generator is optimized with the graphing parameters of 120 minutes of graphable values that are no closer than one minute apart.

If you decrease the interval in seconds between values, you must decrease the duration of values stored, so that only approximately 120 values are stored for graphing.

Purpose: To change the minimum number of seconds between values in a graph.

Start of procedure

1. In the Advisors database, execute:

   ```
   UPDATE CONFIG_PARAMETER SET PARAM_VALUE = 'n'
   ```

   Where

   ```
   PARAM_NAME = warehoused.metrics.min.interval.secs
   ```

   For *n*, substitute your desired value. Note that the value is entered as a character string, surrounded by single quotes.

2. Wait until the configuration parameter cache expires, and the value you set is loaded into the cache.
3. From this point on, XML Generator store values for graphing such that a value is at least *n* seconds after the previous value stored. The graphing service will return the values that have been stored, according to any minimum interval setting that has existed for the duration of storage.

End of procedure

Example

If you want to display a graph of values for one day all the way back to midnight, that is at most 24 hours. We can calculate that (24 hours * 60 minutes per hour / 120 data points) means 1 data point will be graphed not more than every 12 minutes.

1. At installation set the `Store snapshots for graphing` interval to 720 seconds (12 minutes * 60 seconds per minute) This setting corresponds to `warehoused.metrics.min.interval.secs` in `CONFIG_PARAMETER.NAME` in the Advisors database.
2. By hand in the `CONFIG_PARAMETER` table in the Advisors database, set `PARAM_VALUE` to `1440` for the `warehoused.metrics.max.minutes.kept` parameter. That is the result of 24 hours * 60 minutes per hour, for 1440 minutes.
   After XML Generator has been running for 24 hours, a newly opened graph would display the last 24 hours of values, with values spaced at least 12 minutes apart.

Procedure: Changing whether graphed values start at midnight

Purpose: To change the setting that determines whether graphs display values from the previous day.

Start of procedure

1. In the Advisors database, execute:
   ```
   UPDATE CONFIG_PARAMETER SET PARAM_VALUE = 'n'
   ```
   Where

   `PARAM_NAME = warehoused.metrics.start.at.midnight`

   For *n*, substitute your desired value. Legal values are '`true`' and '`false`'
2. Wait until the configuration parameter cache expires, and the value you set is loaded into the cache again.

3. From this point on, when you first open a graphemic value `false` it will not contain values whose times are from the previous day. In addition, open graphs will delete values from the previous day, when the time crosses midnight into the next day.

End of procedure

Deploying XML Generator Service

This section describes how to install the XML Generator service.

Note: The creation of linked servers may be required for either Cisco or Genesys installations.

For a Cisco installation, you will definitely need to link to the server containing the Cisco Intelligent Contact Management AW databases. These must exist before the Advisors installation can proceed.

For a Genesys installation, you may or may not have existing metrics databases. These will either be created during the subsequent Genesys Adapter installation(s), or will have already been created as part of earlier Genesys Adapter installation(s) (for example, for a previous version). The creation of linked servers is required only if the metrics databases exist or will be created on different SQL Server instances.

Deploying the XML Generator

If the option is selected on the `Module to Install` screen and you have installed the Platform, the `XML Generator` screen displays.

Procedure:
Deploying the XML Generator

Start of procedure

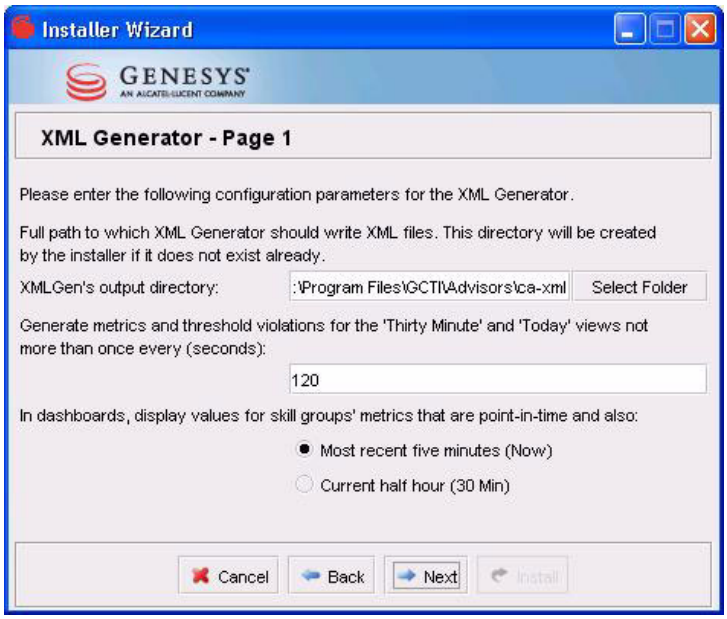


Figure 81: XML Generator Page 1

1. Enter XML Generator's output directory. If XML Generator must write to a drive accessible over the network, enter a path to the directory using the Uniform Naming Convention, which includes the host name and the name of the shared drive. For example:

   ```
   //host_name/shared_drive_name/root_directory_name/directory_1_name/
   directory_2_name
   ```

   You can use forward slashes in the name even on Windows systems. If you use back slashes, they must be escaped.

   ```
   \\\\host_name\\shared_drive_name\\root_directory_name\\directory_1_
   name\\directory_2_name.
   ```

2. Enter the interval for the `30-minute` and `Today` processing schedules. For example, if this parameter is set to 120 seconds, then XML Generator will store metrics and threshold violations for these two views no more often than that. However, XML Generator may store the view data less frequently depending upon load and the complexity of the configuration.
3. Select the time interval to be used for agent groups metrics on the dashboard; either `Now` or `30 Min`. This is a system-wide setting that will determine which agent-group metrics (other than point-in-time) are

displayed on the user Dashboard. If you choose `Now`, then the values are from the most recent five minutes. if you choose `30 Min`, then the values are from the current half hour.

4. Click `Next`.
   The `XML Generator Page 2` screen displays.

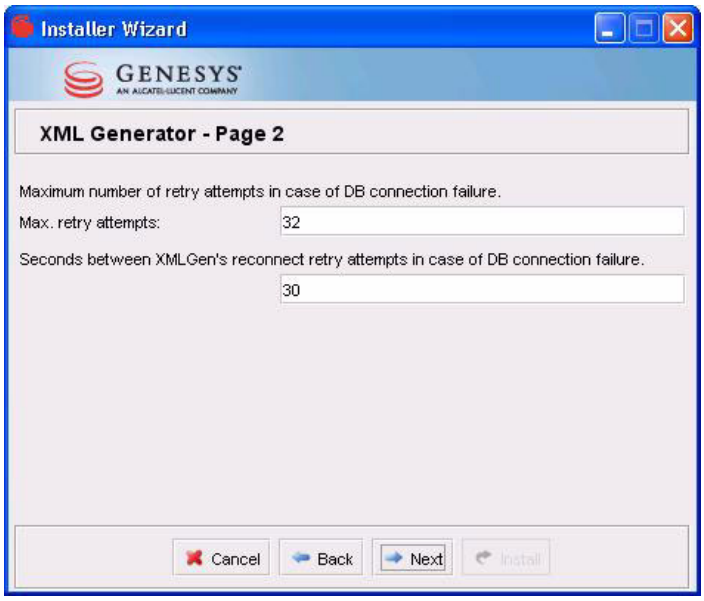


Figure 82: XML Generator Page 2

5. Enter the maximum number of retry attempts in the event of the database connection failure. This parameter governs retrying when XML Generator is already running, after establishing connections at startup.
6. Enter the number of seconds between Contact Center Advisor XML Generator's reconnection attempts in the event of the database connection failure. This parameter governs retrying when XML Generator is already running, after establishing connections at startup.
7. Click `Next`.
   The `XML Generator - Page 3` displays.

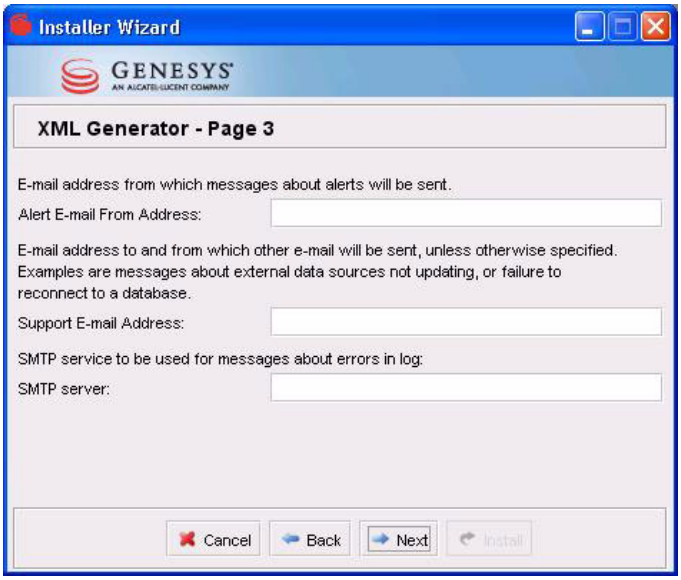


Figure 83: XML Generator - Page 3

8. Enter the e-mail address that will appear in the `From:` header in e-mail that XML Generator sends about alerts.
9. Enter the e-mail address to which XML Generator will send e-mail for support staff. An example is e-mail sent when XML Generator has not been able to connect to an external data source for a configurable number of minutes. This address will also appear in the `From:` header of these e-mails.
10. Enter the host name or IP address of the SMTP server that XML Generator will use to send e-mail with `ERROR` messages. You can also see these messages in XML Generator's log file.
11. Click `Next`.
    The data source installer screen is then displayed.

Figure 84: Data Source 1 Screen

12. For each data source not already in the database:
    a. Enter the database name (including the linked server name if applicable).
    b. Select the source type (Genesys or Cisco)
    c. (Optional) Enter the display name.
    d. Enter the threshold update delay.

    If you have additional data sources to add, select `Add another data source` and repeat this step. Up to five data sources may be added via the installer.
13. Click `Next`.
    The `Installation Progress` screen displays.
14. Click `Show Details`.
    The `Installation Progress` screen displays.
    The progress displays on the `Output` tab. Any errors display on the `Errors` tab.
15. Click `Install`.
    The progress displays on the `Output` tab. Any errors display in the `Errors` tab.

16. If no errors display, close the `Finished` popup. The `Output` tab displays "`Build Successful`" and the total time taken for the deployment, or, if errors display, diagnose them in the `Errors` tab. Delete the installation directory and, after diagnosis, reinstall it.

End of procedure

Note: Advisors Platform Database and Metric Graphing Database passwords used by XML Generator application are encrypted and saved in `..\GCTI\Advisors\conf\xmlgen-properties.xml`. To change the password see "Changing Encrypted Passwords After Installation" on page 76.

Notes for the Data Source Database Name

The data source database name must include the linked server name if the database is present on a different database server from that on which the Platform database is installed. See Chapter 4 on page 43.

For Cisco data sources:

- The linked server must point to the server that hosts the Cisco central ICM/IPCC database
- The database specified must be an AWDB database

Example Data Source Names

Example database name setting for a Genesys data source (if located on the same database as the Platform database):

```
advisors_gametrics
```

Example database name setting for a Cisco data source (using linked server `ICMCENTRAL` and AWDB named `name_awdb`):

```
ICMCENTRAL.name_awdb
```

Example database name setting for a Genesys data source where the linked server name contains special characters (this is for the case when the Genesys datasource database is located on a MSSQL server other than the Platform database):

```
[DS00001Primary-345].advisors_gametrics
```

JDBC Data Source Error Logging

CCAdv uses a third-party JDBC data source.

Procedure:
Reviewing JDBC data source error logs

Purpose:

To see the cause of errors reported by this data source in the log of XML Generator.

Start of procedure

1. Stop the XML Generator Windows service.
2. Edit `xmlgen/log4j.xml`.
3. Find the category for `com.mchange`.
4. Change the level to `DEBUG`.
5. Save the file.
6. Restart the XML Generator Windows service.
7. Examine the XML Generator log.

End of procedure

Custom Time Zones

Custom time zones can be configured for Workforce Advisor.

Procedure:
Configuring custom time zones

Start of procedure

1. Navigate to the `\conf` directory.
2. Create an empty file called `TimeZoneMapping.properties`.
3. Edit this file and enter the custom time zone mappings.

   For example;

   ```
   #This file contains time zone mappings to allow custom time zone
   names to be
   #translated to Java time zones
   #MyTimeZone = CST6CDT
   GENESYS = US/Eastern
   ```

   where `GENESYS` is the name of the custom time zone.

End of procedure

Workforce Advisor Web Service Option

If the `Workforce Advisor Web service` option is selected on the `Module to Install` screen, the `Workforce Advisor` screen displays.

Procedure: Deploying Workforce Advisor Web service

Start of procedure

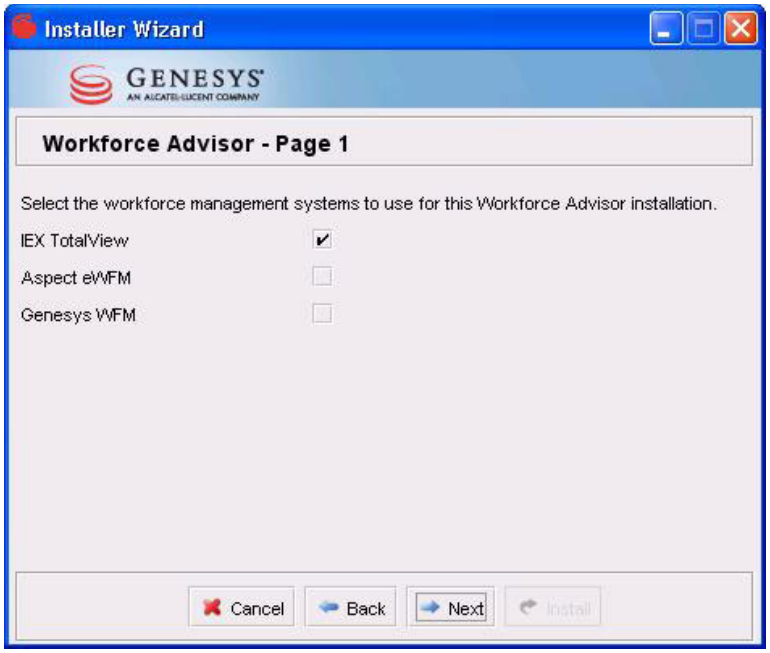


Figure 85: Workforce Advisor Screen 1

1. Select the sources of the workforce management data.
2. Click `Next`. The `Workforce Advisor - Page 2` displays (Figure 86 on page 155).

Figure 86: Workforce Advisor Screen 2

3. Select the time interval to be used for the display of agent group metrics on the Dashboard; either `Now` or `30 Min`. This is a system-wide setting that will determine how agent group metrics (other than point-in-time) are graphed on the user Dashboard.
4. Enter the `To` and `From` e-mail addresses for e-mail notifications.
5. Click `Next`.
   The `Workforce Aspect eWFM` screen displays.

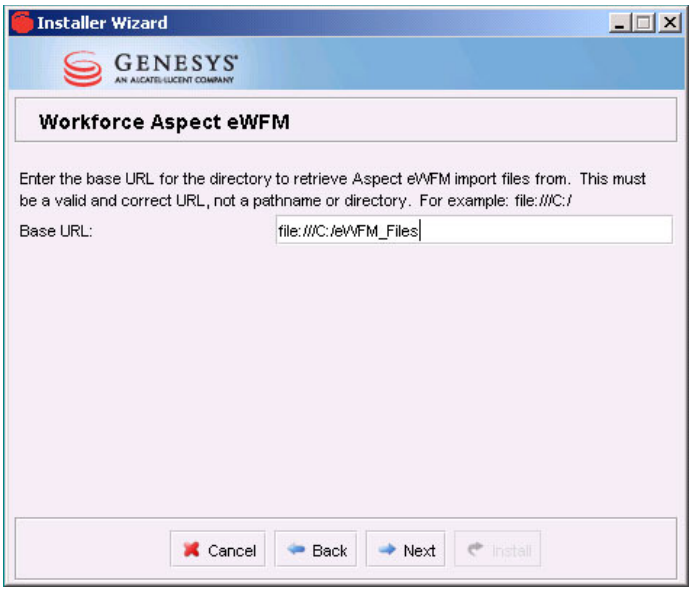


Figure 87: Workforce Genesys WFM Screen

6. Enter the Aspect eWFM base retrieval URL.
   The base retrieval URL should be `file:///`, followed by the location of the eWFM files. For Aspect eWFM, if the component must read or write data kept on a drive accessible over the network, then enter the pathname to the directory using the Uniform Naming Convention, which includes the host name and the name of the shared drive. For example;

   ```
   //host_name/shared_drive_name/root_directory_name/directory_1_name/directory_2_name
   ```

   You can use forward slashes in the name even on Windows systems. If you use back slashes, they must be escaped.

   ```
   \\\\host_name\\shared_drive_name\\root_directory_name\\directory_1_name\\directory_2_name.
   ```

7. Click `Next`.
   If Genesys WFM is selected, the Workforce Genesys WFM screen displays. If not, the `Installation Progress` screen displays and you can skip to Step 9.

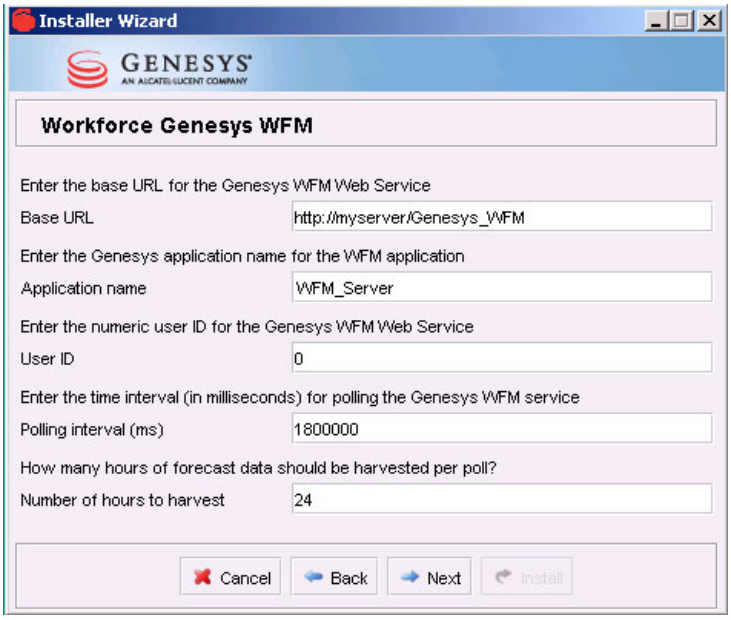


Figure 88: Workforce Genesys WFM Screen

8. Enter the Genesys WFM parameters:
   - `Base URL`
   - `Application name`
   - `User ID`—Use a specific user ID to identify the identity of the requests, or use `0` (zero) for user-less. It is used in the connection string to Genesys WFM for reference.
   - `Polling interval (ms)`
   - `Number of hours to harvest`

   Note: When using numerical IP v6 addresses, please enclose the literal in brackets.

Note: For Workforce Advisor installations connecting to Genesys WFM, the server running WA must be able to access your Genesys WFM installation.

To verify this access, from your WA server machine, ping the following locations:

1. The server name or IP address specified in your base WFM URL;
2. The host name of your Genesys WFM instance, as it appears in your WFM server's Configuration Manager application.

Your WA server must have access to all WFM servers in your WFM installation, each by its associated Configuration Manager host name.

9. Click `Next`.

   The `Installation Progress` screen displays.

10. Click `Show Details`.

    The `Installation Progress` screen displays. Installation progress displays on the `Output` tab. Any errors display on the `Errors` tab.

11. If no errors display, close the `Finished` popup.
    The `Output` tab displays the message `Build Successful` along with the total time taken for the deployment, or if errors display, you can diagnose them in the `Errors` tab. Delete the directory into which the installer has written product files and, after diagnosis, reinstall the files.

12. Mandatory step: After the installation is finished, remove the SQL Server installation script from the customer's environment.

End of procedure

Deploying the Genesys Advisors Browser

This section describes how to install and uninstall the Genesys Advisors browser.

Deploying the Genesys Advisors Browser

Procedure: Deploying the Genesys Advisors Browser

Start of procedure

1. With Microsoft Internet Explorer, open `http://home.genesysadvisors.local`.
   The installation automatically begins.

   Note: If the browser is installed on a machine other than the application server, then you must enter the IP address of the applications server.

2. If prompted, accept the installation of the ActiveX Control.
3. When prompted, click `Install`. The `Login` page is displayed.

4. Install, or download, or upgrade the Flash plug-in if required.

   Note: Since release 8.0, the Flash plug-in is not installed automatically in the Advisors browser installation procedure. The minimum required version is 9.0.124. If the plug-in is not present, a prompt is displayed when the browser is first launched.

5. If there are errors during installation, open `Windows Task Manager|Processes` and end any XULRunner processes (for example, `xulrunner.exe`) that are running by selecting the process, then clicking `End Task`.

End of procedure

Uninstalling the Genesys Advisors Browser

Procedure: Uninstalling the Genesys Advisors Browser

Start of procedure

1. Log out of the browser.
2. Close the browser. You cannot uninstall the browser while it is open.
3. Go to `Control Panel` and select `Add or Remove Programs`.
4. Highlight `Genesys <version>` and click `Change/Remove`.
5. To accept, click `Yes`.
6. Go to `C:\Documents and Settings\[USERNAME]\Application Data\Genesys` and delete the `Enterprise Advisor` folder.
7. Go to `C:\Documents and Settings\[USERNAME]\Local Settings\Application Data\Genesys` and delete the `Enterprise Advisor` folder.

End of procedure

Note: You can also use `C:\Program Files\Genesys\Advisor\uninstall.exe` to remove Genesys Advisors browser. This method deletes the folders mentioned in the steps in the procedure above.

Formatting Alert Messages Sent by Advisors

You can format the messages for threshold violation alerts and alerts about offline peripherals for Contact Center Advisor (CCAdv), as well as threshold violation alerts for Workforce Advisor (WA). You may want to shorten the text to accommodate the smaller screens of pagers.

The template files for message bodies are available after either XMLGen or WA is installed.

Note: If you format the CCAdv alert messages after deploying CCAdv, you must restart XMLGen.

If you format the WA alert messages after deploying WA, you must restart Geronimo.

The list of properties you could add with descriptive text appears in Table 7.

Table 7: Message Properties

Description	Property
A comma-separated list of distribution lists to which an e-mail about an alert was sent.	${distribution.list.names}
The name of the application group related to an element that caused the alert. There may not be one.	${application.group.name}
Alert types: Business, or Technical.	${alert.type}
The name of one contact center, possibly the only contact center, associated with the alert.	${call.center.name}
A list of comma-separated names of all contact centers associated with the alert.	${call.center.name.list}
The subject: an application in CCAdv, a contact group in WA and a peripheral.	${alert.element.name}
A metric's value. There might not be one.	${alert.value}
The display name of the metric whose threshold violation caused the alert. There may not be one.	${alert.metric.name}

Table 7: Message Properties (Continued)

Description	Property
The value entered on the System Configuration page, called "Threshold Trigger Delay Rate (minutes)" in that page. This may not be appropriate for some of these alerts. For example, a technical alert about a PG being offline is reported as soon as it is detected, not after a delay.	${alert.delay.minutes}
The alert's start date and time.	${alert.start.time}
How long the alert is/was active.	${alert.duration.minutes}
The alert's status: active or expired.	${alert.active.status}
The name of the geographic region related to the element that caused the alert. There may not be one.	${geographic.region.name}
The name of the reporting region related to the element that caused the alert. There may not be one.	${reporting.region.name}
Name of the operating unit related to the element that caused the alert. There may not be one.	${operating.unit.name}

To format alert messages, change any of the text in the template except the text between the brackets "{}".

CCAdv Message for an Alert Concerning a Threshold Violation

This is located in:

```
c:\advisors\conf\templates\AlertThresholdViolation_EmailTemplate.txt
Contact Center Advisor has detected the violation of a business alert
to which you are subscribed. You are receiving this alert because the
threshold below has remained outside the acceptable range for longer
than the defined time period of ${alert.delay.minutes} minutes.
This alert affects the Geographic Region ${geographic.region.name},
Reporting Region ${reporting.region.name}, Operating Unit
${operating.unit.name}, and the Contact Center:
{call.center.name.list}.
It involves the application ${alert.element.name} in the Application
Group ${application.group.name}.
Metric violated was: ${alert.metric.name}.
Current metric value: ${alert.value}.
Threshold violation was first detected at: ${alert.start.time}.
The alert has been active for: ${alert.duration.minutes} minutes.
The alert's status is: ${alert.active.status}.
```

CCAdv Message for an Alert Concerning an Offline Peripheral

This is located in:

```
c:\advisors\conf\templates\AlertOther_EmailTemplate.txt
Contact Center Advisor has detected the violation of a ${alert.type}
alert to which you are subscribed.
This alert affects the following contact center(s):
${call.center.name.list}.
It involves the element (peripheral/application/etc):
${alert.element.name}.
Alert was first detected at ${alert.start.time}.
Alert status: ${alert.value}.
The alert has been active for: ${alert.duration.minutes} minutes.
The alert's status is: ${alert.active.status}.
```

WA Message for an Alert Concerning a Threshold Violation

This is located in:

```
c:\advisors\conf\templates\AlertThresholdViolation_EmailTemplateWU.txt
Workforce Advisor has detected the violation of a business alert to
which you are subscribed. You are receiving this alert because the
threshold below has remained outside the acceptable range for longer
than the defined time period of ${alert.delay.minutes} minutes.
This alert affects the Geographic Region ${geographic.region.name},
Reporting Region ${reporting.region.name}, Operating Unit
${operating.unit.name}, and the Contact Center:
${call.center.name.list}.
It involves the contact group ${alert.element.name} in the Application
Group ${application.group.name}.
Metric violated was: ${alert.metric.name}.
Current metric value: ${alert.value}.
Threshold violation was first detected at: ${alert.start.time}.
The alert has been active for: ${alert.duration.minutes} minutes.
The alert's status is: ${alert.active.status}.
```

Changing the XML Generator Connection after Installation

For XML Generator you can change the database connection data after installation. The XML Generator file is:

- `conf/xmlgen_properties.xml`

To change the password see “Changing Encrypted Passwords After Installation” on page 76.

Deploying the XML Generator as a Service

Procedure: Deploying XML Generator as a service

Start of procedure

1. Run the Windows service as a user who has these permissions:
   a. Permission `Log In as a Service`. Services are installed to be run under the Windows local system account. This account is restricted from network I/O by Windows design.
   b. Permission to write to the directory on the network.
2. Either:
   - Navigate to the installation folder in Windows Explorer, then execute the file `[CCA Home]\XMLGen\InstallXMLGen.bat` (which completes this procedure);
   - Open a `Command` prompt window, and continue from Step 3.
3. Change the directory to XMLGen installation.
4. Run the command: `installXmlgen`.

End of procedure

Procedure: Removing XMLGen as a service

Start of procedure

1. Either:
   - Navigate to the installation folder in Windows Explorer, then execute the file `[CCA Home]\XMLGen\UnInstallXMLGen.bat` (which completes this procedure); `or;`
   - Open a `Command` prompt window, and continue from Step 2.
2. Change the directory to `XMLGen installation`.
3. Run the command: `uninstallXmlgen`.

End of procedure

Disabling Performance Monitor and the Workforce What-If Tool

By default, the Performance Monitor and Workforce What-If tool are enabled. To disable these features, run the following statement against the Contact Center Advisor database:

```
UPDATE [<schema-name>].[CONFIG_PARAMETER] SET PARAM_VALUE = 'false'
WHERE PARAM_NAME = 'enableSnapshot'
```

Configuring Contact Groups

Contact Groups' Filename

The prefix of the contact group's filename must remain the same before the first period in order for file updates to be accurate.

For example, `CPWU.20070307_2058.dat` must always begin with `CPWU`. The naming convention is:

`<system>.<group_id>[.<date>].*`

The date is optional and the ending can be anything (`.csv`, `.txt`, `.ewfm`).

The IEX source names and the eWFM source names must be unique.

Contact Group File's Header

Each file must have a header exported by the WFM system, so Workforce Advisor knows which metrics are present, and their order.

In a file from `IEX TotalView` the header records are as follows:

```
#fields:date|period|TZ|custID|saGroupID|saGroupName|ssGroupID|ssGroupNa
me|buID|buName|ctID|ctName|acdID|modify|fcstContactsReceived|fcstContac
tsHandled|fcstAHT|fcstSLPct|slPctObj|slTime|fcstOcc|maxOcc|fcstASA|asaO
bj|fcstReq|revPlanReq|commitPlanReq|schedOpen
```

```
#sort:date,period,TZ,custID,saGroupID,saGroupName,ssGroupID,ssGroupName
,buID,buName,ctID,ctName,acdID,modify,fcstContactsReceived,fcstContacts
Handled,fcstAHT,fcstSLPct,slPctObj,slTime,fcstOcc,maxOcc,fcstASA,asaObj
,fcstReq,revPlanReq,commitPlanReq,schedOpen
```

The `#sort` record is not necessary.

For Aspect eWFM, the forecast and staff groups are either in:

- One file (undistributed), or;

- Two files (distributed).

The header records are as follows:

- **Undistributed scenario**

  In the one file for both forecast and staff groups:

  ```
  PRI_INDEX,ROUTING_SET,START_TIME,STOP_TIME,HOUR,MINUTE,RVOL,RAHT,RSL,RDELAY SEC,SGRREQ,SGRSCH
  ```

- **Distributed scenario**

  In a file of metrics for forecast contact groups:

  ```
  PRI_INDEX,ROUTING_SET,START_TIME,STOP_TIME,HOUR,MINUTE,RVOL,RAHT,RSL,RDELAY SEC,SGRREQ,SGRSCH
  ```

  In a file of metrics for staff contact groups:

  ```
  PRI_INDEX,ROUTING_SET,START_TIME,STOP_TIME,HOUR,MINUTE,SGRSCH,SGRREQ,RDELAY SEC
  ```

Troubleshooting Installation Errors

Table 8 on page 165 describes parameter validation errors that you may encounter at the end of installation.

Table 8: Installation Error Messages

Error Message	Cause

`[java] Failed to connect to the database using connection URL:`
`[java]`
`jdbc:sqlserver://192.168.xx.yy:nnn;DatabaseName=ys_eadb;user=sa;password=very_secure_pwd;selectMethod=cursor`
`[java] The following exception was thrown:`
`com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnn has failed. Error: "Connection refused. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port.`
	Wrong database server name / IP address or port number

Table 8: Installation Error Messages (Continued)

Error Message	Cause
[java] Failed to connect to the database using connection URL: [java] jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=NotAPlatformDB;selectMethod=cursor;user=sa;password=very_secure_pwd [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnnn has failed. Error: "connect timed out. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port."	Wrong database name
[java] Exception while connecting: Login failed for user 'badUserId'. [java] url used: jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=ys_eadb;selectMethod=cursor;user=badUserId;password=very_secure_password	Wrong database user name or password

Chapter

10 Deploying Frontline Advisor

This chapter describes how to install Genesys Frontline Advisor Agent Advisor in a Microsoft Windows 2003 Server environment. It contains the following sections:

- Prerequisites, page 167
- Installation Overview, page 168
- Deploying Frontline Advisor, page 169
- Troubleshooting Installation Errors, page 177
- Starting the Frontline Advisor Service, page 178
- Verifying Server Connections, page 178

Prerequisites

See “Deployment Prerequisites” on page 15.

For each physical server on which you install a Web application (such as Frontline Advisor and Agent Advisor), Platform must be pre-installed.

Before deploying Frontline Advisor, you must have created a Frontline Advisor database. To do this, please see either:

- Chapter 2, “Creating a SQL Server Database,” on page 23, or;
- Chapter 3, “Creating an Oracle Database,” on page 37.

A verified Cisco environment must be ready and available if any of the agents have metrics provided by Cisco Adapter. Credentials with read access to the HDS and AW databases must be available when the Advisors Cisco Adapter Installer is run.

A verified Genesys environment must be ready together with a Genesys Adapter for Genesys installations.

If a mixed Genesys/Cisco environment is to be used, two instances of Frontline Advisor must be installed.

Installation Overview

This document describes how to install Genesys Frontline Advisor and Agent Advisor in a Windows 2003 Server environment. Note that version numbers in the final release may be different from those in the screen captures in this document.

Install Genesys Adapter if you are using a Genesys CTI installation. For Cisco installations, install the Cisco Adapter.

Installation Contents

The following files are shipped with the Frontline Advisor distribution:

MS SQL Server

- Frontline Advisor database script:
  - `fa-new-database-<version>.sql`
- Frontline Advisor installer:
  - `fa-server-installer-<version>.jar`
- Files in the `supplemental` folder:
  - `GeneratePermsStatements.sql`
  - `DropAllFADBObjects.sql`
  - `RemoveFAUsersFromFA.sql`
  - `CleanCmmConfigsAtFadb.sql`
- Files in the `migrations` folder:
  - `fa_mssql_ddl_3.1.sql`
  - `fa_mssql_initial_upload_3.1.sql`
  - `fa-database-migration-3.1-to-3.3.sql`
  - `fa-database-migration-3.3-to-8.0.sql`
  - `fa-database-migration-8.0-to-8.1.sql`
  - `fa-database-migration-8.1-to-8.1.1.sql`

Oracle

- Frontline Advisor database scripts:
  - `fa-<version>_Schema.sql`
  - `fa-<version>_TBS.sql`
  - `fa-new-database-<version>.sql`

FA Hierarchy and Configuration Server

In release 8.1.1, FA now read the hierarchy from the Genesys Configuration Server. Customers can configure which location/folder in the Configuration Server houses the hierarchy, and multiple folders can be chosen if the hierarchy is spread over many different folders or tenants.

If multiple folders are specified, FA creates a consolidated view of the hierarchy with a virtual enterprise node linking all the various hierarchies

together. The hierarchy in the Configuration Server consists of a tree of folders with the terminating nodes being *groups*, which in turn have *agents* as members.

These terms replace *supervisors*, *teams* and *agents* in previous versions.

Notes: Frontline Advisor automatically loads the hierarchy from the Genesys Configuration Server at startup and daily at 02:55 am.

Cisco Impact

For a pure Cisco environment, the hierarchy should be configured in the Configuration Server as it is done for a Genesys or mixed environment.

However, Cisco Adapter requires FA to send the Cisco `AgentSkillID` property to identify the agent while registering and issuing statistics. To accommodate this, the `AgentSkillID` must be added as an `Annex` property to each agent in the hierarchy.

The `ExternalID` attribute must set in the agent/person's `Annex` tab under the `Frontline Advisor` section, and the value of the `ExternalID` will be the `AgentSkillID` for the agent in the Cisco environment.

The hierarchy extractor will first try to extract the skill ID from the `Annex` section for a Cisco configuration. If the `ExternalID` property is undefined in the `Annex` section then it will extract the `EmployeeID` for the Genesys configuration.

Deploying Frontline Advisor

Procedure: Deploying Frontline Advisor

Purpose: To run the provided installer that gathers configuration information and installs the Frontline Advisor server as a Windows service.

Start of procedure

1. Run the installation jar file by either;
   - Using the command `java -jar fa-server-installer-<version>.jar`; or,

- Double-clicking the `fa-server-installer-<version>.jar` in the release bundle.

Notes: 1. Double-click does not work if only JDK is installed (that is, JRE is not present).

2. For 64-bit systems, if double-clicking to launch the installer, please ensure that the Java instance associated with the `jar` file type is 64-bit. Running the installer with a 32-bit Java instance will create a Windows service with the wrong executable.

2. The `Frontline Advisor Destination Directory` screen displays.

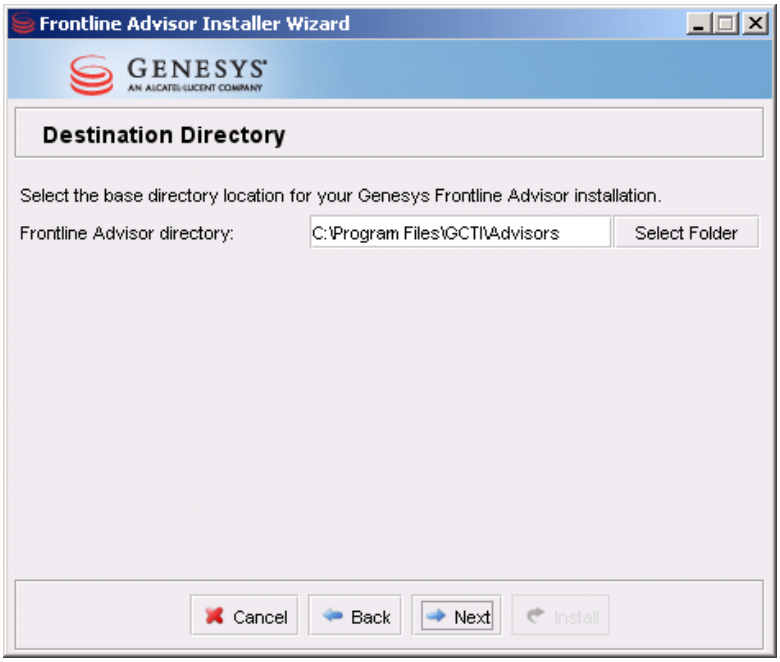


Figure 89: Frontline Advisor Destination Directory

3. Accept the default or install to a new location. The installation directory for Frontline Advisor server must be the same as the directory where Advisors Platform 8.1.x was installed.
4. Click `Next`.
5. The `Adapter Details` screen is displayed.

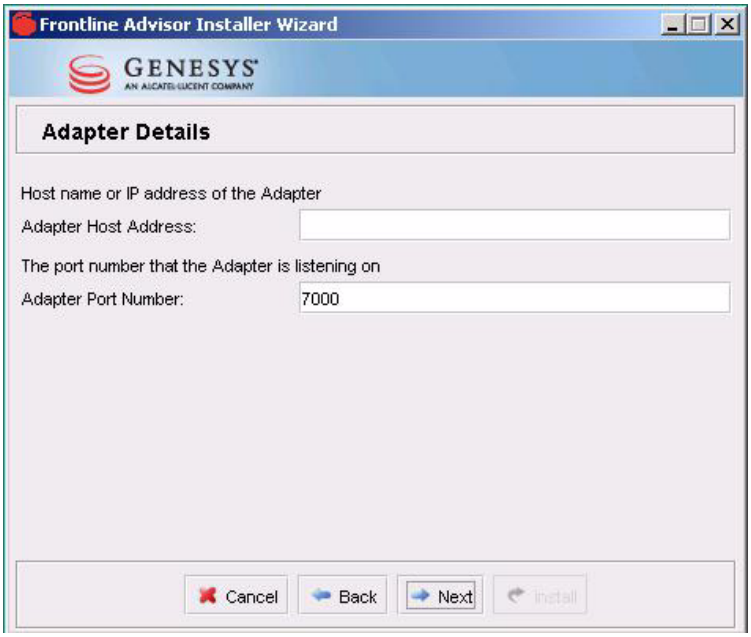


Figure 90: Adapter Details Screen

6. Enter the Adapter `Host Address` and `Port Number` details, then click `Next`. The `Hierarchy Source Details` screen displays.

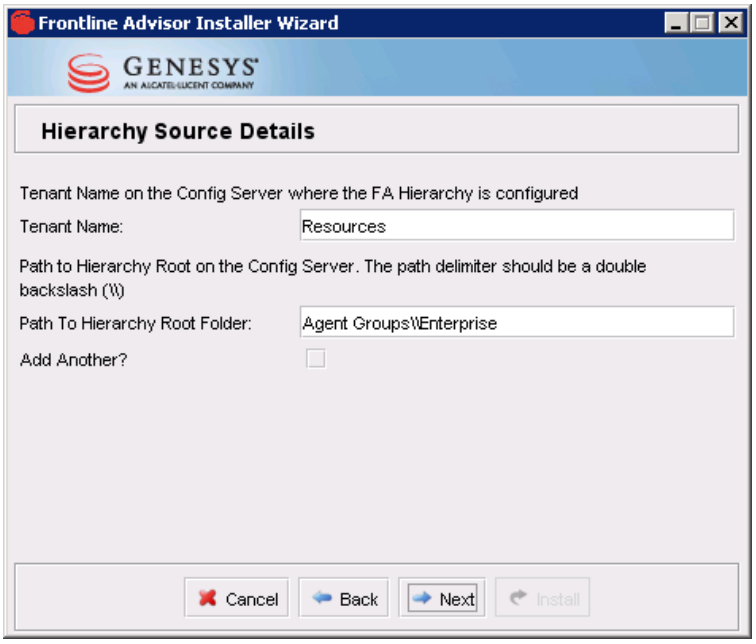


Figure 91: Hierarchy Source Details screen

7. Enter the name of the tenant in the Genesys Configuration Server in which the monitoring hierarchy resides, and the path to the hierarchy root folder.

   Note: In a Cisco environment, the path should look like: `Agent Groups\\<Your Cisco Group Name>`.

   If you need to add more than one tenant, check the `Add Another?` check box, and complete the required details.

8. Click `Next`. The `Database Type` screen displays.

   Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

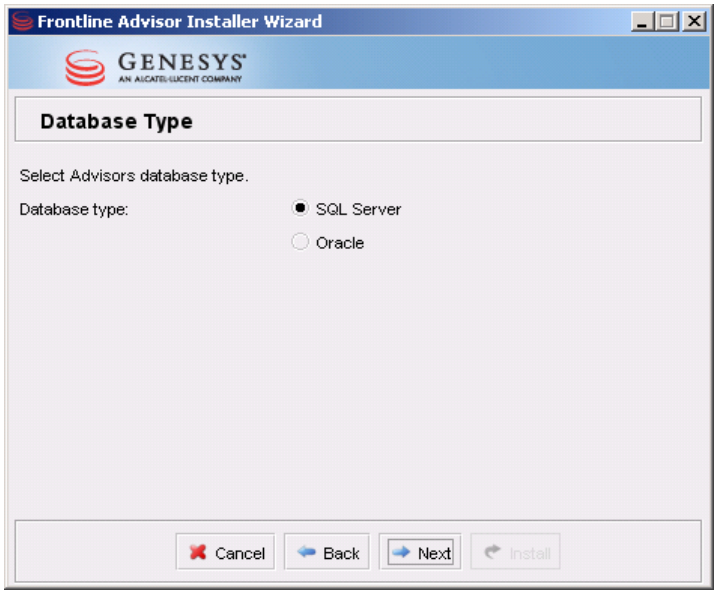


Figure 92: Database Type screen

9. Select the database type for this installation:
   - SQL Server
     Click `Next` and go to Step 10.
   - Oracle
     Click `Next` and go to Step 13

10. The `Genesys Advisor Platform Database` screen for MSSQL is displayed.

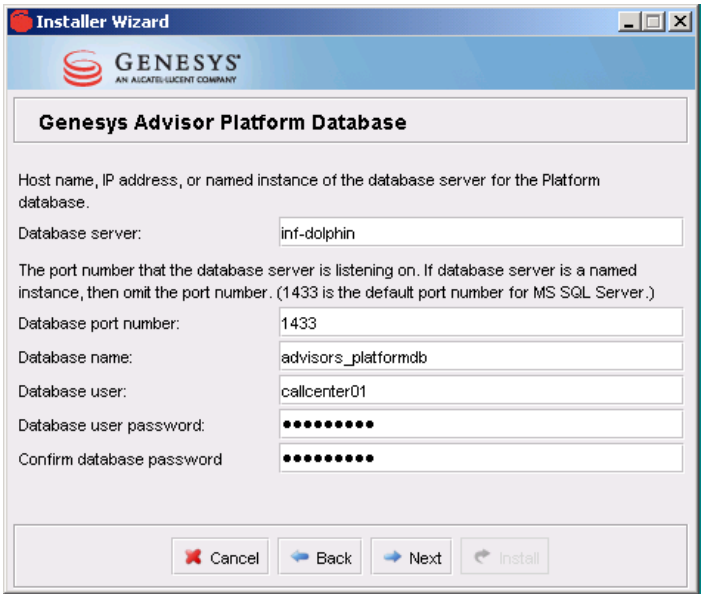


Figure 93: Genesys Advisor Database Screen for MSSQL

11. Enter the database connectivity parameters for the already created or upgraded database (that is, the database must be present and at the current version prior to running the installer). These parameters are server (machine), port number, name, user, and password.

> Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

If the database server is a named instance, then omit the port number. Click Next. The Frontline Advisor (FA) Database screen for MSSQL displays.

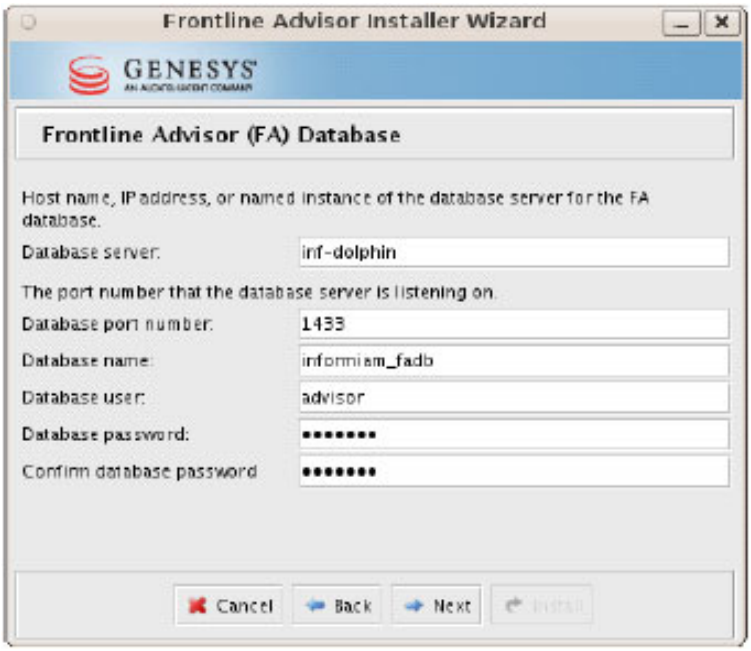


Figure 94: Frontline Advisor (FA) Database Screen

12. Enter the Frontline Advisor database connectivity parameters corresponding to those for the FA database:
    - Database server (machine): for example, `192.168.40.70`, or the host name of the machine where the Platform database is installed.

    > Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

    - Database port number: for example, `1433`
    - If the database server is a named instance, then omit the port number.
    - Database name: for example, `advisors_fadb`
    - Database user: for example, `advisor`
    - Database user password
    - Confirm database password

    Click `Next` and continue from Step 18.
13. The `Genesys Advisor Platform Database` screen for Oracle is displayed.

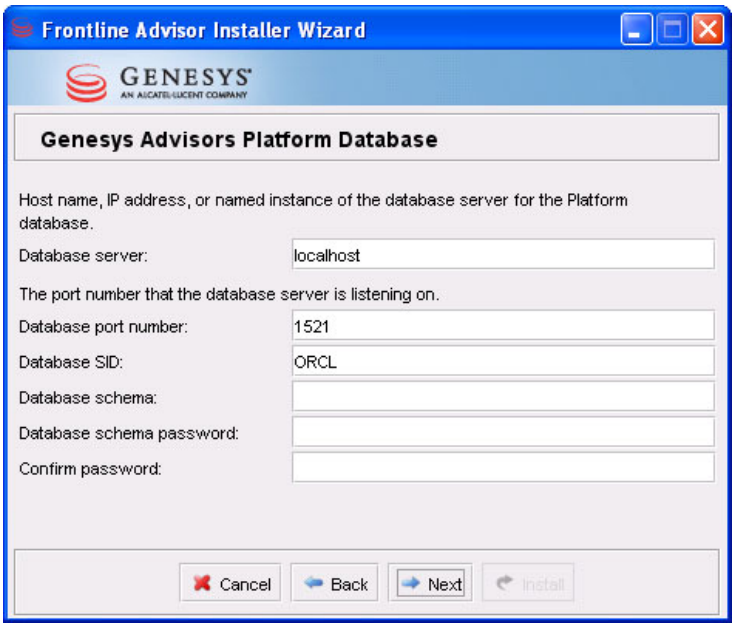
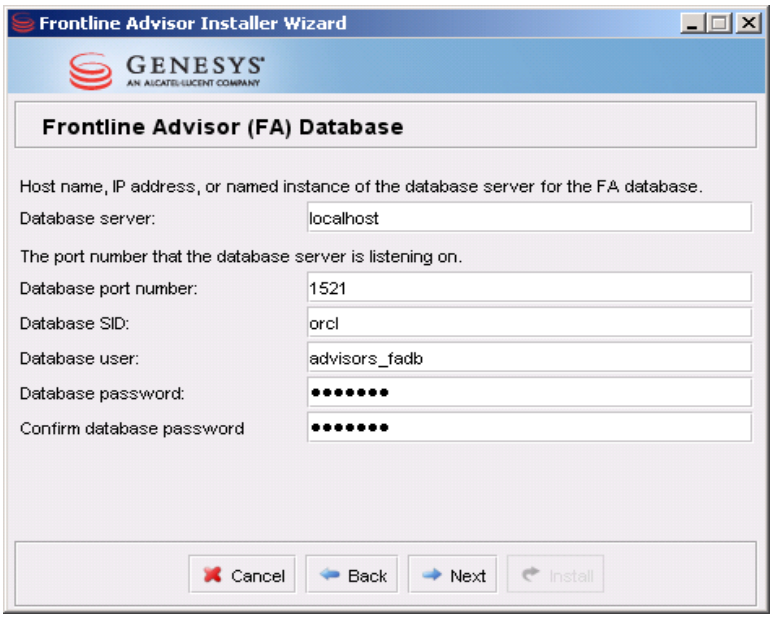


Figure 95: Genesys Advisors Platform Database Screen for Oracle

14. Specify the parameters for the Platform Oracle database:
    - `Database server`—The host name or IP address where the database server is running
    - `Database port number`—The database server's port number
    - `Database SID`—The database instance alias.
    - `Database schema` and `password`—The database schema and password created / used for the Platform database.
15. Click `Next`. The FA Database screen for Oracle displays.



16. Specify the parameters for the FA Oracle database:
    - `Database Server`—The host name or IP address where the database server is running

    Note: When using numerical IPv6 addresses, please enclose the literal in brackets.

    - `Database port number`—The database server's port number
    - `SID`—The database instance alias.
    - `Database user and password`—The database schema created / used for the FA database.

    Click `Next`.
17. The `Failure Notification Configuration` screen displays.

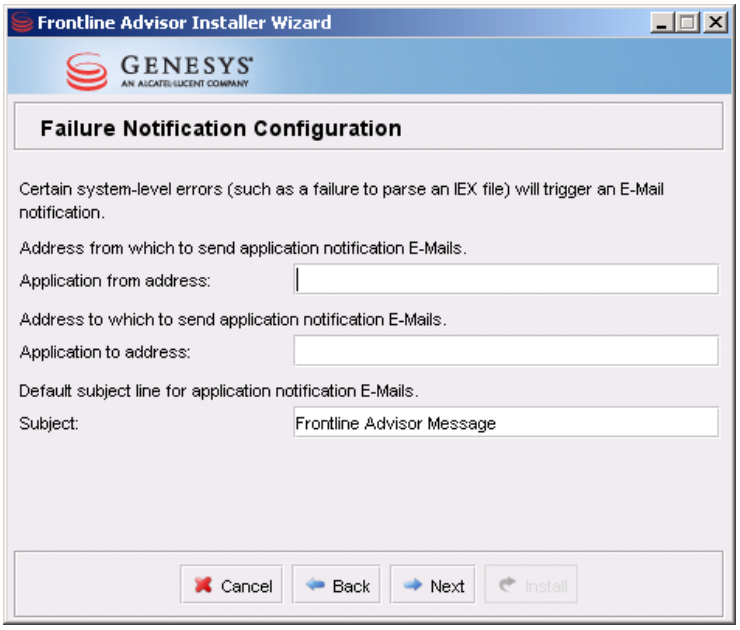


Figure 96: Failure Notification Configuration

18. Enter the e-mail parameters:
    - `Application from address`—For example, `faadmin@genesyslab.com`
    - `Application to address`—For example, `faadmin@genesyslab.com`
    - `Subject`—For example, `Frontline Advisor Message`
19. Click `Next`. The `Installation Progress` screen displays until the installation is complete.
20. After installation is complete, modify the Apache configuration file (`httpd.conf`) and add the following (if necessary) along with the other ProxyPass entries configured for Platform:

    ```
    ProxyPass /fa/ ajp://<FA hostname>:8009/fa/
    ```

Restart of Apache is then required.

End of procedure

Troubleshooting Installation Errors

The following are parameter validation errors that you may encounter at the end of installation:

Table 9: Installation Error Messages

Error Message	Cause
[java] Failed to connect to the database using connection URL: [java] jdbc:sqlserver://192.168.xx.yy:nnn;DatabaseName=ys_fadb;user=sa;password=very_secure_pwd;selectMethod=cursor [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnn has failed. Error: "Connection refused. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port.	Wrong database server name / IP address or port number
[java] Failed to connect to the database using connection URL: [java] jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=NotAPlatformDB;selectMethod=cursor;user=sa;password=very_secure_pwd [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnnn has failed. Error: "connect timed out. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port."	Wrong database name
[java] Exception while connecting: Login failed for user 'badUserId'. [java] url used: jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=ys_fadb;selectMethod=cursor;user=badUserId;password=very_secure_password	Wrong database user name or password

Starting the Frontline Advisor Service

Procedure:
Starting the Frontline Advisor Service

Start of procedure

1. Follow the Platform instructions to install the Windows service.
2. Each time the service is started, the Monitoring Hierarchy Loader runs.
3. Start the service and refresh a few times to make sure the service stays running.
4. Check the Platform log file if you experience problems. It may take up to 45 minutes to fully start depending on the number of agents and the complexity of the hierarchy.

End of procedure

Verifying Server Connections

Verifying the Frontline Advisor Server Connection

In your browser, type:

`http://<IP Address of FA Installation:8080/fa/com.informiam.fa.admin.gwt.AdminConsole/AdminConsole.html`

If the server is configured correctly and this is the first time you are logging in, the `Login` page displays. If this is not the first time you are logging in, the `Administration` page displays. You can exit from the Internet Explorer browser.

Verifying Apache Routing

Using a normal web browser to connect directly to the Apache server, log in and check the site. Use a URL that contains the host or IP address (and, optionally, the port if not on port 80) of the Apache server.

If configured correctly, the `Login` page displays. You can exit from the Internet Explorer browser.

Verifying the Genesys Advisor Browser Connection

To check the Frontline Advisor application, launch the Genesys Advisors browser, log in, and check the site.

Integrating External Links

To configure external links on the Manager Console and Agent Console, change the contents of the property file named `FrontlineAdvisor.properties` which is located in the Frontline Advisor installation directory under `C:\Program Files\GCTI\Advisors\conf`

In addition to setting the URL links, additional parameters can optionally be used:

- `user`
- `moduleId`
- `TeamId`
- `errorCode`

The links can be changed after starting Frontline Advisor. Frontline Advisor must be restarted in order to reflect the changes to the links.

The following are acceptable link-in URLs for Genesys Advisors.

- `informiam://[host]/?user=[user_login]&module=FAAgentConsole`
- `informiam://[host]/?user=[user_login]&module=FASupervisorConsole`
- `informiam://[host]/?user=[user_login]&module=FAAdmin`

The module in the URL represents the code value of each module in Frontline Advisor Agent Advisor module table. Those values might be passed out to an external application by the link-out URL parameters.

The user must enter a password to log in to the Genesys Advisors by link-in URLs.

The following is an example of an acceptable link-out URL that follows the URL template:

`http://somehost?user&moduleId&teamId&errorCode`

- `user`
  Filled in by the server when the user is authenticated.
- `moduleId`
  Retrieved from the Platform database (`MODULE` table) based on the application deployment URL (such as, `/fa/SupervisorConsole`) provided by the client that requests the link-out URL.

The DBA on the client site must put a job in place that truncates the `FA_Violations_Archive` table. This truncation should take place on a schedule defined by customer requirements.

Changing the Values at the Enterprise Node

The rules and thresholds are defined but disabled by default at the Enterprise level and cannot be removed from that level. Once the application starts up, these values can be changed and overridden at lower levels of the hierarchy for lower levels of control.

Chapter

11 Deployment Generics

This chapter describes some generic installation information applicable across multiple components. It contains the following sections:

- Automated Installation Options, page 181
- Installing Services under Windows 2008 Server, page 183
- Adjusting the Log File Roll and Retention Settings, page 184

Automated Installation Options

In addition to deploying Advisors modules by entering all properties in the installer UI screens (*normal* mode), two automated installation modes are also available: *semi-silent* and *silent.*

- Semi-silent mode pre-populates all values in the installer UI. The user will be able to review these values and make corrections if necessary.
- Silent mode is similar to semi-silent mode, except that no UI is displayed. Installation will proceed without confirmation, and will exit automatically with log output being written to file.

Specifying Input Properties

For both semi-silent and silent installation modes, all required properties for the installation options, including installation targets, passwords, and so on, must be present in a property file named `ant.install.properties`. This file must be located in the same directory from which the installer will be run.

An initial template can be generated by running the installer in normal mode, and then supplying values for the targets and other installation options. The installer will save these values (excluding passwords) in a file named `ant.userinstall.properties`. The input property file can then be obtained by copying this file to `ant.install.properties`, and then modifying the installation options as required for the specific configuration.

In order to reduce the risk of revealing sensitive information, password values are not written by the installer to the properties file. When the installer creates the `ant.userinstall.properties` file, password properties are created and commented out. For example:

```
#cp.database.password=
```

Once the `ant.userinstall.properties` file has been copied to `ant.install.properties`, you must locate the necessary password properties, uncomment them, and then add the actual password values. For example:

```
cp.database.password=supersecurepassword
```

Performing a Semi-Silent Installation

Semi-silent installation is enabled by running the installation jar with the `ant.install.properties` file present in the installer directory. No other changes are required.

Performing a Silent Installation

The silent installation mode is enabled by adding the `swing-auto` parameter when running an installation jar on the command line. For example, to perform a silent installation of an Advisors module, open a command prompt, navigate to the directory containing the installer jar, then run the following command (using the proper version number for "<version>"):

```
java -jar <advisor-module>-installer-<version>.jar swing-auto
```

Note: Note that the `ant.install.properties` file must be present in the same directory.

The installer will only create the logging directory when run in manual or semi-silent mode. If the installer is run in silent mode, or if the logging directory has been deleted after installation, the module will create the directory at startup.

For silent installation all the password properties must be provided and the password properties lines must be uncommented.

The installer will then run, using the values in the `ant.install.properties` file, and upon exit will indicate success or failure with a message and error codes. A successful installation will look similar to the following:

```
$ java -jar <advisor-component>-installer-<version>.jar swing-auto
Loading self extractor...
Install Successful.
```

A failed installation will look like the following:

```
$ java -jar <advisor-component>-installer-<version>.jar swing-auto
Loading self extractor...
Install Failed.
```

After the installer has been run, these additional files will be present containing log and installer output information:

```
ant.install.log
installation-output.log
```

In the case of installation failure, the `installation-output.log` file can be consulted for further information. (Possible reasons for failure include a missing input properties file, incorrect property values—for example, database passwords—or any other error that would cause a failure during normal installation mode.)

It is strongly recommended that you examine all generated logs to make sure that all errors and warnings are duly noted.

Advisor Component Names

Substitute the following for the `<advisor-component>` element above:

Table 10: Automated Install Naming Conventions

Component Name	Installer.jar Name
Platform	`advisors-platform`
Contact Center Advisor & Workforce Advisor	`ccadv-wa`
Frontline Advisor/Agent Advisor	`fa-server`
Genesys Adapter	`aga`
Cisco Adapter	`aca`

Installing Services under Windows 2008 Server

For installations on Windows 2008 Server, the Administrator installing the Advisors components and the Apache Web server should have permissions to install an NT service.

If for some reason granting this access is not possible, you can create shortcuts to the service installers that you may run as an Administrator.

To install the Platform Geronimo NT service, create a shortcut for the `InstallAdvisorsServer.bat` file.

To install the XMLGen NT service, create a shortcut for the `InstallXMLGen.bat` file.

To install Apache (including its NT service), create a short cut for the MSI installer.

Once you have created a shortcut, right click on the shortcut, and use the `Run as administrator` option to install the NT service for that component.

Adjusting the Log File Roll and Retention Settings

To limit the disk space consumed by log information, some Advisor components manage both the size and the number of its log files. These components will roll each of its current log files to backup copies both at the beginning of each day, and after the size of the log file reaches a threshold.

`Note:` This applies to CCAdv/WA (XML Gen), FA/AA, Genesys Adapter and Cisco Adapter.

You may adjust this size threshold as well as the number of backup copies retained by editing the properties in the `log4j.properties` file.

Procedure: Adjusting the log file roll & retention settings

Start of procedure

1. Navigate to your base Advisors directory, and then to the `conf` subdirectory.
2. Look for the following properties and for each log file adjust them appropriately:
   - `MaxFileSize`—Sets the size threshold past which the appender will roll the current file. Specify an integer value, along with either `KB` or `MB` (for example, `10MB` for ten megabytes).
   - `MaxRollFileCount`—Sets the maximum number of backup copies retained.

- `ScavengeInterval`—If set to `-1`, `MaxRollFileCount` will be ignored, and all backup copies will be retained.

End of procedure

Notes: Please note the following:

- `MaxFileSize` does not set a hard limit on the maximum size for the associated log file, but rather represents a threshold past which the log file is subject to rolling. The actual size of a log file will depend upon system load and the volume of log entries.
- If you choose to set `ScavengeInterval` to `-1`, you will need to manually clear the backup copies from the log directory on a periodic basis.

Related Documentation Resources

The following resources provide additional information that is relevant to this software. Consult these additional resources as necessary.

Performance Management Advisors

- *Performance Management Advisors 8.1 Contact Center Advisor & Workforce Advisor Administrator User's Guide* describes how to configure your enterprise hierarchy and set up threshold rules/goals and users.
- *Performance Management Advisors 8.1 Contact Center Advisor Help* describes how to personalize your display of information for monitoring and root cause analysis.
- *Performance Management Advisors 8.1 Workforce Advisor Help* describes how to personalize your display of information for monitoring and root cause analysis.
- *Performance Management Advisors 8.1 Frontline Advisor Administrator User's Guide* describes how to perform administration functions for Frontline Advisor.
- *Performance Management Advisors 8.1 Frontline Advisor Manager Help* describes how to perform manager functions for Frontline Advisor.
- *Performance Management Advisors 8.1 Frontline Advisor Agent Advisor Help* describes how to perform agent functions for Frontline Advisor.
- *Performance Management Advisors 8.1 Alert Management Help* describes how to manage the actions taken to resolve alerts and use the database to learn and repeat successes.
- *Performance Management Advisors 8.1 Resource Management Help* describes how to maintain skill levels and agents.
- *Performance Management Advisors 8.1 Performance Monitor Help* summarizes how to personalize your display of information for monitoring.

- *Performance Management Advisors 8.1 Workforce What-If Tool Help* describes and gives examples of scenarios that illustrate how to adjust resource levels to achieve optimal outcomes.

Genesys

- *Genesys Technical Publications Glossary,* which ships on the Genesys Documentation Library DVD and which provides a comprehensive list of the Genesys and computer-telephony integration (CTI) terminology and acronyms used in this document.
- *Genesys Migration Guide*, which ships on the Genesys Documentation Library DVD, and which provides documented migration strategies for Genesys product releases. Contact Genesys Technical Support for more information.
- 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*

Consult these additional resources as necessary:

- *Genesys Hardware Sizing Guide,* which provides information about Genesys hardware sizing guidelines for Genesys releases.
- *Genesys Interoperability Guide,* which provides information on the compatibility of Genesys products with various Configuration Layer Environments; Interoperability of Reporting Templates and Solutions; and GPlus Adapters Interoperability.
- *Genesys Licensing Guide,* which introduces you to the concepts, terminology, and procedures relevant to the Genesys licensing system.

For additional system-wide planning tools and information, see the release-specific listings of System Level Documents on the Genesys Technical Support website, accessible from the system level documents by release tab in the Knowledge Base Browse Documents Section.

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.

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:

81fr_ref_06-2011_v8.1.001.00

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

Screen Captures Used in This Document

Screen captures from the product graphical user interface (GUI), as used in this document, may sometimes contain minor spelling, capitalization, or grammatical errors. 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.

Type Styles

Table 11 describes and illustrates the type conventions that are used in this document.

Table 11: Type Styles

Type Style	Used For	Examples
Italic	• Document titles • Emphasis • Definitions of (or first references to) unfamiliar terms • Mathematical variables Also used to indicate placeholder text within code samples or commands, in the special case where angle brackets are a required part of the syntax (see the note about angle brackets on page 190).	Please consult the *Genesys Migration Guide* for more information. Do *not* use this value for this option. A *customary and usual* practice is one that is widely accepted and used within a particular industry or profession. The formula, $x+1=7$ where *x* stands for . . .

Table 11: Type Styles (Continued)

Type Style	Used For	Examples
Monospace font (Looks like `teletype` or `typewriter text`)	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. • Code samples. Also used for any text that users must manually enter during a configuration or installation procedure, or on a command line.	Select the `Show variables on screen` check box. In the `Operand` text box, enter your formula. Click `OK` to exit the `Properties` dialog box. T-Server distributes the error messages 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. Enter `exit` on the command line.
Square brackets ([ ])	A particular parameter or value that is optional within a logical argument, a command, or some programming syntax. That is, the presence of the parameter or value is not required to resolve the argument, command, or block of code. The user decides whether to include this optional information.	`smcp_server -host [/flags]`
Angle brackets (< >)	A placeholder for a value that the user must specify. This might be a DN or a port number specific to your enterprise. **Note:** In some cases, angle brackets are required characters in code syntax (for example, in XML schemas). In these cases, italic text is used for placeholder values.	`smcp_server -host <confighost>`

Index

Symbols

[] (square brackets) . . . 190
< > (angle brackets) . . . 190

A

Adapters . . . 135, 168
alert messages . . . 160
angle brackets . . . 190
Apache . . . 86
Apache Server . . . 15
Aspect eWFM . . . 155
audience, for document . . . 10
automated installation . . . 181
Avaya Communication Manager . . . 86

B

brackets
  angle . . . 190
  square . . . 190
browser co-residency . . . 21

C

Cisco Adapter Web services . . . 123
Cisco data source configuration . . . 124
Cisco data source server configuration . . . 126
Cisco ICM database . . . 147
commenting on this document . . . 10
contact groups . . . 164
conventions
  in document . . . 189
  type styles . . . 189
creating linked servers . . . 147

D

deploying Cisco Adapter . . . 121
document
  audience . . . 10
  conventions . . . 189
  errors, commenting on . . . 10
  version number . . . 189

E

email templates . . . 21

F

Flash player . . . 15
font styles
  italic . . . 189
  monospace . . . 190
Frontline Advisor database configuration . . . 129

G

Geronimo . . . 86

I

installation errors . . . 182
installation prerequisites
  prerequisites, installation . . . 136, 167
installation troubleshooting . . . 165
intended audience . . . 10
Interaction Server . . . 87
italics . . . 189

J

Java Development Kit installation 143
JDK installation 15
JVM path options 86

L

linked servers 147

M

manual installation 88
MCR extension package 86
metric graphing database 139, 142
Microsoft SQL Server 2008 15
Migrations folder 168
monospace font 190
multiple Adapter core services on a server . 116

O

option query-agent-work-mode 86
option rebind-delay 87
Oracle 11g 15

P

prerequisites 136

R

reconnection 149
reconnection attempts 149

S

semi-silent installation 181, 182
silent installation 181, 182
SQL Server 15
square brackets 190
Stat Server 86
Supplemental folder 168

T

troubleshooting 182
type styles
  conventions 189
  italic 189
  monospace 190
typographical styles 189

V

version numbering, document 189
virtual agent groups 88

W

Workforce Advisor e-mail notifications 155
workforce management data 154

X

XML Generator installation 147