



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Performance Management Advisors Deployment Guide

Pulse Advisors 8.5.0

Table of Contents

Genesys Performance Management Advisors Deployment Guide	5
Planning	6
Deployment Summary	8
Prerequisites	10
Additional Resources	48
Create the Advisors Databases	49
Creating a SQL Server Database	51
Creating an Oracle 11g Database	61
Configure Oracle 11g Metrics Data Sources	67
Database Secure Deployment	71
Create the Advisors User Account	74
Create the Data Manager Base Object Configuration User	80
Deploying Advisors	82
Deploying Advisors Platform	83
Deploying Genesys Adapter	97
Deploying Cisco Adapter	115
Deploying CCAdv and WA	124
Work with XML Generator	134
Upgrade CCAdv-ME	138
Deploy Smartphone Client Applications	139
Deploying FA	140
Deploying SDS and RMC	146
Automated Installation Options	154
Post Installation Configuration	157
General	158
High Availability for Performance Management Advisors	159
Change Memory Allocation	163
Change Encrypted Passwords	165
Customize the Advisors Interface	166
Correct Login Page Latency	167
Deploy and Configure Apache	168
Change a JDBC Data Source Configuration	172
Schedule Periodic Statistics Reissue	174
Adjust the Log File Roll and Retention Settings	175
Advisors Platform	178

Change Advisors Cluster Membership	179
Configure Administrative Actions Logs	180
Change the Mail Server Configuration	182
Advisors Genesys Adapter	183
Operation of Stat Server Redundant Pairs	184
Stat Server Load Balancing	185
Re-distribute Stats Load when Adapters are Added	186
AGA Configuration Parameters	187
Stat Server Configuration Parameters	191
Update AGA Properties in the Database	192
Manage Restart of Multiple Adapters with Single Metrics Database	193
CCAdv and WA	194
Enable and Disable Agent-level Monitoring	195
Configure Metric Graphing Properties	197
Configuring Forecast Metric Graph Shapes	200
Work with Data Source Database Names	201
JDBC Data Source Error Logging in XML Generator	202
Custom Time Zones	203
Change the Time Profile of Agent Groups Metrics from 5 Minute Sliding to 30 Minute Growing	204
Format Alert Messages sent by Advisors	205
Importing Contact Groups into Advisors	210
Bulk Configuration Overview	220
CCAdv/WA Bulk Configuration – Integrated Mode	221
CCAdv Bulk Configuration – Independent Mode	232
WA Bulk Configuration – Independent Mode	241
FA and AA	252
Verify Server Connections	253
Configure the Reason Code Statistic Key	254
Enabling and Editing Filtered Metrics	255
Features Overview	260
Discontinuation of the Advisors Browser	261
Multiple Advisors Deployments on One System	262
Advisors Platform and the Backup Configuration Server	265
Data Manager	266
Adapter Stat Server Configuration	276
Establishing a TLS Connection to Genesys Configuration Server	277
Scaling the System to Increase Capacity	281

Advisors Cluster Information	283
Encryption for AGA Metrics Database Data (Oracle)	284
LoggedIn Scripts	285
FA Message Listening Port	286
Providing a User Interface for Users with Visual Impairment	287
Contact Center Advisor Mobile Edition	288
Advisors Software Distribution Contents	293
Migration Utilities	305
User Migration Utility	306
Object Migration Utility	307

Genesys Performance Management Advisors Deployment Guide

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

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

Planning

This page contains information to help you prepare to deploy Genesys Performance Management Advisors. Also, before you deploy Advisors, ensure you read the [Prerequisites](#) topic. It provides information to help you prepare for your deployment.

General Information about Advisors

Starting in release 8.5.0, the Advisors dashboards are accessed using a commercial browser, such as Mozilla Firefox. Advisors 8.5.x is incompatible with the old Advisors browser.

The installation process has several distinct sections 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.

Advisors requires the Genesys Configuration Server to be present, along with all its supporting components.

NEW Starting in release 8.5.0, you must deploy the Contact Center Advisor application (including XML Generator) and configure one or more Genesys metric data sources to use the Genesys **Base Object Configuration** page in the Administration module. Data manager requests no statistics for pre-configured objects until the CCAAdv module, XML Generator, and Genesys metric data sources are deployed and working.

About Advisors Applications

The following Table shows the dependencies amongst Advisors components. For each Advisors product in the Application column, the Table identifies any additional Advisor component that must be installed with it. See also [Prerequisites](#) for detailed information, as well as information about databases required for each component.

Application	Requires these Components on the Same System	Requires these Components within the Same Advisors Deployment
Frontline Advisor	Advisors Platform	Advisors Genesys Adapter or Advisors Cisco Adapter
Contact Center Advisor	Advisors Platform	Advisors Genesys Adapter in a Genesys environment
Workforce Advisor	Advisors Platform	Contact Center Advisor

Application	Requires these Components on the Same System	Requires these Components within the Same Advisors Deployment
Contact Center Advisor – Mobile Edition	Advisors Platform	Contact Center Advisor
Resource Management Console	Advisors Platform Supervisor Desktop Service	Contact Center Advisor

Deployment Summary

The basic sequence of events when deploying Genesys Performance Management Advisors is shown below. This sequence is repeated throughout the book to help you understand where you are in the deployment process.

Order of installation

1. Install the databases that correspond to the Advisors products you will deploy:
 - a. Advisors Genesys Adapter metrics database
 - b. Advisors Platform database
 - c. Advisors Cisco Adapter database (if you use ACA)
 - d. Metric Graphing database
2. Create the Advisors User and the Object Configuration User accounts.
3. Install the Platform service (Geronimo) on all servers on which you will deploy one of the following Advisors components:
 - Contact Center Advisor web services or XML Generator
 - Workforce Advisor web services or server
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. Install the Advisors components for your enterprise:
 - Contact Center Advisor
 - Workforce Advisor
 - Contact Center Advisor - Mobile Edition
 - Frontline Advisor
 - SDS and Resource Management

Genesys recommends that you test each deployed application immediately after you install it before proceeding to subsequent application deployments. For example, before you deploy Workforce Advisor, run XML Generator to import data and perform a small test with Contact Center

Advisor to ensure it is working.

6. Make any required configuration changes.

Prerequisites

NEW This page describes what you must do before you deploy Genesys Performance Management Advisors. Read all prerequisites relevant to the applications you will deploy before you begin installation.

The tabs below provide general information about the deployment environment, as well as information specific to each application. There is a list of questions to consider for each application. There are also Tables in which you can input data for your environment. Use the data in these Tables as a reference guide when you deploy each application.

<tabber>

General=

Importance of Advisors Platform

Each Performance Management Advisor application (such as dashboards, the System Administration module, the Workforce Web Service, and the XMLGen application) requires the installation of Advisors Platform before installation of the application. Each application relies on Advisors Platform to function.

It is very important that you enter complete information on all installation screens when deploying Advisors Platform to ensure correct functionality in the applications.

The Platform installation file installs the following base services:

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

Environmental Requirements

Before you deploy Genesys Performance Management Advisors, ensure you provide – or can provide –

the following operating environment.

Networks

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

Operating systems

You can deploy Performance Management Advisors on Microsoft Windows or, starting in Release 8.5.0, on Red Hat Linux (64-bit applications running on a 64-bit operating system). The installation of the Advisors products on a Red Hat Linux server differs from the installation of those same products on a Windows operating system. See [Deploying Advisors](#) for procedures.

For information about operating system versions compatible with your Advisors release, see [Genesys Supported Operating Environment Reference Guide](#) and [Genesys Interoperability Guide](#).

Software

The following external software must be installed on the appropriate physical computer involved in Advisors installation:

- Java Development Kit (JDK)
- Apache HTTP Server
If the Apache server is installed on the same machine as Advisors Platform, the Apache server must use a port other than 8080 (which is used by Advisors Platform). In most cases, Apache will be able to use port 80.

Client Software

You must install the Flash player plug-in for non-IE browsers (for example, Firefox) on each user's desktop or laptop that runs the Advisors user interface.

Databases

You require the following databases in an Advisors installation, dependent on the Advisors applications you install:

- Advisors Platform database – Required for all applications.
- Advisors Cisco Adapter database – For Cisco installations only.
- Advisors Genesys Adapter metrics database – Required for AGA, CCAdv, and WA.
- Advisors metrics graphing database – Required for Contact Center Advisor and Workforce Advisor. All components of those products require it (Web services and Web server/XML Generator).

NEW In a situation where CCAdv/WA is deployed on one Platform cluster and FA is deployed on another Platform cluster, Genesys recommends that you use a separate Platform database per cluster; the Platform server clusters should not share a Platform database in this situation.

When the various types of Platform server clusters share one Platform database, those servers are sharing the same Data Manager configuration – especially the Adapter pool configuration that is present in the Platform database – and this can lead to service interruptions when one service is restarted.

If it is absolutely necessary to have the various Platform server clusters for each application share one Platform database, ensure the Administration workbench is installed with only one of the Platform installations. The Advisors Platform installation file gives you the option to install this component. As part of your planning, you should decide on which Platform server you will install the Administration workbench.

You cannot mix database types within an Advisors installation; each installation must be either wholly MS SQL or wholly Oracle. Advisors supports one of the following for databases:

- Microsoft SQL Server 2005 or Microsoft SQL Server 2008. Genesys recommends that you use MS SQL Server Enterprise Edition for optimal performance, although Standard Edition is also supported. You can install the metric graphing feature with or without the MS SQL Server partitioning feature. The partitioning feature provides flexibility and can improve performance; partitioning has more options than non-partitioning for organizing the metric graphing data that comes from Workforce Advisor and Contact Center Advisor. You must use MS SQL Server Enterprise Edition if you plan to install metric graphing and use partitioning. MS SQL Server Standard Edition does not support the partitioning feature. If you use MS SQL Enterprise Edition, but you do not use partitioning, you can use the script(s) from `\sql\mssql-standard`.
- Oracle 11g. You can install the metric graphing feature with or without the Oracle database partitioning feature. The partitioning feature provides flexibility; partitioning has more options than non-partitioning for organizing the metric graphing data that comes from Workforce Advisor and Contact Center Advisor. Ensure you have Oracle Database Enterprise Edition with the partitioning option if you plan to install metric graphing and use partitioning. If you use Oracle database software that includes the partitioning feature, but you do not use partitioning, you can use the scripts from `\sql\oracle-without-partitions`. Advisors support connection to Oracle Real Application Clusters (RAC).

If using Oracle, you also require the appropriate Oracle JDBC driver. You can obtain the driver from Oracle's website, www.oracle.com. Advisors requires versions compatible with supported JDK versions. (Drivers containing tracing code or compiled with the `-g` option are not necessary.) See the [Genesys Supported Operating Environment Reference Guide](#) for supported versions of JDK and Oracle JDBC drivers.

Database Management Tools

Genesys recommends the following tools to manage Advisors database operations:

- Oracle: SQLPlus
- Microsoft SQL Server: Microsoft SQL Server Management Studio

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.

Linked Servers

The creation of linked servers might be required for either Cisco or Genesys installations.

For a Cisco installation, you must link to the server containing the Cisco Intelligent Contact Management (ICM) Distributor Admin Workstation (AW) databases. These must exist before the Advisors installation can proceed.

For a Genesys installation, you might have existing metrics databases. These are either created during the Advisors Genesys Adapter installation(s), or have already been created as part of earlier Genesys Adapter installation(s) (for example, for a previous version). The creation of linked servers in a Genesys environment is required only if the metrics databases exist, or will be created, on different SQL Server instances.

System clocks

You must synchronize the system clocks of all physical servers used in a given Advisors installation with a central time server.

| - | Advisors Platform =

Before you deploy Advisors Platform, it is helpful to answer the following questions:

- Will you deploy Advisors Platform on a Linux Red Hat or a Windows platform?
- Is there a need to have two distinct Advisors deployments on one system?
- On which server will you install the Advisors Administration module? The Administration module must be installed with at least one of the components of Advisors.
- Will you install the applications (FA, CCAdv, WA) in standalone or distributed mode? To administer each application, you must install the Administration workbench with at least one instance of the application. If you are installing Advisors Platform to support a clustered Advisors suite server, on which system in the cluster will you install the Administration module (workbench)?
- Where are you installing Advisors (in which directory)? The default location is `C:\ProgramFiles\GCTI\Advisors`. If you do not create the directory before deployment, you can create it as part of the deployment process.
- Do you want applications to send e-mail notification messages? From what address will an application send notifications (for example, `DONOTREPLY@<your enterprise>.com`)? To what e-mail address will an application send notifications?
- Which language(s) will be used for email notifications from the system? (Advisors supports English and German in release 8.5.0.)
- Each server on which you install Platform requires a unique cluster node. What will you use for node

IDs?

- Will you connect to the Genesys Configuration Server using TLS?
- Do you want update events from the Configuration Server to update the Advisors database with the new information (that is, do you want to synchronize user updates between Configuration Server and the Advisors database)? If yes, which instance of Advisors Platform will maintain the synchronization (in a clustered environment, a single Platform instance must be designated as responsible for maintaining the user account synchronization)?

Prerequisites

Ensure you have completed all the tasks in the following Table before you begin Advisors Platform deployment.

Y or N	Prerequisite
	If you use Genesys Framework, a verified Genesys environment must be ready and available. In a Genesys environment, you have established connection to the Genesys Configuration Server.
	You have initialized databases—databases must be present and at the current version prior to running the installation files. You have configured accounts that can be used by applications to access the databases.
	Each application server and its associated database are in the same time zone, and the time is synchronized. (The client can be in a different timezone.)
	You have configured the Advisors User account in the Genesys Configuration Server. For more information see Creating the Advisors User .
	You have configured the Object Configuration User in the Genesys Configuration Server. For more information, see Data Manager .
	You have installed JDK on the server on which you will be deploying Advisors Platform.
	If you plan to connect to the Configuration Server using TLS, you have configured a secure port for Genesys Configuration Server. For more information, see Genesys 8.1 Security Deployment Guide .
	If you plan to connect to the Configuration Server using TLS, you have configured security certificates: <ul style="list-style-type: none"> • You have configured the security providers and issue security certificates. For more information, see Genesys 8.1 Platform SDK Developer's Guide. • You have assigned a certificate to the Configuration Server host in Configuration Manager. For more information, see Genesys 8.1 Security Deployment Guide.
	On the system on which you are installing Advisors Platform, you have set the Regional and Language options to the locale for which you want the servers to be deployed.
	If you are going to use two different deployments of Advisors on the same machine, then you have chosen different values for the port numbers that each deployment will use. See Multiple Advisors Deployments on One System .
	You have located the <code>advisors-platform-installer-<version>.jar</code> file on the installation CD and have copied it to the local drive of your server.
	If you use Management Framework 8.1.x in your enterprise and you will allow users to modify their Advisors login password, you have changed the following two options in Management Framework to <code>true</code> to avoid potential lockouts:

Y or N	Prerequisite
	<ul style="list-style-type: none"> the no password change at first login option the override password expiration option <p>For information about the no password change at first login and override password expiration options, see Genesys Framework 8.1 Configuration Options Reference Manual.</p> <div> <p>Important</p> <p>After you install the Advisors applications, you must also ensure you assign the <code>Advisors.ChangePassword.canView</code> privilege to all users. Performance Management Advisors support Genesys Management Framework Release 8.1.x, but do not fully support the password security authentication options available in Management Framework. Users can be locked out of the Advisors browser if you use Genesys Management Framework 8.1.x in your enterprise and do not change the preceding Management Framework options to true and fail to assign the <code>Advisors.ChangePassword.canView</code> privilege to all users.</p> </div>

Collect Information

During deployment of Advisors platform, the installer will prompt you for the information in the following Table.

Information	Input
Are you installing the Advisors Administration on this system with this installation of Platform	
Language(s) to use in email notifications from the system (English is the default)	
Location and name of the base directory in which you will install Advisors	
Language(s) to specify for email notifications from the system	
Location of the Java Development Kit (root directory)	
Port numbers that the Geronimo application server will use. If you are not going to install two different deployments of	

Information	Input
<p>Advisors on the same machine, use the default values the installer supplies. See Multiple Advisors Deployments on One System for more information.</p>	
<p>Node ID for this server in the Advisors cluster</p>	
<p>The IP address or host name that other cluster members will use to contact this node (not localhost or 127.0.0.1)</p>	
<p>The port number the members of the cluster will use to communicate. If you are not going to install two different deployments of Advisors on the same machine, use the default value the installer supplies. See Multiple Advisors Deployments on One System for more information.</p>	
<p>The local host address (localhost or 127.0.0.1)</p>	
<p>The port number used for communication by the cluster's distributed cache. If you are not going to install two different deployments of Advisors on the same machine, use the default value the installer supplies. See Multiple Advisors Deployments on</p>	

Information	Input
One System for more information.	
<p>Details to connect to the Genesys Configuration Server:</p> <ul style="list-style-type: none">• The name of the primary configuration server (the application name, obtained from the Configuration Manager)• The name or IP address of the machine that hosts the Configuration Server• The port that the configuration server is listening on (if you are not using a TLS connection). If you use a TLS connection, identify the TLS port number.• The name of the application that Advisors Platform will use to log in to the Configuration Server (for example, default)• The user name and password of the account that Advisors Platform will use to connect to the Configuration Server. This is the <i>Advisors User</i>.	

Information	Input
<ul style="list-style-type: none"> The location of the TLS properties file 	
The name of the Object Configuration User account (configured in Configuration Server)	
Will you synchronize user updates between the Configuration Server and the Advisors database?	
<p>The name of the default tenant in the Configuration Server under which the Advisors metadata is maintained</p> <p>When multiple Advisors suite installations are deployed to use the same Configuration server, the <i>default tenant</i> selected on each Advisors suite installation must be a different tenant. The default tenant configuration is selected when installing the Platform server. Within one Advisors suite, the Platform server for CCAdv/WA and the Platform server for FA can share the same default tenant, but different suites cannot share the same tenant.</p>	
Will you enable forgot your password? functionality (that is, allow password modification)? If you enable it, you can control user access to it with role-based access control	
Type of database used in your enterprise (MS SQL	

Information	Input
<p>or Oracle (including Oracle RAC)), and connection details:</p> <ul style="list-style-type: none">• The host name, IP address, or named instance of the server for the Platform database• Port number that the database listens on (you do not require this information if the server is a named instance)• The Platform database name (the SID for an Oracle installation)• The Platform database username and password associated with the account that Advisors Platform will use to access the Platform database• For an Oracle RAC installation, the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator.• For an Oracle installation, the	

Information	Input
location of the JDBC driver	
<p>(Optional) If you have enabled the "Forgot Password" functionality, you require the following details for the SMTP (mail) service that you will use to send the notification messages:</p> <ul style="list-style-type: none"> • SMTP server host name or IP address • The address from which to send application notification e-mail • The address to which to send application notification e-mail 	

|-| AGA=

Before you deploy Advisors Genesys Adapter, it is helpful to answer the following questions:

- Will you deploy Advisors Genesys Adapter on a Linux Red Hat or a Windows platform?
- Where are you installing Advisors (in which directory)? The default location is C:\ProgramFiles\GCTI\Advisors.
- What filters do you require for your enterprise? There are no filters included with the installation of AGA. You configure filters as business attributes in Genesys Configuration Server.
- Will you require the Resource Management Console (RMC) for the CCAdv dashboard? RMC requires that you also install the Supervisor Desktop Service (SDS). Also, you must install RMC during a second run of the AGA installation file; you can install only a single component (either the AGA core service or RMC) during a single installer run.
- On which server will you install AGA for CCAdv/WA and on which will you install AGA for FA? Serving both FA and CCAdv/WA from one system is not recommended for performance reasons.
- Do you use a TLS connection to the Configuration Server?

Prerequisites

Ensure you have completed all the tasks in the following Table before you begin Advisors Genesys Adapter deployment.

Y or N	Prerequisite
	You have initialized databases—databases must be present and at the current version prior to running the installation files. You have configured administrator accounts that can be used by applications to access the databases.
	Advisors Platform is successfully installed on each physical server on which you will install Advisors Genesys Adapter.
	Oracle JDK is installed. You can download Oracle JDK from http://www.oracle.com/technetwork/java/javase/downloads/index.html . See the Genesys Supported Operating Environment Reference Guide for information about supported versions.
	If you are deploying AGA on a Linux platform, you have created the Advisors group and user. This should be done when deploying Advisors Platform on the server.
	You have located the <code>aga-installer-<version>.jar</code> file on the installation CD and have copied it to the local drive of your server.
	A verified Genesys 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.
	You have the Genesys Statistics Server ready and available, and the MCR extension package is installed if you will collect interaction queue statistics. If you will use third-party media statistics, the third-party media Stat Server extensions are installed.
	If the T-Server is the Avaya Communication Manager, make sure that the T-Server option <code>query-agent-work-mode</code> is set to <code>on-restart</code> . This is the default option. To set this option, go to TServer > Option tab > T-Server Option and locate <code>query-agent-work-mode</code> . This setting is required for the AfterCallWork state changes to be visible.
	All the Stat Server configurations are updated with the <code>statserverEntries.cfg</code> options file supplied with Genesys Adapter. Alternatively, you have reviewed the <code>statserverEntries.cfg</code> file and manually updated the Stat Server options with options recommended in the file.
	You have estimated the number of Advisors Genesys Adapters that you require. Depending upon the number of statistics to be served, you might require more than one AGA.

Collect Information

During deployment of Advisors Genesys Adapter, the installer will prompt you for the information in the following Table.

Information	Input
Application that this instance of AGA serves (CCAdv/WA or FA)	

Information	Input
Location and name of the base directory in which you will install Advisors	
Path to the directory in which log files will be written	
Location of the Java Development Kit (root directory)	
<p>Type of database used in your enterprise (MS SQL or Oracle (including Oracle RAC)).</p> <p>For an Oracle installation, the location of the JDBC driver.</p>	
<p>Connection details to the AGA metrics database:</p> <ul style="list-style-type: none"> • The host name, IP address, or named instance of the server on which the Metrics Graphing database is installed. • Port number on which the database listens (you do not require this information if the server is a named instance) • The Metrics Graphing database name (the SID for an Oracle installation) • The username and password associated with the account that modules will use to access the 	

Information	Input
<p>Metrics Graphing database</p> <ul style="list-style-type: none">• For an Oracle RAC installation, the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator.	
<p>Connection details to the Advisors Platform database:</p> <ul style="list-style-type: none">• The host name, IP address, or named instance of the server on which the Advisors Platform database is installed.• Port number that the database listens on (you do not require this information if the server is a named instance)• The Platform database name (the SID for an Oracle installation)• The username (in an Oracle environment, the schema) and password associated with	

Information	Input
<p>the account that modules will use to access the Platform database</p> <ul style="list-style-type: none">• For an Oracle RAC installation, the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. <p>Use the same database configuration that was specified when the Advisors Platform database was configured.</p>	
<p>Connection details to the Genesys Configuration Server:</p> <ul style="list-style-type: none">• The name of the primary configuration server (the application name, obtained from the Configuration Manager)• The name or IP address of the machine that hosts the Configuration Server• The port that the configuration server is listening on (if	

Information	Input
<p>you are not using a TLS connection). If you use a TLS connection, identify the TLS port number.</p> <ul style="list-style-type: none">• The name of the application that Advisors Platform will use to log in to the Configuration Server (for example, default)• The user name and password of the account that Advisors Platform will use to connect to the Configuration Server. This is the 'Advisors User'.• The location of the TLS properties file <p>If you use a backup Configuration Server, you require the following information, as well:</p> <ul style="list-style-type: none">• The name of the backup configuration server (the application name, obtained from the Configuration Manager)• The name or IP address of the machine that hosts the backup Configuration Server• The port that the backup	

Information	Input
Configuration Server is listening on	
<p>Connection details for the primary Stat Server(s):</p> <ul style="list-style-type: none">• The name of the Stat Server server. The name is obtained from the Configuration Manager and is case sensitive.• The name or IP address of the machine hosting the Stat Server• The port on which the Stat Server listens. <p>NOTE: You can configure up to five Stat Server pairs using the AGA installer. Additional Stat Servers can be configured after the installation by manually configuring them directly in the database.</p>	
<p>(Optional) Connection details for the backup Stat Server(s):</p> <ul style="list-style-type: none">• The name of the backup Stat Server server. The name is obtained from the Configuration Manager and is case sensitive.• The name or IP address of the machine hosting the backup Stat	

Information	Input
<p>Server</p> <ul style="list-style-type: none"> The port on which the backup Stat Server listens. <p>NOTE: You can configure up to five Stat Server pairs using the AGA installer.</p>	
<p>The type of statistics supported on each Stat Server pair you are associating with a Genesys Adapter instance. Options are the following:</p> <ul style="list-style-type: none"> Core 3rd party media Multimedia (this refers to eServices) 	
<p>For registration with the Platform database:</p> <ul style="list-style-type: none"> The port on which the AGA web services will run (you can use the default port, 7000) The name of the AGA server The IP address of the AGA server A description of the AGA server (for example, Advisors Genesys Adapter for CCAdv/WA) In an Oracle environment, the location of the file that 	

Information	Input
contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator.	

|-| ACA=

Before you deploy Advisors Cisco Adapter, it is helpful to answer the following questions:

- Will you deploy Advisors Cisco Adapter on a Linux Red Hat or a Windows platform?
- Where are you installing Advisors (in which directory)? The default location is C:\ProgramFiles\GCTI\Advisors.
- Will you be registering ACA with the Platform database?

Prerequisites

Ensure you have completed all the tasks in the following Table before you begin Advisors Cisco Adapter deployment.

Y or N	Prerequisite
	Credentials with read access to the HDS and AW databases are available.
	Each ICM AWDB that must be accessed by FA has a user mapped to the relevant SQL Server account. The minimum requirement is that this ACA user has permissions to select data from: <ul style="list-style-type: none"> • agent_Real_Time • Termination_Call_Detail
	You have initialized databases—databases must be present and at the current version prior to running the installation files. You have configured administrator accounts that can be used by applications to access the databases.
	Advisors Platform is successfully installed on each physical server on which you will install Advisors Cisco Adapter.
	Oracle JDK is installed. You can download Oracle JDK from http://www.oracle.com/technetwork/java/javase/downloads/index.html . See the Genesys Supported Operating Environment Reference Guide for information about supported versions.
	If you are deploying ACA on a Linux platform, you have created the Advisors group and user. This should be done when deploying Advisors Platform on the server.

Y or N	Prerequisite
	You have located the <code>aca-installer-<version>.jar</code> file on the installation CD and have copied it to the local drive of your server.

Collect Information

During deployment of Advisors Cisco Adapter, the installer will prompt you for the information in the following Table.

Information	Input
Location and name of the base directory in which you will install Advisors	
Path to the directory in which log files will be written	
Location of the Java Development Kit (root directory)	
Connection details for the Cisco HDS and AW databases: <ul style="list-style-type: none">• The host name or IP address of the database server• The AW database name• The HDS database name• Port number that the database listens on• The username and password associated with the account that ACA will use to access the database(s)	
Type of database used in your enterprise (MS SQL or Oracle (including Oracle RAC)), and connection details:	

Information	Input
<ul style="list-style-type: none">• The host name or IP address of the server on which the ACA database is installed• The database name (the SID for an Oracle installation)• Port number that the database listens on• The ACA database username (the schema for an Oracle installation) and password associated with the account that ACA will use to access the database• For an Oracle RAC installation, the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator.• For an Oracle installation, the location of the JDBC driver	
For registration with the Platform database (optional):	

Information	Input
<ul style="list-style-type: none">• The port on which the ACA web services will run (you can use the default port, 7000)• The name of the ACA server• The IP address of the ACA server• A description of the ACA server (for example, Advisors Cisco Adapter)• The source environment (for example, Cisco)	
<p>Connection details for the Advisors Platform database (if you plan to register ACA with the database):</p> <ul style="list-style-type: none">• The host name, IP address, or named instance of the server on which the Platform database is installed• Port number that the database listens on (you do not require this information if the server is a named instance)• The Platform database name• The username (schema in an Oracle installation) and password associated with	

Information	Input
<p>the account that ACA will use to access the Platform database</p> <ul style="list-style-type: none"> For an Oracle RAC installation, the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. 	

| - | CCAdv/WA=

Before you deploy Contact Center Advisor, Workforce Advisor, or AM Administration, it is helpful to answer the following questions:

- Will you deploy the software on a Linux Red Hat or a Windows platform?
- Where did you install Advisors Platform on this system? The installation directory for CCAdv/WA modules (CCAdv, WA, CCAdv-ME, and Alert Management Administration) must be the same as the directory where Advisors Platform was installed.
- Each of the modules associated with a CCAdv/WA installation (CCAdv web services, CCAdv XML Generator, CCAdv-ME, WA server, WA web services, and Alert Management Administration) can be installed on a different machine, or multiple modules can be installed on the same machine. If you are installing multiple modules, on which system will you install each module?
- Will you install the CCAdv application, and if so, will you install it in standalone or distributed mode? If distributed, which CCAdv instance (on which server) will be responsible for data aggregation, and which will be presentation nodes?
- Will you install the WA application, and if so, will you install it in standalone or distributed mode? If distributed, which WA instance (on which server) will be responsible for data aggregation, and which will be presentation nodes?
- If you will install WA, what are your workforce management data sources and how many do you require?
- Will CCAdv or WA send e-mail notifications about alerts ?
- Will you deploy CCAdv-ME?
- Will you deploy AM Administration? You should deploy it on the same system as the Administration Workbench.

Prerequisites

Ensure you have completed all the tasks in the following Table before you begin Contact Center Advisor/Workforce Advisor deployment.

Y or N	Prerequisite
	<p>You have initialized databases—databases must be present and at the current version prior to running the installation files. The following list shows the databases required by each component:</p> <ul style="list-style-type: none"> • Contact Center Advisor: Platform database and metric graphing database • Workforce Advisor: Platform database and metric graphing database • Contact Center Advisor-ME: Platform database and metric graphing database • AM Administration: Platform database <p>You have configured administrator accounts that can be used by applications to access the databases.</p>
	Advisors Platform is successfully installed on each physical server on which you will install Contact Center Advisor, Contact Center Advisor-Mobile Edition, Workforce Advisor, or the AM Administration.
	<p>For Genesys installations, the Advisors Genesys Adapter is installed.</p> <p>(For Cisco installations, no adapter is required.)</p>
	You have located the ccawa-installer- <code><version></code> .jar file on the installation CD and have copied it to the local drive of your server.
	<p>For Contact Center Advisor and Workforce Advisor deployments, there is a database-level connection between the Advisors Platform database and the datasource database (a Genesys metrics database and/or a Cisco ICM AWDB database).</p> <p>To configure the connectivity, see Configure Oracle 11g Metrics Data Sources.</p>
	<p>If you are deploying WA server, verified workforce management data sources must be ready and available.</p> <p>For Workforce Advisor installations connecting to Genesys WFM, the server running WA must be able to access your Genesys WFM installation.</p> <p>To verify this access, ensure you can do all of the following from your WA server machine:</p> <ol style="list-style-type: none"> 1. Successfully ping the server name or IP address specified in the base WFM URL. 2. Successfully telnet the server name or IP address and the port specified in the base WFM URL. 3. Successfully ping the host name of your Genesys WFM instance as it appears in your WFM server's Configuration Manager application. <p>Your WA server must have access to the WFM server by its associated Configuration Manager host name. If it does not, an UnknownHostException occurs because the SOAP API's service locator provides a host name that is not reachable by the WA server.</p> <p>If you cannot ping or access the Genesys WFM instance using the associated Configuration Manager host name from the machine hosting the WA server, then you must add the following lines to the hosts file on the machine that will host the WA server:</p> <pre># For WA connectivity with WFM</pre>

Y or N	Prerequisite
	<p>[IP address of WFM server] [Associated Configuration Manager host name for the WFM instance]</p> <p>Example: 192.168.98.229 demosrv.genesyslab.com</p> <p>The hosts file is OS-specific. For example, for Windows 2003, the host file resides in the following location: %SystemRoot%\system32\drivers\etc\</p>
	For XML Generator, you have identified one or more metric data sources.

Collect Information

During deployment of Contact Center Advisor/Workforce Advisor, the installer will prompt you for the information in the following Table.

Information	Input
All Modules:	
<p>Location and name of the base directory in which you will install Advisors.</p> <p>The installation directory for CCAdv/WA modules must be the same as the directory where Advisors Platform was installed.</p>	
Location of the Java Development Kit (root directory)	
Contact Center Advisor XML Generator:	
<p>The maximum number of times that CCAdv XML Generator should attempt to connect to a database if there is a connection failure.</p> <p>This parameter is applicable to retry attempts when XML Generator is already running; that is, after establishing connections at startup.</p>	
The number of seconds between CCAdv XML Generator's reconnection	

Information	Input
<p>attempts in the event of a database connection failure.</p> <p>This parameter is applicable to retry attempts when XML Generator is already running; that is, after establishing connections at startup.</p>	
<p>Frequency (in seconds) at which CCAAdv XML Generator stores metrics and threshold violations for the values calculated for the Medium and Long groups of time profiles</p> <p>For example, if you enter 120 seconds for this parameter, XML Generator stores metrics and threshold violations for these time profiles no more often than that. However, XML Generator may store the view data less frequently depending upon load and the complexity of the configuration.</p>	
<p>The following details for the SMTP (mail) service that XML Generator will use to send e-mail:</p> <ul style="list-style-type: none"> • (Optional) The address from which to send notification e-mail about alerts. Required if the deployment of XML Generator will be configured to create alerts and to send e-mail about them. 	

Information	Input
<ul style="list-style-type: none"> • The address to which to send notification e-mail for support staff concerning issues with the application. This address will also appear in the From: header of these types of e-mail. • The host name or IP address of the SMTP server that XML Generator will use to send e-mail with ERROR messages also written to its log file. 	
<p>The frequency (in seconds) at which snapshots are stored in the metric graphing database.</p> <p>For example, if you enter 60 seconds for this parameter, XML Generator stores 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.</p>	
<p>Should graphs display values from the previous day?</p>	
<p>What are your sources of real-time data? Specify the following:</p> <ul style="list-style-type: none"> • the database name or linked server name • the source type 	

Information	Input
<p>(Genesys or Cisco)</p> <ul style="list-style-type: none"> • (optional) the display name • the threshold update delay - how long CCAdv will wait for new data from this data source before notifying users via the CCAdv dashboard, and, if configured to do so, administrators via e-mail. • the Relational Database Management System (RDBMS) type (MS SQL or Oracle) <p>Up to five data sources may be added to the deployment of XML Generator.</p>	
CCAdv-ME Server:	
<p>CCAdv-ME server configuration. Specify the following:</p> <ul style="list-style-type: none"> • Interval for file purge (ms) of the charting local cache from the server • Delay for retries on failed response (ms) • Number of retries on failed response • Device refresh interval (ms) of the client views 	

Information	Input
<p>when auto-refresh is enabled</p> <ul style="list-style-type: none"> • Will you allow password caching on clients? • Will you use a logo link URL (image link)? If yes, what is the URL to which users are re-directed when they click the image or logo? 	
<p>The three time periods for trend charting (mins)</p> <p>Period two should be bigger than period one and smaller than period three. Genesys recommends that you enter numerical characters only, such as 30, 60, or 120.</p>	
<p>Workforce Advisor Server:</p>	
<p>Specify your workforce management data sources (IEX TotalView, Aspect eWFM, Genesys WFM)</p>	
<p>The following details for the SMTP (mail) service that WA will use:</p> <ul style="list-style-type: none"> • The 'From' address WA puts in e-mail it sends about alerts to users that are members of distribution lists configured in the Administration 	

Information	Input
<p>Workbench.</p> <ul style="list-style-type: none"> The address to which to send notification e-mail for support staff concerning issues with the application. Note that in 8.5.0, WA does not use this address. The installer still asks for it, but does nothing with it. 	
<p>Specify information about your workforce management data source(s):</p> <ul style="list-style-type: none"> For IEX TotalView, the port number on which the FTP connection in WA listens for data from TotalView. For Aspect eWFM, the URL of the directory from which WA reads data from eWFM. For example file:/// followed by the location of the eWFM files. Additional information is provided in the descriptions of installation screens on the Deploying CCAdv and WA page. For Genesys WFM, you 	

Information	Input
<p>require the following information:</p> <ul style="list-style-type: none">• The URL of the WFM server.• The application name of the WFM server as configured in the Configuration Server or Genesys Administrator• The user ID, either a specific numeric user ID to indicate the identity of the requests, or enter 0 (zero) to indicate no user• The interval (in ms) at which the Genesys WFM service is polled for forecast data• The number of hours of forecast metrics to get during each polling interval	
Contact Center XML Generator and Workforce Advisor Server:	
The time profile of historical metrics that you want to display for agent	

Information	Input
<p>groups, in Contact Center Advisor and Workforce Advisor. The choices are 5 minute sliding, or 30 minute growing. The same choice applies to both applications.</p> <p>For metrics imported from CISCO ICM, Advisors always imports agent group metrics with the 5 minute sliding profile. If you are running Advisors with CISCO ICM, and you choose the 30 minute growing option here, then on the dashboards, historical agent group metrics will display as a dash. Genesys recommends that you use the five minute growing setting if you have a CISCO source of data.</p>	
<p>Type of database used in your enterprise (MS SQL or Oracle (including Oracle RAC)), and connection details to the Advisors Platform database:</p> <ul style="list-style-type: none">• The host name, IP address, or named instance of the server on which the Advisors Platform database is installed.• Port number that the database listens on (you do not require this information if the server is a named instance)• The Platform database name (the SID for an Oracle	

Information	Input
<p>installation)</p> <ul style="list-style-type: none">• The username (the schema for an Oracle installation) and password associated with the account that modules will use to access the Platform database• For an Oracle RAC installation, the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. <p>Use the same database configuration that was specified when the Advisors Platform database was configured.</p>	
<p>Connection details to the Metric Graphing database:</p> <ul style="list-style-type: none">• The host name, IP address, or named instance of the server on which the Metrics Graphing database is installed.• Port number on which the database listens (you do not require this	

Information	Input
<p>information if the server is a named instance)</p> <ul style="list-style-type: none"> • The Metrics Graphing database name (the SID for an Oracle installation) • The username (the schema for an Oracle installation) and password associated with the account that modules will use to access the Metrics Graphing database • For an Oracle RAC installation, the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. 	

|-| FA=

Before you deploy Frontline Advisor, it is helpful to answer the following questions:

- Will you install the FA application in standalone or distributed mode? If distributed, which FA instance (on which server) will be responsible for data aggregation, and which will be presentation nodes?
- Will you deploy the FA application on a Linux Red Hat or a Windows platform?
- Where are you installing Advisors (in which directory)? The default location is C:\ProgramFiles\GCTI\Advisors.
- Do you want the FA application to send e-mail notification messages? From what address will an application send notifications (for example, DONOTREPLY@<your enterprise>.com)? To what e-mail

address will an application send notifications? What is the subject line for such e-mail messages (for example, Frontline Advisor notification?)

Prerequisites

Ensure you have completed all the tasks in the following Table before you begin Frontline Advisor deployment.

Y or N	Prerequisite
	A verified Cisco environment must be ready and available if any of the agents will have metrics provided by Advisors Cisco Adapter.
	For Cisco installations, the Advisors Cisco Adapter is installed.
	For Genesys installations, the Advisors Genesys Adapter is installed.
	You have initialized databases—databases must be present and at the current version prior to running the installation files. You have configured administrator accounts that can be used by applications to access the databases.
	Advisors Platform is successfully installed on each physical server on which you will install the Frontline Advisor or Agent Advisor application.
	The FA hierarchy is configured on the Genesys Configuration Server and you can identify the following: <ul style="list-style-type: none"> the tenant(s) associated with the hierarchy the path to the hierarchy root folder(s) in Genesys Configuration Server
	You have located the fa-server-installer-<version>.jar file on the installation CD and have copied it to the local drive of your server.

Collect Information

During deployment of Frontline Advisor, the installer will prompt you for the information in the following Table.

Information	Input
Location and name of the base directory in which you will install Advisors. (The installation directory for Frontline Advisor server must be the same as the directory where Advisors Platform was installed.)	
Are you running FA in standalone or distributed mode? If distributed, which FA instance (on which server) will be	

Information	Input
<p>responsible for data aggregation? Only one FA instance can be responsible for data aggregation; you must enable the rollup engine on this instance.</p>	
<p>Information about your hierarchy. You require one of the following:</p> <ul style="list-style-type: none"> • The name of the tenant(s) in the Genesys Configuration Server in which the monitoring hierarchy resides, and the path to the hierarchy root folder(s). In a Cisco environment, the path should look like: Agent Groups\\<Your Cisco Group Name> • The name of a Person folder in Configuration Manager, and the path to that Person folder. Selecting this option restricts the hierarchy view that is loaded at startup (or reloaded using the reload feature) to the team of agents belonging to that person (supervisor). 	
<p>Type of database used in your enterprise (MS SQL or Oracle (including</p>	

Information	Input
<p>Oracle RAC)), and connection details:</p> <ul style="list-style-type: none">• The host name, IP address, or named instance of the server on which the Advisors Platform database is installed.• Port number that the database listens on (you do not require this information if the server is a named instance)• The Platform database name (the SID for an Oracle installation)• The username (the schema for an Oracle installation) and password associated with the account that FA will use to access the Platform database• For an Oracle RAC installation, the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator.	

Information	Input
<ul style="list-style-type: none">For an Oracle installation, the location of the JDBC driver	
<p>If you will send e-mail notifications from the application, you require the following details for the SMTP (mail) service that you will use to send the notification messages:</p> <ul style="list-style-type: none">The address from which to send application notification e-mail.The address to which to send application notification e-mail.The subject line to be used for e-mail associated with application notifications.	

Additional Resources


The following resources provide additional information that is relevant to this software. Consult these additional resources as necessary.

- The [Genesys Supported Operating Environment Reference Guide](#) contains information about supported hardware and third-party software. See the [Performance Management Advisors](#) section for information specific to Advisors.
- The [Genesys Interoperability Guide](#) contains information about the compatibility of Genesys products, including Performance Management Advisors, with various Configuration Layer environments.
- The [Genesys Hardware Sizing Guide](#) contains information about tested environments (architecture, number of users per component per installation, and so on). This information is meant to help you develop sizing guidelines for your enterprise.
- The [Genesys Migration Guide](#) provides documented migration strategies for Genesys product releases, including Performance Management Advisors.
- The [Performance Management Advisors 8.5 Release Notes](#) contain information about new features, software modifications, known issues, and recommendations. For your convenience, the Genesys documentation website includes a page that has links to Release Notes for all Genesys products. See [Genesys Release Notes](#).

Create the Advisors Databases

Use the procedures in this section to install the databases that Performance Management Advisors require. Installation of the databases is the first step in Advisors deployment.

Roadmap

1.  Install the databases that correspond to the Advisors products you will deploy:
 - a. Advisors Genesys Adapter metrics database
 - b. Advisors Platform database
 - c. Advisors Cisco Adapter database (if you use ACA)
 - d. Metric Graphing database
2. Create the Advisors User and the Object Configuration User in Configuration Server.
3. **[+] Install the Platform service (Geronimo) on all servers on which you will deploy one of the Advisors components.**
 - Contact Center Advisor
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. **[+] Install the Advisors components for your enterprise.**
 - a. Contact Center Advisor
 - b. Workforce Advisor

- c. Contact Center Advisor – Mobile Edition
 - d. SDS and Resource Management
 - e. Frontline Advisor
6. Make any required configuration changes.

Creating a SQL Server Database

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

<tabber>

Create the DB=

1. Connect to your SQL Server 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.

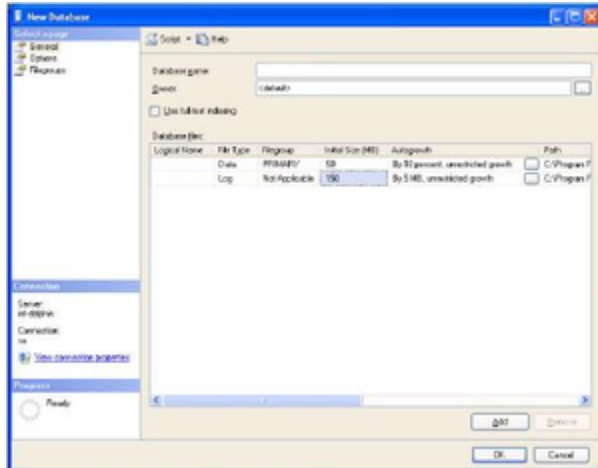
2. In the object explorer right-click on Databases and choose New Database. Open the General screen and configure the following properties. See the Figure that follows—Database Properties - General—as an example.

a. Specify the database name. **[+] See recommended database names.**

Advisors Component	Recommended DB name	Notes
Platform	advisors_platformdb	Required for Advisors implementations.
CCAdv/WA		Uses the Platform and Metric Graphing databases.
FA/AA		Starting in release 8.5.0, the FA/AA database is no longer required. FA database content moves to the Platform database. See Object Migration Utility for information about migrating the FA/AA database data and objects to the Platform database.
Metric Graphing	advisors_mgdb	Metric Graphing database. Required for running CCAdv/WA Dashboards and XML Generator.
Advisors Genesys Adapter	advisors_gametricsdb	Used by AGA to transfer Genesys configuration and statistics values to XML Generator for CCAdv/WA. NEW Starting in release 8.5.0, this database includes a table to support calling list statistics. This database is required for CCAdv/WA and WA server installations only.
Advisors Cisco Adapter	cisco_adapterdb	Required for Cisco Adapter.

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.



Database Properties - General

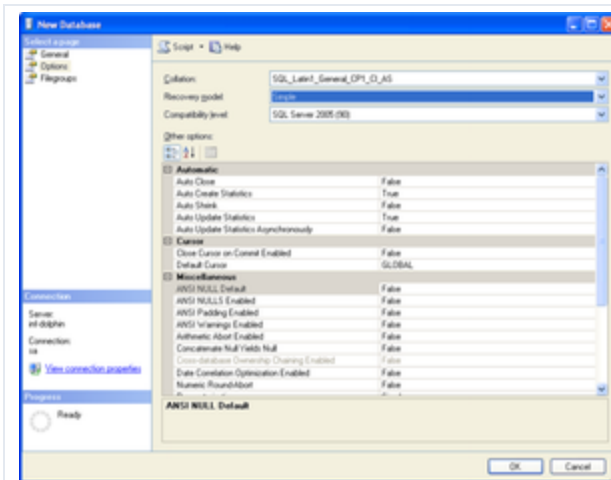
3. Open the Options screen.

- 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 the procedure on the *Create login for Advisors* tab on this page.

6. In the Object Explorer, expand Databases, <dbname_db>, Security, and Schemas. See the following Figure.



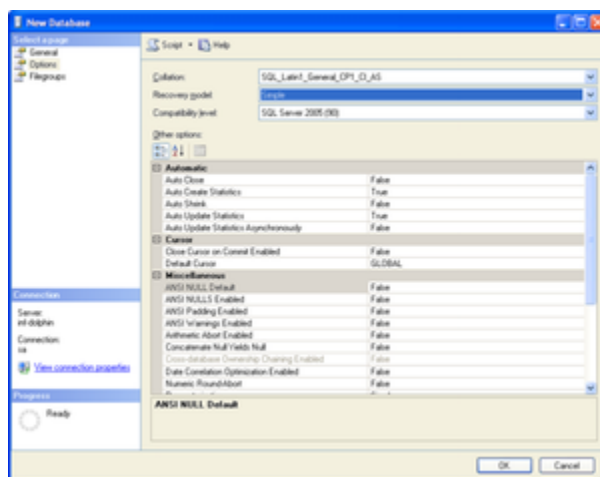
Database Properties - Options

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.

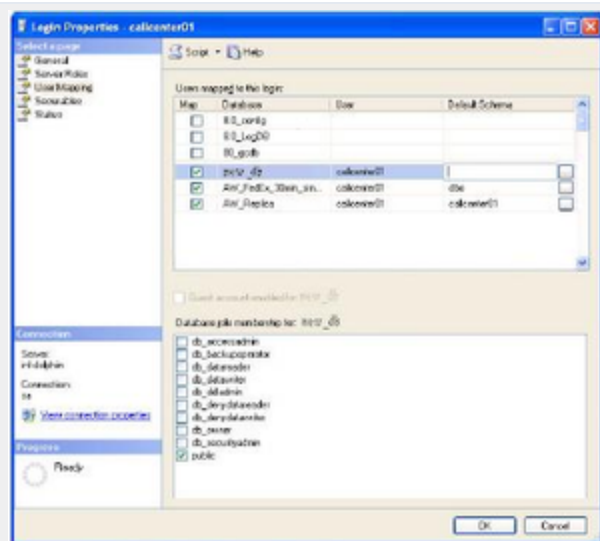
-| Create login for DB=

1. In the Microsoft SQL Server Management Studio object explorer, select Server, and then Security.
2. Right-click Logins and choose New Login. See the Figure that follows—Server-level Security.
 - a. Specify the login name (in this example, callcenter01).
 - b. Click SQL Server Authentication.
 - c. Specify a password that complies with your enterprise's security policy.
 - d. If strong passwords are part of the security policy, check the Enforce password policy check box.



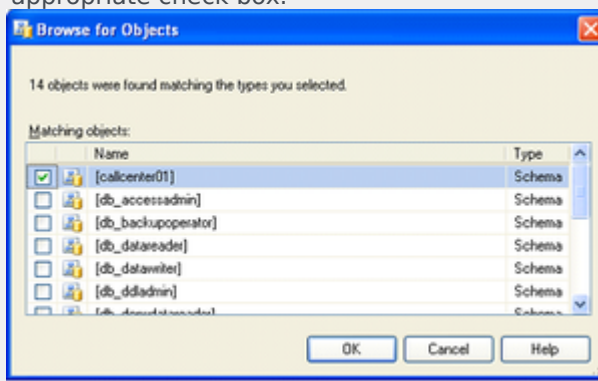
Server-level Security

3. Open the Login Properties - User Mapping screen.



Login Properties – User Mapping

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



Browse for Objects

- b. Choose dbo as a default schema if you skipped steps 5 and 6 in the procedure on the *Create the DB* tab on this page. Otherwise select the name of the created schema.
- 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 the Login Properties – User Mapping window. Select either:
 - The db_owner database role
 - All three of the db_datareader, db_datawriter, and db_ddladmin roles

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 the *Assigning Additional User Permissions* section on the *Create objects in the DB* tab on this page.

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

| Create linked servers for the DB=

Before you start the procedure, identify the data sources that must be accessed. If the customer uses a Cisco environment, then a linked server is necessary for each MSSQL Server used by the CCAdv/WA CISCO ICM databases. Before each linked server is configured, the CISCO ICM database administrator must create a login on each such MSSQL Server and a corresponding AWDB user linked to it. The user must have Read permission on the following AWDB views and a table:

- 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

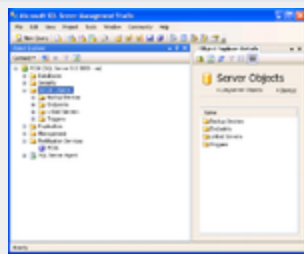
A linked server is normally not required to access the Advisors Genesys Adapter metrics database except in some uncommon cases when the Genesys Adapter metrics database and platform database reside on separate MSSQL Servers. However, each view in the Genesys Adapter metrics database must be accessible by the user defined in the Advisors Platform database. The platform user must be granted access to Genesys Adapter metrics database views that have the same names as the preceding list of CISCO ICM views. The Genesys Adapter metrics database also contains two additional views:

- Virtual_Queue_Set1_Real_Time
- Controller_Time

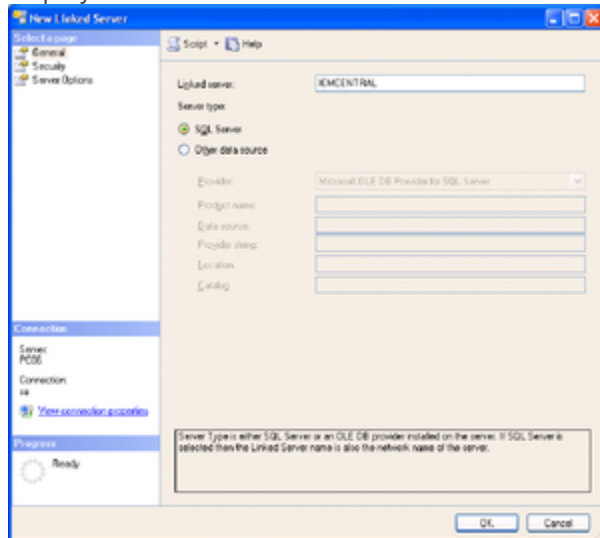
These two views must be accessible by the Platform user, also.

The user can be given the preceding object-level permissions or assigned to an equivalent user-defined database role. If your enterprise's security policy allows it, the user can be assigned to any database standard role that includes the above minimum permissions. For example, the user can be assigned to the standard db_datareader role.

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



2. Right-click on Linked Servers and choose New Linked Server... The New Linked Servers screen displays.



New Linked Server Screen

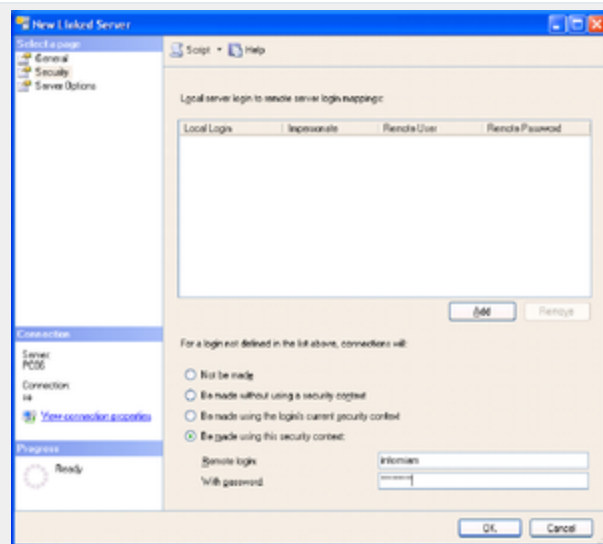
3. Under Server type, select SQL Server.

4. Specify the name of the external SQL database server to be accessed, and click OK.

The New Linked Server – Security screen displays.

5. On the Security screen:

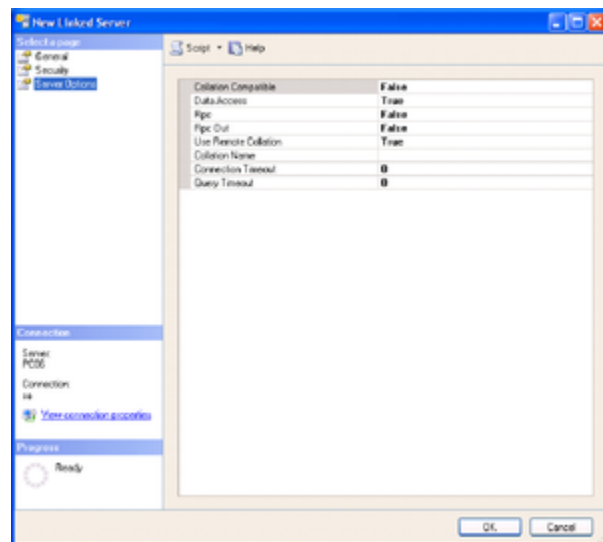
- Select Be made using this security context.
- Specify the remote login and password created by the external administrator for access to the external database.



New Linked Server – Security

6. On the Server Options screen:

- Check the Data Access check box and User Remote Collation check box.
- Click OK.



New Linked Server – Server Options

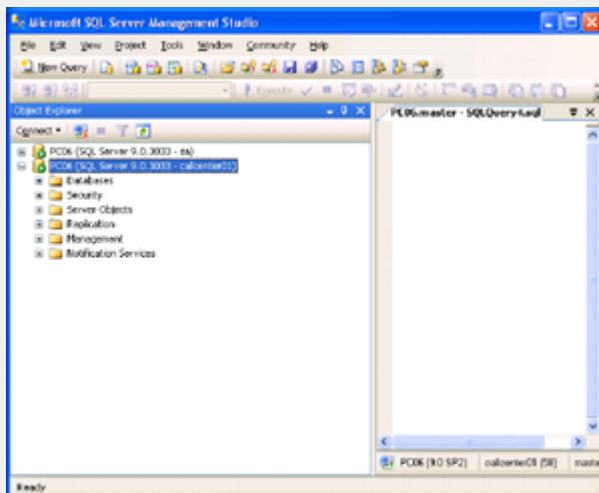
7. To test the linked server connectivity, run some SQL statements from the Microsoft SQL Server Management Studio.

- Enter the correct connection details and click Connect.



Connect to the Database Engine

The New Query screen displays.



Microsoft SQL Management Studio – New Query

b. Click New Query.

c. 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>)]`

For example, for Cisco:

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

`Select * from OpenQuery([ICM_AWDB1], 'select * from company_awdb.dbo.Controller_Time (no lock)')`

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

| Create objects in the DB=

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 *Create login for Advisors* tab on this page).

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

1. From Microsoft SQL Server Management Studio, click File. Connect to the database engine as a user meeting the criteria described 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.

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, and then click CTRL/A, then CTRL/C. Paste the content (CTRL/V) into the query pane and execute the following script. Before executing the script, remember to change <database user> to the ID for your database user.

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

| Migration Scripts=

Platform database deployment/migration in MSSQL is performed by executing the platform-new-database-<version>.sql script supplied in the distribution for releases up to, and including, Release 8.1.4. Starting in Release 8.1.5, the script is labeled advisors-platform-new-database-<version>.sql. The same script can be applied to a new empty database or a database of any previous version. Always check Release Notes for exceptions to this rule.

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.

Creating an Oracle 11g Database

This page describes how to create a generic Oracle 11g database. Each individual Oracle database in an Advisors implementation has its own creation script in the 8.5 release.

In 8.5.x releases, all Oracle scripts are creation scripts except those that contain the word migrate in the name. Any existing schema with the same name must be dropped prior to running the scripts. Use the migration scripts when upgrading your software version.

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

The procedure applies to an Oracle user who has permissions to create tablespaces, users, and to grant permissions. Follow your enterprise's policies in production environments. If necessary, have the DBA create tablespaces, users, and grant permissions. Use scripts relevant to your environment after the DBA completes the work. Refer to the script content description contained in [Advisors Software Distribution Contents](#).

[+] See recommended database names.

Advisors Component	Recommended DB name	Notes
Platform	advisors_platformdb	Required for Advisors implementations.
CCAdv/WA		Uses the Platform and Metric Graphing databases.
FA/AA		Starting in release 8.5.0, the FA/AA database is no longer required. FA database content moves to the Platform database. See Object Migration Utility for information about migrating the FA/AA database data and objects to the Platform database.
Metric Graphing	advisors_mgdb	Metric Graphing database. Required for running CCAdv/WA Dashboards and XML Generator.
Advisors Genesys Adapter	advisors_gametricsdb	Used by AGA to transfer Genesys configuration and statistics values to XML Generator for CCAdv/WA. NEW Starting in release 8.5.0, this database includes a table to support calling list statistics. Only required for CCAdv/WA and WA server installations.
Advisors Cisco Adapter	cisco_adapterdb	Required for Cisco Adapter.

<tabber>

Before You Begin=

You must perform all the steps in the procedure 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>

It is important to use <alias to the oracle instance contained in the local tnsnames.ora file> as a response on all prompts where the database scripts ask you to <Enter the database instance alias>.

For 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:

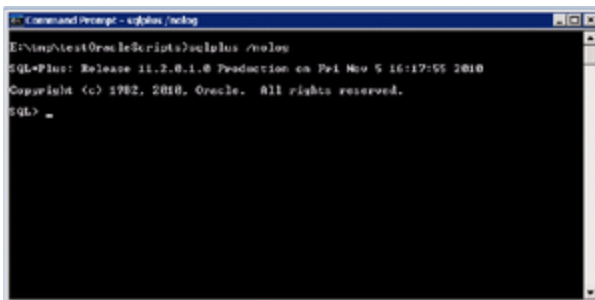
```
C:>tnsping wolf
```

The successful message will look as follows:

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

| Procedure=

1. Copy all of your Oracle database scripts to a folder on the machine where you have the Oracle client installed. The path name for this location must not contain spaces.
2. On the machine where the Oracle client is installed, open a command prompt and change directory to the folder where the database scripts now reside.
3. Review the readme files located in the script directories.
4. Start SQLPlus by entering sqlplus /nolog at the command prompt. You should see the prompt change to SQL>.

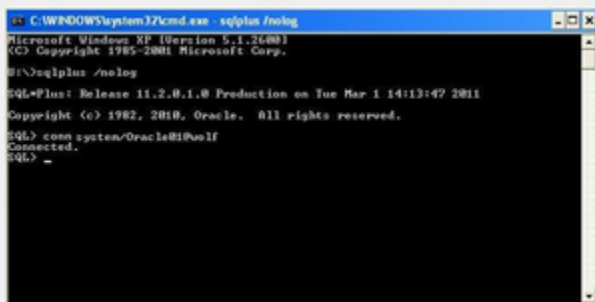
A screenshot of a Windows Command Prompt window titled "Command Prompt - sqlplus /nolog". The prompt shows the execution of "E:\test\Oracle\scripts\sqlplus /nolog", followed by the Oracle SQL*Plus version information: "SQL*Plus: Release 11.2.0.1.0 Production on Fri Nov 5 16:17:55 2010 Copyright (c) 1982, 2010, Oracle. All rights reserved." and the "SQL>" prompt.

```
Command Prompt - sqlplus /nolog
E:\test\Oracle\scripts\sqlplus /nolog
SQL*Plus: Release 11.2.0.1.0 Production on Fri Nov 5 16:17:55 2010
Copyright (c) 1982, 2010, Oracle. All rights reserved.
SQL>
```

SQL Command Prompt

5. 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.

A screenshot of a Windows Command Prompt window titled "C:\WINDOWS\system32\cmd.exe - sqlplus /nolog". It shows the execution of "D:\sqlplus /nolog", the Oracle version information, and the successful connection command: "SQL> conn system/Oracle@10wolf Connected." followed by the "SQL>" prompt.

```
C:\WINDOWS\system32\cmd.exe - sqlplus /nolog
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
D:\sqlplus /nolog
SQL*Plus: Release 11.2.0.1.0 Production on Tue Mar 1 14:13:47 2011
Copyright (c) 1982, 2010, Oracle. All rights reserved.
SQL> conn system/Oracle@10wolf
Connected.
SQL>
```

SQL Command Prompt 2

6.

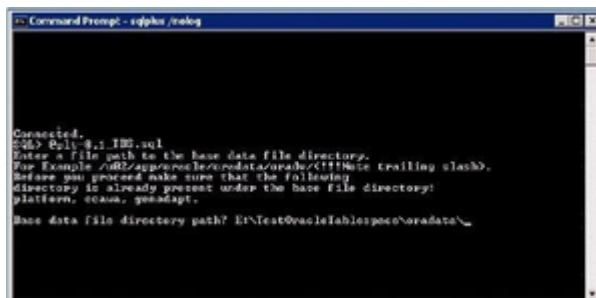
[+] Show steps if required Tablespaces are already present

- a. 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.

A screenshot of a Windows Command Prompt window titled "Command Prompt - sqlplus /nolog". It shows the "Connected." message, the execution of "SQL> @11-01-100.sql", and a prompt for the base data file directory path. The prompt text includes instructions: "Enter a file path to the base data file directory. For Example /u02/app/oracle/oradata/oracle/ (Note trailing slash). Before you proceed make sure that the following directory is already present under the base file directory: platform, common, gsmadapt." The prompt ends with "Base data file directory path? E:\Test\Oracle\10wolf\oradata\".

```
Command Prompt - sqlplus /nolog
Connected.
SQL> @11-01-100.sql
Enter a file path to the base data file directory.
For Example /u02/app/oracle/oradata/oracle/ (Note trailing slash).
Before you proceed make sure that the following
directory is already present under the base file directory:
platform, common, gsmadapt.
Base data file directory path? E:\Test\Oracle\10wolf\oradata\
```

SQL Command Prompt 4

- b. When prompted, enter the schema password.

```

C:\Windows\system32\cmd.exe - sqlplus /nolog

Enter a schema name for the platform db objects.
For example: AdvObj

Platform schema name? AdvPlatform

Enter a password (no special characters) for AdvPlatform
For example: callcenter01.
Password for AdvPlatform? _

```

SQL Command Prompt 7

- c. On the SID prompt, enter the alias to the Oracle instance contained in the local tnsnames.ora.

```

C:\Windows\system32\cmd.exe - sqlplus /nolog

Enter a schema name for the platform db objects.
For example: AdvObj

Platform schema name? AdvPlatform

Enter a password (no special characters) for AdvPlatform
For example: callcenter01.
Password for AdvPlatform? callcenter01
Enter the database instance alias (SID).
SID? call

```

SQL Command Prompt 8

- d. 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.

[+] Show steps if required Tablespaces do not yet exist

- a. Run the tablespace script by entering
 @<script name>
 at the prompt, where <script name> is the name of your tablespace script. For example, @advisors-platform-8.5.0_TBS.sql if you are creating a Platform database (see the following Figure).

```

C:\WINDOWS\system32\cmd.exe - sqlplus /nolog

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

H:\>sqlplus /nolog

SQL*Plus: Release 11.2.0.1.0 Production on Tue Mar 1 14:13:47 2011
Copyright (c) 1982, 2010, Oracle. All rights reserved.

SQL> conn system/Oracle@call
Connected.
SQL> @plt-8.5_TBS.sql

```

SQL Command Prompt 3

See for details of script names supplied in the distribution.

- b. When prompted, enter the full path to your base data file directory (from [Step 2](#)), including the trailing slash. This is the path on the server where ORACLE is installed; you are indicating where to put the files that will contain the tablespace's data.
 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.


```

C:\> Command Prompt - sqlplus /nolog

Connected.
SQL> @plt-8.1.1DB.sql
Enter a file path to the base data file directory.
For Example: /u02/app/oracle/oradata/oracle/ (Note trailing slash).
Before you proceed make sure that the following
directory is already present under the base file directory:
platform, cdata, gnsadapt.
Base data file directory path? E:\Test\Oracle\11g\space\oradata\

```

SQL Command Prompt 4

c. Verify the results of your script execution:

- i. 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.
- ii. 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

d. 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.

```

C:\> Command Prompt - sqlplus /nolog

Connected.
SQL> @plt-8.1-ORAPROJ_Schema.sql

```

SQL Command Prompt 5

e. When prompted, enter your schema name for the database objects. (The following Figures use AdvPlatform as an example.)

```

C:\> Command Prompt - sqlplus /nolog

Connected.
SQL> @plt-8.1_Schema.sql
Enter a schema name for the platform db objects.
For example: ADVP
Platform schema name? _

```

SQL Command Prompt 6

f. When prompted, enter the schema password.

```

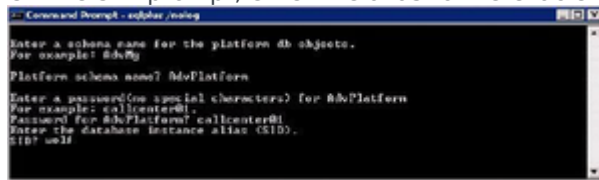
C:\> Command Prompt - sqlplus /nolog

Enter a schema name for the platform db objects.
For example: ADVP
Platform schema name? ADVPlatform
Enter a password (no special characters) for ADVPlatform
For example: callcenter01.
Password for ADVPlatform? _

```

SQL Command Prompt 7

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



```
-- Command Prompt - sqlplus /nolog
Enter a schema name for the platform db objects.
For example: #dbObj
Platform schema name? #dbPlatform
Enter a password (or special characters) for #dbPlatform
For example: callcenter@!
Password for #dbPlatform? callcenter@!
Enter the database instance alias (SID).
SID? uolif
```

SQL Command Prompt 8

- h. 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.

Configure Oracle 11g Metrics Data Sources

Use the information on this page to configure a connection to your metrics data sources.

To AGA Metrics Schema on the Same Oracle Instance as the Platform Schema

Use the information on this tab to configure connectivity to AGA metrics where the AGA data source is on the same Oracle instance as the Platform schema.

1. Do one of the following:

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

```
GRANT SELECT ON <aga metrics schema>.AGENT_SKILL_GROUP_REAL_TIME TO <platform user>;
GRANT SELECT ON <aga metrics schema>.CALL_TYPE TO <platform user>;
GRANT SELECT ON <aga metrics schema>.CALL_TYPE_REAL_TIME TO <platform user>;
GRANT SELECT ON <aga metrics schema>.CONTROLLER_TIME TO <platform user>;
GRANT SELECT ON <aga metrics schema>.INTERACTION_QUEUE TO <platform user>;
GRANT SELECT ON <aga metrics schema>.INTERACTION_QUEUE_REAL_TIME TO <platform user>;
GRANT SELECT ON <aga metrics schema>.LOGICAL_INTERFACE_CONTROLLER TO <platform user>;
GRANT SELECT ON <aga metrics schema>.PERIPHERAL TO <platform user>;
GRANT SELECT ON <aga metrics schema>.PERIPHERAL_REAL_TIME TO <platform user>;
GRANT SELECT ON <aga metrics schema>.QUEUE_SET1_REAL_TIME TO <platform user>;
GRANT SELECT ON <aga metrics schema>.QUEUE_SET2_REAL_TIME TO <platform user>;
GRANT SELECT ON <aga metrics schema>.SERVICE TO <platform user>;
GRANT SELECT ON <aga metrics schema>.SERVICE_MEMBER TO <platform user>;
GRANT SELECT ON <aga metrics schema>.SERVICE_REAL_TIME TO <platform user>;
GRANT SELECT ON <aga metrics schema>.SKILL_GROUP TO <platform user>;
GRANT SELECT ON <aga metrics schema>.SKILL_GROUP_REAL_TIME TO <platform user>;
```
- Connect to the AGA 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 QUEUE_SET1_REAL_TIME TO <platform user>;
GRANT SELECT ON QUEUE_SET2_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>;
```

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

```
SELECT * FROM <aga metrics schema>.AGENT_SKILL_GROUP_REAL_TIME;
SELECT * FROM <aga metrics schema>.CALL_TYPE;
SELECT * FROM <aga metrics schema>.CALL_TYPE_REAL_TIME;
SELECT * FROM <aga metrics schema>.CONTROLLER_TIME;
SELECT * FROM <aga metrics schema>.INTERACTION_QUEUE;
SELECT * FROM <aga metrics schema>.INTERACTION_QUEUE_REAL_TIME;
SELECT * FROM <aga metrics schema>.LOGICAL_INTERFACE_CONTROLLER;
SELECT * FROM <aga metrics schema>.PERIPHERAL;
SELECT * FROM <aga metrics schema>.PERIPHERAL_REAL_TIME;
SELECT * FROM <aga metrics schema>.QUEUE_SET1_REAL_TIME;
SELECT * FROM <aga metrics schema>.QUEUE_SET2_REAL_TIME;
SELECT * FROM <aga metrics schema>.SERVICE;
SELECT * FROM <aga metrics schema>.SERVICE_MEMBER;
SELECT * FROM <aga metrics schema>.SERVICE_REAL_TIME;
SELECT * FROM <aga metrics schema>.SKILL_GROUP;
SELECT * FROM <aga metrics schema>.SKILL_GROUP_REAL_TIME;
```

To AGA Metrics Schema on a Different Oracle Instance than the Platform Schema

Use the information on this tab to configure connectivity to the AGA metrics data source when it is installed on a different Oracle instance than the Platform schema. Before you begin:

- 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.

- To ensure a database link can be created, the user who will perform this operation must be granted the following permission:
`GRANT CREATE DATABASE LINK TO <platform user>`

1. Create a database link inside the Platform schema or a public database link.

For example:

```
CREATE DATABASE LINK atl12.gcldb81 CONNECT TO "<aga metrics
schema>" IDENTIFIED BY "<aga metrics schema owner pwd>" USING
'atlanta12';
```

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

For example:

```
SELECT * FROM Controller_Time@atl12.gcldb81;
```

To Cisco ICM Data Source from Platform Database on Oracle Instance

Use the information on this tab to configure connectivity to the Cisco ICM data source (ICM AWDB) when the Platform database is installed on an Oracle instance. Before you begin:

- Identify all ICM AWDBs that must be accessed by CCAdv and WA, as well as the SQL Servers that host those databases.
- Ensure that SQL Server accounts exist on all SQL Servers that host the ICM AWDBs accessed by CCAdv and WA.
- Ensure that each MSSQL Server account (see preceding bullet) has the MSSQL master database as a default database.
- Ensure that each ICM AWDB that must be accessed by CCAdv and WA has a user mapped to the relevant SQL Server account (see preceding bullets). The minimum requirement is that this 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
```

- Ensure the user has the preceding object-level permissions or this user is assigned to an equivalent user-defined database role. If it is allowed by your organization's 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.

- Ensure the Oracle Database Gateway for SQL Server is installed.
- Ensure the Gateway Initialization parameter file(s) exists for each Cisco ICM data source used by CCAdv and WA.
- Ensure the Oracle Net Listener configuration file has an entry for every gateway instance that exists for Cisco ICM data sources.
- Ensure the Oracle database that hosts the Platform schema is configured for Gateway Access and its tnsnames.ora configuration file contains a separate entry for each gateway instance. The alias from each such entry is used as database link creation parameters.

For detailed information about SQL Server security configuration, see the online documentation for Microsoft SQL Server at <http://msdn.microsoft.com>.

For detailed information about Oracle Database Gateway for SQL Server installation and configuration, see http://docs.oracle.com/cd/E18283_01/gateways.112/e12061/sqlserver.htm.

1. Create – or have your DBA create – a separate database link for each ICM source using a corresponding gateway instance. The links can be created inside the Platform schema or they can be created as public database links.

Create database links using the following pattern:

```
CREATE [PUBLIC] 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 entry of the corresponding gateway instance contained in the tnsnames.ora file.

For example:

```
CREATE PUBLIC DATABASE LINK "prod67543.icm1" CONNECT TO "user1"  
IDENTIFIED BY "password1" USING 'dg4mssql2';
```

2. Test the links from SqlDeveloper or run a select statement against the whole set of views as Platform user.

For example:

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

The configuration of ICM data sources is now complete.

Database Secure Deployment

This page describes secure deployment for MS SQL 2008 and Oracle 11g databases.

<tabber>

Secure Deployment for MS SQL Server 2008=

For MS SQL Server 2008 secure deployment, Genesys recommends using MS SQL Server Transparent Data Encryption (TDE) which performs a real-time I/O encryption and decryption of the data and log files. This method has only a minor impact on performance, which is critical for the Advisors Suite.

It is important to mention that TDE is available only for MS SQL Server Enterprise edition. The data cannot be encrypted using TDE if any other MS SQL Server edition is used.

Advisors Suite MS SQL databases do not have any properties that can prevent the application of TDE. The databases do not contain any READ-ONLY file groups, full text indexes, or filestreams. Users must follow the standard Microsoft documentation related to this topic.

The Advisors Suite does not support MS SQL Server cell-level encryption.

|= 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 Oracle 11g, which allows the encryption of the entire content of a tablespace.

To verify that databases are secured with TDE encryption, do the following:

1. Run the following query and all your tables should be using the ENCRYPTED_TS tablespace:
`select * from user_tables`
2. Run the following query and check if the ENCRYPTED_TS table space shows Yes:
`select tablespace_name,encrypted from user_tablespaces`

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

[+] Platform, Metric Graphing, and Genesys Adapter Metrics Databases

Initial Platform, Metric Graphing, and Genesys Adapter Metrics database scripts contain tablespace names in the form of variables in each create SQL statement for tables, primary keys, and indexes. The tables and indexes are distributed among several groupings based on Genesys' recommendations related to the data update patterns and its usage characteristics.

The Platform deployment script replaces the variables dynamically with the values you provide in the deployment script dialog. The deployment script generates a new `runObjCre.sql` script with the substituted variables. The deployment script executes `runObjCre.sql` and other SQL scripts in a

certain order.

It is important to make a decision about what objects need encryption and what objects should go to what tablespace before the deployment script execution.

If you decide to place all objects into one single encrypted tablespace, specify the tablespace as a user default data tablespace, and then read the script dialog prompts to insure this tablespace is used for all objects (that is, on all prompts, specify the name of this tablespace, or simply press Enter). If you want to use different encrypted tablespaces for different groups of objects predefined in the scripts, you must specify the tablespace names you have chosen for this purpose on the corresponding prompts. Review the `Readme.txt` file supplied with the scripts to find out how the objects are grouped in the scripts.

If a more granular customization is necessary (for instance change table/index grouping or encrypt the data on the column level), you will need to implement the following steps:

1. Run the deployment script from SQL*plus to generate `runObjCre.sql`.
2. Drop the previously created user.
3. Customize the generated `runObjCre.sql`.
4. Save it and then execute the scripts in the following order:
 - a. Platform schema:


```
runUshrCre.sql
runObjCre.sql
version_ROUTINE.sql
version_FA_ROUTINE.sql
version_INIT_DATA.sql
version_CUSTOM_ROUTINE.sql
exec spCompileInvalid();
```
 - b. Metrics Graphing schema:


```
runMgUshrCre.sql
runObjCre.sql
version_INIT_DATA.sql
version_ROUTINE.sql
exec spCompileInvalid();
```
 - c. Genesys Adapter Metrics schema:


```
runMetricsUshrCre.sql
runObjCre.sql
gc_metrics_new_version_ROUTINE.sql
exec spCompileInvalid();
```

List of Function-Based Indexes


TDE limitations related to the column-based encryption of the content with function-based indexes are applicable to the Advisors Suite. The Advisors schema contains a number of function-based indexes that need to be modified or dropped if the column-based encryption of the related columns is chosen. See the following Table.

Platform Schema

Index	Table	Column expression
IX_APPLICATION_NAME	APPLICATION – Contains application group metadata	UPPER("NAME")
IX_CALL_APP_UP	CALL_APPLICATION – Contains metadata for queues, call types, services, interaction queues	UPPER("NAME")
IX_CALL_CENTER_NAME	CALL_CENTER – Contains contact center metadata	UPPER("NAME")
IX_CALL_CREGION_NAME	REGIONS – Contains metadata for geographic regions, reporting regions and operating units	UPPER("NAME") , UPPER("TYPE")
IX_CG_UP	CONTACT_GROUP – Contains metadata for workforce contact groups	UPPER("NAME")
IX_CG_ORIGIN	CONTACT_GROUP	UPPER("WFM_EQUIVALENT_ID") , UPPER("SOURCE_SYSTEM")
IX_CONTACT	CONTACT – Contains Advisors users contact data	UPPER("EMAIL")
IX_PG_NAME	PG – Contains metadata for peripheral gateways	UPPER("PG_NAME")
IX_USERS_USERNAME	USERS – Contains the list of Advisor users	UPPER("USERNAME")
IX_KEY_ACTION_NAME	KEY_ACTION	UPPER("NAME")
IX_ADAPTER_INST_HOST_PORT	ADAPTER_INSTANCES	UPPER("HOST")

Create the Advisors User Account

Roadmap


1. **[+] Install the databases that correspond to the Advisors products you will deploy.**
 - a. Advisors Genesys Adapter metrics database
 - b. Advisors Platform database
 - c. Advisors Cisco Adapter database (if you use ACA)
 - d. Metric Graphing database
2.  Create the Advisors User and the Object Configuration User in Configuration Server.
3. **[+] Install the Platform service (Geronimo) on all servers on which you will deploy one of the Advisors components.**
 - Contact Center Advisor
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. **[+] Install the Advisors components for your enterprise.**
 - a. Contact Center Advisor
 - b. Workforce Advisor
 - c. Contact Center Advisor – Mobile Edition

- d. SDS and Resource Management
- e. Frontline Advisor
- 6. Make any required configuration changes.

You must create an account in the Configuration Server that can be used by the Advisors products to connect to and retrieve information from the Configuration Server. In this Deployment Guide, the account is referred to as the Advisors User account, but you can give the account a name of your choice. That is, it is not necessary to name the account *Advisors User*. The permissions shown in the following Table are required for this account.

Object	Permissions	Notes
Applications folder	Execute	Only for Configuration Server 8.1.2 and later. Required for the Platform and AGA user account to connect to the Configuration Server and Stat Servers.
Stat Server Applications	Read	
Tenants	Read	
Agent Groups	Read, Read Permissions, Change, Change Permissions	Starting in Release 8.1.5, Change and Change Permissions are

Object	Permissions	Notes
		needed to propagate changes saved in the Base Object Configuration page to Configuration Server.
Switches	Read	
DNs (of type ACD Queues and Virtual Queues)	Read, Read Permissions, Change, Change Permissions	Starting in Release 8.1.5, Change and Change Permissions are needed to propagate changes saved in the Base Object Configuration page to Configuration Server.
Persons	Read, Read Permissions	
	Change	Only required if Advisors Administration module will be used to modify user accounts, or if the Resource Management


Object	Permissions	Notes
		Console will be used to modify an agent's skill.
 Skills folder	Read	Only required if the Resource Management Console will be used to modify an agent's skill.
Scripts (of type Interaction Queues)	Read, Read Permissions, Change, Change Permissions	Starting in Release 8.1.5, Change and Change Permissions are needed to propagate changes saved in the Base Object Configuration page to Configuration Server.
Access Groups	Read, Read Permissions	
	Change	Only required if Advisors Administration module will be

Object	Permissions	Notes
		used to modify user accounts.
NEW Calling lists	Read, Read Permissions, Change, Change Permissions	Starting in Release 8.5.0, Change and Change Permissions are needed to propagate changes saved in the Base Object Configuration page to Configuration Server.
Roles	Read, Read Permissions	Used to determine functional permissions for users.
Business Attributes	Read, Read Permissions	Used to determine access to Advisors metadata objects.
Advisors Metrics Business Attributes	Read, Create, Change, NEW Delete, Read Permissions, Change Permissions	Used for the Metric Manager beginning in Release 8.1.3.
Folders in Persons	Read, Read Permissions	Required for

Object	Permissions	Notes
		FA.
Folder in Agent Groups	Read, Read Permissions	Required for FA.

Create the Data Manager Base Object Configuration User

Roadmap

1. **[+] Install the databases that correspond to the Advisors products you will deploy.**
 - a. Advisors Genesys Adapter metrics database
 - b. Advisors Platform database
 - c. Advisors Cisco Adapter database (if you use ACA)
 - d. Metric Graphing database
2.  Create the Advisors User and the Object Configuration User in Configuration Server.
3. **[+] Install the Platform service (Geronimo) on all servers on which you will deploy one of the Advisors components.**
 - Contact Center Advisor
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. **[+] Install the Advisors components for your enterprise.**
 - a. Contact Center Advisor
 - b. Workforce Advisor

- c. Contact Center Advisor – Mobile Edition
 - d. SDS and Resource Management
 - e. Frontline Advisor
6. Make any required configuration changes.

You must configure a user account in Configuration Server so that security permissions can be assigned to allow object configuration for the CCAdv/WA module in the Advisors Administration module (Base Object Configuration page). This is the *Object Configuration User*. This user must be created in the Configuration Server *before* you install Advisors Platform. Advisors Platform installer prompts you for the account name.

You create the Object Configuration User account in Genesys Configuration Manager. This user account is a container for security permissions for objects (agent groups, calling lists, and queues) in the Configuration Server. You grant a Read permission for the monitored objects to select one or more source objects as monitored objects in a deployment.

This configuration is not required on Platform deployments that do not have CCAdv/WA deployed. For example, if only FA is deployed on a particular Platform instance, this configuration must be left blank.

For more information about Data Manager and the Object Configuration User, see [Data Manager](#).

Deploying Advisors


The Deploying Advisors section contains topics to assist you when you use the Performance Management Advisors installation files to deploy Advisors components. Ensure you read the **Prerequisites** before you begin deployment.

Deploying Advisors Platform

You run a .jar installation file to deploy Advisors Platform.

You can deploy Advisors Platform on a Red Hat Linux or a Windows platform, and with Oracle or MS SQL databases.

Roadmap

1. **[+] Install the databases that correspond to the Advisors products you will deploy.**
 - a. Advisors Genesys Adapter metrics database
 - b. Advisors Platform database
 - c. Advisors Cisco Adapter database (if you use ACA)
 - d. Metric Graphing database
2. Create the Advisors User and the Object Configuration User in Configuration Server.
3.  Install the Platform service (Geronimo) on all servers on which you will deploy one of the Advisors components.
 - Contact Center Advisor
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. **[+] Install the Advisors components for your enterprise.**
 - Contact Center Advisor

- Workforce Advisor
 - Contact Center Advisor – Mobile Edition
 - Frontline Advisor
 - SDS and Resource Management
6. Make any required configuration changes.

<tabber>

Procedure=

1. If you are deploying Advisors platform on a Linux system, you must first create the Advisors group and user. The Advisors Platform is run as the *advisors user*, which belongs to the *advisors group*.

[+] Show Steps

- a. Open the shell.
- b. As root, create the Advisors group:

```
groupadd advisors
```

- c. As root, create the Advisors user in the Advisors group:

```
useradd -s /bin/bash -g advisors advisors
```

The preceding command creates the `/home/advisors` directory. If you want a different directory, you can use the following command:

```
useradd -g advisors -d <path to the desired directory> advisors
```

You can optionally set a password for the Advisors user:

```
passwd advisors
```

Genesys recommends that you mount `/home` as a separate partition.

2. Install Oracle Java Development Kit (JDK).

[+] Help with Linux environments

- a. Download the latest version of an Advisors-supported Oracle JDK from <http://www.oracle.com/>

technetwork/java/javase/downloads/index.html

The correct file is an archive binary file (.tar.gz). In the following Steps of this procedure, JDK 7 is used as an example. Ensure you enter the correct version number of the Oracle JDK you use in your installation.

- b. As root, navigate to the directory that has the downloaded Oracle JDK and copy the Oracle JDK archive binary file to the Advisors home directory:

```
cp ./jdk-7u<version>-linux-x64.tar.gz /home/advisors
```

- c. Navigate to the Advisors home directory:

```
cd /home/advisors
```

- d. As root, unpack the archive and install the JDK:

```
tar zxvf jdk-7u<version>-linux-x64.tar.gz
```

- e. As root, change the owner of the installed JDK:

```
chown -R advisors:advisors jdk1.7.0_<version>
```

- f. As root, change to the Advisors user and test JDK:

```
su - advisors
```

```
./jdk1.7.0_<version>/bin/java -version
```

You should see output similar to the following:

```
java version "1.7.0_40"
```

```
Java(TM) SE Runtime Environment (build 1.7.0_40-b43)
```

```
Java HotSpot(TM) 64-Bit Server VM (build 24.0-b56, mixed mode)
```

3. Place the advisors-platform-installer-<version>.jar file into the Advisors home directory.

[+] Show additional information for Linux environments

- a. You can start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled:

```
ssh -X root@<host>
```

- b. As root, place the advisors-platform-installer-<version>.jar file into the Advisors home directory.

4. Launch the installation file.

[+] Show Steps for Linux

- a. As root, navigate to the Advisors home directory:

```
cd /home/advisors
```

- b. As root, run the Advisors platform installer. The page format of this document might cause a line break in the following command, but you must enter it on one line in the command prompt window:

```
./jdk1.7.0_<version>/bin/java -jar advisors-platform-installer-<version>.jar
```

[+] Show Step for Windows

Do one of the following:

- Open a command line window, and enter the following command:

```
advisors-platform-installer-<version>.jar
```

- Double-click the advisors-platform-installer-<version>.jar file in the release bundle.

Double-clicking might not work due to system settings, but using the command line terminal should always work. Genesys recommends using the command line window to launch the installer.

5. On the **Module to Install** screen, install the Administration workbench, if required.

[+] Show Important Notes

On the **Module to Install** screen, select the Administration workbench checkbox to install this package. Selecting this option installs the Administration module.

Starting in Release 8.1.5, Frontline Advisor administration is combined with the Administration workbench (module). To administer FA, you must install the Administration workbench with at least one FA instance.

If you are installing Advisors Platform to support a clustered Advisors suite server, then install only one instance of the Administration workbench, on one system in the cluster. It is best to install the Administration workbench on a system that is not running the web services for one of the Advisors applications.

For more information about a clustered Advisors suite server, see [Scaling the System to Increase Capacity](#).

6. On the **Languages for E-mail Templates** screen, specify the languages to use in e-mail templates.

[+] Show Notes

If no languages are selected, English is used.

You can select one option, or more than one, regardless of the regional and language setting of the system on which you are installing the platform.

7. On the **Destination Directory** screen, specify the directory for your Advisors installation.

[+] Show Notes

Select the 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.

8. On the **Java Development Kit** screen, enter or select the root directory of the Java Development Kit (JDK).

9. On the **Application Server Configuration** screen enter the port numbers that the Geronimo application server will use. If you are installing only one deployment of Advisors, then accept the defaults

that the installer offers.

Important

If you install Advisors on Linux and need to change the naming port, update the Advisors Platform service startup script as specified in [Step 18](#).

10. On the **Cluster Node configuration** screen, configure the Advisors Platform installation as a unique node in the cluster. Each server on which you install Advisors Platform requires a unique cluster node ID. On this screen you also enter the port number that nodes in this cluster use to communicate.

[+] Show Notes

Configure the node with the following information:

- **Node ID** – A unique ID across all Platform installations. The ID must not contain spaces or any special characters, and must be only alpha numeric. Node IDs are not case sensitive. Within one cluster, Node1, node1, and NODE1 are considered to be the same ID. You can use node1, node2, and so on.
- **IP Address/Hostname** – The IP address or host name that other cluster members will use to contact this node, for example, 192.168.100.1. It is not localhost or 127.0.0.1. When using numerical IP v6 addresses, enclose the literal in brackets.
- **NEW** **Port number** that the nodes in this cluster use to communicate. If you are installing only one deployment of Advisors, accept the default that the installer offers. The port number must be unique to this deployment of Advisors. All nodes in one cluster must use the same port number.
- **Localhost address** – The local host address: localhost or 127.0.0.1.

11. **NEW** On the **Cache Configuration** screen, specify the port to be used by the distributed cache for communication. If you are installing only one deployment of Advisors, accept the default that the installer offers.

The port number must be unique to this deployment of Advisors. All nodes in one cluster must use the same port number.

12. On the **Genesys Config Server Connection Details** screen, configure the connection to the Genesys Configuration Server.

[+] Show Notes

- **Config Server Name** – The name of the primary configuration server; for example, confserv. The name is obtained from the Configuration Manager and is case sensitive.
- **Config Server Address** – The name or IP address of the machine hosting the Configuration Server. When using numerical IPv6 addresses, enclose the literal in brackets.
- **Config Server Port Number** – The port on which the configuration server is listening; for example, 2020. If you enter a port number in this field, and then enable a TLS connection, this port number is ignored.
- **Config Server Client Name** – Enter the name of the application that Advisors Platform will use to log in to the Configuration Server (for example, default).
- **Config Server user** – The user name of the account that Advisors Platform will use to connect to the Configuration Server; for example, default.
- **Config Server password** – The password of the account that Advisors Platform will use to connect to the Configuration Server. The Genesys Configuration Server password is encrypted and saved in the

..\GCTI\Advisors\conf\GenesysConfig.properties file by default (unless altered in [Step 5](#)). To change the password, see [Change Encrypted Passwords](#).

- **Enable TLS connection** – To configure a TLS connection to the Configuration Server, select this option on the installation screen.
- **Config Server TLS Port Number** – Enter the Configuration Server TLS port number. When TLS is enabled, Advisors Platform uses the TLS port number instead of the unsecured port number.
- **Locate TLS properties file** – Identify the location of the TLS properties file. The TLS properties file contains all the properties required to connect successfully using TLS, as well as any other optional TLS attributes that you use.
- **Add backup server** – Select this checkbox if you have a backup Configuration Server for this installation.
If you select the Add backup server checkbox, the **Backup config server** screen displays after you click Next. Enter the backup Configuration Server details on the **Backup config server** screen:
 - Backup Server Name
 - Backup Server Address
 - Backup Server Port Number

13. On the **CCAdv/WFAdv Object Configuration User** screen, enter the name of the Object Configuration User account (configured in Configuration Server). You must enter this information if you use a Genesys data source and will be deploying Contact Center Advisor/Workforce Advisor (CCAdv/WA). This is not applicable on a Platform installation if CCAdv/WA is deployed with only Cisco data sources, or if you intend to deploy only Frontline Advisor (FA).

[+] Show Notes

The Object Configuration User account is used by Data Manager for object configuration for the CCAdv/WA modules.

You are not prompted for the password for this user account because there is no user authentication performed for this user.

14. On the **User Management Options** screen, configure options associated with user activities.

[+] Show Steps

1. To synchronize user updates, select the checkbox. 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. Enabling this option on multiple clustered instances of Platform will result in redundant updates to the database. Other Platform instances in the cluster will continue to provide PSDK access to Advisors modules, so for them, this configuration option can be deselected. Genesys recommends selecting the Synchronize user updates? checkbox on a node that is not running the web services for one of the Advisors applications.
2. Add the name of the default Genesys tenant to which new users will be added. The name of the tenant is case sensitive.
3. Select the Allow Password Modification? checkbox to enable the Forgot your password? functionality in the Advisors login page, the Administration module, and the dashboards. If you leave this option unselected, you still see the functionality in the user interface, but if you try to use it, Advisors tells you that password modification is not enabled.
Note that the user's ability to see this functionality depends on the

Advisors.ChangePassword.canView privilege being granted to the user in Configuration Manager.

Warning

Performance Management Advisors support Genesys Management Framework Release 8.1.x, but do not fully support the password security authentication options available in Management Framework. Users can be locked out of Advisors if you use Genesys Management Framework 8.1.x in your enterprise. To avoid lockouts, do one or both of the following:

- Change the following two options in Management Framework to true: the no password change at first login option and the override password expiration option.
- Assign the Advisors.ChangePassword.canView privilege to all users.

For information about the no password change at first login and override password expiration options, see *Genesys Framework Configuration Options Reference Manual*.

15. On the **Database Type** screen, select either the SQL Server or the Oracle option – whichever you use for Advisors platform database(s). The screens that follow are dependent on your selection:

[+] Show Step for SQL Server

On the **Genesys Advisors Platform Database** screen, 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). If the database server is a named instance, then omit the port number.

If you use numerical IPv6 addresses, enclose the literal in brackets.

[+] Show Steps for Oracle

1. On the **Oracle setup type** screen, select the Basic option.
2. On the **Genesys Advisors Platform Database** screen, specify the parameters for the Advisors platform database:
 - Database server—The host name or IP address of the database server. When using numerical IP v6 addresses, enclose the literal in brackets.
 - Database port number—The database server's port number.
 - SID—The unique name of the database instance.
 - Database user—The Advisors user with full access to the Advisors platform database.
 - Database user password—The password created and used for the Advisors platform database.
3. On the **Oracle JDBC Driver** screen, specify the location of the Oracle JDBC driver. 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.

[+] Show Steps for Oracle RAC

1. On the **Oracle setup type** screen, select the RAC connectivity setup option.
2. On the **Genesys Advisors Platform Database** screen, specify the parameters for the Advisors platform database:
 - Database user and Database user password—The database schema and password created and used for the Platform database.
 - Locate file—Enter the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. The installation wizard applies the specified advanced connection string when configuring the data sources.
3. On the **Oracle JDBC Driver** screen, specify the location of the Oracle JDBC driver. 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.

16. On the **Mail Service Configuration** screen, specify the e-mail settings that the Forgot Password functionality will use to send e-mail.

- SMTP Server—The SMTP service to use.
- Application from address—The *sender* of this e-mail; for example, D0-NOT-REPLY@genesys.com.
- Application to address—The *recipient* of this e-mail; for example, admin@genesys.com.

17. Click **Install**.

If errors display, diagnose them in the **Errors** tab, or refer to the **Troubleshooting** tab on this page.

18. If you use a Windows platform, install the Advisors windows service as follows:

[+] Show Steps

1. Open a command prompt, and change directory first to your Advisors base directory (for example, Program Files\GCTI\Advisors), then to bin\windows-x86.
2. Run InstallAdvisorsServer.bat.

If you use a Linux platform, validate that Advisors Platform installed successfully and then configure Advisors Platform to run automatically as a system service:

[+] Show Steps

- a. Open the shell.
- b. As root, run the following export command to add the JDK to your path:

```
export PATH=/home/advisors/jdk1.7.0_<version>/bin:$PATH
```

- c. As root, change the owner of the directory in which you installed the Advisors Platform to the Advisors user:

```
chown -R advisors:advisors <Advisors directory>
```

- d. Test the installation as the Advisors user.

- i. Specify the JDK path for this session (temporarily):

```
export JAVA_HOME=/home/advisors/jdk1.7.0_<version>
```

- ii. Start Advisors Platform:

```
./<Advisors directory>/geronimo-tomcat6-minimal-2.2.1/bin/geronimo.sh run
```

- iii. Ensure that there are no errors reported and that the Advisors Administration module is available at <http://<host>:8080/admin/>.

- e. Configure Advisors Platform to run automatically as a system service.

- i. As root, create an `/etc/init.d/advisors` file with the following contents; remember to replace `<version>` with the version number of your file and `<Advisors directory>` with your directory's name:

```
#!/bin/bash
# description: Advisors Platform Start Stop Restart
# processname: advisors
# chkconfig: 235 20 80

JAVA_HOME=/home/advisors/jdk1.7.0_<version>
export JAVA_HOME
PATH=$JAVA_HOME/bin:$PATH
export PATH
GERONIMO_BIN=/home/advisors/<Advisors directory>/geronimo-tomcat6-minimal-2.2.1/bin

case $1 in
start)
/bin/su advisors $GERONIMO_BIN/startup.sh
;;
stop)
$GERONIMO_BIN/shutdown.sh --user system --password manager
;;
restart)
$GERONIMO_BIN/shutdown.sh --user system --password manager
/bin/su advisors $GERONIMO_BIN/startup.sh
;;
esac
exit 0
```

Important

If you modified the default naming port when running the installer, and the naming port number is no longer 1099, then your non-default port number should be added to the above service control script. For example, if your naming port is 7075, you should add this port to the shutdown and restart sections:

```
stop)
```

```
$GERONIMO_BIN/shutdown.sh --port 7075 --user system --password manager  
;;
```

- ii. As root, make the startup script executable:

```
chmod 755 /etc/init.d/advisors
```

- iii. As root, configure the system to start the Advisors process at boot time:

```
chkconfig --add advisors  
chkconfig --level 235 advisors on
```

- iv. As root, check that the configuration is correct:

```
chkconfig --list advisors
```

The output should be similar to the following:

```
advisors 0:off 1:off 2:on 3:on 4:off 5:on 6:off
```

- v. As root, test the service startup script:

```
service advisors start
```

Wait until startup is complete and then open the browser (<http://<host>:8080/admin/>). The Administration module should be available after you log in.

- vi. As root, test the service stop script:

```
service advisors stop
```

Wait until shutdown is complete and then open the browser (<http://<host>:8080/admin/>). The page should be unavailable.

- vii. As root, test that Advisors Platform starts automatically after a reboot:

Warning

The following command restarts the whole system.

```
shutdown -r now
```

Wait until the system reboots, and then open the browser (<http://<host>:8080/admin/>). The Administration module should be available after you log in.

19. If you are running Platform with a 64-bit JVM, Genesys recommends that you increase your **Geronimo**

PermGen memory settings.

[-] Troubleshooting=

The following Table shows parameter validation errors that you may encounter at the end of installation.

Installation Error Message	Cause
<pre>[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:450) [java] at oracle.jdbc.driver.T4CPreparedStatement. doAll8(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)</pre>	<p>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).</p> <p>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 an Oracle database when someone runs a query such as 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.</p>
<pre>[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:</pre>	<p>Wrong database server name / IP address or port number</p>

Installation Error Message	Cause
"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.	
<pre>[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."</pre>	Wrong database name
<pre>[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</pre>	Wrong database user name or password
<pre>[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.</pre>	<p>The cluster member node identified by the IP address specified is not reachable. This may be for one of the following reasons:</p> <ul style="list-style-type: none"> • 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 to not respond to ICMP ping requests
<pre>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</pre>	<p>Produced in error and can be ignored.</p> <p>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.</p>


Installation Error Message	Cause
<pre> register) at java.security.AccessControlContext.checkPermission(Unknown Source) at java.lang.SecurityManager.checkPermission(Unknown Source) at com.sun.jmx.interceptor.DefaultMBeanServerInterceptor.checkMBeanTrust Permission(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) </pre>	
<pre> 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) </pre>	Produced in error and can be ignored.
<pre> [loadfile] Unable to load file: java.io.FileNotFoundException: C:\ (The system cannot find the path specified) </pre>	Produced in error and can be ignored.
<div>NEW</div> <pre> java.sql.SQLRecoverableException: IO Error: Connection reset </pre>	<p>Related to the operation of the Oracle JDBC driver. Use the following workaround.</p> <p>Edit the <jdk>/jre/lib/security/java.security file:</p>

Installation Error Message	Cause
	Change <code>securerandom.source=file:/dev/urandom</code> to <code>securerandom.source=file:///dev/urandom</code> .

Deploying Genesys Adapter

You run a .jar installation file to deploy Advisors Genesys Adapter (AGA) and Resource Management Console (RMC). You use the same installation file to deploy both, although you can install only a single component (either the AGA core service or RMC) during a single installer run. The installer guides you through the deployment. The screens displayed during your deployment are dependent on the selections you make on the **Install Type** and **Server Install Type** screens. The procedures on this page are specific to AGA deployment. If you are deploying RMC, see [Deploying SDS and RMC](#).

Roadmap

1. **[+] Install the databases that correspond to the Advisors products you will deploy.**
 - a. Advisors Genesys Adapter metrics database
 - b. Advisors Platform database
 - c. Advisors Cisco Adapter database (if you use ACA)
 - d. Metric Graphing database
2. Create the Advisors User and the Object Configuration User in Configuration Server.
3. **[+] Install the Platform service (Geronimo) on all servers on which you will deploy one of the Advisors components.**
 - Contact Center Advisor
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4.  Install each adapter you will use (AGA and ACA). See additional information for CCAAdv/WA installations.

5. **[+] Install the Advisors components for your enterprise.**

- Contact Center Advisor
- Workforce Advisor
- Contact Center Advisor – Mobile Edition
- Frontline Advisor
- SDS and Resource Management

6. Make any required configuration changes.

You can deploy AGA on a Red Hat Linux or a Windows platform, and with Oracle or MS SQL databases.

Starting in Release 8.1.5, source metric definitions and statistics templates that were previously stored in the Advisors Genesys Adapter (AGA) database move to Advisors Platform tables. Configured objects and filters that were previously stored in the Advisors Genesys Adapter database move to Genesys Configuration Server. If you are migrating to Advisors release 8.1.5 as part of a migration to release 8.5.x, you have the additional step of recreating the AGA metrics schema before migrating from 8.1.5 to 8.5.0. See the [Genesys 8.1 Performance Management Advisors Deployment Guide](#).

<tabber>

Migration Notes=

If you are migrating to a new software release, and not installing Advisors Genesys Adapter (AGA) for the first time, there is an existing AGA entry in the Adapter_Instances table in the Platform database. You have two options when upgrading your AGA instance:

1. Install the new AGA instance with the same host name and port number as the previous installation. The previous adapter is updated with the new configuration. For this option, you must have information about the earlier adapter to ensure you overwrite it successfully: host and port number. Ensure you enter that information on the Adapter Port and Registration Option installation screen to match the previous entry exactly. If this information is unavailable, you can find it in the ADAPTER_INSTANCES database table on the Platform database.
2. Install the new AGA instance with a different adapter host name and port number; it is added as a second adapter in the Platform database. Use this option to install a new adapter instance, or if you need to move the adapter to a new host name or port number. If moving the adapter to a new host name or port number, you must manually remove the previous adapter entry from the Platform database.

NEW Migrating the AGA Metrics Database or Schema

In release 8.1.5, you dropped and recreated the metrics schema or database as part of migration. This is unnecessary for release 8.5.0. To migrate to release 8.5.0, you use scripts supplied by

Genesys to simply remove old objects and then add new objects to the Advisors Genesys Adapter metrics database. Genesys provides two scripts for Oracle and one for MS SQL; see the following procedures. Review the `Readme.txt` file included with the scripts. The `Readme` file includes important information, including which tools Genesys recommends to execute the scripts.

Migration of AGA Oracle METRICS Schemas

1. Connect as the METRICS user.
2. Execute `gc_metrics_<version>_ObjectsDrop.sql`
3. Execute `gc_metrics_new_<version>_ObjectsPlus.sql`

Migration of AGA MS SQL Databases

1. Connect to the AGA metrics database.
2. Execute `gc_metrics_newdb_<version>.sql`

| MCR Extensions=

MCR extensions are required for your Stat Server only if Interaction Queue statistics are to be collected. Use the following procedure to deploy the extensions.

1. Install Stat Server.
2. Install the MCR extension package. The MCR version corresponding to the most recent Stat Server release can be obtained from the Genesys installation CD image.
3. Configure the JVM path options for the Stat Server in Configuration Manager using the Stat Server application Options tab. If you require more information about Stat Server configuration than is provided below, see *Framework 8.0 Stat Server Deployment Guide*.
 - a. Configure Stat Server Java options, such as `[java-config]`, `[java-options]`, and `[java-extensions]`.
 - b. Set the JVM Path to the `jvm.dll` file (for example: `C:\Program Files\Java\jre5\bin\client\jvm.dll`).
 - c. Set the `ext` directory to the relative path of the extensions directory under the Stat Server installation (the default is `./java/ext`).
 - d. Set the `lib` directory to the relative path of the library directory under the Stat Server installation (the default is `./java/lib`).
 - e. Select the `eServiceContactStat.jar` and `eServiceInteractionStat.jar` Java Extension jar files to be loaded.
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 table, set `enable-java` to `true`.
6. Under the Stat Server application Options tab, create a new section named `common`. Set the value of option `rebind-delay` to 0 (zero).

If you previously loaded the `statserverentries.cfg` file, this option is already there. Ensure you verify it is correct.
7. 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.

8. Restart both the Interaction Server and the Stat Server.

|–| AGA Server for CCAAdv/WA=

1. Place the aga-installer-<version>.jar file into the Advisors home directory.

[+] Show additional information for Linux environments

a. You can start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled:

```
ssh -X root@<host>
```

b. As root, place the aga-installer-<version>.jar file into the Advisors home directory.

2. Launch the AGA installation file.

[+] Show Steps for Linux

a. As root, navigate to the Advisors home directory:

```
cd /home/advisors
```

b. As root, run the AGA installer. The page format of this document might cause a line break in the following command, but you must enter it on one line in the command prompt window:

```
./jdk1.7.0_<version>/bin/java -jar aga-installer-<version>.jar
```

[+] Show Steps for Windows

Do one of the following:

- Open a command line window, and enter the following command:

```
java -jar aga-installer-<version>.jar
```

- Double-click the aga-installer-<version>.jar file in the release bundle.

Double-clicking might not work due to system settings, but using the command line terminal should always work. Genesys recommends using the command line window to launch the installer.

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.

3. On the **Install Type** screen, select the **Install Server** radio button. You can install only a single component (either the core service or RMC) during a single installer run.

4. On the **Server Install Type** screen, select the **Contact Center Advisor/Workforce Advisor** radio button.

After installation, you must install and start the AGA service.

5. On the **Installation details** screen, specify the installation directory and the directory in which the log files will appear. The default installation directory is C:\Program Files\GCTI\Advisors\Genesys\Adapter.

6. On the **Java Development Kit** screen, specify the location of the root directory of the Java installation.

7. On the **Database Type** screen, select either the SQL Server or the Oracle option – whichever you use for databases in your installation. The screens that follow are dependent on your selection:

[+] Show Step for SQL Server

On the **CCAdv/WA Metrics Database Configuration** screen, specify the parameters for the metrics database:

- **Server hostname**—The host name or IP address of the database server. When using numerical IPv6 addresses, enclose the literal in brackets.
- **Database port**—The database server's port number.
- **Database name/SID**—The unique name of the database instance; for example, `advisors_gametricsdb`.
- **Database user**—The Advisors user that will be used by the Adapter to access the database.
- **Database user password**—The password associated with the Advisors user that will be used by the Adapter to access the database.

Important

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 [Change Encrypted Passwords](#).

[+] Show Steps for Oracle

- On the **Oracle setup type** screen, select the Basic radio button.
- On the **Oracle JDBC Driver** screen, specify the location of the Oracle JDBC driver. 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`.
- On the **CCAdv/WA Metrics Database Configuration** screen, specify the parameters for the metrics database:
 - **Server hostname**—The host name or IP address of the machine where the CCAdv/WA metrics database is installed. When using numerical IP v6 addresses, enclose the literal in brackets.
 - **Database port**—The database server's port number.
 - **Database name/SID**—The unique name of the database instance; for example, `advisors_gametricsdb`.
 - **Database user**—The Advisors user that will be used by the Adapter to access the database.
 - **Database user password**—The password associated with the Advisors user that will be used by the Adapter to access the database.

Important

The CCAAdv/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 [Change Encrypted Passwords](#).

[+] Show Steps for Oracle RAC

- a. On the **Oracle setup type** screen, select the RAC connectivity setup option.
- b. On the **Oracle JDBC Driver** screen, specify the location of the Oracle JDBC driver. 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.
- c. On the **CCAAdv/WA Metrics Database Configuration - RAC** screen, specify the parameters for the metrics database:
 - Database user—The Advisors user that will be used by the Adapter to access the database.
 - Database password—The password associated with the Advisors user that will be used by the Adapter to access the database.

Important

The CCAAdv/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 [Change Encrypted Passwords](#).

- Locate file—Enter the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. The installation wizard applies the specified advanced connection string when configuring the data sources.

8. On the **Platform Database Configuration** screen, specify connection information for the the Advisors Platform database with which this AGA will be registered. You must complete this screen for all database types (MS SQL, Oracle basic, or Oracle RAC). If you use Oracle RAC, you will be prompted for additional information about the Advisors Platform database at [Step 11](#).

[+] Show More

Enter the following information about the Advisors platform database with which this adapter will register:

- server hostname or IP address
- SID
- port

- schema and corresponding password

9. On the **Genesys Data Source - Configuration Server** screen, configure the connection to the Genesys Configuration Server(s).

[+] Show Steps

- To connect to the primary (mandatory) Configuration Server in the Genesys environment, enter information in the following text fields:
 - **Name** – The name of the primary configuration 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 Configuration Server. When using numerical IPv6 addresses, enclose the literal in brackets.
 - **Port** – The port that the configuration server is listening on. If you enter a port number in this field, and then enable a TLS connection, this port number is ignored.
 - **Client name** – The name of the application that Advisors Platform will use to log in to the Configuration Server (for example, default).
 - **User name** – The user name of the account the Adapter will use to connect to the Configuration Server.
 - **Password** – The corresponding password of the account the Adapter will use to connect to the Configuration Server.

Important

The Genesys Configuration Server password is encrypted and saved in the <adapterhome>\conf\inf_genesys_adapter.properties file by default. To change the password, see [Change Encrypted Passwords](#).

- **Add backup server** – Select this checkbox only if you plan to configure the connection to a backup Configuration Server. The backup Configuration Server can be, but does not need to be, configured in a high-availability pair in Genesys.
- If you use a TLS connection to the Configuration Server, also complete the following:
 - **Enable TLS connection** – To configure a TLS connection to the Configuration Server, select this option on the installation screen. If you have a backup Configuration Server, AGA also connects to it using TLS if you enable a TLS connection to the primary Configuration Server.
 - **Config Server TLS Port Number** – Enter the Configuration Server TLS port number. If you enable a TLS connection, the TLS port number is used for both the primary and backup Configuration Servers. The port number for an unsecured connection is ignored. The primary and backup Configuration Servers must use the same TLS port number.
 - **Locate TLS properties file** – Identify the location of the TLS properties file. The TLS properties file contains all the properties required to connect successfully using TLS, as well as any other optional TLS attributes that you use. If you use a backup Configuration Server, the TLS properties for the primary server are also used for the backup server.
 - **Add backup server** – Select this checkbox only if you have a backup Configuration Server. The

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

- c. If you opted to add a backup Configuration Server, enter the information required to connect to that server on the **Genesys Data Source - Backup Configuration Server** screen:
 - Backup server name – The name of the backup configuration server. The name is obtained from the Configuration Manager and is case sensitive.
 - Backup host – The name or IP address of the machine hosting the backup Configuration Server. When using numerical IPv6 addresses, enclose the literal in brackets.
 - Backup server port – The port that the backup Configuration Server is listening on. If you enter a port number in this field, but enabled a TLS connection for the primary Configuration Server, this port number is ignored. If the primary server connection uses a TLS connection, then the backup server connection is also a TLS connection. When you enable the TLS connection, you must enter the Configuration Server TLS port number; Advisors uses that port for the connection for both the primary and backup Configuration Servers.

10. On the **Genesys Data Source - Stat Server Configuration** screen, configure the connection to the data source Stat Server(s).

[+] Show Steps

- a. To connect to the primary (mandatory) Stat Server in the Genesys environment, enter information in the following text fields:
 - 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. When using numerical IPv6 addresses, enclose the literal in brackets.
 - Port – The port that the Stat Server is listening on.
- b. If you have a backup Stat Server, also complete the following:
 - 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. When using numerical IPv6 addresses, enclose the literal in brackets.
 - Backup server port – The port on which the backup Stat Server listens.
- c. To configure a second or subsequent Stat Server (or Stat Server pair), select the Another Stat Server? checkbox. Repeat this step for each Stat Server (pair) you want to add. Up to four additional Stat Server pairs can be configured—that is, a total of 10 Stat Servers can be configured.
- d. On the **Genesys Data Source - Stat Server (continued)** screen, specify the types of statistics supported on the Stat Server pair you are associating with this Genesys Adapter instance. The default is the Core statistics type for the Stat Server pair if you do not make a selection from the options. After installation, the configuration option is unavailable in the Advisors user interface. If you require a change in the configuration after installation, you must update the Stat Server configuration table. If you make changes, you must restart the Genesys Adapter. The 3rd Party Media and Multimedia statistics options require you to install the corresponding Java extensions on the Stat Servers. For more information, see [Adapter Stat Server Configuration](#).

11. On the **Adapter Port and Registration Option** screen, you enter information that the Advisors

Platform database requires to register this adapter instance.

If your enterprise has an Oracle RAC database installation, the **Enter Advisor Platform Database information for Adapter Registration** screen prompts you for additional information about the Platform database with which the adapter will register.

[+] Show More

You must enter the following information about your adapter:

- The port number on which the Genesys Adapter web services will run. You can use the default port, 7000, if no other application is using that port.
- The name, host IP address, and description of the AGA server.

For an Oracle RAC installation, you must also enter the following information about the Advisors Platform database on the **Enter Advisor Platform Database information for Adapter Registration** screen:

- The database schema and corresponding password created and used for the platform database.
- Enter the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. The installation wizard applies the specified advanced connection string when configuring the data sources.

12. After installation is complete, click Show Details, and then click Install and verify that there were no errors reported during installation.

13. Configure AGA to run automatically as a system service.

[+] Show Steps for Linux

- As root, create an /etc/init.d/advisors-aga file with the following contents; remember to replace <version> with the version number of your file and <Advisors directory> with your directory's name:

```
#!/bin/bash
# description: Advisors Genesys Adapter Start Stop Restart
# processname: advisors-aga
# chkconfig: 235 20 80
#
# This script should be edited and installed in /etc/init.d directory
#
# Before using please edit PATH and AGA_BIN.
#

export PATH=/<path to jdk>/jdk1.7.0_<version>/bin:$PATH

#NOTE: if AGA is installed not in home/advisors, change this part of the path too
AGA_BIN=/home/advisors/<AGA directory>/bin

cd $AGA_BIN

case $1 in
start)
/bin/su advisors ./startup.sh
;;
stop)
./shutdown.sh
;;
restart)
./shutdown.sh
```

```
/bin/su advisors ./startup.sh
;;
esac
exit 0
```

- b. As root, make the startup script executable:

```
chmod 755 /etc/init.d/advisors
```

- c. As root, configure the system to start the Advisors process at boot time:

```
chkconfig --add advisors
chkconfig --level 235 advisors on
```

- d. As root, check that the configuration is correct:

```
chkconfig --list advisors
```

The output should be similar to the following:

```
advisors 0:off 1:off 2:on 3:on 4:off 5:on 6:off
```

- e. As root, test the service starts correctly:

```
service advisors-aga start
```

Wait until startup is complete. Open the Advisors interface in your browser (<http://<host>:8080/admin/>) and log in; the page should be available.

- f. As root, test that the service stops correctly:

```
service advisors-aga stop
```

Wait until shutdown is complete. Open the Advisors interface in your browser (<http://<host>:8080/admin/>) and log in; the page should be unavailable.

[+] Show steps for Windows

To install the Windows service, do one of the following:

1. Navigate to the \bin folder and double-click the Install-Adapter-NT.bat file.
2. Open a command line window, navigate to the \bin folder, and execute the bat file.

14. For every Stat Server (primary and backup) that you specified as part of the AGA server deployment, 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 the location you specified in which to install the Advisors 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
```

| - | AGA Server for FA=

1. Place the `aga-installer-<version>.jar` file into the Advisors home directory.

[+] Show additional information for Linux environments

- a. You can start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled:

```
ssh -X root@<host>
```

- b. As root, place the `aga-installer-<version>.jar` file into the Advisors home directory.

2. Launch the AGA installation file.

[+] Show Steps for Linux

- a. As root, navigate to the Advisors home directory:

```
cd /home/advisors
```

- b. As root, run the AGA installer. The page format of this document might cause a line break in the following command, but you must enter it on one line in the command prompt window:

```
./jdk1.7.0_<version>/bin/java -jar aga-installer-<version>.jar
```

[+] Show Steps for Windows

Do one of the following:

- Open a command line window, and enter the following command:

```
java -jar aga-installer-<version>.jar
```
- Double-click the `aga-installer-<version>.jar` file in the release bundle.

Double-clicking might not work due to system settings, but using the command line terminal should always work. Genesys recommends using the command line window to launch the installer.

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.

3. On the **Install Type** screen, select the **Install Server** radio button. You can install only a single component (either the core service or RMC) during a single installer run.

4. On the **Server Install Type** screen, select the **Frontline Advisor** radio button.

After installation, you must install and start the service.

5. On the **Installation details** screen, specify the installation directory and the directory in which the log files will appear. The default installation directory is `C:\Program Files\GCTI\Advisors\Genesys\Adapter`.

6. On the **Java Development Kit** screen, specify the location of the root directory of the Java installation.

7. On the **Database Type** screen, select either the **SQL Server** or the **Oracle** option – whichever you use for databases in your installation.

If you select **Oracle** as your database type, you are prompted for additional information.

[+] Show Steps for single-instance Oracle installations

- a. On the **Oracle setup type** screen, select the Basic radio button.
- b. On the **Oracle JDBC Driver** screen, specify the location of the Oracle JDBC driver. 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.

[+] Show Steps for Oracle RAC installations

- a. On the **Oracle setup type** screen, select the RAC connectivity setup option.
- b. On the **Oracle JDBC Driver** screen, specify the location of the Oracle JDBC driver. 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.

8. On the **Platform Database Configuration** screen, specify connection information for the the Advisors Platform database with which this AGA will be registered. You must complete this screen for all database types (MS SQL, Oracle basic, or Oracle RAC). If you use Oracle RAC, you will be prompted for additional information about the Advisors Platform database at [Step 11](#).

[+] Show More

Enter the following information about the Advisors platform database with which this adapter will register:

- server hostname or IP address
- SID
- port
- schema and corresponding password

9. On the **Genesys Data Source - Configuration Server** screen, configure the connection to the Genesys Configuration Server(s).

[+] Show Steps

- a. To connect to the primary (mandatory) Configuration Server in the Genesys environment, enter information in the following text fields:
 - Name – The name of the primary configuration 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 Configuration Server. When using numerical IPv6 addresses, enclose the literal in brackets.
 - Port – The port that the configuration server is listening on. If you enter a port number in this field, and then enable a TLS connection, this port number is ignored.

- **Client name** – The name of the application that Advisors Platform will use to log in to the Configuration Server (for example, default).
- **User name** – The user name of the account the Adapter will use to connect to the Configuration Server.
- **Password** – The corresponding password of the account the Adapter will use to connect to the Configuration Server.

Important

The Genesys Configuration Server password is encrypted and saved in the <adapterhome>\conf\inf_genesys_adapter.properties file by default. To change the password, see [Change Encrypted Passwords](#).

- **Add backup server** – Select this checkbox only if you plan to configure the connection to a backup Configuration Server. The backup Configuration Server can be, but does not need to be, configured in a high-availability pair in Genesys.
- b. If you use a TLS connection to the Configuration Server, also complete the following:
- **Enable TLS connection** – To configure a TLS connection to the Configuration Server, select this option on the installation screen. If you have a backup Configuration Server, AGA also connects to it using TLS if you enable a TLS connection to the primary Configuration Server.
 - **Config Server TLS Port Number** – Enter the Configuration Server TLS port number. If you enable a TLS connection, the TLS port number is used for both the primary and backup Configuration Servers. The port number for an unsecured connection is ignored. The primary and backup Configuration Servers must use the same TLS port number.
 - **Locate TLS properties file** – Identify the location of the TLS properties file. The TLS properties file contains all the properties required to connect successfully using TLS, as well as any other optional TLS attributes that you use. If you use a backup Configuration Server, the TLS properties for the primary server are also used for the backup server.
 - **Add backup server** – Select this checkbox only if you have a backup Configuration Server. The backup Configuration Server can be, but does not need to be, configured in a high-availability pair in Genesys.
- c. If you opted to add a backup Configuration Server, enter the information required to connect to that server on the **Genesys Data Source - Backup Configuration Server** screen:
- **Backup server name** – The name of the backup configuration server. The name is obtained from the Configuration Manager and is case sensitive.
 - **Backup host** – The name or IP address of the machine hosting the backup Configuration Server. When using numerical IPv6 addresses, enclose the literal in brackets.
 - **Backup server port** – The port that the backup Configuration Server is listening on. If you enter a port number in this field, but enabled a TLS connection for the primary Configuration Server, this port number is ignored. If the primary server connection uses a TLS connection, then the backup server connection is also a TLS connection. When you enable the TLS connection, you must enter the Configuration Server TLS port number; Advisors uses that port for the connection for both the primary and backup Configuration Servers.

10. On the **Genesys Data Source - Stat Server Configuration** screen, configure the connection to the

data source Stat Server(s).

[+] Show Steps

- a. To connect to the primary (mandatory) Stat Server in the Genesys environment, enter information in the following text fields:
 - 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. When using numerical IPv6 addresses, enclose the literal in brackets.
 - Port – The port that the Stat Server is listening on.
- b. If you have a backup Stat Server, also complete the following:
 - 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. When using numerical IPv6 addresses, enclose the literal in brackets.
 - Backup server port – The port on which the backup Stat Server listens.
- c. To configure a second or subsequent Stat Server (or Stat Server pair), select the Another Stat Server? checkbox. Repeat this step for each Stat Server (pair) you want to add. Up to four additional Stat Server pairs can be configured—that is, a total of 10 Stat Servers can be configured.
- d. On the **Genesys Data Source - Stat Server (continued)** screen, specify the types of statistics supported on the Stat Server pair you are associating with this Genesys Adapter instance. The default is the Core statistics type for the Stat Server pair if you do not make a selection from the options. After installation, the configuration option is unavailable in the Advisors user interface. If you require a change in the configuration after installation, you must update the Stat Server configuration table. If you make changes, you must restart the Genesys Adapter. The 3rd Party Media and Multimedia statistics options require you to install the corresponding Java extensions on the Stat Servers. For more information, see [Adapter Stat Server Configuration](#).

11. On the **Adapter Port and Registration Option** screen, you enter information that the Advisors Platform database requires to register this adapter instance.

If your enterprise has an Oracle RAC database installation, the **Enter Advisor Platform Database information for Adapter Registration** screen prompts you for additional information about the Platform database with which the adapter will register.

[+] Show More

You must enter the following information about your adapter:

- The port number on which the Genesys Adapter web services will run. You can use the default port, 7000, if no other application is using that port.
- The name, host IP address, and description of the AGA server.

For an Oracle RAC installation, you must also enter the following information about the Advisors Platform database on the **Enter Advisor Platform Database information for Adapter Registration** screen:

- The database schema and corresponding password created and used for the platform database.
- Enter the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database

administrator. The installation wizard applies the specified advanced connection string when configuring the data sources.

12. After installation is complete, click **Show Details**, and then click **Install** and verify that there were no errors reported during installation.

13. Configure AGA to run automatically as a system service.

[+] Show Steps for Linux

- a. As root, create an `/etc/init.d/advisors-aga` file with the following contents; remember to replace `<version>` with the version number of your file and `<Advisors directory>` with your directory's name:

```
#!/bin/bash
# description: Advisors Genesys Adapter Start Stop Restart
# processname: advisors-aga
# chkconfig: 235 20 80
#
# This script should be edited and installed in /etc/init.d directory
#
# Before using please edit PATH and AGA_BIN.
#

export PATH=/<path to jdk>/jdk1.7.0_<version>/bin:$PATH

#NOTE: if AGA is installed not in home/advisors, change this part of the path too
AGA_BIN=/home/advisors/<AGA directory>/bin

cd $AGA_BIN

case $1 in
start)
/bin/su advisors ./startup.sh
;;
stop)
./shutdown.sh
;;
restart)
./shutdown.sh
/bin/su advisors ./startup.sh
;;
esac
exit 0
```

- b. As root, make the startup script executable:

```
chmod 755 /etc/init.d/advisors
```

- c. As root, configure the system to start the Advisors process at boot time:

```
chkconfig --add advisors
chkconfig --level 235 advisors on
```

- d. As root, check that the configuration is correct:

```
chkconfig --list advisors
```

The output should be similar to the following:

```
advisors 0:off 1:off 2:on 3:on 4:off 5:on 6:off
```

e. As root, test the service starts correctly:

```
service advisors-aga start
```

Wait until startup is complete. Open the Advisors interface in your browser (<http://<host>:8080/admin/>) and log in; the page should be available.

f. As root, test that the service stops correctly:

```
service advisors-aga stop
```

Wait until shutdown is complete. Open the Advisors interface in your browser (<http://<host>:8080/admin/>) and log in; the page should be unavailable.

14. For every Stat Server (primary and backup) that you specified as part of the AGA server deployment, 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 the location you specified in which to install the Advisors 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
```

| Multiple instances on a server=

It is possible to deploy multiple instances of the Genesys Adapter core service on a single server. If you do use the same metrics database for more than one adapter, each adapter must monitor a completely distinct set of objects. For each installation, you should:

- Create the metrics database.
- Install and configure the AGA core service.

Deploy the second, and subsequent AGA instances, using the same procedure you use to deploy a single instance, and follow these rules:

- You must install each Genesys Adapter instance 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`.
- You must specify a unique log directory for each Genesys Adapter instance.
- You must specify a unique port number for each Genesys Adapter instance.

You must also edit the configuration file for each additional AGA core service deployment. See the following procedure.

1. Once the additional adapter has been installed, navigate to the conf folder for this installation.

2. Locate the file wrapper.conf and edit it as follows:

- a. Search for the # Name of service string.
- b. Edit the parameter below it (wrapper.ntservice.name=) so that the service name is different from the original instance. For example, enter 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.

3. Save and close the file.

4. Navigate to the bin folder for the second installation, and execute the Install-Adapter-NT.bat file. 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=

The following Table shows parameter validation errors that you may encounter at the end of installation.

Installation Error Message	Cause
<pre>[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."</pre>	Wrong database server name / IP address or port number
<pre>[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."</pre>	Wrong database name
<pre>[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;</pre>	Wrong database user name or password

Installation Error Message	Cause
password=very_secure_password	
[loadfile] Unable to load file: java.io.FileNotFoundException: C:\ (The system cannot find the path specified)	Produced in error and can be ignored.

Deploying Cisco Adapter

You run a .jar installation file to deploy Advisors Cisco Adapter (ACA).


You can deploy ACA on a Red Hat Linux or a Windows platform, and with Oracle or MS SQL databases.

All database passwords used by the Cisco Adapter application are encrypted and saved in the `..GCTI\Advisors\CiscoConnector\conf\ cisco_adapter.properties` file.

To change the password, see [Change Encrypted Passwords](#).

Roadmap

1. **[+] Install the databases that correspond to the Advisors products you will deploy.**
 - a. Advisors Genesys Adapter metrics database
 - b. Advisors Platform database
 - c. Advisors Cisco Adapter database (if you use ACA)
 - d. Metric Graphing database
2. Create the Advisors User and the Object Configuration User in Configuration Server. (Note that ACA itself does not require these users.)
3. **[+] Install the Platform service (Geronimo) on all servers on which you will deploy one of the Advisors components. (Note that ACA itself does not require Advisors Platform, but components that ACA serves require it.)**
 - Contact Center Advisor
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition

- Resource Management Console
- 4.  Install each adapter you will use (AGA and ACA). See additional information for CCAdv/WA installations.
- 5. **[+] Install the Advisors components for your enterprise.**
 - Contact Center Advisor
 - Workforce Advisor
 - Contact Center Advisor – Mobile Edition
 - Frontline Advisor (ACA works only with FA.)
 - SDS and Resource Management
- 6. Make any required configuration changes.

<tabber>

Procedure=

1. If you are deploying Advisors Cisco Adapter on a Linux system, you must first place the aca-installer-<version>.jar file into the Advisors home directory.

[+] Show Additional Information

- a. You can start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled:

```
ssh -X root@<host>
```

- b. As root, place the aca-installer-<version>.jar file into the Advisors home directory.

2. Launch the installation file.

[+] Show Step for Linux

- a. As root, navigate to the Advisors home directory:

```
cd /home/advisors
```

- b. As root, run the ACA installer. The page format of this document might cause a line break in the following command, but you must enter it on one line in the command prompt window:

```
./jdk1.7.0_<version>/bin/java -jar aca-installer-<version>.jar
```

[+] Show Step for Windows

Do one of the following:

- Open a command line window, and enter the following command:

```
java -jar aca-installer-<version>.jar
```
- Double-click the aca-installer-<version>.jar file in the release bundle.

Double-clicking might not work due to system settings, but using the command line terminal should always work. Genesys recommends using the command line window to launch the installer.

3. On the **Server Install Type** screen, the **Install the service** checkbox is selected by default. You can choose to start the service automatically by also selecting the **Start the service** checkbox. This is applicable to installations on Windows only.

4. On the **Installation details** screen, enter the installation directory for this deployment of Advisors Cisco Adapter. The default directory is C:\Program Files\GCTI\Advisors\CiscoAdapter, but you can specify a directory of your choice.

On this screen, you also specify the directory in which log files will go. The default log directory is C:\Program Files\GCTI\Advisors\CiscoAdapter\Log.

5. On the **Java Development Kit** screen, specify the root directory for your JDK installation by either entering it or by browsing to it with the **Select Folder** button.

6. On the **Cisco Database Configuration** screen, enter the information required for connecting to the databases.

In the Database server field, enter either the host name or IP address of the server. When using numerical IPv6 addresses, enclose the literal in brackets.

7. On the **Database Type** screen, select either the **SQL Server** or the **Oracle** option – whichever you use for databases in your installation. The screens that follow are dependent on your selection.

[+] Show Step for SQL Server

On the **Advisors Cisco Adapter Database Configuration** screen, specify the parameters for the database:

- Database server—The host name or IP address of the machine where the database is installed. When using numerical IPv6 addresses, enclose the literal in brackets.
- Database name—The unique name of the database instance; for example, ciscoadapter_db.
- Database port—The database server's port number.
- User name—The Advisors user that will be used by the Adapter to access the database.
- Database password—The password associated with the Advisors user that will be used by the Adapter to access the database.

[+] Show Steps for Oracle

- a. On the **Oracle JDBC Driver** screen, specify the location of the Oracle JDBC driver.
- b. On the **Oracle setup type** screen, select the Basic radio button.
- c. On the **Advisors Cisco Adapter Database Configuration** screen, specify the parameters for the ACA database:
 - Database server—The host name or IP address of the machine where the CCAAdv/WA metrics database is installed. When using numerical IP v6 addresses, enclose the literal in brackets.
 - Database SID—The unique name of the database instance; for example, orcl.
 - Database port—The database server's port number.
 - Database schema—The Advisors user that will be used by the Adapter to access the database.
 - Database schema password—The password associated with the Advisors user that will be used by the Adapter to access the database.

[+] Show Steps for Oracle RAC

- a. On the **Oracle JDBC Driver** screen, specify the location of the Oracle JDBC driver. You can use only the Oracle database 11g release 2 (11.2.0.2.0) driver. The download file is ojdbc6.jar.
- b. On the **Oracle setup type** screen, select the RAC connectivity setup option.
- c. On the **Advisors Cisco Adapter Database Configuration - RAC** screen, specify the parameters for the ACA database:
 - Database schema—The Advisors user that will be used by the Adapter to access the database.
 - Database schema password—The password associated with the Advisors user that will be used by the Adapter to access the database.
 - Locate file—Enter the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. The installation wizard applies the specified advanced connection string when configuring the data sources.

8. On the **Adapter Port and Registration Option** screen, specify the ACA port number, and indicate if you want to register the ACA in the platform database or not.

You can use the default port, 7000, if no other application is using that port.
If you leave the Skip Registration checkbox empty (unselected), you must enter additional information about the adapter and about your Advisors platform database.

[+] Show Steps

- a. Enter the following information about the adapter on the **Register Adapter** screen:
 - Name
 - Host Address
 - Description (for example, Advisors Cisco Adapter)
 - Source Environment (for example, Cisco)

b. Enter the following information about your Advisors platform database:

- For MS SQL or basic Oracle (single instance) databases – On the **Platform Database Configuration** screen, enter the Server, Name, Port, User Name, and Password for the platform database with which the adapter is to be registered.
- For Oracle RAC databases – On the **Platform Database Configuration - RAC** screen, enter the Database schema and corresponding password. In the Locate file field, enter the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. The installation wizard applies the specified advanced connection string when configuring the data sources.

9. On the **Installation Progress** screen, click Show Details, and then Install.

10. Verify that there are no errors during installation.

11. 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 (applicable to installations on Windows only).

If you use a Linux platform, manually configure ACA to run automatically as a system service:

[+] Show steps

a. As root, create an /etc/init.d/advisors-aca file with the following contents; remember to replace <version> with the version number of your file and <Advisors directory> with your directory's name:

```
#!/bin/bash
# description: Advisors Cisco Adapter Start Stop Restart
# processname: advisors
# chkconfig: 235 20 80
#

export PATH=/home/advisors/jdk1.7.0_<version>/bin:$PATH

ACA_BIN=/home/advisors/<Cisco Adapter directory>/bin

cd $ACA_BIN

case $1 in
start)
/bin/su advisors ./startup.sh
;;
stop)
./shutdown.sh
;;
restart)
./shutdown.sh
/bin/su advisors ./startup.sh
;;
esac
exit 0
```

b. As root, make the startup script executable:

```
chmod 755 /etc/init.d/advisors
```

- c. As root, configure the system to start the Advisors process at boot time:

```
chkconfig --add advisors
chkconfig --level 235 advisors on
```

- d. As root, check that the configuration is correct:

```
chkconfig --list advisors
```

The output should be similar to the following:

```
advisors 0:off 1:off 2:on 3:on 4:off 5:on 6:off
```

- e. As root, test the service starts correctly:

```
service advisors-aca start
```

Wait until startup is complete. Open the Advisors interface in your browser (<http://<host>:8080/admin/>) and log in; the page should be available.

- f. As root, test that the service stops correctly:

```
service advisors-aca stop
```

Wait until shutdown is complete. Open the Advisors interface in your browser (<http://<host>:8080/admin/>) and log in; the page should be unavailable.

| Deploying multiple instances of ACA on a single server=

It is possible to deploy multiple instances of Advisors Cisco Adapter on a single server. Multiple Cisco Adapters can be installed to provide metrics from separate HDS/AWDB source environments.

For each installation, you will:

- Create the database.
- Install and configure the ACA core service. On the the Server Install Type screen, the Install the service checkbox is preselected; ensure the Start the Service check box is unchecked.

Deploy the second, and subsequent ACA instances, using the same procedure you use to deploy a single instance, and follow these rules:

- You must install each Cisco Adapter instance in a different directory. For example, the first instance could use the following location:
C:\Program Files\GCTI\Advisors\CiscoAdapter
and the second instance could be located at:
C:\Program Files\GCTI\Advisors\CiscoAdapter2.
- You must specify a unique log directory and a unique data directory for each Cisco Adapter instance.
- You must specify a unique port number for each Cisco Adapter instance.

Ignore the following error if it occurs during installation of additional ACA instances. The missing service will be installed in **Step 1**.

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

You must also edit the configuration file for each additional ACA core service deployment. After the adapter is installed, navigate to the \conf folder and follow the procedure below.

1. Locate and edit the wrapper.conf file:

- a. Search for the # Name of service string.
- b. 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.
- c. 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. It is not necessary for it to match the name above.
- d. Save and close the file.

2. Navigate to the /bin folder of the second installation, and execute the Install-Adapter-NT.bat file to install the renamed service. You can then locate and start the service in the Services Control Panel applet.

[-] Troubleshooting=

The following Table shows parameter validation errors that you may encounter at the end of installation.

Installation Error Message	Cause
<pre>[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.</pre>	Wrong database server name / IP address or port number
<pre>[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</pre>	Wrong database name

Installation Error Message	Cause
port."	
<pre>[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</pre>	Wrong database user name or password
<pre>[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)</pre>	Wrong path to JDK or wrong version of the JDK specified.
<pre>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)</pre>	<p>Produced in error and can be ignored.</p> <p>Displays in the Errors tab when installing Cisco Adapter with Oracle JDBC driver of jsc6-11.2.0.2.0, and accurately reports that installation was successful.</p>
Exception in thread "AWT-	Produced in error and can be ignored.

Installation Error Message	Cause
<pre>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)</pre>	
<pre>[loadfile] Unable to load file: java.io.FileNotFoundException: C:\ (The system cannot find the path specified)</pre>	Produced in error and can be ignored.

Deploying CCAdv and WA

If you are installing any or all of the following Advisors modules, use the procedures and information in this section:

- Contact Center Advisor (CCAdv)
- Contact Center Advisor-Mobile Edition (CCAdv-ME)
- Workforce Advisor (WA)
- Alert Management (AM) Administration

You can deploy these modules on a Red Hat Linux or a Windows platform, and with Oracle or MS SQL databases.

If you use a Genesys computer-telephony integration (CTI) installation, you must install Advisors Genesys Adapter with CCAdv and WA applications. For Cisco installations, no adapter is required.




If you are upgrading your version of CCAdv-ME, ensure you read [Upgrade CCAdv-ME](#).

For information about deploying smartphone client applications, see [Deploy Smartphone Client Applications](#).

Roadmap

1. **[+] Install the databases that correspond to the Advisors products you will deploy.**
 - a. Advisors Genesys Adapter metrics database
 - b. Advisors Platform database
 - c. Advisors Cisco Adapter database (if you use ACA)
 - d. Metric Graphing database
2. Create the Advisors User and the Object Configuration User in Configuration Server.
3. **[+] Install the Platform service (Geronimo) on all servers on which you will deploy one of the**

Advisors components.

- Contact Center Advisor
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA). See additional information for CCAdv/WA installations.
 5. Install the Advisors components for your enterprise:
 -  Contact Center Advisor
 -  Workforce Advisor
 -  Contact Center Advisor – Mobile Edition
 - Frontline Advisor
 - SDS and Resource Management
 6. Make any required configuration changes.

You run a single .jar installation file to deploy any or all of the modules. Use the procedure below to start your installation. The installer guides you through the deployment. The screens displayed during your deployment are dependent on the selections you make on the **Modules to Install** screen. Information about each screen is available on the Installation Screens tab below.

<tabber>

Procedure=

1. Copy the installation file to the Advisors home directory.

[+] Show additional information for Linux environments

- a. Ensure the Advisors Platform service has been installed. The Advisors Platform service hosts the CCAdv and WA applications.
- b. Open the shell.
- c. Start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11

forwarding enabled:

```
ssh -X root@<host>
```

- d. As root, copy the ccadv-wa-installer-<version>.jar file to the /home/advisors directory.

```
cp ./ccadv-wa-installer-<version>.jar /home/advisors
```

2. Launch the installation file.

[+] Show Steps for Linux

- a. As root, navigate to the Advisors home directory:

```
cd /home/advisors
```

- b. As root, run the CCAdv/WA installer. The page format of this document might cause a line break in the following command, but you must enter it on one line in the command prompt window:

```
./jdk1.7.0_<version>/bin/java -jar ccadv-wa-installer-<version>.jar
```

[+] Show Step for Windows

Do one of the following:

- Open a command line window, and enter the following command:

```
java -jar ccadv-wa-installer-<version>.jar
```
- Double-click the ccadv-wa-installer-<version>.jar file in the release bundle.

Double-clicking might not work due to system settings, but using the command line terminal should always work.

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.

3. On the **Modules to Install** screen, select which Advisors application(s) you will install. You can install an individual application or as many applications as you require during a single run of the installation file.

Each of the modules 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 Advisors Platform, are installed only once.

[+] Show Information about Selections

The modules are:

- Contact Center Advisor XML Generator application—Install this module only once in one cluster of Advisor systems.
- Contact Center Advisor Web services, including the dashboard—You can install more than one instance in one deployment of Advisors. You can install it on the same system on which you installed the XML Generator, or on a different system.
- Contact Center Advisor Mobile Edition—Contact Center Advisor application for mobile devices.
- Workforce Advisor server—Install this module only once in one cluster of Advisor systems.

- Workforce Advisor Web service, including the dashboard—You can install more than one instance in one deployment of Advisors. You can install it on the same system on which you installed the Workforce Advisor server, or on a different system.
- Alert Management administration— Install this module on the same system on which you installed the Administration Workbench when installing Platform.

4. On the **Destination Directory** screen, specify the destination directory in which the files will be installed (the Advisors base directory).

For all module 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. The default directory is Program Files\GCTI\Advisors.

5. Use the information provided on the **Installation Screens** tab on this page to assist you to complete the remaining deployment screens.

|–| Installation Screens=

[+] CCAdv-ME Server Configuration

- Allow client password caching—Determines whether the server will tell its clients to cache the password on the client. If this checkbox is not selected, the user is redirected to the login page every time he or she launches an application.
- Logo link URL (image link)—Enter the URL to which users are redirected when they click on your enterprise's logo on the login screen. This is optional configuration; it is not required.
- URL that Logo links to—You can enter an image URL of the company's logo that will be visible on the login page. This hyperlinked image is used to personalize the login page. This is optional configuration; it is not required.
- Interval for file purge (ms)—This value (in milliseconds) specifies the frequency at which to delete the charting local cache from the server.
- Delay for retries on failed response—This value (in milliseconds) specifies the delay between retries when a failure occurs.
- Number of retries—Number of times each resource retries to build the response when a failure occurs in the Advisors server.
- Device refresh interval (ms)—This value (in milliseconds) represents the refresh time of the client views when auto-refresh is enabled.

[+] CCAdv-ME Trend Charting Configuration

Enter the time periods for trend charting on the CCAdv-ME Trend Charting Configuration screen. The values are in minutes. Period two should be bigger than period one and smaller than period three. Period three should be smaller than the retention period set by the CCAdv server.

Genesys recommends that you enter numerical characters only in these fields, such as 30, 60, or 120.

[+] Data Source

For each data source not already in the database, specify the following:

- the database name or linked server name
- the source type (Genesys or Cisco)
- (optional) the display name
- the threshold update delay. This is how long CCAdv will wait for new data from this data source before notifying users via the CCAdv dashboard, and, if configured to do so, administrators via e-mail.
- the Relational Database Management System (RDBMS) type

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 using the installer.

[+] Database Type

Specify the type of database you use in your enterprise.

[+] Genesys Advisor Platform Database

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).

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

If the database server is a named instance, then omit the port number.

[+] Genesys Advisor Platform Database - RAC

- Database user and Database user password—The database schema and password created and used for the Platform database.
- Locate file—Enter the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. The installation wizard applies the specified advanced connection string when configuring the data sources.

[+] Java Development Kit

Enter or select the folder location for the Java Development Kit.

[+] Metric Graphing Database

Specify the connection parameters for the Metric Graphing database.

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

[+] Metric Graphing Database - RAC

- Database user and Database user password—The database schema and password created and used for the Metric Graphing database.
- Locate file—Enter the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. The installation wizard applies the specified advanced connection string when configuring the data sources.

[+] Oracle setup type

Specify whether you use Oracle basic (single instance) or Oracle Real Application Cluster (RAC) databases.

[+] Workforce Advisor Server - IEX TotalView

Enter the FTP Server port number on which the FTP connection in WA listens for data from TotalView.

[+] Workforce Aspect eWFM

Enter the Aspect eWFM base retrieval URL.

The base retrieval URL should be `file:///` followed by the location of the eWFM files.

If the component must read or write data kept on a drive accessible over the network, then enter the path name 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.

For example:

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

[+] Workforce Genesys WFM

- Base URL—The base URL should contain the server name or IP address of the machine where the WFM server is installed, as well as the port on which the server is configured and listening. For example, `http://192.168.98.215:5007`. When using numerical IP v6 addresses, enclose the literal in brackets.
- Application name—The application name of the WFM server as configured in the Configuration Server or Genesys Administrator.
- User ID—Enter either a specific user ID to indicate the identity of the requests, or enter 0 (zero) to indicate no user. The user ID is used as a reference in the connection string to Genesys WFM.
- Polling interval (ms)—The interval at which the Genesys WFM service is polled for forecast data.

- Number of hours to harvest—The number of hours of forecast metrics to get during each polling interval.

[+] Workforce Advisor Server - Page 1

Select your sources for workforce management data.

[+] Workforce Advisor Server - Page 2

Enter the e-mail address that will appear in the From: header of e-mail that WA sends about alerts, to users that are members of distribution lists configured in the Administration Workbench. For example, DONOTREPLY@genesys.com.

<toggledisplay showtext="[+] XML Generator - Page 1" hidetext="[-] XML Generator - Page 1">
Enter the interval for the Medium and Long groups of time profiles. For example, if you enter 120 seconds for this parameter, XML Generator stores metrics and threshold violations for these time profiles no more often than that. However, XML Generator might store the view data less frequently depending on load and the complexity of the configuration.

[+] XML Generator - Page 2

Enter the maximum number of retry attempts in the event of a database connection failure. This parameter is applicable to retry attempts when XML Generator is already running; that is, after establishing connections at startup.

Enter the number of seconds between Contact Center Advisor XML Generator's reconnection attempts in the event of a database connection failure. This parameter is applicable to retry attempts when XML Generator is already running; that is, after establishing connections at startup.

[+] XML Generator - Page 3

Alert E-mail From Address: Enter the e-mail address that will appear in the From: header of e-mail that XML Generator sends about alerts, to users that are members of distribution lists configured in the Administration Workbench. For example, DONOTREPLY@genesys.com.

Enter the e-mail address that will appear in the From: header of e-mail that WA sends about alerts. For example, DONOTREPLY@genesys.com.

Support E-mail Address: Enter the e-mail address to which XML Generator will send e-mail about events other than alerts. For example, an e-mail sent when XML Generator has not been able to connect to an external data source within the configured number of minutes. The address entered in this field also appears in the From: header of these types of e-mails.

SMTP Server: 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 see the ERROR messages in the log file for XML Generator.

[+] XML Generator - Page 4

Specify how frequently (in seconds) snapshots should be stored in the metric graphing database. For example, if you enter 60 seconds, XML Generator stores 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.

Specify whether graphs should display values from the previous day. If you select 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.

See [Configure Metric Graphing Properties](#) for detailed information.

[+] XML Generator and Workforce Advisor

Previously called Dashboards. Select the time profile for the historical agent group metrics that CCAAdv and WA will display.

If you choose 5 minute sliding, then CCAAdv and WA will display agent group metrics from the most recent 5 minutes. If you choose 30 minute growing, then they will display agent group metrics from the current half hour.

For metrics imported from CISCO ICM, Advisors always imports agent group metrics with the 5 minute sliding profile. If you are running Advisors with CISCO ICM, and you choose the 30 minute growing option here, then on the dashboards, historical agent group metrics will display as a dash. Genesys recommends that you use the five minute growing setting if you have a CISCO source of data.

[-] Start the XML Gen Service on Linux Platform=

If you use a Linux platform, configure XML Generator to run automatically as a system service:

1. As root, create an /etc/init.d/advisors-xmlgen file with the following contents; remember to replace <version> with the version number of your file and <Advisors directory> with your directory's name:

```
#!/bin/bash
# description: Advisors Cisco Adapter Start Stop Restart
# processname: advisors
# chkconfig: 235 20 80
#
# This script should be edited and installed in /etc/init.d directory
#
# Before using please edit PATH and XMLGEN_HOME.
#

export PATH=/home/advisors/jdk1.7.0_<version>/bin:$PATH

XMLGEN_HOME=/home/advisors/<path to xmlgen directory>

cd $XMLGEN_HOME

case $1 in
start)
/bin/su advisors ./startup.sh
;;
stop)
```

```
./shutdown.sh
;;
restart)
./shutdown.sh
/bin/su advisors ./startup.sh
;;
esac
exit 0
```

2. As root, make the startup script executable:

```
chmod 755 /etc/init.d/advisors
```

3. As root, configure the system to start the Advisors process at boot time:

```
chkconfig --add advisors
chkconfig --level 235 advisors on
```

4. As root, check that the configuration is correct:

```
chkconfig --list advisors
```

The output should be similar to the following:

```
advisors 0:off 1:off 2:on 3:on 4:off 5:on 6:off
```

-| Troubleshooting=

The following Table shows parameter validation errors that you may encounter at the end of installation.

Installation Error Message	Cause
<pre>[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.</pre>	Wrong database server name / IP address or port number
<pre>[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</pre>	Wrong database name

Installation Error Message	Cause
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."	
[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
[loadfile] Unable to load file: java.io.FileNotFoundException: C:\ (The system cannot find the path specified)	Produced in error and can be ignored.

Work with XML Generator

Use the information on the tabs below to help you work with Contact Center Advisor XML Generator, including how to correctly start and stop XML Generator, and how to modify the XML Generator configuration.

<tabber>

Deploy XMLGen as a Service=

1. Run the Windows service as a user who has these permissions:

- Log In as a Service permission. Services are installed to be run under the Windows local system account. This account is restricted from network I/O by Windows design.
- Permission to write to the directory on the network.

2. Do one of the following:

- Navigate to the installation folder in Windows Explorer, then execute the following file:
[CCA Home]\XMLGen\InstallXMLGen.bat.
- Open a command prompt window, and do the following:
 - a. Change the directory to point to the XML Generator installation.
 - b. Run the following command:
installXmlgen

| - | Remove XMLGen as a Service=

1. Do one of the following:

- Navigate to the installation folder in Windows Explorer, then execute the following file:
[CCA Home]\XMLGen\UnInstallXMLGen.bat
- Open a command prompt window, and do the following:
 - a. Change the directory to point to the XML Generator installation.
 - b. Run the following command:
uninstallXmlgen

| - | Stopping and Starting XMLGen and CCAdv Web Service=

The relationships between applications and agent groups support certain functionality in the dashboards. First, they support highlighting agent groups when applications are selected, and vice versa. Second, they support displaying the set of agent groups related to both a contact center and an application group. The XML Generator updates these relationships when it starts, and after that once per day, overnight. For the configuration to take effect immediately, stop and restart XMLGen.

As part of enhancements to the security of XML passed from XML Generator to CCAdv, XML

Generator and the CCAdv web service share a cache. No XML is written to disk storage.

This dependency between the two components means that stopping and starting them needs to be done as described in the procedure below to avoid problems.

It is important to start Geronimo before you start the XML Generator. If you start the XML Generator before starting a Geronimo instance that is hosting the CCAdv web service, you experience the following problem:

Geronimo will start. The cache will not contain the XML for the above relationships, since the XML Generator could not send it when it was produced. You will see errors in the `geronimo.log` about XML files for relationships not being available for dashboards. Functionality in the dashboard that depends on this XML will not work.

The following procedure ensures that all XML produced by the XML Generator is stored for Contact Center Advisor's dashboards.

1. Start all the Geronimo servers that host the CCAdv web service. (Other instances of Geronimo do not matter.)
2. Start XML Generator.
3. If you restart Geronimo on one of those systems, also re-start the XML Generator.

|–| Edit XMLGen Configuration=

Use the procedures on this page to modify XML Generator configuration:

- [Modifying the XML Generator Configuration](#)
- [Modifying XML Generator Email Notifications about Logged Errors](#)
- [Changing the XML Generator Connection](#)

Modifying the XML Generator Configuration

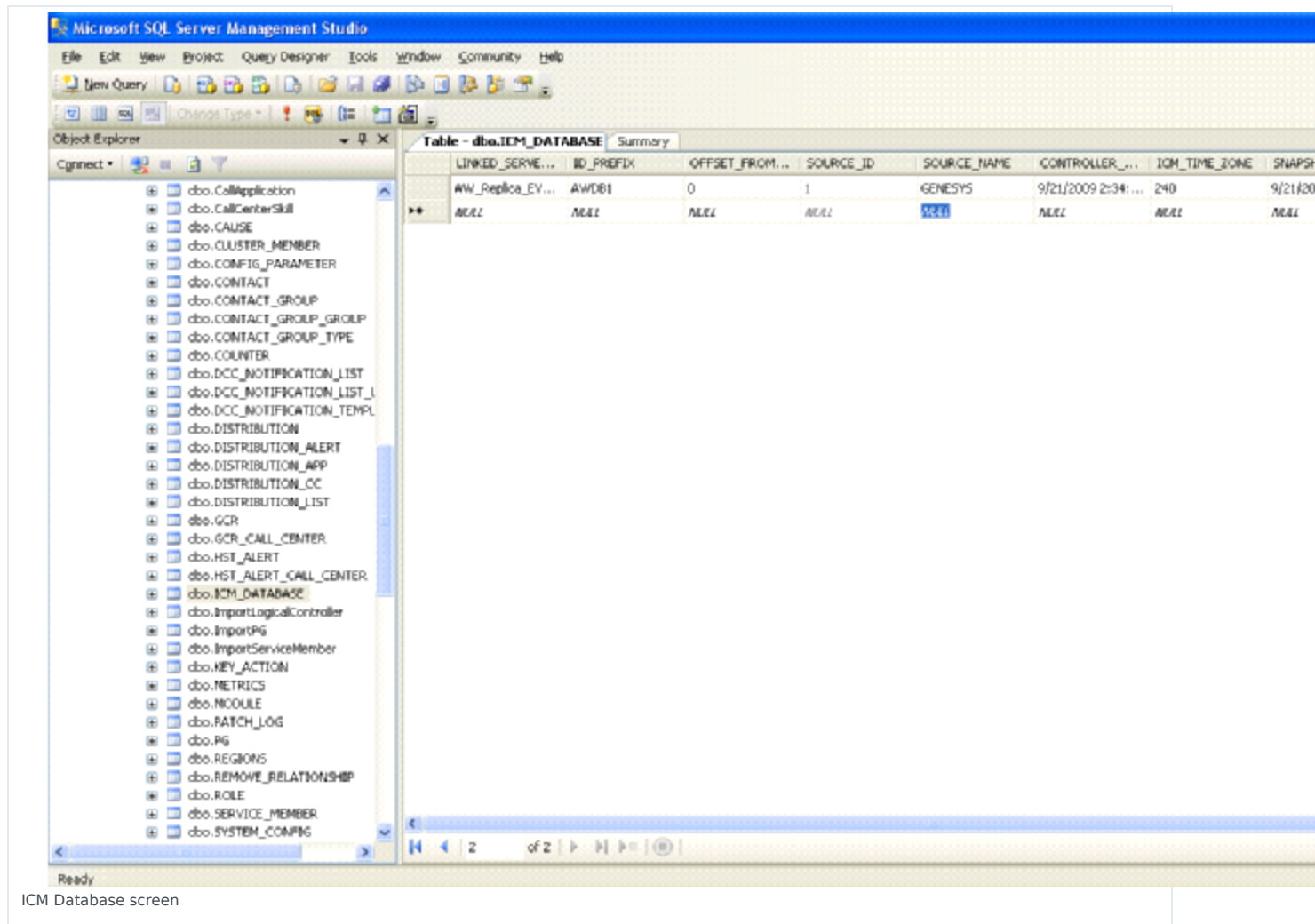
1. After installation of XMLGen, there should be a row in the Platform database in the ICM_DATABASE table corresponding to the CCAdv/WA metrics database. If not, add this row. This row is necessary to ensure that XMLGen works properly with the metrics database.

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>')
```

The (<metrics_db_1>, <metrics_db_2>... , <metrics_db_n>) string is a list of metrics database destinations for the Genesys Adapter.

The ICM database should then look like the following Figure.



Modifying XML Generator Email Notifications about Logged Errors

The XML Generator log files are in the `xmlgen\log` directory. For every ERROR-level message written to its log, XML Generator sends an email to the address entered at installation. You can change certain properties of this log, or turn this logging off.

XML Generator uses log4j to send the email messages. The configuration for email is in the `xmlgen\log4j.xml` file. Look for the appender named MAIL. The instructions about how to turn off the logging, or change the properties defined there, are in the file. The properties you can change are:

- mail server host name
- subject line of messages
- email addresses to send to
- email address for “from” address
- log4j format (conversion pattern) of the content of the ERROR message

After changing any of the preceding properties, you must restart the XML Generator for the changes to take effect.

Changing the XML Generator Connection

You can change the database connection data for XML Generator after installation. The XML Generator file is:
`conf/XMLGen.properties`

To change the password, see [Change Encrypted Passwords](#).

Upgrade CCAdv-ME

Use the following procedure if you are upgrading your installation of CCAdv-ME. The procedure ensures you properly prepare your system to accept a new version of the application.

Procedure

1. Uninstall the Mobile Edition application:
 - a. Under Advisors root directory, remove the ccadv-me folder.
 - b. Under the <Advisors_root_dir>/geronimo-tomcat6-minimal-2.2.1/repository/com/genesyslab/advisors/ folder, remove the ccadv-me-web folder.
 - c. Open the <Advisors_root_dir>/geronimo-tomcat6-minimal-2.2.1/var/config/config.xml file, and remove the following line:
`<module name="com.genesyslab.advisors/ccadv-me-web/[version]/war" />`
 - d. Save the changes and close the file.
2. Deploy the new version.

Deploy Smartphone Client Applications

The following procedures describe how to install the client applications for Blackberry, Android, and Apple devices:

- [Deploy Blackberry Clients](#)
- [Deploy Android Clients](#)
- [Deploy Apple Clients](#)

Deploy Blackberry Clients

The Blackberry app is also distributed through the Blackberry App Store or BlackBerry App World.

1. Copy the blackberry directory from the software CD to the apache/htdocs folder.
2. From the device, point to the URL of the web server and, in the ota folder inside the appropriate device type, click on the .jad file.
For Blackberry devices that have a physical keyboard (with or without a touch screen), use the Classic device type. For Blackberry devices that do not have a physical keyboard use the Touch device type.
3. Confirm to download and follow the prompts.

Deploy Android Clients

The Android Client application is distributed through Google Play services. To locate the app, search for the following keyword string (including the quotation marks) "contact center advisor mobile".

For download instructions, see the following Google Play Help topic: [Download Android applications](#).

Deploy Apple Clients

The iOS Client application is distributed through the Apple App Store. To locate the app, search for the following keyword string (including the quotation marks) "contact center advisor mobile".

Use the standard Apple App Store download procedures to obtain the app.


Deploying FA

You run a `.jar` installation file to deploy Genesys Frontline Advisor.

You can deploy FA on a Red Hat Linux or a Windows platform, and with Oracle or MS SQL databases.

Roadmap

1. **[+] Install the databases that correspond to the Advisors products you will deploy.**
 - a. Advisors Genesys Adapter metrics database
 - b. Advisors Platform database
 - c. Advisors Cisco Adapter database (if you use ACA)
 - d. Metric Graphing database
2. Create the Advisors User and the Object Configuration User in Configuration Server.
3. **[+] Install the Platform service (Geronimo) on all servers on which you will deploy one of the Advisors components.**
 - Contact Center Advisor
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. Install the Advisors components for your enterprise in the following order:
 - Contact Center Advisor
 - Workforce Advisor

- Contact Center Advisor – Mobile Edition
 -  Frontline Advisor
 - SDS and Resource Management
6. Make any required configuration changes.

<tabber>

Procedure=

1. Copy the installation file to the Advisors home directory.

[+] Show additional information for Linux environments

- a. Ensure the Advisors Platform service has been installed. The Advisors Platform service hosts the FA application.
- b. Open the shell.
- c. Start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled:

```
ssh -X root@<host>
```

- d. As root, copy the fa-server-installer-<version>.jar file to the /home/advisors directory.

```
cp ./fa-server-installer-<version>.jar /home/advisors
```

2. Launch the installation file.

[+] Show Steps for Linux

- a. As root, navigate to the Advisors home directory:

```
cd /home/advisors
```

- b. As root, run the FA installer. The page format of this document might cause a line break in the following command, but you must enter it on one line in the command prompt window:

```
./jdk1.7.0_<version>/bin/java -jar fa-server-installer-<version>.jar
```

[+] Show Step for Windows

Do one of the following:

- Open a command line window, and enter the following command:
`java -jar fa-server-installer-<version>.jar`
- Double-click the `fa-server-installer-<version>.jar` file in the release bundle.

Double-clicking might not work due to system settings, but using the command line terminal should always work.

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.

3. On the **Destination Directory** screen, accept the default directory, or specify a different directory. The installation directory for Frontline Advisor server must be the same as the directory where Advisors Platform has been installed.

4. Configure FA to run as a single instance, or in distributed mode.

[+] Show Steps for single instance installation

- a. If you are installing a single instance of Frontline Advisor, select the `Run as a single instance` option. This is the default setting.
- b. On the **Hierarchy Source Details** screen, enter either:
 - The name of the tenant in the Genesys Configuration Server in which the monitoring hierarchy resides, and the path to the hierarchy root folder.
In a Cisco environment, the path should look like:
`Agent Groups\\<Your Cisco Group Name>`
 - The name of a Person folder in Configuration Manager, and the path to that Person folder.
Selecting this option restricts the hierarchy view that is loaded at startup (or reloaded using the reload feature) to the team of agents belonging to that person (supervisor).
- c. To add more than one tenant or person, check the **Add Another?** check box, and complete the required details.

[+] Show Steps for distributed mode installation

- a. If you are installing multiple FA instances for use in distributed mode, and this instance is one of those, select the `Run as a cluster member` option.
- b. On the **Distributed Mode - Rollup Engine** screen, select one of the two options:
 - **Enable Rollup Engine**—Enable the rollup engine if you intend the FA instance you are installing to be responsible for data aggregation. When installing Advisors Platform to support the FA instance on which the rollup engine will be enabled, you must install the Administration workbench.

Warning

Enable the rollup engine for only one of the FA instances in a cluster.

- **Disable rollup engine**—Disable the rollup engine if you intend the FA instance you are installing to be responsible for presentation only. When installing Advisors Platform to support the FA

instance on which the rollup engine will be disabled, do not install the Administration workbench.

5. On the **Database Type** screen, select either the SQL Server or the Oracle option – whichever you use for Advisors platform database(s). The screens that follow are dependent on your selection:

[+] Show Step for SQL Server

On the **Genesys Advisor Platform Database** screen, specify the parameters for the Advisors platform database:

- Database server—The host name or IP address of the database server. When using numerical IP v6 addresses, enclose the literal in brackets.
- Database port number—The database server's port number.
- Database name—The unique name of the database instance.
- Database user—The Advisors user with full access to the Advisors platform database.
- Database user password—The password created and used for the Advisors platform database.

[+] Show Steps for Oracle

- a. On the **Oracle setup type** screen, select the Basic option.
- b. On the **Genesys Advisor Platform Database** screen, specify the parameters for the Advisors platform database:
 - Database server—The host name or IP address of the database server. When using numerical IP v6 addresses, enclose the literal in brackets.
 - Database port number—The database server's port number.
 - SID—The unique name of the database instance.
 - Database user—The Advisors user with full access to the Advisors platform database.
 - Database user password—The password created and used for the Advisors platform database.

[+] Show Steps for Oracle RAC

- a. On the **Oracle setup type** screen, select the RAC connectivity setup option.
- b. On the **Genesys Advisor Platform Database** screen, specify the parameters for the Advisors platform database:
 - Database schema and Database schema password—The database schema and password created and used for the Platform database.
 - Locate file—Enter the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. The installation wizard applies the specified advanced connection string when configuring the data sources.

6. On the **Failure Notification Configuration** screen, specify the e-mail settings for system-level notifications:

- Application from address—The default *sender* of the notification message; for example, faadmin@genesys.com
- Application to address—The default *recipient* of the notification message; for example, faadmin@genesys.com
- Subject—The default subject line for notification messages; for example, Frontline Advisor Message

7. After you deploy FA, you must modify the Apache configuration file (httpd.conf). See [Deploy and Configure Apache](#).

| Start the FA Service=

To start the Frontline Advisor service from the command prompt, you must set the MaxPermSize parameter to 256 in the setenv.bat file. The FA log generates errors or exceptions if you start the service with the default setting of 128.

1. Follow the Advisors 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.

| Troubleshooting=

The following Table shows parameter validation errors that you may encounter at the end of installation.

Installation Error Message	Cause
<pre>[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.</pre>	Wrong database server name / IP address or port number
<pre>[java] Failed to connect to the database using connection URL: [java] jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=Q0001;user=sa; selectMethod=cursor;user=sa;password=very_secure_pwd [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException:</pre>	Wrong database name


Installation Error Message	Cause
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."	
[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
[loadfile] Unable to load file: java.io.FileNotFoundException: C:\ (The system cannot find the path specified)	Produced in error and can be ignored.

Deploying SDS and RMC

Use the information on this page to deploy the Resource Management Console and the Supervisor Desktop Service (required for RMC).

Roadmap

1. **[+] Install the databases that correspond to the Advisors products you will deploy.**
 - a. Advisors Genesys Adapter metrics database
 - b. Advisors Platform database
 - c. Advisors Cisco Adapter database (if you use ACA)
 - d. Metric Graphing database
2. Create the Advisors User and the Object Configuration User in Configuration Server.
3. **[+] Install the Platform service (Geronimo) on all servers on which you will deploy one of the Advisors components.**
 - Contact Center Advisor
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. Install the Advisors components for your enterprise:
 - Contact Center Advisor
 - Workforce Advisor

- Contact Center Advisor – Mobile Edition
 - Frontline Advisor
 -  SDS and Resource Management
6. Make any required configuration changes.

<tabber>

Supervisor Desktop Service=

Important

- Supervisor Desktop Service (SDS) requires a 32-bit Java installation (JVM). SDS will run on a 64-bit operating system, including both Windows 2008 and Windows 2003 Server, but attempting to run the SDS startup executable against 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.
- Performance Management Advisors support Oracle JDK 1.7, but SDS does not. If you deploy SDS with Advisors Release 8.1.401 or later, and you have Java 7 installed, you must also install a version of JDK 1.6.0 for SDS.
- Install SDS and the Resource Management Console (RMC) only after you have installed all other Advisors components that you use in your enterprise. Genesys recommends that you verify the dashboards are working for all installed components (CCAdv, WA, FA), and that the hierarchy in each dashboard rolls up correctly before you install SDS and RMC. After you have verified Advisors is working correctly, install JDK 1.6 (if it is not already installed as your primary JDK version), and then install SDS and RMC.

1. If an older version of SDS is already installed, you must uninstall it.

[+] Show More

- 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 configure the SDS application.

[+] Show Steps

- a. Open the Hosts folder under the Environment tenant. Create a host object for the machine on which you will deploy the SDS, if one does not already exist.
Genesys recommends that the IP address configured in this host object be the actual IP address of the server, not a loopback address.
- b. Open the Application Templates folder. Import the application template called `Genesys_Supervisor_Desktop_Service_763.adp`. This template is located with the SDS installation files.
- c. Open the Applications folder. Right-click in the pane on the right and select `New > Application`.
- d. Select the `Genesys_Supervisor_Desktop_Service_763.adp` application template and a new window should open showing the application.
 - i. On the General tab, set the name of the application to `Genesys Supervisor Desktop`.
 - ii. (Multi-tenant environments only) On the Tenants tab, add the non-Environment tenant that SDS will monitor.
 - iii. 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.
 - iv. On the Start Info tab, enter a single period (.) for the working directory, command line, and command line arguments.
 - v. 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`).
 - Specify the following options under the supervisor section:
 - `set calculated-statistics-enable` to `true`
 - `set stat-on-request` to `true`
 - `set stat-threads` to `-1`
 - `set stat-peeking` to `false`
 - `set show-env-tenant` to `false` for multi-tenant configurations, or to `true` for single-tenant configurations

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.

- vi. On the Connections tab, add connections to the T-Servers, Interaction Servers, and the Stat Server to which the SDS will connect.
SDS can be connected to one primary/backup Stat Server pair.
- vii. Save the application.
- e. Open the SDS application properties again.
- f. Open 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.
- g. Go to the Options tab and double-click the Supervisor option. Add the properties for your e-mail messaging system; see the following Table for additional information.

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	The 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 are on or off.
email-use-SSL		Does the e-mail server use SSL? Valid values are on or off.
password		The password for the e-mail server. Ignored if email-authenticate is set to off.

- h. Verify that the T-Server(s), Interaction Server(s), and Stat Server(s) are configured with a correct host (that is, they do not use localhost).
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 localhost host, the SDS tries 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.
- i. If not already done, create a new person in your SDS-monitored tenant. (For single-tenant installations, create the person in the Environment tenant.) Leave the password fields blank and ensure that the IsAgent checkbox is selected. The person object should have the following attributes:
 - First Name: Spv
 - Last Name: Spv_Last
 - Employee ID: Spv
 - User Name: Spv
- j. Open 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

k. Save the user.

l. Open the user properties again. Open 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.

m. Add permissions as follows:

- For single tenant installations, add Spv to the Administrators group for the Environment tenant:
 - Under AccessGroups, select Administrators, then right-click.
 - Select New > Shortcut to Person. Locate and add Spv.
- To enable agent maintenance for multiple tenant installations, you must give the Spv user the same subset of permissions that are given to tenant Administrators. You must also give the Spv user Change permission to Person objects (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, add the Spv user to the existing tenant's Administrators Access Group, and grant the group Change permission to Person objects.

5. In the folder containing the Supervisor Desktop Service installation package, run setup.exe. The Genesys Installation Wizard for SDS displays and guides you through the rest of the installation.

[+] Show Steps

- a. On the **Connection Parameters to the Configuration Server** screen, enter information in all fields.
- b. On the **Select Application** screen, select the application that you created using Configuration Manager (at Step 4 in this procedure).
- c. On the **Choose Destination** screen, specify the directory in which to install SDS. Clicking the Default button enters C:\GCTI\GenesysSupervisorDesktopService\Genesys_Supervisor_Desktop. Click the Browse button to navigate to a directory of your choice.

Important

The Supervisor Desktop Service (SDS) installation path must contain no spaces. For example, C:\Advisors\SDS\ADV_Supervisor_Desk_Serv is a valid installation path, but C:\Advisors\SDS\ADV Supervisor Desk Serv is not.

- d. To configure a connection to a backup Configuration Server, enter the connection parameters on the **Connection Parameters to the Backup Configuration Server** screen. This is optional; you can leave this screen empty.
- e. On the **Configuration Parameters** screen, enter the Tomcat port information.



6. In the Configuration Manager, edit the options for your Stat Server application:

- a. Import the `StatServerEntries.cfg` file (found in the Advisors Genesys Adapter installation directory) into the Stat Server application options. When prompted to overwrite the existing options, choose NO.
- b. If prompted to overwrite/update any statistics options, do this. The file does not alter any default Stat Server metrics, only ones specific to Advisors. Changing any logging options is optional.
- c. Restart the Stat Server.

7. 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*`.

8. Restart any Stat Server to which you added the `StatServerEntries.cfg` file.

9. On the server containing your SDS service, navigate to the `bin` directory, and edit the `GDesktopStarter.ini` batch file. Find the line starting with `echo JavaArgs:`

- Change the value of `-Xms` to 512.
- Change the value of `-Xmx` to 1024.
- Append the following to the end of the line – the following options improve performance of the SDS:
`-XX:+UseConcMarkSweepGC`
- If SDS is being installed in a multiprocessor environment, add the following to the end of the line:
`-XX:+UseParNewGC`

10. Open the Windows services control panel, and start the new Genesys Supervisor Desktop Service.

| Resource Management Console=

1. Launch the AGA installation file.

[+] Show Steps for Linux

- a. As root, navigate to the Advisors home directory:

```
cd /home/advisors
```

- b. As root, run the AGA installer. The page format of this document might cause a line break in the following command, but you must enter it on one line in the command prompt window:

```
./jdk1.7.0_<version>/bin/java -jar aga-installer-<version>.jar
```

[+] Show Steps for Windows

Do one of the following:

- Open a command line window, and enter the following command:

```
java -jar aga-installer-<version>.jar
```

- Double-click the aga-installer-<version>.jar file in the release bundle.

Double-clicking might not work due to system settings, but using the command line terminal should always work. Genesys recommends using the command line window to launch the installer.

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. On the **Install Type** screen, select the Deploy Resource Management Console radio button. You can install only a single component (either the core service or RMC) during a single installer run.

3. On the **Database Type** screen, select either the SQL Server or the Oracle option – whichever you use for Advisors platform database(s). The screens that follow are dependent on your selection:

[+] Show Step for SQL Server

- Select the base location of the Advisors installation (that is, the base directory where the Platform components and Geronimo are installed). In most cases, this is C:\Program Files\GCTI\Advisors.
- On the **Genesys Advisor Platform Database** screen, specify the parameters for the Advisors platform database:
 - Database server—The host name or IP address of the database server. When using numerical IPv6 addresses, enclose the literal in brackets.
 - Database port number—The database server's port number.
 - Database name—The unique name of the database instance.
 - Database user—The username to be used by the Adapter to access the database.
 - Database user password—The password associated with the database user.

[+] Show Steps for Oracle

- On the **Oracle setup type** screen, select the Basic option.
- Select the base location of the Advisors installation (that is, the base directory where the Platform components and Geronimo are installed). In most cases, this is C:\Program Files\GCTI\Advisors.
- On the **Genesys Advisor Platform Database** screen, specify the parameters for the Advisors platform database:
 - Database server—The host name or IP address of the database server. When using numerical IPv6 addresses, enclose the literal in brackets.
 - Database port number—The database server's port number.
 - Database name—The unique name of the database instance.
 - Database user—The username to be used by the Adapter to access the database.
 - Database user password—The password associated with the database user.

[+] Show Steps for Oracle RAC

- a. On the **Oracle setup type** screen, select the RAC connectivity setup option.
- b. Select the base location of the Advisors installation (that is, the base directory where the Platform components and Geronimo are installed). In most cases, this is C:\Program Files\GCTI\Advisors.
- c. On the **Genesys Advisor Platform Database** screen, specify the parameters for the Advisors platform database:
 - Database user and Database password—The username and corresponding password to be used by the Adapter to access the database.
 - Locate file—Enter the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. The installation wizard applies the specified advanced connection string when configuring the data sources.

4. After installation is complete, click Show Details, and then click Install and verify that there were no errors reported during installation.

5. After RMC has installed successfully, you must edit the RMCInfo.xml configuration file to provide the information required to make Resource Management function and available to Contact Center Advisor. The file is found in the following directory:

```
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 CCAAdv/WA-prefixed properties refer to the CCAAdv/WA installation host.

Use the following values:

- SDS_IP – The IP address for the SDS Service host.
- SDS_Port – The port number for the SDS path (default 8080).
- If you are using the Spv user with blank password in the SDS configuration, do not change SDS_DeployPath, SDS_UserName, or SDS_Password. If the user for SDS is not the Spv user with blank password, you must enter that user and password (the SDS_UserName and SDS_Password parameters) in the RMCInfo.xml file. The password must be encrypted. To encrypt the password, use the password encryption utility (see [Change Encrypted Passwords](#)).
- CCAWA_IP – The IP address for the CCAAdv/WA server host. When using numerical IPv6 addresses, enclose the literal in brackets.
- CCAWA_Port – The port number for the CCAAdv/WA server (default 8080).

6. To access the Resource Management Notification administration pages through the Advisors interface (Advisors Administration module), you must add the following entry 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).

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

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.

Warning

Use semi-silent and silent modes with caution. Use the `ant.install.properties` files with identical types of installations. For example, the `ant.install.properties` file you used to install Platform with an Oracle database should not be used to install Platform with an MS SQL Server database.

Advisor Component Names

Use the component names from the Table, as applicable, for the `<advisor-component>` variable in the instructions on the following tabs.

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

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.

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.`

<tabber>

Perform 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.

When the `ant.install.properties` file is re-used for a semi-silent installation, and a path to a folder needs to be changed using the **Select Folder** button, verify the selected path and adjust it manually, if necessary.

|= Perform 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:

1. Open a command prompt window.
2. Navigate to the directory containing the installer .jar file.
3. Run the following command (using the correct version number for <version>):
`java -jar <advisor-module>-installer-<version>.jar swing-auto`

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

The installer will create the logging directory only 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 runs, using the values in the `ant.install.properties` file. When it exits, it indicates 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 you have run the installer, the following additional files are present and contain 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, incorrect database passwords, or any other error that would cause a failure during normal installation mode).

Genesys strongly recommends that you examine all generated logs to ensure that all errors and warnings are duly noted.

Post Installation Configuration

You perform initial Performance Management Advisors configuration during the deployment phase. At a later date, after installation is complete, you might require re-configuration of some components. Use the topics in the Post Installation Configuration section to assist you to find relevant configuration files and so on.

General

This section contains information and procedures to help you change configuration for Performance Management Advisors after the Advisors modules are deployed.

High Availability for Performance Management Advisors

Performance Management Advisors support High Availability starting in release 8.5.0. High Availability in release 8.5.0 means you have redundant servers available for each of the nodes in the Platform database's `Cluster_Member` table for which you require backup, and also for any data adapters (Advisors Genesys Adapter or Advisors Cisco Adapter) configured in the system. When an Advisors component or its host server fails, you switch over to the backup system.

You can install the backup system before the primary goes down, or after the primary fails. In either case, after the backup system is installed, you need only make small manual adjustments in the Platform database to replace the primary server with the backup server, and back again.

<tabber>

Install Redundant Servers=

1. Review the list of nodes in the Advisors Platform database `Cluster_Member` table, and then identify a backup server machine for each node for which you require a backup.
2. On each backup machine, install the same Advisors components that are installed on the primary machine. Use the installer properties files (`ant.install.properties`) from the original system.
3. For pre-installing the backups, ensure that the `Cluster_Node` page attributes are exactly the same on the backup as they were for the primary; that is, do not change the node name or host values. Using the identical configuration ensures the backup system installation does not overwrite the primary. You can change the following, if necessary, on the backup machine, but it is very important that you do not change any other installer options:
 - the installation path
 - the Java path
 - the folder from which the Oracle JDBC driver is provided to the installer
 - the log folder, depending on your file folder structure
4. Follow [Step 3](#) for data adapters (Advisors Genesys Adapter or Advisors Cisco Adapter). Again, do not change the host values or names of the adapters on their registration pages.
5. Run the primary system.
6. If a primary system fails and you must switch over to the backup, follow the relevant procedure on the other tabs of this page.

|= Switchover on a Cluster Node Server=

If the primary server, or the platform service on a primary server goes down, use the following procedure to switch over to the redundant system. This procedure assumes the redundant server is installed. See the procedure on the *Install Redundant Servers* tab if you have not already installed the backup system.

1. Stop the system service on all other Advisors nodes in the deployment. The data adapters can continue to run, but you will have to restart them later.

2. Update the row in the Platform database `Cluster_Member` table that identifies the failed node; set the `IP_Address` column to the IP or hostname of the backup server for that node. If you use an Oracle database, commit the changes.
3. Update any affected addresses for ProxyPass entries in the Apache configuration file (`httpd.conf`) so that they point to the backup server. See information on the *HA and Apache Server* tab.
4. Restart the system service on all data adapters.
5. Start the main Advisors Platform node first (the node on which you installed the administration workbench), regardless of whether it is a primary or a backup node.
6. Follow the Advisors startup sequence to bring the full deployment back up, starting the other nodes on their respective servers in the correct order, and depending on which components you have installed:
 - a. Main (administration) Platform
 - b. Apache service
 - c. AGA for FA, if present
 - d. AGA for CCAdv, if present
 - e. CCAdv Web services, if not on the administration node
 - f. FA Platform
 - g. WA server, if present
 - h. XML Generator Platform, if it is different from the administration Platform
 - i. WA Web service, if not on the WA Platform
 - j. SDS, if present
 - k. XML Generator service
7. Users that were logged into the Advisors interface must log out, or close their browsers, and then log in again.

|–| Switchover on an Adapter=

If a data adapter (Advisors Genesys Adapter or Advisors Cisco Adapter) or its host server fails, use the following procedure to switch over to the redundant adapter/server.

To switch over from a backup adapter to the primary adapter again, you use the same procedure, but there is no need to update the `inf_genesys_adapter.properties` file on the primary server. That server's properties file was not changed during the switch over to the backup adapter; it therefore contains the correct information.

1. Stop the system service for all other adapters and all Advisors nodes in the deployment (you must restart nodes that depend on the adapters, and therefore all other nodes, as well).
2. In the Platform database `Adapter_Instances` table, identify the record that corresponds to the adapter that needs to be switched over. Update the `Host` property of this record to that of the redundant system's host name or IP address. Commit the change, if necessary.
3. On the redundant adapter server, open the `inf_genesys_adapter.properties` file (in the Advisors installation `/conf` folder). Update the following line to point to the redundant server's host name or IP address; if you used an IP address in **Step 2**, you must use the IP address here (the same is true of the host name – you must use the same type of entry in both locations):


```
informiam.genesys_connector.host.name =
```

4. Repeat the preceding Steps (2 and 3) for each adapter instance that you want to switch over to its backup system.

5. Start the redundant adapters, and then restart all other adapters.

6. Restart the system service for each node in the correct Advisors startup sequence:

- a. Main (administration) Platform
- b. Apache service
- c. AGA for FA, if present
- d. AGA for CCAdv, if present
- e. CCAdv Web services, if not on the administration node
- f. FA Platform
- g. WA server, if present
- h. XML Generator Platform, if it is different from the administration Platform
 - i. WA Web service, if not on the WA Platform
 - j. SDS, if present
- k. XML Generator service

6. Users that were logged into the Advisors interface must log out, or close their browsers, and then log in again.

| - | HA and Apache Server=

If you move any Advisors node to a backup server, you must update the ProxyPass section of the Apache server configuration file (`httpd.conf`). It is important that you find every instance of the IP address or host name of the system that is being replaced, and change those instances to the IP address or host name of the system that you have configured as the backup.

After you complete and save updates to the Apache Server configuration file, stop and then restart the Apache service.

| - | HA and RMC=

The Supervisor Desktop Service (SDS) server that supports the Resource Management Console (RMC) has no inherent High Availability (HA) capability. Loss of the SDS server requires recovery of the service or machine, or a redundant SDS installation with the same configuration as the existing SDS installation (that is, it must point to the same Configuration Server, Stat Server(s), and TServer(s)), and with the same permission structure.

If you transfer from one SDS server to another, you must update the `RMCInfo.xml` file in the RMC installation to point to the new SDS instance. Instructions are available in the [Deploying SDS and RMC section](#) of the Performance Management Advisors Deployment Guide.

If your Advisors deployment uses RMC, Genesys strongly advises you to install the CCAdv Web services component into the Advisors Platform instance where the administration workbench is installed because RMC uses objects in both the workbench and in the Web services. RMC cannot

connect to both sets of objects if the workbench and Web services are on different servers.

If you install RMC with both the administration workbench and CCAdv Web Services, RMC is supported for HA along with the entire node.

Change Memory Allocation

Change Memory Allocation for Advisors Platform and Advisors Genesys Adapter

You should consider changing the memory allocation for Advisors Platform server and Advisors Genesys Adapter (AGA) if:

- the `geronimo.log` for the Advisors Suite server is reporting an out of memory error; set the heap size higher by editing the `<install_dir>/conf/advisors-server-wrapper.conf` file.
- the AGA log is reporting an out of memory error; set the heap size higher by editing the `<install_dir>/conf/wrapper.conf` file.

About a third down the file, change the following lines—the following memory settings are examples only and are not intended to be recommendations (actual settings would be based on hardware sizing for your environment):

```
# 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 Advisors Platform or AGA uses a 64-bit JVM. The most memory you can allocate to `wrapper.java.maxmemory` under 32-bit Windows is 1600 MB, 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).

Changing Memory Allocation in Other Environments

If you are not running Advisors in a Windows environment, or prefer to run Advisors from the command line instead of as a service, then you should make any necessary memory allocation changes by editing the `setenv.sh` or `setenv.bat` file appropriate for your platform as described below.

- Edit the `setenv.sh` file contained in your Geronimo `bin` directory for Linux-based environments, or the `setenv.bat` file for Windows-based environments if not running Advisors as a service.
- Change the Java JVM memory-related arguments as described above. For example:

```
export GERONIMO_OPTS="-ms800m -mx1200m -XX:MaxPermSize=256m ...
```

sets the initial heap size to 800MB, the maximum heap size to 1200MB, and the maximum PermGen space to 256MB.

Important

When you specify memory allocation in the `setenv.sh` file, you should comment out the following block in `<Advisors>/geronimo-tomcat6-minimal-2.2.1/bin/geronimo.sh`:

```
if [ -z "$JAVA_OPTS" ]; then
    JAVA_OPTS="-Xmx256m -XX:MaxPermSize=128m"
fi
```

- For more information on these arguments, or other JVM options, see <http://docs.oracle.com/javase/7/docs/technotes/tools/windows/java.html> for Windows environments or <http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/java.html> for Linux environments.

Change Memory Allocation for CCAdv XML Generator

You can configure memory allocation for XML Generator in the following file: `<XMLGen>/startup.sh`

Change Encrypted Passwords

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

1. Open the command prompt window 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 resulting encrypted password and replace the old password in the configuration file.

Customize the Advisors Interface

Use the following procedure to add your company's logo to the Advisors interface, or to change the color scheme.

1. **NEW** To customize the logo on the Advisors login page, navigate to the following folder in the deployment directory:

C:\<installation directory>\baseweb\images

2. **NEW** Replace the existing logo file (genesys-logo.png) with your custom logo.

The custom logo filename must be genesys-logo.png and the file should have the same dimensions as the genesys-logo.png file (112 x 26 pixels).

3. **NEW** To customize colors in the Advisors modules, update the stylesheet for each installed module. You can find stylesheets in the following folder:

C:\<installation directory>\baseweb\landing\stylesheets

4. **NEW** To modify colors on the login page, update the following stylesheet:

C:\<installation directory>\baseweb\modules\login\login.css

5. **NEW** To add a custom message on the Login page, edit the remote-message text file in the following directory:

C:\<installation directory>\baseweb

You must retain the remote-message file name.

Correct Login Page Latency

If the Apache log files on the Web server show the following, consider raising the `ThreadsPerChild` setting to 1024:

- [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

Deploy and Configure Apache

Use the information on this page to install an Apache Web Server instance to direct http requests to the appropriate server. It is recommended to install Apache Web Server on a separate box.

You do not require a second Apache instance on the XML Generator server (local files are not produced). You can install a single Apache instance on a standalone server that points to the Advisors IP addresses and ports.

In a Frontline Advisor distributed mode configuration, the Apache HTTP configuration can be configured on any FA instance.

You can configure Apache to support HTTPS; to do so, you must:

- Generate the SSL security certificate and private key.
- Reconfigure Apache.

Both procedures are described on the *Configure Apache to Support HTTPS* tab below.

<tabber>

Deploy and Configure Apache for Advisors=

1. To enable Apache Web Server serving different modules in the Advisors interface (for example, Administration, Contact Center Advisor, Workforce Advisor), edit the `httpd.conf` file as described below. The `httpd.conf` file is located in the `conf` folder of the Apache Web Server installation.

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 lines shown below (see [Platform and Advisors Modules](#) below) to the bottom of the file and change the IP addresses or host names, as necessary. The format of this page might cause lines to wrap, but it is very important that each entry is on a single line in your httpd.conf file. You can comment out or exclude lines to proxy passes that are not installed.

The trailing slash must appear at the end of each line, as indicated below. If it is omitted, users might see a 404 or Not Found error, get no response when clicking, or see empty white screens in the Advisors interface. Errors can typically be seen in the Geronimo log if DEBUG is enabled. For example, ProxyPass /gc-admin/ ajp://server:8009/gc-admin will generate an error. Should this happen, the solution is to fix the httpd.conf and restart Apache.

If you need to access external applications through the Advisors interface, you should have lines for each of those applications.

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

```
# Platform and Advisors Modules
ProxyPass /am/ ajp://192.168.40.234:8009/am/
ProxyPass /admin/ ajp://192.168.40.234:8009/admin/
```

Important

Remove, or comment out, the ProxyPass /admin/ ajp://192.168.40.234:8009/admin/ statement on FA presentation-only instances. If you use a load balancer, do not direct requests to the /admin/ context to FA presentation-only instances.

```
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 /base-ws/ ajp://192.168.40.234:8009/base-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/
ProxyPass /ca-xml/ ajp://192.168.40.234:8009/ca-xml/

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

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

# Contact Center Advisor Mobile Edition
```

```
ProxyPass /ma/ ajp://HOSTNAME:8009/ma/
```

Important

If there is no Administration workbench module installed on the FA Platform server, add the following re-directs before `ProxyPass /fa/ ajp://192.168.40.234:8009/fa/` – this allows you to access the FA Administration module from the CCAAdv/WA Platform server:

- `ProxyPass /fa/Admin ajp://192.168.40.234:8009/fa/Admin`
Note that there is no slash at the end of the preceding statement; while this is different from most other ProxyPass statements, it is correct syntax for the fa/Admin statement.
- `ProxyPass /fa/com.informiam.fa.admin.gwt.AdminConsole/ ajp://192.168.40.234:8009/fa/com.informiam.fa.admin.gwt.AdminConsole/`

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.

[-] Configure Apache to Support HTTPS=

Generating the SSL security certificate and private key

1. If not already installed, download and install the C++ redistributables from the official Microsoft downloads site.
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 and choose `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`

Reconfiguring Apache to support HTTPS

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`.

-
- a. Uncomment `LoadModule ssl_module modules/mod_ssl.so` (line 120).
 - b. Uncomment `Include conf/extra/httpd-ssl.conf` (line 474).
 - c. Comment out `Listen 80` (line 46).
3. Edit `{Apache conf}\extra\httpd-ssl.conf` and point `SSLCertificateFile` and `SSLCertificateKeyFile` to the certificate.
 4. Restart Apache.
 5. 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.

Change a JDBC Data Source Configuration



There are two modules that contain JDBC data source configuration information:

- com.informiam.platform/platform-datasource-service/<version>/rar
- com.informiam.ea/metric-graphing-datasource/<version>/rar

There is no FA data source starting in release 8.5.0; earlier releases of Advisors included an FA data source.

You must re-deploy each instance of the preceding modules for which you modify the `geronimo-ra.xml` descriptor (see the following procedures).

Before you perform either of the procedures below, read the following carefully:

- Perform the following procedure offline; Geronimo must be fully stopped.
- Ensure that Advisors NT service is not running.
- After you stop Geronimo, Genesys recommends that you take a complete directory backup of <GCTI>/Advisors/ before you do any manual operations.

<tabber>

Advisors Platform=

1. Copy `geronimo-ra.xml` from

```
**/GCTI/Advisors/geronimo-tomcat6-minimal-2.2.1/repository/com/ informiam/platform/platform-datasource-  
service/<version>/platform- datasource-service-<version>.rar/rar/META-INF  
to  
**/GCTI/Advisors/platform-datasource.
```

2. Edit the descriptor (`geronimo-ra.xml` that you copied to `**/GCTI/Advisors/platform-datasource`), as required.

3. Ensure the Advisors service is stopped before proceeding.

4. Open a command prompt window.

5. Navigate to the `**/GCTI/Advisors/geronimo-tomcat6-minimal-2.2.1/bin` directory.

6. Run the following command:

```
java -jar deployer.jar --offline --user system --password manager redeploy ../../platform-datasource/platform-  
datasource.rar ../../platform-datasource/geronimo-ra.xml
```

Note: In the preceding command line, `../../platform-datasource/geronimo-ra.xml` is the path to the recently-edited descriptor.

7. Start the Advisors service and verify that the reconfigured data source works.

8. If the database parameters require further updates, edit the data source descriptor file and run the command again to re-deploy it.

For example:

Edit ../../platform-datasource/geronimo-ra.xml and run the command again.

| Metric Graphing Datasource=

1. Copy geronimo-ra.xml from

```
**/GCTI/Advisors/geronimo-tomcat6-minimal-2.2.1/repository/com/Informiam/ea/metric-graphing-  
datasource/<version>/ metric-graphing-datasource-<version>.rar /rar/META-INF  
to  
**/GCTI/Advisors/metric-graphing-datasource.
```

2. Edit the descriptor (geronimo-ra.xml that you copied to **/GCTI/Advisors/metric-graphing-datasource), as required.

3. Ensure the Advisors service is stopped before proceeding.

4. Open a command prompt window.

5. Navigate to the **/GCTI/Advisors/geronimo-tomcat6-minimal-2.2.1/bin directory.

6. Run the following command:

```
java -jar deployer.jar --offline --user system --password manager redeploy ../../metric-graphing-datasource/  
metric-graphing-datasource.rar ../../metric-graphing-datasource/geronimo-ra.xml
```

Note: In the preceding command line, ../../metric-graphing-datasource/geronimo-ra.xml is the path to the recently-edited descriptor.

7. Start the Advisors service and verify that the reconfigured data source works.

8. If the database parameters require further updates, edit the data source descriptor file and run the command again to re-deploy it.

For example: Edit ../../metric-graphing-datasource/geronimo-ra.xml and run the command again.

Schedule Periodic Statistics Reissue

Starting in release 8.1.5, the Periodic Statistics Reissue Scheduling screen is no longer included in the Genesys Adapter installer.

For Contact Center Advisor and Workforce Advisor, use the Platform installation conf\AdvisorsGenesysAdapter.properties file to configure the schedule for the overnight reissue of statistics.

The property to configure in the file is:
`periodicResetJob.cronExpression=0 0 2 * * ?`

The default value is 2 AM refresh for CCAdv/WA.

Frontline Advisor automatically loads the hierarchy from the Genesys Configuration Server at startup and daily at 02:55 a.m., by default.

The reload frequency can be adjusted using the following setting in the Platform installation conf\FrontlineAdvisor.properties file:
#Cron expression that specifies how often FA should reload its hierarchy
`hierarchy.reload.cronExpression=0 55 2 * * ?`

The default setting is 2:55 a.m.

 See documentation in the Quartz library to help you with configuration:
<http://www.quartz-scheduler.org/documentation/quartz-1.x/tutorials/crontrigger>

Adjust 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 their log files. These components will roll each of their current log files to backup copies both at the beginning of each day, and after the size of the log file reaches a threshold. You can do this for:

- Platform log of authorizations, which records users logging in to and out of Advisors
- Administration module log, which records many actions carried out in the module
- Contact Center Advisor (CCAdv) Web services
- CCAdv XML Generator
- Workforce Advisor (WA) server and Web services
- Frontline Advisor (FA)
- Advisors Genesys Adapter (AGA)

Starting in release 8.5.001, the default setting for rollover of the log files is daily or when the log file size exceeds 10 MB.

See also [Configuring the Audit Logs](#) for more information.

Configuring Rollover of the Log File

Starting in release 8.5.001, you can configure the `log4j.xml` and the `log4j.properties` files to use a rolling filename in this format: `<Component><Date><Time>.log`. `<Date>` and `<Time>` are configurable parameters. The appropriate component name is automatically added to the log filename.

The following are the rolling attributes for a log file:

- `datePattern`—Specifies the schedule on which the log file rolls over (closes the log file, renames it to a rolling file, and starts a new file). You can set the schedule so the log file rolls over by year, month, day, half day, hour, and minute. See [DatePattern Conventions](#) for more information.
- `maxFileSize`—Sets the size threshold past which the log file rolls over. Specify an integer value, along with either KB, MB, or GB (for example, 10MB for ten megabytes). `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.
- `suffixPattern`—Specifies the suffix for the log's filename when the log file rolls over. The parameter supports Java's `SimpleDateFormat` conventions, such as `' 'yyyy-MM-dd_HH-mm-ss' ' .log'`. The literal text must be escaped within a pair of single quotes.

- **MaxRollFileCount**—Sets the number of backup log files to keep.
- **ScavengeInterval**—An interval in milliseconds. On this schedule, log4j checks to see if it should delete backed-up log files because there are more than **MaxRollFileCount** files. If you set **ScavengeInterval** to -1, **MaxRollFileCount** will be ignored, and all backup copies will be retained. You will need to manually clear the backup copies from the log directory on a periodic basis.

See [Modules Running in the Geronimo Application Server](#), [Contact Center Advisor XML Generator](#), [Frontline Advisor](#), and [Advisors Genesys Adapter](#) for procedures to configure log filenames and additional log file attributes.

DatePattern Conventions

You can specify the schedule on which the log file rolls over to a new file using the **DatePattern** parameter. The parameter uses Java's **SimpleDateFormat** conventions. The Table below shows the possible entries to specify for the **DatePattern** parameter.

DatePattern	Rollover Schedule
yyyy-MM	Rollover at the beginning of each month.
yyyy-ww	Rollover on the first day of each week. The first day of the week depends on the locale.
yyyy-MM-dd	Rollover at midnight each day.
yyyy-MM-dd-a	Rollover at midnight and midday of each day.
yyyy-MM-dd-HH	Rollover at the top of every hour.
yyyy-MM-dd-HH-mm	Rollover at the beginning of every minute.

For example, if you set the **File** option to `/xxx/yyy.log`, you set the **DatePattern** to `yyyy-MM-dd`, and you set the **SuffixPattern** to `'.'yyyy-MM-dd`, the logging file `/xxx/yyy.log` is copied to `/xxx/yyy.log.2014-02-16` on 2014-02-16 at midnight and logging for 2014-02-17 continues in the `/xxx/yyy.log` file until it rolls over the next day, and so on.

Modules Running in the Geronimo Application Server

You can adjust the size threshold, as well as the number of backup copies retained, by editing the properties in the logging properties file. Use the following procedure.

1. Navigate to your base Advisors directory, and then to the `geronimo-tomcat6-minimal-2.2.1\var\log` subdirectory.
2. Edit the `server-log4j.properties` file.
3. Look for the rolling properties and, for each log file, adjust them appropriately.

Contact Center Advisor XML Generator

CCAdv XML Generator uses a logging properties file that is different from the one used by the modules running in the Geronimo application server. Use the following procedure to make changes to the logging properties file for CCAdv XML Generator.

1. Navigate to your base Advisors directory, and then to the xmlgen subdirectory.
2. Edit the log4j.xml file.
3. Look for the rolling properties and, for each log file, adjust them appropriately.

Frontline Advisor

FA uses a logging properties file that is different from the one used by the modules running in the Geronimo application server. Use the following procedure to make changes to the logging properties file for FA.

1. Navigate to your base Advisors directory, and then to the conf subdirectory.
2. Edit the FrontlineAdvisor-log4j.properties file.
3. Look for the rolling properties and, for each log file, adjust them appropriately.

Advisors Genesys Adapter

Use the following procedure to make changes to the logging properties file for AGA.

1. Navigate to your base AGA directory, and then to the conf subdirectory.
2. Edit the log4j.properties file.
3. Look for the rolling properties and, for each log file, adjust them appropriately.

Advisors Platform

This section contains information and procedures to help you change configuration for Advisors Platform after this module is deployed.

Change Advisors Cluster Membership

For the definition and overview of an Advisors modules cluster, see [Advisors Cluster Information](#).

Information about nodes is stored in the `CLUSTER_MEMBER` table of the Platform database. Each node in the cluster is represented by one row in that table.

When you install Advisors Platform on a system that is a cluster member, the installer creates an entry for that node in the table. Each node entry in the `CLUSTER_MEMBER` table has the following properties:

- `NAME`
- `IP_ADDRESS`
- `LOCALHOST_ADDRESS`

The Platform installer adds the values you enter in the `Cluster Node` configuration screen to that node entry in the Platform database table. Valid values for the properties are specified in [Deploying Advisors Platform](#).

The names on the `Cluster Node` configuration screen, and the properties in the `CLUSTER_MEMBER` table, correspond as follows:

- Node ID = `NAME`
- IP address/hostname = `IP_ADDRESS`
- Localhost address = `LOCALHOST_ADDRESS`

In addition to the `CLUSTER_MEMBER` table, the installer saves some properties in files in the `Advisors/conf` directory.

- The node ID is in `Node.properties`.
- The port number used by the cluster members to communicate is in `ActiveMQ.properties`.

To change information about the cluster after installing Advisors, you can modify the `CLUSTER_MEMBER` table in the Platform database. You may also need to update some properties in the above files. Make sure that the values you enter meet the specifications in the procedure about installing Platform (see [Deploying Advisors Platform](#)).

To change any of the below, first shut down Advisors components on all node in the cluster.

- To change the Node ID, update the value in the `CLUSTER_MEMBER` table and in `conf/Node.properties`.
- To change the IP address or localhost address, update the `CLUSTER_MEMBER` table.
- To change the port number on which nodes of the cluster communicate, change the value in `ActiveMQ.properties`.

Configure Administrative Actions Logs

All administration actions carried out in the Advisors environment are logged. The following sections give information about how the logging should be configured.

Modules for which Actions are Logged

The following modules have administrative logging available:

- Advisors Administration for Contact Center Advisor and Workforce Advisor
- Advisors Genesys Adapter

Metrics logs are replaced with Metric Manager audit logs (generated when a user creates a new metric, attempts but fails to create a new metric, or deletes a metric).

Modules for which Actions are Not Logged

- Configuration Server, for actions on objects used by Contact Center Advisor and Workforce Advisor.
- Frontline Advisor Administration
- Resource Management Administration
- Alert Management
- Action Management

Actions Not Logged by This Functionality

Changes to contact groups that are made when contact groups are imported from a WFM system are not captured by this logging functionality.

Information Logged

The following information about each action is logged:

- A timestamp of when the action's data was saved in the format specified by the log configuration properties. (See *Configuring the Audit Logs* below.)

- The username of the user who performed the action.
- The properties or relationships of the object that are being changed by the action, showing their values both before and after the action.
- Whether the action succeeded or not.

Configuring the Audit Logs

The audit logs are separate files written in the directory that contains the Geronimo logs. This directory is:

```
...\Advisors\geronimo-tomcat6-minimal-2.2.1\var\log\
```

The audit log is configured by log4j properties in Geronimo's server-log4j.properties file, which is located in this directory:

```
...\Advisors\geronimo-tomcat6-minimal-2.2.1\var\log
```

Sample log4j Appender

The following information is the definition of the appender that configures the audit logs.

```
log4j.appender.ADMINISTRATIONAUDIT.append=true
log4j.appender.ADMINISTRATIONAUDIT.file=${org.apache.geronimo.server.dir}/var/log/
AdministrationAudit.log
log4j.appender.ADMINISTRATIONAUDIT.bufferedIO=false
log4j.appender.ADMINISTRATIONAUDIT.maxBackupIndex=3
log4j.appender.ADMINISTRATIONAUDIT.maxFileSize=10MB
log4j.appender.ADMINISTRATIONAUDIT=org.apache.log4j.RollingFileAppender
log4j.appender.ADMINISTRATIONAUDIT.threshold=INFO
log4j.appender.ADMINISTRATIONAUDIT.layout=org.apache.log4j.PatternLayout
log4j.appender.ADMINISTRATIONAUDIT.layout.ConversionPattern=%d %m%n
```

The appender ensures the log file names indicate the day on which they were written. If more than one file is written per day, then the name also indicates the order in which the file was produced on that day. For example:

```
AdministrationAudit.log
AdministrationAudit.log.2011-12-01.1
AdministrationAudit.log.2011-12-01.2
AdministrationAudit.log.2011-11-31.1
AdministrationAudit.log.2011-11-31.2
```

Definitions

- `MaxFileSize` of 10 MB—Indicates that the largest size of any individual log file is 10 MB.
- `MaxBackupIndex` of 3—Indicates that on any day, a maximum of three files will be written. If more than that are actually produced, the oldest ones will be deleted.

Change the Mail Server Configuration

1. In the conf directory, locate the MailService.properties.
2. Edit the settings.
3. For the new settings to take effect, you must restart the server.
4. If you have installed Contact Center Advisor XML Generator, then also change the configuration of the SMTP appender in the logging properties file for XML Generator. See [Work with XML Generator](#).

Advisors Genesys Adapter

This section contains information and procedures to help you change configuration for Advisors Genesys Adapter after this module is deployed.

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, and requests the historical statistics from both the Stat Servers of the pair at the same time.

For the purposes of Advisors Genesys Adapter, Primary and Backup are determined by the specified Adapter installation options. Primary and Backup, in this case, is not related to the Primary and Backup Stat Server designation in Configuration Manager.

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.

Stat Server Load Balancing

The relationship between a statistic and the Stat Server pair against which it is requested is maintained. This means that on (re)start or refresh of the adapter, statistics are now re-requested against the same Stat Server(s) as previously. AGA no longer depends on the value set for the Stat Server `old-stats-remove-interval` option.

If any additional Stat Servers are added after the initial starting of the Adapter, the statistics already requested with previous Stat Servers are not automatically re-distributed with the newly added Stat Server pair. You have two options if a redistribution is needed. Use **Option 2** to maintain existing mapping with some of the Stat Servers.

Option 1

1. Run the following SQL statement to truncate the ADAPTER_SS_OBJ_MAPPING platform database table:

```
DELETE FROM ADAPTER_SS_OBJ_MAPPING WHERE SS_PAIR_ID = <Id of the stat server pair>
where the ID is the ID of the stat server pair from the ADAPTER_SS_CONFIG table.
```

2. Restart the Stat Servers (this flushes any previous requests).
3. Restart the adapter and Platform server.

Option 2

Run the following SQL statements to selectively update the ADAPTER_SS_OBJ_MAPPING table to point a range of objects to a new Stat Server installation:

```
SELECT SS_PAIR_ID FROM ADAPTER_SS_CONFIG WHERE NAME = [Name of the new pair's primary Stat Server]
```

```
UPDATE ADAPTER_SS_OBJ_MAPPING SET SS_PAIR_ID = ["ID" from above] WHERE OBJECTID IN (
) AND OBJECTTYPE = ?
```

Add Stat Servers after Installation

To add Stat Server capacity after the deployment of Advisors Genesys Adapter, use the following procedure. You require access to the Platform configuration database.

1. Insert additional rows into the `adapter_ss_config` table that describe the additional Stat Servers. Name, Host, and Port are required. One row includes the primary Stat Server and its backup, if applicable.
2. After committing the changes to the database, restart the Platform server and Genesys Adapter.

Re-distribute Stats Load when Adapters are Added

Initially, in your deployment, you might have one or more Advisors Genesys Adapters (AGA) running and the total statistics load is being evenly distributed among the adapters.

If, in this deployment, you must add one or more adapters, the existing statistics will not be automatically re-routed to the newly added adapters because Data Manager uses persisted adapter Stat Server object mappings.

Use the following procedure to re-distribute the total load of statistics among the adapters, including the adapters you added after the initial deployment.

1. Stop all server components (Platform server, all Genesys adapters). **Jeeva: Also XMLGen for CCAdv Genesys Adapters**

2. Connect to the platform database and remove all the entries from the Adapter_ss_obj_mapping table and commit the following transaction:

```
delete from adapter_ss_obj_mapping
```

3. Restart all server components.

After the restart, the total load of statistics should be re-distributed among all the Genesys Adapters, including the new adapters.

AGA Configuration Parameters

This page contains information about the Advisors Genesys Adapter (AGA) configuration properties file (`inf_genesys_adapter.properties`). Use this information to help you to edit the AGA configuration.

Parameter	Description
<code>informiam.genesys_connector.transformer.CCAdv</code> <code>= 10</code>	Frequency of the transformer upload task for CCAdv. CCAdvChannel If the transformer upload task has not finished before the next scheduled one, the subsequently scheduled task waits in a queue.
<code>informiam.genesys_connector.ObjectChangeStatRequest.Frequency</code> <code>= 60</code>	Frequency for requesting incremental statistics for the selected object changes (in seconds). This property determines the interval at which the Genesys Adapter will handle changes to agent groups such as the addition or removal of agents. Reducing this value enables the adapter to handle those changes immediately and send updates for the Advisors dashboard. Increasing this value enables the adapter to batch the changes and request any additional statistics for the agents added.
<code>informiam.genesys_connector.statServer.maxOpenRequestsPerGroup</code> <code>= 1000</code> <code>informiam.genesys_connector.statServer.interGroupDelay</code> <code>= 1</code>	Statistics open request grouping. This property controls the maximum number of statistic open requests that will be sent to the Stat Server consecutively with no pause, as well as the pause delay (in seconds) when that many number of statistics are requested. Reducing this value ensures that the Stat Servers are not overloaded with large number of requests. Increasing this value enables quicker processing of the statistics and therefore shorter startup/restart/overnight refresh times.
<code>informiam.genesys_connector.statServer.allowRedistribution</code> <code>= false</code>	Allow redistribution to other Stat Servers. This property allows redistribution of statistics between multiple Stat Servers when more than one Stat Server pair is configured. The purpose of this flag is to allow another available Stat Server pair to support the statistics, when the Genesys Adapter can not re-establish a connection to a given Stat Server pair. If connection to both the primary Stat Server and the backup Stat Server are not available during the runtime, the Genesys Adapter receives a connection close event after the ADDP timeout. The Genesys Adapter then tries to re-establish a connection to the same pair for a number of times as configured by the following parameters: <ul style="list-style-type: none"><code>informiam.genesys_connector.statServer.reconnect.attempts</code><code>informiam.genesys_connector.statServer.reconnect.attempt-interval</code>

Parameter	Description
	<p>If the adapter cannot re-establish the connection before the expiry of the reconnect period, redistribution of the statistics is attempted, provided the capacity of the other Stat Server pair is within the limit configured by:</p> <pre>informiam.genesys_connector.statServer.maxNumOfStatsLimit</pre> <p>This functionality is disabled by default. If the statistics requested with one Stat Server pair are distributed to another Stat Server pair it could result in overloading of the other Stat Server pair.</p> <p>This property can be set to true for small customers where the total number of statistics requested is small or where the amount of statistics redistributed is small and will not result in overloading of the Stat Servers.</p>
<pre>informiam.genesys_connector.statServer.onStartWaitTimeForAllSSConnectionsToOpen = 20</pre>	<p>Time in seconds to wait on Stat Server connection to open before sending statistics requests to all opened Stat Server connections.</p> <p>This property controls how long the adapter waits for the connection to Stat Server to be established before distributing the request more widely. On start, if it is taking longer to establish connections to the configured Stat Servers, consider increasing this time limit. Waiting a longer time before establishing connection to all Stat Servers ensures more equal distribution of the statistics to the configured Stat Servers.</p>
<pre>informiam.genesys_connector.configServer.reconnect_attempts = 5</pre> <pre>informiam.genesys_connector.configServer.reconnect_attempt_interval = 30</pre>	<p>Indicates the number of reconnect attempts to the Configuration Server before trying to connect to the backup Configuration Server in the case of the connection dropping and the interval between the reconnect attempts (in seconds).</p> <p>This is in addition to – and after – the ADDP time out, if configured.</p>
<pre>informiam.genesys_connector.statServer.reconnect_attempts = 3</pre> <pre>informiam.genesys_connector.statServer.reconnect_attempt_interval = 10</pre>	<p>Indicates the number of reconnect attempts to the Stat Server before trying to connect to the backup server in the case of the connection dropping and the interval between the reconnect attempts (in seconds).</p> <p>This is in addition to – and after – the ADDP timeout, if configured</p>
<pre>informiam.genesys_connector.api.port =</pre>	The port of communication between CCAAdv and the Genesys Adapter and between FA and the Genesys Adapter.
<pre>informiam.genesys_connector.waitForStatOpenEventResponseTime = 600</pre>	<p>Process timeout values, in seconds.</p> <p>This property controls how long the Genesys Adapter waits for a response from the Stat Servers after requesting to open the statistic requests. If there is a slow response from the Stat Server, or if there are too many objects configured, consider increasing this timeout.</p>
<pre>informiam.genesys_connector.numOfMaxStatRerequestTimes = 3</pre>	Number of times the connector will attempt to re-request statistics.

Parameter	Description
	When there is an error in the process of requesting the statistics, this property determines the number of times the adapter should try and re-request all the statistics, to clear away any runtime issues. If the issue is with the configuration of statistics, it is not likely to be cleared by re-requesting of the statistics.
<pre>informiam.genesys_connector.configServer.addp.turnon = true informiam.genesys_connector.configServer.addp.tracemode = informiam.genesys_connector.configServer.addp.servvertimeout = 300 informiam.genesys_connector.configServer.addp.clienttimeout = 120 informiam.genesys_connector.configServer.protocol.request.timeout = 180</pre>	ADDP Settings to be used with the Configuration Server connection.
<pre>informiam.genesys_connector.statServer.addp.turnon = true informiam.genesys_connector.statServer.addp.tracemode = informiam.genesys_connector.statServer.addp.servvertimeout = 300 informiam.genesys_connector.statServer.addp.clienttimeout = 120</pre>	ADDP Settings to be used with the Stat Server connections.
<pre>informiam.genesys_connector.transformerjob.pausechecklimit = 25000 informiam.genesys_connector.statsissue.pausechecklimit = 5000</pre>	<p>Pause parameters that check against the queue of the incoming Stat Server messages.</p> <p>When statistics are requested, in order to avoid the JVM being overwhelmed by processing of the incoming messages from the Stat Server, the above check limits are prescribed. This enables the adapter to pause the writing of updates to the metrics database and any further processing of requests of more statistics. Once the number of statistics waiting to be processed goes below the configured limits, the paused jobs are resumed.</p> <p>In environments where sufficient runtime memory is not available, consider setting these limits to a smaller value.</p> <p>Setting a very small value could lead to delay in sending the updates to the Advisors dashboard.</p>
<pre>informiam.genesys_connector.psdk.server.fileEncoding = windows-1252</pre>	<p>File encoding to be used with the Configuration Server and the Stat Server connections.</p> <p>This file encoding property is used in encoding the text that is read from the Configuration Server and sent to the Stat Server in requesting the statistics. Adjustments to this may be needed depending upon the supported language's character encoding.</p>
<pre>genesys_connector.configServer.tls.enabled</pre>	<p>Enable or disable a TLS connection to the Configuration Server (applicable to both the primary and backup servers if using Configuration Server warm standby configuration).</p> <p>You can set the flag to <code>true</code> post-installation if you require a TLS connection to the Configuration Server, but did not enable the TLS connection when deploying Advisors Genesys Adapter</p>

Parameter	Description
	(AGA). The <code>genesys_connector.configServer.tls.enabled</code> property is the only property that AGA recognizes to enable or disable a TLS connection to Configuration Server. TLS is configured and enabled completely inside Advisors, unlike other applications whose TLS configuration can be stored in a Configuration Server Application object. A setting to disable or enable TLS (<code>tls=0</code> or <code>tls=1</code>) in the TLS properties file that you prepare is also ignored.
<code>genesys_connector.configServer.tls.port</code>	<p>Identify the Configuration Server port number for establishing a TLS connection from AGA.</p> <p>If you enable a TLS connection, the TLS port number is used for both the primary and backup Configuration Servers, where both are configured. The port number for an unsecured connection, if configured, is ignored. The primary and backup Configuration Servers must use the same TLS port number.</p>
<code>genesys_connector.configServer.tlsproperties.file</code>	<p>When using a TLS connection to the Configuration Server, specify the location of the TLS properties file that you prepared.</p> <p>The TLS properties file contains all the properties required to connect successfully using TLS, as well as any other optional TLS attributes that you use. If you use a backup Configuration Server, the TLS properties for the primary server are also used for the backup server.</p>

Stat Server Configuration Parameters

Genesys recommends that the Stat Servers configured for Advisors are configured as described on this page.

```
[java-config]
java-extensions-dir=./java/ext
java-libraries-dir=./java/lib

[java-extensions]
eServiceContactStat.jar=true
eServiceInteractionStat.jar=true

[statserver]
enable-java=true
accept-clients-in-backup-mode=yes
auto-backup-interval=0
```

The [java-config] and [java-extensions] options, as well as the Stat Server enable-java=true option, are required for supporting interaction queue statistics. If interaction queue statistics are not monitored in a given deployment, these settings are unnecessary.

The Stat Server accept-clients-in-backup-mode option should be set to Yes to allow Genesys Adapter to request statistics from both the primary and the backup Stat Servers on start. This is to support High Availability on switchover from the primary to the backup Stat Server.

The Stat Server auto-backup-interval=0 option tells the Stat Server not to create a backup file. This will ensure that the Stat Servers do not start automatically re-requesting the statistics on restart based on the stat requests cached in the backup file. The Genesys Adapter will be re-requesting the statistics and, therefore, this option should be turned off. In rare circumstances, the Stat Servers could be potentially be overloaded if this option is not set.

The configuration param file includes the statistic types of some of the standard CCAdv/WA/FA source metrics. Some of the statistics types listed in the file are needed for Resource Management Console, but not by the Advisors Genesys Adapter. Any changes made to the imported stat types in the Stat Server configuration do not affect how Genesys Adapter requests the statistics values with the Stat Server and, therefore, does not affect metric values on the CCAdv or FA dashboard.

Update AGA Properties in the Database

The **Manage Adapters** page in the Administration module is read-only. To manage Advisors Genesys Adapters (AGA), you must update the configuration in the Platform database. Use the following procedure. A new Advisors Genesys Adapter instance is automatically created in the database whenever you install a Genesys Adapter.

Important



When you install Advisors Genesys Adapter, the host name and port of the adapter that you enter in the installer screens are saved in the adapter configuration file and in the platform database. The properties must be identical in those two locations. After installation, if you make a change to one of these properties, you must make the same change in both locations (see the following procedure). If an IP address is used for the host property, then that IP address must appear in both locations. If a DNS name is used for the host property, you must use the DNS name in both locations. Names must match in case.

1. To update the properties of an installed AGA, edit the properties (HOST and PORT) in the ADAPTER_INSTANCES table in the Platform database.

2. Navigate to the installation folder for the adapter and update the following properties in the inf_genesys_adapter.properties file:

```
informiam.genesys_connector.host.name =  
informiam.genesys_connector.api.port =
```

3. Restart the Advisors suite server (Platform server) and the AGA for which you edited the properties.

4. To remove a configured AGA instance, remove the associated record from the ADAPTER_INSTANCES table in the Platform database. However, before removing an adapter instance record, you must remove any records that are dependent on it from the ADAPTER_SS_OBJ_MAPPING and ADAPTER_SS_CONFIG tables. Dependent records are keyed to the adapter_instance_id, and any delete statements need to specify this in a where clause.

Manage Restart of Multiple Adapters with Single Metrics Database

NEW In earlier releases of Advisors, if an Advisors Genesys Adapter (AGA) required a restart in a deployment where multiple instances of Contact Center Advisor (CCAdv) adapters were configured to use the same metrics database, it was necessary to restart all adapters – even if only one required the restart.

Starting in release 8.5.0, you can manage the number of adapters that must be restarted in this scenario using the `advisors.genesys_connector.dbimporter.CCAdv.metricsdb.truncateOnStart` property in the `conf/inf_genesys_importer.properties` file. Values you can enter for this property are `true` and `false`. The default value for the property is `true` (`advisors.genesys_connector.dbimporter.CCAdv.metricsdb.truncateOnStart = true`). When only one CCAdv/WA adapter is installed, it is unnecessary to change the value of the property.

The property determines if the metrics database must be truncated on startup of the CCAdv adapter. If you have multiple adapters installed in this type of deployment, Genesys recommends that you reset the flag to `false` on all the adapters *except one*.

The adapters on which you have set the flag to `false` can be restarted independently of the other adapters. On the single instance adapter where this flag is set to `true`, you must restart all other adapters when this adapter must be restarted.

CCAdv and WA

This section contains information and procedures to help you change configuration for Contact Center Advisor and Workforce Advisor after these modules are deployed.

Enable and Disable Agent-level Monitoring

You enable and disable agent-level monitoring by modifying the statistics templates for CCAdv; use the following procedures.

Enabling and Disabling the agent level statistics templates for CCAdv

NEW The procedure of enabling and disabling agent reporting in CCAdv/WA changes in release 8.5.0.

Agent reporting is enabled, by default, in all releases except 8.5.000. In release 8.5.000, agent reporting is disabled in all new installations.

Enabling Agent Reporting

1. In the Platform database/schema, execute the following statement:

```
BEGIN
UPDATE CONFIG_PARAMETER
SET PARAM_VALUE='1' WHERE PARAM_NAME='ccadv.agent.reporting.on';
COMMIT;
END;
/
```

2. This Step is applicable to release 8.5.000 only. If you have installed release 8.5.001, skip this Step.

In release 8.5.000, open the table-config.xml file in the conf folder of the Genesys Adapter deployment and ensure the following section is not commented out:

```
<tableconfig title="AgentSkillGroupRealTime">
<type>data</type>
<tablename>t_Agent_Skill_Group_Real_Time</tablename>
<formatfile>format_files/Agent_Skill_Group_Real_Time.fmt</formatfile>
<key-fields>SkillGroupSkillTargetID,SkillTargetID</key-fields>
</tableconfig>
```

3. Restart AGA. Changes will take effect during the overnight refresh cycle. If you require the changes to take effect before the overnight refresh, you must restart Advisors Platform.

Warning

Restarting Advisors Platform disconnects all users who are logged in.

Disabling Agent Reporting

1. In the platform database/schema execute the following statement:

```
BEGIN
```

```
UPDATE CONFIG_PARAMETER
SET PARAM_VALUE='0' WHERE PARAM_NAME='ccadv.agent.reporting.on';
COMMIT;
END;
/
```

2. This Step is applicable to release 8.5.000 only. If you have installed release 8.5.001, skip this Step.

Warning

If you have installed release 8.5.001, you must not delete the following tag for any reason.

In release 8.5.000, open the table-config.xml file in the conf folder of the Genesys Adapter deployment and comment out the following content, as shown:

```
<!--
<tableconfig title="AgentSkillGroupRealTime">
<type>data</type>
<tablename>t_Agent_Skill_Group_Real_Time</tablename>
<formatfile>format_files/Agent_Skill_Group_Real_Time.fmt</formatfile>
<key-fields>SkillGroupSkillTargetID,SkillTargetID</key-fields>
</tableconfig>
-->
```

3. Restart AGA. Changes will take effect during the overnight refresh cycle. If you require the changes to take effect before the overnight refresh, you must restart Advisors Platform.

Warning

Restarting Advisors Platform disconnects all users who are logged in.

Configure Metric Graphing Properties

You configure metric graphing properties during the installation of the CCAdv and WA modules.

There is no system-wide setting that determines the time period of values displayed in graphs. Users can graph five minutes and thirty minutes data in the same graph. Use the **Time Profile** for Charting option on the **Metric Manager** page of the Administration module to enable a metric for graphing.

If changes are required in the metric graphing properties after installation, use the CONFIG_PARAMETER table in the Advisors database. The following list describes the properties that govern metric graphing in the CONFIG_PARAMETER table:

- The duration of the historical values retained for graphing.
The default number is 120 minutes, or 2 hours. Changing this number will increase or decrease the number of minutes that the historical data for metrics is kept in the metric graphing database. See **Change the duration of historical values**.
- The duration of the future values displayed for graphing.
The default number is 120 minutes, or 2 hours. Changing this number increases or decreases the number of minutes that the future data of WA forecast metrics is displayed on the complete X axis (horizontal axis) of a graph. See **Change the duration of future values**.
- The minimum interval in seconds between graphed values in all graphs for points stored after the change.
See **Change the interval between values**.
- Whether graphed values display from midnight.
The default value is true. Changing this to false means that a graph will not show values with times from the previous day. See **Retain or delete values at midnight**.

<tabber>

Change the duration of historical values=

Use the following procedure to change the duration, in minutes, of the historical values that are retained for graphing.

Note that CCAdv/WA 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 the procedure on the **Change the interval between values** tab on this page.

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. The configured value for the warehoused.metrics.max.minutes.kept parameter is maintained when you upgrade to another software release.

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, CCAdv/WA stores up to n minutes of historical values for each metric in the metric graphing database. The graphing service will return n minutes of values for each graph. The graphing service also returns future values when they are available. See the procedure on the **Change the duration of future values** tab on this page.

| Change the duration of future values=

Use the following procedure to change the duration, in minutes, of the future values that are displayed for graphing. Only WA contact group forecast metrics have future values.

1. In the Advisors database, execute:

```
UPDATE CONFIG_PARAMETER SET PARAM_VALUE = 'm'
Where
PARAM_NAME = warehoused.metrics.forecast.minutes.displayed
```

For m, 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, CCAdv/WA displays up to m minutes of future values for each metric in the metric graphing database.

The graphing service returns n (warehoused.metrics.max.minutes.kept) minutes of historical values, plus m (warehoused.metrics.forecast.minutes.displayed) minutes of future values (when available) for each graph.

| Change the interval between values=

The supported amount of historical data that CCAdv/WA stores for one graphed metric is 120 values. By default, CCAdv/WA keeps 120 values that are not 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.

Use the following procedure to change the minimum number of seconds between values in a graph.

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, CCAdv/WA stores values for graphing such that a value is at least n seconds after the previous value stored. The graphing service returns the values that have been stored, according to any minimum interval setting that has existed for the duration of storage.

Example

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. Manually, 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 CCAdv/WA 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.

| - | Retain or delete values at midnight =

Use this procedure to specify whether graphs display values from the previous day.

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 graph, 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.

Configuring Forecast Metric Graph Shapes

The shape of the graph that displays in the Metric Graphing window for forecast metrics is configurable. Default values for forecast metric graph shapes are shown in the Table below.

Metric	Metrics/Graphing_Style
FNCO	saw
FNCOTotal	saw
FAHT	flat
FSL	flat
FASA	flat
REQ	flat
SCH	flat
AdjREQ	flat
AdjSCH	flat
All others	null

To change the default graph shape for a forecast metric, use the `graph_style` column in the platform database metrics table to define the shape of the graph.

The graph shapes have the following characteristics:

- saw: forecast metrics; saw-style graph. Interval in historical area: 30 minutes
- flat: forecast metrics; flat-style graph. Interval in historical area: 30 minutes
- null: the default graph shape for all non-forecast metrics; flat-style graph. Interval in historical area: 1 minute (configurable)

Work with Data Source Database Names

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 [Configure Oracle 11g Metrics Data Sources](#).

For Cisco ICM 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.

Examples of Data Source Names

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

`advisors_gametrics`

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

`ICMCENTRAL.name_awdb`

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

`[DS00001Primary-345].advisors_gametrics`

JDBC Data Source Error Logging in XML Generator

CCAdv XML Generator uses a third-party JDBC data source.

To review JDBC data source error logs, use the following procedure.

1. Stop the XML Generator Windows service.
2. Edit `xmlgen/log4j.xml`:
 - a. Find the category for `com.mchange`.
 - b. Change the level to `DEBUG`.
 - c. Save the file.
3. Restart the XML Generator Windows service.
4. Examine the XML Generator log.

Custom Time Zones

You can configure custom time zones for Workforce Advisor; use the following procedure.

1. Navigate to the \conf directory.
2. Create an empty file called `TimeZoneMapping.properties`.
3. Edit the 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.

Change the Time Profile of Agent Groups Metrics from 5 Minute Sliding to 30 Minute Growing

You can change the time profile of displayed agent group metrics from 5 Minute Sliding to 30 Minute Growing, or from 30 Minute Growing to 5 Minute Sliding, for Contact Center Advisor and Workforce Advisor.

Application metrics are unaffected by this process. Users should log out before you perform this configuration change.

1. Stop the Windows services for Advisors CCAdv XML Generator, CCAdv Web Services, Workforce Advisor Server, and WA Web Services.

2. Execute the following statements on your Advisors Platform database:

- a. View the configuration parameters:
`select * from config_parameter`
- b. Update one configuration parameter:
`update config_parameter set param_value = 'ThirtyMin' where param_name = 'skill.group.metrics.period.type'`
or
`update config_parameter set param_value = 'FiveMin' where param_name = 'skill.group.metrics.period.type'`
- c. View the parameters again to ensure your update was successful:
`select * from config_parameter`

3. Start the Windows services for Advisors CCAdv XML Generator, Workforce Advisor server, CCAdv Web Services, and WA Web Services.

Users may log in again.

4. If a column with the previous time profile continues to appear in an Agent Groups pane, do the following:

- a. Open the Column Chooser.
- b. Un-pin (de-select) that column.
- c. Find the correct Agent Group metric for the time profile you want.
- d. Pin (select) that column for display.

If you cannot see any columns with the time profile you want in the CCAdv Agent Groups pane, ensure the correct choice of Short or Medium button in the title bar is selected.

Format Alert Messages sent by Advisors

You can format the e-mail that Contact Center Advisor and Workforce Advisor send about alerts. You can format both the subject and body text of an e-mail. You may want to shorten the text to accommodate the smaller screens of pagers.

The template files for messages' subjects and body text are available after either XML Generator or the WA server is installed.

Note the following:

- 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 *Message Properties* below. The properties whose names end in `.de` are for inclusion in German text. The properties whose names end in `.en` are for inclusion in English text. The properties whose names end in `.fr` are for inclusion in French text. (Performance Management Advisors currently offer the French-language option in release 8.1.4 only.).

Properties without a suffix can be included in text in any language.

The names of business objects that you create in the Configuration Server are available in only one language. So, for example, in an e-mail sent about an alert, the name of a contact center will be in only one language. The contact center's name will replace both `${call.center.name.en}` and `${call.center.name.de}` in the template for the e-mail's subject or body.

Even though the same object name replaces the property for the name in any language, it is still necessary to have three properties – one per language. If an object name is not present, Advisors enters the word none, which is different in every language.

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

[+] Show Message Properties

Description	Property
A comma-separated list of distribution lists to which an e-mail about an alert was sent.	<code>\${distribution.list.names}</code>
The name of the application group related to an element that caused the alert. There might not be one.	<code>\${application.group.name.en}</code> <code>\${application.group.name.de}</code> <code>\${application.group.name.fr}</code>
Alert types: Business, or Technical.	<code>\${alert.type.en}</code> <code>\${alert.type.de}</code> <code>\${alert.type.fr}</code>
The name of one contact center, possibly the only contact center, associated with the alert.	<code>\${call.center.name.en}</code>

Description	Property
	<code>\${call.center.name.de}</code> <code>\${call.center.name.fr}</code>
A list of comma-separated names of all contact centers associated with the alert.	<code>\${call.center.name.list.en}</code> <code>\${call.center.name.list.de}</code> <code>\${call.center.name.list.fr}</code>
The subject: an application or a peripheral in CCAdv, a contact group in WA.	<code>\${alert.element.name.en}</code> <code>\${alert.element.name.de}</code> <code>\${alert.element.name.fr}</code>
A metric's value. There might not be one.	<code>\${alert.value.en}</code> <code>\${alert.value.de}</code> <code>\${alert.value.fr}</code>
The display name of the metric whose threshold violation caused the alert. There might not be one.	<code>\${alert.metric.name.en}</code> <code>\${alert.metric.name.de}</code> <code>\${alert.metric.name.fr}</code>
The value entered on the System Configuration page, called Threshold Trigger Delay Rate (minutes) in that page. This might not be appropriate for some of these alerts. For example, a technical alert about a peripheral gateway being offline is reported as soon as it is detected, not after a delay.	<code>\${alert.delay.minutes}</code>
The alert's start date and time.	<code>\${alert.start.time.en}</code> <code>\${alert.start.time.de}</code> <code>\${alert.start.time.fr}</code>
How long the alert is/was active.	<code>\${alert.duration.minutes}</code>
The alert's status: active or expired.	<code>\${alert.active.status.en}</code> <code>\${alert.active.status.de}</code> <code>\${alert.active.status.fr}</code>
The name of the geographic region related to the element that caused the alert. There might not be one.	<code>\${geographic.region.name.en}</code> <code>\${geographic.region.name.de}</code> <code>\${geographic.region.name.fr}</code>
The name of the reporting region related to the element that caused the alert. There might not be one.	<code>\${reporting.region.name.en}</code> <code>\${reporting.region.name.de}</code> <code>\${reporting.region.name.fr}</code>
Name of the operating unit related to the element that caused the alert. There might not be one.	<code>\${operating.unit.name.en}</code> <code>\${operating.unit.name.de}</code> <code>\${operating.unit.name.fr}</code>

[+] Show Examples

CCAdv Message for an Alert Concerning a Threshold Violation

This is located in: c:\advisors\conf\templates\AlertThresholdViolation_EmailTemplate.txt. This example assumes that, at installation, you chose both German and English. Therefore, the template file contains the text in both languages.

Contact Center Advisor hat eine Verletzung eines Business-Alarms festgestellt, den Sie abonniert haben. Sie erhalten diesen Alarm, da der nachstehende Schwellenwert länger als der definierte Zeitraum außerhalb des akzeptablen Bereichs von `${alert.delay.minutes}` Minuten lag.

Dieser Alarm betrifft das geografische Gebiet `${geographic.region.name.de}`, Berichtsgebiet `${reporting.region.name.de}`, Einheit `${operating.unit.name.de}` und das Contact Center: `${call.center.name.list.de}`.
Betroffene Anwendung: `${alert.element.name.de}` in der Anwendungsgruppe `${application.group.name.de}`.
Verletzte Metrik: `${alert.metric.name.de}`.
Aktueller Metrikwert: `${alert.value.de}`.
Schwellenwertverletzung zuerst festgestellt bei: `${alert.start.time.de}`.
Der Alarm ist aktiv seit: `${alert.duration.minutes}` Minuten.
Der Alarmstatus ist: `${alert.active.status.de}`.

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 `${geographic.region.name.en}`, Reporting Region `${reporting.region.name.en}`, Operating Unit `${operating.unit.name.en}`, and the Contact Center: `${call.center.name.list.en}`. It involves the application `${alert.element.name.en}` in the Application Group `${application.group.name.en}`.

Metric violated was: `${alert.metric.name.en}`.
Current metric value: `${alert.value.en}`.
Threshold violation was first detected at: `${alert.start.time.en}`.
The alert has been active for: `${alert.duration.minutes}` minutes.
The alert's status is: `${alert.active.status.en}`.

CCAdv Message for an Alert Concerning an Offline Peripheral

This is located in: c:\advisors\conf\templates\AlertOther_EmailTemplate.txt. This example assumes that, at installation, you chose both German and English. Therefore, the template file contains the text in both languages.

Contact Center Advisor hat eine Verletzung des Alarms `${alert.type.de}` festgestellt, den Sie abonniert haben. Dieser Alarm betrifft die folgenden Contact Center(s): `${call.center.name.list.de}`.
Betroffenes Element (Peripheriegerät/Anwendung etc.): `${alert.element.name.de}`.
Alarm zuerst festgestellt bei: `${alert.start.time.de}`.
Alarmstatus: `${alert.value.de}`.
Der Alarm ist aktiv seit: `${alert.duration.minutes}` Minuten.
Der Alarmstatus ist: `${alert.active.status.de}`.

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

WA Message for an Alert Concerning a Threshold Violation

This is located in: `c:\advisors\conf\templates\AlertThresholdViolation_EmailTemplateWU.txt`. This example assumes that, at installation, you chose both German and English. Therefore, the template file contains the text in both languages

Workforce Advisor hat eine Verletzung eines Business-Alarms festgestellt, den Sie abonniert haben. Sie erhalten diesen Alarm, da der nachstehende Schwellenwert länger als der definierte Zeitraum außerhalb des akzeptablen Bereichs von `${alert.delay.minutes}` Minuten lag.
 Dieser Alarm betrifft das geografische Gebiet `${geographic.region.name.de}`, Berichtsgebiet `${reporting.region.name.de}`, Einheit `${operating.unit.name.de}` und das Contact Center: `${call.center.name.list.de}`.
 Betroffene Kontaktgruppe: `${alert.element.name.de}` in der Anwendungsgruppe `${application.group.name.de}`.
 Verletzter Metrik: `${alert.metric.name.de}`.
 Aktueller Metrikwert: `${alert.value.de}`.
 Schwellenwertverletzung zuerst festgestellt bei: `${alert.start.time.de}`.
 Der Alarm ist aktiv seit: `${alert.duration.minutes}` Minuten.
 Der Alarmstatus ist: `${alert.active.status.de}`.

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 `${geographic.region.name.en}`, Reporting Region `${reporting.region.name.en}`, Operating Unit `${operating.unit.name.en}`, and the Contact Center: `${call.center.name.list.en}`.

It involves the contact group `${alert.element.name.en}` in the Application Group `${application.group.name.en}`.

Metric violated was: `${alert.metric.name.en}`.
 Current metric value: `${alert.value.en}`.
 Threshold violation was first detected at: `${alert.start.time.en}`.
 The alert has been active for: `${alert.duration.minutes}` minutes.
 The alert's status is: `${alert.active.status.en}`.

Language Order in Templates

If required, you can re-order the languages used in the e-mail templates by editing the template file

directly.

Testing E-mail Sent by XML Generator

You can test the mail sent by XML Generator without actually running the application and configuring the conditions that would cause it to send the e-mail.

1. Change directory to the Advisors base directory (the one in which you installed Genesys Advisors), and then change it to \xmlgen.

2. Run the command:

```
emailtest.bat
```

Importing Contact Groups into Advisors

Files for Contact Groups

Workforce Advisor accepts data from three WFM systems:

- Genesys Workforce Management (WFM)
- IEX TotalView
- Aspect eWFM

See the [Genesys Interoperability Guide](#) for information about supported versions.

From Genesys WFM

WA requests data from Genesys WFM directly using the API of Genesys WFM. The properties that govern this are set at installation. The properties are stored in the `conf/WorkforceAdvisor.properties` file.

The `WorkforceUtilization-GenesysMetricsMapping.properties` file is another properties file specific to importing from Genesys WFM. The properties in the file let you choose the KPIs that WA imports from Genesys WFM. For information about how to map those KPIs to WA's metrics, see [Metrics Correspondences among WFM Systems](#).

From IEX TotalView

Input files from IEX TotalView are sent by FTP to a port number chosen at installation. The port number is preserved in a property in the `conf/WorkforceAdvisor.properties` file. WA's FTP functionality listens on that port for incoming data.

IEX TotalView can send data to WA directly using FTP. That is, it is not necessary to first write the data to files on the disk, and then send those to WA by FTP.

After WA accepts one of these data sets, it backs it up in a file in the Advisors directory. The file is placed in the subdirectory `geronimo-tomcat6-minimal-2.2.1\bin\ftpd\iex`. There you can find the latest version of the data that WA accepted, although WA does not use this file. Changing this file does not affect WA. The `conf/WorkforceUtilization.properties` file has properties that tell WA how to remove these files from the directory:

- `iexLogCleaner.repeatInterval`: The default setting checks for files to remove every 12 hours.
- `iexLogCleaner.period`: The default setting removes files older than three days.

One data set from IEX TotalView can contain data from more than one contact group.

Sending IEX TotalView files to WA using an FTP server

Unlike eWFM forecast data that WA fetches, IEX files are pushed to WA. WA does not read the IEX files until the FTP server pushes them to WA. IEX TotalView can send data to WA directly using FTP. That is, it is not necessary to first write the data to files on the disk, and then send those to WA by FTP.

To achieve this, you require the following, in addition to the IEX files:

1. A batch file that contains the following:

```
REM sends the current IEX file to the ftp service in WU on port 6021.
ftp -s:sendIEXFile.txt
pause
```
2. A SendIEX file that contains the names of the IEX files:

```
open localhost 6021
iex
iex!bat
bin
send "<<Enter your IEX filename here and repeat this line for every IEX file that
exists>>"
quit
```

Use a *Cron-job* to send the IEX files on a daily basis using the FTP server. To create a Cron-job, go to Start > Accessories > System tools > Scheduled Tasks. Create a new scheduled task and set up the batch file to run automatically at specific times.

From Aspect eWFM

Input files from Aspect eWFM are read from a directory chosen at installation. WA preserves the directory path in a property in the `conf/WorkforceUtilization.properties` file.

WA reads the files at an interval configured by a property in the `conf/WorkforceAdvisor.properties` file. That file also has properties that determine the field separator character and date format it uses when reading the file's data. WA does not back up these files, nor does it delete them after reading them.

One file from Aspect eWFM can contain data for only one contact group.

How WA Distributes Metrics from eWFM

For the distributed scenario of data from Aspect eWFM, the data for each contact group is in more than one file. The metrics for one forecast contact group are in one file.

Metrics for related staff contact groups are in one or more different files.

WA apportions the metrics' values from the forecast contact group among the staff contact groups, and then ignores the forecast contact group. That is, essentially it imports only the staff contact groups, but these have all the necessary metrics.

Below is how WA apportions the metrics' values from the forecast contact group to the related staff

contact groups. For one staff contact group:

Staff CG RVOL = (Forecast CG RVOL * (Staff CG SGRSCH / Sum(SGRSCH of all Staff CGs related to Forecast CG))

Staff CG RSL = Forecast CG RSL

Staff CG RDELAY SEC = Forecast CG RDELAY SEC

Staff CG RAHT = Forecast CG RAHT

[Back to Top](#)

Contact Group Synchronization Log

WA does not create a separate log file to record the effect of an import of data for contact groups from any system. WA logs the data in the `geronimo.log` file of the Geronimo in which the WA Server is deployed. This log file is in the Advisors deployment directory, in subdirectory `geronimo-tomcat6-minimal-2.2.1\var\log`.

This logging is controlled by a category in the `server-log4j.properties` file in the same subdirectory. The category is `com.informiam.workforceutilization.service.integration.batch.ContactGroupImporterImpl` and, by default, is set to `INFO`, which will output the messages described here.

An example of an entry in the log is:

```
ContactGroupImportLogEntry{
  logDate=Fri Jun 01 22:34:58 EDT 2012,
  netNewContactGroups=[ContactType{id=WFMPProd01-Complaints, name='Complaints'}],
  inactivatedContactGroups=[],
  reactivatedContactGroups=[]}
```

This log entry says that:

- On the last import of a contact group or set of them, there was one new contact group.
- The new contact group's source system's name is `WFMPProd01`.
- The group's ID in its system of origin, (as far as Advisors can determine), is `Complaints`. The name is `Complaints`.

[Back to Top](#)

File Names for Contact Groups

The names of the files with contact group data have special meaning, as described in the following sections. The file names carry this meaning because the contents of the file cannot carry it.

From IEX TotalView

The format of the name of a file from IEX TotalView is:
`sourceSystemName.anyText`

The segment `.anyText` is mandatory, but can simply be the file's extension. For example:
`IEXSystem1.ContactGroupsForecastData.txt`
`Prod02.DailyForecast.csv`

The source system name establishes a namespace for the names of all the contact groups that the file contains. It allows Advisors to distinguish contact groups with the same name from different WFM systems.

Source system names are case-sensitive. Source names must be unique across all sources. That is, data from IEX TotalView and Aspect eWFM cannot have the same source name.

Once you first import a file with a given source system name, you should not change it. If you change it, WA will not recognize that the contact groups come from the same source system. It will create in the Advisors database a new set of contact groups with a different source system name.

The source system name appears in the Administration module, in the **Contact Groups Configuration** page, Contact Group Details tab. It can also qualify contact groups' names in other places in which Advisors displays them.

Advisors assigns the type forecast to all contact groups from IEX TotalView. This type also appears in the Administration module, in the **Contact Groups Configuration** page, Contact Group Details tab. Advisors does not use this type; it is for information only.

From Aspect eWFM

The format of the name of a file from Aspect eWFM is:
`sourceSystemName.contactGroupName.anyText.csv`

The segment `.anyText` is optional. WA ignores it if it is present. If you replace `anyText` with a timestamp, you can use this text to differentiate the same data sent at different times. This prevents WA from trying to read a file that something else is currently writing. For example:

`AspectSystem1.RS.csv`
`Aspect.RS.csv`
`ewfm.03_RET.csv`
`Aspect1.04DESQ.2011-09-13.csv`

The source system name establishes a namespace for the contact group whose name follows it in the file name. It allows Advisors to distinguish contact groups with the same name from different WFM systems.

Source system names are case-sensitive. Source names must be unique across all sources. That is, data from IEX TotalView and Aspect eWFM cannot have the same source name.

Once you first import a file with a given source system name, you should not change it. If you change it, WA will not recognize that the contact groups come from the same source system. It will create in

the Advisors database a new set of contact groups with a different source system name.

The source system name appears in the Administration module, in the **Contact Groups Configuration** page, Contact Group Details tab. It can also qualify contact groups' names in other places in which Advisors displays them.

The contact group name is the name of the contact group.

If the contact group name starts with FG, then Advisors assigns the type forecast to the contact group; otherwise it assigns the type staff. This type (forecast) also appears in the Administration module, in the **Contact Groups Configuration** page, Contact Group Details tab. Advisors does not use this type; it is for information only.

You can put multiple files in the ewfm folder for a given `sourceSystemName.contactGroupName`. Genesys recommends that you format the files using the following convention to ensure WA imports the most recent file:

`<sourceSystemName>.<contactGroupName>.<yyyyMMddhhmmss>`

For example:

- Pipkins1.CAE.20130605101010.csv
- Pipkins1.CAE.20130605111010.csv

These two files have the same `sourceSystemName` and `contactGroupName`, but the time values differ. WA compares these values and imports the most recent file. From the previous example, WA imports the line items in the Pipkins1.CAE.20130605111010.csv file, and ignores the Pipkins1.CAE.20130605101010.csv file.

Distributed and Undistributed Scenarios

From Aspect eWFM, the real-time data for one contact group is in:

- One file (the undistributed scenario)
- More than one file (the distributed scenario)

For WA to read these files, you must follow a convention about where to put them in the file system.

For the undistributed scenario, put the files into the directory you supplied for WA at installation.

For the distributed scenario, the data for each contact group is in more than one file. Metrics for forecast contact groups are in one file. Metrics for related staff contact groups are in one or more different files.

Put the file of forecast contact group metrics in the directory supplied for WA at installation.

Put the files of staff contact groups in a subdirectory of that directory. The name of the subdirectory should be the name of the file of the forecast contact group.

Example

Data for the forecast contact group is in:

Aspect.A_FCAST_GROUP.csv

Data for the staff contact groups is in:

Aspect.A_STF_GROUP_1.csv

Aspect.A_STF_GROUP_2.csv

Aspect.A_STF_GROUP_3.csv

Aspect.A_STF_GROUP_4.csv

1. In the directory chosen at installation, put Aspect.A_FCAST_GROUP.csv.
2. In that directory, create a subdirectory named Aspect.A_FCAST_GROUP.
3. In the subdirectory, put the other files. The names of these files do not matter. WA knows they belong to Aspect.A_FCAST_GROUP.csv because the directory name matches its file name.

You can mix both scenarios. That is, you could also put Aspect.A_CONTACT_GROUP.csv in the top directory, and WA would read and interpret it as usual.

See [How WA Distributes Metrics from eWFM](#) for information about how the distributed scenario affects the way WA collects metric values for contact groups.

[Back to Top](#)

Contact Group File Header

Each file must have a header exported by the WFM system so that Workforce Advisor knows which metrics are present, and their order. The columns in these files can be in any order. The only requirement is that the column's header, in the first row, must be in the same position in that row as the data in the following rows for that column. For example, if period is the fifth column header, then the values for period must be the fifth value in each row.

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

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

```
#sort:date,period,TZ,custID,saGroupID,saGroupName,ssGroupID,ssGroupName,buID,buName,
ctID,ctName,acdID,modify,fcstContactsReceived,fcstContactsHandled,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 of the following formats:

- One file (undistributed)
- Two files (distributed)

The header records are as follows:

- Undistributed scenario
In the one file for both forecast and staff groups, WA uses the data from the following fields:
START_TIME, HOUR, MINUTE, RVOL, RAHT, RSL, RDELAY SEC, SGRREQ, SGRSCH
- Distributed scenario
In a file of metrics for forecast contact groups, WA uses the data from the following fields:
START_TIME, HOUR, MINUTE, RVOL, RAHT, RSL, RDELAY SEC, SGRREQ, SGRSCH

In a file of metrics for staff contact groups, WA uses the data from the following fields:
START_TIME, HOUR, MINUTE, SGRSCH, SGRREQ, RDELAY SEC

WA does not use the PRI_INDEX, ROUTING_SET, or STOP_TIME fields.

WA uses the following fields from eWFM data files:

- START_TIME—WA uses the date component of the start time to determine the day, month, and year to which the data applies.
- HOUR, MINUTE—WA uses these fields to determine the time of day to which the data applies.

[Back to Top](#)

Importing Contact Groups with Fifteen Minute Forecasts into WA

Workforce Advisor will accept data in which the forecast intervals are 15 minutes instead of 30 minutes. It will accept such data from any of the supported WFM systems.

Because WA is designed to display metrics only for a 30-minute forecast period that starts on the current half hour, WA has to combine the metrics from 15-minute periods in order to use them.

The simplest case is two 15-minute forecast periods, starting on a half hour and 15 minutes after that. For example, two periods starting at 09:00 (period 1) and 09:15 (period 2). The information below describes how WA combines the forecast metrics from these periods into metrics for the 30-minutes period starting at 09:00.

In the equations, a metric for period 1 is M^1 , and a metric for period 2 is M^2 .

- $FNCO \text{ for 30 minutes} = FNCO^1 + FNCO^2$.
 - If either $FNCO^1$ or $FNCO^2$ is null, then the result is the value of the other.
 - If both are null, then the result is null.
- $FNCO_{Total} \text{ for 30 minutes} = FNCO_{Total}^1 + FNCO_{Total}^2$.
 - If either $FNCO_{Total}^1$ or $FNCO_{Total}^2$ is null, then the result is the value of the other.
 - If both are null, then the result is null.
- $FAHT \text{ for 30 minutes} = (FAHT^1 * FNCO^1 + FAHT^2 * FNCO^2) / (FNCO^1 + FNCO^2)$.

-
- If either metric from period 1 is null, then the result is $FAHT^2$.
 - If either metric from period 2 is null, then the result is $FAHT^1$.
 - If the denominator is 0, then the result is null.
 - $FSL \text{ for 30 minutes} = (FSL^1 * FNCO^1 + FSL^2 * FNCO^2) / (FNCO^1 + FNCO^2)$.
 - If either metric from period 1 is null, then the result is FSL^2 .
 - If either metric from period 2 is null, then the result is FSL^1 .
 - If the denominator is 0, then the result is null.
 - $REQ \text{ for 30 minutes} = (REQ^1 * FNCO^1 * FAHT^1 + REQ^2 * FNCO^2 * FAHT^2) / (FNCO^1 * FAHT^1 + FNCO^2 * FAHT^2)$.
 - If any metric from period 1 is null, then the result is REQ^2 .
 - If any metric from period 2 is null, then the result is REQ^1 .
 - If the denominator is 0, then the result is null.
 - $SCH \text{ for 30 minutes} = (SCH^1 * FNCO^1 * FAHT^1 + SCH^2 * FNCO^2 * FAHT^2) / (FNCO^1 * FAHT^1 + FNCO^2 * FAHT^2)$.
 - If any metric from period 1 is null, then the result is SCH^2 .
 - If any metric from period 2 is null, then the result is SCH^1 .
 - If the denominator is 0, then the result is null.
 - $AdjREQ \text{ for 30 minutes} = (AdjREQ^1 * FNCO^1 * FAHT^1 + AdjREQ^2 * FNCO^2 * FAHT^2) / (FNCO^1 * FAHT^1 + FNCO^2 * FAHT^2)$.
 - If any metric from period 1 is null, then the result is $AdjREQ^2$.
 - If any metric from period 2 is null, then the result is $AdjREQ^1$.
 - If the denominator is 0, then the result is null.
 - $AdjSCH \text{ for 30 minutes} = (AdjSCH^1 * FNCO^1 * FAHT^1 + AdjSCH^2 * FNCO^2 * FAHT^2) / (FNCO^1 * FAHT^1 + FNCO^2 * FAHT^2)$.
 - If any metric from period 1 is null, then the result is $AdjSCH^2$.
 - If any metric from period 2 is null, then the result is $AdjSCH^1$.
 - If the denominator is 0, then the result is null.

WA combines 15-minute periods as follows:

- Period 1 starting at n:00 and period 2 at n:15 combine to one 30-minute period starting at n:00.
 - Period 1 starting at n:30 and period 2 at n:45 combine to one 30-minute period starting at n:30.
 - A missing period 1 starting at n:00 and available period 2 starting at n:15 combine to one 30 minute period starting at n:00 that has the metrics from period 2.
-

- A missing period 1 starting at n:30 and available period 2 starting at n:45 combine to one 30 minute period starting at n:30 that has the metrics from period 2.
- Period 1 starting at n:00 and a missing period 2 starting at n:15 combine to one 30 minute period starting at n:00 that has the metrics from period 1.
- Period 1 starting at n:30 and a missing period 2 starting at n:45 combine to one 30 minute period starting at n:30 that has the metrics from period 1.

[Back to Top](#)

Metrics Correspondences among WFM Systems

The Table below shows the relationships among the WFM metrics from different WFM systems. If a metric is not available from a WFM system, then its name in the Table, in the context of that system, is '-'.

Notes:

- Name shows the data in the NAME column of the METRICS table in the Advisors database.
- Display Name shows the data in the DISPLAY_NAME column of the METRICS table in the Advisors database.
- IEXTotalView names are in the headers of files imported from that system.
- Aspect eWFM names are in the headers of files imported from that system.
- Genesys WFM's names are constants in `com.genesyslab.wfm7 ... EPerfInfoItems`. They are supplied to `WFMPerformanceService750Soap.getPerformanceData()`. If these parameters are not correct, you can map different ones to WA's canonical names in the `conf/WorkforceUtilization-GenesysMetricsMapping.properties` file.

Name	Display Name	WA Canonical Name	IEX TotalView	Aspect eWFM	Genesys WFM
FNCO	Forecast NCO	fcstContactsReceived	fcstContactsReceived	RVOL	PERF_ITEM_FRC_IV
FAHT	Forecast AHT	fcstAHT	fcstAHT	RAHT	PERF_ITEM_FRC_AHT
FSL	Forecast SL%	fcstSLPct	fcstSLPct	RSL	PERF_ITEM_FRC_CALC_SERVICE
FASA	Forecast ASA	fcstASA	fcstASA	RDELAY SEC	PERF_ITEM_FRC_CALC_ASA
REQ	Required Staff	fcstReq	fcstReq	SGRREQ	PERF_ITEM_FRC_REQ_STAFFING
SCH	Scheduled Staff	schedOpen	schedOpen	SGRSCH	PERF_ITEM_SCH_COVERAGE
AdjREQ	Adjusted Required Staff	fcstReqAdj	-	SGRREQ JU	-
AdjSCH	Adjusted Scheduled Staff	schedOpenAdj	-	SGRSCH J	-
FNCOTotal	Forecast NCO Total	fcstContactsReceivedTotal		RVOL_TOTAL	-

[Back to Top](#)

Bulk Configuration Overview

The bulk configuration tool allows you to quickly configure Contact Center Advisor (CCAdv), Workforce Advisor (WA), or both outside of the Advisors Administration module. The tool configures CCAdv, WA, or both based on the lists of objects you define and export from other systems and load into temporary structures in the Advisors Platform database. The bulk configuration tool retrieves the data from the temporary structures, validates it, and transforms it into CCAdv, WA, or CCAdv/WA rollup configuration.

You can use spreadsheets or CSV files to collect the configuration information into a simple file structure that can be loaded into a database table. Templates of Excel spreadsheets are supplied in the installation package.

Alternatively, you can omit the file preparation and load the data directly into the database table from the sources available through your relational database management system (RDBMS).

The bulk configuration procedures for CCAdv and WA can be executed on the Platform Oracle schema or Advisors Platform MS SQL Server database. The configuration logic, rollups, and dashboard views depend on which of the following two configuration modes you select:

- integrated configuration mode: you can configure CCAdv and WA simultaneously if the aggregation mappings of WA contact groups are expected to match the aggregation mappings of the applications related to those contact groups. Set the integrated configuration mode for CCAdv and WA and use the bulk configuration tool for integrated mode. Contact groups listed in the prepared data structures inherit the aggregation mappings specified for the relevant CCAdv applications.
- independent configuration mode: if you require the aggregation mappings to be different between CCAdv and WA, set the independent configuration mode and use the bulk configuration tools for the independent mode.

For information about the configuration modes and how to set the mode, see [Contact Center Advisor and Workforce Advisor Administrator User's Guide](#). You must select the configuration mode before you perform bulk configuration.

CCAdv/WA Bulk Configuration – Integrated Mode

For information about the configuration modes and how to set the mode, see [Contact Center Advisor and Workforce Advisor Administrator User's Guide](#). You must select the configuration mode before you perform bulk configuration. Integrated mode is the default mode of operation.

Use the CCAdv/WA bulk configuration tool when you run CCAdv and WA in integrated configuration mode. When you set the integrated configuration mode:

- Agent group-to-application relationships are automatically propagated to the configured contact groups mapped to these applications.
- Applications are available for mapping to a contact group only if they are configured and have a compatible aggregation structure with this contact group.
- Applications mapped to contact groups are included in the WA rollup only if those applications are configured and have a compatible aggregation structure. Any change of application configuration for CCAdv, or a change of contact group configuration for WA that makes the aggregation structures incompatible, removes the application from WA configuration. A configured application and a configured contact group mapped to a non-AGCC contact center have compatible aggregation structures if both are mapped to the same contact center, application group, and regions. A configured application and a configured contact group mapped to an AGCC contact center have compatible aggregation structures if both are mapped to the same application group and regions and the application is mapped to a contact center that represents a parent of the AGCC to which the contact group is mapped.
- Agent groups cannot be mapped to network contact center (NCC) contact groups directly. The list of available agent groups is always empty for NCC contact groups, while the list of assigned agent groups represents the agent groups derived from the contact group-application-agent group relationships.
- Agent groups mapped to an agent group contact center (AGCC) can be mapped to contact groups associated with the AGCC, but they are not included in WA dashboard views until mapped to an application that belongs to the parent NCC and that has a compatible aggregation structure.

<verttabber>

Database Structures, Scripts, and Procedures=

An object creation script, `blkObjectsCre.sql`, is supplied in the installation package, in the `sql\oracle\bulkconfig\integrated\ccadv-wa-bulkload` folder. You must execute `blkObjectsCre.sql` as a script – not as a statement – if opened and executed from the SQL Developer SQL Worksheet.

You apply the `blkObjectsCre.sql` object creation script to the Platform schema to create the following tables, which are required for the contact group bulk configuration:

- `blkAllNames`
- `blkAllAgntGr`
- `blkAllLog`

You must create all of the preceding tables, but the content is optional. Any and all tables can remain empty. Empty tables do not impact the configuration in any way.

Objects already present in CCAdv/WA configuration, but absent from these tables, remain in the WA configuration after you perform the bulk configuration procedure.

Stored Procedure for Bulk Configuration

You implement the bulk configuration by running a stored procedure, `spblkConfigCCAdvWAIIntegrated`, which is also created when you run the `blkObjectsCre.sql` script. You execute the procedure against the Platform Oracle schema, or against the Advisors Platform MS SQL Server database, after all base data is prepared in the tables created by running the `blkObjectsCre.sql` script.

Script to Remove Objects Used in Bulk Configuration Process

The `blkObjectsDrop.sql` script removes all objects used in the bulk configuration (such as the tables that the `blkObjectsCre.sql` script creates). You must execute the `blkObjectsDrop.sql` script before you switch to the independent configuration mode and use bulk configuration tools for that mode.

Stored Procedure for Removing Configuration

You can quickly and completely remove all CCAdv application, agent group and related AGCCs configuration created inside or outside the bulk configuration tool. To remove the configuration, execute the `spblkRemoveConfigCCAdv` stored procedure.

In integrated configuration mode, WA configuration depends on the CCAdv configuration. The removal of CCAdv configuration also removes parts of the WA configuration, specifically all relationships of contact groups to applications and agent groups. As a result, the WA dashboard will not contain real-time metrics and agent groups. If you restore the CCAdv configuration, all WA relationships will be restored, unless the WA configuration removal procedure is applied before the CCAdv configuration is restored.

Execute the `spblkRemoveConfigWA` stored procedure to remove the WA contact group configuration including relationships to applications, agent groups, and agent group contact centers and to remove the agent group contact centers associated with WA.

Executing the `spblkRemoveConfigCCAdv` procedure (Oracle):

```
DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkRemoveConfigCCAdv"
(
M => M,
R => R
);
END;
```

Executing the `spblkRemoveConfigWA` procedure (Oracle):

```
DECLARE
M VARCHAR2(200);
```

```

R NUMBER;
BEGIN
"spblkRemoveConfigWA"
(
M => M,
R => R
);
END;

```

In an MS SQL Server installation, execute the procedure as follows:

```

USE <name of Advisors platform database>
GO
DECLARE@m varchar(255),
@r int
EXEC spblkRemoveConfigWA
@m = @m OUTPUT,
@r = @r OUTPUT
SELECT @m as N'@m',
@r as N'@r'
GO

```

```

DECLARE@m varchar(255),
@r int
EXEC spblkRemoveConfigCCAdv
@m = @m OUTPUT,
@r = @r OUTPUT
SELECT @m as N'@m',
@r as N'@r'
GO

```

Important

The procedure will remove all data left from previous configurations that may have a negative impact on the new configurations. It can be very useful before the configuration mode is changed.

To be able to restore the configuration, you must have a reliable set of bulk configuration files or blk tables that you can use to re-load the configuration. Before you execute the configuration removal procedures, make sure that such data exists.

You also can execute the bulk configuration removal procedures if you are comfortable with the current configuration loss and want to re-configure the applications from the beginning.

The configuration removal procedure does not remove the data from blk files. Those are always preserved unless the tables are dropped by running the blkObjectsDrop.sql script.

[-] Prerequisites and Preparations=

- The application server and XML Generator service must be up and successfully running until the required data (see the following three bullets) displays on the pages of the Advisors Administration module. To ensure that the import runs successfully, check the XML Generator log for import-related errors.
 - Log in to the Advisors application; Advisors automatically imports all relevant aggregated objects (regions, operating units, contact centers, and application groups) from the Genesys Configuration Server.
 - All relevant applications and agent groups have been automatically imported by XML Generator, and are available for configuration.
-

- If WA configuration is included in the bulk data, all relevant contact groups have been automatically imported by the WA server from the WFM system(s) specified during Advisors installation, and are available for configuration.
- Prior to bulk configuration, ensure that all relevant application groups, reporting regions, geographic regions, operating units, and network contact centers are configured. You configure these manually using Advisors administration module.
- No existing configuration is removed when using the bulk configuration tool. If any objects are already configured, or any application-to-agent group relationships are added manually (using the Administration module), they are not removed by the bulk configuration tool. The tool adds to the configuration or changes the mappings of the existing configured objects based on the data contained in the temporary structures.
- If an AGCC does not already exist, one is created by the bulk configuration procedure under every network call center where each application mapped to it (that is, to the NCC) is also mapped to an agent group and that agent group is mapped to an AGCC.

Genesys recommends that all aggregated objects participating in CCAdv/WA configuration are activated in Advisors administration module prior to performing bulk configuration. Optionally, you can complete this step after bulk configuration. In either case, it is required to make the objects visible on the dashboard view.

[-] Bulk Configuration of CCAdv/WA in Integrated Configuration Mode=

The following procedure summarizes the steps to perform bulk configuration of CCAdv and WA when you use the applications in integrated configuration mode. The information following this procedure provides additional information to assist you.

1. Start Advisors Application Server and XML Generator.

2. Watch the XML Generator and Geronimo logs.

The logs must be free of any import-related errors.

3. Allow the Advisors application to run for approximately 10 minutes.

4. Open the Administration module in the browser.

5. When the aggregated objects are available, configure all those that you plan to use in CCAdv/WA rollups (see *Prerequisites and Preparations*).

6. Open each of the following pages and ensure that you can see objects among the available and/or configured object lists, as applicable:

- Application Configuration page
- Agent Group Configuration page
- Contact Group Configuration page

7. Connect to the Oracle or MS SQL instance as the platform user.

8. Execute the blkObjectsCre.sql script.

You must execute blkObjectsCre.sql as a script – not as a statement – if opened and executed from the SQL Developer SQL Worksheet.

9. Populate the database tables with your contact group data.

For information about preparing your data, see *Data Preparation*.

For information about importing data from spreadsheets to the database, see *Loading Data from Spreadsheets into Temporary Database Structures*.

10. Execute the `spblkConfigCCAdvWAIIntegrated` procedure; for example, use the following string with an Oracle schema:

```
DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkConfigCCAdvWAIIntegrated"(
M => M,
R => R
);
END;
```

In an MS SQL Server installation, execute the procedure as follows:

```
USE <name of Advisors platform database>
GO
DECLARE@m varchar(255),
        @r int

EXEC    spblkConfigCCAdvWAIIntegrated
        @m = @m OUTPUT,
        @r = @r OUTPUT

SELECT  @m as N'@m',
        @r as N'@r'

GO
```

11. Verify the log stored in the `blkAllLog` table.

For information about logs related to the bulk configuration, see *Bulk Configuration Validation and Logs*.

12. Correct the data, if necessary, and go back to Step 10.

13. Examine all relevant configuration pages in the Advisors Administration module to verify the configuration.

14. Examine the dashboards to verify the configuration.

15. Do one of the following:

- a. If you are satisfied with the resulting configuration, connect to the Oracle instance as platform user and execute the `blkObjectsDrop.sql` script to remove all temporary structures and bulk load procedures.
- b. If you are not satisfied with the resulting configuration, go to Step 12. Alternatively, if you see unpredictable results, and you have a reliable set of bulk configuration data loaded into `blk` tables, you can remove the whole CCAdv/WA configuration by executing the CCAdv and WA configuration removal procedures. After that you can reload the configuration as described in Step 10. You can remove the whole configuration by executing the following (Oracle):

```
DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkRemoveConfigCCAdv"
```

```
(
M => M,
R => R
);
END;

DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkRemoveConfigWA"
(
M => M,
R => R
);
END;
```

In MSSQL Server installations the procedure calls are done as follows:

```
USE <name of Advisors platform database>
GO
```

```
DECLARE@m varchar(255),
        @r int
```

```
EXEC    spblkRemoveConfigCCAdv
        @m = @m OUTPUT,
        @r = @r OUTPUT
```

```
SELECT @m as N'@m',
        @r as N'@r'
```

```
GO
```

```
DECLARE @m varchar(255),
        @r int
```

```
EXEC    spblkRemoveConfigWA
        @m = @m OUTPUT,
        @r = @r OUTPUT
```

```
SELECT @m as N'@m',
        @r as N'@r'
```

```
GO
```

| Data Preparation=

You can use spreadsheets or CSV files to collect data in a simple file structure that can be loaded into a database table. Data preparation for WA can be done while doing data preparation for CCAdv.

Alternatively, you can omit the file preparation and load the data directly into the database table from the sources available through your relational database management system (RDBMS).

If you use spreadsheets or CSV files to collect your data, use the information in this section.

Applications

Your spreadsheet or CSV file contains the list of all application names that need to be configured together with the corresponding application display names, contact center names, application group names, reporting region, and operating unit names. Your file must contain eight columns with headers (headers are mandatory), and provide the following information:

- Application Name
- Application Display Name
- Contact Center Name
- Application Group Name
- Reporting Region Name
- Operating Unit Name
- Contact Group Name
- Contact Group Display Name

Add relevant data to the spreadsheet or file under the corresponding column headers. You then import this data into the `blkAllNames` database table. To expedite the import of the data from the file into the database table, use the column names exactly as they are used in the associated `blkAppNames` database table.

Guidelines

Use the following guidelines when preparing your data for bulk configuration:

- If a display name, reporting region, or operating unit is not defined, you must leave the related cell empty (that is, do not populate the cell with N/A or any other identifier). The reporting region or the operating unit must have a valid name – both cells cannot be empty. The whole content of the data row is rejected if any incomplete configuration is detected or there are names that cannot be resolved.
- Each application name (that is, the application name shown on the Application rollup page in the Administration module) must match the name contained in the `tmpImportCallType.PeripheralName`, `tmpImportInteractionQueue.PeripheralName`, or `tmpImportApp.PeripheralName` column of the Platform database.
- Each contact center name must match the name contained in the `CALL_CENTER.NAME` column of the Platform database.
- Each application group name must match the name contained in the `APPLICATION.NAME` column of the Platform database.
- Each reporting region name must match the name contained in the `REGION.NAME` column of the Platform database, where `TYPE='R'`.
- Each operating unit name must match the name contained in the `REGION.NAME` column of the Platform database, where `TYPE='O'`.
- If used, each contact group name must match the name contained in the `CONTACT_GROUP.NAME` column of the Platform database.
- Include only contact groups that will be mapped to applications; do not include contact groups that you do not want mapped to applications.

WA does not support interaction queues. Any contact groups specified and associated with interaction queues are ignored.

Application-to-Agent Group Relationships

Your spreadsheet or CSV file contains a list of application names, agent group names, and display names. If the related agent groups must be assigned to agent group contact centers (AGCC), you also specify the names of these AGCCs. If the specified agent group contact center does not exist, the tool creates it, but only if the related application is already mapped to a contact center or listed in the blkAllNames table. If no AGCC, contact group, or display name needs to be specified, leave the corresponding field(s) empty.

This structure is not used for application-to-contact group mapping. A contact group is mentioned in this structure only if you want the contact group to be assigned to an AGCC and the associated agent group.

Your file must contain five columns with headers and provides the following information:

- Application Name
- Agent Group Name
- Agent Group Contact Center Name
- Contact Group Name
- Contact Group Display Name

Add relevant data to the spreadsheet or file under the corresponding column headers. You then import this data into the blkAllAgntGr database table. To expedite the import of the data from the file into the database table, use the column names exactly as they are used in the associated blkAppAgntGr database table.

Guidelines

Each agent group name must match the name contained in the tmpImportSkill.EnterpriseName column of the Platform database.

| - | Loading Data from Spreadsheets into Temporary Database Structures =

Import content from the spreadsheets or files into the relevant columns of the corresponding database tables using the Oracle SQL Developer or the MS SQL import option. Follow the procedure for each table.

Importing Content into Tables (Oracle)

1. Open SQL Developer and register a connection to the Advisors Platform schema.
2. Navigate to the Advisors platform schema, then to each created table.
3. Right-click on a table and select the Import Data ... option from the menu.
4. Navigate to the relevant file and select it.
5. Follow the SqlDeveloper Import Data Wizard instructions; the wizard guides you through the import process.

Ensure that you verify the data for each step of the Data Import Wizard, in particular:

- Review the data on the Data Preview screen to ensure accuracy.
- Ensure you exclude any unrelated columns that might be present in the file. It is best if you remove unwanted columns from the file before you start the import, rather than excluding columns each time you run the import wizard.
- Ensure that you correctly map columns in the database table to columns in the file. Verify each and every column.
- Verify the parameters before import.

See the SQL Developer documentation if you have questions related to data import using SQL Developer.

Importing Content into Tables (MS SQL)

You must match each spreadsheet with a destination table. Ensure you choose the table that was created for bulk configuration and not the one suggested by the wizard.

1. Open Microsoft SQL Server Management Studio and register a connection to Advisors Platform database.
2. Navigate to the Advisors Platform database and launch the import tool for one of the created tables.
3. Following the import wizard instructions.
4. Import the data from each file that contains prepared configuration data.

With MS SQL Server, data can be loaded in one import session if you use Microsoft Excel and the data is consolidated into one spreadsheet with tabs representing the content of each table.

Ensure that you verify the data for each step of the Data Import Wizard, in particular:

- Review the data on the Data Preview screen to ensure accuracy.
- Ensure you exclude any unrelated columns that might be present in the file. It is best if you remove unwanted columns from the file before you start the import, rather than excluding columns each time you run the import wizard.
- Ensure that you correctly map columns in the database table to columns in the file. Verify each and every column.

See the MS SQL Server documentation if you have questions related to data import using Microsoft SQL Server Management Studio.

MSSQL Server Import is very sensitive to special characters which, if present in the files, can trigger import failure accompanied by a message that may seem completely unrelated and will not explain the actual reason. Make sure that the files are clean. Special characters are often invisible and to avoid import failure, you need to check the files for unnecessary empty trailing spaces, empty rows or formatting and remove them before you proceed with the import. While preparing the data, do not copy it from web pages or forms that may contain such characters.

| - | Bulk Configuration Validation and Logs =

The contact group bulk configuration procedure (spblkConfigCCadvWAIIntegrated) validates each record in the database blk structures. The procedure does not add to the configuration if any serious

misconfiguration is discovered in the blk tables. Instead, the procedure records a message in the blkAllLog table and exits. Always review the blkAllLog table content; note rows that contain an asterisk (*). The asterisks typically indicate problems with data in the tables. The number of asterisks normally indicates the number of found issues in the configuration for the related object. See *Prerequisites and Preparations* and *Data Preparation* for information about correct data preparation.

Examine the log to see if you encountered errors when performing the bulk configuration. If there are errors reported in the log, correct the data in the spreadsheets or files, and reload the content to the related tables and columns. You can also correct the data directly in the tables and then save the change for the future by exporting the new table content into the files. You can correct only some of the records leaving the rest intact. When you execute the bulk configuration procedure, the procedure applies changes to objects present in both the CCA and WA parts of bulk configuration tables.

Re-run the procedure to complete or correct the configuration using the updated data. Repeat the process as many times as necessary. The procedure does not reduce existing configuration. The procedure applies all modifications and additions that occurred in the blk tables after your previous execution of the procedure. Any deletion of data from the blk tables, however, is ignored.

The resulting configuration can be verified from the Advisor Administration module and on the dashboard.

Correct Configuration Validation in Advisors Administration Module

Execution of the spblkConfigCCAdvWAIIntegrated procedure results in the following configuration, which you can validate in the Advisors Administration module:

- Associates applications contained in the blkAllNames table with contact centers, application groups, reporting regions, and operating units contained in the associated columns. The applications for which all names are resolved (all objects with those names are found in the Platform database and their IDs can be located through associations and assignments) are added to the existing CCAdv configuration and included in the rollup. The procedure also updates display names based on the content in the columns of the table. If the AppDisplayName column in the table is blank for an application, the existing display name for that application, present in the CCAdv configuration, is removed (replaced with the blank name).
- Associates contact groups, where specified, with applications and assigns these contact groups to the contact center, application group, reporting region, and operating unit specified in the row with the contact group.
- Associates the contact group with the specified contact group display name. If the CgDisplayName column is blank, the existing display name of the contact group (present in WA configuration) is replaced with the blank name.
- Establishes relationships between applications and agent groups contained in the blkAllAgntGr table.
- Establishes relationships between contact groups and agent groups contained in the blkAllAgntGr table. Each contact group displays in a row with the relevant agent group based on the specified agent group contact center. The contact group inherits the properties of the application contained in the same row of the table as the contact group.
- Records the outcome in the blkAllLog table, which you can examine after the procedure exits.

[-] Exporting CCAdv/WA Configuration=

You can export the existing CCAdv/WA configuration into a set of temporary structures compatible

with CCAdv/WA bulk configuration. You can then export the structures into delimited files, edit them by adapting to the bulk configuration format and use those for CCAdv/WA configuration in another environment. You can also use the exported structures to compare the actual CCAdv/WA configuration to your expected configuration.

Run the blkCfgExp.sql script in your Oracle or MS SQL Server installation to export the data.

The script creates and populates or updates the following tables:

- blkExpAllNames
- blkExpAllAgntGr

All entries for which there is a problem contain an explanation of the issue in the Message column of each table.

CCAdv Bulk Configuration – Independent Mode

This section describes the bulk configuration of CCAdv objects; the bulk configuration tool configures CCAdv outside of the Advisors Administration module.

You can use the tool to rapidly configure WA based on the lists of objects you define and export from other systems and load into temporary structures in the Advisors Platform database. The bulk configuration tool retrieves the data from the temporary structures, validates it, and transforms it into CCAdv rollup configuration. This tool is designed for use in independent configuration mode. For information about the configuration modes and how to set the mode, see [Contact Center Advisor and Workforce Advisor Administrator User's Guide](#). You must select the configuration mode before you perform bulk configuration.

Database Structures, Scripts, and Procedures

An object creation script, `blkObjectsCre.sql`, is supplied as a temporary addition to the installation package in the `sql\oracle\bulkconfig\independent\ccadv-bulkload` folder. You must execute `blkObjectsCre.sql` as a script – not as a statement – if opened and executed from the SQL Developer SQL Worksheet. You must apply the `blkObjectsCre.sql` script to the Platform schema to create the following tables; the tables are required for CCAdv bulk configuration:

- `blkAppNames`
- `RepRegionName`
- `blkAppAgntGr`
- `blkAgntGrNames`
- `blkAppLog`

You must create all of the preceding tables, but the content is optional. Any or all tables can remain empty. Empty tables do not impact the configuration in any way.

Objects already present in CCAdv configuration, but absent from these tables, remain in the CCAdv configuration after you perform the bulk configuration procedure.

Stored Procedure for Bulk Configuration

You implement the bulk configuration by running a stored procedure, `spblkConfigCCAdvIndependent`, which is also created when you run the `blkObjectsCre.sql` script. You execute the procedure against the Platform schema after all base data is prepared in the tables created by running the `blkObjectsCre.sql` script.

Script to Remove Objects Used in Bulk Configuration Process

The `blkObjectsDrop.sql` script removes all objects used in the bulk configuration (such as the tables that the `blkObjectsCre.sql` script creates). You can execute this script whenever necessary. There is no negative impact because of the presence of these objects; they can be retained. The `blkObjectsDrop.sql` script does not remove any configuration. You must execute the `blkObjectsDrop.sql` script before you switch to another configuration mode and use bulk configuration tools for that mode.

Stored Procedure for Removing Configuration

You can quickly and completely remove all CCAdv applications, agent groups, and agent group contact centers configured in CCAdv inside or outside the bulk configuration tool. To remove CCAdv configuration, run the `spblkRemoveConfigCCAdv` stored procedure, which is created when you run the `blkObjectsCre.sql` script. Run the `spblkRemoveConfigCCAdv` stored procedure against the Platform schema.

Important

The procedure will remove all data left from previous configurations that may have a negative impact on the new configurations. It can be very useful when the configuration mode must be changed.

In order to be able to restore the configuration, you must have a reliable set of bulk configuration files or blk tables that you can use to re-load the configuration. Before you execute the procedure, make sure that such data exists.

You also can execute the bulk configuration removal procedure if you are comfortable with the current configuration loss and want to re-configure the applications from the beginning.

The configuration removal procedure does not remove the data from blk files. Those are always preserved unless the tables are dropped by running the `blkObjectsDrop.sql` script.

Prerequisites and Preparations

- The application server and XML Generator service must be up and successfully running until the required data (see the following two bullets) displays on the pages of the Advisors Administration module. To ensure that the import runs successfully, check the XML Generator log for import-related errors.
- Log in to the Advisors application; Advisors automatically imports all relevant aggregated objects (regions, operating units, contact centers, and application groups) from the Genesys Configuration Server.
- All relevant applications and agent groups have been automatically imported by XML Generator, and are available for configuration.
- Prior to bulk configuration, ensure that all relevant application groups, reporting regions, geographic regions, operating units, and network contact centers are configured. You configure these manually using Advisors administration module.

No existing configuration is removed when using the CCAdv bulk configuration tool. If any objects are already configured, or any application-to-agent group relationships are added manually, they are not

removed by the bulk configuration tool. The tool adds to the configuration or changes the mappings of the existing configured objects based on the data contained in the temporary structures.

If an AGCC does not already exist, one is created by the bulk configuration procedure under every network call center (NCC) where each application mapped to it (that is, to the NCC) is also mapped to an agent group and that agent group is mapped to an AGCC.

Genesys recommends that all aggregated objects participating in CCAdv configuration are activated in Advisors administration module prior to performing bulk configuration. Optionally, you can complete this step after bulk configuration. In either case, it is required to make the objects visible on the dashboard view.

Bulk Configuration of CCAdv in Independent Configuration Mode

The following procedure summarizes the steps to perform bulk configuration of CCAdv when you use the application in independent configuration mode. The information following this procedure provides additional information to assist you.

1. Start Advisors Application Server and XML Generator.

2. Watch the XML Generator and Geronimo logs.

The logs must be free of any import-related errors.

3. Allow the Advisors application to run for approximately 10 minutes.

4. Open the Administration module in the browser.

5. When the aggregated objects are available, configure all those that you plan to use in CCAdv rollups (see *Prerequisites and Preparations*).

6. Open each of the following pages and ensure that you can see objects among the available and/or configured object lists, as applicable:

- a. Application Configuration page
- b. Agent Group Configuration page
- c. Contact Group Configuration page

7. Connect to the Oracle instance as platform user.

8. Execute the blkObjectsCre.sql script.

You must execute blkObjectsCre.sql as a script – not as a statement – if opened and executed from the SQL Developer SQL Worksheet.

9. Populate the database tables with your contact group data.

- For information about preparing your data, see *Prerequisites and Preparations* and *Data Preparation for Application names, Application Display names, and Aggregated Object Names*.

- For information about importing the data from spreadsheets to the database, see *Loading Data from Spreadsheets into Temporary Database Structures*.

10. Execute the spblkConfigCCadvIndependent procedure:

Oracle:

```
DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkConfigCCadvIndependent"
(
M => M,
R => R
);
END;
```

MSSQL:

```
USE <name of Advisors platform database>
GO
```

```
DECLARE
    @r int,
    @m varchar(255)

EXEC    spblkConfigCCadvIndependent
        @r = @r OUTPUT,
        @m = @m OUTPUT

SELECT    @r as N'@r',
          @m as N'@m'

GO
```

11. Verify the log stored in the blkAppLog table.

For information about logs related to the bulk configuration, see *Bulk Configuration Validation and Logs*.

12. Correct the data, if necessary, and go back to Step 10.

If no correction is necessary, go to Step 13.

13. Examine all relevant configuration pages in the Advisors Administration module to verify the configuration.

14. Examine the CCAdv dashboard to verify the configuration.

15. Do one of the following:

- a. If you are satisfied with the resulting configuration, and you do not plan to use the WA independent

configuration tool, connect to the Oracle instance as platform user and execute the blkObjectsDrop.sql script to remove all temporary structures and bulk load procedures.

- b. If you are not satisfied with the resulting configuration, go to Step 12. Alternatively, if you see unpredictable results, and you have a reliable set of bulk configuration data loaded into blk tables, you can remove the whole CCAdv configuration by executing the CCAdv configuration removal procedure. After that you can reload the configuration as described in Step 10.

Oracle:

```
DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkRemoveConfigCCAdv"
(
M => M,
R => R
);
END;
```

MSSQL:

```
USE <name of Advisors platform database>
GO
```

```
DECLARE@m varchar(255),
        @r int
```

```
EXEC    spblkRemoveConfigCCAdv
        @m = @m OUTPUT,
        @r = @r OUTPUT
```

```
SELECT @m as N'@m',
        @r as N'@r'
```

```
GO
```

Data Preparation for Application names, Application Display names, and Aggregated Object Names

You can use spreadsheets or CSV files to collect the CCAdv configuration information into a simple file structure that can be loaded into a database table. Alternatively, you can omit the file preparation and load the data directly into the database table from the sources available through your relational database management system (RDBMS). If you use spreadsheets or CSV files to collect your CCAdv configuration data, use the following sections as guides.

Object Names

Your spreadsheet or CSV file contains the list of all the application names that need to be configured, as well as the corresponding application display names, contact center names, application group

names, reporting region, and operating unit names. Your file must contain six columns with headers (headers are mandatory), and provide the following information:

- Application Name
- Application Display Name
- Contact Center Name
- Application Group Name
- Reporting Region Name
- Operating Unit Name

Add relevant data to the spreadsheet or file under the corresponding column headers. You then import this data into the blkAppNames database table. To expedite the import of the data from the file into the database table, use the column names exactly as they are used in the blkAppNames database table.

Guidelines

Use the following guidelines when you create the spreadsheets to import information about object names to be used for CCAdv bulk configuration:

- If a display name, reporting region, or operating unit is not defined, you must leave the related cell empty (that is, do not populate the cell with N/A or any other identifier). Where used, the reporting region or the operating unit must have a valid name – both cells cannot be empty. The whole content of the data row is rejected if any incomplete configuration is detected or there are names that cannot be resolved (objects with those names are not found among the imported objects and, therefore, their IDs cannot be located through associations and assignments).
- Each application name (that is, the application name shown on the Application rollup page in the Administration module) must match the name contained in the tmpImportCallType.PeripheralName, tmpImportInteractionQueue.PeripheralName, or tmpImportApp.PeripheralName column of the Platform database.
- Each application group name must match the name contained in the APPLICATION.NAME column of the Platform database.
- Each reporting region name must match the name contained in the REGION.NAME column of the Platform database, where TYPE='R'.
- Each operating unit name must match the name contained in the REGION.NAME column of the Platform database, where TYPE='O'.

Applications and Agent Group Relationships

To configure application-to-agent group relationships, your spreadsheet or CSV file contains the list of application names, as well as the agent group names and AGCC names. If the related agent groups must also be assigned to agent group contact centers, the names of these contact centers are specified with the agent groups. If a specified AGCC does not exist, the bulk configuration tool creates it, but only if the related application is already mapped to a contact center (that is, it is listed in the blkAppNames structure). If no AGCC needs to be specified, leave the field empty. Your file must contain three columns:

- Application Name
-

- Agent Group Name
- Agent Group Contact Center Name

Add relevant data to the spreadsheet or file under the column headers. You then import this data into the blkAllAgntGr database table. To expedite the import of the data from the file into the database table, use the column names exactly as they are used in the blkAppAgntGr database table.

Guidelines

Use the following guidelines when you create the spreadsheets to import configuration information about application and agent group relationships:

- Each agent group name must match the name contained in the tmpImportSkill.EnterpriseName column of the Platform database.

You can prepare agent group descriptive names in a separate blkAgntGrNames file, if required. This table is shared between CCAdv and WA bulk configuration tools.

Loading Data from Spreadsheets into Temporary Database Structures

Import content from the spreadsheets or files into the relevant columns of the corresponding database tables using the Oracle SQL Developer or the MS SQL import option. Follow the procedure for each table.

Importing Content into Tables (Oracle)

1. Open SQL Developer and register a connection to the Advisors Platform schema.
2. Navigate to the Advisors platform schema, then to each created table.
3. Right-click on a table and select the Import Data ... option from the menu.
4. Navigate to the relevant file and select it.
5. Follow the SqlDeveloper Import Data Wizard instructions; the wizard guides you through the import process.

Ensure that you verify the data for each step of the Data Import Wizard, in particular:

- Review the data on the Data Preview screen to ensure accuracy.
- Ensure you exclude any unrelated columns that might be present in the file. It is best if you remove unwanted columns from the file before you start the import, rather than excluding columns each time you run the import wizard.
- Ensure that you correctly map columns in the database table to columns in the file. Verify each and every column.
- Verify the parameters before import.

See the SQL Developer documentation if you have questions related to data import using SQL

Developer.

Importing Content into Tables (MS SQL)

You must match each spreadsheet with a destination table. Ensure you choose the table that was the created for bulk configuration.

1. Open Microsoft SQL Server Management Studio and register a connection to Advisors Platform database
2. Navigate to the Advisors Platform database and launch the import tool for one of the created tables.
3. Following the import wizard instructions.
4. Import the data from each file that contains prepared configuration data.

With MS SQL Server, data can be loaded in one import session if you use Microsoft Excel and the data is consolidated into one spreadsheet with tabs representing the content of each table.

Ensure that you verify the data for each step of the Data Import Wizard, in particular:

- Review the data on the Data Preview screen to ensure accuracy.
- Ensure you exclude any unrelated columns that might be present in the file. It is best if you remove unwanted columns from the file before you start the import, rather than excluding columns each time you run the import wizard.
- Ensure that you correctly map columns in the database table to columns in the file. Verify each and every column.

See the MS SQL Server documentation if you have questions related to data import using Microsoft SQL Server Management Studio.

MSSQL Server Import is very sensitive to special characters which, if present in the files, can trigger import failure accompanied by a message that may seem completely unrelated and will not explain the actual reason. Make sure that the files are clean. Special characters are often invisible and to avoid import failure, you need to check the files for unnecessary empty trailing spaces, empty rows or formatting and remove them before you proceed with the import. While preparing the data, do not copy it from web pages or forms that may contain such characters.

Bulk Configuration Validation and Logs

The bulk configuration procedure (spblkConfigCCAdvIndependent) validates each record in the database blk structures. The procedure does not add any configuration if any data contained in the corresponding tables fails to pass validation or cannot be found (or created) in the database. Instead, the procedure records a message in the blkAppLog table and proceeds to the next record. See *Prerequisites and Preparations* and *Data Preparation for Application names, Application Display names, and Aggregated Object Names* for information about correct data preparation.

Examine the log to see if you encountered errors when performing the bulk configuration. If there are

errors reported in the log, correct the data in the spreadsheets or files, and reload the content to the related tables and columns. You can also correct the data directly in the tables.

Re-run the procedure to complete or correct the configuration using the updated data. Repeat the process as many times as necessary. The procedure does not reduce the existing configuration. The procedure applies all modifications and additions that occurred in the blk tables after your previous execution of the procedure. Any deletion of data, however, is ignored.

The resulting configuration can be verified from the Advisor Administration module and on the dashboard.

Exporting CCAdv Configuration

You can export the existing CCAdv configuration into a set of temporary structures compatible with CCAdv bulk configuration. You can then export the structures into delimited files, edit them by adapting to the bulk configuration format, and use those for CCAdv configuration in the current or another environment. You can also use the exported structures to compare the actual CCAdv configuration to your expected configuration. Run the blkCfgExp.sql script in your Oracle or MS SQL Server installation to export the data. The script creates and populates or updates the following tables:

- blkExpAppNames
- blkExpAppAgntGr
- blkExpAgntGrNames

All entries for which there is a problem contain an explanation of the issue in the Message column of each table.

WA Bulk Configuration – Independent Mode

This page describes the bulk configuration of WA contact groups; the bulk configuration tool configures WA rollups outside of the Advisors Administration module.

You can use the tool to rapidly configure WA based on the lists of objects you define and export from other systems and load into temporary structures in the Advisors Platform database. The bulk configuration tool retrieves the data from the temporary structures, validates it, and transforms it into WA rollup configuration. This tool is designed for use in independent configuration mode. For information about the configuration modes and how to set the mode, see [Contact Center Advisor and Workforce Advisor Administrator User's Guide](#). You must select the configuration mode before you perform bulk configuration.

If the independent configuration mode is set, then:

- Agent group-to-application relationships created in CCAdv are not propagated to the configured contact groups mapped to these applications. Instead, the direct network contact center (NCC) contact group-to-agent group mappings are used.
- Applications mapped to contact groups inherit all aggregation properties from those contact groups that are mapped to them. All properties that applications acquire in CCAdv configuration are ignored.
- Agent groups mapped to agent group contact centers (AGCC) inherit all the properties from the contact groups that are mapped to those AGCC. Each contact group can be mapped to only one contact center.

You can map contact groups, which are not mapped to AGCCs, to applications. You can map each such contact group (a contact group mapped to an application) directly to an agent group. In the independent configuration mode, mapping a contact group to an application does not trigger the automatic mapping of all the agent groups already assigned to that application.

You can map contact groups, which are mapped to AGCCs, only to agent groups. Each contact group configured under an agent group contact center has a parent in the form of a contact group mapped to the related network contact center. A combination of participating aggregated objects is derived from the specified parent, and an agent group contact center is automatically created under the derived network contact center, if one does not already exist.

All contact group-related aggregated objects that are derived from the parent (AGCCs, application groups, regions, and operating units) are automatically assigned to the children contact groups. All agent groups associated with the contact group that is mapped to an AGCC are mapped to this same AGCC automatically. Initially, these agent groups are excluded from CCAdv rollup by the bulk configuration tool, unless the agent group is already assigned to a contact center and included in CCAdv.

Database Structures, Scripts, and Procedures

An object creation script, `blkObjectsCre.sql`, is supplied as a temporary addition to the installation package. You must execute `blkObjectsCre.sql` as a script – not as a statement – if opened and executed from the SQL Developer SQL Worksheet. You must apply the `blkObjectsCre.sql` object creation script to the Platform schema to create the following tables, which are required for the

contact group bulk configuration:

- blkCgNames
- blkAgCgNames
- blkCgApp
- blkCgAgntGr
- blkAgntGrNames
- blkCgLog

You must create all of the preceding tables, but the content is optional. Any or all tables can remain empty. Empty tables do not impact the configuration in any way.

Objects already present in WA configuration, but absent from these tables, remain in the WA configuration after you perform the bulk configuration procedure.

Stored Procedure for Bulk Configuration

You implement the bulk configuration by running a stored procedure, `spblkConfigWAIndependent`, which is also created when you run the `blkObjectsCre.sql` script. You execute the procedure against the Platform schema after all base data is prepared in the tables created by running the `blkObjectsCre.sql` script.

Script to Remove Objects Used in Bulk Configuration Process

The `blkObjectsDrop.sql` script removes all objects used in the bulk configuration (such as the tables that the `blkObjectsCre.sql` script creates). You can execute this script whenever necessary. There is no negative impact because of the presence of these objects; they can be retained. The `blkObjectsDrop.sql` script does not remove any configuration.

Stored Procedure for Removing Configuration

You can quickly and completely remove all configured WA contact groups, their relationships to applications and agent groups, and agent group contact centers created inside or outside the bulk configuration tool. To remove the configuration, run the `spblkRemoveConfigWA` stored procedure, which is created when you run the `blkObjectsCre.sql` script. Run the `spblkRemoveConfigWA` stored procedure against the Platform schema.

Important

The procedure will remove all data left from previous configurations that may have a negative impact on the new configurations. It can be very useful before the configuration mode must be changed.

In order to be able to restore the configuration, you must have a reliable set of bulk configuration files or blk tables that you can use to re-load the configuration. Before you execute the configuration removal procedures, make sure that such data exists.

You also can execute the bulk configuration removal procedures if you are comfortable with the current configuration loss and want to re-configure the applications from the beginning.

The configuration removal procedure does not remove the data from blk files. Those are always

preserved unless the tables are dropped by running the blkObjectsDrop.sql script.

Prerequisites and Preparations

- The application server and XML Generator service must be up and successfully running until the required data (see the following three bullets) displays on the pages of the Advisors Administration module. To ensure that the import runs successfully, check the XML Generator log for import-related errors.
- Log in to the Advisors application; Advisors automatically imports all relevant aggregated objects (regions, operating units, contact centers, and application groups) from the Genesys Configuration Server.
- All relevant applications and agent groups have been automatically imported by XML Generator, and are available for configuration.
- All relevant contact groups have been automatically imported by the WA server from the WFM system(s) specified during Advisors installation, and are available for configuration.
- Prior to bulk configuration, ensure that all relevant application groups, reporting regions, geographic regions, operating units, and network contact centers are configured. You configure these manually using Advisors administration module.

No existing configuration is removed when using the WA bulk configuration tool. If any objects are already configured, or any applications or agent groups are added manually using the Administration module, they are not removed by the bulk configuration tool. The tool adds to the configuration – or changes the mappings of the existing configured objects – based on the data contained in the temporary structures.

If an AGCC does not already exist, one is created by the bulk configuration procedure under every network call center where contact groups have children (in the form of contact groups mapped to agent groups).

Genesys recommends that all aggregated objects participating in WA configuration are activated in Advisors administration module prior to performing bulk configuration. Optionally, you can complete this step after bulk configuration. In either case, it is required to make the objects visible on the dashboard view.

Bulk Configuration of Contact Groups in WA independent Configuration Mode

The following procedure summarizes the steps to perform contact group bulk configuration when you use WA in independent configuration mode. The information following this procedure provides additional information to assist you.

1. Start Advisors Application Server and XML Generator.
2. Watch the XML Generator and Geronimo logs.

The logs must be free of any import-related errors.

3. Allow the Advisors application to run for approximately 10 minutes.

4. Open the Administration module in the browser.

5. When the aggregated objects are available, configure all those that you plan to use in WA rollups (see *Prerequisites and Preparations*).

6. Open each of the following pages and ensure that you can see objects among the available and/or configured object lists, as applicable:

- a. Application Configuration page
- b. Agent Group Configuration page
- c. Contact Group Configuration page

7. Connect to the Oracle instance as platform user.

8. Execute the blkObjectsCre.sql script in the WA bulk configuration section.

You must execute blkObjectsCre.sql as a script – not as a statement – if opened and executed from the SQL Developer SQL Worksheet.

9. Populate the database tables with your contact group configuration data.

- For information about preparing your contact group data, see *Data Preparation for Contact Group Names, Contact Group Display Names and Aggregated Object Names*.
- For information about importing the contact group data from spreadsheets to the database, see *Loading Data from Spreadsheets into Temporary Database Structures*.

10. Execute the spblkConfigWAIIndependentprocedure.

Oracle:

```
DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkConfigWAIIndependent"(
M => M,
R => R
);
END;
```

MSSQL:

```
USE <name of Advisors database>
GO
DECLARE @return_value int,
        @r int,
        @m varchar(255)
```

```
EXEC spblkConfigWAIIndependent
@r = @r OUTPUT,
@m = @m OUTPUT
SELECT @r as N'@r',
@m as N'@m'
GO
```

11. Verify the log stored in the blkCgLog table.

For information about logs related to the bulk configuration, see *Bulk Configuration Validation and Logs*.

12. Correct the data, if necessary, and go back to Step 8.

If no correction is necessary, go to Step 13.

13. Examine the Contact Group Configuration page in the Advisors Administration module to verify the configuration.

14. Examine the WA dashboard to verify the configuration.

15. Do one of the following:

- a. If you are satisfied with the resulting configuration, connect to the Oracle instance as platform user and execute the blkObjectsDrop.sql script to remove all temporary structures and bulk load procedures.
- b. If you are not satisfied with the resulting configuration, go to Step 12. Alternatively, if you see unpredictable results, and you have a reliable set of bulk configuration data loaded into blk tables, you can remove the whole WA configuration by executing the WA configuration removal procedure. After that you can reload the configuration as described in Step 10. You can remove the whole configuration by executing the spblkRemoveConfigWA procedure. Oracle:

```
DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkRemoveConfigWA"
(
M => M,
R => R
);
END;
```

MSSQL:

```
USE <name of Advisors platform database>
GO

DECLARE @m varchar(255),
        @r int

EXEC      spblkRemoveConfigWA
        @m = @m OUTPUT,
        @r = @r OUTPUT
```

```
SELECT  @m as N'@m',  
        @r as N'@r'  
  
GO
```

Data Preparation for Contact Group Names, Contact Group Display Names and Aggregated Object Names

You can use spreadsheets or CSV files to collect contact group configuration information into a simple file structure that can be loaded into a database table. Alternatively, you can omit the file preparation and load the data directly into the database table from the sources available through your relational database management system (RDBMS). If you use spreadsheets or CSV files to collect your contact group data, use the following sections as guides.

Contact Groups mapped to Objects other than AGCC

Your spreadsheet or CSV file contains the list of all contact group names that must be configured, together with the corresponding contact group display names, network contact center names, application group names, reporting region, and operating unit names. Your file must contain six columns with headers (headers are mandatory), and provide the following information:

- Contact Group Name
- Contact Group Display Name
- Contact Center Name
- Application Group Name
- Reporting Region Name
- Operating Unit Name

Add relevant data to the spreadsheet or file under the corresponding column headers. You then import this data into the blkCgNames database table. To expedite the import of the data from the file into the database table, use the column names exactly as they are used in the blkCgNames database table.

Guidelines

Use the following guidelines when you create the spreadsheets to import configuration information about contact groups mapped to objects other than AGCC:

- If a display name, reporting region, or operating unit is not defined, you must leave the related cell empty (that is, do not populate the cell with N/A or any other identifier). Where used, the reporting region or the operating unit must have a valid name – both cells cannot be empty for any given contact

group. The whole content of the data row is rejected if any incomplete configuration is detected or there are names that cannot be resolved.

- Each contact group name must match the name contained in the CONTACT_GROUP.NAME column of the Platform database. Do not put contact groups that need to be mapped to agent group contact centers in the spreadsheet (or table).
- Each contact center name must match the name contained in the CALL_CENTER.NAME column of the Platform database.
- Each application group name must match the name contained in the APPLICATION.NAME column of the Platform database.
- Each reporting region name must match the name contained in the REGION.NAME column of the Platform database, where TYPE='R'.
- Each operating unit name must match the name contained in the REGION.NAME column of the Platform database, where TYPE='O'.

Contact Groups mapped to AGCC

The mapping of contact groups-mapped-to-AGCC to aggregated objects is derived from their parent contact groups, which are already mapped to the relevant network contact centers. Your spreadsheet or CSV file for this information contains the list of all contact group names that must be mapped to agent group contact centers, and further to agent groups. Your file must contain four columns:

- Contact Group Name
- Name of AGCC to which contact group is related
- Parent Contact Group Name
- Contact Group Display Name

The parent contact group name is the name of the contact group mapped to the associated network contact center.

Add relevant data to the spreadsheet or file under the column headers. You then import this data into the blkAgCgNames database table. To expedite the import of the data from the file into the database table, use the column names exactly as they are used in the blkAgCgNames database table.

If you supply data in a file related to contact groups mapped to AGCC, then the bulk configuration tool creates a WA configuration with participating agent group contact centers. If the blkAgCgNames database table remains empty, no agent group contact centers are added to WA configuration. To be included in WA configuration, the child contact group must be specified in a pair with a parent contact group that is already mapped to a network contact center and other aggregated objects. That is, the parent contact group exists among the assigned contact groups in the current WA configuration, or it exists in the blkCgNames database table.

Guidelines

Use the following guidelines when you create the spreadsheets to import configuration information about contact groups mapped to AGCC:

- If a display name is not defined, you must leave the related cell empty (that is, do not populate the cell with N/A or any other identifier).

- Each contact group name and parent contact group name must match the name contained in the CONTACT_GROUP.NAME column of the Platform DB.

Contact Groups and Related Applications

The word *application*, as used with Advisors, refers to Advisors objects that originate from the following:

- Genesys ACD and virtual queues
- Genesys interaction queues
- CISCO call types
- CISCO services

Relationships between contact groups and applications is a necessary part of WA configuration. The functionality of the bulk configuration tool assumes that only contact groups associated with anything other than agent group contact centers can be associated also with applications. Your spreadsheet or CSV file for this information contains two columns:

- Contact Group Name
- Application Name

Add relevant data to the spreadsheet or file under the corresponding column headers. You then import this data into the blkCgApp database table. To expedite the import of the data from the file into the database table, use the column names exactly as they are used in the blkCgApp database table.

Guidelines

Use the following guidelines when you create the spreadsheets to import configuration information about contact groups and associated applications:

- Each contact group name must match the name contained in the CONTACT_GROUP.NAME column of the Platform DB. A contact group will be mapped to the specified application only if this contact group is already mapped to something other than an agent group contact center. That is, the contact group exists among assigned contact groups or is mentioned in the blkAgCgNames DB table.
- Each application name must match the name contained in the tmplImportCallType.PeripheralName or tmplImportApp.PeripheralName column of the Platform database.

Contact Groups and Related Agent Groups

You can associate contact groups mapped to network contact centers with agent groups.

Contact groups related to AGCC can be mapped only to agent groups that are mapped to AGCC and identified as agent groups to include in WA.

Your spreadsheet or CSV file for this information contains three columns:

- Contact Group Name
 - Agent Group Name
-

- AGCC Name

Add relevant data to the spreadsheet or file under the corresponding column headers. You then import this data into the blkCgAgntGr database table. To expedite the import of the data from the file into the database table, use the column names exactly as they are used in the blkCgAgntGr database table.

Guidelines

- Each contact group name must match the name contained in the CONTACT_GROUP.NAME column of the Platform database.
- Each agent group name must match the name contained in the tmpImportSkill.EnterpriseName column of the Platform database.
- If necessary, agent group descriptive (display) names can be prepared in a separate file blkAgntGrNames. If the blkAgntGrNames table is populated, the bulk configuration tool applies the agent group descriptive names. The following table shows an example of a blkAgntGrNames file.

Example of content in an blkAgntGrNames file

AGNTGRNAME	AGNTGRDISPLAYNAME
V_TH0_PK_TR_EntertainIP_Generalist_KristallRetention_100	KristallRetention_100_cca
[Tenant1] V_IDR_PK_CF_Kundenbindung_120	Kundenbindung_120

Loading Data from Spreadsheets into Temporary Database Structures

Import content from the spreadsheets or files into the relevant columns of the corresponding database tables using the Oracle SQL Developer import option (Import Data ...). Follow the procedure below.

Importing Content into Tables

1. Open SQL Developer and register a connection to the Advisors Platform schema.
2. Navigate to the Advisors platform schema, then to each created table.
3. Right-click on a table and select the Import Data ... option from the menu.
4. Navigate to the relevant file and select it.
5. Follow the SqlDeveloper Import Data Wizard instructions; the wizard guides you through the import process.

Ensure that you verify the data for each step of the Data Import Wizard, in particular:

- Review the data on the Data Preview screen to ensure accuracy.
- Ensure that you correctly map columns in the database table to columns in the file. Verify each and every column.

- Verify the parameters before import.

See the SQL Developer documentation if you have questions related to the import of data.

Bulk Configuration Validation and Logs

The contact group bulk configuration procedure (`spblkInsertIntoCg`) validates each record in the database blk structures. The procedure does not add a contact group or a relationship to the WA configuration if any data contained in the corresponding tables fails to pass validation or cannot be found (or created) in the database. Instead, the procedure records a message in the `blkCgLog` table and proceeds to the next record. See *Prerequisites and Preparations* and *Data Preparation for Contact Group Names, Contact Group Display Names and Aggregated Object Names* for information about correct data preparation.

Examine the log to see if you encountered errors when performing the bulk configuration. If there are errors reported in the log, correct the data in the spreadsheets or files, and reload the content to the related tables and columns. You can also correct the data directly in the tables. You can correct only some of the records leaving the rest intact. When you execute the bulk configuration procedure, the procedure applies changes to objects present in WA configuration and in the bulk configuration tables.

Re-run the procedure to complete or correct the configuration using the updated data. Repeat the process as many times as necessary. The procedure does not remove the mapping of objects already present in WA configuration, but not present in the `blkCgNames` table, or otherwise damage existing configuration. The procedure applies all modifications and additions that occurred in the blk tables after your previous execution of the procedure. Any deletion of data, however, is ignored.

The resulting configuration can be verified from the Advisor Administration module and on the dashboard.

Correct Configuration Validation in Advisors Administration Module

Execution of the `spblkConfigWAIndependent` procedure results in the following configuration, which you can validate in the Advisors Administration module:

- Associates contact groups contained in the `blkCgNames` table with contact centers (excluding agent group contact centers), application groups, reporting regions, and operating units contained in the related columns. The contact groups for which all the names are resolved (all objects whose names are found in the Platform database) are added to the existing WA configuration and included in the rollup. The procedure also updates display names based on the content in the related column. For example, if the `CGDISPLAYNAME` column is blank, the existing display name of the contact group, present in the WA configuration, is replaced with the blank name.
- Associates contact groups contained in the `blkAgCgNames` table with parent contact groups (contact groups associated with network call centers).
- Creates agent group contact centers associated with the derived network contact centers, if the AGCC are not already present.
- Associates contact groups contained in the `blkAgCgNames` table with agent group contact centers, derived application groups, reporting regions, and operating units. The procedure also includes these contact groups in the rollup and assigns contact group display names. If the `CGDISPLAYNAME` column is blank, the existing display name of the contact group, present in the WA configuration, is replaced with

the blank name.

- Establishes relationships between contact groups and agent groups contained in the blkCgAgntGr table. The table can contain contact groups mapped to contact centers of any type. Each contact group mapped to an agent group contact center is mapped to this agent group contact center, to the contact group related to this agent group contact center, and is indirectly mapped to the parent contact group that is mapped to a network contact center. Each contact group mapped to something other than an agent group contact center is mapped to the specified agent groups directly.
- Assigns descriptive names to agent groups if the blkAgntGrNames table is populated.
- Records the outcome in the blkCgLog table, which you can examine after the procedure exits.

Exporting WA Configuration

You can export the existing WA configuration into a set of temporary structures compatible with WA bulk configuration. You can then export the structures into delimited files, edit them by adapting to the bulk configuration format and use those for WA configuration in the current or another environment. You can also use the exported structures to compare the actual WA configuration to your expected configuration. Run the blkCfgExp.sql script in your Oracle or MS SQL Server installation to export the data. The script creates and populates or updates the following tables:

- blkExpAgntGrNames
- blkExpCgNames
- blkExpAgccCgNames
- blkExpAgCgNames
- blkExpCgApp
- blkExpCgAgntGr

All entries for which there is a problem contain an explanation of the issue in the Message column of each table.

FA and AA

This section contains information and procedures to help you change configuration for Frontline Advisor and Agent Advisor after these modules are deployed.

Verify Server Connections

Use the information on this page to help you check that all connections are working correctly for Frontline Advisor.

Verify 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.

Verify Apache Routing

Use the following procedure to check that Apache routing is working. If configured correctly, the Login page will display.

1. Use the Firefox browser to connect directly to the Apache server. Use a URL that contains the host or IP address (and, optionally, the port if not on port 80) of the Apache server.
2. Log in.
3. Check the site.

Change 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. See the [Frontline Advisor Administration User's Guide](#) for more information.

Configure the Reason Code Statistic Key

NEW In Advisors release 8.1.5, you ran an update SQL script to configure the reason code statistic key. In release 8.5.0, use the Metric Manager to configure the reason code key. See [Contact Center Advisor and Workforce Advisor Administrator User's Guide](#) for information about Metric Manager and how to configure the reason code statistic key.

Enabling and Editing Filtered Metrics

Frontline Advisor includes performance metrics for which you must configure a filter to display the metrics for selection in the Column Chooser. For information about which metrics are enabled and which require filters when you install Frontline Advisor, see [Performance Management Advisors Metrics Reference Guide](#).

The enabled filtered metrics are for use with the Advisors Genesys Adapter only. The Advisors Cisco Adapter cannot provide data for the filtered metrics.

Filters are for metrics of the following types:

- ACD interactions
- Non-ACD interactions
- Not Ready Time, Filter x, where x=1, 2, ..., 9

If you do not configure the filters, Frontline Advisor does not request statistics for these metrics from the Advisors Genesys Adapter and does not display them as options in the dashboard Column Chooser. If you configure one or more filters, the associated source metrics are enabled, as well as the team-level metrics that are dependent on the filtered source metrics for their aggregation.

There is a stored procedure, `FA_Configured_Filtered_Metrics`, in the Frontline Advisor database after you upgrade to Advisors release 8.1.4 or later. You can use this procedure to enable the filtered metrics. Specify one or more filter names depending on the filters (and associated metrics) you want to activate. After you configure a filter name, the procedure creates entries in the `FA_Metrics`, `FA_Thresholds`, and `FA_Threshold_Patterns` tables. The filter names you specify display only in the tables. After you enable the filters, the associated metrics behave like other performance metrics. To rename a filter, run the procedure again. The existing metric and threshold are updated.

To edit the name of a filtered metric, at least one filtered metric must be enabled.

<tabber>

Enabling filtered metrics for Frontline Advisor=

1. Open the `FA_Configured_Filtered_Metrics` stored procedure in the Frontline Advisor database.

2. Enter a name (value) for any filter that you want to enable.

Enabling the filter enables all metrics associated with that filter, both source and team-level aggregated metrics that are dependent on the enabled source metrics for calculations.

3. Ensure a null value is configured for filters (and associated metrics) that you want to suppress.

4. Click OK.

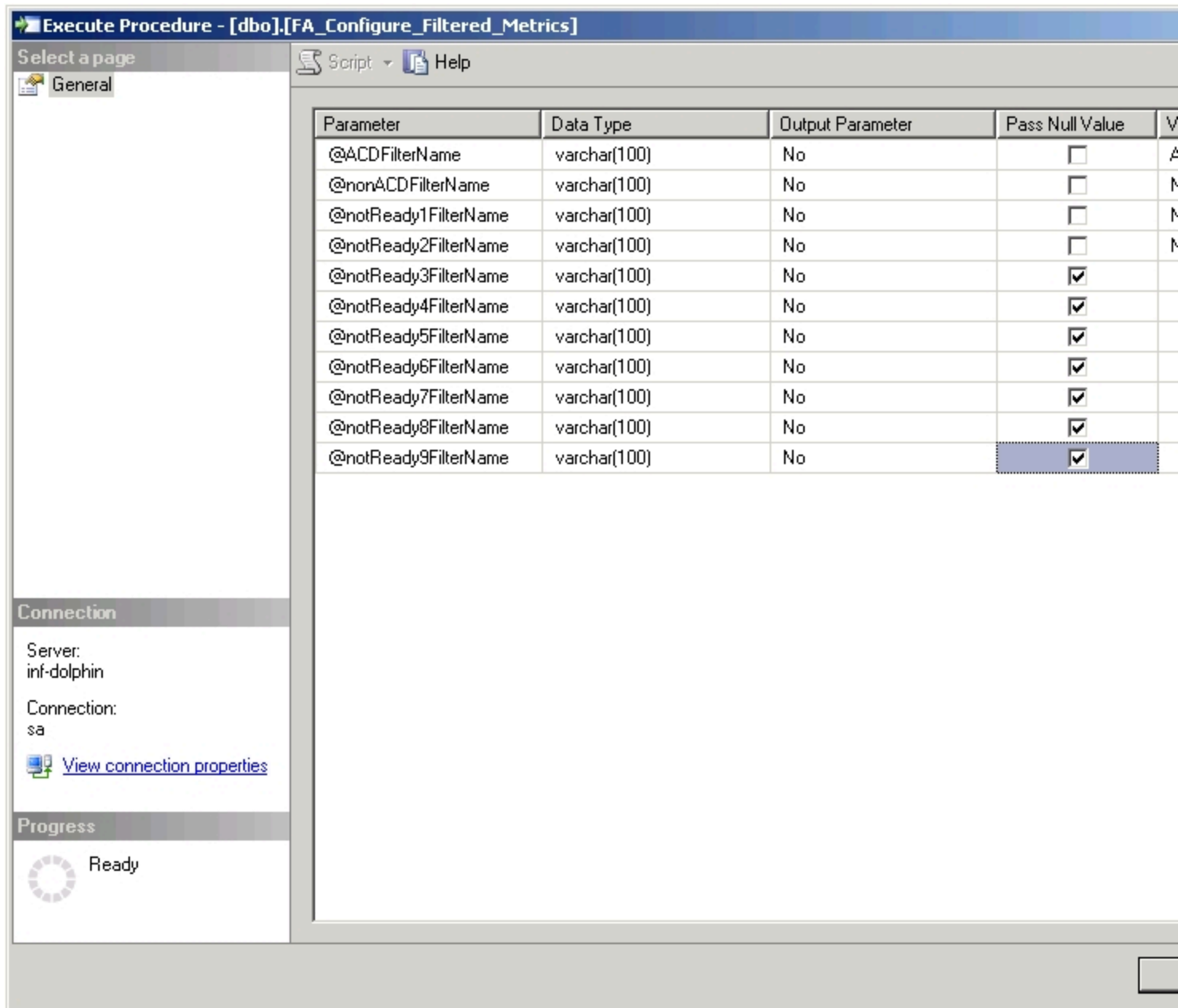
Next Steps

1. After the metrics are enabled, they must be imported into the Configuration Server using the Advisors

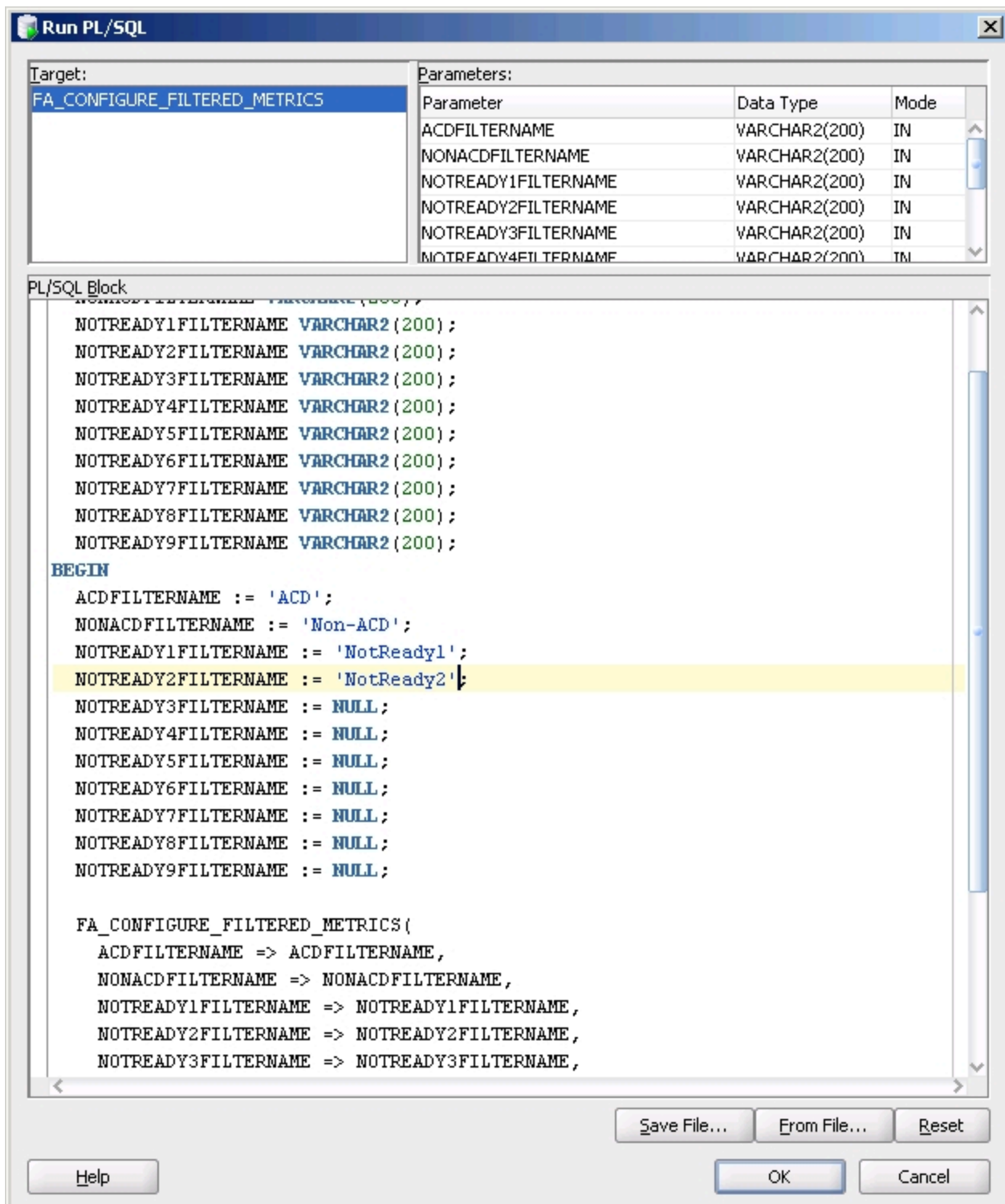
Object Migration Wizard (select Frontline Advisor Metrics when prompted for the migration path). For more information, see [Object Migration Utility](#). Running the Advisors Object Migration Wizard creates corresponding business attribute values for the enabled metrics. As with other FA metrics, you must grant permissions to read these values for allowed supervisors.

2. You must restart the Frontline Advisor server for the new metric information to load and be available in the Column Chooser.

The following Figures show examples of configuring filter names to enable metrics. A null value is used for filters for which you do not configure a name. Metrics associated with the null value filters are suppressed in the Column Chooser (that is, those metrics are unavailable for use on the dashboard and no thresholds are available for those metrics).



Configuring the filtered metrics with an MS SQL Server database



Configuring the filtered metrics with an Oracle database

-| Editing the name of a filtered metric=

-
1. Stop Frontline Advisor if it is running.
 2. Open the FA_Configured_Filtered_Metrics stored procedure in the Frontline Advisor database.
 3. Update the existing name (value) for a filtered metric.

You can edit the name of any previously-enabled filtered metric. Deleting the name and entering a null value does not disable the filtered metric – you cannot use the stored procedure to disable filtered metrics.

4. Click OK.

Features Overview

The Features Overview section contains descriptions of the Performance Management Advisors features and functionality. Use the information in this section to help you understand how Advisors work.

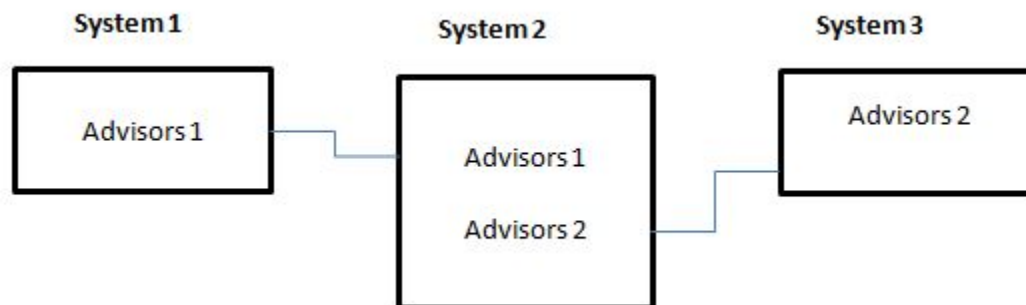
Discontinuation of the Advisors Browser

NEW Starting in release 8.5.0, there is no longer a standalone Advisors browser. Advisors modules run in a standard, commercially-available browser. See the [Genesys Supported Operating Environment Reference Guide](#) for information about supported browsers in which you can run the Advisors modules. You can find additional information about logging in to the 8.5 Advisors interface in the [Frontline Advisor Administration User's Guide](#) and the [Contact Center Advisor and Workforce Advisor Administrator User's Guide](#).

You must enter the Advisors URL provided by your system administrator in the browser address bar to open the Advisors login page.

Multiple Advisors Deployments on One System

NEW Starting in release 8.5.0, you can deploy more than one distinct Advisors deployments on one system (see the Figure – Multiple Advisors Deployments on one System). Each Advisors deployment has its own independent configuration, and its own databases.



Multiple Advisors Deployments on one System

To manage this:

- There are two port numbers that Advisors modules use to communicate; these are stored in properties files after installation:
 - `ActiveMQ.properties` governs aspects of Java Message Service (JMS) communication.
 - `Caching.properties` defines the port used by the distributed caching facility.
- The Platform installer accepts and sets values for configurable ports of Geronimo. The properties of the Geronimo configurable ports are defined in `geronimo-tomcat6-minimal-2.2.1\var\config\config-substitutions.properties`.

If there are no port number defined, or if they are not valid number, then Geronimo will not start.

The Advisors installer supplies default values for these ports. It saves the values you choose, default or different, in the properties file created by the installation. You can change these values for a second deployment of Advisors, and preserve the values in the `ant.install.properties` file to be used when re-installing.

The default value that you see in the Platform installer for the `activeMQ.port` is 61616.

The default value that you see in the Platform installer for the `distributed.caching.port` is 11211.

The default values that you see in the Platform installer for the Geronimo configurable ports are the following:

- `HTTPPort=8080`
- `NamingPort=1099`

- JMXPort=9999
- HTTPSPort=8443
- AJPPort=8009

Example

The nodes of an Advisors deployment (Advisors 1) use a set of values for the ports on every system on which the nodes are installed. For example:

- ActiveMQ.port 61616
- distributed.caching.port 11211
- HTTPPort=8080
- NamingPort=1099
- JMXPort=9999
- HTTPSPort=8443
- AJPPort=8009
- ftpService.port=6021

The nodes of a second Advisors deployment (Advisors 2) must use different values for the ports. For example:

- ActiveMQ.port 61617
- distributed.caching.port 11212
- HTTPPort=8081
- NamingPort=1100
- JMXPort=10000
- HTTPSPort=8444
- AJPPort=8010
- ftpService.port=6022

Workforce Advisor contains an FTP server that accepts data directly from the IEX TotalView data source. The FTP server listens on port 6021, by default. This is the ftpService.port number used in the example. You specify this port number during installation of Contact Center Advisor/Workforce Advisor. Advisors stores the FTP service port number in the conf/WorkforceAdvisor.properties file.

The following Table shows the configuration file associated with each Platform installer screen on which you enter port-related values. The Table also shows the port properties that are saved, and which you can re-configure post-installation.

Platform Installer Screen	Corresponding Configuration File	Port Property
Application Server Configuration	geronimo-	HTTPPort, NamingPort, JMXPort,

Platform Installer Screen	Corresponding Configuration File	Port Property
	tomcat6-minimal-2.2.1\var\config\config-substitutions.properties	HTTPSPort, AJPPort
Cluster Node Configuration	conf/ActiveMQ.properties	ActiveMQ.port
Cache Configuration	conf/Caching.properties	distributed.caching.port
Workforce Advisor Server - IEX TotalView	conf/WorkforceUtilization.properties	ftpService.port

Recommendations for Configuration

Genesys recommends the following configuration for multiple deployments on one system:

- Separate the two Advisors deployments by tenant in the Genesys Configuration Server. If you cannot do this for any reason, then separate the object permissions for the respective connection users (that is, the Advisors user for each of the nodes) in the Configuration Server so objects are not used in both nodes.
- Use two separate Object Configuration users; one for each deployment.
- Deploy two separate Apache instances. Ensure the Apache configuration file (`httpd.conf`) for the Advisors Platform node for which you entered port numbers (that is, the node that does not use the default port numbers) includes the same HTTP and AJP ports as specified in the Platform installer. For example, if you specified AJP port 8019 and HTTP port 8015 for your second Platform instance, then the Apache configuration file must use those same port numbers for AJP and HTTP proxy passes in the ProxyPass sections.

Advisors Platform and the Backup Configuration Server

NEW Starting in release 8.5.0, you can configure a connection from the Advisors Platform server to a backup Configuration Server in addition to the primary Configuration Server connection. Connection to the backup Configuration Server is optional.

Backup Configuration Server Properties

The following backup Configuration Server properties are available in the `<PLATFORM_INSTALL>/conf/GenesysConfig.properties` file.

- `genesys.configServer.backup.name`
- `genesys.configServer.backup.host`
- `genesys.configServer.backup.port`

If you configure a connection to the backup Configuration Server during installation, the information you enter is stored in the preceding properties.

You can modify the backup Configuration Server properties as needed to enable or disable backup Configuration Server support. To disable the connection to the backup Configuration Server post-installation, remove the backup Configuration Server name from the `genesys.configServer.backup.name` property. Restart Advisors Platform after you update the properties file.

How it Works

The backup Configuration Server must be set up as a *warm standby* to the primary Configuration Server. When the Advisors Platform server loses connection to the primary Configuration Server, connection to the backup Configuration Server happens automatically, including subscription to the same notifications from the backup Configuration Server that were received from the primary Configuration Server.

When the primary Configuration Server comes back online, it becomes the backup server and the former backup Configuration Server continues as the primary Configuration Server. Advisors supports subsequent switchovers between the primary and backup Configuration Servers.

The Platform log file records:

- a lost connection to either the primary or the backup Configuration Server
- re-connection to a Configuration Server

Data Manager

Data Manager feature provides the following functionality:

- Support for multiple Genesys and Cisco Adapters.
- Load balancing across multiple adapters using the same data source in a single Genesys environment.
- Management of the flow of statistics from Advisors Genesys Adapters (AGA) to both Frontline Advisor (FA) and Contact Center Advisor/Workforce Advisor (CCAdv/WA).
- Maintenance of the authoritative configuration data. Data Manager monitors Adapters to ensure that the issued statistics conform to its configuration.
- Use of statistics template definitions to determine the statistics requests that need to be sent to the Genesys Adapters for each Advisors module (such as CCAdv or FA).
- Use of a handshake protocol to establish connection with all adapters.

Data Migration

In Advisors release 8.1.5, source metric definitions and statistics templates stored in the Adapter database had to be migrated to the corresponding platform tables. The migration included any custom metrics you use in your enterprise and had to be done for all Advisors modules that use Genesys Adapter.

- The source metrics that migrated to the platform tables were for the CCAdv, WA, and FA modules that require Genesys data sources.
- The statistics templates that migrated to the platform tables were only for the CCAdv and WA modules. Because the FA statistics templates are of a transient nature, there was no need to migrate them and the migration tool ignored them.

For more information, see the [Genesys 8.1 Performance Management Advisors Deployment Guide](#).

Installation and Configuration

During the installation of any Adapter, the installer optionally prompts for:

- The connection details for the Platform database.
- A unique name for the Adapter and the source environment (the source environment is not prompted for in a Genesys environment).

This information, along with the Adapter's host name, port and type (GENESYS or

CISCO) is written to the Platform database. Data Manager uses this configuration information to establish connections to all installed Adapters.

The Adapter type is always set to either GENESYS or CISCO. You must register all Genesys Adapters, although you can choose to bypass Cisco Adapter registration.

Object Configuration User account

You must configure a user account in Configuration Server so that security permissions can be assigned to allow object configuration for the CCAdv module in the Advisors Administration module (Base Object Configuration page). This is the *Object Configuration User*.

Important

This user must be created in the Configuration Server *before* you install Advisors Platform. Advisors Platform installer prompts you for the account name.

Account Permissions for Data Manager

Object Configuration User—You must create the Object Configuration User account in the Genesys Configuration Layer. You create this user account in Configuration Server as a container for security permissions for objects (Agent Groups, Queues, and Calling Lists). The Object Configuration User requires Read permission for any object that should be considered a configured or monitored object.

Platform Configuration Server User—The Platform Configuration Server user (that is, the Advisors User account) also requires specific permissions to manage object configuration in Configuration Manager related to Data Manager. See [Create the Advisors User Account](#).

Configuration in Advisors Administration Module

The **Manage Adapters** page is read-only.

- To make changes to the properties for an Advisors Genesys Adapter, update the configuration in the database (see [Update AGA Properties in the Database](#)).
- To manage objects, use the **Base Object Configuration** page in the **Administration** Module.

Base Object Configuration Considerations

- **NEW** Starting in release 8.5.0, you must deploy the Contact Center Advisor application (including XML Generator) and configure the Genesys metric sources before you can use the Genesys **Base Object Configuration** page in the Administration module. Data manager requests no statistics for pre-configured objects until the CCAdv module, XML Generator, and Genesys metric data sources are deployed and working.
- The object configuration is done once and independently of any underlying adapters.
- You can identify and filter objects by object type on both mapping screens.
- The page displays the count of configured objects. **NEW** Calling list objects are counted as queues.
- The page prevents contradictory configuration. If you select **No Filter** for an object and then later attempt to assign a filter, you receive an error message. You must de-select **No Filter** before you can assign a filter to that object.
- The associations that display on the **Base Object Configuration** page represent a global configuration for CCAdv/WA.

Configuration Server Integration

Data Manager uses the Configuration Server connection provided by Platform to load Genesys object metadata from Configuration Server. Changes in configuration made on the **Base Object Configuration** page are saved in the Configuration Server for incorporation. Therefore, the Configuration Server system user that is configured on the platform installation (that is, the Advisors user account) should have Change and Change Permissions privileges on the agent groups or queues that are monitored, as well as Read and Read Privilege access permissions for the Advisors User account (see [Create the Advisors User Account](#)).

In Genesys Configuration Manager, you create the Object Configuration User account and assign security permissions for objects (agent groups, calling lists, and queues) to the account. The agent groups, calling lists, and queues to which the Object Configuration User has **Read** access permission are treated as the configured objects for CCAdv/WA. If this user has access to agent groups, calling lists, or queues when Data Manager starts, Data Manager immediately issues statistics requests to the configured Genesys Adapter(s).

Integration with Configuration Server involves a number of aspects, discussed in the following sections:

[+] How Configuration Objects Are Identified

The Configuration Server metadata includes:

- Object Type
- Object ID
- External ID
- Source Environment

The Object Type/Object ID combination (known as the *node ID*) enables an object to be uniquely identified. This node ID is used when applications need to reference a specific object in Configuration Server. The object referenced by the node ID will have a different identifier in the external source environment. Data Manager is responsible for translating the node ID provided by the application into

the appropriate external ID when forwarding requests to the appropriate Adapter.

The object identifier in metadata is composed of the following:

- **ObjectId:** The DBID for the object (provided by Configuration Server).
- **ObjectType:** One of Agent, AgentGroup, or Queue.
- **TenantName**
- **ObjectName:**
 - For Genesys agents: EmployeeId
 - For Agent Groups and Queues: the name provided by Configuration Server
 - For Cisco Agents: N/A

Genesys recommends that one single data source supplies all statistics of a specific statistic type for a given object.

Propagation of Configuration Changes Made in Configuration Manager

Changes made to configured objects (Agent Groups, Queues, Calling Lists, or Interaction Queues) affect the **Base Object Configuration** page in the Administration module in the following ways:

- The addition of an object to the Configuration Server is reflected on the **Base Object Configuration** page when the page is reloaded.
- A name change to an existing object is reflected on the **Base Object Configuration** page when the page is reloaded.
- Any change in an object's Annex properties, such as Filter or Queue Type, is reflected on the **Base Object Configuration** page on restart of the Platform server.
- The addition of the **Read** permission for an object (either new or existing) for the Object Configuration User is reflected on the **Base Object Configuration** page only after the overnight refresh or on restart of the Platform server. If you change one or more configuration objects to make them monitored objects, the additional statistics for those additional objects are not immediately requested. They are scheduled to be picked up during the overnight refresh, at which time the additional statistics are requested. Similarly, if you remove the **Read** permission on an object for the Object Configuration User, statistics are not closed immediately—that happens during the overnight refresh.

If you need any of the above changes (adding an object or removing an object to or from being monitored) to be immediately available, make the changes on the **Base Object Configuration** page instead of making them in Configuration Manager or Genesys Administrator.

[+] Base Object Configuration Page Users and Permissions

The master list of objects on the **Base Object Configuration** page in the Administration Module is the list of agent groups, calling lists, and queues for which the Advisors User account has **Read** access permission.

When the administrator adds more objects to monitor from the available objects, the Object Configuration User is automatically granted **Read** access permission for those objects in Configuration Server. When the administrator removes existing configured objects, the **Read** access permission for those objects is revoked for the Object Configuration User.

The objects for which the Object Configuration User has **Read** permission should always be the same set or a subset of the objects for which the Advisors User account has **Read** access permission.

Important

- If there are objects for which the Object Configuration User has **Read** access permission, but the Advisors User account does not, those objects are not considered and do not display on the Object Configuration page.
- Genesys recommends that you always configure the Advisors User account and the Object Configuration User to be two distinct accounts (not one user account used as both). If one account is used for both users, the administrative user could not add new objects using the Object Configuration page (all objects would be configured objects); the user could view and remove currently configured objects only.

[+] Filter Configuration

The master list of filters for Advisors (for CCAdv, WA, or FA) comes from the Business Attributes configured in the Configuration Server. You can see the list under **Advisors Filters** in the Advisors Business Attributes section of Configuration Manager or Genesys Administrator.

Important

The Advisors Filters business attribute must exist on one—and only one—tenant. Genesys recommends you configure the Advisors Filters business attribute on a tenant that is the default tenant for the Advisors suite installation, on which you configure all Advisors metadata. If there are Advisors Filters business attributes configured on multiple tenants, an error message displays when Genesys Adapter starts, and the filters are not loaded.

Configuring the Advisors Filters

The filter expression is in the **Description** field on the **General** tab of the filter's **Properties** window.

Tip

In a migration scenario, the Migration utility migrates existing filters from the previously-used Stat Server configuration to be the Advisors Filter business attributes, and populates the **Description** field with the filter expression. You configure any additional filters you require by entering the filter expression as the description of the filter.

When filters are associated with configured objects on the **Base Object Configuration** page in the Administration module, the filter and object combination is stored on the **Annex** tab of the object's **Properties** window.

Data Manager uses the configured filters from the **Annex** properties of the object when it requests statistics. When one or more filter combinations are applied, Data Manager requests statistics for each filter. If no filters are applied to an object, then only one statistic is requested for each source metric for that object.

For example, if three filters (Gold, Silver and Platinum) are combined with an ACD Queue object, then three variations of CallsHandled are requested. The three filters are individually applied to yield three statistics: CallsHandled.Gold, CallsHandled.Silver, and CallsHandled.Platinum.

Filters and Interaction Queues

Filter categorization is not applicable for interaction queue statistics. **No Filter** is the only option you can successfully apply to interaction queues. If you attempt to combine filters with an interaction queue, the filters are discarded and the **No Filter** option is automatically selected again.

Filters and Calling Lists

Do not associate a statistic filter with a calling list because Stat Server ignores this type of filter on a calling list statistic.

Frontline Advisor Base Object Configuration

For each source environment in which a given object is present, a corresponding object must exist in the Genesys environment.

When the object already exists in the Genesys environment (that is, it handles interactions monitored by Genesys components, the External ID has the format:

[Tenant Name] Employee ID

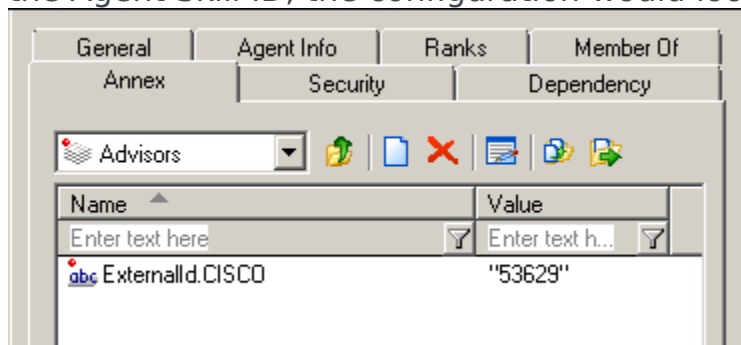
For all other source environments, the object must be created and an entry must be added to the object's Annex tab under an Advisors section. The key for each such entry has the format:

ExternalId.SourceEnvironment

The value is the ExternalID itself.

- For Genesys Adapters, the source Environment is always GENESYS.
- The Cisco Adapter installer prompts for the environment name, with the default value CISCO.

For example, if you are using a Cisco Adapter and want to set the External ID to the Agent Skill ID, the configuration would look as shown in the following figure:



Setting the External ID for a Cisco Agent to their Agent Skill ID

Load Balancing

When two or more Adapters share the same source environment, this indicates that they are connected to the same underlying data provider infrastructure and hence are all able to provide the same set of source metrics. Data Manager is free to select from any Adapter with the same source environment to issue a given statistic. Data Manager attempts to distribute sets of statistics for a given source evenly across all Adapters associated with that source.

NEW Starting in release 8.5.0, if you add adapters to your deployment after the initially-installed adapters are running, the existing statistics are not automatically re-routed to the newly added adapters. That is, load balancing is not re-distributed among all the adapters, including the ones you added. For the procedure to re-distribute the statistics load balancing to include newly-deployed adapters, see [Re-distribute Stats Load when Adapters are Added](#).

Once a statistic is opened for a given object with an Adapter, all subsequent statistics for that object will be opened using the same Adapter. This helps maintain (but does not guarantee) consistency among related metrics reported for this object.

Statistics for a given object can span multiple Adapters, but only if the associated metrics have different Stat Server Type (SST) attributes. Examples of SST include **Core** (which all Stat Servers can provide), **Interaction Queue**, and **Open Media**. Statistics are partitioned by (object, SST). Each (object, SST) group is issued against the same Adapter. The Adapter requires the following:

- A source environment that matches the object's External ID
- A Stat Server Type supported by the Adapter

If a limited number of Adapters support metrics of a specific SST, such as **Open Media**, statistics of this type constitute the bulk of statistics issued to these Adapters. Statistics for more generally-supported metrics, such as **Voice**, are concentrated with Adapters that do not support such specialized statistic types.

Cisco Impact

Advisors Cisco Adapter is used with FA only. Because the Cisco Adapter automatically collects metrics for all agents in that source environment, there is no benefit to load balancing across multiple instances. The only scenario in which multiple Cisco Adapters should be installed is if they provide metrics from separate HDS/AWDB source environments.

Troubleshooting Data Manager

If you are experiencing issues with Data Manager, check for the following problems:

No Genesys Adapters Installed or Configured

If there are no Genesys Adapters installed or configured for a given module (for example, CCAdv), Data Manager cannot issue statistics for that module. This condition (that there are no supported Adapters) is reported in the `geronimo.log` file as a warning message.

Important

After installing an Adapter for a module, you must restart the Advisors Suite server.

Genesys Adapter is Unavailable

If there is one or more Genesys Adapter installed and configured for a given module, but the Adapter is not running or is unreachable, Data Manager cannot request statistics for that module. This condition is reported in the `geronimo.log` file as an error message with an exception (Multiple Adapters Exception). The error is no longer reported after the configured Adapter is started.

NEW Data Manager does not Re-distribute Stat Requests to other Adapters when one Adapter's Service is Stopped

When one or more adapter (ACA or AGA) instances are installed, ensure that they are always in use. A deployed adapter that is not running can prevent Data Manager from sending requests to the other live adapters. If you have a deployed adapter that is not going to be in use, Genesys recommends that you remove the adapter configuration from the Advisors Platform table `ADAPTER_INSTANCES` to

prevent disruption of service in the active adapters.

If you have a deployed, but inactive adapter, use the following procedure to remove all the objects from its configuration.

1. Determine which objects are associated with the inactive adapter:

- Run the `select adapter_instance_id, name from adapter_instances` statement against the Advisors Platform database – this provides the ID value for each adapter instance.
- Run the `select adapter_instance_id, ss_pair_id from adapter_ss_config where adapter_instance_id = <ID of adapter>` statement against the Advisors Platform database – this shows you which Stat Server pairs are associated with the adapter.
- Run the `select distinct objectid, objecttype, from adapter_ss_Mapping where ss_pair_id = <ID of Stat Server>` statement against the Advisors Platform database – this shows you which objects are associated with the Stat Server pair for each adapter. Remove the objects associated with the Stat Server pair for the adapter that you must delete from the table. If there is more than one pair, replace = <ID of Stat Server> with `IN (Id,Id)`.

2. To remove the identified objects, run the `Delete from adapter_ss_mapping where ss_pair_id = <the pair associated with your inactive Adapter>` statement. If there is more than one pair, replace = <the pair associated with your inactive Adapter> with `IN (Id,Id)`.

3. To remove the Stat Server pair rows associated with the adapter, run the `Delete from adapter_ss_config where adapter_instance_id = <ID of adapter to delete>` statement.

4. To delete the adapter_instance row, run the `Delete from adapter_instances where adapter_instance_id = <ID>` statement.

No Object Configuration User Specified

For the CCAAdv module, an Object Configuration User must be specified when you install Advisors Platform. If configuration of this user name is omitted, no statistics are issued with the Adapters. This is indicated by an information message in the Platform `geronimo.log` file. The information message indicates that no statistics are requested because no agent groups and queues are found. To correct this:

1. Update `genesys.configServer.objectconfig-username` in the Platform `GenesysConfig.properties` file.
2. Restart Platform after you update the properties file.

No Object Configuration User Exists

If the Object Configuration User does not exist in the Genesys Configuration Server, an error message is logged in the form of an exception. To correct this issues:

1. Create the user in Configuration Server.
2. Update `genesys.configServer.objectconfig-username` in the Platform `GenesysConfig.properties` file.
3. Restart Platform after you update the properties file.

Base Object Configuration page is empty - unable to publish CCAAdv base objects

Ensure the Administration user who is logged in to the Administration module (workbench) has been

assigned the Read permission for the tenant under which the source objects exist that the user must monitor.

Adapter Stat Server Configuration

Selecting Stat Servers to Support Specific Statistic Types

If your environment uses third-party media statistics or multimedia statistics, you must have a corresponding Java Stat Server extension installed on the respective Stat Servers. To avoid having to install Java extensions on all the configured Advisors Stat Servers, you can use a configuration option to identify the configured Stat Servers to use to request specific types of statistics when statistics are requested from a pool of configured Stat Server pairs. For example, you can choose to collect core statistics only on certain pairs of Stat Servers and third-party media statistics on other specific pairs. The configuration option is part of the Genesys Adapter installation process. For information about installing Genesys Adapter, including the option to associate specific types of statistics with a Stat Server pair, see [Deploying Genesys Adapter](#).

If there are no Stat Server extensions deployed on a Stat Server, then typically it supports only core statistics. Therefore, you can configure such a Stat Server to be a core Stat Server.

On installation, your selection of these properties is stored in the Platform database table `ADAPTER_SS_CONFIG`. After installation, you can change these properties in this database table. Adapters need to be restarted after changes are made.

Establishing a TLS Connection to Genesys Configuration Server

Performance Management Advisors supports an optional TLS connection to the Genesys Configuration Server. Both the Advisors Suite Server (the Platform server) and the Advisors Genesys Adapter (AGA) can establish individual TLS connections to the Configuration Server. CCAdv, WA, FA, and AA also have a secure connection to the Configuration Server if you enable a TLS connection on Advisors Platform.

If you plan to connect to the Configuration Server using TLS, you must first do the following:

1. Create a TLS properties file, as explained in the **TLS Properties File** section below.
2. Configure a secure port for Genesys Configuration Server. For more information, see [Genesys 8.1 Security Deployment Guide](#).
3. Configure security certificates.
4. Configure the security providers and issue security certificates. For more information, see [Genesys 8.1 Platform SDK Developer's Guide](#).
5. Assign a certificate to the Configuration Server host. For more information, see [Genesys 8.1 Security Deployment Guide](#).

You can use the same certificates for both AGA and Advisors Platform if you enable a TLS connection on both, because all the same components are involved in the subsequent interactions across the TLS connection.

To configure a TLS connection to the Configuration Server, you can select the option to do so on the installation screen when you deploy Advisors Platform and AGA, or you can enable TLS post-deployment using the properties files. If you have a backup Genesys Configuration Server and you enable a TLS connection to the primary Configuration Server when deploying AGA, AGA also connects to the backup Configuration Server using TLS.

If a TLS connection to Configuration Server cannot be established when you start the installed instance of Advisors Platform or AGA, error messages are logged in the log file. You can correct the TLS properties supplied during installation in the relevant property file post-installation.

Advisors Configuration Properties Files for TLS

The Advisors Platform properties file, <PLATFORM_INSTALL>/conf/GenesysConfig.properties, has the following TLS-related properties:

- genesys.configServer.tlsproperties.file
- genesys.configServer.tls.port
- genesys.configServer.tls.enabled

The AGA properties file, `<AGA_INSTALL>/conf/inf_genesys_adapter.properties`, has the following TLS-related properties:

- `genesys_connector.configServer.tls.enabled`
- `genesys_connector.configServer.tls.port`
- `genesys_connector.configServer.tlsproperties.file`

You can enable or disable the TLS connection to Configuration Server by changing the `configServer.tls.enabled` flag to `true` (enables TLS) or `false` (disables TLS) on a Platform installation or on an AGA installation.

Important

If you did not enable TLS initially during deployment, you can change the `configServer.tls.enabled` flag to `true`, but you must also add the TLS port and the TLS property file information using the relevant properties file (Platform or AGA) to fully enable TLS support post-installation.

Supported TLS Port Mode and Providers

Configure the port mode on the Configuration Server.

- Although there are three port modes for TLS configuration, only the upgrade port mode is supported for an Advisors TLS connection to Genesys Configuration Server.

The upgrade port mode allows an unsecured connection to be established; the connection switches to TLS mode only after Advisors retrieves the TLS settings from Configuration Server.

Supported TLS Providers

Advisors support the following security providers:

- PEM
- MSCAPI
- PKCS#11

TLS Properties File

The TLS properties file is not supplied with Advisors; it is unique to your enterprise.

Important

You must create a TLS properties file before deploying Advisors Platform or AGA if you intend to enable a TLS connection to the Genesys Configuration Server during Advisors installation. The Advisors Platform and AGA installers prompt for the location of the TLS properties file.

The TLS configuration required to support each provider varies slightly, but each can be configured uniquely in a properties file. You can save the TLS properties file using any filename you choose.

Important

On a Windows OS, do not use a backslash (/) in the file path to separate folders; use a slash (/) only.

The TLS properties file uses a simple key value pair format. On each line of the file, a key is followed by an equal sign (=), which is followed by a value for the key. For example:

```
provider=PEM
certificate=C:/advisors/security/conf/client1-cert.pem
certificate-key=C:/advisors/security/conf/client1-key.pem
trusted-ca=C:/advisors/security/conf/ca.pem
tls-crl=C:/advisors/security/conf/crl.pem
tls-mutual=0
```

In the preceding example, the provider key has a value of PEM, identifying the security provider type. For this particular provider, additional security parameters (keys) must be supplied, and which are included in the example. You must copy the certificate files to a folder on the local hard drive.

The TLS properties file path you enter during installation (or in the Advisors Platform or AGA properties file post-installation) points to those security files.

Important

The TLS property flags `tls=0` and `tls=1` are valid properties to indicate whether the TLS connection is enabled or disabled, but the Advisors `configServer.tls.enabled` property flag overrides the

TLS property set in the TLS properties file. That is, setting or resetting the TLS property to indicate TLS is enabled or disabled in the `tls.properties` file has no effect on an Advisors connection to Configuration Server.

For information about supported TLS properties, see the relevant section in the [Genesys 8.1 Platform SDK Developer's Guide](#).

Troubleshooting the TLS Connection

When Advisors Platform or AGA attempt to establish the TLS connection to Configuration Server, progress is written in the log file. You can ignore a warning message in the log file that indicates that there is no TLS configuration for Advisors found in the Configuration Server. Advisors is not an application configured in Configuration Server, therefore it returns an empty configuration and relies on the TLS configuration supplied by the connection properties.

For information about troubleshooting issues with TLS connections, see [Genesys 8.1 Security Deployment Guide](#).

Scaling the System to Increase Capacity

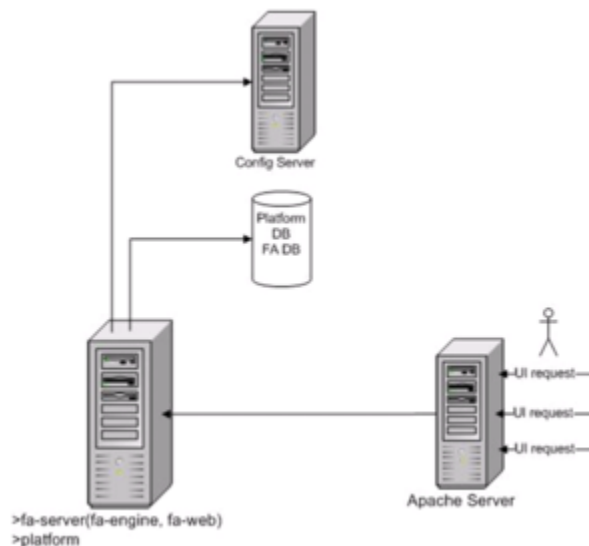
You can horizontally scale the web services module for Contact Center Advisor (CCAdv), Workforce Advisor (WA), and Frontline Advisor (FA).

Frontline Advisor

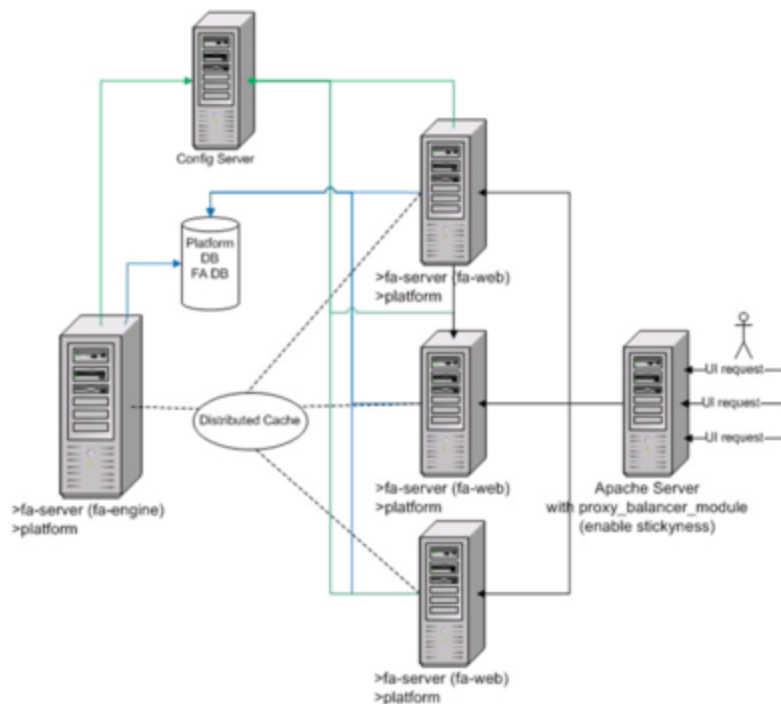
FA supports a distributed mode. You can deploy FA on multiple servers or hosts in distributed mode.

- For the procedure to deploy FA in standalone or distributed mode, see [Deploying FA](#).

The first figure below, Architecture of the FA standalone mode, shows a basic installation of Frontline Advisor. There is one FA server that provides both the aggregation and presentation layers to support the FA module in the Advisors browser.



The second figure below shows Frontline Advisor deployed in distributed mode. In distributed mode, all FA instances share the Platform database and FA database. Only one FA instance, the FA engine, performs data aggregation. You enable the rollup engine on this FA instance during installation. The other FA instances, which provide FA web services, retrieve dashboard data and metrics from the FA engine. Together, the FA web instances provide the presentation layer. You disable the rollup engine on each such member of the distributed cluster during installation.



Workforce Advisor

You can install WA web services on multiple WA nodes in a way similar to Frontline Advisor distributed mode. To accomplish this, the calculation functionality of WA is separated from the presentation functionality. The CCAdv/WA installer offers two choices for WA installation:

- Workforce Advisor server—Reads data from external systems and calculates WA's metrics.
- Workforce Advisor web services—Responds to requests from clients and sends data about metrics and alerts to clients.

Contact Center Advisor

You can install CCAdv web services on multiple CCAdv nodes in a way similar to Frontline Advisor distributed mode. The CCAdv/WA installer offers the following options for CCAdv installation:

- CCAdv XML Generator—Reads data from external systems and calculates CCAdv's metrics.
- CCAdv web services—Responds to requests from clients and sends data about metrics and alerts to clients.

Advisors Cluster Information

Every system on which you install a module in the Advisors suite, where the module uses an Advisors Platform database, is a node in a cluster.

- A module is an application in the Advisors suite that you can install separate from other applications. For example, a WA Server or Contact Center Advisor XML Generator is a module.
- A node in a cluster is an entity that has an IP address. An example is a physical computer, or a virtual machine on a VM host.
- A node in a cluster is also referred to as a member of the cluster.

Members of the cluster communicate to share data that is cached in memory, and to transmit messages to perform workflows that require more than one module.

Even if you install Advisors on only one system, that system is a node in a cluster containing that one system.

A system that is a node in a cluster can run one Advisors module, or more than one Advisors module.

For example, the WA Server and WA Web Services are two modules, and you can install both on the same node. Alternatively, you can install the WA server on one cluster member, and WA web services on another cluster member.

Another example: WA Server and CCAdv XML Generator are two modules, and you can install them both on the same node or on different nodes. In the first case, you would have one cluster member, and in the second case, you would have two.

- For instructions about how to modify a cluster after you have installed Advisors, see [Change Advisors Cluster Membership](#).

Encryption for AGA Metrics Database Data (Oracle)

Advisors Genesys Adapter (AGA) metrics schema objects hold metadata related to queues and agent groups, and save snapshots of the real)time queue and agent group metrics produced by the Genesys Stat Server.

If you categorize this as sensitive data within your enterprise that should be secured, Genesys recommends placing AGA metrics schema objects into a separate tablespace and securing the tablespace with Oracle TDE tablespace encryption. Use one of the following common standardized ciphering methods:

- 3DES168
- AES128
- AES192
- AES256

Considering the specifics of AGA data flow and the real)time nature of the Advisors application, Genesys does not recommend TDE column encryption for AGA.

Important

Oracle 11g documentation contains detailed information about TDE.

LoggedIn Scripts

Contact Center Advisor and Workforce Advisor support LoggedIn scripts for virtual agent groups (VAG). Agent group membership information is retrieved from the Stat Server for VAGs that are defined using the LoggedIn script.

FA Message Listening Port

Frontline Advisor performs metric rollups in memory. In earlier releases, FA performed the metric rollups through database stored procedures.

Genesys Adapters report source metrics directly to FA using a persistent connection. When an FA instance initially requests to register with an adapter, the request includes the host and port on which FA is listening for inbound connections. The host information is retrieved from the `CLUSTER_MEMBER` table in the Platform database. The `message.listening.port` entry in the `FrontlineAdvisor.properties` configuration file specifies the port. The value may be a static port number, or zero. Zero means that FA should use any available port. The default value is static port 8350.

Configuring the Messaging Port between FA and Genesys Adapter

The port on which FA listens for connections from Adapter for source metric reporting is `message.listening.port=8350`.

The installation defaults to port 8350 for communication between FA and AGA. Post installation, if you must change this port, go to the Advisor Platform installation `/conf` folder. Edit the property file named `FrontlineAdvisor.properties`; change the property as required.

Providing a User Interface for Users with Visual Impairment

Contact Center Advisor and Workforce Advisor support JAWS Standard version 11, an accessibility interface for users with visual impairment. JAWS provides audio and a series of keyboard shortcuts for navigating the tabulated information on the screen. If you have users in your enterprise who require this type of user interface, you must ensure those users have Internet Explorer 6 or higher (Genesys recommends that you use Internet Explorer 8) to use the JAWS functionality.

Frontline Advisor (manager console) also supports JAWS Standard version 11.

The CCAdv login page URL uses the following format:

```
http(s)://<server>[:port]/ca-xml/accessibleDashboard[?language=<en|de|fr>]
```

You can also reach the CCAdv accessible dashboard by clicking the gear icon at the top right of the CCAdv dashboard.

The WA login page URL uses the following format:

```
http(s)://<server>[:port]/wu/accessibleDashboard[?language=<en|de|fr>]
```

You can also reach the WA accessible dashboard by clicking the gear icon at the top right of the CCAdv dashboard.

The FA login page URL uses the following format:

```
http(s)://<server>[:port]/fa/accessibleSupervisorDashboard[?language=<en|de|fr>]
```

See Release Notes specific to your Advisors software release for the list of supported languages—not all languages are supported in all releases.

The server and port variables relate to the server or servers on which you have installed CCAdv and WA. The functionality to work with JAWS is installed when you install CCAdv and WA—there is no additional installation or configuration required. Users specify their language preference at login; again, no additional configuration is required to provide language options.

Contact Center Advisor Mobile Edition

Contact Center Advisor—Mobile Edition (CCAdv—ME) installation is an option in the CCAdv/WA module installer. For installation instructions, see [Deploying CCAdv and WA](#).

Role-Based Access Control for Mobile Devices

It is important to define a basic set of permissions in Configuration Server, so that users can view objects and functionality in the Application interface. For example, users with permissions to the CCAdv module (and ME) and permissions to view the Performance Monitor cannot view anything if they do not have access to any of the metrics and/or business attributes. They can log in to the Advisor interface, but the real-time tab will not appear if they do not have permissions to use at least one metric.

Required Permissions

Users who have access to ME will need the following minimum permissions:

- permissions to at least one contact center and/or application
- permissions to one of the following objects:
 - reporting region
 - geographic region
 - operating unit
- permissions to at least one metric

Important

If a user does not have permissions to view any of the default metrics, the first metric that displays in the ME Metrics or Hierarchy list is the first metric in the Column Chooser Available metrics list to which the user does have access permissions.

Using object permissions, you can assign a user's access permission to certain objects. When you apply permissions to an object, they apply equally to all properties of the object—if a user has access permissions, they see the entire object.

CCAdv—ME loads metrics dynamically based on user permissions taken from the server cache. It loads the metrics through `/ca-ws/columns.do`, to ensure the metrics information is up-to-date. If

metrics permissions change after a user chooses to display that metric, it is displayed with no data. However, when a user reselects the metrics to display, the list is refreshed.

The following permissions are implemented in the CCAdv—ME MapResource:

- metrics
- operating units
- reporting regions
- geographical regions
- contact centers
- application groups

Relevant objects are loaded on-demand, based on the user access permissions granted for each object.

Mobile Edition Privileges

Compared to Contact Center Advisor, the Mobile Edition has limited functionality. Therefore, CCAdv—ME requires only a subset of functional privileges. The following table provides a comparison of CCAdv privileges with Mobile Edition privileges.

Privileges	In CCAdv	In ME
ContactCenterAdvisor.Dashboard.canView		✓
ContactCenterAdvisor.Dashboard.AgentGroupsPane.canView		
ContactCenterAdvisor.Dashboard.ColumnChooser.canView		✓
ContactCenterAdvisor.Dashboard.EnterpriseStats.canView		✓
ContactCenterAdvisor.Dashboard.PivotSelect.canView		
ContactCenterAdvisor.PerformanceMonitor.canView		✓
ContactCenterAdvisor.PerformanceMonitor.CallFlowPane.canView		✓
ContactCenterAdvisor.PerformanceMonitor.CurrentCapacity.canView		✓
ContactCenterAdvisor.ActionManagementReport.canView		
ContactCenterAdvisor.AlertManagement.canView		

[+] Dashboard Privilege

The Dashboard privilege (ContactCenterAdvisor.Dashboard.canView) controls access to the CCAdv dashboard. Users with this privilege can access the CCAdv dashboard, the CCAdv tab in the Advisor browser, and log in to CCAdv—ME.

Important

Users cannot log in to CCAdv—ME if they do not have the privilege to access the Dashboard.

[+] Column Chooser Privilege

The Column Chooser privilege (`ContactCenterAdvisor.Dashboard.ColumnChooser.canView`) determines which metrics the user can choose for display. Users with this privilege can choose which metrics to display on the dashboard, access the **Column Chooser** button on the dashboard, and access the **Metrics** tab in the Mobile application.

Important

Users will either see a disabled Metrics tab (iOS) or will not see the Metrics menu/button (Blackberry) if they do not have the privilege to access Column Chooser.

[+] Enterprise Stats Privilege

The Enterprise Stats privilege (`ContactCenterAdvisor.Dashboard.EnterpriseStats.canView`) controls the display of the Enterprise Stats row in the dashboard. Users with this privilege can see the Enterprise Performance row in the dashboard.

Important

Users will see N/A in the Enterprise Performance row in the dashboard, if they do not have the privilege to access Enterprise Stats.

[+] Performance Monitor Privilege

The Performance Monitor privilege (`ContactCenterAdvisor.PerformanceMonitor.canView`) determines who can view the Performance Monitor. Users with this privilege can access to the **Performance Monitor** button on the dashboard and the right-arrow button (which directs to the **Performance Monitor** view) on each row of stats.

Important

Users will not see any arrow buttons (iOS) or menu/buttons (Blackberry) if they do not have the privilege to access Performance Monitor.

[+] Call Flow Stats Privilege

The Call Flow Stats privilege (`ContactCenterAdvisor.PerformanceMonitor.CallFlowPane.canView`) determines who can view the Call Flow stats in the Performance Monitor. Users with this privilege can view the Call Flow stats in the Performance Monitor.

Important

Users will see the Call Flow stats pane, but no data will be displayed if they do not have the privilege to access Call Flow Stats. The behavior prompted by this flag is the same for both CCAdv and CCAdv—ME.

[+] Current Capacity Stats Privilege

The Current Capacity Stats privilege (`ContactCenterAdvisor.PerformanceMonitor.CurrentCapacity.canView`) determines who can view the Current Capacity stats in the Performance Monitor. Users with this privilege can view the Current Capacity stats in the Performance Monitor.

Important

Users will see the Current Capacity stats pane, but no data will be displayed if they do not have the privilege to access Call Flow Stats. The behavior prompted by this flag is the same for both CCAdv and CCAdv—ME.

Functionality Privileges

Functionality privileges determine what tasks the user can perform or what functions a user can

execute on objects to which he/she has access.

Privileges are configured by using roles. If a privilege is present in a role, then any users assigned that role have access to the functionality controlled by that privilege. The value for the privilege key can be anything, or can be left blank.

Privileges for each role are stored as key-value pairs in the Annex tab of that role in Genesys Configuration Manager.

For more information about the CCAAdv functional privileges, see the [Contact Center Advisor and Workforce Advisor Administrator User's Guide](#).

Advisors Software Distribution Contents

Click the links below to view the software contents that Genesys provides for each Performance Management Advisors product.

[+] Advisors Platform

Distribution Artifacts	Contents	Notes
advisors-platform-installer- <version>.jar		The installer for the Platform.
advisors-migration-wizard- <version>.jar user-migration-util-<version>.jar (See User Migration Utility)		Migration utilities located in supplement directory: ip\ supplement
baseweb-<version>-static- web.zip		A copy of the static files that can be served by Apache.
SQL Server platform-new-database-<version>.sql	Creates DB objects for MS SQL Platform database after the Platform database is created. Refer to Creating a SQL Server Database for instructions about MS SQL Server database creation.	The creation and migration script for the Platform database for MSSQL. This script is located in the sql\mssql directory.
Oracle advisors-platform-migrate_<old version>_<new version>.sql advisors-platform- <version>_CUSTOM_ROUTINE.sql advisors-platform- <version>_INIT_DATA.sql advisors-platform- <version>_ObjectsCustom.sql advisors-platform- <version>_ObjectsDefault.sql advisors-platform- <version>_ObjectsPlus.sql advisors-platform-<version>_Readme.txt advisors-platform- <version>_ROUTINE.sql advisors-platform-<version>_Schema.sql advisors-platform-<version>_TBS.sql advisors-platform-<version>_User.sql	<ol style="list-style-type: none"> 1. ..._CUSTOM_ROUTINE.sql Not to be executed manually. Used by the scripts in runtime. 2. ..._INIT_DATA.sql Not to be executed manually. Used by the scripts in runtime. 3. ..._ROUTINE.sql Not to be executed manually. Used by the scripts in runtime. 4. ..._TBS.sql To be executed by a database user who has permission to create tablespaces. The script generates a resulting script, runTbsCre.sql, based on the user dialog input. The script issues a prompt which allows you to postpone the execution of the resulting script. If necessary, the 	<p>The creation scripts for the Platform database for Oracle. These scripts are located in the sql\oracle directory.</p> <p>For additional details, please refer to:</p> <ul style="list-style-type: none"> • migrate_plt_Readme.txt, if present. Otherwise, refer to the Release Notes. • plt_Readme.txt, if present. Otherwise, refer to the Release Notes.

Distribution Artifacts	Contents	Notes
	<p>resulting script can be customized to meet your needs and environment and executed later. A minimum requirement is to create at least one user default tablespace and a separate user temporary tablespace exclusively for the platform user/schema. In most cases, tablespaces are created by your DBA. The file can be used for DBA information as it shows sizing and possible table distribution among multiple tablespaces. Note, the sizing must be adjusted before the script execution. If created by the DBA, the DBA provides the tablespaces information to the engineer who proceeds with the installation.</p> <p>5. ...User.sql Creates platform user and schema. To be executed by a database user who has permission to create other users. In most cases, users are created by your DBA. The file can be used as is or for DBA information as it shows user permission and tablespace requirements. If the user/schema is created by DBA, the DBA provides the relevant information to the engineer who proceeds with the installation.</p> <p>6. ...ObjectsPlus.sql An SQL*Plus script that creates all platform database objects. To be executed by the previously-created platform user and after all planned tablespaces are created.</p> <p>7. ...ObjectsCustom.sql An alternative script that has the same purpose as ...ObjectsPlus.sql, but can be executed from Oracle</p>	

Distribution Artifacts	Contents	Notes
	<p>Sql Developer by the previously-created platform user and after all planned tablespaces are created. The script allows table and index distribution among multiple tablespaces by issuing pop-up prompts.</p> <p>8. ...ObjectsDefault.sql An alternative script similar to ...ObjectsCustom.sql that has the same purpose as ...ObjectsPlus.sql. To be executed from Oracle Sql Developer by the previously-created platform user. The script does not issue any pop-up prompts and creates all platform database objects in the platform user default tablespace assigned during platform user creation.</p> <p>9. ...Schema.sql Creates the platform user, schema, and all database objects. To be executed by a database user who has permission to create other users. An alternative script that replaces, and has the same purpose as, ...User.sql and ...ObjectsPlus.sql combined.</p>	

[+] Advisors Genesys Adapter

Distribution Artifacts	Contents	Notes
aga-installer-<version>.jar		The installer for Genesys Adapter.
SQL Server gc_metrics_newdb_<version>.sql		The creation and migration scripts for the Genesys Adapter database for MSSQL. These scripts are located in the configuration-schema\mssql directory.
Oracle gc_metrics_new_<version>_ObjectsCustom.sql gc_metrics_new_<version>_ObjectsDefault.sql	1 ..._ROUTINE.sql Not to be executed manually.	The creation and migration scripts for the Genesys Adapter databases for Oracle. These scripts are located in the

Distribution Artifacts	Contents	Notes
gc_metrics_new_<version>_ObjectsPlus.sql gc_metrics_new_<version>_ROUTINE.sql gc_metrics_new_<version>_User.sql gc_metrics_new_<version>_TBS.sql gc_metrics_new_<version>_Schema.sql	<p>Used by the scripts in runtime.</p> <p>2. ...TBS.sql To be executed by a database user who has permission to create tablespaces. The script contains some sizing recommendations. The sizing must be adjusted before the script execution. The script issues a prompt that allows you to postpone the actual tablespace creation. Instead, a resulting script, runTbsCre.sql, is generated based on the user dialog input. If necessary, the resulting script can be customized to the needs of the environment and executed later. A minimum requirement is to create at least one user default tablespace and a separate user temporary tablespace exclusively for AGA metrics user/schema. In most cases, tablespaces are created by your DBA. If created by the DBA, the DBA provides the tablespaces information to the engineer who proceeds with the installation.</p> <p>3. ...User.sql Creates the AGA metrics user and schema. To be executed by a database user who has permission to create other users. In most cases, users are created by your DBA. The file can be used as is or for DBA information as it shows user permission and tablespace requirements. If the user/schema is created by the DBA, the DBA provides the relevant information to the engineer who proceeds with the installation.</p> <p>4. ...ObjectsPlus.sql An SQL*Plus script that creates all AGA metrics DB</p>	configuration-schema\oracle directory.

Distribution Artifacts	Contents	Notes
	<p>objects. To be executed by the previously-created AGA metrics user and after all the planned tablespaces are created.</p> <p>5. ...ObjectsCustom.sql An alternative script that has the same purpose as ...ObjectsPlus.sql, but can be executed from Oracle Sql Developer by the previously-created AGA metrics user and after all the planned tablespaces are created. The script allows table and index distribution among multiple tablespaces by issuing pop-up prompts.</p> <p>6. ...ObjectsDefault.sql An alternative script similar to ...ObjectsCustom.sql that has the same purpose as ...ObjectsPlus.sql. To be executed from Oracle Sql Developer by the previously-created platform user. The script does not issue any pop-up prompts and creates all AGA metrics database objects in the platform user default tablespace assigned during platform user creation.</p> <p>7. ...Schema.sql Creates the AGA metrics user, schema, and all database objects. To be executed by a database user who has permission to create other users. An alternative script that replaces, and has the same purpose as, ...User.sql and ...ObjectsPlus.sql combined.</p>	

[+] Supervisor Desktop Service

Distribution Artifacts	Notes
sds-installer-<version >.jar	The installer for Supervisor Desktop Service

[+] Advisors Cisco Adapter

Distribution Artifacts	Contents	Notes
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 aca-migration-8.1.1-to-8.1.2.sql aca-migration-8.1.2-to-8.1.3.sql aca-migration-8.1.3-to-8.1.4.sql aca-migration-8.1.4-to-8.1.5.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 aca-migration-8.1-to-8.1.1.sql aca-migration-8.1.1-to-8.1.2.sql aca-migration-8.1.2-to-8.1.3.sql aca-migration-8.1.3-to-8.1.4.sql aca-migration-8.1.4-to-8.1.5.sql	<ol style="list-style-type: none"> 1. aca_..._TBS.sql The script creates ACATBS_USER data tablespace and ACATBS_TMP temporary tablespace under the path specified on the prompt. To be executed by a database user who has permission to create tablespaces. If necessary, the sizing can be adjusted before the script execution. If it is necessary to change the suggested tablespace names, the script must be edited before execution as follows: <ol style="list-style-type: none"> a. ACATBS_USER must be replaced with another suitable tablespace name that must be used as the default FA user tablespace. b. ACATBS_TMP must be replaced with another suitable tablespace name that must be used as the temporary ACA user tablespace. The script generates a resulting script, runTbsCre.sql, based on user dialog input. If there is any error, the resulting script can be customized to the needs and environment and executed again. A minimum requirement is to create one user default 	The creation and migration scripts for the Cisco Adapter databases for Oracle. These scripts are located in the oracle directory.

Distribution Artifacts	Contents	Notes
	<p>tablespace and a separate user temporary tablespace exclusively for the ACA user/schema. In most cases, tablespaces are created by your DBA. If created by a DBA, the DBA provides the tablespaces information to the engineer who proceeds with the installation.</p> <p>2. <code>faca-new-database-... .sql</code> Creates all ACA database objects. Executed by the previously-created ACA user. In most cases users are created by your DBA. The DBA can use <code>aca_... .Schema.sql</code> (see the description below) for information about required user permissions and tablespace requirements. If the user/schema is created by the DBA, the DBA provides the relevant information to the engineer who proceeds with the database object creation and further installation.</p> <p>3. <code>aca_... .Schema.sql</code> Creates the ACA user, schema, and all database objects. Replaces manual user creation and <code>aca-new-database-... .sql</code>. To be executed by a database user who has permission to create other users. This is an alternative script normally used in non-production environments.</p>	

[+] Contact Center Advisor/Workforce Advisor

Distribution Artifacts	Contents	Notes
<code>ccadv-wa-server-installer-<version>.jar</code>		The installer for CCAdv and WA modules, as well as CCAdv-ME starting in Release 8.1.5.

Distribution Artifacts	Contents	Notes
SQL Server mg-new-database-<version>.sql		<p>The creation and migration database script for Metric Graphing for MS SQL. This script is located in the sql\mssql directory.</p> <p>You have the following folders:</p> <ul style="list-style-type: none"> mssql-standard (for installations that use MS SQL Standard Edition) mssql-enterprise (for installations that use MS SQL Enterprise Edition) <p>Files within each folder use the same filename convention as previous releases. Ensure you use the files from the folder that corresponds to your edition of Microsoft SQL Server.</p>
Oracle mg-<version>_User mg-<version>_TBS.sql mg-<version>_Schema.sql mg-<version>_ROUTINE.sql mg-<version>_ObjectsPlus mg-<version>_ObjectsDefault mg-<version>_ObjectsCustom mg-<version>_INIT_DATA.sql	<ol style="list-style-type: none"> 1. ..._CUSTOM_ROUTINE.sql Not to be executed manually. Used by the scripts in runtime. 2. ..._INIT_DATA.sql Not to be executed manually. Used by the scripts in runtime. 3. ..._ROUTINE.sql Not to be executed manually. Used by the scripts in runtime. 4. ..._TBS.sql To be executed by a database user who has permission to create tablespaces. The script generates a resulting script, runTbsCre.sql, based on the user dialog input. The script issues a prompt that allows you to postpone execution of the generated resulting script. If necessary, the resulting script can be customized to meet your needs and environment and executed later. A minimum requirement is to create at least one user default tablespace and a separate user temporary tablespace exclusively for the CCA/WA 	<p>The creation database scripts for Metric Graphing for Oracle. These scripts are located in the sql\oracle directory.</p> <p>You have the following folders:</p> <ul style="list-style-type: none"> oracle-without-partitions (for installations that use Oracle without the partitioning option) oracle-with-partitions (for installations that use Oracle with the partitioning option) <p>Files within each folder use the same filename convention as previous releases. Ensure you use the files from the folder that corresponds to your edition of Oracle.</p> <p>For additional details, refer to the migrate_mg_8.1.<version>Readme.txt file, if present. Otherwise, refer to Release Notes.</p>

Distribution Artifacts	Contents	Notes
	<p>metric graphing user/schema. Note, the sizing must be adjusted before the script execution. In most cases tablespaces are created by your DBA. The file can be used for DBA information as it shows sizing and possible table distribution among multiple tablespaces. If created by the DBA, the DBA provides the tablespaces information to the engineer who proceeds with the installation.</p> <p>5. ...User.sql Creates the CCAdv/WA metrics graphing user and schema. To be executed by a database user who has permission to create other users. In most cases, users are created by your DBA. The file can be used as is or for DBA information as it shows user permission and tablespace requirements. If the user/schema is created by the DBA, the DBA provides the relevant information to the engineer who proceeds with the installation.</p> <p>6. ...ObjectsPlus.sql An SQL*Plus script that creates all CCA/WA database objects necessary for metrics graphing. To be executed by the previously-created CCAdv/WA metric graphing user and after all planned tablespaces are created.</p> <p>7. ...ObjectsCustom.sql An alternative script that has the same purpose as ...ObjectsPlus.sql, but can be executed from Oracle Sql Developer by the previously-created CCAdv/WA metric graphing user and after all planned tablespaces are created. The script allows table and index distribution</p>	

Distribution Artifacts	Contents	Notes
	<p>among multiple tablespaces by issuing pop-up prompts.</p> <p>8. ...ObjectsDefault.sql An alternative script similar to ...ObjectsCustom.sql that has the same purpose as ...ObjectsPlus.sql. To be executed from Oracle Sql Developer by the previously-created CCAdv/WA metric graphing user. The script does not issue any pop-up prompts and creates all platform database objects in the platform user default tablespace assigned during platform user creation.</p>	

[+] Frontline Advisor/Agent Advisor

Distribution Artifacts	Contents	Notes
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 fa-database-migration-8.1.1-to-8.1.2.sql fa-database-migration-8.1.2-to-8.1.3.sql fa-database-migration-8.1.3-to-8.1.4.sql fa-database-migration-8.1.4-to-8.1.5.sql	Creates database objects for the MSSQL FA database after the FA database is created. Refer to Creating a SQL Server Database for instruction about MSSQL Server database creation.	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 fa-database-migration-8.1-to-8.1.1.sql fa-database-migration-8.1.1-to-8.1.2.sql fa-database-migration-8.1.2-to-8.1.3.sql fa-database-migration-8.1.3-to-8.1.4.sql fa-database-migration-8.1.4-to-8.1.5.sql	1. fa_..._TBS.sql The script creates the FATBS_USER data tablespace and FATBS_TMP temporary tablespace under the path specified on the prompt and appends <i>frontline</i> to this path sub-folder name. The script contains sizing recommendations. The sizing must be adjusted before the script execution. To be executed by a database user who has permission to create tablespaces. If it is necessary to change the suggested tablespace name and the file	The creation and migration scripts for the FA/AA database for Oracle. These scripts are located in the oracle and oracle\migrations directories.

Distribution Artifacts	Contents	Notes
	<p>path, the script must be edited before its execution as follows:</p> <ol style="list-style-type: none"> FATBS_USER must be replaced with another suitable tablespace name that needs to be used as the default FA user tablespace. FATBS_TMP must be replaced with another suitable tablespace name that must be used as the temporary FA user tablespace. Replace the line <pre>fapath := '' fapath 'frontline' osfs;</pre> with <pre>fapath := '' fapath osfs;</pre> to prevent the script from appending a <i>frontline</i> sub-folder name to the specified path. In this case, the files are created under the path specified on the related prompt issued by the script when it is executed. <p>The script generates a resulting script, <i>runTbsCre.sql</i>, based on user dialog input. If there is an error, the resulting script can be customized to the needs of the environment and executed again. A minimum requirement is to create at least one user default tablespace and a separate user temporary tablespace exclusively for FA user/schema.</p> <p>In most cases, tablespaces are created by your DBA. If created by the DBA, the DBA provides the tablespaces information to the engineer who proceeds with the installation.</p> 	
	<ol style="list-style-type: none"> fa-new-database-...sql Creates all FA database 	

Distribution Artifacts	Contents	Notes
	<p>objects. Executed by the previously-created FA user. In most cases, users are created by your DBA. The DBA can use <code>fa_...Schema.sql</code> for information about required user permissions and tablespace requirements. If the user/schema is created by the DBA, the DBA provides the relevant information to the engineer who proceeds with the database object creation and installation.</p> <p>3. <code>fa_...Schema.sql</code> Creates the FA user, schema, and all database objects. Replaces manual user creation and <code>fa-new-database-...sql</code>. To be executed by a database user who has permission to create other users. This is an alternative script normally used in non-production environments.</p>	
SQL Server <code>fa-hierarchy-mssql-<version>.sql</code> <code>hierarchy-migration-3.1-to-3.3.sql</code> <code>hierarchy-migration-3.3-to-8.0.sql</code> <code>hierarchy-migration-8.0-to-8.1.sql</code>		The creation and migration scripts for the FA/AA hierarchy database for MSSQL. These scripts are located in the <code>mssql</code> and <code>mssql\migrations</code> directories.
Oracle Not applicable.		

Migration Utilities

This section describes Performance Management Advisors migration utilities.

To migrate metrics added in a release to the Configuration Server, run the Advisors Object Migration Wizard.

NEW Release 8.5.0 introduces additional privileges for role-based access control. When migrating to release 8.5.0, the new privileges are not defined in any existing Advisors role in the Configuration Server settings. An administrative user must update existing roles or create new roles and add the privilege to allow the described access or activity. Role-based access control, including lists of available privileges, is described in the [Contact Center Advisor and Workforce Advisor Administrator User's Guide](#) and the [Frontline Advisor Administration User's Guide](#).

User Migration Utility

A user migration utility is packaged with the Advisors Platform distribution. This utility allows migration of Advisors users from the 3.3, 8.0, or 8.1.0 Advisors Platform database to Genesys Configuration Manager.

The migration tool migrates user and contact records along with user's module access information from the 3.3, 8.0, or 8.1.0 Advisors Platform Database to Configuration Manager.

Specifically the following user information is migrated:

- User name
- Password
- First name
- Last name
- Email
- Employee ID
- Whether the user is an agent or not
- User's module access information
- User's role information

The utility contains a `ReadMe.txt` that summarizes the use of the tool and the procedure to run the tool.

Prerequisites

Before you run the user migration utility, ensure you have a supported version of Java installed and `JAVA_HOME` is added to system classpath.

The supplied Configuration Manager user must have read, create and change permissions on the selected tenant.

Procedure

1. Extract the `user-migration-util-<version>.zip` file from the `advisors-platform-distribution-<version>.zip` file/supplement folder.
2. Go to the `conf` folder in the extracted directory and edit `migration.properties`. Follow the configuration comments in the file and enter the configuration values. Save the file.
3. Open the command prompt and change to the directory where the `migration.bat` file is extracted.
4. Run the following command on the command prompt:
`migration.bat`
5. When the migration is complete, review the log for errors or warnings.

Object Migration Utility

Many of the objects you use to configure the Advisors modules exist in Genesys Configuration Server. That is, what you see in Genesys Configuration Server is what you have to build your Advisors configuration. You use the Advisors Object Migration Wizard to automate the migration of objects from databases to Configuration Server. Any object you will require in your configuration must be either migrated from an earlier release using the Object Migration Wizard, or you must manually create the objects in Configuration Manager.

Be aware of any new privileges added to Advisors for each release. Those new privileges have never been defined in any existing Advisors role in the Configuration Server; they cannot be migrated using a migration utility. To use new privileges added to Advisors in release 8.5.0, an administrative user must update existing roles or create new roles and add the privilege to allow the described access or activity.

The Advisors Object Migration Wizard is packaged with the Advisors Platform distribution. Use of the Object Migration Wizard is one Step in the migration process; for information about the full migration process for your release, see the [Genesys Migration Guide](#).

In general, migration of CCAdv/WA metrics data is a required step of your Contact Center Advisor/Workforce Advisor migration, but migration of other CCAdv/WA objects is optional. If you use Frontline Advisor, migration of FA metrics data is a required step.

You can select only one option at a time for migration, but you can run the migration tool as many times as required to migrate all objects and metrics.

Starting in release 8.5.0, FA no longer has a standalone database. The FA database content moves to the Advisors Platform database. The Object Migration Wizard includes an option in release 8.5.0 to move the FA database content to the Platform database (Frontline Advisor Database Transfer). If you use FA, you must run the FA options in the Object Migration Utility in this order:

1. Frontline Advisor Database Transfer
2. Frontline Advisor Metrics

The object migration wizard provides three paths in release 8.5.0:

- Frontline Advisor Database Transfer – The FA database transfer option moves all FA database content to the Platform database. You must perform the database transfer before migrating FA metrics to Genesys Configuration Server.
- Frontline Advisor Metrics – In release 8.5.0, the FA metrics migration path exports the FA metrics from the Platform database to the Configuration Server. Only those FA metrics that are not present in Configuration Server are migrated. **NEW** Before you use the object migration wizard to migrate FA metrics data, you must manually remove the FA metrics business attribute values. In Configuration Manager, the values are under the default tenant; the path is Business Attributes\Advisors Metrics\Attribute values\Frontline Advisor.
- Contact Center/Workforce Advisor Objects – The CCAdv/WA option migrates the following:
 - Metrics for both CCAdv and WA.
 - Metadata records of contact centers, application groups, and regions (geographic, reporting, and

operating units).

- User permission records for contact centers and application groups.
- Module access privileges of the existing users. Although this option is placed under CCAdv/WFA migration path, it migrates the module privileges for all the Advisors components.

Prerequisites

Ensure a supported version of Java is installed.

If you must run the user migration utility, ensure you run it before running the object migration wizard.

If you are migrating from release 8.1.5 to 8.5.0, the database migration scripts must be executed before running this wizard.

The Configuration Server user supplied must have read, create, and change permissions on the selected tenant.

Procedure

1. Extract the file `advisors-migration-wizard-<version>.jar` from the folder `advisors-platform-distribution-<version>.zip/ip/supplement`.

2. Open the command prompt and change to the directory where the file `advisors-migration-wizard-<version>.jar` is extracted.

3. Run the following command:

```
java -jar advisors-migration-wizard-<version>.jar
```

The migration wizard launches; click Next.

4. Select the migration path and click Next.

You can select only one migration option in a single run of the wizard, but you can run the wizard as many times are necessary to complete your migration.

5. Click your migration option below for information:

[+] Contact Center/Workforce Advisor Objects

a. Select the items you want to migrate from the Advisors database. You can select more than one item at a time, but the following rules apply:

- You must migrate contact center objects before you can migrate contact center permissions.
- You must migrate application groups before you can migrate application group permissions.

Click Next.

b. Select the type of database you use in your enterprise.

If you select Oracle, the wizard also prompts you for the following information:

- Oracle setup – Select the Basic option if you are using a single-instance Oracle database. Select the RAC connectivity setup option to connect to Oracle RAC.
- Oracle JDBC driver location

Click Next.

- c. The **Migration Source Database** screen prompts for connection details for the Platform database. After you enter your information on the screen, click Next.
- d. Enter details about the Genesys Configuration Server to which selected objects are to be migrated. Click Next.
The **Installation Progress** screen displays.
- e. If required, check the details you have entered by using the Show Details button. When the details are correct, click Install to proceed with the migration.
- f. When the migration is complete, review the log for errors or warnings.

[+] Frontline Advisor Database Transfer

- a. Select the type of database you use in your enterprise.
If you select Oracle, the wizard also prompts you for the following information:
 - Oracle setup – Select the Basic option if you are using a single-instance Oracle database. Select the RAC connectivity setup option to connect to Oracle RAC.
 - Oracle JDBC driver locationClick Next.
- b. The **Migration Source Database** screen prompts for connection details for the Frontline Advisor database.
Enter your information, and then click Next.
- c. The **Migration Target Database** screen prompts for connection details for the Platform database.
Enter your information, and then click Next.
- d. The **Database Schema Names** screen prompts for the name of the source database schema that you are migrating, as well as the name of the target database schema to which you are migrating. Enter your information, and then click Next.
The **Installation Progress** screen displays.
- e. If required, check the details you have entered by using the Show Details button. When the details are correct, click Install to proceed with the migration.
- f. When the migration is complete, review the log for errors or warnings.

[+] Frontline Advisor Metrics

- a. Select the type of database you use in your enterprise.
If you select Oracle, the wizard also prompts you for the following information:
 - Oracle setup – Select the Basic option if you are using a single-instance Oracle database. Select the RAC connectivity setup option to connect to Oracle RAC.
 - Oracle JDBC driver locationClick Next.
- b. The **Migration Source Database** screen prompts for connection details for the Advisors Platform database.
After you enter your information on the screen, click Next.
- c. Enter details about the Genesys Configuration Server to which selected objects are to be migrated. Click Next.

The **Installation Progress** screen displays.

- d. If required, check the details you have entered by using the Show Details button. When the details are correct, click Install to proceed with the migration.
- e. When the migration is complete, review the log for errors or warnings.