



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 8.5.1

12/29/2021

Table of Contents

Genesys Performance Management Advisors Deployment Guide	5
New in Release 8.5.1	6
Planning	9
Deployment Summary	11
Prerequisites	13
Prerequisites for Advisors Platform	18
Prerequisites for AGA	26
Prerequisites for ACA	31
Prerequisites for CCAdv and WA	35
Prerequisites for FAAA	43
Additional Resources	46
Create the Advisors Databases	47
Creating a SQL Server Database	48
Creating the Oracle Schema for Advisors	58
Configure Oracle Metrics Data Sources	67
Database Secure Deployment	71
Create the Advisors User Account	74
Advisors Roles	81
Create the Data Manager Base Object Configuration User	105
Deploying Advisors	107
Deploying Components Controlled by Solution Control Server	109
Configuring Advisors as a Solution	112
Deploying Advisors Platform	114
Deploying Advisors Genesys Adapter	127
MCR Extensions	138
Deploying Advisors Cisco Adapter	139
Deploying CCAdv and WA	148
Upgrade CCAdv-ME	159
Deploy Smartphone Client Applications	160
Deploying FAAA	161
Deploying SDS and RMC	167
Automated Installation Options	184
Post Installation Configuration	187
General	188
Cold Standby Configuration and Switchover	189

Change Memory Allocation	193
Change Encrypted Passwords	196
Customize the Advisors Interface	197
Correct Login Page Latency	198
Deploy and Configure Apache	199
Change a JDBC Data Source Configuration	203
Schedule Periodic Statistics Reissue	207
Adjust the Log File Roll and Retention Settings	208
Advisors Platform	211
Change Advisors Cluster Membership	212
Configure Administrative Actions Logs	213
Change the Mail Server Configuration	215
Advisors Genesys Adapter	216
Manage Advisors Stat Server Instances	217
Operation of Stat Server Redundant Pairs	227
Configure the Daily Reset Time for Statistics on a Stat Server	228
Redistribute Statistics Load when Adapters are Added	230
AGA Configuration Parameters	232
Stat Server Configuration Parameters	236
Update AGA Properties in the Database	237
Manage Restart of Multiple Adapters with Single Metrics Database	238
CCAdv and WA	239
Purge Key Action Reports and Historical Alerts	240
Find and Edit XML Generator Properties	243
Configure Resource Management Console Properties	248
Enable and Disable Agent-level Monitoring	250
Configure Metric Graphing Properties	252
Change the Default Service Level Threshold Setting	255
Configuring Forecast Metric Graph Shapes	256
Work with Data Source Database Names	257
JDBC Data Source Error Logging in XML Generator	258
Custom Time Zones	259
Change the Time Profile of Agent Groups Metrics from 5 Minute Sliding to 30 Minute Growing	260
Format Alert Messages sent by Advisors	261
Importing Contact Groups into Advisors	266
Bulk Configuration Overview	276
CCAdv/WA Bulk Configuration - Integrated Mode	277

CCAdv Bulk Configuration – Independent Mode	290
WA Bulk Configuration – Independent Mode	300
FA and AA	312
Verify Server Connections	313
Edit the FA Message Listening Port	314
Configure the Reason Code Statistic Key	315
Enabling and Editing Filtered Metrics	316
Features Overview	321
Advisors Clusters	322
Integration with Solution Control Server and Warm Standby	323
Scaling the Web Services to Increase Capacity	329
Simplified High Availability Architecture	331
Applications, Advisors Servers, and Cluster Nodes	332
Multiple Advisors Deployments on One System	335
Establishing a TLS Connection to Genesys Configuration Server	338
Advisors and the Backup Configuration Server	342
Advisors and the Backup Solution Control Server	343
Data Manager	345
Adapter Stat Server Configuration	355
Encryption for AGA Metrics Database Data (Oracle)	356
FA Dynamic Hierarchy	357
LoggedIn Scripts	362
Discontinuation of the Advisors Browser	363
Providing a User Interface for Users with Visual Impairment	364
Contact Center Advisor Mobile Edition	365
Advisors Software Distribution Contents	370

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

The organization of this Guide is based on the recommended order in which you should approach deployment of Advisors applications.

New in Release 8.5.1

This page describes the major changes to the *Genesys Performance Management Advisors Deployment Guide* in release 8.5.1. To help you understand when Genesys released specific new features or functionality for Performance Management Advisors, or when certain updates or corrections were made to this Guide, changes to this Guide are grouped by Advisors Platform releases.

Introduced with Advisors Platform Release 8.5.101.17

- The minimum supported version of the Adobe Flash Player is now 20.0.0.286.
- Advisors applications support Genesys Stat Server 8.5.1. At the time of this release, Genesys had completed testing with Stat Server release 8.5.102.
- Support has been added for the Oracle database 12c JDBC driver.
- The [Prerequisites for Advisors Platform](#) have been updated with additional information in the following areas:
 - [things to consider](#) before making the connection to the Genesys Configuration Server
 - [prerequisite information](#) about connecting to the Genesys Configuration Server
 - [collecting information](#) to connect to the Genesys Configuration Server
- An [Important note](#) has been added to the [Prerequisites for CCAdv and WA](#) page related to XML Generator and the connection to the Genesys Configuration Server when you are installing XML Generator on an existing Advisors Platform server.
- The list of permissions to assign to the [Advisors User](#) has been updated. Starting with this release, the Advisors User requires additional permissions if you use the Resource Management Console (RMC) to manage agent skills in your enterprise. Related to this, there is a change in the permissions that you assign to the RMC users (that is, the people in your enterprise who manage skills using the RMC) – see [Configuring RMC Users in the Genesys Configuration Layer](#) in the *Genesys Contact Center Advisor and Workforce Advisor Administrator User's Guide*.
- The page in this Guide that describes the use of [LoggedIn scripts](#) has been updated to include information about the use of LoggedIn script-based virtual agent groups (VAG) in the RMC.
- The ProxyPass statement that allows you to access the FA Administration module from the CCAdv/WA Platform server has been updated to include a [timeout value](#). While this is updated in this Guide for Advisors Platform Release 8.5.101.17, Genesys recommends that you add the timeout value for all Advisors 8.5.1 releases.
- Additional information has been added to the [How it Works](#) section of the *Advisors and the Backup Solution Control Server* topic.

Introduced with Advisors Platform Release 8.5.101.09

- The [deployment procedures](#) for the Supervisor Desktop Service (SDS) and the Resource Management Console (RMC) have been updated. The procedures reflect improvements made to the RMC in this release. For information about changes to the configuration of RMC Users in the Genesys environment, see [Configuring RMC Users in the Genesys Configuration Layer](#) in the *Genesys Contact Center Advisor*

and Workforce Advisor Administrator User's Guide.

- You can deploy the Supervisor Desktop Service (SDS) and the Resource Management Console (RMC) on Red Hat Enterprise Linux.
- There are new role-based access control (RBAC) privileges available for the configuration of RMC users. The new privileges provide more control over tasks that each user can perform. For information, see [Advisors Roles](#).
- This Guide now provides more information about configuring the RMC after installing it, including new configuration parameters. For information, see [Configure Resource Management Console Properties](#).
- You can specify at what time each Stat Server is to reset the statistics daily (that is, for the One day/ Growing time profiles). The configuration is applicable to both Contact Center Advisor/Workforce Advisor (CCAdv/WA) and Frontline Advisor (FA) Stat Servers configured on the respective Advisors Genesys Adapter (AGA) instances. For information, see [Configure the Daily Reset Time for Statistics on a Stat Server](#). The [AGA Configuration Parameters](#) page has also been updated to reflect this change.
- Genesys has extended the bulk configuration export utility. You can now use the export utility to generate a copy of your bulk configuration tables from existing application configuration, and the copy contains no redundancies. For information, see the following sections:
 - [Exporting CCAdv/WA configuration using the integrated configuration mode](#)
 - [Exporting CCAdv configuration using the independent configuration mode](#)
 - [Exporting WA configuration using the independent configuration mode](#)

Introduced with Advisors Platform Release 8.5.100.14

- Starting in release 8.5.1, Stat Server registration is no longer done during deployment. Previously, you input Stat Server connection information in installer screens, which registered the Stat Servers. You now execute dedicated database procedures against the Advisors Platform database to:
 - register or remove Stat Server instances
 - add, edit, or remove Stat Server configuration settings related to Advisors

For information, see [Manage Advisors Stat Server Instances](#).

- Some Advisors modules now require integration with Solution Control Server. Advisors now support warm standby high availability for these modules. For information, see [Integration with Solution Control Server and Warm Standby](#).
- CCAdv XML Generator is a standalone module starting in release 8.5.1. You can continue to install it on a system on which you installed Advisors Platform, or you can install XML Generator on a system without Advisors Platform. For information about properties stored in XML Generator files, see [Find and Edit XML Generator Properties](#)
- Starting in release 8.5.1, Advisors Genesys Adapters (AGA) can request statistics for CCAdv configured objects only after you start XML Generator.
- Advisors now support Oracle 12c and Microsoft SQL Server 2012 servers, including SQL Server clustering. Installer screens related to database connection have changed. The **Basic** connection properties for Oracle no longer include SID. Instead, the Oracle service name must be provided. For more flexibility, an **Advanced** connectivity option is available for both Microsoft SSQL and Oracle that allows adding a custom connection string previously prepared in a text file.
- Advisors alert and action management features can accumulate obsolete historical alert and action management report data that the Advisors application never removes automatically. A maintenance procedure is added to the Platform database that can remove the obsolete data based on configurable

criteria. A database administrator can schedule a job or execute the procedure manually to periodically delete CCAdv and WA expired alerts, archived FA threshold violations, or purge key action reports that are associated with expired alerts. For more information, see [Purge Key Action Reports and Historical Alerts](#).

Planning

This page contains information to help you prepare to deploy Genesys Performance Management Advisors.

Before you begin deployment, you will make a plan to meet your specific needs. See the [Genesys Hardware Sizing Guide](#) for information about tested environments for Advisors (architecture, number of users per component per installation, and so on). The information is meant to help you develop sizing guidelines for your enterprise.

Also, before you deploy Advisors, ensure you read the [Prerequisites](#) topic. It provides additional information to help you prepare for your deployment.

General Information about Advisors

The Advisors dashboards are accessed using a commercial browser, such as Mozilla Firefox. Advisors 8.5.x is incompatible with the Advisors browser from pre-8.5.0 releases. See the [Performance Management Advisors](#) section in the [Genesys Supported Operating Environment Reference Guide](#) for information about supported browsers.

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 require the Genesys Configuration Server to be present, along with all its supporting components. Genesys recommends that you review the [Contact Center Objects](#) section in the *Management Framework Deployment Guide* before creating the Advisors business objects; in particular, note that there are specific requirements for [Person objects' user names](#).

NEW Advisors require the Genesys Solution Control Server to be present. Starting in release 8.5.1, some Advisors modules integrate with the Solution Control Server. You require Genesys Management Framework components to support the integration. For those modules, Advisors supports warm standby high availability. See the [General Prerequisites](#) and [Integration with Solution Control Server and Warm Standby](#) sections of this book for more information.

Important

Integration with the Solution Control Server is not optional – it is required in environments that do not use the warm standby setup, as well as those that do.

You must deploy the Contact Center Advisor (CCAdv) 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 CCAdv module, XML Generator, and Genesys metric data sources are deployed and working.

NEW Starting in release 8.5.1, Advisors Genesys Adapters (AGA) can request statistics for CCAdv configured objects only after you start XML Generator. Previously, starting the Advisors Platform server was sufficient to have the CCAdv adapters request statistics for the CCAdv configured objects.

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 and/or Advisors Cisco Adapter
Contact Center Advisor	Advisors Platform	Advisors Genesys Adapter in a Genesys environment
Workforce Advisor	Advisors Platform	Contact Center Advisor
Contact Center Advisor – Mobile Edition	Advisors Platform	Contact Center Advisor
Resource Management Console	Advisors Platform Supervisor Desktop Service	Contact Center Advisor

Important

NEW The startup of CCAdv XML Generator is no longer dependent on Advisors Platform (Geronimo) startup. Previously, Advisors Platform was required on the server on which you were deploying XML Generator, and you had to start Advisors Platform and ensure it was running before you started XML Generator. Starting in release 8.5.1, XML Generator can be installed on a server with Advisors Platform, but that is not required. XML Generator runs independently of Platform.

Deployment Summary

The basic sequence of events for 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.

NEW Advisors now integrate with the Genesys Management Layer. If you have installed earlier releases of Advisors and are familiar with the process, be aware that there are additional tasks required starting in release 8.5.1. See [Integration with the Genesys Solution Control Server](#) for information. The deployment summary below is specific to Advisors deployment; it assumes that you have installed the Local Control Agent (LCA) on any servers that require it, and that you have configured your Application and Host objects. During the deployment of the Advisors components, some installers will prompt you for information about Applications, Hosts, LCA, and the Solution Control Server (SCS).

NEW Also starting in release 8.5.1, you register and manage Stat Servers differently than in previous releases. The Advisors Genesys Adapter installer no longer prompts you for Stat Server information. You now execute dedicated database procedures against the Advisors Platform database to:

- register or remove Stat Server instances
- add, edit, or remove Stat Server configuration settings related to Advisors

See [Manage Advisors Stat Server Instances](#) for information.

See the [Prerequisites](#) and the various deployment procedures in [Deploying Advisors](#) for detailed information.

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 accounts.
3. Install the Platform service (Geronimo) on servers on which you will deploy one of the following Advisors components:
 - Contact Center Advisor Web services

- Workforce Advisor server or Web services
 - Frontline Advisor server or Web services
 - Contact Center Advisor-Mobile Edition server
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
 5. Register the Stat Servers that you plan to use with Advisors.
 6. Install the Advisors components for your enterprise:
 - Contact Center Advisor
 - Workforce Advisor
 - Contact Center Advisor - Mobile Edition
 - Frontline Advisor
 - SDS and Resource Management
 7. Make any required configuration changes.

Prerequisites

This page provides general information about the Genesys Performance Management Advisors deployment environment. Also in the **Prerequisites** section is information specific to each Performance Management Advisors component. Read all prerequisites relevant to the components you will deploy before you begin installation. There is a list of questions to consider for each component. 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 component. The Advisors components are:

- [Advisors Platform](#)
- [Advisors Genesys Adapter](#)
- [Advisors Cisco Adapter](#)
- [Contact Center Advisor and Workforce Advisor](#)
- [Frontline Advisor and Agent Advisor](#)

Integration with the Genesys Solution Control Server

NEW Starting in release 8.5.1, the following Advisors components are controlled with the Solution Control Server:

- Advisors Genesys Adapter
- Advisors CISCO Adapter
- Contact Center Advisor XML Generator
- Workforce Advisor WA Server
- Frontline Advisor FA Server (that is, FA with the rollup engine)

Integration with the Solution Control Server means you must:

- Install the Local Control Agent (LCA) on each system that runs any of the preceding components. See the [Management Framework Deployment Guide](#) for installation of LCA.
- Configure a Host in Configuration Manager or Genesys Administrator for each system that runs any of the preceding components. See [Framework 8.1 Configuration Manager Help](#) or [Genesys Administrator Extension Help](#) for information.
- Configure an Application in Configuration Manager or Genesys Administrator for each Advisors server that runs one or more of the preceding components. See [Framework 8.1 Configuration Manager Help](#) or [Genesys Administrator Extension Help](#) for information.

If you are deploying Advisors in a warm standby configuration, you must also configure a second Application for each Advisors component in Genesys Administrator for the secondary server, and associate the two Applications as a primary and backup pair for failover.

After the Advisors components listed above are installed and controlled by the Solution Control

Server, you can monitor them using the Solution Control Interface (SCI), Genesys Administrator, or Configuration Manager.

For more details, see [Integration with Solution Control Server and Warm Standby](#) and [Deploying Components Controlled by Solution Control Server](#).

Importance of Advisors Platform

Most Performance Management Advisor applications require the installation of Advisors Platform before installation of the application. The applications rely on Advisors Platform to function. The exceptions to this rule are Contact Center Advisor XML Generator, Advisors Genesys Adapter, and Advisors CISCO Adapter, that do not need the Advisors Platform.

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

Licenses

For information about licenses (for example, you might require a license for High Availability), see the [Genesys Licensing Guide](#).

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.

Genesys Management Software

You can use Genesys Administrator for much of the post-deployment configuration associated with Genesys Performance Management Advisors, however you also must have access to the Genesys Configuration Manager to perform some of the administrative functions related to Role-Based Access Control (RBAC). You can use Configuration Manager or Genesys Administrator to define and maintain roles, and associate roles with users. This configuration is stored in the Genesys Configuration Server. There are limitations, however, that prevent you from viewing and editing privileges and permissions for Advisors roles; for those tasks, you require Configuration Manager.

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).

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 2008 or **NEW** Microsoft SQL Server 2012, including SQL Server Cluster. 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 or **NEW** Oracle 12c. 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.

Prerequisites for 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 on at least one system.
- Will you install the applications (FA, CCAAdv, WA) distributed in a cluster on several systems, or all on one system?
- Each system on which you install Advisors Platform or XMLGen is a unique cluster node. What will you use for the node ID?
- Where are you installing Advisors (in which directory)? The default location on Windows 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 support English, German, and French in release 8.5.1.)
- **NEW** Will you later deploy, on this system, one of the following modules?
 - CCAAdv XML Generator
 - Workforce Advisor Server
 - Frontline Advisor Server (with the rollup engine)
 - Resource Management Console

If so, when installing Advisors Platform, you must specify a Configuration Server connection that has permission to change applications and agent groups in the Configuration Layer.

- 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)?
- Plan your **integration of Advisors with Solution Control Server**.
 - Ensure you understand the **limitations and special configuration** requirements when planning which Advisors applications will be installed on a server.
 - If you plan an HA deployment that supports warm standby, you might require an additional license. See **Licenses**.
 - You require a Solution Control Server (SCS), and optionally, the Solution Control Interface (SCI) (you can also use Genesys Administrator or Configuration Manager).

- You must configure Application and Host objects in Genesys Administrator or Configuration Manager for some Advisors modules. See [Integration With Solution Control Server](#).

Prerequisites

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

Y or N	Prerequisite
	A verified Genesys environment must be ready and available.
	<p>In a Genesys environment, you have established connection to the Genesys Configuration Server and to its backup if there is one.</p> <p>NEW If you are later going to deploy one of the following modules on this system, then this connection must have permission to change applications and agent groups in the Configuration Layer:</p> <ul style="list-style-type: none"> CCAdv XML Generator Workforce Advisor Server Frontline Advisor Server (with the rollup engine) Resource Management Console <p>Additionally, if this is a server on which you will later deploy CCAdv XML Generator, Workforce Advisor Server, or the Frontline Advisor Server, you must use a Configuration Server connection that <i>writes</i> to the Configuration Server (avoid using a read-only-type connection to the Configuration Server). The preceding components use the Configuration Server connection properties that you supply during the Advisors Platform installation; these components must be able to write to the Configuration Server to function correctly.</p>
	In a Genesys environment, you have established connection to the Genesys Solution Control Server and to its backup if there is one.
	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 .
	<p>If you plan to connect to the Configuration Server using TLS, you have configured security certificates:</p> <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.

Y or N	Prerequisite
	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 .
	<p>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.</p> <p>[+] Show additional information for Linux environments</p> <ol style="list-style-type: none"> 1. You can start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled: <pre>ssh -X root@<host></pre> 2. As root, place the <code>advisors-platform-installer-<version>.jar</code> file into the Advisors home directory.
	You have created the required Application and Host objects in Genesys Administrator or Configuration Server for any server on which you will install the administration module. If you are configuring Advisors in warm standby mode, then you have configured both primary and backup Applications and associated each primary Application with its backup for failover. See Deploying Components Controlled by Solution Control Server for information.
	<p>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 <i>advisors user</i>, which belongs to the <i>advisors group</i>.</p> <p>[+] Show Steps</p> <ol style="list-style-type: none"> 1. Open the shell. 2. As root, create the Advisors group: <pre>groupadd advisors</pre> 3. As root, create the Advisors user in the Advisors group: <pre>useradd -s /bin/bash -g advisors advisors</pre> <p>The preceding command creates the <code>/home/advisors</code> directory. If you want a different directory, you can use the following command:</p> <pre>useradd -g advisors -d <path to the desired directory> advisors</pre> <p>You can optionally set a password for the Advisors user:</p> <pre>passwd advisors</pre>

Y or N	Prerequisite
	<p>Genesys recommends that you mount /home as a separate partition.</p>
	<p>Install Oracle Java Development Kit (JDK). [+] Help with Linux environments</p> <ol style="list-style-type: none"> 1. 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. 2. 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: <pre>cp ./jdk-7u<version>-linux-x64.tar.gz /home/advisors</pre> 3. Navigate to the Advisors home directory: <pre>cd /home/advisors</pre> 4. As root, unpack the archive and install the JDK: <pre>tar zxvf jdk-7u<version>-linux-x64.tar.gz</pre> 5. As root, change the owner of the installed JDK: <pre>chown -R advisors:advisors jdk1.7.0_<version></pre> 6. As root, change to the Advisors user and test JDK: <pre>su - advisors</pre> <pre>./jdk1.7.0_<version>/bin/java -version</pre> <p>You should see output similar to the following:</p> <pre>java version "1.7.0_40"</pre> <pre>Java(TM) SE Runtime Environment (build 1.7.0_40-b43)</pre> <pre>Java HotSpot(TM) 64-Bit Server VM (build 24.0-b56, mixed mode)</pre>
	<p>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 true to avoid potential lockouts:</p>

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 interface 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 prompts you for the information in the following Table. Default values provided by the installer are entered in the 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, and the default metric name and description language.	
Location and name of the base directory in which you will install Advisors.	<p>Default on Windows:</p> <p><code>C:\Program Files\GCTI\Advisors</code></p> <p>Default on Linux:</p> <p><code>/opt/gcti/advisors</code></p>
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 Advisors on the same machine, use the default values the installer supplies. See Multiple Advisors Deployments on One System for more information.	<p>Default values are:</p> <ul style="list-style-type: none"> HTTP port: 8080 HTTPS port: 8443 AJP port: 8009 JMX port: 9999 Naming (JNDI) port: 1099
This section applies if you are installing the Administration module. You require the name, in Configuration Server, of the primary Solution Control Server Application that you will use with Advisors.	Default value is SCServer.
This section applies if you are installing the Administration module.	Default value for both port

Information	Input
<p>From the Configuration Server, you require:</p> <ul style="list-style-type: none"> the name of the XML Generator application the port number on which that application listens the name of the host associated with that application <p>If you are deploying Advisors in a warm standby configuration, then you require this information for both the primary and backup XML Generator applications.</p>	<p>numbers is 8090.</p>
Node ID for this server in the Advisors cluster. Use letters, numbers, or the dash character. Maximum 16 characters. For more information see Advisors Cluster Information .	
The IP address or host name that other cluster members will use to contact this node (not localhost or 127.0.0.1)	
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.	Default value is 61616.
The local host address (localhost or 127.0.0.1)	
The port numbers 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 values the installer supplies. See Multiple Advisors Deployments on One System for more information.	Default values are 11211 and 11212.
<p>Details to connect to the Genesys Configuration Server:</p> <ul style="list-style-type: none"> The name of the Configuration Server (the Application name, obtained from Genesys Administrator). If you have Configuration Servers configured in High Availability mode, enter the name of the primary Configuration Server. 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> account (see Create the Advisors User Account for information). <p>NEW If you are later going to deploy one of the following modules on this system, then the connection to the Genesys Configuration Server must have permission to change applications and agent groups in the Configuration Layer:</p> <ul style="list-style-type: none"> CCAdv XML Generator Workforce Advisor Server Frontline Advisor Server (with the rollup engine) 	<p>Defaults are:</p> <ul style="list-style-type: none"> Configuration server name: confserv Configuration server port: 2020 Application name: default

Information	Input
<ul style="list-style-type: none"> Resource Management Console <p>Additionally, if this is a server on which you will later deploy CCAdv XML Generator, Workforce Advisor Server, or the Frontline Advisor Server, you must use a Configuration Server connection that <i>writes</i> to the Configuration Server (avoid using a read-only-type connection to the Configuration Server). The preceding components use the Configuration Server connection properties that you supply during the Advisors Platform installation; these components must be able to write to the Configuration Server to function correctly.</p> <p>If you will connect to the Configuration Server using TLS, then you also require the following information:</p> <ul style="list-style-type: none"> The TLS port number for the Configuration Server. 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 Genesys Administrator). The name or IP address of the machine that hosts the backup Configuration Server. The port on which the backup Configuration Server listens. 	
The name of the Object Configuration User account (configured in Configuration Server). See Create the Data Manager Base Object Configuration User for information.	
<p>Will you synchronize user updates between the Configuration Server and the Advisors database?</p> <p>To synchronize user updates, an installation must include the Administration module.</p>	
<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.	
<p>Type of database used in your enterprise (MS SQL or Oracle), 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 Service name for an Oracle installation). 	<p>Default values for port number:</p> <ul style="list-style-type: none"> Oracle: 1521 MS SQL: 1433

Information	Input
<ul style="list-style-type: none">• The Platform database username and password associated with the account that Advisors Platform will use to access the Platform database.• For clustered databases, 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.	
<p>(Optional) If you have enabled the Forgot your 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	

Prerequisites for 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?
- **NEW** Are you configuring multiple AGAs with warm standby? Each primary AGA among the multiple adapters configured should use Stat Servers different from those used by other primary adapters. The primary and the backup AGA in a pair must be configured with the same Stat Servers. See [the section on integrating AGA with SCS and the Management Layer](#).

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.
	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.
	<p>You have located the aga-installer-<version>.jar file on the installation CD and have copied it to the local drive of your server. Place the aga-installer-<version>.jar file into the Advisors home directory.</p> <p>[+] Show additional information for Linux environments</p> <ol style="list-style-type: none"> 1. You can start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled:

Y or N	Prerequisite
	<pre>ssh -X root@<host></pre> <p>2. As root, place the aga-installer-<version>.jar file into the Advisors home directory.</p>
	<p>A verified Genesys environment is ready and available.</p> <p>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.</p>
	<p>You have installed the Local Control Agent (LCA) on the server on which you will deploy AGA. See Integration with Solution Control Server and Warm Standby for more information about integrating Advisors with the Genesys Management Framework.</p>
	<p>You have a Solution Control Server (SCS) available and configured to communicate with the LCAs on the Advisors servers.</p>
	<p>You have created the required Application and Host objects for each AGA instance in Genesys Administrator. If you are configuring Advisors in warm standby mode, then you have configured both the primary and backup Applications and associated the two Applications as a primary and backup pair for failover. See Deploying Components Controlled by Solution Control Server for information.</p>
	<p>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.</p>
	<p>If the T-Server is the Avaya Communication Manager, make sure that the T-Server option query-agent-work-mode is set to on-restart. This is the default option. To set this option, go to TServer > Option tab > T-Server Option and locate query-agent-work-mode. This setting is required for the AfterCallWork state changes to be visible.</p>
	<p>All the Stat Server configurations are updated with the statserverEntries.cfg options file supplied with Genesys Adapter. Alternatively, you have reviewed the statserverEntries.cfg file and manually updated the Stat Server options with options recommended in the file.</p>
	<p>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.</p>

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).	
Location and name of the base directory in which you will install Advisors.	<p>Default on Windows:</p> <p>C:\Program Files\GCTI\Advisors\</p> <p>Default on Linux:</p>

Information	Input
	/opt/gcti/advisors
Path to the directory in which log files will be written.	C:\Program Files\GCTI\Advisors\ Default on Linux: /opt/gcti/advisors
Location of the Java Development Kit (root directory).	
Type of database used in your enterprise (MS SQL or Oracle). For an Oracle installation, the location of the JDBC driver.	
Connection details to the AGA metrics database: <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 Service name for an Oracle installation) The username and password associated with the account that modules will use to access the Metrics Graphing database For clustered databases, 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. 	Default database port is 1433.
Connection details to the Advisors Platform database (use the same database configuration that was specified when the Advisors Platform database was configured): <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 Service name for an Oracle installation) The username (schema for clustered databases or an Oracle environment) and password associated with the account that modules will use to access the Platform database. For clustered databases, 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. 	Default database port is 1433.

Information	Input
<p>Connection details to the Genesys Configuration Server:</p> <ul style="list-style-type: none"> The name of the Configuration Server (the Application name, obtained from Genesys Administrator). If you have Configuration Servers configured in High Availability mode, enter the name of the primary Configuration Server. 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 'Advisors User'. <p>If you will connect to the Configuration Server using TLS, then you also require the following information:</p> <ul style="list-style-type: none"> The TLS port number for the Configuration Server. 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 Genesys Administrator). The name or IP address of the machine that hosts the backup Configuration Server. The port on which the backup Configuration Server listens. 	<p>Default port that the configuration server is listening on is 2020.</p>
<p>For integration with the Solution Control Server:</p> <ul style="list-style-type: none"> The name of the AGA Application; this information must match the information in Configuration Server. If you are deploying Advisors in a warm standby configuration, then you require this information for both the primary and backup AGA Applications. The port number on which the server's LCA listens. The name, in Configuration Server, of the Solution Control Server Application that you will use with Advisors. 	<p>Default LCA port is 4999.</p> <p>Default SCS application name is SCServer.</p>
<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 IP address of the AGA server. A description of the AGA server (for example, Advisors Genesys Adapter for CCAAdv/WA). 	<p>Default port number is 7000.</p>

Information	Input
<ul style="list-style-type: none">• In an Oracle environment, 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.	

Prerequisites for 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?
- **NEW** Are you deploying ACA in a warm standby configuration? See [Integration with Solution Control Server and Warm Standby](#) and [Deploying Components Controlled by Solution Control Server](#) for information.

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.
	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.
	<p>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.</p> <p>If you are deploying Advisors Cisco Adapter on a Linux system, you must first place the <code>aca-installer-<version>.jar</code> file into the Advisors home directory.</p> <p>[+] Show Additional Information</p> <p>a. You can start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled:</p>

Y or N	Prerequisite
	<pre>ssh -X root@<host></pre> <p>b. As root, place the <code>aca-installer-<version>.jar</code> file into the Advisors home directory.</p>
	You have installed the Local Control Agent (LCA) on the server on which you will deploy ACA. See Integration with Solution Control Server and Warm Standby for more information about integrating Advisors with the Solution Control Server in the Genesys Management Framework.
	You have a Solution Control Server (SCS) available and configured to communicate with the LCAs on the Advisors servers.
	You have created the required Application and Host objects for each ACA instance in Genesys Administrator. If you are configuring Advisors in warm standby mode, then you have configured both the primary and backup Applications and associated the two Applications as a primary and backup pair for failover. See Deploying Components Controlled by Solution Control Server for information.

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.	<p>Default on Windows:</p> <p>C:\Program Files\GCTI\Advisors</p> <p>Default on Linux:</p> <p>/opt/gcti/advisors</p>
Path to the directory in which log files will be written.	<p>Default on Windows:</p> <p>C:\Program Files\GCTI\Advisors</p> <p>Default on Linux:</p> <p>/opt/gcti/advisors</p>
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 each database server. • The AW database name. • The HDS database name. 	<p>Default port number for AWDB is 1433.</p> <p>Default port number for the HDS database is 1127.</p>

Information	Input
<ul style="list-style-type: none"> • Port number on which each database listens. • The username and password associated with the account that ACA will use to access each database. 	
<p>Type of database used in your enterprise (MS SQL or Oracle).</p> <p>For an Oracle installation, the location of the JDBC driver.</p>	
<p>Connection details to the ACA database:</p> <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 Service name for an Oracle installation). • Port number on which the database listens. • The ACA database username (the schema for clustered databases or an Oracle installation) and password associated with the account that ACA will use to access the database. • For clustered databases, 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>Default database port is 1433.</p>
<p>Connection details to the Genesys Configuration Server:</p> <ul style="list-style-type: none"> • The name of the Configuration Server (the Application name, obtained from Genesys Administrator). If you have Configuration Servers configured in High Availability mode, enter the name of the primary Configuration Server. • 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 'Advisors User'. <p>If you will connect to the Configuration Server using TLS, then you also require the following information:</p> <ul style="list-style-type: none"> • The TLS port number for the Configuration Server. • 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 Genesys Administrator). 	<p>Default port on which Configuration Server listens is 2020.</p>

Information	Input
<ul style="list-style-type: none"> The name or IP address of the machine that hosts the backup Configuration Server. The port on which the backup Configuration Server listens. 	
<p>For integration with the Solution Control Server:</p> <ul style="list-style-type: none"> The name of the ACA Application; this information must match the information in Configuration Server. If you are deploying Advisors in a warm standby configuration, then you require this information for both the primary and backup ACA Applications. The port number on which the server's LCA listens. The name, in Configuration Server, of the Solution Control Server Application that you will use with Advisors. 	Default LCA port is 4999.
<p>Connection details for the Advisors Platform database (if you plan to register ACA with the database - this is optional):</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. The Platform database name. Port number on which the database listens (you do not require this information if the server is a named instance). The username (schema for clustered databases or an Oracle installation) and password associated with the account that ACA will use to access the Platform database. For clustered databases, 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. 	Default port is 1433.
<p>For registration with the Platform database (optional):</p> <ul style="list-style-type: none"> The port on which the ACA web services will run (you can use the default port, 7000). 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>Default port is 7000.</p> <p>Default source environment is CISCO.</p>

Prerequisites for CCAdv and WA

Before you deploy Contact Center Advisor (CCAdv), Workforce Advisor (WA), or Alert Management (AM) Administration, it is helpful to answer the following questions:

- Will you deploy the software on a Linux Red Hat or a Windows platform?
- 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?
- Some of these modules require integration with SCS. For details see [Integration with Solution Control Server and Warm Standby](#). Ensure you understand the [limitations and special configuration](#) requirements when planning which Advisors applications to install on a server.
- Will you install the CCAdv application, and if so, will you install it with XMLGenerator and CCAdv Web Services on the same system? Or will you install it in distributed mode, with CCAdv Web Services on different system(s) than the XML Generator? If distributed, which systems will host the XML Generator, and which will host the Web Services?
- Each system on which you install XMLGen is a unique cluster node. What will you use for the node ID?
- Will you install the WA application, and if so, will you install it with WA Server and WA Web Services on the same system? Or will you install it in distributed mode, with WA Web Services on different system(s) than the WA Server? If distributed, which systems will host the WA Server, and which will host the Web Services?
- 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.
- Where did you install Advisors Platform on this system? When installing a module that depends on Platform, its installation directory must be the same as the directory where Platform was installed.

Prerequisites

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

If you have already installed Advisors Platform on the same system, then you will have done many of these tasks. If you are installing CCAdv XML Generator on a system on which Platform is not installed, then you must do them.

Y or N	Prerequisite
	All Modules
	A verified Genesys environment must be ready and available.
	In a Genesys environment, you have established connection to the Genesys Configuration

Y or N	Prerequisite
	Server.
	If you primarily use Genesys Administrator as your management user interface, ensure you also have access to Configuration Manager. You can use Configuration Manager or Genesys Administrator to define and maintain roles, and associate roles with users (Role-Based Access Control). There are limitations, however, that prevent you from viewing and editing privileges and permissions for Advisors roles; for those tasks, you require Configuration Manager.
	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 .
	<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>
	<p>Advisors Platform is successfully installed on each system on which you will install all modules (it is no longer required for CCAdv XML Generator).</p> <p>(For Cisco installations, no adapter is required.)</p>
	You have located the ccawa-installer- <version>.jar file on the installation CD and have copied it to the local drive of your server.
	CCAdv XML Generator
	In a Genesys environment, you have established connection to the Genesys Solution Control Server and to its backup if there is one.
	You have installed the Local Control Agent (LCA). See Integration with Solution Control Server and Warm Standby and Deploying Components Controlled by Solution Control Server for more information.
	You have created the required Application and Host objects in Genesys Administrator or Configuration Server. If you are configuring Advisors in warm standby mode, then you have configured both primary and backup Applications and associated each primary Application with its backup for failover. See Integration with Solution Control Server and Warm Standby and Deploying Components Controlled by Solution Control Server for more information.
	<p>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 Metrics Data Sources.</p>
	For Genesys installations, the Advisors Genesys Adapter is installed.
	You have set the Regional and Language options to the locale for which you want the servers to be deployed.

Y or N	Prerequisite
	Workforce Advisor Server
	In a Genesys environment, you have established connection to the Genesys Solution Control Server.
	You have installed the Local Control Agent (LCA). See Integration with Solution Control Server and Warm Standby and Deploying Components Controlled by Solution Control Server for more information.
	You have created the required Application and Host objects in Genesys Administrator or Configuration Server. If you are configuring Advisors in warm standby mode, then you have configured both primary and backup Applications and associated each primary Application with its backup for failover. See Deploying Advisors in Warm Standby Mode for information.
	<p>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 [IP address of WFM server] [Associated Configuration Manager host name for the WFM instance]</pre> <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>

Collect Information

During deployment of Contact Center Advisor/Workforce Advisor, the installer will prompt you for the information in the following Table. Default values provided by the installer are entered in the 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 CCAAdv/WA modules must be the same as the directory where Advisors Platform was installed. Contact Center Advisor XML Generator does not require Platform, so can be installed independently.</p>	<p>Default on Windows:</p> <p>C:\Program Files\GCTI\Advisors</p> <p>Default on Linux:</p>

Information	Input
	/opt/gcti/advisors
Location of the Java Development Kit (root directory).	
Contact Center Advisor XML Generator	
<p>Connection details to the Genesys Configuration Server:</p> <ul style="list-style-type: none"> The name of the Configuration Server (the Application name, obtained from Genesys Administrator). If you have Configuration Servers configured in High Availability mode, enter the name of the primary Configuration Server. 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 XML Generator will use to log in to the Configuration Server (for example, default). The user name and password of the account that XML Generator will use to connect to the Configuration Server. This is the 'Advisors User'. <div> <p>Important</p> <p>NEW If you are installing CCAAdv XML Generator on an existing Advisors Platform server, you must use the Configuration Server connection properties that were provided during the Advisors Platform installation. See also the Advisors Platform installation prerequisites for additional information.</p> </div> <p>If you will connect to the Configuration Server using TLS, then you also require the following information:</p> <ul style="list-style-type: none"> The TLS port number for the Configuration Server. 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 Genesys Administrator). The name or IP address of the machine that hosts the backup Configuration Server. The port on which the backup Configuration Server listens. 	<p>Defaults are:</p> <ul style="list-style-type: none"> Configuration server name: confserv Configuration server port: 2020 Application name: default
The name of the Object Configuration User account (configured in Configuration Server). See Integration with Solution Control Server for information.	
<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 default tenant selected on each Advisors suite installation must be a different</p>	

Information	Input
tenant. The default tenant configuration is selected when installing the Advisors Platform server.	
The name, in Configuration Server, of the XML Generator Application. See Integration with Solution Control Server and Warm Standby for more information.	
The name, in Configuration Server, of the primary Solution Control Server application.	Default is SCServer.
The port number on which Local Control Agent listens on this system.	Default is 4999.
Node ID for this server in the Advisors cluster. Use letters, numbers, or the dash character. The maximum 16 characters. For details see Advisors Cluster Information .	
The IP address or host name that other cluster members will use to contact this node (not localhost or 127.0.0.1).	
The local host address (localhost or 127.0.0.1).	Default is localhost.
The HTTP port number the members of the cluster will use to communicate with XML Generator. If you are going to install two different deployments of XML Generator on the same machine see Multiple Advisors Deployments on One System for how to choose this port number.	Default is 8090.
The Java Messaging Service port number the members of the cluster will use to communicate with XML Generator. If you are going to install two different deployments of XML Generator on the same machine see Multiple Advisors Deployments on One System for how to choose this port number.	Default is 61616.
The port number the cluster's distributed caching will use to communicate with XML Generator. If you are going to install two different deployments of XML Generator on the same machine see Multiple Advisors Deployments on One System for how to choose this port number.	Defaults are 11211 and 11212.
The maximum number of times that XML Generator should attempt to connect to a database if there is a connection failure. This parameter is applicable to retry attempts when XML Generator is already running; that is, after establishing connections at startup.	Default is 32 times.
The number of seconds between CCAdv 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.	Default is 30 seconds.
The following details for the SMTP (mail) service that XML Generator will use to send e-mail: <ul style="list-style-type: none"> The host name or IP address of the SMTP server that XML Generator will use to send e-mail. (Optional) The address from which XML Generator will send notification e-mail about alerts. 	

Information	Input
<ul style="list-style-type: none"> The address to which to send notification e-mail for support staff concerning issues with XML Generator. This address will also appear in the From: header of these types of e-mail. 	
<p>Frequency (in seconds) at which CCAdv 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>	Default is 120 seconds.
<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>	Default is 60 seconds.
Should graphs display values from the previous day? Do <i>not</i> check the Start at midnight box if you want graphs to display values from the previous day.	
<p>What are XML Generator's 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 (Genesys or Cisco) (optional) the display name the threshold update delay—how long CCAdv will wait for new data from this data source before notifying users on the CCAdv dashboard, and, if configured to do so, administrators by 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"> 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? Interval (ms) for purging the charting local cache from the server. Delay for retries on a failed response (ms). Number of retries on a failed response. Device refresh interval (ms) for the client views when auto-refresh is enabled. 	<p>Defaults are:</p> <ul style="list-style-type: none"> Interval for purging: 500 ms. Delay for retries: 1000 ms. Number of retries: 10. Device refresh interval: 60000 ms.

Information	Input
Time intervals for trend charting.	Defaults are: <ul style="list-style-type: none"> • Period one: 30 min. • Period two: 60 min. • Period three: 120 min.
Workforce Advisor Server	
The name, in Configuration Server, of the WA Server Application.	
The name, in Configuration Server, of the Solution Control Server application.	Default is SCServer.
The port number on which Local Control Agent listens on this system.	Default is 4999.
Specify your workforce management data sources (IEX TotalView, Aspect eWFM, Genesys WFM).	
The 'From' address WA puts in e-mail it sends about alerts to users that are members of distribution lists configured in the Administration module.	
If you are using WFM data from IEX TotalView , then specify: <ul style="list-style-type: none"> • the port number on which the FTP connection in WA listens for data from TotalView. 	Default port number is 6021.
If you are using WFM data from Aspect eWFM , then specify: <ul style="list-style-type: none"> • 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. 	
If you are using WFM data from Genesys WFM , then specify: <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. • 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 on each polling. 	Default values are: <ul style="list-style-type: none"> • Application name: WFM_Server • User ID: 0 (no user.) • Polling interval: 1800000 ms. (30 minutes.) • Number of hours of forecast metric to retrieve: 24 hours.
CCAdv XML Generator, CCAdv Web Services, Workforce Advisor Server, and Workforce Advisor Web Services	
The time profile to use for default historical metrics that you want to display for agent 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.	Default is 5 minutes sliding.
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	

Information	Input
<p>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), 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 Service name for an Oracle installation) • The username (the schema for clustered databases or an Oracle installation) and password associated with the account that modules will use to access the Platform database • For Oracle environments, the location of the JDBC driver. • For clustered databases, 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>Default values for port number:</p> <ul style="list-style-type: none"> • Oracle: 1521 • MS SQL: 1433
<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 if the server is a named instance). • The Metrics Graphing database name (the Service name} } for an Oracle installation). • The username and password associated with the account that modules will use to access the Metrics Graphing database. • For clustered databases, 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>Default values for port number:</p> <ul style="list-style-type: none"> • Oracle: 1521 • MS SQL: 1433

Prerequisites for FAAA

Before you deploy Frontline Advisor/Agent Advisor (FAAA), 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)?
- The FA Server requires integration with the Solution Control Server. For details see [Integration with Solution Control Server and Warm Standby](#). Ensure you understand the [limitations and special configuration](#) requirements when planning which Advisors applications to install on a server.

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.
	You have installed the Local Control Agent (LCA). See Integration with Solution Control Server and Warm Standby and Deploying Components Controlled by Solution Control Server for more information.
	You have created the required Application and Host objects in Genesys Administrator or Configuration Server. If you are configuring Advisors in warm standby mode, then you have configured both primary and backup Applications and associated each primary Application with its backup for failover. See Integration with Solution Control Server and Warm Standby and Deploying Components Controlled by Solution Control Server for more information.
	In a Genesys environment, you have established connection to the Genesys Solution Control Server.
	The FA hierarchy is configured on the Genesys Configuration Server and you can identify

Y or N	Prerequisite
	<p>the following:</p> <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
	<p>You have located the <code>fa-server-installer-<version>.jar</code> file on the installation CD and have copied it to the local drive of your server. Copy the installation file to the Advisors home directory.</p> <p>[+] Show additional information for Linux environments</p> <ol style="list-style-type: none"> Ensure the Advisors Platform service has been installed. The Advisors Platform service hosts the FA application. Open the shell. Start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled: <pre>ssh -X root@<host></pre> As root, copy the <code>fa-server-installer-<version>.jar</code> file to the <code>/home/advisors</code> directory. <pre>cp ./fa-server-installer-<version>.jar /home/advisors</pre>
	<p>If you primarily use Genesys Administrator as your management user interface, ensure you also have access to Configuration Manager. You can use Configuration Manager or Genesys Administrator to define and maintain roles, and associate roles with users (Role-Based Access Control). There are limitations, however, that prevent you from viewing and editing privileges and permissions for Advisors roles; for those tasks, you require Configuration Manager.</p>

Collect Information

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

Information	Input
<p>Location and name of the base directory in which you will install Advisors.</p> <p>(The installation directory for Frontline Advisor server must be the same as the directory where Advisors Platform was installed.)</p>	<p>Default on Windows:</p> <p><code>C:\Program Files\GCTI\Advisors</code></p> <p>Default on Linux:</p> <p><code>/opt/gcti/advisors</code></p>
<p>Are you running FA in standalone or distributed mode? If distributed, which FA instance (on which server) will be responsible for data aggregation? Only one FA instance in a cluster can be responsible for data aggregation; you must enable the rollup engine on this instance. In a warm standby configuration, however, you must enable the rollup engine</p>	

Information	Input
on both the primary and backup applications. The two applications do not run simultaneously, and in the event of failover, the backup must be able to continue the data aggregation processes.	
<p>You require the following information to integrate with the Genesys Management Layer if you are installing the FA Server (FA that includes the rollup engine):</p> <ul style="list-style-type: none"> The FA Server Application name exactly as it appears in Configuration Server. The port number on which the server's LCA listens. The name, in Configuration Server, of the Solution Control Server Application that you will use with Advisors. 	<p>Default LCA port is 4999.</p> <p>Default name of the SCS is SCServer.</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>Default tenant name is Resources.</p> <p>Default path to the hierarchy is Agent Groups\\Enterprise.</p>
<p>Type of database used in your enterprise (MS SQL or Oracle), 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 on which the database listens (you do not require this information if the server is a named instance). The Platform database name (the Service name 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 clustered databases, 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>Default database server name is localhost.</p> <p>Default port on which the Platform database listens is 1433.</p>
<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. 	

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 Advisors chapter in the *Migration Guide* also includes information about the Performance Management Advisors migration wizards and utilities.

Tip


Information about updating your Advisors product suite to release 8.5.1 is available in a standalone *Advisors Migration Guide*, which is available at docs.genesys.com/Documentation/PMA.

- 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*.
- The *Genesys Management Framework Deployment Guide* and *Management Layer User's Guide* contain information about the Solution Control Server and the Local Control Agent.

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.

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 servers where it is required for Advisors components.**
 - Contact Center Advisor Web Services
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. Register the Stat Servers that you plan to use with Advisors.
6. **[+] 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
7. 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.

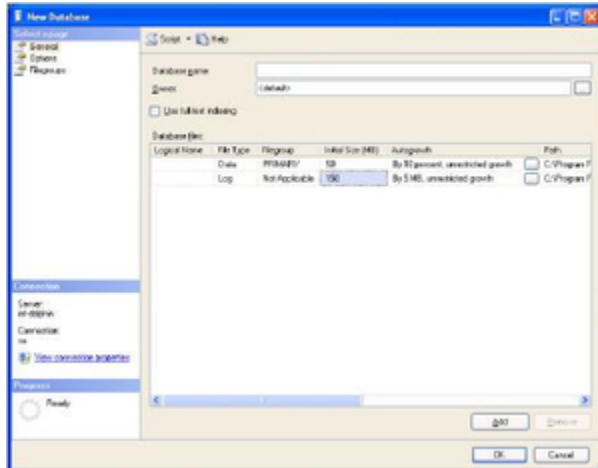
2. In the object explorer right-click on Databases and choose New Database. Open the General screen and configure the following properties. See the Figure that follows—Database Properties - General—as an example.

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. 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

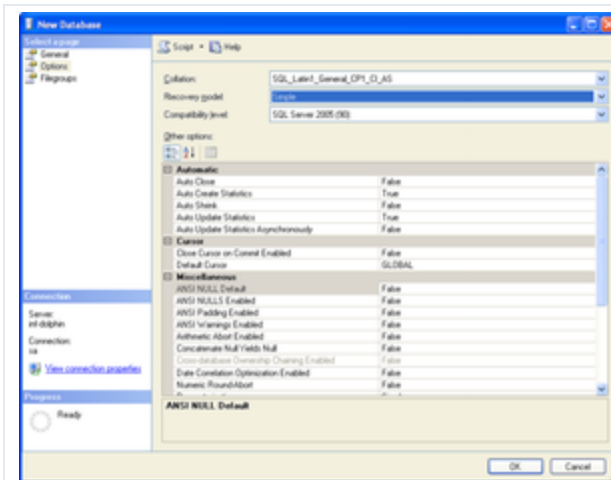
3. Open the Options screen.

- 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.



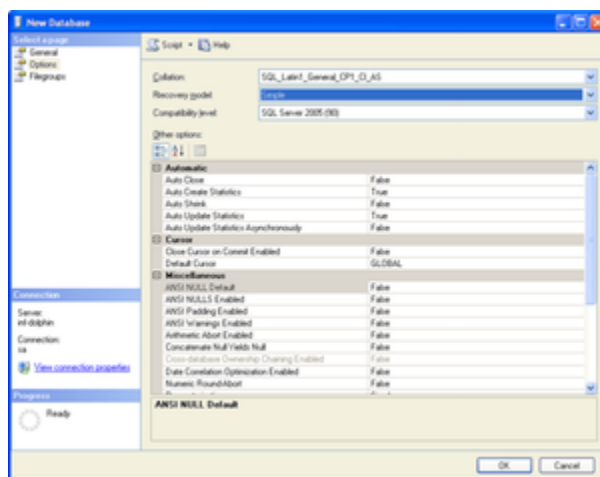
Database Properties - Options

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.

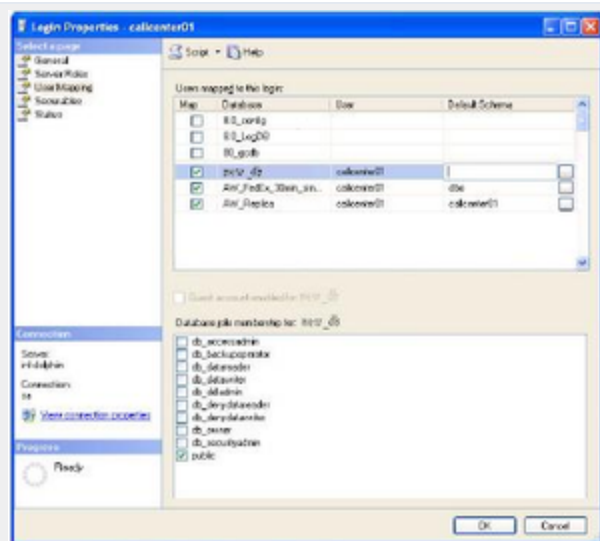
-| Create login for DB=

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.



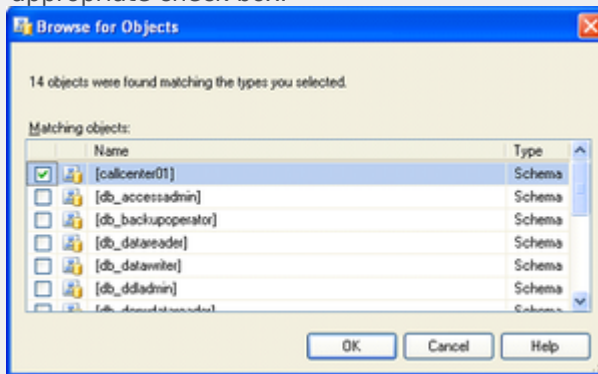
Server-level Security

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

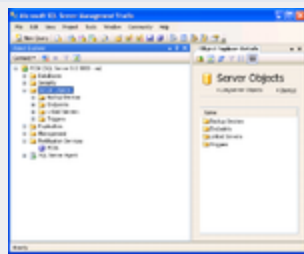
A linked server is normally not required to access the Advisors Genesys Adapter metrics database except in some uncommon cases when the Genesys Adapter metrics database and platform database reside on separate MSSQL Servers. However, each view in the Genesys Adapter metrics database must be accessible 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

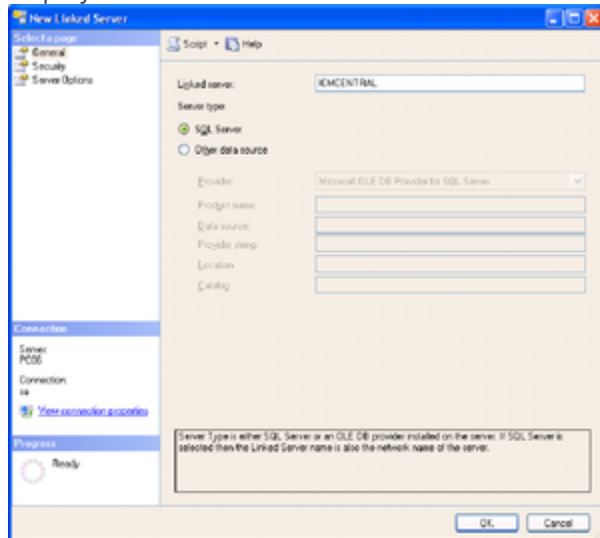
These two views must be accessible by the Platform user, also.

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

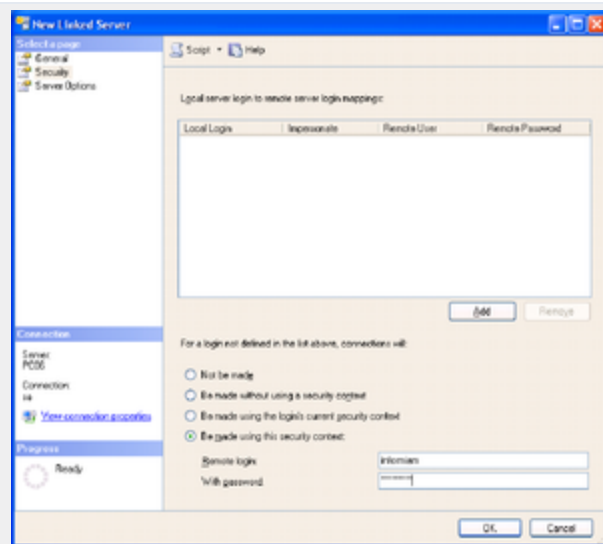
3. Under Server type, select SQL Server.

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:

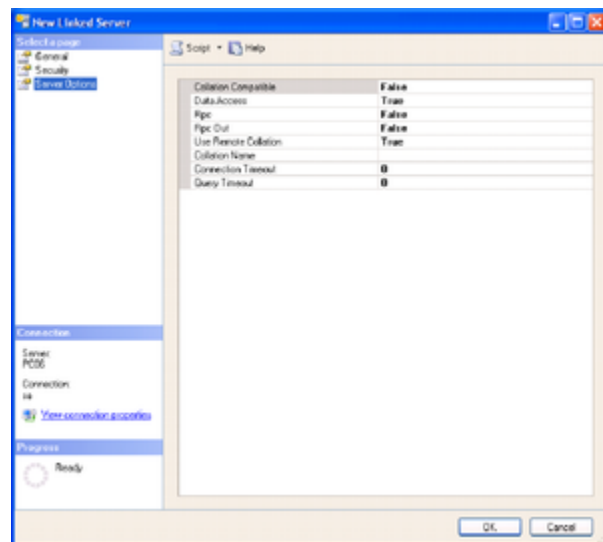
- Select Be made using this security context.
- Specify the remote login and password created by the external administrator for access to the external database.



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

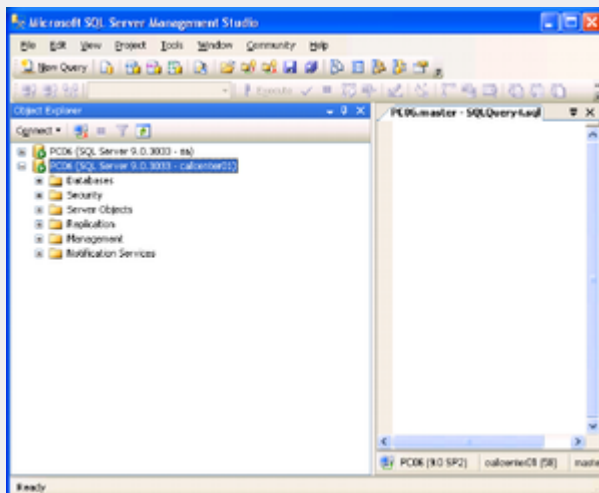
7. To test the linked server connectivity, run some SQL statements from the Microsoft SQL Server Management Studio.

- 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 the Oracle Schema for Advisors

This page describes how to create a generic Oracle schema for Advisors. Each individual Oracle schema 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 Database Administrator (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 in the Advisors release 8.5.0 documentation 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. 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 for the oracle instance contained in the local tnsnames.ora file>

It is important to use <alias for 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=

Procedure: Creating the Advisors Oracle Schema

Steps

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. Database scripts are encoded in Windows-1252 format. Before you start SQL*Plus, be sure to set your session to a value with this encoding. See the Oracle [NLS_LANG FAQ](#) for more information. Set the NLS_LANG variable and start SQL*Plus.

The figure below shows an example of the commands for Linux and Oracle 11g.

```
login as: oracle
oracle@inf-rac2's password:
Last login: Mon Apr 18 15:56:29 2016 from ca-to-a
[oracle@inf-rac2 ~]$ export NLS_LANG=AMERICAN_AMERICA.WE8MSWIN1252
[oracle@inf-rac2 ~]$ echo $NLS_LANG
AMERICAN_AMERICA.WE8MSWIN1252
[oracle@inf-rac2 ~]$ sqlplus /nolog

SQL*Plus: Release 11.2.0.1.0 Production on Mon May 9 20:41:02 2016

Copyright (c) 1982, 2009, Oracle. All rights reserved.

SQL>
```

SQL Command Prompt

5. Using a user account that has DBA privileges (for example, SYSTEM), enter the following at the prompt to connect to the Oracle instance:
conn <User>/<Password>@<alias for the Oracle instance contained in your local tnsnames.ora file>

See the following figure for an example of the command entry.

```
login as: oracle
oracle@inf-rac2's password:
Last login: Mon Apr 18 15:56:29 2016 from ca-to-a
[oracle@inf-rac2 ~]$ export NLS_LANG=AMERICAN_AMERICA.WE8MSWIN1252
[oracle@inf-rac2 ~]$ echo $NLS_LANG
AMERICAN_AMERICA.WE8MSWIN1252
[oracle@inf-rac2 ~]$ sqlplus /nolog

SQL*Plus: Release 11.2.0.1.0 Production on Mon May 9 20:41:02 2016

Copyright (c) 1982, 2009, Oracle. All rights reserved.

SQL> conn system/Oracle01@oradv
Connected.
SQL>
```

SQL Command Prompt 2

6. **NEW** If the tablespaces are already present, you can go to [Step 7](#). Otherwise, create tablespaces as described in this Step.
You can either edit the tablespace script in order to adapt it to your environment, or you can create the tablespaces manually. Genesys recommends that you create at least a dedicated data tablespace and a dedicated temporary default tablespace for each Advisors user/schema.
 - a. You, as a privileged user, or your DBA if you do not have privileged user access, must run the tablespace script contained in the installation package (the script name ends with _TBS.sql). To run the tablespace script, enter @<script name> at the SQL*Plus prompt. For example:
@advisors-platform-8.5.xxx_TBS.sql, if you are creating a Platform schema; or
@gc-metrics-8.5.xxx_TBS.sql, if you are creating an AGA METRICS schema; or
@mg-8.5.xxx_TBS.sql, if you are creating a metric graphing schema.

See the following figure for an example of the command entry. The figure shows an example that uses Linux. The name of the script supplied in the installation package contains the specific release number of Advisors Platform that you will be installing.

```
login as: oracle
oracle@inf-bobcat-10's password:
Last login: Mon Apr 18 14:15:00 2016 from ca-to-a
[oracle@inf-bobcat-10 ~]$ cd /home/oracle/tmp/DeploymentScripts
[oracle@inf-bobcat-10 ~]$ export NLS_LANG=AMERICAN_AMERICA.WE8MSWIN1252
[oracle@inf-bobcat-10 DeploymentScripts]$ echo $NLS_LANG
AMERICAN_AMERICA.WE8MSWIN1252
[oracle@inf-bobcat-10 DeploymentScripts]$ sqlplus / as sysdba

SQL*Plus: Release 12.1.0.2.0 Production on Mon Apr 18 14:22:33 2016

Copyright (c) 1982, 2014, Oracle. All rights reserved.

Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing opt
ions

SQL> alter session set container =bobcat101;
Session altered.

SQL> @advisors-platform-8.5.101.07_TBS.sql
```

SQL Command Prompt 3

- b. When prompted, enter the full path to your base data file directory 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 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 SQL*Plus connection, which you can reuse later in this procedure.

The following figure shows an example.

```
Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing opt
ions

SQL> alter session set container =bobcat101;
Session altered.

SQL> @advisors-platform-8.5.101.07_TBS.sql

*****
Enter a full path to the base data file directory with the trailing slash
(// for Unix-like systems and \ for Windows).
For Example: /u02/app/oracle/oradata/oradb/ (Note trailing slash).
If you want to place the files into a separate folder,
make sure that you create it before you run this script
and include it into the full path.
You can cancel the script at any time by entering ctrl/c
Full base data file directory path with trailing slash=ORADATA/datafile/
```

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. Alternatively, you can run the following query from any Oracle client connected as the system user:


```
SELECT * FROM dba_data_files
```

7. **NEW** Starting with Advisors Platform release 8.5.101.17, you must create a job class with the name GenAdvisorsJobClass before the creation of the Platform schema objects. Only a

privileged user, either you or your DBA, can create the job class. The privileged user must run the `advisors-platform-<version>_DBMS_SCHEDULER.sql` script supplied in the installation package. Verify the results as shown in the following figure.

```

Tablespace creation complete!!
You can verify the installation in runTbsCre.log.
SQL> @advisors-platform-8.5.101-SNAPSHOT_DBMS_SCHEDULER.sql
SQL> column JOB_CLASS_NAME format a30
SQL> column LOGGING_LEVEL format a30
SQL> SELECT JOB_CLASS_NAME, LOGGING_LEVEL
  2 FROM DBA_SCHEDULER_JOB_CLASSES
  3 WHERE JOB_CLASS_NAME='GENADVISORSJOBCLASS';
GENADVISORSJOBCLASS          OFF
SQL>

```

SQL Command Prompt 5

8. **NEW** Create the user/schema and schema objects.

[+] Show steps to create the user/schema and schema objects separately

- a. You, as a privileged user, or your DBA if you do not have privileged user access, must run the user creation script that is contained in the installation package (the script name ends with `_User.sql`). To run the user creation script, enter `@<script name>` at the prompt. For example:
`@advisors-platform-8.5.xxx_User.sql`, if you are creating a Platform schema; or
`@gc-metrics-8.5.xxx_User.sql`, if you are creating an AGA METRICS schema; or
`@mg-8.5.xxx_User.sql`, if you are creating a metric graphing schema.

The script prompts you to enter the user/schema name, the password, the default data and temporary tablespace names, and the SID. Genesys recommends that you create dedicated data and temporary default tablespaces for each Advisors user/schema. Make sure that the tablespaces are created and that you know the names before you start the user/schema creation procedure.

In the local client `tnsnames.ora` file, find the alias for the Oracle instance, and enter it at the SID prompt. For example, if your local client `tnsnames.ora` file contains the following entry for the target Oracle instance, you would enter `bobcat101` at the SID> prompt (note that the alias name is case-sensitive):

```

bobcat101 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = inf-wolf.qalab.com)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl.qalab.com)
    )
  )

```

See the following figure for an example of the command entry.

```

oracle@pltf bobcat 10:~/App/DeploymentScripts
SQL> @advisors-platform-8.5.101_User.sql

*****
The following script creates the platform user/schema
It grants all permissions necessary for Advisors application
You can cancel the script at any time by entering ctrl/c
Enter the database instance alias (SID)
SID? bobcat101
Enter a default tablespace name for platform user(must be already in place)
If skipped USERS tablespace will be assigned as platform default tablespace
> PLT_DATA
Enter a temporary tablespace name for platform user(must be already in place)
If skipped TEMP tablespace will be assigned as platform
default temporary tablespace
> PLT_TEMP
Enter a schema name for the platform db objects
For example: AdvPit
Platform schema name? advisors_plt85101
Enter a password(no special characters) for advisors_plt85101
For example: callcenter01
Password for advisors_plt85101? password123

*****
-- advisors_plt85101's DEFAULT TABLESPACE: PLT_DATA
-- advisors_plt85101's TEMPORARY TABLESPACE: PLT_TEMP
CREATE USER advisors_plt85101 IDENTIFIED BY password123 DEFAULT TABLESPACE PLT_
DATA QUOTA UNLIMITED ON PLT_DATA TEMPORARY TABLESPACE PLT_TEMP;
GRANT CREATE SESSION,CREATE TABLE,CREATE OPERATOR,CREATE TYPE,CREATE CLUSTER,CRE
ATE TRIGGER,CREATE INDEXTYPE,CREATE PROCEDURE,CREATE SEQUENCE,CREATE VIEW,CREATE
 MATERIALIZED VIEW ,CREATE JOB TO advisors_plt85101;
GRANT UNLIMITED TABLESPACE TO advisors_plt85101;
GRANT EXECUTE ON SYS.GENADVISORJOBCLASS TO advisors_plt85101;
CONN advisors_plt85101/password123@bobcat101;
SHOW USER;

PL/SQL procedure successfully completed.

Elapsed: 00:00:00.00

User created.

Elapsed: 00:00:00.38

Grant succeeded.

Elapsed: 00:00:00.07

Grant succeeded.

Elapsed: 00:00:00.01

Grant succeeded.

Elapsed: 00:00:00.08
Connected.
USER is "ADVISORS_PLT85101"
User creation complete!

```

Creating the User/Schema and Schema Objects Separately: SQL
Command Prompt 1

- b. After the script completes and SQL*Plus exits, examine the runUsrCre.log file (located in the same directory as your installation scripts) to verify the results.
- c. Connect as the owner of the Platform schema and execute the object creation script that is contained in the installation package (the script name ends with _ObjectsPlus.sql). To execute the object creation script, enter `@<script name>` at the prompt. For example: `@advisors-platform-8.5.xxx_ ObjectsPlus.sql`, if you are creating a Platform schema; or `@gc-metrics-8.5.xxx_ ObjectsPlus.sql`, if you are creating an AGA METRICS schema; or `@mg-8.5.xxx_ ObjectsPlus.sql`, if you are creating a metric graphing schema.

The script prompts you to enter tablespace names for various groups of tables and indexes, as well as the SID. Genesys recommends that you create dedicated default tablespaces for each Advisors user/schema and that, at the very least, you put the tables into those dedicated default tablespaces. The tablespaces must be created and available after the user/schema is created.

In the local client tnsnames.ora file, find the alias for the Oracle instance, and enter it at the SID prompt. For example, if your local client tnsnames.ora file contains the following entry for the target Oracle instance, you would

enter bobcat101 at the SID> prompt (note that the alias name is case-sensitive):

```
bobcat101 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = inf-wolf.qalab.com)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl.qalab.com)
    )
  )
```

See the following figure; the figure shows empty entries at all prompts for tablespaces, which means that all the data and indexes will go to the default tablespace, which, in this case, is PLT_DATA. For better performance, you can separate indexes, group the tables by I/O patterns. Each prompt for a tablespace represents a table or index group.

```

C:\oracleinf\bobcat101> AmpDeploymentScripts
SQL> conn advisors_plt85101/password123@bobcat101
SQL> show user;
USER is 'ADVISORS_PLT85101'
SQL> @advisors-platform-8.5.101_ObjectsDeflue.sql
*****
The following script creates objects within the current schema
and assigns tables and indexes to the existing tablespaces.
You must be connected as the schema owner in order to run this script.
You can cancel the script at any time by entering ctrl/c
Provide tablespace names for each group of objects when requested
Check the exact names of the existing tablespaces in the result returned
by the following query: select * from user_tablespaces
Press "Enter" key where you want to use
the user default tablespace
Check the user default and temporary tablespaces in the result returned
by the following query: select * from user_users
*****
Enter a tablespace name created for Advisors configuration
Enter a tablespace name created for configuration indexes
Enter a tablespace name created for alerts and threshold violations
*****
Enter tablespace names created for staging area
If only one tablespace is allocated for staging area,
enter the same name on each request
Press "Enter" key everywhere where you want to use
the user default tablespace
*****
Agent activity tablespace name
Queue activity tablespace name
Agent Group activity tablespace name
Merge tablespace name
Index tablespace name for staging
*****
Creating objects. Please wait...
Once the script exits Sql*plus, you can verify the installation in runObjCre.log
Discontinued from Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options
(connected-bobcat101 DeploymentScripts)
  
```

Creating the User/Schema and Schema Objects Separately: SQL Command Prompt 2

If you prefer, you can use SQL Developer, instead of SQL*Plus, to create objects within the schema that you created earlier. You must connect as the owner of the corresponding schema, and then execute the object creation script (the script name ends with either `_ObjectsDefault.sql` or `_ObjectsCustom.sql`). The difference between the two scripts is:

- the `_ObjectsDefault.sql` script silently creates all objects and places them into your default tablespace.
 - the `_ObjectsCustom.sql` script issues prompts, allowing you to place the table groups or indexes into different tablespaces. This script requires an explicit tablespace name on every prompt, even if you want to place the table group into your default tablespace.
- d. After the script completes and SQL*Plus exits, examine the `runUsrCre.log` file (located in the same directory as your installation scripts) to verify the results.

[+] Show steps to create the user/schema and schema objects in one step

If you have privileged user access, you can create the user/schema and the objects in one step. You must use SQL*Plus – and only SQL*Plus – to execute the script.

- a. You, as a privileged user, or your DBA if you do not have privileged user access, must run the script contained in the installation package (the script name ends with `_Schema.sql`). To run the script, enter `@<script name>` at the prompt. For example:
`@advisors-platform-8.5.xxx_Schema.sql`, if you are creating a Platform schema; or
`@gc-metrics-8.5.xxx_Schema.sql`, if you are creating an AGA METRICS schema; or
`@mg-8.5.xxx_Schema.sql`, if you are creating a metric graphing schema.

The script prompts you to enter the user/schema name, the password, the default data and temporary tablespace names, and the SID. Genesys recommends that you create dedicated data and temporary default tablespaces for each Advisors user/schema. Make sure that the tablespaces are created and that you know the names before you start the schema creation procedure.

In the local client `tnsnames.ora` file, find the alias for the Oracle instance, and enter it at the SID prompt. For example, if your local client `tnsnames.ora` file contains the following entry for the target Oracle instance, you would enter `bobcat101` at the `SID>` prompt (note that the alias name is case-sensitive):

```
bobcat101 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = inf-wolf.qalab.com)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl.qalab.com)
    )
  )
```

After the user is created, the script prompts you to enter tablespace names for various groups of tables and indexes. Genesys recommends that, at the very least, you put the tables into the dedicated default tablespaces that you created for each Advisors user/schema. The tablespaces must be created and available before you execute the `_Schema.sql` script.

See the following figure; the figure shows empty entries at all prompts for tablespaces, which means that all the data and indexes will go to the default tablespace, which, in this case, is `PLT_DATA`. For better performance, you can separate indexes, group the tables by I/O patterns. Each prompt for a tablespace represents a table or index group.



Creating the User/Schema and Schema Objects in One Step: SQL Command Prompts

- b. After the script completes and SQL*Plus exits, examine the `runUsrCre.log` and `runObjCre.log` files (located in the same directory as your installation scripts) to verify the results.

No additional action is required if you create the Platform schema with the scripts supplied in the installation package - that is, using only the `advisors-platform-<version>_Schema.sql` script (run by a privileged user), or using the `advisors-platform-<version>_User.sql` script (run by a privileged user) *plus* the `advisors-platform-<version>_Objects<...>.sql` script (run by the Platform user), as described above.

If the user is created in any way other than what is described in this Step, then an additional action is required; see [Step 9](#).

9. If the user is created in any way other than what is described in **Step 8**, then a privileged user, either you or your DBA, must ensure that all privileges listed in the `advisors-platform-<version>_User.sql` script are granted to the Platform user, either directly or through database roles.

Configure Oracle 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

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 servers where it is required for Advisors components.**
 - Contact Center Advisor Web services
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. Register the Stat Servers that you plan to use with Advisors.
6. **[+] 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
7. 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.


Important

You must use Configuration Manager to edit the permissions as described in the following Table; in Genesys Administrator, you cannot edit permissions for everything listed below.

Important

You must grant the Advisors user a privilege that allows that user to create materialized views if you are not using the supplied deployment scripts to create the user.

Object	Permissions	Notes
Applications folder	Execute,  Change	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. Starting with release 8.5.1, Change permission is required so the

Object	Permissions	Notes
		installers can update properties of Application objects that correspond to Advisors servers.
 Hosts folder	Read	Starting with release 8.5.1, Read permission is required on the Hosts folder so that the hosts on which Solution Control Server is deployed can be read from the Configuration Server.
Stat Server Applications	Read	
Tenants	Read	
Agent Groups	Read, Read Permissions, Change, Change Permissions	Starting with release 8.1.5, Change and Change Permissions are required to

Object	Permissions	Notes
		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 with release 8.1.5, Change and Change Permissions are required to propagate changes saved in the Base Object Configuration page to Configuration Server.
	Read, Read Permissions	
Persons	Change	Required only in the following circumstances: <ul style="list-style-type: none"> if the Advisors Administration module will be used to modify user accounts

Object	Permissions	Notes
		<ul style="list-style-type: none"> NEW starting with Advisors Platform release 8.5.101.17, if the Resource Management Console will be used to modify agent skills (the Change permission is required to save the agent skill changes)
NEW Skills	Read	Starting with Advisors Platform release 8.5.101.17, Read permission is required to view skills in the Resource Management Console.
Scripts (of type Interaction Queues)	Read, Read Permissions, Change, Change Permissions	Starting with release 8.1.5, Change and

Object	Permissions	Notes
		Change Permissions are required 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 used to modify user accounts.
Calling lists	Read, Read Permissions, Change, Change Permissions	Starting with release 8.5.0, Change and Change Permissions are required to propagate changes saved in the Base Object Configuration page to Configuration Server.
Roles	Read, Read Permissions	Used to

Object	Permissions	Notes
		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, Delete, Read Permissions, Change Permissions	Used for the Metric Manager beginning in release 8.1.3.
Folders in Persons	Read, Read Permissions	Required for FA.
Folder in Agent Groups	Read, Read Permissions	Required for FA.
SDS Application	Read, Change, Read Permissions	Only required if you deploy Supervisor Desktop Service.

Advisors Roles

You can control access to information in the Contact Center Advisor (CCAdv), Workforce Advisor (WA), and Frontline Advisor (FA) dashboards and in the administration module using roles, and associating permissions and privileges with each role. Controlling information using roles, and associated privileges and permissions, is called Role-Based Access Control (RBAC).

It is typical to require access to various Advisors components early in the deployment and configuration process. The following sections describe Role-Based Access Control (RBAC) in terms of Genesys Performance Management Advisors, and include the list of privileges available with Advisors release 8.5.1.

Important

You must use Genesys Configuration Manager to add or edit privileges associated with roles.

[+] RBAC and Advisors

Performance Management Advisors support role-based access control (RBAC). You can use RBAC to control which users can access specific components—for example, you can use RBAC to configure access to the Advisors administration module for a specific subset of managers.

Advisors applications use Configuration Server business attributes, which means that the Advisors applications can take advantage of Genesys Roles for controlling access at a detailed level to Advisors' business objects and metrics.

RBAC is enforced primarily by visibility in the interface. What a user sees is determined by the Roles which have been assigned. If the user is not assigned a Role that grants him or her access to a piece of functionality, that functionality is not displayed to that user.

There are three important concepts associated with RBAC:

- **Permissions**
Permissions protect access to a whole object; if you have access permissions, you see the entire object.
- **Roles**
Roles protect properties of an object by hiding or disabling those properties to which you want to restrict access. Roles are intended to work with permissions to more finely control what a user can access.
- **Privileges**
Privileges determine what tasks or functions a user can execute on objects to which he or she has access. You assign privileges to Roles to further refine access to objects and object functionality.

What are RBAC permissions?

Elementary permissions protect access to a whole object. Permissions applied to an object apply equally to all properties of the object – if you have access permissions, you see the entire object.

Object permissions determine which users have access to a certain object or to what objects a given user has access. This is done through the use of access groups or on an individual user basis. Objects include the following:

- Contact Center Advisor and Workforce Advisor
 - Metrics
 - Operating Units
 - Reporting Regions
 - Geographic Regions
 - Contact Centers
 - Application Groups
- Frontline Advisor
 - Metrics
 - Levels of the Frontline Advisor hierarchy (that is, the folders and agent groups)

What are RBAC roles?

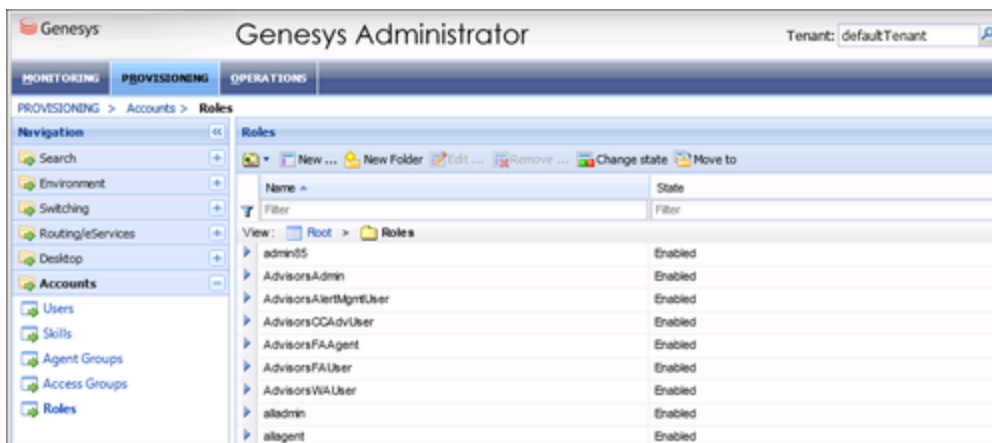
The major component of RBAC is a Role. If it is important in your enterprise to control users' access to information (metrics, hierarchy levels, and business objects), you configure Users and Roles – including the assignment of permissions and privileges to each Role – before any of those users log in for the first time. Each time you have a new user in your enterprise, you assign that person to Roles in a Genesys configuration interface, such as Genesys Administrator.

Roles define what facilities are provided to users to review and manipulate various types of data. These include which property controls are available for items permitted by object permissions, what modules are visible, and access control for entities not represented by configuration objects. A Role is assigned to a User, and that User is then able to do only what that Role permits. One User can be assigned multiple Roles, and one Role can be assigned to multiple Users. A Role may also be assigned to an Access Group, and Users in that Access Group are then able to do what the Role permits.

Different Roles can have different access and allowed functionality for the same objects. In essence, Roles resolve both problems associated with using only permissions – users can access and work with only those parts of the object to which they are allowed.

Roles can also be used to protect access to entities that are not configured as configuration objects, such as logs. In general, when determining the accessibility to an object by a user, the user session cannot retrieve objects if they are not among those objects to which the user has access (as defined by object-access permissions). For data that is available in the session, Role privileges refine what can be done with the data.

Assigning Roles to Users and Access Groups



Roles can be assigned to either Users or Access Groups.

Important

To inherit permissions, Access Groups and Users must belong to the tenant specified during the Advisors Platform installation.

Once a Role is assigned to an Access Group, all Users in the Access Group are assigned that Role. The Access Groups and/or Users must have Read access to the Role to be able to access the Role.

Important

Names of Access Groups must not contain spaces.

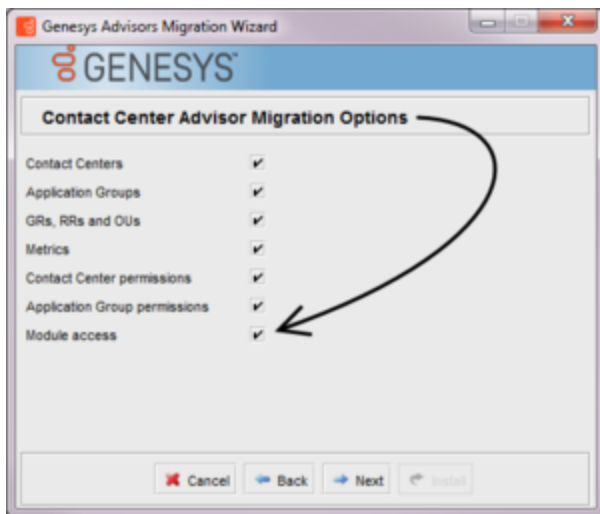
The figure shows an example of Advisors Role configuration.

New Users

By default, new users are not assigned any default Roles. They must be assigned Roles by a system administrator or by an existing user with appropriate permissions.

Default Roles Created by Migration

Module access is determined by the Roles associated with a user's profile. An optional check box on the Advisors migration utility, which is provided in the software distribution package, creates the module access schema. The figure, Migration Wizard, shows the optional **Module access** check box.



Migration Wizard

The utility creates default Roles in the Configuration Server, with each one representing access to a particular module. Each Role has a limited set of privileges associated with it. The default Roles are:

1. AdvisorsAdmin – allows access to the Advisors administration module for Frontline Advisor, Contact Center Advisor, and Workforce Advisor users, to whom you have assigned that Role.
2. AdvisorsFAUser
3. AdvisorsFAAgent
4. AdvisorsCCAdvUser
5. AdvisorsWAUser
6. AdvisorsAlertMgmtUser

You can change the preceding Role names post-migration.

Further Reading on Roles

Additional sources of information on Role-based access, privileges and permissions are:

- [Genesys Security Deployment Guide](#)
- [Genesys Administrator Extension Deployment Guide](#)
- [Framework Configuration Manager Help](#)
- [Genesys Administrator Extension Help](#)

What are RBAC privileges?

Roles consist of a set of role privileges (Read, Change, Execute, and so on). Privileges determine what tasks or functions a user can execute on objects to which he or she has access. You must define Advisors Role privileges in a Genesys configuration interface, such as Genesys Administrator or GAX.

Tip

While you can use any Genesys configuration interface to import Advisors privileges into a Role, or to assign Role-based permissions to Users or Access Groups for access to the Advisors business attributes, you can view the privileges associated with a Role only in Genesys Configuration Manager.

By default, Role privileges are not assigned to any Role, so you must explicitly assign privileges to Roles. Role privileges range from general to very specific tasks. An authorized user, typically a system administrator, bundles these tasks into Roles. The Roles are then assigned to Users. As a result, each User can perform only those tasks for which they have privileges.

Functionality permissions, or privileges, determine what tasks or functions a user can execute on objects to which he or she has access. If a privilege is present in a Role, then any user who is assigned that Role has access to the functionality controlled by that privilege.

Where do I configure roles, permissions, and privileges?

Roles, and related configuration, are stored in the Genesys Configuration Server.

Typically, you configure RBAC in the following order:

1. Add Roles.
2. Add tasks to Roles.
3. Assign Access Groups to Business Attribute instances.
4. Assign Users to Roles.

Use a Genesys configuration interface, such as Genesys Administrator, to add Users to a Role. Add users with one of the following methods:

- indirectly, as a member of an Access Group
- directly, as a member of a role

You also use a Genesys configuration interface to import Advisors privileges into a Role, or to assign Role-based permissions to Persons or Access Groups.

Tip

A user must have Read access to the Role (either directly or through an Access Group) to which he or she is assigned.

Each Advisors privilege name uses the following general structure:

[application name].[module name].[task grouping].[privilege name]

Ensure you copy the exact privilege with no leading or trailing spaces. Some privileges work as single entries; some require a group of privileges to ensure full access as you expect. For the list of privileges for each Advisors component, see the [CCAdv/WA Access Privileges](#) and [FA Access Privileges](#) pages.

Tip

While you can use any Genesys configuration interface to import Advisors privileges into a Role, or to assign Role-based permissions to Users or Access Groups for access to the Advisors business attributes, you can view the privileges associated with a Role only in Genesys Configuration Manager.

Am I limited to a specific number of users, access groups, or roles?

There is no limit on:

- the number of Roles that can be present in the Configuration Server
- the number of Access Groups or Users that can be present in the Configuration Server
- the number of Roles supported by Advisors
- the number of Access Groups that are supported by Advisors

Roles, and the privileges associated with Roles, are cumulative. A single User or Access Group can be assigned multiple Roles. In such cases, the user will have the combined set of privileges granted by each Role. In other words, the user is granted any privilege that is granted by at least one of the assigned Roles. This ensures that the user is able to perform the tasks of all Roles in which they participate.

Each user can also belong to multiple Access Groups, with different permissions coming from each group. In such scenarios, the user's permissions are a union of the permissions of all the Access Groups to which he or she belongs, unless access is specifically denied for one group, which takes precedence (see the following scenarios).

Advisors applications follow the principle of least privilege. The following scenarios show how this union should work:

- User A is part of Access Groups X and Y.
Group X does not have any defined access to a metric.
Group Y has explicit access granted to the metric.
In this case, user A is granted access to the metric.
- User A is part of Access Groups X and Y.
Group X is explicitly denied access to a metric.

Group Y is explicitly given access to the same metric.

In this case, user A is denied access to the metric.

- User A is part of Access Groups X and Y.
Group X is explicitly denied access to a metric.

Group Y does not have any defined access to the same metric.

In this case, user A will be denied access to the metric.

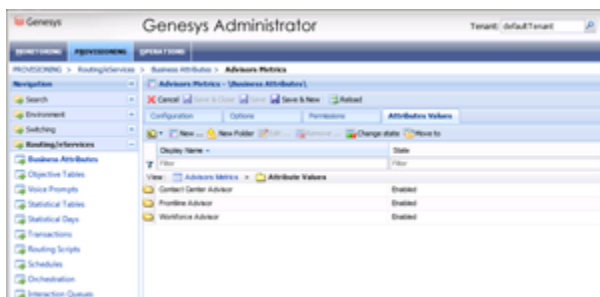
- User A is part of Access Groups X and Y.
Neither group has defined access to the metric.

In this case, user A will be denied access to the metric.

Can I control access to metrics?

Metrics are handled differently than other Advisors business objects. You must add the Advisors metrics in Genesys Configuration Server before you can assign the necessary permissions to Users or Access Groups (you use permissions to control access to metrics (see *What are RBAC permissions?*, above)).

Metrics for Contact Center Advisor, Workforce Advisor, and Frontline Advisor are stored under the Advisors Metrics business attribute; a folder structure segments the metrics for each application and for each object. The following figure shows an example of the folder structure for Advisors metrics. The folder structure shown below is mandatory. The business attributes must be created in the “Default Tenant” chosen during Advisors installation. Click the figure to enlarge it.



Advisors metrics in Genesys Administrator

Each application’s metrics are created under the appropriate folder, and are subdivided by the object types with which they are associated.

To avoid confusion over similarly-named metrics, and because Configuration Server does not allow duplicated names for attribute values, the names of the metrics use a namespace and are case-sensitive. The format of the namespace is:

[Application].[ObjectType].[Channel].[Name]

The values for each characteristic of the namespace are described in the following table:

Namespace characteristic	Definition or values
Application	FrontlineAdvisor, WorkforceAdvisor, or ContactCenterAdvisor
ObjectType	Represents the object type associated with this metric. This could be AgentGroup, Agent, ContactGroup, Application, or Team
Channel	Email, WebChat, Voice, All, or AllNonVoice
Name	The name of the metric

For example, FA metrics would have names like:

- FrontlineAdvisor.Agent.Voice.nch
- FrontlineAdvisor.Team.Voice.taht

[+] Show CCAdv/WA Privileges

The following Tables list all Contact Center Advisor/Workforce Advisor privileges. The Tables include a description of the consequence to the user if the privilege is present or absent.

The Administration module **Users** page is not controlled by an option; all users who can access the Administration module have access to the **Users** page. However, the Users page no longer displays any information about the user accounts, so there is no need to control access to this page. Please refer to the following documents for more information about configuring user profiles:

- [Framework Configuration Manager Help](#)
- [Genesys Administrator Extension Help](#)

Advisors Interface

Privilege	Behavior When Present	Behavior When Absent
Advisors.ChangePassword.canView	User sees the Change Password button located at the top of the Advisors interface.	Change Password button is hidden.
		User does not see options to launch the

Privilege	Behavior When Present Behavior When Absent
<p>NEW Advisors.RMC.canView</p> <p>NOTE: Replaces AdvisorsAdministration.RMC.canView starting with Advisors release 8.5.101.</p> <p>For detailed information about configuring users to access RMC in Advisors release 8.5.101 and later, including which permissions to assign, see Configuring RMC Users in the Genesys Configuration Layer.</p>	<p>can access the Resource Management Console (RMC) from either the CCAdv dashboard or the WA dashboard.</p> <p>the CCAdv dashboard and the WA dashboard.</p>
<p>NEW Advisors.RMC.ManageAgentSkills.canView</p> <p>Introduced in release 8.5.101.</p> <p>For detailed information about configuring users to access RMC in Advisors release 8.5.101 and later, including which permissions to assign, see Configuring RMC Users in the Genesys Configuration Layer.</p>	<p>When the user opens the RMC window from either the CCAdv dashboard or the WA dashboard, there is no Manage Skills pane in the RMC window.</p> <p>When the user opens the RMC window from either the CCAdv dashboard or the WA dashboard, there is no Manage Skills pane in the RMC window.</p> <p>When the user opens the RMC window from either the CCAdv dashboard or the WA dashboard, there is no Manage Skills pane in the RMC window.</p>
<p>NEW Advisors.RMC.ManageAgentStatus.canView</p> <p>Introduced in release 8.5.101.</p> <p>For detailed information about configuring users to access RMC in Advisors release 8.5.101 and later, including which permissions to assign, see Configuring RMC Users in the Genesys Configuration Layer.</p>	<p>When the user opens the RMC window from either the CCAdv dashboard or the WA dashboard, there is no Manage Status pane in the RMC window.</p> <p>When the user opens the RMC window from either the CCAdv dashboard or the WA dashboard, there is no Manage Status pane in the RMC window.</p> <p>When the user opens the RMC window from either the CCAdv dashboard or the WA dashboard, there is no Manage Status pane in the RMC window.</p>

Privilege	Behavior When Present Behavior When Absent
	CCAdv dashboard or the WA dashboard, the Manage Status pane displays in the RMC window and is active.

Contact Center Advisor

Privilege	Behavior When Present Behavior When Absent
<p>ContactCenterAdvisor.ActionManagementReport.canView</p> <p>Introduced in release 8.1.3.</p> <p>NOTE: The privilege to grant access to the Action Management Report in Contact Center Advisor or Workforce Advisor is related to the Alert Management privilege. That is, if a user has the ContactCenterAdvisor.ActionManagementReport.canView privilege, then that user should also have the privilege to view Alert Management (AlertManagement.canView).</p>	<p>User can access an Action Management Report by double-clicking on an Alert tile. Clicking on the tiles in the Map pane does not launch an Action Management Report, and the Action Management Report arrow for alerts in the Alerts pane is not shown.</p> <p>pane, or by clicking on the arrow for each alert in the</p>

Privilege	Behavior When Present	Behavior When Absent
	Alerts pane.	
ContactCenterAdvisor.Dashboard.canView	User can access the CCAdv dashboard. This is a replacement for the module access that was previously assigned on a user-by-user basis.	User cannot access CCAdv dashboard, and the Contact Center Advisor tab is not shown to the user.
ContactCenterAdvisor.Dashboard.AgentGroupsPane.canView	User can see data in the Agent Groups pane.	User sees an empty Agent Groups pane at all times.
ContactCenterAdvisor.Dashboard.ColumnChooser.canView	User has access to the column chooser button on the dashboard.	The column chooser button is not displayed on the dashboard.
ContactCenterAdvisor.Dashboard.EnterpriseStats.canView	User can see the Enterprise row	The Enterprise row is not sent from the server to the dashboard, which means the user does not see it.

Privilege	Behavior When Present Behavior When Absent
	and statistics on the dashboard.
ContactCenterAdvisor.PerformanceMonitor.canView	User can access Performance Monitor. User does not see the Performance Monitor button on the dashboard.
ContactCenterAdvisor.PerformanceMonitor.CallFlowPane.canView NOTE: If both ContactCenterAdvisor.PerformanceMonitor.CallFlowPane.canView and ContactCenterAdvisor.PerformanceMonitor.CurrentCapacity.canView are excluded from a user's role, then the left side of the Performance Monitor window is not displayed to the user.	User can see the Call Flow pane. The Call Flow pane is shown, but no metrics or values are displayed. and metrics in the Performance Monitor window.
ContactCenterAdvisor.PerformanceMonitor.CurrentCapacity.canView NOTE: If both ContactCenterAdvisor.PerformanceMonitor.CallFlowPane.canView and ContactCenterAdvisor.PerformanceMonitor.CurrentCapacity.canView are excluded from a user's role, then the left side of the Performance Monitor window is not displayed to the user.	User can see the Current Capacity pane. The Current Capacity pane is shown, but no metrics or values are displayed. and metrics in the Performance Monitor window.
ContactCenterAdvisor.Dashboard.PivotSelect.canView	User has access to the pivot list that allows them to switch. Drop-down list is not shown in the left pane.

Privilege	Behavior When Present Behavior When Absent
	views of the pivot table.
<p>ContactCenterAdvisor.AlertManagement.canView</p> <p>NOTE: In release 8.1.3, this privilege was replaced with Alert Management-specific privileges.</p>	<p>User has access to the Alert Management tab and the Action Management Report page. User can access the Action Management Report page. The Alert Management tab is not shown; clicking on the tiles in the map does not bring the Action Management Report; and the Action Management Report show for alerts in the Alerts pane is not shown.</p> <p>Management tab, by double-clicking on the alert tiles in the map, or by clicking on the arrow for each alert</p>

Privilege	Behavior When Present
	in the Alerts pane.

Workforce Advisor

Privilege	Behavior When Present
<p>WorkforceAdvisor.ActionManagementReport.canView</p> <p>This privilege is applicable to Release 8.1.3 and later. In a migration scenario, this privilege is 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.</p>	<p>User can access an Action Management Report page by double-clicking on an Alert tile in the Map pane, or by clicking on the arrow for each alert in the Alerts pane.</p> <p>Clicking on the tiles in the Map pane does not launch an Action Management Report page, and the Action Management Report arrow for alerts does not display in the Alerts pane.</p>
<p>WorkforceAdvisor.Dashboard.AgentGroupsPane.canView</p> <p>Introduced in release 8.1.3.</p>	<p>User can see data. User always sees an empty Agent Groups pane with a message stating the lack of access to the Agent Groups pane.</p>
WorkforceAdvisor.Dashboard.canView	User cannot access WA dashboard, and

Privilege	Behavior When Present Behavior When Absent
	can access the Workforce Advisor tab is not shown to the user. WA dashboard.
WorkforceAdvisor.Dashboard.ColumnChooser.canView Introduced in release 8.1.3.	User has access to the Column Chooser button on the dashboard. The Column Chooser button is not displayed on the dashboard.
WorkforceAdvisor.Dashboard.EnterpriseStats.canView Introduced in release 8.1.3.	User can see the Enterprise row in the pivot table (Contact Centers pane). The Enterprise row does not display in the pivot table (Contact Centers pane).
WorkforceAdvisor.Dashboard.PivotSelect.canView NOTE: Because there are additional hierarchies in WA specifically to display agent group contact centers, users must have permission to access the hierarchy grouping (WorkforceAdvisor.Dashboard.PivotSelect.canView) if agent group contact centers are configured. Introduced in release 8.1.3.	User has access to the hierarchy drop-down list on the Contact Centers pane. The hierarchy drop-down list does not display on the Contact Centers pane.

Alert Management

Privilege	Behavior When Present Behavior When Absent
AlertManagement.canView	User Alert Management tab does not display for the user.

Privilege	Behavior When Present Behavior When Absent
Introduced in release 8.1.3.	access to the Alert Management tab.
AlertManagement.ActionManagementReport.canView Introduced in release 8.1.3.	User can create a new Action Management Report. The New and Delete buttons are not displayed in the Action Management Report pane, and the Edit/Delete column is not shown. update or delete an existing report.

Administration Module

Privilege	Behavior When Present Behavior When Absent
AdvisorsAdministration.canView	User has access to the Administration module, and the module tab is not shown to the user. Administration module.
AdvisorsAdministration.SystemConfiguration.canView	User can access System Configuration page. System Configuration option is not shown on the Administration menu. option is shown on menu.
AdvisorsAdministration.Regions.canView	User can access Regions page. Regions option is not shown on the Administration menu. Regions page;

Privilege	Behavior When Present Behavior When Absent
	option is shown on the Administration menu.
AdvisorsAdministration.ApplicationGroups.canView	User can access the Application Groups/Thresholds option is shown on the Administration menu. option shown on menu.
AdvisorsAdministration.ContactCenters.canView	User can access the Contact Centers option is not shown on the Administration menu. option shown on menu.
AdvisorsAdministration.ApplicationConfiguration.canView	User can access the Application Configuration option is not shown on the Administration menu. option shown on menu.
AdvisorsAdministration.AgentGroupConfiguration.canView	User can access the Agent Group Configuration option is not shown on the Administration menu. option shown on

Privilege	Behavior When Present Behavior When Absent
	menu.
AdvisorsAdministration.ContactGroupConfiguration.canView	User can access the Contact Group Configuration option is not shown on the Administration menu. option shown on menu.
AdvisorsAdministration.Metrics.canView	User can access the Report Metrics option is not shown on the Administration menu. option shown on menu.
AdvisorsAdministration.MMW.canCreate Introduced in release 8.1.3.	User can Create function and the Copy function do not display in the Metric Manager. metrics.
AdvisorsAdministration.MMW.canEdit Introduced in release 8.1.3.	Grants privilege to Edit function does not display in the Report Metrics Manager. any metrics.
AdvisorsAdministration.MMW.canDelete Introduced in release 8.1.3.	Grants privilege to Delete function does not display in the Report Metrics Manager. custom metrics.
AdvisorsAdministration.MMW.SourceMetrics.canView	Grants privilege to view the Source Metrics page. The Source Metrics page, and the link to it in the Administration module, do not display.
AdvisorsAdministration.MMW.SourceMetrics.canCreate	Grants Create Source Metrics button

Privilege	Behavior When Present Behavior When Absent
	privilege to delete a page from source metrics. The Delete function does not display on the Source Metrics page.
AdvisorsAdministration.MMW.SourceMetrics.canEdit	Grants privilege to edit the Edit function does not display on the Source Metrics page. source metrics.
AdvisorsAdministration.MMW.SourceMetrics.canDelete	Grants privilege to delete the Delete function does not display on the Source Metrics page. custom source metrics.
AdvisorsAdministration.DistributionLists.canView	User can access the Distribution Lists option is not shown on the Administration menu. page; option shown on menu.
AdvisorsAdministration.ManualAlerts.canView	User can access the Manual Alerts option is not shown on the Administration menu. page; option shown on menu.
AdvisorsAdministration.AlertManagement.AlertCauses.canView	User can access the Alert Causes option is not shown on the Administration menu. page; option shown on

Privilege	Behavior When Present Behavior When Absent
AdvisorsAdministration.AlertManagement.KeyActions.canView	<p>menu.</p> <p>User can access the Key Actions option is not shown on the Administration menu.</p> <p>option shown on menu.</p>
AdvisorsAdministration.GenesysAdapter.Configuration.canView	<p>User can access the Genesys Adapter Configuration section (which includes the Object Configuration and Manage Adapters options) is not shown on the Administration menu.</p> <p>option shown on menu.</p>
<p>AdvisorsAdministration.RMC.canView</p> <p>NOTE: The AdvisorsAdministration.RMC.canView privilege is discontinued starting with Advisors release 8.5.101; Advisors.RMC.canView and AdvisorsAdministration.RMC.Notifications.canView replace it.</p> <p>If your existing Advisors installation includes AdvisorsAdministration.RMC.canView, and you migrate to Advisors release 8.5.101 or higher, the AdvisorsAdministration.RMC.canView privilege remains in your installation, but Advisors ignores it. You must add the Advisors.RMC.canView privilege to provide user access to the RMC and the AdvisorsAdministration.RMC.Notifications.canView privilege to maintain the role-based access control of RMC notification lists and templates in the Administration module.</p>	<p>User can access the Resource Management-related pages in the Administration module.</p> <p>Control Panel section (which includes the Notification Lists and Notification Templates options) is not shown on the Administration module menu.</p> <p>Notification Lists and Notification Templates; both options are shown on the Administration module</p>

Privilege	Behavior When Present Behavior When Absent
	menu.
<p>User has access to the following pages in the Administration module:</p> <ul style="list-style-type: none"> • Notification <p>The Control Panel section does not appear in the Administration module's navigation pane and there are no links to the following pages:</p> <ul style="list-style-type: none"> • Notification Lists • Notification Templates • Notification Lists <p>User can create a new notification template or create a template in the Resource Management window and use it once; there is no option to save a new template for reuse. the Resource Management window and use it once, or save the template to use it again.</p> <p>NEW AdvisorsAdministration.RMC.Notifications.canView NOTE: Replaces AdvisorsAdministration.RMC.canView starting with Advisors release 8.5.101.</p>	
AdvisorsAdministration.PeripheralGateways.canView	User can access the Switches/Peripherals option is not shown on the Administration menu. Switches/Peripherals page.
AdvisorsAdministration.DeletedObjects.canView	User can see deleted objects in Genesys Administrator are not shown in the corresponding Administration page. Deleted objects in

Privilege	Behavior When Present Behavior When Absent
	Genesys Administrator server in the corresponding Administration pages.

[+] Show FA Privileges


In FA, you use RBAC to control users' access to:

- tabs on the FA administration page
- portions of tabs
- the entire FA dashboard

The following Table lists the privileges available in Configuration Manager for Frontline Advisor. The Table includes a description of the consequence to the user if the privilege is present or absent.


Privilege	Behavior When Present	Behavior When Absent
AdvisorsAdministration.Metrics.canView	User can access the Report Metrics page; option shown on menu.	Report Metrics option is not shown on the Administration menu.
AdvisorsAdministration.MMW.canCreate	User can create custom metrics.	The Create function and the Copy function do not display in the Report Metrics Manager.
AdvisorsAdministration.MMW.canEdit	Grants privilege to edit any metrics.	The Edit function does not display in the Report Metrics Manager.
AdvisorsAdministration.MMW.canDelete	Grants privilege to delete custom metrics.	The Delete function does not display in the Report Metrics Manager.
AdvisorsAdministration.MMW.SourceMetrics.canView	Grants privilege to view the Source Metrics page.	The Source Metrics page, and the link to it in the Administration module, do not display.
AdvisorsAdministration.MMW.SourceMetrics.canCreate	Grants privilege to create custom source metrics.	The Create Source Metrics button does not display on the Source Metrics page.
AdvisorsAdministration.MMW.SourceMetrics.canEdit	Grants privilege to edit source metrics.	The Edit function does not display on the Source Metrics page.
AdvisorsAdministration.MMW.SourceMetrics.canDelete	Grants privilege to delete custom source metrics.	The Delete function does not display on the Source Metrics page.
FrontlineAdvisor.SupervisorDashboardSearchView	User can access the FA Search View	User cannot access the FA

Privilege	Behavior When Present	Behavior When Absent
	Supervisor Dashboard.	Supervisor dashboard, and the FA Dashboard tab is not shown to the user.
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView <i>Requires the FrontlineAdvisor.SupervisorDashboard.canView privilege</i>	User can see the Teams pane.	The Teams pane is hidden along with both alerts panes.
FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView <i>Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges</i>	User can see the Team and Agent Alerts panes.	Neither of the alerts panes is displayed on the dashboard. If access to the Team pane is not available, the Alert pane is not shown even though user has access.
FrontlineAdvisor.SupervisorDashboard.ColumnChooser.canView <i>Requires the FrontlineAdvisor.SupervisorDashboard.canView privilege</i>	User can access the column chooser.	The column chooser button on the dashboard is hidden.
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canSort <i>Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges</i>	User can sort the entries in the Team pane. The cursor changes when hovering over the header of a column that can be sorted.	User cannot sort entries in the Team pane. The cursor does not change when hovering over a column header.
FrontlineAdvisor.SupervisorDashboard.TeamAlertsPane.canSort <i>Requires the FrontlineAdvisor.SupervisorDashboard.canView, FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView and FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privileges</i>	User can sort the entries in the Team Alerts pane. The cursor changes when hovering over the header of a column that can be sorted.	User cannot sort entries in the Team Alerts pane. The cursor does not change when hovering over a column header.
FrontlineAdvisor.SupervisorDashboard.AgentAlertsPane.canSort <i>Requires the FrontlineAdvisor.SupervisorDashboard.canView, FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView and FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privileges</i>	User can sort the entries in the Agent Alerts pane. The cursor changes when hovering over the header of a column that can be sorted.	User cannot sort entries in the Agent Alerts pane. The cursor does not change when hovering over a column header.
 FrontlineAdvisor.SupervisorDashboard.Export.canView	User can see the Print button on the Frontline Advisor dashboard.	The Print button is not displayed on the Frontline Advisor dashboard.
FrontlineAdvisor.Administration.canView	User can access the FA Administration module.	User cannot access the FA Administration module, and the FA Administration tab is not shown to the user.
FrontlineAdvisor.Administration.Settings.canView <i>Requires the FrontlineAdvisor.Administration.canView</i>	User can access the Settings tab in the FA Administration module.	Settings tab is not shown to the user.

Privilege	Behavior When Present	Behavior When Absent
<i>privilege</i>		
FrontlineAdvisor.Administration.Hierarchy.canReload <i>Requires the FrontlineAdvisor.Administration.canView and FrontlineAdvisor.Administration.Settings.canView privileges</i>	User can initiate a hierarchy reload through the action on the Settings tab.	Hierarchy reload action is not accessible.
FrontlineAdvisor.AgentDashboard.canView	User can access the FA Agent Dashboard.	User cannot access the FA Agent dashboard, and the FA Agent Dashboard tab is not shown to the user.
FrontlineAdvisor.AgentDashboard.AlertsPane.canView <i>Requires FrontlineAdvisor.AgentDashboard.canView privilege</i>	User can see the Alerts pane.	The Alerts pane is not displayed.
FrontlineAdvisor.AgentDashboard.ColumnChooser.canView <i>Requires FrontlineAdvisor.AgentDashboard.canView privilege</i>	User can see the Column Chooser.	The Column Chooser is not displayed.
 FrontlineAdvisor.AgentDashboard.Export.canView	User can see the Print button on the Agent Advisor dashboard.	The Print button is not displayed on the Agent Advisor dashboard.

Create the Data Manager Base Object Configuration User

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 servers where it is required for Advisors components.**
 - Contact Center Advisor Web services
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. Register the Stat Servers that you plan to use with Advisors.
6. **[+] 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
7. 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 CCAAdv/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 enable selection of one or more source objects as monitored objects in a deployment.

This configuration is not required on Platform deployments that do not have CCAAdv/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 Components Controlled by SCS

For general information about deploying components controlled by the Genesys Solution Control Server, see:

[Deploying Components Controlled by Solution Control Server](#)

Deploying Advisors Platform

To deploy Advisors Platform, see:

[General Prerequisites](#)

[Prerequisites for Advisors Platform](#)

[Deploying Advisors Platform](#)

Deploying Advisors Genesys Adapter

To deploy Advisors Genesys Adapter, see:

[General Prerequisites](#)

[Prerequisites for AGA](#)

[Deploying Advisors Genesys Adapter](#)

Deploying Advisors Cisco Adapter

To deploy Advisors Cisco Adapter, see:

[General Prerequisites](#)

[Prerequisites for ACA](#)

[Deploying Advisors Cisco Adapter](#)

Deploying Contact Center Advisor or Workforce Advisor

To deploy Contact Center Advisor or Workforce Advisor, see:

Deploying Frontline Advisor and Agent Advisor

To deploy Frontline Advisor, see:

General Prerequisites

Prerequisites for CCAdv and WA

Deploying CCAdv and WA

General Prerequisites

Prerequisites for FAAA

Deploying FAAA

Deploying Resource Management Console

To deploy the Resource Management Console, see:

General Prerequisites

Prerequisites for AGA

Deploying SDS and RMC

Deploying Components Controlled by Solution Control Server

Related Information

See the following topics for more detailed information:

- [Integration with Solution Control Server and Warm Standby](#)
- [Prerequisites](#)
- [Deploying Advisors](#)
- [Find and Edit XML Generator Properties](#)

Procedure: Deploying Advisors Components that Solution Control Server Will Control

Purpose: To deploy Advisors components that Solution Control Server (SCS) will control. This procedure is a summary of the tasks you perform to do this.

Steps

1. Install a supported version of the LCA on any server that includes, or will include, an Advisors module that SCS will control. See [Integration With Solution Control Server](#) for a list of such modules.
Some Genesys products install LCA as part of the product deployment, but Advisors do not. For information about supported versions of LCA, see [Genesys Interoperability Guide](#).
2. Locate the `lca.cfg` file in your LCA installation directory and change the `AppRespondTimeout` parameter to 60 seconds:

```
[lca]
AppRespondTimeout = 60
```
3. Restart the LCA.

4. For each Advisors component that will be controlled by Solution Control Server, perform the following tasks in Genesys Administrator.
 - a. Create an Application Template of type Genesys Generic Server; Advisors Application objects will use this Application Template. Do not use UI Application-type templates. Use only Server Application-type templates.
 - b. Create a Host object representing the host on which the Advisors component will run.
 - c. Create an Application representing this Advisors component.
 - d. For the Application, choose the template you created earlier, with type Genesys Generic Server.
 - e. Associate the Application object with its Host.
 - f. In the **[Server Info]** section of the Application object:
 - You must supply the **default port number** in the **[Server Info]** section. In release 8.5.1, Advisors ignore these port numbers. You can enter any port number, but Genesys recommends that you enter the server's HTTP port as follows. Where the Application represents:
 - Geronimo running WA Server or FA with the rollup engine: HTTP port, by default 8080.
 - CCAdv XML Generator: HTTP port, by default 8090.
 - AGA: HTTP port that will be used for the AGA instance.
 - ACA: HTTP port that will be used for the ACA instance.
 - Enter a period (.) as a placeholder in the **Working Directory** and **Command Line** fields.
 - If this component has a backup in an HA deployment, specify the Application that is the **Backup Server** and choose the **Redundancy Type** of Warm Standby.
5. Install each Advisors component on its system.

For applications that have a corresponding Application object in Configuration Server, the installer replaces the "." placeholders with the working directory specified during installation, and with the command that starts the server. The installer also updates the startup timeout and shutdown timeout, if necessary.

Important

For an Advisors server to support HA, it must be configured as an Application complete with a backup Application in the Configuration Server at the time the Advisors server starts. If you configure an Advisors server as an Application, start the Advisors server, and then add the backup Application to the server's Application, the server will not fail over correctly.

6. Genesys recommends that you specify a **disconnect-switchover-timeout** value on the SCS to avoid failovers due to temporary connection losses such as very short network disconnects. In Genesys Administrator or Configuration Manager, configure the option on the **Options** tab for your SCS Application. For additional information, see the [Genesys Management Framework](#)

documentation.

Configuring Advisors as a Solution

Using a Genesys configuration interface, such as Genesys Administrator or Genesys Administrator Extension (GAX), you can create an Advisors Solution object that gives you centralized control: you can start, stop, and run the components as a group, rather than as individual Applications.

The following procedure describes how to configure the Advisors Application objects as a Solution.

Procedure: Create an Advisors Solution object

Purpose: To create an Advisors Solution using existing Advisors Application objects. Once the Advisors suite is configured as a Solution, you can start, stop, and run the Advisors components using either Genesys Administrator or the Solution Control Interface (SCI).

Prerequisites

- Ensure the Advisors Application objects exist that will be part of the Solution.

Steps

1. Follow the **Creating Solution Objects** procedure, available on the [Solutions](#) page in the *Genesys Administrator Extension Help*, to create the Advisors Solution object. Note the following recommended settings for an Advisors Solution:

- You must select an option for **Solution Type**, but note the following limitations:
 - If you select Default Solution Type or Framework, you might have problems to start and stop the Applications with the Solution Control Interface (see the Note related to this topic in the [Creating Solution Objects](#) procedure).
 - If you specify the type as Unknown, the Solution might fail to save.

- For **Application Type**, use Genesys Generic Server for Advisors. Enter the precise version number of the Generic Server template in your system.

If the Generic Server template version you enter does not match that of the template used for the Advisors Application objects, then you will not be able to start or stop the Solution; its commands will be disabled in menus and toolbars.

If the Generic Server template versions are different for some of the Advisors Applications, make an entry for each version on the **Application Definitions** tab.

- In the **Application Definitions** tab, you can use a **Startup Priority** of 1.
- In the **Applications** tab, set the following startup priority for the Advisors Applications (it is acceptable to use the same **Startup Priority** number for more than one Application; Applications that have the same startup priority setting will start concurrently):

a. Advisors Genesys Adapters (for Frontline Advisor [FA] and/or Contact Center Advisor [CCAdv]) = 1

b. CCAdv XML Generator = 2

c. FA Server = 2 or 3

d. Advisors Administration, Platform, and CCAdv Web services = 4

e. Workforce Advisor (WA) server = 5

f. WA Web service = 6


If you deploy WA Server and WA Web service together, and you configure one Application object that controls both, then set the startup priority as 5 for that Application object.

Deploying Advisors Platform

You run a .jar installation file to deploy Advisors Platform. 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 **Module to Install** screen. Information about each screen is available on the **Installation Screens** tab below.

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

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 servers on which you will deploy one of the following Advisors components:
 - Contact Center Advisor Web Services
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. Register the Stat Servers that you plan to use with Advisors.
6. **[+] Install the Advisors components for your enterprise.**
 - Contact Center Advisor
 - Workforce Advisor
 - Contact Center Advisor - Mobile Edition

- Frontline Advisor
 - SDS and Resource Management
7. Make any required configuration changes.

<tabber>

Procedure=

Procedure: Deploying Advisors Platform

Prerequisites

- Review the [General Prerequisites](#) and [prerequisites specific to Advisors Platform deployment](#) before beginning deployment.

Steps

1. 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.

2. Use the **Next** and **Back** buttons on the installer to navigate through the installation screens. Enter your information on each screen; see the *Installer Screens* descriptions for additional information. Ensure you provide complete information on each screen.
3. On the final screen, click **Install**.
If errors display, diagnose them in the **Errors** tab, or refer to the **Troubleshooting** tab on this page.
4. If you use a Windows platform, install the Advisors windows service as follows:
[+] Show Steps
 1. Do this only for Advisors servers that will not be controlled by Solution Control Server. For a list of those, see [Integration With Genesys Management Layer](#).
 2. Open a command prompt, and change directory first to your Advisors base directory (for example, Program Files\GCTI\Advisors), then to bin\windows-x86.
 3. 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. Do this only for Advisors servers that will not be controlled by Solution Control Server. For a list of those, see [Integration With Genesys Management Layer](#).
- b. Open the shell.
- c. As root, run the following export command to add the JDK to your path:

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

f. 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.

5. If you are running Platform with a 64-bit JVM, Genesys recommends that you increase your [Geronimo PermGen memory settings](#).

| - | Installer Screens =

[+] Administration Configuration - CCAdv XMLGen

NEW The **Administration Configuration - CCAdv XMLGen** screen displays for nodes on which you opted to install the Administration module (on the **Module to Install** screen). If your Advisors deployment includes XML Generator, you must enter information on this screen. This ensures XML Generator stays up-to-date with changes made in the Administration module.

If you are not deploying Advisors in a warm standby configuration, then enter information about the XML Generator application in the fields for the primary application.

If your deployment does not include XML Generator (for example, if you are installing only Frontline Advisor in this deployment), then leave the fields on the **Administration Configuration - CCAdv XMLGen** screen blank.

[+] Administration Configuration - SC Server

NEW The **Administration Configuration - SC Server** screen displays for nodes on which you opted to install the Administration module (on the **Module to Install** screen). If your Advisors deployment includes XML Generator, you must enter information on this screen. This ensures XML Generator stays up-to-date with changes made in the Administration module.

If your deployment does not include XML Generator (for example, if you are installing only Frontline Advisor in this deployment), then leave the field on the **Administration Configuration - SC Server** screen blank.

[+] Application Server Configuration

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 the Procedure, Step 5.

[+] Backup Config Server

The **Backup Config Server** screen displays only if you selected the Add backup server checkbox on the **Genesys Config Server Connection Details** screen. Enter the backup Configuration Server details:

- Backup Server Name
- Backup Server Address
- Backup Server Port Number

[+] Cache Configuration

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.

[+] CCAdv/WA Object Configuration User

On the **CCAdv/WA 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).


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.

[+] Cluster Node Configuration

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.

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.
-  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.

[+] Destination Directory

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

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.

[+] Genesys Advisors Platform Database

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.

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.
- Database name (SQL Server) or Service name (Oracle)—The unique name or service 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.

[+] Genesys Advisors Platform Database - Advanced

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.

On the **Genesys Advisors Platform Database - Advanced** 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.

[+] Genesys Config Server Connection Details

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

- 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). 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.

[+] Java Development Kit

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

[+] Language Options

On the **Language Options** screen, specify the languages to use in e-mail templates. 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. You can also specify which language to use as the default language; you can select only one default language. The default language is the language in which metric names and descriptions will be shown if there are none provided for the language in which the user is viewing the dashboard.

[+] Mail Service Configuration

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`.

[+] Module to Install

On the **Module to Install** screen, select the Administration workbench checkbox to install this package. Selecting this option installs the Administration module and adds an Administration.properties file to the <advisors>\conf folder.

In previous releases, if you were installing Advisors Platform to support a clustered Advisors suite server, then you installed only one instance of the Administration module on one system in the cluster. That restriction is no longer applicable; you can install more than one instance of the Administration module in a clustered environment.

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

[+] Oracle JDBC Driver

On the **Oracle JDBC Driver** screen, specify the location of the Oracle Java Database Connectivity (JDBC) driver. See the [Genesys Supported Operating Environment Reference Guide](#) for information about drivers supported in release 8.5.1.

[+] RDBMS Type And JDBC Connectivity

NEW On the **RDBMS Type And JDBC Connectivity** screen, select either the SQL Server or the Oracle option – whichever you use for database(s). You must also select the Java Database Connectivity (JDBC) type that matches your environment. Select **Basic** for standalone databases or **Advanced** for clustered database configurations. The screens that follow are dependent on your selections on this screen.

[+] User Management Options

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

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*.

[-] 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.DatabaseError.throwSQLException(DatabaseError.java:112) [java] at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:331) [java] at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:288) [java] at oracle.jdbc.driver.T4C80all.receive(T4C80all.java:745) [java] at oracle.jdbc.driver.T4CPreparedStatement.doOall8(T4CPreparedStatement.java:219) [java] at oracle.jdbc.driver.T4CPreparedStatement.executeForRows(T4CPreparedStatement.java:970) [java] at oracle.jdbc.driver.OracleStatement.doExecuteWithTimeout(OracleStatement.java:1190) [java] at oracle.jdbc.driver.OraclePreparedStatement.executeInternal(OraclePreparedStatement.java:3370) [java] at oracle.jdbc.driver.OraclePreparedStatement.executeUpdate(OraclePreparedStatement.java:3454) [java] at com.informiam.installer.DA0.executeTimedOutUpdate(DA0.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 <code>ORA-01013: user requested cancel of current operation</code>. Typically this could happen with an Oracle database when someone runs a query such as <code>DELETE FROM <TABLE_NAME></code> without then executing <code>COMMIT</code>, 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 <code>COMMIT</code>; after the <code>DELETE</code> statement and re-run the installer. To prevent this situation, always run <code>COMMIT</code> after manually updating tables in Oracle.</p>
<pre>[java] Failed to connect to the database using connection URL:</pre>	Wrong database server name / IP address or port number

Installation Error Message	Cause
<pre>[java] jdbc:sqlserver://192.168.xx.yy:nnn;DatabaseName=ys_pldb;user=sa; password=very_secure_pwd;selectMethod=cursor [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnn has failed. Error: "Connection refused. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port."</pre>	
<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 register) at java.security.AccessControlContext.checkPermission(Unknown Source) at java.lang.SecurityManager.checkPermission(Unknown Source) at com.sun.jmx.interceptor.DefaultMBeanServerInterceptor.checkMBeanTrust</pre>	<p>Produced in error and can be ignored.</p> <p>Displays in the Errors tab when installing Platform with Oracle JDBC ojdbc6-11.2.0.2.0, and accurately reports that installation was successful.</p>

Installation Error Message	Cause
<pre>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.
<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: Change securerandom.source=file:/dev/urandom to securerandom.source=file:///dev/urandom.</p>
<p>NEW The installer fails or gives the following error message:</p> <pre>Caused by: java.security.AccessControlException: access denied ("javax.management.MBeanTrustPermission" "register")</pre>	<p>To correct this error, go to the Java installation that is specified in the path included in the error message, or the Java installation defined as JAVA_HOME.</p> <p>To the java.policy file under jre/lib/security, add the following to granted permissions:</p> <pre>permission java.util.PropertyPermission "javax.management.MBeanTrustPermission", "register"</pre>

Deploying Advisors 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 **Module to Install** and **Server Type** screens. Information about each screen is available on the **Installer Screens** tab below.

The procedures on this page are specific to AGA deployment. If you are deploying RMC, see [Deploying SDS and RMC](#).

NEW If you will be configuring multiple Genesys Adapters, note the following:

- Each primary AGA among the multiple adapters configured should use Stat Servers different from those used by other primary adapters.
- The primary and the backup AGA in a pair must be configured with the same Stat Servers.

For example, if there are two pairs of adapters configured (AGA1 and AGA2, and AGA3 and AGA4). AGA1 and AGA2 form a primary-backup HA pair. AGA3 and AGA4 form another primary-backup HA pair. The Stat Servers configured for the AGA1/AGA2 pair must not be the same Stat Servers configured for the AGA3/AGA4 pair. The Stat Servers configured for AGA1 and AGA2 must be the same Stat Servers, and the Stat Servers configured for AGA3 and AGA4 must be the same.



The preceding rules ensure the following:

1. On restart of the system, based on the last persisted Stat Server-object mapping, the statistics are requested with the same adapters, and each adapter queries the same Stat Servers as previously.
2. On switching over from the primary adapter to the backup adapter, the statistics are requested with the same Stat Servers as previously.

Important

Genesys recommends that the AGA metrics database selected for the primary and the backup AGA instances of a given adapter pair should be the same metrics database.

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 servers where it is required for Advisors components.**
 - Contact Center Advisor Web services
 - 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.  Register the Stat Servers that you plan to use with Advisors.
6. **[+] Install the Advisors components for your enterprise.**
 - Contact Center Advisor
 - Workforce Advisor
 - Contact Center Advisor - Mobile Edition
 - Frontline Advisor
 - SDS and Resource Management
7. 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.

<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.

Migrating the AGA Metrics Database or Schema

To migrate to release 8.5.1, 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.

Procedure: Migration of AGA Oracle METRICS Schemas

Steps

1. Connect to your database management interface as the AGA METRICS user.
2. Execute one of the following scripts:
 - `gc_metrics_<version>_ObjectsPlus.sql` (if you use SQL*Plus)
 - `gc_metrics_<version>_ObjectsDefault.sql` (if you use sqlDeveloper and all objects reside in the default tablespaces assigned to the METRICS user)
 - `gc_metrics_<version>_ObjectsCustom.sql` (if you use sqlDeveloper and you want to specify explicit names for tablespaces)
3. Re-issue the GRANT SELECT commands on each METRICS schema view to the Platform user.

Procedure: Migration of AGA MS SQL Databases

Steps

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

| Procedure=

Procedure: Deploying Advisors Genesys Adapter

Steps

1. Review the [General Prerequisites](#) and [prerequisites specific to Advisors Genesys Adapter deployment](#) before beginning deployment.

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 **Module to Install** screen, select the **Adapter Server** radio button. You can install only a single component (either the core service or RMC) during a single installer run.
4. Use the **Next** and **Back** buttons on the installer to navigate through the installation screens. Enter your information on each screen; see the *Installer Screens* tab on this page for additional information. Ensure you provide complete information on each screen.
5. Click **Show Details** and verify that there were no errors reported during installation.
6. Register and associate Stat Servers with the Advisors Genesys Adapter. For information on registering Stat Servers, see [Manage Advisors Stat Server Instances](#)

| - | Installer Screens =

[+] Adapter Port And Registration

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

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 IP address of the host.
- A description of the AGA server.

[+] CCAdv/WA Metrics Database Configuration

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 name/Service name**—The unique name of the database instance; for example, `advisors_gametricsdb`.
- **Database port**—The database server's port number.
- **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](#).

[+] CCAAdv/WA Metrics Database Configuration - Advanced

On the **CCAAdv/WA Metrics Database Configuration - Advanced** 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).

On the **CCAAdv/WA Metrics Database Configuration - Advanced** screen, specify the parameters for the Advisors platform database:

- Database user—The database user created and used for the Platform database.
- Database password—The password associated with the database user.
- 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.

[+] Enter Advisor Platform Database Information for Adapter Registration

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.

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.

[+] Genesys Data Source - Configuration Server

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

1. 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](#).

2. 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.

3. **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.

[+] Genesys Data Source - Backup Configuration Server

You see the **Genesys Data Source - Backup Configuration Server** screen only if you opted to add a backup Configuration Server on the **Genesys Data Source - Configuration Server** screen.

Enter the information required to connect to the backup Configuration Server:

- **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.

[+] Installation Details

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.

[+] Java Development Kit

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

[+] Oracle JDBC Driver

On the **Oracle JDBC Driver** screen, specify the location of the Oracle Java Database Connectivity (JDBC) driver. See the [Genesys Supported Operating Environment Reference Guide](#) for information about drivers supported in release 8.5.1.

[+] Platform Database Configuration

On the **Platform Database Configuration** screen, specify connection information for the the Advisors Platform database with which this AGA will be registered.

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

You are prompted for the following information on the **Platform Database Configuration** screen:

- **Database server**—The host name or IP address of the database server. When using numerical IP v6 addresses, enclose the literal in brackets.
- **Database Name (SQL Server) or Service name (Oracle)**—The unique name of the database instance.
- **Database port**—The database server's port number.
- **User Name or Database schema**—The Advisors user with full access to the Advisors platform database.
- **Password or Database schema password**—The password created and used for the Advisors platform database.

If you select Oracle Advanced, you will be prompted for information about the Advisors Platform database on the **Enter Advisor Platform Database Information for Adapter Registration** screen.

[+] Platform Database Configuration - Advanced

On the **Platform Database Configuration - Advanced** 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).

On the **Platform Database Configuration - Advanced** screen, specify the parameters for the Advisors platform database:

- **User Name**—The database user created and used for the Platform database.
- **Password**—The password associated with the database user.
- **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.

If you select **Oracle Advanced**, you will be prompted for information about the Advisors Platform database on the **Enter Advisor Platform Database Information for Adapter Registration** screen.

[+] RDBMS Type and JDBC Connectivity

NEW On the **RDBMS Type And JDBC Connectivity** screen, select either the **SQL Server** or the **Oracle** option – whichever you use for database(s). You must also select the Java Database Connectivity (JDBC) type that matches your environment. Select **Basic** for standalone databases or **Advanced** for clustered database configurations. The screens that follow are dependent on your selections on this screen.

[+] SCS Integration Configuration

You enter information about the AGA connection to the Genesys Management Layer on the **SCS Integration Configuration** screen. You must configure these properties even if you are not configuring warm standby mode of operation.

- **Adapter application name**—The application name specified in Configuration Manager or Genesys Administrator for this AGA instance.
- **LCA port**—Unless you changed the LCA port number, accept the default.
- **SCS application name**—The name of the Solution Control Server application object as it appears in Configuration Manager or Genesys Administrator.

[+] Server Type

On the **Server Type** screen, select the radio button that corresponds to the Advisors module for which you are deploying this AGA instance. The options are **Contact Center Advisor/Workforce Advisor** and **Frontline Advisor**. You can select only one option on this screen.

-| 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.

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 select a unique application name for each Genesys Adapter instance.

-| 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</pre>	Wrong database name

Installation Error Message	Cause
port."	
[java] Exception while connecting: Login failed for user 'badUserId'. [java] url used: jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=ys_gadb;selectMethod=cursor;user=badUserId; password=very_secure_password	Wrong database user name or password
[loadfile] Unable to load file: java.io.FileNotFoundException: C:\ (The system cannot find the path specified)	Produced in error and can be ignored.

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.

Deploying Advisors 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](#).

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. (Note that ACA itself does not require these users.)
3. **[+] Install the Platform service (Geronimo) on servers where it is required for Advisors components. (Note that ACA itself does not require Advisors Platform, but components that ACA serves require it.)**
 - Contact Center Advisor Web services
 - 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. Register the Stat Servers that you plan to use with Advisors.
6. **[+] 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
7. Make any required configuration changes.

<tabber>

Procedure=

Procedure: Deploying ACA

Steps

1. Review the [General Prerequisites](#) and [prerequisites specific to Advisors Cisco Adapter deployment](#) before beginning deployment.

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. Use the **Next** and **Back** buttons on the installer to navigate through the installation screens. Enter your information on each screen; see the *Installer Screens* tab on this page for additional information. Ensure you provide complete information on each screen.
4. After installation is complete, click **Show Details**. Verify that there were no errors reported during installation.

|<| Installer Screens=

[+] Advisors Cisco Adapter Database Configuration

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 (SQL Server) or Service name (Oracle)—The unique name of the database instance; for example, `ciscoadapter_db`.
- Database port—The database server's port number.
- User Name or Database schema—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.

[+] Advisors Cisco Adapter Database Configuration - Advanced

On the **Advisors Cisco Adapter Database Configuration - Advanced** screen, specify the parameters for the 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.

[+] Cisco AWDB Database Configuration

On the **Cisco AWDB 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.

[+] Cisco HDS Database Configuration

On the **Cisco HDS 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.

[+] Genesys Data Source - Configuration Server

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

1. 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](#).

2. 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.
3. **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.

[+] Genesys Data Source - Backup Configuration Server

You see the **Genesys Data Source - Backup Configuration Server** screen only if you opted to add a backup Configuration Server on the **Genesys Data Source - Configuration Server** screen.

Enter the information required to connect to the backup Configuration Server:

- **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.

[+] Installation details

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.

[+] Java Development Kit

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.

[+] Oracle JDBC Driver

On the **Oracle JDBC Driver** screen, specify the location of the Oracle Java Database Connectivity

(JDBC) driver. See the [Genesys Supported Operating Environment Reference Guide](#) for information about drivers supported in release 8.5.1.

[+] Platform Database Configuration

On the **Platform Database Configuration** screen, specify connection information for the the Advisors Platform database with which this AGA will be registered.

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

You are prompted for the following information on the **Platform Database Configuration** screen:

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

[+] Platform Database Configuration - Advanced

On the **Platform Database Configuration - Advanced** 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).

On the **Platform Database Configuration - Advanced** screen, specify the parameters for the Advisors platform database:

- Database schema—The database user created and used for the Platform database.
- Password—The password associated with the database user.
- 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.

[+] RDBMS Type and JDBC Connectivity

NEW On the **RDBMS Type And JDBC Connectivity** screen, select either the **SQL Server** or the **Oracle** option - whichever you use for database(s). You must also select the Java Database Connectivity (JDBC) type that matches your environment. Select **Basic** for standalone databases or **Advanced** for clustered database configurations. The screens that follow are dependent on your selections on this screen.

[+] Register Adapter

Enter the following information about the adapter on the **Register Adapter** screen:

- Port Information—You can use the default port, 7000, if no other application is using that port.
- Host Address
- Description (for example, Advisors Cisco Adapter)
- Source Environment (for example, Cisco)

[+] SCS Integration Configuration

You enter information about the ACA connection to the Genesys Management Layer on the **SCS Integration Configuration** screen. You must configure these properties even if you are not configuring the warm standby mode of operation.

- Adapter application name—The application name specified in Configuration Manager or Genesys Administrator for this ACA installation.
- LCA port—Unless you changed the LCA port number, accept the default.
- SCS application name—The name of the Solution Control Server application object as it appears in Configuration Manager or Genesys Administrator.

[-] Multiple instances on a 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 must create the database.

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.

[-] Troubleshooting=

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

Installation Error Message	Cause
[java] Failed to connect to the database using connection URL:	Wrong database server name / IP address or port number

Installation Error Message	Cause
<pre>[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>	
<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_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.</pre>	<p>Produced in error and can be ignored.</p> <p>Displays in the Errors tab when installing Cisco Adapter with Oracle JDBC driver ojdbc6-11.2.0.2.0, and accurately reports that installation was successful.</p>

Installation Error Message	Cause
<pre>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>	
<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.

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](#).

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 servers where it is required for Advisors components.**
 - Contact Center Advisor Web services
 - 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. Register the Stat Servers that you plan to use with Advisors.
 6. Install the Advisors components for your enterprise:
 -  Contact Center Advisor
 -  Workforce Advisor
 -  Contact Center Advisor – Mobile Edition
 - Frontline Advisor
 - SDS and Resource Management
 7. 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=

Procedure: Deploying CCAAdv, CCAAdv XML Generator, WA, or CCAAdv-ME

Steps

1. Review the [General Prerequisites](#) and [prerequisites specific to CCAAdv/WA deployment](#) before beginning deployment.
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 ccawa-installer-<version>.jar
```
- Double-click the `ccawa-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. Advisors Platform must be installed on each server where a module is installed, with the exception of CCAdv XML Generator. CCAdv XML Generator does not require Advisors Platform. 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 no more than twice in one cluster of Advisors systems. One instance will run as the primary, and the second, if present, will run as the backup. Starting in release 8.5.1, CCAdv XML Generator runs independently of Advisors Platform.
- 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 no more than twice in one cluster of Advisors systems. One instance will run as the primary, and the second, if present, will run as the backup.
- 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 systems on which you installed the Administration Workbench when installing Platform.
- 4. On the **Destination Directory** screen, specify the location and name of the base directory in which you will install Advisors. The installation directory for CCAdv/WA modules must be the same as the directory where Advisors Platform was installed. Contact Center Advisor XML Generator does not require Platform, so can be installed independently.
- 5. Use the information provided on the *Installer Screens* tab on this page to assist you to complete the remaining deployment screens.

|–| Installer Screens=

[+] CCAdv-ME Server

- 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

Enter the time periods for trend charting on the **CCAdv-ME Trend Charting** 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.

Enter numerical characters only in these fields, such as 30, 60, and 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 CCAAdv will wait for new data from this data source before notifying users via the CCAAdv 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 - Advanced

- 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 - Advanced

- 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.

[+] RDBMS Type and JDBC Connectivity

On the **RDBMS Type And JDBC Connectivity** screen, select either the **SQL Server** or the **Oracle** option - whichever you use for database(s). You must also select the Java Database Connectivity (JDBC) type that matches your environment. Select **Basic** for standalone databases or **Advanced** for clustered database configurations. The screens that follow are dependent on your selections on this screen.

[+] Workforce Advisor Page 1 - SCS Integration

Enter the WA Server Application name exactly as it is configured in Genesys Configuration Server.

[+] Workforce Advisor Server Page 2 - WFM Systems

Select your sources for workforce management data.

[+] Workforce Advisor Server Page 3 - EMail Addresses

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.

[+] Workforce Advisor Server Page 4 - IEX TotalView

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

[+] Workforce Advisor Server Page 5 - 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 Advisor Server Page 6 - 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.

[+] XML Generator Page 1 - Config Server

Starting in release 8.5.1, CCAdv XML Generator runs independently of Advisors Platform; it is no longer necessary to install Advisors Platform to support XML Generator. Also, XML Generator more actively communicates with Genesys Configuration Server, particularly in warm standby setups. You must, therefore, enter some of the same information for XML Generator's use that you entered for Advisors Platform.

On the **XML Generator Page 1 - Config Server** screen, enter information about the Genesys Configuration Server that is part of your deployment:

- **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). 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.

NEW **[+] XML Generator Page 2 - Backup Config Server**

The **XML Generator Page 2 - Backup Config Server** screen displays only if you selected the Add backup server checkbox on the **XML Generator Page 1 - Config Server** screen.
Enter the backup Configuration Server details:

- Backup Server Name
- Backup Server Address
- Backup Server Port Number

NEW **[+] XML Generator Page 3 - Config Server**

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. This is not applicable if you use only Cisco data sources.
You are not prompted for the password for this user account because there is no user authentication performed for this user.

NEW **[+] XML Generator Page 4 - Config Server**

Enter the name of the default Genesys tenant.

NEW **[+] XML Generator Page 5 - SCS Integration**

Enter the XML Generator application name exactly as it is configured in the Genesys Configuration Server.

NEW **[+] XML Generator Page 6 - Cluster Member**

Configure this XML Generator installation as a unique node in the cluster. Each server on which you install XML Generator requires a unique cluster node ID. On this screen you also enter the port number that nodes in this cluster use to communicate. The data you enter on this screen, and the following screen (**XML Generator Page 7 - Cluster Member**), is entered in the `ActiveMQ.properties` and `Caching.properties` files in the Advisors Platform database. Configure the node with the following information:

- **Node ID**—A unique ID across all XML Generator 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.
- **Localhost address**—The local host address: `localhost` or `127.0.0.1`.
- **XMLGen Port Number**—The 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.

[+] XML Generator Page 7 - Cluster Member

Enter information about port numbers used for communication within the cluster. The data you enter on the preceding screen (**XML Generator Page 6 - Cluster Member**) and on this screen is entered in the `ActiveMQ.properties` and `Caching.properties` files in the Advisors Platform database.

- **JMS port**—The Java Message Service (JMS) port number.
- **The first port in range and The last port in range**—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.

[+] XML Generator Page 8 - 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 9 - Generation Interval

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 10 - DB Connection Retry

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 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 11 - EMail Addresses

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.

[+] XML Generator Page 12 - Metric Graphing

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 - Page 1

Select the time profile for the historical agent group metrics that CCAdv and WA will display.

If you choose **5 minute sliding**, then CCAdv 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.

[+] XML Generator and Workforce Advisor - Page 2

Enter information to connect to the Genesys Management Layer on the **XML Generator and Workforce Advisor - Page 2** screen. You must configure these properties for both a basic Advisors setup, as well as a warm standby setup.

- LCA port—The LCA port number for the server on which you are currently deploying a CCAAdv or WA component. Unless you changed the LCA port number, accept the default.
- SCS application name—The name of the Solution Control Server application in Configuration Manager or Genesys Administrator.

[-] 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 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_eadb;selectMethod=cursor;user=badUserId; password=very_secure_password</pre>	Wrong database user name or password
<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.

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 FAAA

You run a .jar installation file to deploy Genesys Frontline Advisor/Agent Advisor. The fa-server-installer-<version>.jar file installs both Frontline Advisor and Agent Advisor dashboards; you use **Role-Based Access Control (RBAC) privileges** to control which dashboard each user can see and use.

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

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 servers where it is required for Advisors components.**
 - Contact Center Advisor Web services
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. Register the Stat Servers that you plan to use with Advisors.
6. 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
7. Make any required configuration changes.

<tabber>

Procedure=

Procedure: Deploying Frontline Advisor and Agent Advisor

Steps

1. Review the [General Prerequisites](#) and [prerequisites specific to Frontline Advisor deployment](#) before beginning deployment.

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. Use the information provided on the *Installation Screens* tab on this page to assist you to complete the remaining deployment screens.
5. After you deploy FA, you must modify the Apache configuration file (`httpd.conf`). See [Deploy and Configure Apache](#).

|–| Installer Screens=

[+] Distributed Mode Configuration

If you are installing a single instance of Frontline Advisor, select the `Run as a single instance` option. This is the default setting.

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.

[+] Distributed Mode - Rollup Engine

You see the **Distributed Mode - Rollup Engine** screen only if you selected the `Run as a cluster member` option on the **Distributed Mode Configuration** screen.

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.

Tip

Enable the rollup engine for only one of the FA instances in a cluster for a basic setup. In a warm standby configuration, however, ensure you enable the rollup engine on both the primary and backup applications; the two do not run simultaneously, and in the event of failover, the backup must be able to continue the data aggregation processes.

- **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.

[+] Failure Notification Configuration

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

[+] Genesys Advisor Platform Database

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 or Service name—The unique name of the database instance.
- Database user or Database schema—The Advisors user with full access to the Advisors platform database.
- Database user password—The password created and used for the Advisors platform database.

[+] Genesys Advisor Platform Database - Advanced

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

- Database user or Database schema—The Advisors user with full access to the Advisors platform database.
- Database user password or Database schema password—The password created and used for the Advisors 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.

[+] Hierarchy Source Details

You see the **Hierarchy Source Details** screen only if you selected the Run as a single instance option on the **Distributed Mode Configuration** screen.

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).

[+] RDBMS Type And JDBC Connectivity

On the **RDBMS Type And JDBC Connectivity** screen, select either the **SQL Server** or the **Oracle** option – whichever you use for database(s). You must also select the Java Database Connectivity (JDBC) type that matches your environment. Select **Basic** for standalone databases or **Advanced** for clustered database configurations. The screens that follow are dependent on your selections on this screen.

[+] SCS Integration

Enter the Geronimo Application name exactly as it is configured in Genesys Configuration Server.

|-| 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</pre>	Wrong database server name / IP address or port number

Installation Error Message	Cause
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.	
<p>[java] Failed to connect to the database using connection URL:</p> <pre>[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
<p>[java] Exception while connecting: Login failed for user 'badUserId'.</p> <pre>[java] url used: jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=ys_fadb;selectMethod=cursor; user=badUserId;password=very_secure_password</pre>	Wrong database user name or password
<p>[loadfile] Unable to load file: java.io.FileNotFoundException: C:\ (The system cannot find the path specified)</p>	Produced in error and can be ignored.

Deploying SDS and RMC

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 servers where it is required for Advisors components.**
 - Contact Center Advisor Web services
 - Workforce Advisor
 - Frontline Advisor
 - Contact Center Advisor-Mobile Edition
 - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. Register the Stat Servers that you plan to use with Advisors.
6. Install the Advisors components for your enterprise:
 - Contact Center Advisor
 - Workforce Advisor
 - Contact Center Advisor - Mobile Edition
 - Frontline Advisor
 -  SDS and Resource Management Console
7. Make any required configuration changes.

Resource Management and Resource Management User Configuration

The Resource Management Console (RMC) is subject to Role-Based Access Control (RBAC). After you have deployed RMC, a system administrator must assign privileges and permissions to users who will use RMC in the Contact Center Advisor or Workforce Advisor dashboard. These privileges and permissions control a user's or group's access to RMC and, for users or groups who have access to RMC, access to specific functionality within it.

NEW In addition to configuring permissions and privileges, you might need to change property file settings. See [Related Information](#) for links to related topics.

Related Information

See the following for more information:

- For general information about using RBAC with Advisors, see [Role-Based Access Control for Advisors](#).
- For information about creating RMC Users in the Genesys environment, see [Configuring RMC Users in the Genesys Configuration Layer](#).
- For information about privileges and permissions for users of RMC, see [CCAdv/WA Access Privileges](#).
- For information about configuring RMC after installing it, see [Configure Resource Management Console Properties](#).
- Procedures on this page assume that you are familiar with, and regularly use, one of the Genesys configuration interfaces for creating users, roles, access groups, and so on, in the Configuration Layer. If you need detailed information about using the Genesys configuration interface, see the Help for the interface used in your enterprise:
 - [Configuration Manager Help \(8.1\)](#)
 - [Genesys Administrator Help](#)
 - [Genesys Administrator Extension Help](#)

Important Information about the SDS and RMC Operating Environment

Before you deploy Supervisor Desktop Service (SDS) and Resource Management Console (RMC),

ensure you have the correct operating environment for both. Read the following information carefully:

- Supervisor Desktop Service SDS is available in both 32-bit and 64-bit versions.
- **NEW** When connecting SDS to a Configuration Server proxy, SDS supports a connection only to non-secure ports of the proxy server.
- Performance Management Advisors support Oracle JDK 1.7, but SDS does not. If you deploy SDS, you must also install a version of JDK 1.6.0 for SDS on the host machine. Use the following table as a guide. Follow this basic rule: if the SDS is 32-bit, use 32-bit Java. If SDS is 64-bit, use 64-bit Java. The SDS server for Linux is 32-bit only.

Operating System	SDS Version	Java 32 or 64
Linux 32 or 64 bit	7.6.300.08 32-bit	Java 1.6.x 32-bit
Windows 32-bit	7.6.300.09 32-bit	Java 1.6.x 32-bit
Windows 64-bit	7.6.300.09 32-bit	Java 1.6.x 32-bit
Windows 64-bit	7.6.300.09 64-bit	Java 1.6.x 64-bit

- Install SDS and the 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.
- If you use the Resource Management Console in Contact Center Advisor and/or Workforce Advisor, note the following:
 - Avoid running Resource Management in Microsoft Internet Explorer 10 or earlier versions; older versions of Internet Explorer can cause serious problems with the Resource Management console.
 - For 8.5.1 releases prior to 8.5.101, deploy Resource Management on a supported Microsoft Windows operating system. Resource Management is not compatible with Red Hat Enterprise Linux until Advisors release 8.5.101. See the *Genesys Supported Operating Environment Reference Guide* for information about supported Windows operating systems.

SDS and RMC Deployment Procedures

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

Task Summary

The following tasks are listed in the order in which Genesys recommends you install and configure the Supervisor Desktop Service and the Resource Management Console.

You can deploy the Supervisor Desktop Service and Resource Management Console on a supported Red Hat Enterprise Linux operating system starting with Advisors release 8.5.101. For information about supported operating systems, see *the Advisors section in the Supported Operating Environment Reference Guide*.

1. Configure the Supervisor Desktop Service Application in the Genesys Configuration Layer.

See *Procedure: Configuring the SDS Application in the Genesys Configuration Layer*.

2. Configure the Spv user for the Supervisor Desktop Service.

If you are deploying Advisors release 8.5.100 or earlier, you must configure the Spv user. The Spv user is not required starting with Advisors release 8.5.101.

See [Procedure: Configure the Spv User \(Required for Advisors release 8.5.100\)](#).

3. Deploy Supervisor Desktop Service on a supported Windows or Linux operating system. In addition to Windows deployments, you can deploy RMC on supported versions of Linux starting with Advisors release 8.5.101. Use one of the following procedures:

- [Procedure: Deploying Supervisor Desktop Service on Windows](#)
- [Procedure: Deploying Supervisor Desktop Service on Linux](#)

4. Complete the Supervisor Desktop Service configuration.

See [Procedure: Completing the Supervisor Desktop Service Configuration](#).

5. Deploy the Resource Management Console on a supported Windows or Linux operating system. In addition to Windows deployments, you can deploy RMC on supported versions of Linux starting with Advisors release 8.5.101.

See [Procedure: Deploying the Resource Management Console](#).

6. Configure the Resource Management Console:

- For Advisors release 8.5.100, see [Procedure: Configuring the Resource Management Console for Advisors release 8.5.100](#).
- For Advisors release 8.5.101, see [Procedure: Configuring the Resource Management Console for Advisors release 8.5.101](#).

Procedure: Configuring the SDS Application in the Genesys Configuration Layer

Steps

1. On the Genesys server, launch the Genesys configuration interface (for example, Genesys Administrator).
2. Create a host object, under the Environment tenant, 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.
3. Import the application template called `Genesys_Supervisor_Desktop_Service_763.adp`. This template is located with the SDS installation files.
4. Create a new Application using the `Genesys_Supervisor_Desktop_Service_763.adp` application template. Configure the Application using the following guidelines:
 - a. Specify the name of the application as `Genesys Supervisor Desktop`.

- b. 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.
- c. (Multi-tenant environments only) Add the non-Environment tenant that SDS will monitor.
- d. Select the host object configured in **Step 2** above (that is, the server on which you will install SDS). If necessary, change the port number to 8080.
- e. Enter a single period (.) for the working directory, command line, and command line arguments.
- f. Ensure you select a login account that has full control privileges. For example, you can select the option to log in as System as long as your System user has full control access privileges.
- g. Configure options as follows:
 - 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

Tip

The stat-threads= -1 setting can be used to indicate “use all available processors”.

For smaller customers the following settings can be used to create periodic SDS statistics polling at 30-second intervals:

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

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

For larger customers the stat-peeking=true setting can be used to define on-demand statistics retrieval.

- Add the properties for your e-mail messaging system under the **[supervisor]** section in the list of options; see the following Table for additional information.

[+] Show Table

Property Name	Example Property Value	Description
email-sender-address	adminaccount@email-	The From address used for

Property Name	Example Property Value	Description
	server.com	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.

5. In the Applications's permissions, grant to the Advisors user the following permissions on the Application: Read, Change, Read Permissions. See [Create the Advisors User Account](#).

- Save the Application.
- 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.

Next Steps

Do one of the following:

- If you are deploying Advisors release 8.5.100, you must configure the Spv user before you deploy the Supervisor Desktop Service. See [Procedure: Configure the Spv User](#).
- If you are deploying Advisors release 8.5.101, you can now deploy the SDS on a supported Windows or Linux host machine. See one of the following:
 - [Procedure: Deploying Supervisor Desktop Service on Windows](#)
 - [Procedure: Deploying Supervisor Desktop Service on Linux](#)

For information about supported operating systems for Advisors deployments, see [the Advisors section in the Supported Operating Environment Reference Guide](#).

Procedure: Configure the Spv User (Required for Advisors release 8.5.100)

Steps

1. On the Genesys server, launch the Genesys configuration interface (for example, Genesys Administrator).
2. 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 **Agent** check box is selected (that is, identify this user as an agent). The Person should have the following attributes:
 - First Name: Spv
 - Last Name: Spv_Last
 - Employee ID: Spv
 - User Name: Spv
3. On the **Annex**, add a new section named **[security]**. Open the **[security]** section, and add the following properties:
 - Supervisor = 1
 - SupervisorAdhoc = 2
 - SupervisorExtended = 10
 - SupervisorMonitoring = 1
4. On the **Permissions** tab, add the default user to the list and give that user Full Control as the type of access (if this does not already exist).
5. Save the Spv user configuration.
6. Configure the Spv user to have additional permissions as follows:
 - For single tenant installations, add Spv to the Administrators access group for the Environment tenant.

- 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.

Next Steps

You can now deploy the SDS on a supported Windows host machine. See [Procedure: Deploying Supervisor Desktop Service on Windows](#). For information about supported operating systems for Advisors deployments, see [the Advisors section in the Supported Operating Environment Reference Guide](#).

Procedure: Deploying Supervisor Desktop Service on Windows

Steps

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

[+] Show Steps for Using Command Line

- a. Stop 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.

[+] Show Steps for Using SDS Installer

- a. Stop the SDS service.
- b. Run the SDS installer, selecting the option to update an existing installation.
- c. When prompted, select the option to remove the SDS.
- 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. Copy the installation package to a directory of your choice.
4. Run setup.exe.
You can find the setup.exe file in the folder containing the Supervisor Desktop Service installation package.
The Genesys Installation Wizard for SDS displays and guides you through the rest of the installation.

[+] See information about installer screens

- 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**.
- 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.

Next Steps

There are additional steps to complete the SDS configuration. See [Procedure: Completing the Supervisor Desktop Service Configuration](#).

Procedure: Deploying Supervisor Desktop Service on Linux (Support starts with Advisors release 8.5.101)

Steps

1. If an older version of SDS is already installed, you must uninstall it.
This should be unnecessary for Advisors release 8.5.1 because Genesys' support for SDS on Linux begins in Advisors release 8.5.101. However, if you must uninstall SDS from a Linux platform for any reason, manually remove the installation directory and delete the web application from the server.
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. Copy the installation package to a directory of your choice.
4. Run `./install.sh`.
You can find the `./install.sh` file in the folder containing the Supervisor Desktop Service installation package.
[+] See information about installer screens
 - 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**.
 - 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.

Next Steps

There are additional steps to complete the SDS configuration. See [Procedure: Completing the Supervisor Desktop Service Configuration](#).

Procedure: Completing the Supervisor Desktop Service Configuration

Steps

1. On the Genesys server, launch the Genesys configuration interface (for example, Genesys Administrator).
2. Edit the options for your Stat Server application as described below:
 - a. Import the StatServerEntries.cfg file (found in the Advisors Genesys Adapter installation directory) into the Stat Server application options. If prompted to overwrite the existing options, choose NO.
 - b. If prompted to overwrite/update any statistics options, do so. 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.
3. If you are deploying Advisors release 8.5.101, omit this Step. If, however, you are deploying Advisors release 8.5.100, in the Genesys configuration interface, browse to the scripts for the tenant(s) that you use for the SDS installation. Delete all scripts named User.Stat.Spv*.
4. For performance reasons, Genesys recommends that you update xms and xmx values for servers that host your SDS. Edit these values based on information in the [Genesys Hardware Sizing Guide](#), Chapter 17: Performance Management Advisors, in section Improving Supervisor Desktop Service Performance.
5. Use Solution Control Server, Genesys Administrator, or the SDS host to start SDS. To start SDS from the host machine:
 - On a Windows host machine: Use the Windows service
 - On a Linux host machine: Execute ./startup.sh in the /bin folder

Next Steps

Deploy the Resource Management Console. See [Procedure: Deploying the Resource Management Console](#).

Procedure: Deploying the Resource Management Console

Steps

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 **Module to Install** screen, select the Resource Management Console radio button. You can install only a single component (either the Adapter Server or RMC) during a single installer run.
3. On the **RDBMS Type And JDBC Connectivity** screen, select either the **SQL Server** or the **Oracle** option – whichever you use for database(s). You must also select the Java Database Connectivity (JDBC) type that matches your environment. Select **Basic** for standalone databases or **Advanced** for clustered database configurations. The screens that follow are dependent on your selections on this screen.
4. Enter the following information on subsequent screens:
 - 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, which is the default location.
 - On the **Genesys Advisor Platform Database** screen, specify the parameters for the

Advisors platform database – the fields might vary depending on your selection of **Basic** or **Advanced** database type:

- Database host—If requested, enter the host name or IP address of the database server. When using numerical IPv6 addresses, enclose the literal in brackets.
- Database name/Service name—If requested, enter the unique name of the database instance.
- Database port number—If requested, enter the database server's port number.
- Database user—The username to be used by the Adapter to access the database.
- Database user password—The password associated with the database user.
- 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.

5. After you have entered information on all installer screens, click **Install**.

6. Click **Show Details**. Use the **Errors** tab to verify that no errors were reported during installation.

Next Steps

See information about configuring the RMC:

- For Advisors release 8.5.100, see [Procedure: Configuring the Resource Management Console for Advisors release 8.5.100](#).
- For Advisors release 8.5.101, see [Procedure: Configuring the Resource Management Console for Advisors release 8.5.101](#).

Procedure: Configuring the Resource Management Console for Advisors release 8.5.100

Steps

1. **Configure the RMC properties file**

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 `RMCInfo.xml` file is found in the following directory:
`Advisors\geronimo-tomcat6-minimal-2.2.1\repository\com\informiam\genesys\rmc-web\<version>\rmc-web-8.x.xxx_<version>.war\WEB-INF\classes`

Properties prefixed with SDS refer to the Supervisor Desktop Service, installed earlier.

Properties prefixed with CCAWA refer to the host on which CCAdv web services is installed.

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 host running CCAdv web services. When using numerical IPv6 addresses, enclose the literal in brackets.
- `CCAWA_Port` – The port number for CCAdv web services on that host (default 8080).

2. Add an entry to Apache `httpd.conf`

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).

3. Restart the Geronimo server

Open the Windows Services window and restart the Geronimo server.

Next Steps

- See [Configure Resource Management Console Properties](#) for information about configuring RMC properties for optimal performance.
- Configure permissions and privileges to allow users access to RMC in the Contact Center Advisor and Workforce Advisor dashboards:
 - See [Role-Based Access Control for Advisors](#) for general information about using RBAC with Advisors.
 - See [CCAdv/WA Access Privileges](#) for information about privileges and permissions for users of

RMC.

Procedure: Configuring the Resource Management Console for Advisors release 8.5.101

Steps

1. Configure the RMC properties file

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

```
Advisors\geronimo-tomcat6-minimal-2.2.1\repository\com\informiam\genesys\rmc-web\<version>\rmc-web-8.x.xxx_<version>.war\WEB-INF\classes
```

Properties prefixed with SDS refer to the Supervisor Desktop Service, installed earlier.

Properties prefixed with `CCADV_WebServices` refer to the host on which CCAdv web services is installed.

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).
- `CCADV_WebServices_IP` – The IP address for the CCAdv/WA server host. When using numerical IPv6 addresses, enclose the literal in brackets.
- `CCADV_WebServices_Port` – The port number for the CCAdv/WA server (default 8080).

2. Enable transmission of login events to RMC

When an Advisors user logs in to or out of Advisors, a message describing this event is sent on a topic to the RMC Web application. The RMC receives the message and logs the user in to or out of the SDS server. By default, messages remain alive in the topic for 1 second, but the default value of 1 second is not long enough for the RMC to receive the messages. Using the default value, the RMC will not log users in to the SDS and, when the users try to open the RMC, they will see messages stating that they are not logged in to the SDS server.

To change how long the Advisors application keeps alive login messages in the topic, update the `advisors.user.auth.event.queue.ttl.secs` parameter in the `conf/ActiveMQ.properties` file. You must update the file for every Geronimo server that will receive requests from users to log in to Advisors.

Genesys recommends setting the `advisors.user.auth.event.queue.ttl.secs` property to 300 seconds:

```
advisors.user.auth.event.queue.ttl.secs=300
```

Warning

To ensure that the login messages do not expire prematurely, the system time must be identical on the nodes in the Advisors cluster. The logic that decides if a message should expire uses the system time on *both the sending and receiving system*, so the system time must be synchronized within the cluster.

3. Add an entry to Apache `httpd.conf`

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).

4. Restart Geronimo servers

Restart every Geronimo server for which you changed either the `RMCInfo.xml` properties or the `ActiveMQ.properties` file.

If the Geronimo server is running an Advisors application that is integrated with Solution Control Server, then restart the Advisors server from the Solution Control Interface.

If not integrated with Solution Control Server, then:

- On a Windows host machine: Open the Windows Services window and restart the Geronimo server.
- On a Linux host machine:
 - If you have not configured Geronimo to start as a service, then from the `/bin` folder, execute `./shutdown.sh` and then `./startup.sh` to stop and restart the Geronimo server.
 - If you have configured Geronimo to start as a service, then stop and start the Linux service that controls Geronimo.

Next Steps

- See [Configure Resource Management Console Properties](#) for information about configuring RMC properties for optimal performance.

-
- Configure permissions and privileges to allow users access to RMC in the Contact Center Advisor and Workforce Advisor dashboards:
 - See [Role-Based Access Control for Advisors](#) for general information about using RBAC with Advisors.
 - See [CCAdv/WA Access Privileges](#) for information about privileges and permissions for users of RMC.
 - See [Configuring RMC Users in the Genesys Configuration Layer](#) for information about RMC User configuration in the Genesys environment.

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.

Cold Standby Configuration and Switchover

Performance Management Advisors support *cold standby* High Availability starting in release 8.5.0. *Cold standby* 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.

Note that starting in release 8.5.1, Advisors support warm standby HA for certain modules, integrating with Solution Control Server. See [Integration with Solution Control Server and Warm Standby](#).

<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

General

Consider changing the memory allocation of an Advisors server if it is reporting out memory errors in its log.

Increasing PermGen memory is normally required only when the Advisors server is running on 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 with memory persists, experiment with higher values; however, the Advisors server 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).

For more information on the Java Virtual Machine options used in this section, 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 Advisors Platform

Advisors Server Controlled By Solution Control Server

This section describes how to change memory allocations for an Advisors server that is controlled by Solution Control Server (SCS). For a list of those components that are controlled by the SCS, see [Integration with Solution Control Server and Warm Standby](#).

You should consider changing the memory allocation for Advisors Platform server if the `geronimo.log` for the Advisors server is reporting an out of memory error. Set the heap size higher by editing one of these files:

- On Windows, `geronimo-tomcat6-minimal-2.2.1\bin\setenv.bat`
- On Linux, `geronimo-tomcat6-minimal-2.2.1/bin/setenv.sh`

Change the following settings—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):

```
GERONIMO_OPTS= ... -ms128m -mx1024m ...
```

to

```
GERONIMO_OPTS= ... -ms800m -mx1200m ...
```

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:

```
GERONIMO_OPTS= ... -XX:MaxPermSize=128m ...
```

to

```
GERONIMO_OPTS= ... -XX:MaxPermSize=256m ...
```

Important

When you specify memory allocation in the `setenv.sh` file, Genesys recommends that you 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
```

Advisors Server Controlled By Windows or Linux Service

This section describes how to change memory allocations for an Advisors server that is controlled by an OS service, not by SCS. For a list of those components controlled by an OS service, see [Integration with Solution Control Server and Warm Standby](#).

Set the heap size higher by editing the `<install dir>/conf/advisors-server-wrapper.conf` file.

About a third down the file, change the following lines—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
```

Change Memory Allocation for Advisors Genesys Adapter

Consider changing the memory allocation for Advisors Genesys Adapter (AGA) if its log is reporting an out of memory error. Set the heap size higher by editing one of these files:

- On Windows, run.bat
- On Linux, setenv.sh

Change the following settings—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):

```
set JAVA_OPTS=-ms128m -mx1024m ...
```

to

```
set JAVA_OPTS=-ms800m -mx1200m ...
```

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

```
set JAVA_OPTS= ... -XX:MaxPermSize=256m ...
```

Change Memory Allocation for CCAdv XML Generator

Consider changing the memory allocation for CCAdv XML Generator if its log is reporting an out of memory error. Set the heap size higher by editing one of these files:

- On Windows, xmlgen/run.bat
- On Linux, xmlgen/run.sh

Change the following settings—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):

```
.../java" -server -ms512m -mx1024m ...
```

to

```
.../java" -server -ms800m -mx1200m ...
```

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

```
.../java" ... -XX:MaxPermSize=128m ...
```

to

```
.../java" ... -XX:MaxPermSize=256m ...
```

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

`C:\<installation directory>\baseweb\images`

2. 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. 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. To modify colors on the login page, update the following stylesheet:

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

5. 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 `Require all denied` and to add `Require all granted`:

```
<Directory />
AllowOverride none
#Require all denied
Require all granted</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 /admin/ ajp://192.168.40.234:8009/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/
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://192.168.40.234:8009/wu/
ProxyPass /ca-xml/ ajp://192.168.40.234:8009/ca-xml/

# Genesys Resource Management Console Web Application
ProxyPass /rmc/ ajp://192.168.40.234:8009/rmc/

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

# Contact Center Advisor Mobile Edition

ProxyPass /ma/ ajp://192.168.40.234:8009/ma/
```

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.

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.

- **NEW** ProxyPass /fa/com.informiam.fa.admin.gwt.AdminConsole/
ajp://192.168.40.234:8009/fa/com.informiam.fa.admin.gwt.AdminConsole/
timeout=86400

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

Use the procedures on this page if you must change database connection information for Performance Management Advisors.

Advisors Platform and the Metric Graphing Data Source

There are two modules that contain JDBC data source configuration information for Advisors Platform and metric graphing:

- `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 procedures offline; Geronimo must be fully stopped.
- After you stop Geronimo, Genesys recommends that you take a complete directory backup of `<GCTI>/Advisors/` before you do any manual operations.
- Ensure that the Advisors service is not running.

Procedure: Changing Database Connection Parameters for Advisors Platform

Steps

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
```

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.

Procedure: Changing Database Connection Parameters for the Metric Graphing Data Source

Steps

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
```

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.

Changing Database Connection Parameters for CCAdv XML Generator

You can change the database connection information for XML Generator after installation. The XML Generator database connection information is located in the following file:

- conf/XMLGen.properties

See also [Modifying the XML Generator Configuration](#) for information about ensuring XML Generator works properly with the metrics database.

Changing Database Connection Parameters for Advisors Genesys Adapter

You can change the database connection information for Advisors Genesys Adapter after installation. The Advisors Genesys Adapter database connection information is located in the following files:

- conf\inf_genesys_adapter.properties
- conf\inf_genesys_importer.properties

Changing Database Connection Parameters for Advisors Cisco Adapter

You can change the database connection information for Advisors Cisco Adapter after installation. The Advisors Cisco Adapter database connection information is located in the following file:

-
- `conf\cisco_adapter.properties`

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. See also [Adjust the Log File Roll and Retention Settings](#).

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.

Advisors Genesys Adapter

This section contains information and procedures to help you change configuration for Advisors Genesys Adapter after this module is deployed.

Manage Advisors Stat Server Instances

NEW Starting in release 8.5.1, Stat Server registration is no longer done during deployment. Previously, you input Stat Server connection information in installer screens, which registered the Stat Servers. You now execute dedicated database procedures against the Advisors Platform database to:

- register or remove Stat Server instances
- add, edit, or remove Stat Server configuration settings related to Advisors

Performance Management Advisors include two stored procedures that you use to perform the preceding tasks:

- SPSTATSERVERCONFIG
- SPCHANGEOBJDISTRIBUTION

Microsoft SQL Server Database Procedures

If you have a Microsoft SQL Server database environment, you can use the `spStatServerConfig` and `spChangeObjDistribution` database procedures and parameters as shown in the [examples](#) for an Oracle environment, but replace the syntax to execute the stored procedures. MS SQL Server syntax is shown below.

MS SQL Server Syntax for `spStatServerConfig`

```
DECLARE @r int,
        @m varchar(4000);

EXEC spStatServerConfig
@p_SsPairId = null,
@p_ModuleCode = N'CCAdv',
@p_AdapterId = 1,
@p_StatServerHost = N'statserverhost.company.com',
@p_StatServerPort = 7002,
@p_StatServerName = N'SS812-68',
@p_StatServerDescr = N'CCAdv core stats',
@p_Core = 1,
@p_MultiMedia = 0,
@p_ThirdPartyMedia = 0,
@p_StatServerBackHost = NULL,
@p_StatServerBackPort = NULL,
@p_StatServerBackName = NULL,
@r = @r OUTPUT,
@m = @m OUTPUT;

SELECT @r as N'@r',
@m as N'@m';
```

MS SQL Server Syntax for spChangeObjDistribution

```
DECLARE @r int, @m varchar(255);
EXEC spChangeObjDistribution

@p_SsPairId_old = <original stat server pair id>, --from
@p_SsPairId_new = <target stat server pair id>, --to
@p_ModuleCode='CCAdv',
@r = @r OUTPUT,
@m = @m OUTPUT;

SELECT @m;
```

Oracle Database Example Procedures

Use the SPSTATSERVERCONFIG and SPCHANGEOBJDISTRIBUTION database procedures and parameters as shown in the following [examples](#).

The following examples show you how to use the stored database procedures to manage your Advisors Stat Server configuration if you use an Oracle environment, but the MS SQL Server procedures use the same parameters and processes:

- [Register a New Stat Server and Link the Stat Server to an Adapter](#)
- [Change the Connection Properties of the Stat Server](#)
- [Add New Statistic Types to the Existing Stat Server](#)
- [Remove Stat Server Statistic Type Assignments](#)
- [Re-distribute the Statistics Load when Stat Servers are Added](#)

Register a New Stat Server and Link the Stat Server to an Adapter

The following procedure uses CCAdv (Contact Center Advisor) for the module code. For Frontline Advisor, use the same procedure, but enter FA for the module code.

Procedure: Registering a Stat Server and Linking the Stat Server to the CCAdv Adapter

Purpose: In this example, the CCAdv adapter has id=1. The procedure instructs Stat Server to process only core statistics.

Steps

1. Call the procedure:

```
SET SERVEROUTPUT ON
SET FEEDBACK OFF
DECLARE
  R NUMBER;
  M VARCHAR2(4000);

BEGIN
  SPSTATSERVERCONFIG(
    P_SSPAIRID => NULL,
    P_MODULECODE => 'CCAdv',
    P_ADAPTERID => 1,
    P_STATSERVERHOST => 'statserverhost.company.com',
    P_STATSERVERPORT => 7002,
    P_STATSERVERNAME => 'SS812-68',
    P_STATSERVERDESCR => 'CCAdv core stats',
    P_CORE => 1,
    P_MULTIMEDIA => 0,
    P_THIRDPARTYMEDIA => 0,
    P_STATSERVERBACKNAME => NULL,
    P_STATSERVERBACKHOST => NULL,
    P_STATSERVERBACKPORT => NULL,
    R => R,
    M => M
  );
END;
/
```

Change the Connection Properties of the Stat Server

Procedure: Changing the Stat Server Connection Properties

Purpose: This example changes the connection properties of the Stat Server added in the **first example** above.

Steps

1. Determine the Stat Server pair ID:

```
SELECT SS_PAIR_ID FROM STAT_SERVER_INSTANCES WHERE NAME='SS812-33';
```

2. In this example, assume the Stat Server pair ID is 5. Call the procedure:

```
SET SERVEROUTPUT ON
SET FEEDBACK OFF
DECLARE
R NUMBER;
M VARCHAR2(4000);

BEGIN
SPSTATSERVERCONFIG(
P_SSPAIRID => 5,
P_MODULECODE => 'CCAdv',
P_ADAPTERID =>1,
P_STATSERVERHOST => 'statserverhost2.company.com',
P_STATSERVERPORT => 7003,
P_STATSERVERNAME => 'SS812-70'
P_STATSERVERDESCR => 'CCAdv core stats',
P_CORE => 1,
P_MULTIMEDIA => 0,
P_THIRDPARTYMEDIA => 0,
P_STATSERVERBACKNAME => NULL,
P_STATSERVERBACKHOST => NULL,
P_STATSERVERBACKPORT => NULL,
R => R,
M => M
);
END;
/
```

Add New Statistic Types to the Existing Stat Server

Procedure: Adding new Statistic Types to a Registered Stat Server

Purpose: In this example, the procedure adds the multimedia statistic type.

Steps

1. Determine the Stat Server pair ID:

```
SELECT SS_PAIR_ID FROM STAT_SERVER_INSTANCES WHERE NAME='SS812-33';
```

2. In this example, assume the Stat Server pair ID is 5. Call the procedure:

```
SET SERVEROUTPUT ON
SET FEEDBACK OFF
DECLARE
R NUMBER;
```

```

M VARCHAR2(4000);

BEGIN
SPSTATSERVERCONFIG(
P_SSPAIRID => 5,
P_MODULECODE => 'CCAdv',
P_ADAPTERID =>1,
P_STATSERVERHOST => 'statserverhost2.company.com',
P_STATSERVERPORT => 7003,
P_STATSERVERNAME => 'SS812-70',
P_STATSERVERDESCR => 'CCAdv core stats',
P_CORE => 1,
P_MULTIMEDIA => 1,
P_THIRDPARTYMEDIA => 0,
P_STATSERVERBACKNAME => NULL,
P_STATSERVERBACKHOST => NULL,
P_STATSERVERBACKPORT => NULL,
R => R,
M => M
);
END;
/

```

Remove Stat Server Statistic Type Assignments

Procedure: Removing Stat Server Statistic Type Assignments

Purpose: In this example, the procedure removes multimedia and third party media statistic types.

Steps

1. Determine the Stat Server pair ID:

```
SELECT SS_PAIR_ID FROM STAT_SERVER_INSTANCES WHERE NAME='SS812-33';
```

2. In this example, assume the Stat Server pair ID is 5. Call the procedure; set the parameters to 0 that are associated with statistic types that you want to remove. For example, the following procedure removes multimedia and third party media statistic types:

```

SET SERVEROUTPUT ON
SET FEEDBACK OFF
DECLARE
R NUMBER;
M VARCHAR2(4000);

BEGIN

```

```

SPSTATSERVERCONFIG(
P_SSPAIRID => 5,
P_MODULECODE => 'CCAdv',
P_ADAPTERID =>1,
P_STATSERVERHOST => 'statserverhost2.company.com',
P_STATSERVERPORT => 7003,
P_STATSERVERNAME => 'SS812-70',
P_STATSERVERDESCR => 'CCAdv core stats',
P_CORE => 1,
P_MULTIMEDIA => 0,
P_THIRDPARTYMEDIA => 0,
P_STATSERVERBACKNAME => NULL,
P_STATSERVERBACKHOST => NULL,
P_STATSERVERBACKPORT => NULL,
R => R,
M => M
);
END;
/

```

The procedure returns a message depending on the outcome: success, or failure with further instructions.

The failure to remove a statistic type usually occurs when there are already objects associated with the Stat Server and the corresponding statistic type.

If the goal is to move the processing of a statistic type to another Stat Server, then you must move all related objects to the corresponding Stat Server. You can move the objects by executing the following procedure:

```

SET SERVEROUTPUT ON
SET FEEDBACK OFF
DECLARE
P_SSPAIRID_OLD NUMBER;
P_SSPAIRID_NEW NUMBER;
P_MODULECODE VARCHAR2(200);
R NUMBER;
M VARCHAR2(4000);

BEGIN
P_SSPAIRID_OLD := <original Stat Server pair id>; --from
P_SSPAIRID_NEW := <target Stat Server pair id>; --to
P_MODULECODE:= NULL;

SPCHANGEOBJDISTRIBUTION(
P_SSPAIRID_OLD => P_SSPAIRID_OLD,
P_SSPAIRID_NEW => P_SSPAIRID_NEW,
P_MODULECODE => P_MODULECODE,
R => R,
M => M
);

COMMIT;
dbms_output.put_line(M);
END;
/

```

After the objects are moved, execute the SPSTATSERVERCONFIG procedure again using the same parameters you used initially.

Remove a Stat Server Record

Procedure: Removing a Stat Server Record

Prerequisites

- You must remove Stat Server statistic type assignments (see [Remove Stat Server Statistic Type Assignments](#)) before removing a Stat Server record.

Steps

1. Execute SPSTATSERVERCONFIG to remove all statistic types as explained in [Remove Stat Server Statistic Type Assignments](#). If the procedure returns a failure, do one of the following:
 - a. Move objects to another Stat Server by executing the SPCHANGEOBJDISTRIBUTION procedure as explained in [Remove Stat Server Statistic Type Assignments](#). After objects have been moved to another Stat Server, execute SPSTATSERVERCONFIG again using the same parameters you used initially.
 - b. Force object deletion. In this case, object distribution will be done automatically by the Advisors Genesys Adapter when it starts or during the overnight update. To force object deletion, execute the SPCHANGEOBJDISTRIBUTION procedure with stat type parameters set to -1:

```
SET SERVEROUTPUT ON
SET FEEDBACK OFF
DECLARE
  R NUMBER;
  M VARCHAR2(4000);

BEGIN
  SPSTATSERVERCONFIG(
    P_SSPAIRID => 5 ,
    P_MODULECODE => 'CCAdv',
    P_ADAPTERID => 1,
    P_STATSERVERHOST => 'statserverhost2.company.com',
    P_STATSERVERPORT => 7003,
    P_STATSERVERNAME => 'SS812-70',
    P_STATSERVERDESCR => 'CCAdv core stats',
    P_CORE => -1 ,
    P_MULTIMEDIA => -1,
    P_THIRDPARTYMEDIA => -1,
    P_STATSERVERBACKNAME => NULL,
    P_STATSERVERBACKHOST => NULL,
    P_STATSERVERBACKPORT => NULL,
    R => R,
    M => M
  );
END;
/
```

2. Execute a simple delete statement to remove the Stat Server instance:

```
DELETE STAT_SERVER_INSTANCES WHERE SS_PAIR_ID=<the id of the Stat Server to be
deleted>;

COMMIT;
```

Re-distribute the Statistics Load when Stat Servers are Added

The relationship between a statistic and the Stat Server pair against which it is requested is maintained. This means that after a start, restart, or refresh of the adapter, each adapter continues to request statistics from the same Stat Server(s) from which it requested stats before the restart. 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 adapters, the statistics already requested from existing Stat Servers are not automatically re-distributed to the newly added Stat Server pair. The following procedures describe two scenarios in which you would re-distribute the statistics load on the Advisors Stat Servers. See:

- [Moving Statistics of a Specific Type to a New Stat Server](#)
- [Evenly Distributing Stats Load After Adding a New Stat Server](#)

Procedure: Moving Statistics of a Specific Type to a New Stat Server

Purpose: In this example, you have a Stat Server configured to process core and multimedia statistics. You decide to add a Stat Server to handle only multimedia statistics. You will move all multimedia processing to the new Stat Server.

Steps

1. Stop the Advisors server, all Advisors Genesys Adapters, and XML Generator.
2. [Register a new Stat Server](#).
3. Determine the `SS_PAIR_ID` of each Stat Server:

```
P_SSPAIRID_OLD,P_SSPAIRID_NEW
SELECT SS_PAIR_ID,NAME FROM STAT_SERVER_INSTANCES;
```

4. Execute the `SPCHANGEOBJDISTRIBUTION` procedure:


```

SET SERVEROUTPUT ON
SET FEEDBACK OFF
DECLARE
P_SSPAIRID_OLD NUMBER;
P_SSPAIRID_NEW NUMBER;
P_MODULECODE VARCHAR2(200);
R NUMBER;
M VARCHAR2(4000);

BEGIN
P_SSPAIRID_OLD := <original stat server pair id>; --from
P_SSPAIRID_NEW := <target stat server pair id>; --to
P_MODULECODE := NULL;

SPCHANGEOBJDISTRIBUTION(
P_SSPAIRID_OLD => P_SSPAIRID_OLD,
P_SSPAIRID_NEW => P_SSPAIRID_NEW,
P_MODULECODE => P_MODULECODE,
R => R,
M => M
);

COMMIT;
dbms_output.put_line(M);
END;
/

```

5. To ensure that no multimedia statistics are ever distributed to your original Stat Server again, disassociate the multimedia statistic type from that Stat Server:

```

SET SERVEROUTPUT ON
SET FEEDBACK OFF
DECLARE
R NUMBER;
M VARCHAR2(4000);

BEGIN
SPSTATSERVERCONFIG(
P_SSPAIRID => 5 ,
P_MODULECODE => 'CCAdv', --mandatory if P_ADAPTERID is not supplied
P_ADAPTERID =>1, --mandatory if P_MODULECODE is not supplied
P_STATSERVERHOST => 'statserverhost2.company.com',
P_STATSERVERPORT => 7003,
P_STATSERVERNAME => 'SS812-70',
P_STATSERVERDESCR => 'CCAdv core stats',
P_CORE => 1 ,
P_MULTIMEDIA => 0,
P_THIRDPARTYMEDIA => 0,
P_STATSERVERBACKNAME => NULL,
P_STATSERVERBACKHOST => NULL,
P_STATSERVERBACKPORT => NULL,
R => R,
M => M
);
END;
/

```

6. Start all Advisors Genesys Adapters, XML Generator, and the Advisors server.

Procedure: Evenly Distributing Stats Load After Adding a New Stat Server

Purpose: In this example, you have a Stat Server configured to process one or more statistic types. You decide to add another Stat Server to process the same statistic types. You will distribute the statistics load evenly between the two Stat Servers and not separate the statistic type processing.

In this scenario, it is best to initiate the automatic statistic load distribution.

Steps

1. Stop the FA Server, all Advisors Genesys Adapters, and, for CCAdv, XML Generator.
2. Connect to the platform database.
3. Remove all entries from STAT_GROUP_OBJ_MAPPING, and commit the changes:

- **Oracle:**

```
DELETE STAT_GROUP_OBJ_MAPPING;  
COMMIT;
```

- **MSSQL:**

```
BEGIN TRANSACTION;  
DELETE STAT_GROUP_OBJ_MAPPING;  
COMMIT TRANSACTION;
```

4. Restart all stopped components:
 - For CCAdv: Restart all CCAdv adapter servers and XML Generator.
 - For FA adapters: Restart all FA adapter servers and the FA Server.

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 options specified in the **stored procedures**. Primary and backup, in this case, are not related to the primary and backup Stat Server designation in Configuration Manager.

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 the original primary Stat Server has only just come back online, it needs to be given sufficient time to accumulate historical aggregated statistic counts. One-day metrics are used in CCAdv; therefore 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.

Configure the Daily Reset Time for Statistics on a Stat Server

NEW Prior to Advisors release 8.5.101, statistics from each Stat Server for the One day/Growing time profiles reset daily at 00:00 hours (midnight) in the time zone configured at each Stat Server. If the Stat Servers were in a very different time zone than the Advisors users, then the statistics might reset during the users' work day.

Starting with Advisors release 8.5.101, you can specify at what time each Stat Server is to reset the statistics daily (that is, for the One day/Growing time profiles). Midnight (00:00 hours) continues to be the default value. You must specify the reset time for each Stat Server, as applicable. The configuration is applicable to both Contact Center Advisor/Workforce Advisor (CCAdv/WA) and Frontline Advisor (FA) Stat Servers configured on the respective Advisors Genesys Adapter (AGA) instances.

In the Stat Server options, the default time profile is defined in the TimeProfiles section. For example, the default value is:

```
[TimeProfiles]
Default,Growing=00:00
```

In the preceding example, there is one time profile configured – it is the default growing time profile, and it is configured to grow for 24 hours (daily). The reset time is not specified; the Stat Server will reset, by default, at 00:00 hours. Another way to specify this is:

```
Default,Growing=00:00+00:00
```

The value before the "+" sign indicates the reset time of 00:00 hours.

If you need to change the reset time for daily statistics, you must specify it using the 24-hour format. For example, if you want to specify a reset time of 02:00 hours, use the following configuration:

```
[TimeProfiles]
Default,Growing=02:00+00:00
```

Tip

The name of the default time profile is configurable. If the default time profile already exists on a given Stat Server for other purposes, then you can configure a different time profile name to use with Advisors.

See also `genesys_connector.default_time_profile.oneday = Default,Growing`.

When do Changes Take Effect?

If you change the One day/Growing time profile reset time in the Stat Server options, the corresponding AGA instances must be restarted for the configuration changes to take effect. To avoid the restart, Genesys recommends that you configure the Stat Server TimeProfiles options, as required, at the time of deployment.

Redistribute Statistics 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 redistribute the total load of statistics among the adapters, including the adapters you added after the initial deployment.

Redistributing the Statistics Load

Procedure:

Steps

1. Stop the FA Server and all Advisors Genesys Adapters. For CCAdv, you also need to stop XML Generator.
2. Connect to the platform database.
3. Remove all entries from the STAT_GROUP_OBJ_MAPPING table, and commit the changes:

- **Oracle:**

```
DELETE STAT_GROUP_OBJ_MAPPING;  
COMMIT;
```

- **MSSQL:**

```
BEGIN TRANSACTION;  
DELETE STAT_GROUP_OBJ_MAPPING;  
COMMIT TRANSACTION;
```

4. Restart all stopped components:
 - For CCAdv: Restart all CCAdv adapter servers and XML Generator.
 - For FA adapters: Restart all FA adapter servers and the FA server.

After the restart, the total load of statistics should be redistributed among all the Advisors

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.CCAdvChannel</code> = 10	Frequency of the transformer upload task for CCAdv. 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> = 60	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> = 1000 <code>informiam.genesys_connector.statServer.interGroupDelay</code> = 1	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> = false	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.</p> <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 <code>true</code> 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>
<code>informiam.genesys_connector.statServer.onStartWaitTimeForAllSSConnectionsToOpen = 20</code>	<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>
 <code>genesys_connector.default_time_profile.oneday = Default, Growing</code>	<p>Specify the time profile to use in the statistics requests.</p> <p>Starting with Advisors release 8.5.101, you can specify the time at which each Advisors Stat Server is to reset the daily statistics by configuring the One day/Growing TimeProfiles options in the Stat Servers.</p> <p>Ensure you configure the AGA parameter to match the time profile specified on the Stat Server from which AGA is requesting statistics.</p> <p>See Configure the Daily Reset Time for Statistics on a Stat Server for more information.</p>
<code>informiam.genesys_connector.configServer.reconnect.attempts = 5</code> <code>informiam.genesys_connector.configServer.reconnect.attemptInterval = 30</code>	<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>
<code>informiam.genesys_connector.statServer.reconnect.attempts = 3</code> <code>informiam.genesys_connector.statServer.reconnect.attemptInterval = 10</code>	<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>
<code>informiam.genesys_connector.api.port =</code>	The port of communication between CCAAdv and the Genesys Adapter and between FA and the Genesys Adapter.

Parameter	Description
<code>informiam.genesys_connector.waitForStatOpenEventsTimeout</code> = 600	Process timeout values, in seconds. 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.
<code>informiam.genesys_connector.numOfMaxStatRerequestTimes</code> = 3	Number of times the connector will attempt to re-request statistics. 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.
<code>informiam.genesys_connector.configServer.addp.turnon</code> = true <code>informiam.genesys_connector.configServer.addp.tracemode</code> = <code>informiam.genesys_connector.configServer.addp.servvertimeout</code> = 300 <code>informiam.genesys_connector.configServer.addp.clienttimeout</code> = 120 <code>informiam.genesys_connector.configServer.protocol.request.timeout</code> = 180	ADDP Settings to be used with the Configuration Server connection.
<code>informiam.genesys_connector.statServer.addp.turnon</code> = true <code>informiam.genesys_connector.statServer.addp.tracemode</code> = <code>informiam.genesys_connector.statServer.addp.servvertimeout</code> = 300 <code>informiam.genesys_connector.statServer.addp.clienttimeout</code> = 120	ADDP Settings to be used with the Stat Server connections.
<code>informiam.genesys_connector.transformerjob.pausechecklimit</code> = 25000 <code>informiam.genesys_connector.statsissue.pausechecklimit</code> = 5000	Pause parameters that check against the queue of the incoming Stat Server messages. 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. In environments where sufficient runtime memory is not available, consider setting these limits to a smaller value. Setting a very small value could lead to delay in sending the updates to the Advisors dashboard.
<code>informiam.genesys_connector.psdk.server.fileEncoding</code> = windows-1252	File encoding to be used with the Configuration Server and the Stat Server connections. 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.

Parameter	Description
<code>genesys_connector.configServer.tls.enabled</code>	<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 (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.</p>
<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</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 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.

NEW 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 the Stat Servers configured for that adapter instance. You can use the SPSTATSERVERCONFIG stored procedure to remove the Stat Server configuration records. See [Manage Advisors Stat Server Instances](#) for more information.

Manage Restart of Multiple Adapters with Single Metrics Database

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. This property is not applicable to FA adapters.

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.

When primary and backup adapter instances are deployed for warm standby, this property must be set to `true` on only one pair of Adapters (on both the primary and backup of one selected pair).

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.

Purge Key Action Reports and Historical Alerts

NEW Advisors alert and action management features can generate historical alert and action management report data that the Advisors application never removes automatically. An Advisors database administrator can delete or purge the data with a scheduled job or a manual operation.

The historical data purge process relies on properties recorded in the Platform database table `CONFIG_PARAMETER`:

- `keyactions.purging.timeframe.months`: Applicable to CCAdv and WA only.
- `keyactions.purging.successrating.value`: Applicable to CCAdv and WA only. *Success rating* refers to the success rating system used in Key Action Reports (see [Key Action Reports Table](#) for more information about Key Action Reports).
- `keyactions.purging.successrating.range`: Applicable to CCAdv and WA only. *Success rating* refers to the success rating system used in Key Action Reports (see [Key Action Reports Table](#) for more information about Key Action Reports).
- `fa.archive.purging.timeframe.months`: applicable to FA only; purges archived threshold violations

Your database administrator can modify the parameters to address your enterprise's needs and data cleanup policies.

Parameter Name	Parameter Value	Description
keyactions.purging.timeframe.months	12	Number of months to purge historical data.
keyactions.purging.successrating.value	2	The value of the success rating system used in Key Action Reports.
keyactions.purging.successrating.range	<	The range of the success rating system used in Key Action Reports.
fa.archive.purging.timeframe.months	12	Number of months to purge archived threshold violations.

Alert and Action Management Report Parameters

The Figure "Alert and Action Management Report Parameters" shows the default values for the relevant parameters in the `CONFIG_PARAMETER` table.

The `keyactions.purging.successrating.value` and `keyactions.purging.successrating.range` parameters depend on each other. If one of the parameters is not defined, the other is ignored.

Example

To trigger the purge of data related to Action Management reports that have a success rating less than two, you must set `keyactions.purging.successrating.value` to 2 and `keyactions.purging.successrating.range` to `<`.

If the `keyactions.purging.successrating.value` and `keyactions.purging.successrating.range` parameters are not defined, *all* records are removed based on the `keyactions.purging.timeframe.months` parameter setting.

If, in affected Action Management report data, the success rating is not defined (that is, NULL), the records are removed if the related historical alerts meet the `keyactions.purging.timeframe.months` condition.

Calling Stored Procedures to Purge Key Action Reports and Historical Alerts

Regardless of the method used to purge key action reports and historical alerts (manual operation and/or scheduled job), the process must contain a call of the stored procedure that removes the data from all related tables. The stored procedure has no input parameters. The procedure purges the data based on the criteria generated from the related configuration parameters present in the `CONFIG_PARAMETER` table at the time of procedure execution.

MSSQL procedure call

```
EXEC      [spPurgeAMHistory]
          @p_AmrPurged = @p_AmrPurged OUTPUT,
          @p_HstAlertsPurged = @p_HstAlertsPurged OUTPUT,
          @p_HstFATHresholdsPurged = @p_HstFATHresholdsPurged OUTPUT,
          @p_AmrEndDate = @p_AmrEndDate OUTPUT,
          @p_HstAlertEndDate = @p_HstAlertEndDate OUTPUT,
          @p_HstFaThresholdEndDate = @p_HstFaThresholdEndDate OUTPUT,
          @r = @r OUTPUT,
          @m = @m OUTPUT,
          @r1 = @r1 OUTPUT,
          @m1 = @m1 OUTPUT,
          @r2 = @r2 OUTPUT,
          @m2 = @m2 OUTPUT,
          @r3 = @r3 OUTPUT,
          @m3 = @m3 OUTPUT

SELECT    @p_AmrPurged as N'@p_AmrPurged',
          @p_HstAlertsPurged as N'@p_HstAlertsPurged',
          @p_HstFATHresholdsPurged as N'@p_HstFATHresholdsPurged',
          @p_AmrEndDate as N'@p_AmrEndDate',
          @p_HstAlertEndDate as N'@p_HstAlertEndDate',
          @p_HstFaThresholdEndDate as N'@p_HstFaThresholdEndDate',
          @r as N'@r',
          @m as N'@m',
          @r1 as N'@r1',
          @m1 as N'@m1',
          @r2 as N'@r2',
          @m2 as N'@m2',
          @r3 as N'@r3',
          @m3 as N'@m3'
```

GO

Oracle procedure call

```
SET SERVEROUTPUT ON
SET FEEDBACK OFF
DECLARE
  P_AMRPURGED NUMBER;
  P_HSTALERTSPURGED NUMBER;
  P_HSTFATHRESHOLDSPURGED NUMBER;
  P_AMRENDDATE DATE;
  P_HSTALERTENDDATE DATE;
  P_HSTFATHRESHOLDENDDATE DATE;
```

```
R NUMBER;
M NVARCHAR2(2000);
R1 NUMBER;
M1 NVARCHAR2(2000);
R2 NUMBER;
M2 NVARCHAR2(2000);
R3 NUMBER;
M3 NVARCHAR2(2000);
BEGIN

SPPURGEAMHISTORY(
  P_AMRPURGED => P_AMRPURGED,
  P_HSTALERTSPURGED => P_HSTALERTSPURGED,
  P_HSTFATHRESHOLDSPURGED => P_HSTFATHRESHOLDSPURGED,
  P_AMRENDDATE => P_AMRENDDATE,
  P_HSTALERTENDDATE => P_HSTALERTENDDATE,
  P_HSTFATHRESHOLDENDDATE => P_HSTFATHRESHOLDENDDATE,
  R => R,
  M => M,
  R1 => R1,
  M1 => M1,
  R2 => R2,
  M2 => M2,
  R3 => R3,
  M3 => M3
);

END;

/
```

Find and Edit XML Generator Properties

NEW Starting in release 8.5.1, XML Generator no longer requires Advisors Platform to function; that is, it is no longer necessary to install Advisors Platform to support Contact Center Advisor XML Generator.

XML Generator now monitors the Administration module; if you change configuration in the Administration module, XML Generator directs Genesys Adapter to retrieve stats data.

Also starting in release 8.5.1, you must configure an XML Generator **Application** in Configuration Manager or Genesys Administrator. For more information, see [Integration with Solution Control Server and Warm Standby](#).

Important

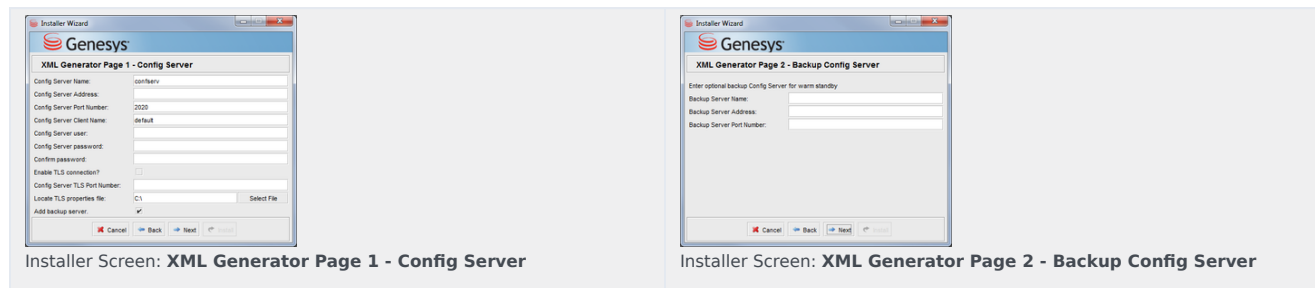
Business objects such as application groups or contact centers are not loaded in the database by starting the XML Generator alone, and will only appear after the Geronimo application server has started.

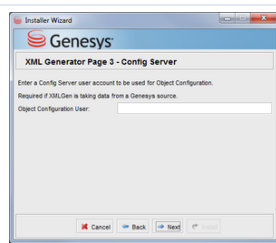
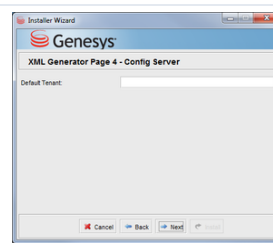
Properties Files

When you deploy XML Generator, the installer prompts for properties for which the Advisors Platform also prompts because XML Generator now contains and installs some of the same functionality. The XML Generator properties files are described below, including the relationship of the files to the installer screens.

GenesysConfig.properties File

XML Generator stores the data you enter on the following installer screens in the GenesysConfig.properties file.



Installer Screen: **XML Generator Page 3 - Config Server**Installer Screen: **XML Generator Page 4 - Config Server**

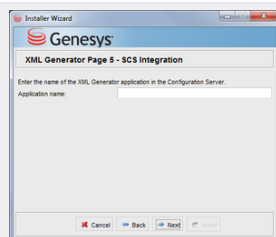
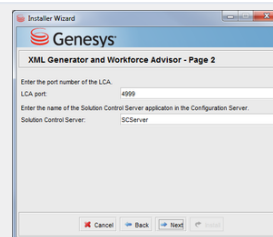
Important

When you install XML Generator, it will not overwrite an existing GenesysConfig.properties file in the conf directory (created by a previous installation of Advisors Platform).

Due to the separation of Advisors Platform and XML Generator, it is no longer necessary to launch Advisors Platform before you launch XML Generator.

XMLGen.properties File

Data from the following installer screens is stored in the XMLGen.properties file:

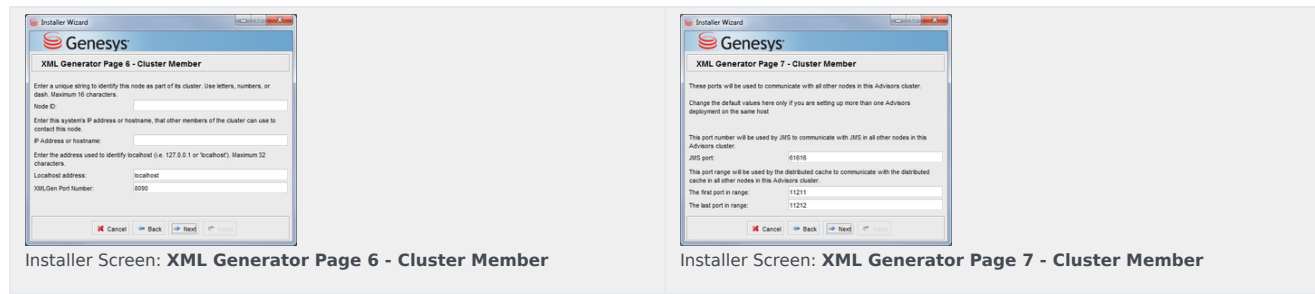
Installer Screen: **XML Generator Page 5 - SCS Integration**Installer Screen: **XML Generator and Workforce Advisor - Page 2**

Tip

A new property has been added to the XMLGen.properties file starting in release 8.5.1: `advisors.xmlgen.webserver.port`. The default port number is 8090, however this port number must be the same as the port specified for the XML Generator Application in the Configuration Server. Ensure you manually update the port number associated with the `advisors.xmlgen.webserver.port` property if you change the port number for the XML Generator Application in the Configuration Server.

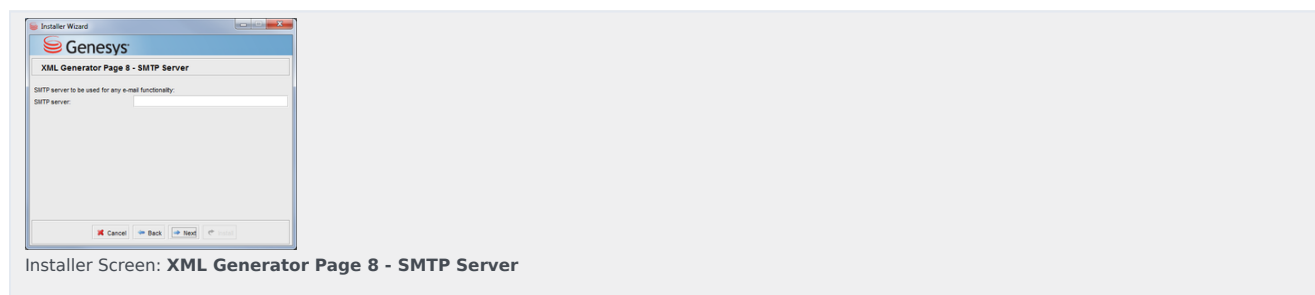
ActiveMQ.properties and Caching.properties Files

Data from the following installer screens is entered in the ActiveMQ.properties and Caching.properties files in the Advisors database:



MailService.properties File

Data from the following screen is stored in MailService.properties file:



Edit XML Generator Configuration

Use the following procedures to modify XML Generator configuration:

- [Modifying the XML Generator Configuration](#)
- [Changing the XML Generator Connection](#)

Modifying the XML Generator Configuration

Procedure:

Purpose: To ensure that XML Generator works properly with the metrics database.

Steps

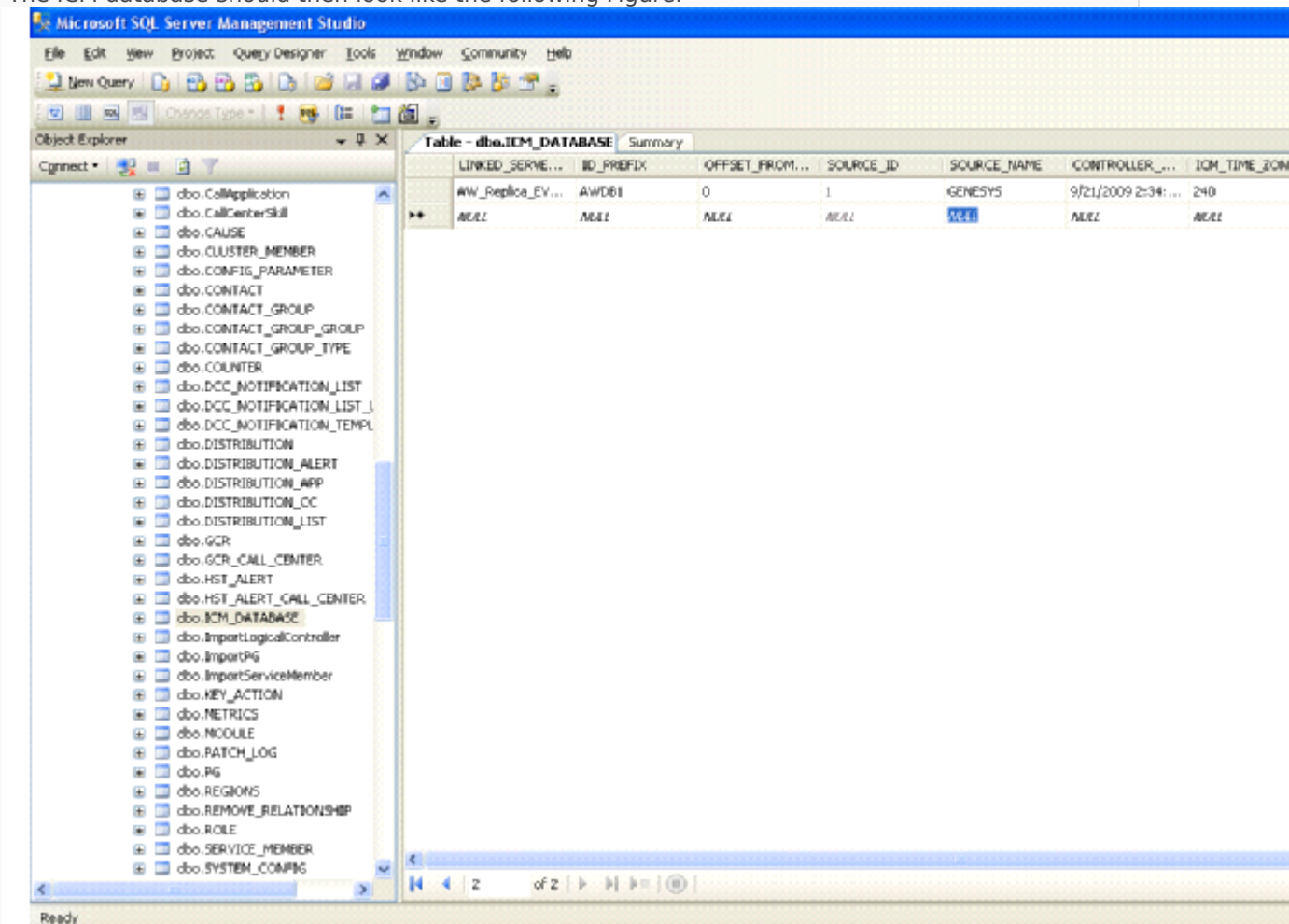
1. After installation of XML Generator, there should be a row in the Platform database in the ICM_DATABASE table corresponding to the CCAdv/WA metrics database. If not, add this row. This

row is necessary to ensure that XML Generator works properly with the metrics database.

- 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.



ICM Database screen

Changing the XML Generator Connection

You can change the database connection information for XML Generator after installation. The XML

Generator database connection information is located in the following file:

- `conf/XMLGen.properties`

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

Configure Resource Management Console Properties

NEW You can configure parameters for the Resource Management console (RMC) to make the application more specific to the user configuration in your enterprise.

Edit the `RMCInfo.xml` configuration file, found in the following directory:

```
Advisors\geronimo-tomcat6-minimal-2.2.1\repository\com\informiam\genesys\rmc-web\<version>\rmc-web-8.x.xxx_<version>.war\WEB-INF\classes
```

After you change properties in this file, restart the Advisors server on which RMC is running.

Automatic Dashboard Refresh Interval

By default, the RMC dashboard does not refresh the content automatically, however you can configure an automatic refresh. Set `refreshTime` to a number of seconds that is not zero (the default value). Genesys suggests a value of 60 or more. There is no benefit to setting the refresh interval to less than 60 seconds because it can take more than 45 seconds to retrieve information if a user opens the RMC dashboard to display the agents related to a level in the **Contact Centers** pane of a CCAdv or WA dashboard.

```
<param name="refreshTime" value="60" />
```

Users of RMC can still click the **Refresh** button to refresh the dashboard at any time if it is not refreshing automatically.

Procedure: Tuning the RMC Refresh Interval

Purpose: To find out how long it takes for the RMC server to respond to a typical query for data, and to tune the refresh time based on that information.

Steps

1. Edit the `geronimo-tomcat6-minimal-2.2.1\var\log\server-log4j.properties` file:
 - a. Set the logging category `log4j.category.com.informiam.genesys.dcc` to `DEBUG`.

- b. Save the file and wait at least one minute.
2. Use RMC, opening its dashboard on data as you typically would in the CCAdv or WA dashboard.
3. Examine the log to see how long it takes to process each request for agents' data.
4. Set the refresh time to a higher value than the longest duration found.
5. Set the logging category `log4j.category.com.informiam.genesys.dcc` to `INFO`.
6. Restart the Geronimo server that is running RMC.

Maximum Skill Level in Dashboard

In the RMC dashboard, users with the correct Advisors permission can assign and remove agent skills, as well as change the skill level of the agents' existing skill. The dashboard presents a set of numeric skill levels, from 0 to n , where n is the maximum that can be assigned.

The default maximum skill level is 10. You can change it by setting `maxSkillLevel` to a different value. To set it to 5, for example:

```
<param name="maxSkillLevel" value="5" />
```

Number of Concurrent Users of RMC (8.5.101 Only)

The default value of the `expectedNumberConcurrentUsers` property is 10, which you can leave unchanged if you have 10 or fewer users using RMC simultaneously.

If you typically have more than 10 people using RMC simultaneously, the value you specify for the `expectedNumberConcurrentUsers` property should more accurately reflect the maximum number. If the value you use for the `expectedNumberConcurrentUsers` property is too small in relation to the number of people simultaneously using RMC, then RMC might become slow to respond as more and more users open RMC.

Change the number of concurrent RMC users by setting `expectedNumberConcurrentUsers` to a different value. For example, to set it to 20:

```
<param name="expectedNumberConcurrentUsers" value="20" />
```

Other RMC Properties

For details on the other properties in `RMCInfo.xml`, see [Deploying SDS and RMC](#).

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 XML Generator.

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 XML Generator.

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 **Report Metrics** page of the Administration module to enable a metric and time profile 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**.
- The number of metric/time profile combinations that can be graphed.
See **Specify the number of metric/time profile combinations**.

<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 should 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 should 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.

| -| Specify the number of metric/time profile combinations=

Use this procedure to specify the number of metric/time profile combinations that users can graph. Use this procedure if you try to configure more than the default maximum number of metric/time profile combinations for graphing in the **Report Metrics** page of the Administration module, and you receive an error saying you cannot configure any more.

1. In the Advisors database, execute:

```
UPDATE CONFIG_PARAMETER SET PARAM_VALUE = 'n'  
Where  
PARAM_NAME = 'max.metrics.graphing.enabled'
```

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

Important

This parameter is shared by all Advisors modules, including CCAdv and WA. The parameter governs the total number of graphable combinations in both CCAdv and WA. While this property can theoretically be set to any value, Genesys recommends you configure the limit to be 5 or less for performance reasons. Each metric/time profile combination is counted as 1. For example, if you select AHT 30 Min Growing and AHT 5 Min Sliding, that is counted as 2 graph-enabled metrics.

Change the Default Service Level Threshold Setting

Advisors uses the following four raw report metrics to calculate the SL% (Aband) metric value for CCAdv:

- SLC
- SLAbn
- SLCH, and
- ServiceLevelCallsOnHold (SLCHId)

To change the Service Level threshold configuration, you edit the preceding four metrics. Changes to the Service Level threshold take effect after the overnight refresh, or if you stop and then restart XML Generator. If you have an HA deployment, you must stop the primary XML Generator, and then the backup XML Generator, and restart both to force changes to take effect.

A change to the Service Level threshold setting does not affect the applications that are already assigned to roll up on the **Application Configuration** page of the administration module; those applications maintain the Service Level threshold that was selected at the time of the rollup assignment.

Procedure: Changing the Default Service Level Threshold Configuration (CCAdv)

Purpose: The example in the procedure below changes the Service Level threshold from the default 20 seconds to 30 seconds.

Prerequisites

- You require permissions to edit raw report metrics in the Report Metric Manager.

Steps

1. For the SLC and SLAbn metrics, change the **Time Range Upper Bound** from the default value of 20 to 30.
2. For the SLCH and ServiceLevelCallsOnHold metrics, change the **Time Range Lower Bound** from the default value of 20 to 30.

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 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

Procedure:

Purpose: CCAdv XML Generator uses a third-party JDBC data source. Use this procedure to review the JDBC data source error logs.

Steps

1. Edit `xmlgen/log4j.xml`:
 - a. Find the category for `com.mchange`.
 - b. Change the level to `DEBUG`.
 - c. Save the file.
2. Wait at least 60 seconds.
3. 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

When you deploy CCAdv and WA, you specify a time profile for the historical agent group metrics that will display on the dashboards of those components. Post-installation, 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 CCAdv Web Services and WA Web Services.
2. Stop Advisors CCAdv XML Generator and Workforce Advisor Server from the Solution Control Server UI.
3. 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`
4. Start Advisors CCAdv XML Generator and Workforce Advisor server from the Solution Control Server UI.
5. Start the Windows services for CCAdv Web Services and WA Web Services.

Users may log in again.

6. 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 about alerts that is sent by Contact Center Advisor XML Generator and Workforce Advisor Server. 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 the Geronimo that is running WA Server.

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 and 8.5.1.)

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	<code>\${call.center.name.en}</code>

Description	Property
contact center, associated with the alert.	<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 Alert Creation Delay Interval (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 `${application.group.name.de}`.
 Verletzte Metrik: `${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}`.

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. In the Solution Control Server UI, stop the application that controls CCAdv XML Generator on the system on which you are going to run the e-mail tester.
2. Change directory to the Advisors base directory (the one in which you installed Genesys Advisors), and then change it to `\xmlgen`.
3. Run the command:
`emailtest.bat` or
`emailtest.sh` or
4. Wait until the test application has exited, and check its output for errors.
5. Check the e-mail received at the address that is the value of the `connectionFailureRetryParams.supportEmail` property in `conf/XMLGen.properties`.
6. Update the templates for the e-mail and repeat the above steps until you are satisfied.
7. In the Solution Control Server UI, clear the effect of the e-mail tester: choose Stop again on the application that controls XML Generator.
8. Start CCAdv XMLGenerator again from the Solution Control Server UI.

Importing Contact Groups into Advisors

Data for Contact Groups

Workforce Advisor accepts data from three WFM systems:

- Genesys Workforce Management (WFM)
- IEX TotalView
- Aspect eWFM

See *Workforce Advisor* in the [Genesys 7.x - 9.x Product Availability table](#) of 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](#)

Importing Contact Groups into Primary and Backup WA Servers

In a deployment of WA Server that supports **warm standby HA**, WA Server is installed on two different systems.

The same is true in a deployment that supports **cold standby**.

In such deployments, the configuration to import contact groups must be done on both of those systems.

If you perform the configuration, for example, only on the system that runs the primary WA Server, and then that system fails over to the backup system, the WA Server that runs there will not have any forecast data about contact groups to use in its calculations. The WA dashboards will display N/A for contact groups' metrics and metrics that depend on them.

[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=WFMProd01-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 WFMProd01.
- 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.
- $FNCOTotal \text{ for 30 minutes} = FNCOTotal^1 + FNCOTotal^2$.
 - If either $FNCOTotal^1$ or $FNCOTotal^2$ 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.
- $AdjSCH \text{ for 30 minutes} = (AdjSCH^1 * FNCO^1 * FAHT^1 + AdjSCH^2 * FNCO^2 * FAHT^2) / (FNCO^1 * FAHT^1 + FNCO^2 * FAHT^2)$.

$FNCO^2 * FAHT^2$).

- 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	RAVL	PERF_ITEM_FRC_IV
FAHT	Forecast AHT	fcstAHT	fcstAHT	RAHT	PERF_ITEM_FRC_AHT

Name	Display Name	WA Canonical Name	IEX TotalView	Aspect eWFM	Genesys WFM
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 blk database tables. Templates of Excel spreadsheets are supplied in the installation package.

Alternatively, you can omit the file preparation and load the data directly into blk database tables 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 supplied in the `\bulkconfig\integrated\ccadv-wa-bulkload` folder 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.

Database Structures, Scripts, and Procedures

An object creation script, `blkObjectsCre.sql`, is supplied in the installation package, in the `\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 CCAdv/WA configuration after you perform the bulk configuration procedure.

Stored Procedure for Bulk Configuration

You implement the bulk configuration by running a stored procedure, `spblkConfigCCAdvWAIntegrated`, 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 might 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.

If you do not have a copy of your bulk configuration files or blk tables, you can use the extended export utility to generate a "clean" copy of blk tables from the existing application configuration before you run the configuration removal procedure. The extended bulk configuration export utility is supplied beginning with version 8.5.001. See additional details in [Exporting CCAdv/WA Configuration](#).

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.
- 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 blk database tables with your application, agent group, and contact group configuration 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 blk database tables. 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 blk database tables 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 – ten columns beginning with release 8.5.001 – 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
- Application Include in Rollup Property (for release 8.5.001 and later)
- Contact Group Include in Rollup Property (for release 8.5.001 and later)

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 blkAllNames 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.
- An empty cell, or any values in the `Include in Rollup` properties that are different from Y or N are interpreted as Y (two new `Include in Rollup` columns are available beginning with release 8.5.001 – see [Applications](#) above).

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
- Contact Group Include in Rollup Property (for release 8.5.001 and later)

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 blkAllAgntGr database table.

Guidelines

- Each agent group name must match the name contained in the tmpImportSkill.EnterpriseName column of the Platform database.
- If used, each contact group name must match the name contained in the CONTACT_GROUP.NAME column of the Platform database.
- Do not include contact groups that need to be mapped to network contact centers. Such contact groups must be placed into the blkAllNames table instead.
- If an AGCC name is supplied, include only contact groups that you want to be mapped to the specified AGCC and agent group; do not include contact groups if the AGCC name is not specified.
- An empty cell, or any values in the Contact Group Include in Rollup property that are different from Y or N are interpreted as Y. If the contact group is not specified, the Contact Group Include in Rollup property is ignored (applicable beginning with release 8.5.001).

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. Beginning with release 8.5.001, the Include in Rollup property can be controlled from the utility. The property value can be supplied in the additional column added to the blkAllNames table. The value can be Y or N. An empty cell, or any values other than Y or N are interpreted as Y for compatibility with the previous versions. 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. Includes the contact group in the rollup. Beginning with release 8.5.001, the Include in Rollup property can be controlled from the utility. The property value can be supplied in the additional column added to the blkAllNames table. The value can be Y or N. An empty cell, or any values other than Y or N are interpreted as Y for compatibility with the previous versions.
- 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 two tables:

- blkExpAllNames
- blkExpAllAgntGr

All entries for which there is a problem contain an explanation of the issue in the Message column of each table. Make sure you always review the content of this column.

Beginning with release 8.5.001, the export utility exports data into four tables:

- blkExpAllNames
- blkExpAllAgntGr
- blkAllAgntGr
- blkAllNames

The first two blkExp tables contain expanded configuration data that is presented in a redundant form for diagnostic purposes. As with releases prior to 8.5.001, the Message field contains a warning or error information, where applicable. The other two blk tables contain a "clean" non-redundant copy of your Advisors configuration that can be further used "as is" by the bulk configuration tool.

If, at the time of export, the Advisors Platform schema already contains the two blk tables, the utility will create a backup copy of each table with the name containing a timestamp.

For example:

- blk12MAY15063407AllAgntGr
- blk12MAY15063407AllNames

The timestamp format is: DD MON YY HH24 MI SS

Once the content of blkAllAgntGr and blkAllNames is saved into the timestamped backup tables, the tables are cleared and the current Advisors configuration is loaded into them.

Beginning with release 8.5.001, there is no need to adapt the exported diagnostic blkExp data in

order to craft the Advisor configuration blk structures. The content recorded into the blk tables by the export utility can be used as a data source for the bulk configuration tool. The data can be used for migration to another schema or for re-loading the saved configuration into the same schema after you apply the configuration removal procedure. Genesys recommends that you first verify the content of the diagnostic export tables before loading the configuration data from the blk tables created by the export tool.

The export utility can also be used for saving the versions of Advisors configuration while you are in the process of configuring Advisors. The blkExp data will help to capture and correct a problem as soon as you run the export utility. Any copy of the backup data can be loaded into the blk tables and used for reverting the configuration to any earlier, saved version. Genesys recommends that you use the bulk configuration removal procedure before each configuration load.

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 CCAdv 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 in the installation package, in the `\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`
- `blkAppAgntGr`
- `blkAgntGrNames`
- `blkAppLog`

All of the preceding tables created by the script must be present at the point when you apply the bulk configuration procedure, 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 might 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.

If you do not have a copy of your bulk configuration files or blk tables, you can use the extended export utility to generate a "clean" copy of blk tables from the existing application configuration before you run the configuration removal procedure. The extended bulk configuration export utility is supplied beginning with version 8.5.001. See additional details in [Exporting CCAdv Configuration](#).

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.
- 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

7. Connect to the Oracle or SQL Server 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. 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

```

10. Verify the log stored in the blkAppLog table.

For information about logs related to the bulk configuration, see [Bulk Configuration Validation and Logs](#).

11. Correct the data, if necessary, and go back to Step 10.

If no correction is necessary, go to Step 13.

12. Examine all relevant configuration pages in the Advisors Administration module to verify the configuration.

13. Examine the CCAdv dashboard to verify the configuration.

14. 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 blk database tables.

Alternatively, you can omit the file preparation and load the data directly into blk database tables 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 – seven columns beginning with release 8.5.001 – 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
- Application Include in Rollup Property (for releases 8.5.001 and later)

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'.
- An empty cell, or any values in the Include in Rollup property that are different from Y or N are interpreted as Y (the new Application Include in Rollup Property column is available beginning with release 8.5.001 – see [Object Names](#) above).

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. The blkAgntGrNames table is shared between the CCAdv and WA bulk configuration tools for Independent mode.

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 three 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. Make sure you always review the content of this column.

Beginning with release 8.5.001, the export utility exports data into six tables:

- blkExpAppNames
- blkExpAppAgntGr
- blkExpAgntGrNames
- blkAppNames
- blkAppAgntGr
- blkAgntGrNames

The first three blkExp tables contain expanded application configuration data that is presented in a redundant form for diagnostic purposes. As with releases prior to 8.5.001, the Message field contains a warning or error information, where applicable. The other three blk tables contain a "clean" non-redundant copy of your Advisors application configuration that can be further used "as is" by the bulk configuration tool.

If, at the time of the export, the Advisors Platform schema already contains the three blk tables, the utility will create a backup copy of each table with the name containing a timestamp.

For example:

-
- blk12MAY15063407AppAgntGr
 - blk12MAY15063407AppNames
 - blk12MAY15063407AgntGrNames

The timestamp format is: DD MON YY HH24 MI SS

Once the content of blkAppNames, blkAppAgntGr, and blkAgntGrNames is saved into the timestamped backup tables, the tables are cleared and the current Advisors application configuration is loaded into them.

Beginning with release 8.5.001, there is no need to adapt the exported diagnostic blkExp data in order to craft the Advisor application configuration blk structures. The content recorded into the blk tables by the export utility can be used as a data source for the bulk configuration tool. The data can be used for migration to another schema or for re-loading the saved configuration into the same schema after you apply the configuration removal procedure. Genesys recommends that you first verify the content of the diagnostic export tables before loading the configuration data from the blk tables created by the export tool.

The export utility can also be used for saving the versions of Advisors configuration while you are in the process of configuring Advisors. The blkExp data will help to capture and correct a problem as soon as you run the export utility. Any copy of the backup data can be loaded into the blk tables and used for reverting the configuration to any earlier, saved version. Genesys recommends that you use the bulk configuration removal procedure before each configuration load.

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 in the installation package, in the `\bulkconfig\independent\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 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 might 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.

If you do not have a copy of your bulk configuration files or blk tables, you can use the extended export utility to generate a "clean" copy of blk tables from the existing contact group configuration

before you run the configuration removal procedure. The extended bulk configuration export utility is supplied beginning with version 8.5.001. See additional details in [Exporting WA Configuration](#).

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.
- 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 or SQL Server instance as the 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;

MSSL:

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 blk database tables.

Alternatively, you can omit the file preparation and load the data directly into blk database tables 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 – seven beginning with release 8.5.001 – 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
- Contact Group Include in Rollup Property (for release 8.5.001 and later)

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'`.
- An empty cell, or any values in the `Include in Rollup` properties that are different from Y or N are interpreted as Y (the new `Contact Group Include in Rollup Property` column is available beginning with release 8.5.001 – see [Contact Groups mapped to Objects other than AGCC](#) above).

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 – five columns beginning with release 8.5.001:

- Contact Group Name
- Name of AGCC to which contact group is related
- Parent Contact Group Name
- Contact Group Display Name
- Contact Group Include in Rollup Property (for release 8.5.001 and later)

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 the 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.
- An empty cell, or any values in the `Include in Rollup` properties that are different from Y or N are interpreted as Y (the new `Contact Group Include in Rollup Property` column is available beginning with release 8.5.001 – see [Contact Groups mapped to AGCC](#) above).

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
- Genesys calling lists
- 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 six 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. Make sure you always review the content of this column.

Beginning with release 8.5.001, the export utility exports data into 12 tables:

- Diagnostic tables
 - blkExpAgntGrNames
 - blkExpCgNames
 - blkExpAgccCgNames
 - blkExpAgCgNames
 - blkExpCgApp

- blkExpCgAgntGr
- Clean configuration tables
 - blkAgntGrNames
 - blkCgNames
 - blkAgccCgNames
 - blkAgCgNames
 - blkCgApp
 - blkCgAgntGr

The first six blkExp tables contain expanded configuration data that is presented in a redundant form for diagnostic purposes. As with releases prior to 8.5.001, the Message field contains a warning or error information, where applicable. The other six blk tables contain a "clean" non-redundant copy of your Advisors contact group configuration that can be further used "as is" by the bulk configuration tool.

If, at the time of the export, the Advisors Platform schema already contains the six blk tables, the utility will create a backup copy of each table with the name containing a timestamp.

For example:

- blk12MAY15063407AgntGrNames
- blk12MAY15063407CgNames
- blk12MAY15063407AgccCgNames
- blk12MAY15063407AgCgNames
- blk12MAY15063407CgApp
- blk12MAY15063407CgAgntGr

The timestamp format is: DD MON YY HH24 MI SS

Once the content of the six blk tables is saved into the timestamped backup tables, the tables are cleared and the current Advisors contact group configuration is loaded into them.

Beginning with release 8.5.001, there is no need to adapt the exported diagnostic blkExp data in order to craft Advisor contact group configuration blk structures. The content recorded into the blk tables by the export utility can be used as a data source for the bulk configuration tool. The data can be used for migration to another schema or for re-loading the saved configuration into the same schema after you apply the configuration removal procedure. Genesys recommends that you first verify the content of the diagnostic export tables before loading the configuration data from the blk tables created by the export tool.

The export utility can also be used for saving the versions of Advisors configuration while you are in the process of configuring Advisors. The blkExp data will help to capture and correct a problem as soon as you run the export utility. Any copy of the backup data can be loaded into the blk tables and used for reverting the configuration to any earlier, saved version. Genesys recommends that you use the bulk configuration removal procedure before each configuration load.

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.

Edit the FA Message Listening Port

Frontline Advisor (FA) performs metric rollups in memory. For more information about Frontline Advisor's dynamic hierarchy, see the [FA Dynamic Hierarchy](#) topic.

Advisors Genesys Adapters (AGA) 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 Advisors Genesys Adapter

The port on which FA listens for connections from AGA 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 FrontlineAdvisor.properties property file.

Configure the Reason Code Statistic Key

In Advisors release 8.1.5, you ran an update SQL script to configure the reason code statistic key. Starting 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.

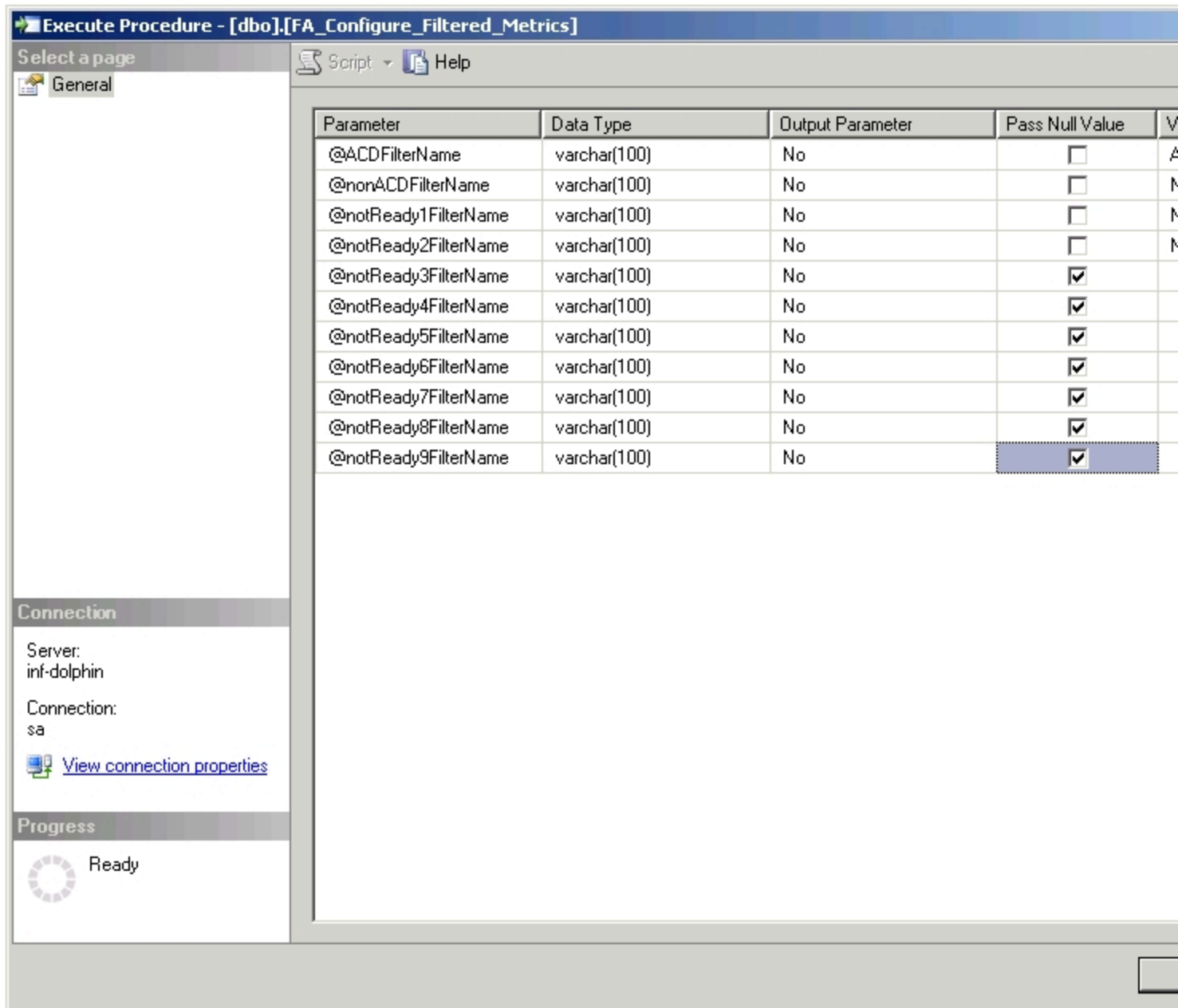
Next Steps

1. After the metrics are enabled, they must be imported into the Configuration Server using the Advisors

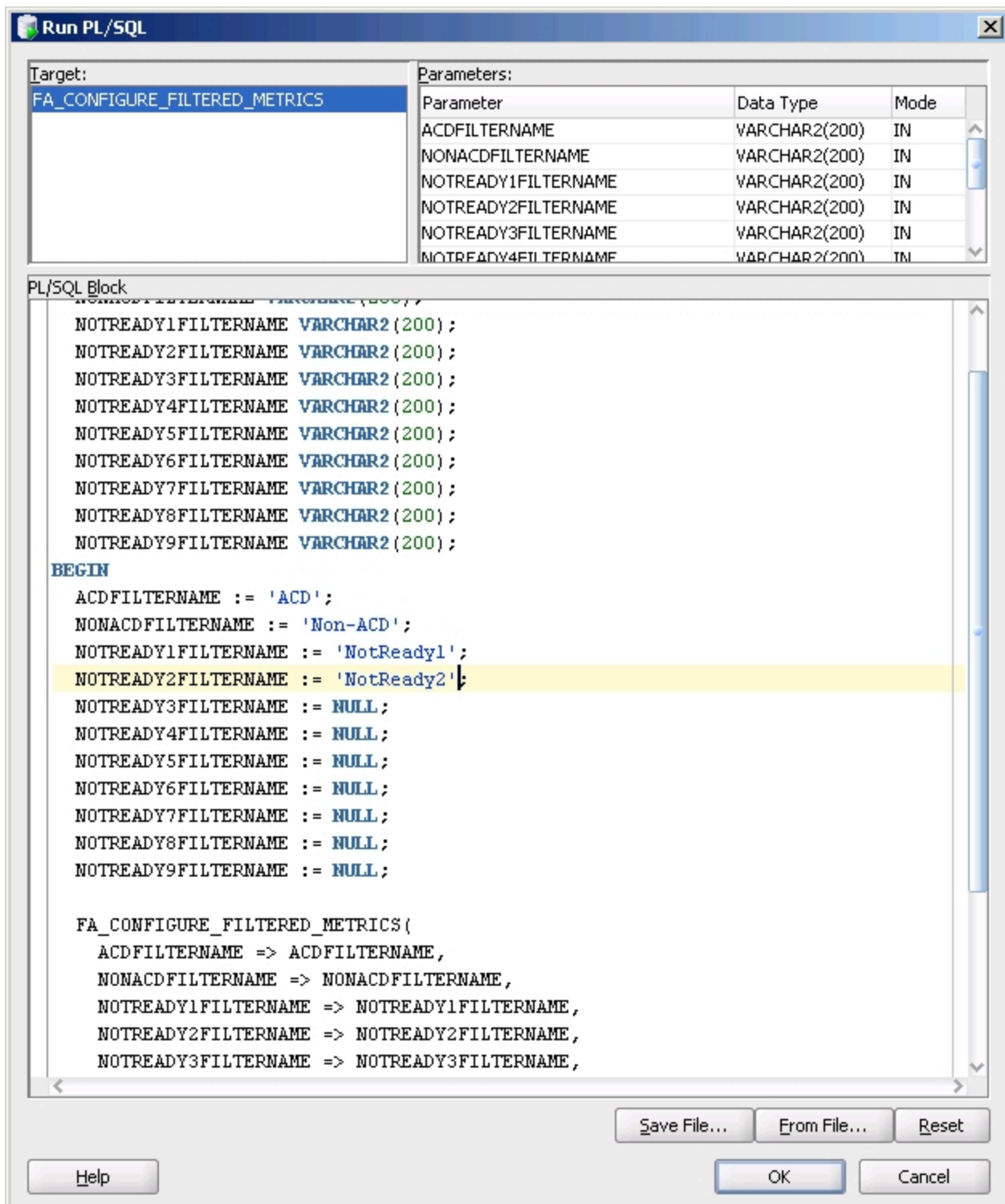
Object Migration Wizard (select Frontline Advisor Metrics when prompted for the migration path). For more information, see [Object Migration Utility](#). Running the Advisors Object Migration Wizard creates corresponding business attribute values for the enabled metrics. As with other FA metrics, you 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.

Advisors Clusters

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. It can be a physical computer, or a virtual machine on a VM host. It has an IP address.

A node in a cluster is also referred to as a *member* of the cluster.

Even if you install Advisors on only one system, that system is a node in a cluster containing that one system.

A **module** is an application in the Advisors suite that you can install separate from other applications. For example, WA Server is a module, and Contact Center Advisor XML Generator is a module.

Members of the cluster communicate to share data that is cached in memory. They also communicate via messages, to perform workflows that require more than one module.

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. See [diagrams of possible configurations](#).

For instructions about how to modify a cluster after you have installed Advisors, see [Change Advisors Cluster Membership](#).

Integration with Solution Control Server and Warm Standby

Starting in release 8.5.1, Performance Management Advisors support warm standby – a form of high availability (HA) in which a backup server application remains initialized and ready to take over the operations of the primary server. Warm standby mode does not ensure the continuation of interactions in progress when a failure occurs.

In a Genesys environment, an application that supports HA is typically integrated with the Genesys Management Layer, specifically the Local Control Agent (LCA), the Solution Control Server (SCS), and the Genesys Administrator or Configuration Manager. LCA, SCS, and the management interface manage the primary/backup pair of applications.

In release 8.5.1, the Advisors modules that support warm standby must be integrated with and installed with the LCA and SCS, even if you do not have a licence for an HA deployment.

Additional Information

For information about Genesys Management Layer, see [Management Framework Deployment Guide](#) and [Management Layer User's Guide](#).

Integration with Solution Control Server

Starting in release 8.5.1 some Advisors modules must integrate with the Solution Control Server, while others do not need to. For those that do, you must create Application and Host objects for those modules whether you are installing a basic deployment or a warm standby deployment. See the following sections for the list of modules that require integration with the management layer and the list of modules that do not.

[+] Advisors Modules Controlled by SCS

In release 8.5.1, the following Advisors modules are integrated with the LCA, SCS, and the Genesys Management Layer user interface (Genesys Administrator or Configuration Manager) to support warm standby.

- Advisors Genesys Adapter
- Advisors CISCO Adapter
- Contact Center Advisor XML Generator

- Workforce Advisor WA Server
- Frontline Advisor FA Server (that is, FA with the rollup engine)

Because the preceding modules are integrated with the Management Layer, proceed as follows. For exact instructions on carrying out the following tasks, see [Deploying Components Controlled by Solution Control Server](#).

- install and run the LCA on a system that runs any of the preceding modules
- configure a Host for the system in Configuration Manager or Genesys Administrator
- configure an Application in Configuration Manager or Genesys Administrator for each Advisors server that runs one or more of the preceding modules
- if you have a licence for an HA deployment, configure a second Application in Configuration Manager or Genesys Administrator for the secondary server, and associate the two Applications as a primary and backup pair for failover
- specify the properties, during installation, that permit the Advisors server to integrate with the LCA, SCS, the Application, and the Host
- do not create a Windows or Linux service to control this module, because SCS will control it.

[+] Advisors Modules Not Controlled by SCS

The following Advisors modules are not controlled by SCS. They have been automatically highly-available since release 8.1.5, because you can install each of these modules on more than one system – you do not configure them as primary-backup pairs:

- Contact Center Advisor Web Services
- Workforce Advisor Web Services
- Frontline Advisor FA Web Services (that is, FA without the rollup engine and installed as a cluster member)
- Contact Center Advisor-Mobile Edition Server

Because the preceding modules are independent of LCA, SCS, or other parts of the Management Layer:

- it is unnecessary to install the LCA on a system that runs any of the preceding modules
- it is unnecessary to configure a Host or Application for the system or module in Configuration Manager or Genesys Administrator.
- you must create a Windows or Linux service to control this module, because SCS will not control it.

[+] Advisors Modules that do not Support HA

The following Advisors modules are not automatically highly-available in release 8.5.1:

- Advisors Administration module
 - Resource Management Console
-

Tip

You can use different operating systems on primary and backup servers. For example, the host for your primary instance of the WA server can be a Windows-based system, while the host running the backup instance of the WA server uses a Linux platform.

Limitations and Special Configuration

Does Not Support Stop Gracefully

Advisors do not support the Stop Gracefully functionality available in the Solution Control Server UI. If you choose Stop Gracefully, it is the same as choosing Stop.

Multiple Advisors Servers on One System

You can install more than one Advisors server, all part of the same cluster, on one system.

For example, you can install both CCAdv XML Generator and WA Server on one system. XML Generator does not require Advisors Platform to run, but the WA Server does.

For this deployment, you must create two Application objects in Configuration Server. One Application object is for CCAdv XML Generator, and the other is for the Geronimo instance that runs WA Server.

For a diagram illustrating such a deployment, see [Applications, Advisors Servers, and Cluster Nodes](#).

Separating Advisors Servers that SCS Controls from Those That It Does Not

Genesys recommends that you install the Advisors modules that SCS controls, and the modules that it does not, on different systems. For example, Genesys recommends that you not install Workforce Advisor WA Server and Workforce Advisor Web Services on the same system. This is because it is easier to think about the deployment of Advisors if you keep them separate.

For example, imagine the following: you install WA Server and WA Web services on the same system, in one Advisors server. Because that server runs WA Server, it must be controlled by SCS via an application in the CME. WA Server communicates with SCS and indicates its status in the SCI, but WA web services does not communicate with SCS.

Here are some consequences of that:

- If WA web services fails and stops sending data to WA dashboards, the SCS UI will not indicate this. The application's status in the SCS UI will be Running.
- In the SCS UI, the execution mode of the application will not always reflect the state of WA Web Services. For example, if the application's execution mode is Backup, WA Web Services will still actually be running and will respond to requests from dashboards. This is because the module does not know about execution modes, and is not controlled by SCS.

If you think you can keep such things in mind and deal with the consequences, feel free to combine the installation of Advisors modules in servers however you please.

Advisors Genesys Adapter

When configuring AGA instances on primary and backup systems, use the following rules:

- Configure the same number of adapter instances on both the systems. For example, if the primary system has two CCAdv/WA adapters, then the backup system should also have two adapters for CCAdv/WA.
- Configure the same Stat Servers exactly on the adapters of the two systems.

Frontline Advisor

Frontline Advisor requires integration with SCS and supports HA only when installed with the FA rollup engine. The following two configurations do this.

- FA installed as a cluster member with the rollup engine.
- FA installed standalone, which automatically includes the rollup engine.

Administration Module

The Advisors Administration module does not have separate warm standby configuration. The following sections describe the two HA solutions for the Administration module.

Fellow-Traveller Warm Standby

You could install the Administration module on the same system with either WA Server or FA with the rollup engine. Because the resulting Advisors server communicates with LCA and SCS, it does support warm standby. If that server fails, SCS will fail over to its backup, on which you have installed the same Advisors modules, including the Administration module.

The Administration module can sync Person objects from Configuration Server and users in the Platform database. Only one Advisors server should be configured to perform this task. In this scenario, configure only one of the servers to do this. The reason is that the Administration module does not know about execution modes. If both primary and backup servers are configured to synch users, and both servers are started at the same time, both will synch users at the same time, and both will fail.

Cold Standby

Deploy a second installation of the module, with the platform to support it. If the primary installation fails, manually switch to the second installation, **as described in Cold Standby Configuration and Switchover**.

Warm Standby and the FA Admin

When a deployment of Advisors includes Frontline Advisor, then in the Administration module, there is an FA Admin command in the navigation menu.



That command takes you to the FA Administration pages.

The functionality for the FA Admin pages is not in the Administration module. Instead, it is included in the same server as the FA Server. This is a requirement for the FA Administration to operate. This means that if primary and backup FA Server installations exist, then primary and backup FA Admin modules also exist.

Failover Scenarios

In an HA deployment of Advisors, failover from the primary system to the backup system might occur for the following reasons.

Problem	Solution
Machine or Virtual machine (VM) is not available.	Processing fails over to the waiting backup VM or machine running the same modules.
An Advisors server is not available, although the VM is still running.	Processing fails over to a similarly-configured backup server on another VM or machine.
An important process in the Advisors server does not complete before a timeout period. The process, and the timeout period, are different for the various Advisors modules.	Processing fails over to a similarly-configured backup server on another VM or machine.

An Advisors server does not fail over from primary to backup if the reason for the failure is something that would also cause the backup to fail. In this case, there is no point failing over.

Contact Center Advisor XML Generator does not fail over from primary to backup if its connections to a database fail. Functionality in XML Generator from before 8.5.1 re-tries the connections to the database for a configured interval, until the connection is restored.

Managing Failover with the Solution Control Server

As with other Genesys products, the SCS manages failovers for primary-backup pairs. You can use Genesys Administrator or the Solution Control Interface (SCI) to manually switch processing from the primary Application to the backup, or to stop or start a primary or backup Application. See also [Deploying Components Controlled by Solution Control Server](#), particularly [Step 6](#) of the procedure.

The SCS controls the request to fail over, however the primary and backup server in a pair also communicate with each other, as a backup mechanism for failover. This is important because the SCS or LCA can sometimes fail, or a network communication path between the server and the SCS can

fail.

Advisors Warm Standby and Databases

All Advisors components are designed to restore the loss of database connectivity automatically. Ensure a backup Advisors application instance uses the same database as the primary application instance.

The solution for High availability of the Advisors databases relies on the respective database vendor's solutions. Advisors support the following HA solutions for databases:

- Oracle Database with Oracle Real Application Clusters (Oracle RAC) and combinations with RAC for scalability and disaster recovery offered by Oracle.
- Microsoft SQL Server Failover Cluster. Advisors databases can be installed on a Failover Cluster Instance (FCI) where FCI is a single instance installed across Windows Server Failover Clustering (WSFC) nodes. MSSQL 2012 FCI with multiple subnets is also supported.

Important

Database mirroring, log shipping, and MSSQL 2012 AlwaysOn Availability Groups feature are not supported because of the Simple recovery model requirement for all Advisors MSSQL databases.

Scaling the Web Services to Increase Capacity

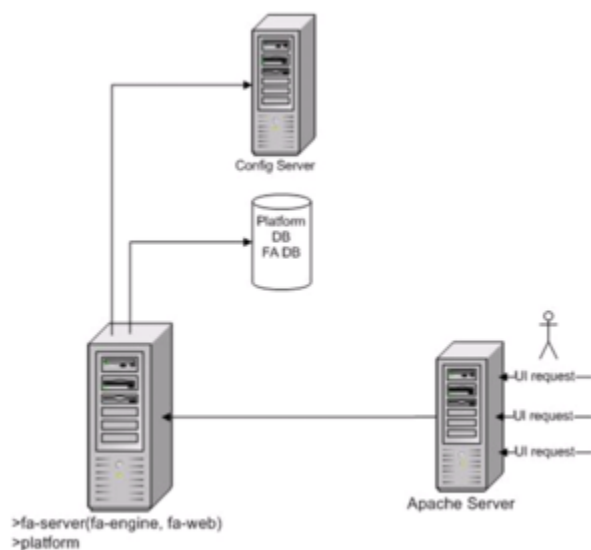
You can horizontally scale the web services module for Contact Center Advisor (CCAdv), Workforce Advisor (WA), and Frontline Advisor (FA).

Frontline Advisor

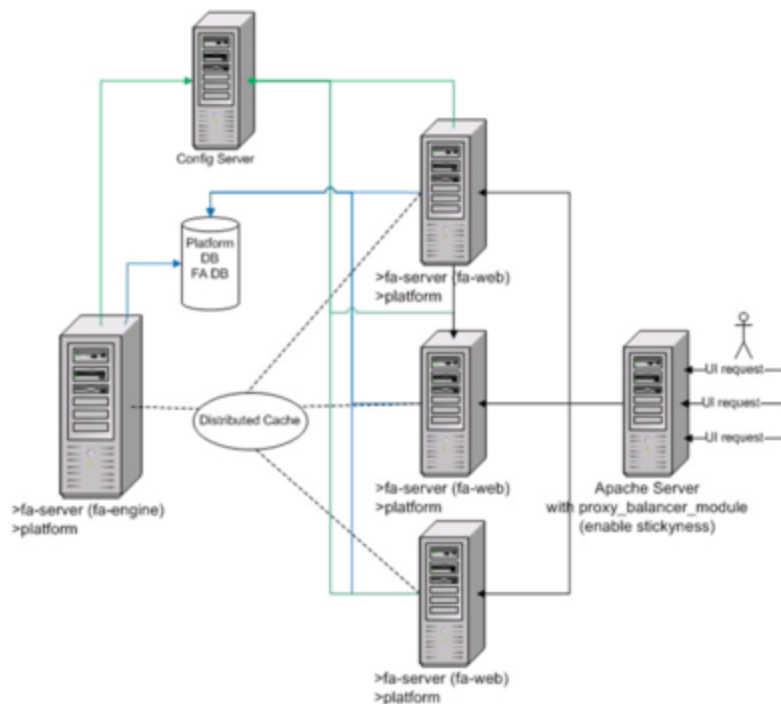
FA supports a distributed mode. You can deploy FA on multiple servers or hosts in distributed mode.

For the procedure to deploy FA in standalone or distributed mode, see [Deploying FAAA](#).

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 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.

Simplified High Availability Architecture

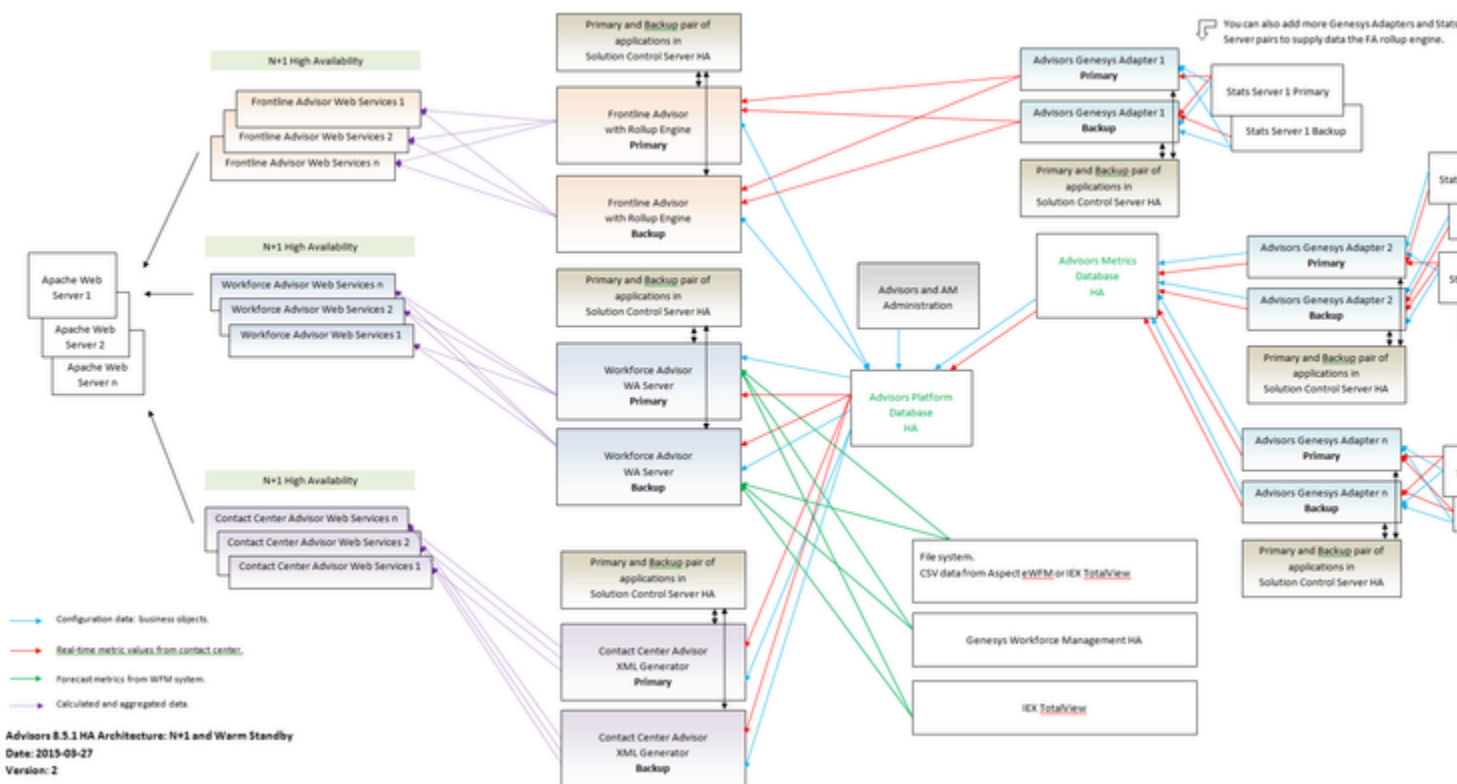
The Figure on this page shows that Advisors supports two kinds of High Availability (HA), by default.

For an N+1 HA form of HA, you can deploy the web services modules any number of times, each on a different cluster node.

For the warm standby form of HA, other modules can be deployed as primary and backup servers, each on a different cluster node and controlled by Solution Control Server.

For more details on the different kinds of support and the requirements of each, see [Integration With Solution Control Server](#).

You can also manually configure any Advisors module to offer [Cold Standby HA](#).



Simplified Advisors Architecture in Warm Standby Configuration

Applications, Advisors Servers, and Cluster Nodes

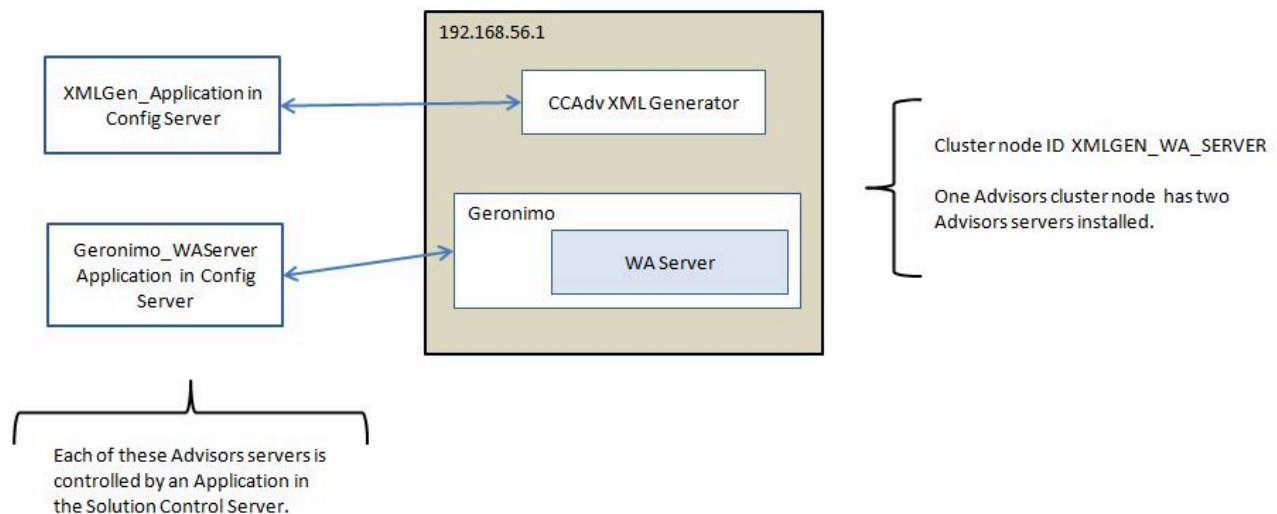
General

For background information see:

- [Advisors Cluster Information](#).
- [Integration with Solution Control Server and Warm Standby](#).

Two Advisors Servers on One Cluster Node

The following figure illustrates that two Advisors servers can be installed on the same cluster node.



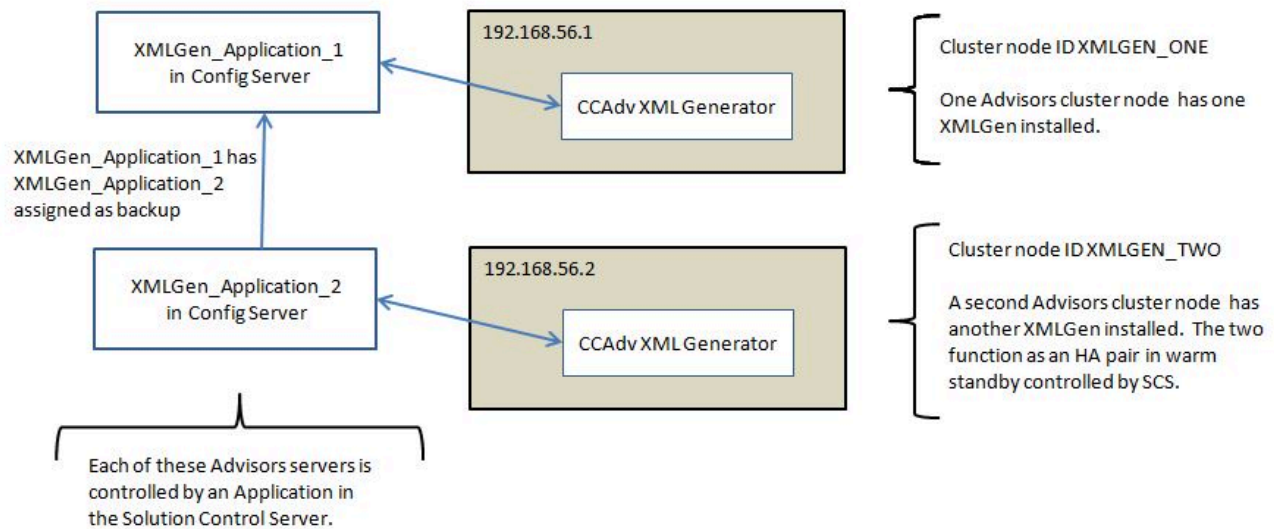
There is one cluster node with one ID.

CCAdv XMLGen is installed on the node. It is controlled by Solution Control Server (SCS) through an application created in the Management Layer.

WA Server is also installed on the node. It runs in Geronimo, which is controlled by SCS through a different application.

Primary/Backup Pair of Advisors Servers on Two Cluster Nodes

The following figure shows how a primary and backup pair of Advisors servers is deployed.



The example uses CCAdv XMLGen as the Advisors server.

One XMLGen is deployed on one cluster node and controlled by an application using SCS.

The second XMLGen is similarly deployed on a different cluster node.

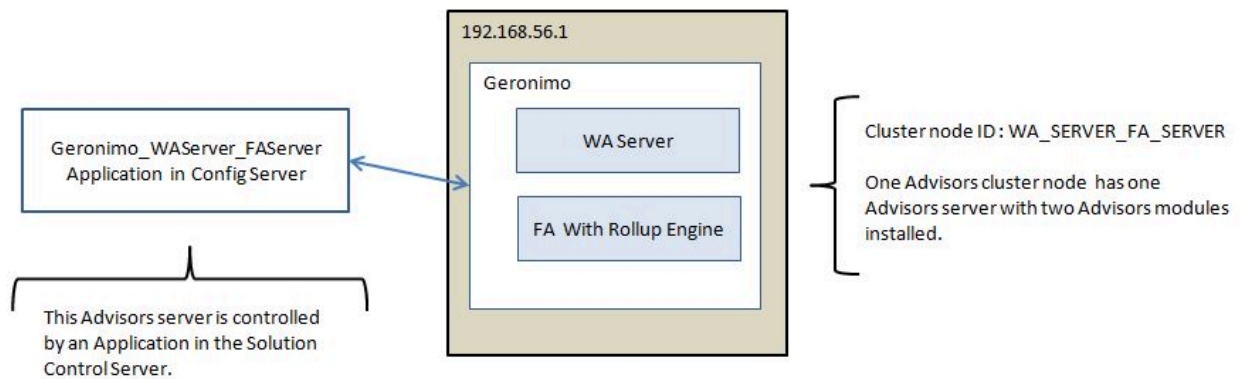
In this scenario, there are two cluster nodes with two different node IDs.

The two applications are linked as primary and backup applications in the Management Framework.

One Advisors Server with Two Modules on One Cluster Node

Controlled by Solution Control Server

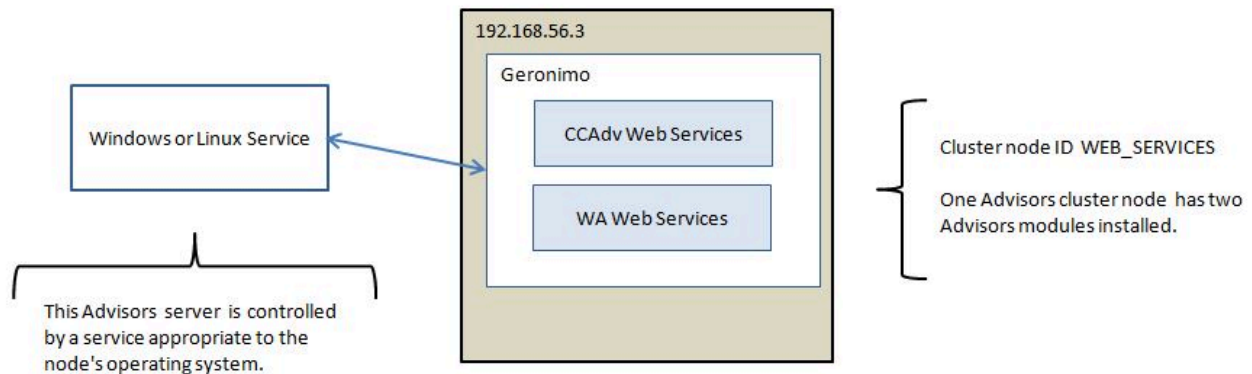
The following figure shows two Advisors modules running in one Advisors server on one cluster node.



These modules are controlled by SCS. Both modules run in the same Geronimo server and the server is controlled by an application in SCS.

Controlled by Service on Operating System

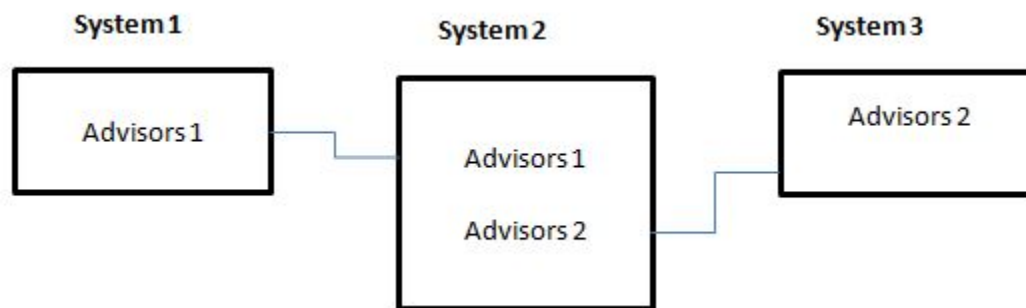
The following figure shows two Advisors modules running in one Advisors server on one cluster node.



Because these modules are not controlled by SCS, the Advisors server is managed by a Windows or Linux service.

Multiple Advisors Deployments on One System

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 three 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 numbers defined, or if they are not valid numbers, 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 in the Platform installer for the Java `activeMQ.port` is 61616.

The default values in the Platform installer for the distributed caching ports are:

- `distributed.caching.port=11211`
- `distributed.caching.maxport=11212`

The default values in the Platform installer for the Geronimo configurable ports are the following:

- HTTPPort=8080
- NamingPort=1099
- JMXPort=9999
- HTTPSPort=8443
- AJPPort=8009

The following Table shows the configuration file associated with each 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-tomcat6-minimal-2.2.1\var\config\config-substitutions.properties	HTTPPort, NamingPort, JMXPort, HTTPSPort, AJPPort
Cluster Node Configuration	conf/ActiveMQ.properties	ActiveMQ.port
Cache Configuration	conf/Caching.properties	distributed.caching.port distributed.caching.maxport
Workforce Advisor Server - IEX TotalView	conf/WorkforceUtilization.properties	ftpService.port

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
- distributed.caching.maxport 11212
- 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 11213
- distributed.caching.maxport 11214
- 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.

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.

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 Security Deployment Guide](#).
3. Configure security certificates.
4. Configure the security providers and issue security certificates. For more information, see [Genesys Platform SDK Developer's Guide](#).
5. Assign a certificate to the Configuration Server host. For more information, see [Genesys 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 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 Security Deployment Guide](#).

Advisors and the Backup Configuration Server

Starting in release 8.5.0, you can configure a connection from an Advisors 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 `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

Advisors and the Backup Solution Control Server

Starting in release 8.5.1, some Advisors modules require a connection to a Solution Control Server (SCS). For a list of those modules, see [Integration with Solution Control Server and Warm Standby](#).

Connection to a backup SCS is optional.

Backup Configuration Server Properties

You must supply the name of the application that represents the primary SCS in the Advisors' installers. The Advisors modules obtain the properties of the backup SCS from Configuration Server through that application for the primary SCS. Without the application, Advisors acquires no information about the backup SCS.

How it Works

The backup Solution Control Server must be set up as a *warm standby* to the primary Solution Control Server. When Advisors loses connection to the primary SCS, connection to the backup SCS happens automatically.

When the primary SCS comes back online, it becomes the backup server and the former backup SCS continues as the primary SCS. Advisors supports subsequent switchovers between the primary and backup Solution Control Servers.

The Platform log file records:

- a lost connection to either the primary or the backup Solution Control Server.
- re-connection to a Solution Control Server.

NEW When There is No Backup SCS Configured

When there is no backup SCS configured, Advisors servers use the warm standby mechanism to connect again to the primary SCS.

NEW SCS Warm Standby and the Reconnect Timeout

In both cases – backup SCS configured or not – the warm standby-reconnect mechanism has a timeout setting after which it stops retrying. Genesys recommends configuring this setting to a value higher than the expected disconnect times between Advisor servers and the SCS.

The following settings are configured in the properties of the primary SCS:

- Reconnect timeout interval in seconds
- Number of reconnect attempts

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

- 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. 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

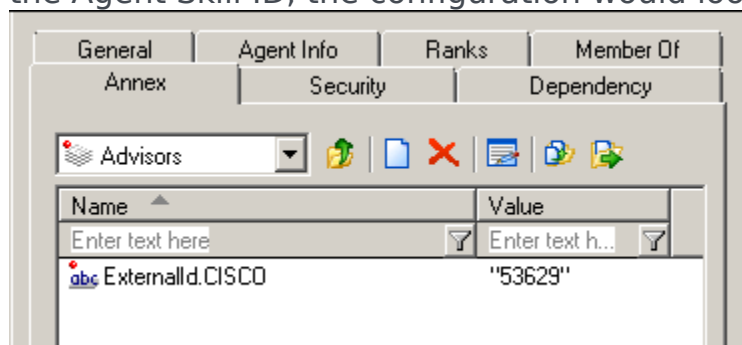
For all other source environments, the object must be created and an entry must be added to the object's Annex tab under an Advisors section. The key for each such entry has the format:

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, therefore, 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.

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 Stat Server Type, 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.

If you have multiple adapter instances installed, make sure that you start, or restart, all of them at the same time.

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:

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. Monitor the status of the AGA applications in Genesys Administrator or the Solution Control Interface (SCI).

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 multiple adapter instances installed, make sure that you start, or restart, all of them at the same time. 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 following statement against the Advisors Platform database – this provides the ID value for each adapter instance:

```
select adapter_instance_id, name from adapter_instances
```

- Run the following statement against the Advisors Platform database – this shows you which Stat Server pairs are associated with the adapter and which objects are associated with the Stat Server pair for each adapter:

```
SELECT * FROM STAT_GROUP_OBJ_MAPPING where STAT_GROUP_ID in (select STAT_GROUP_ID from
STAT_GROUP_CONFIG where
ss_pair_id in (select ss_pair_id from ADAPTER_STAT_SERVER where ADAPTER_INSTANCE_ID =
```



```
<ID of adapter>))
```

Remove the objects associated with the Stat Server pair for the adapter that you must delete from the table.

2. To remove the identified objects, run the following statement:

```
DELETE FROM STAT_GROUP_OBJ_MAPPING where STAT_GROUP_ID in (select STAT_GROUP_ID from
STAT_GROUP_CONFIG where
ss_pair_id in (select ss_pair_id from ADAPTER_STAT_SERVER where ADAPTER_INSTANCE_ID = <ID
of adapter>))
```

3. To remove the Stat Server pair rows associated with the adapter, run the following statement:

```
Delete from adapter_stat_server where adapter_instance_id = <ID of adapter to delete>
```

4. To delete the adapter_instance row, run the following statement:

```
Delete from adapter_instances where adapter_instance_id = <ID of adapter to delete>
```

No Object Configuration User Specified when Installing Platform

For the CCAAdv module, an Object Configuration User must be specified when you install Advisors Platform. The same is true when you install CCAAdv XML Generator; you must specify the Object Configuration User. If configuration of this user name is omitted, no statistics are issued with the Adapters. This is indicated by an information message in the XMLGen.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 the Advisors server and XML Generator after you update the properties file.

No Object Configuration User Exists in Configuration Server

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 issue:

1. Create the user in Configuration Server.
2. Update `genesys.configServer.objectconfig-username` in the Platform `GenesysConfig.properties` file.
3. Restart the Advisors server and XML Generator 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.

Data Manager reports an error - no Stat Server connections are open

If Data Manager reports that no Stat Server connections are open, check the following:

- Ensure your Advisors Genesys Adapters are configured with Stat Servers. See [Manage Advisors Stat Server Instances](#), particularly the section called [Register a New Stat Server and Link the Stat Server to an Adapter](#).
- Ensure that the configured Stat Servers are up and running.

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.

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.

FA Dynamic Hierarchy

In release 8.5, the Frontline Advisor (FA) hierarchy is monitored in real time, with structural changes being reflected almost immediately in the dashboards rather than requiring a 24-hour reload cycle or a manual hierarchy reload.

Metrics Generation

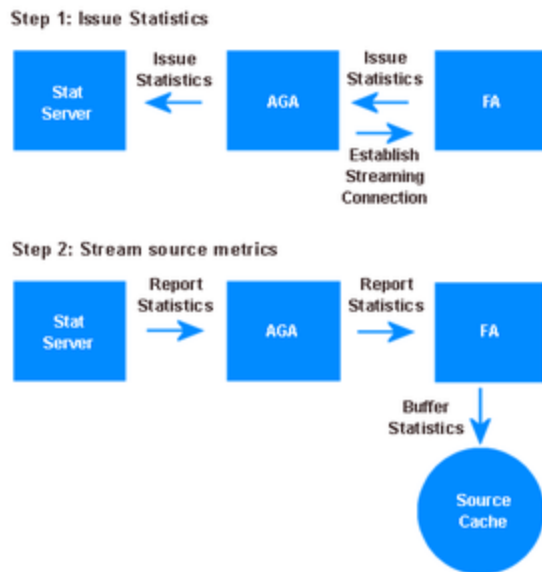
An administrator specifies how often state and performance metrics *roll up* to the hierarchy pane in the FA manager dashboard; this is the *rollup cycle*. The Frontline Advisor service generates metrics values at the beginning of each rollup cycle. There are two types of metrics:

- Source metrics
- Report metrics

Related Information

See [FA Administration Overview](#) for information about the FA page in the administration module and how to use it to configure your FA dashboard, which includes specifying the rollup intervals on the **Settings** tab.

Source Metrics



Source Metric Streaming

Advisors Genesys Adapters (AGA) for FA request source metrics from Stat Servers, and then open a reverse connection back to FA. The adapters stream source metrics to FA as they receive the metrics from Stat Servers. Source metrics do not require additional configuration or computation; their values are simply reported by adapters. The Figure, "Source Metric Streaming", shows this process.

FA Message Listening Port

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. For information about viewing or editing the port number post-installation, see [FA Message Listening Port](#).

Report Metrics

Frontline Advisor performs metric rollups in memory. All report metrics that the aggregation engine must compute include additional configuration to tell the engine how to compute each metric (what *formula*, if any, to use) and the order (priority, or *rank*) in which to compute each metric relative to other contributing metrics.

Hierarchies and the Caches

The *monitoring* hierarchy is loaded from the Genesys Configuration Server at startup based on the configured top-level node. After this initial load, changes to the hierarchy in Configuration Server take effect immediately and are reflected in the FA dashboards at the end of each rollup cycle. You need no longer wait for the overnight refresh, nor force a hierarchy reload. For exceptions, see [Aggregation Engine](#) and [Restrictions and Limitations](#).

While the monitoring hierarchy is a mutable structure, updated as relevant Configuration Server events occur, an immutable *rollup* hierarchy is generated from it during each rollup cycle. During the generation phase, events from the Configuration Server are temporarily buffered and do not resume until generation is complete. After the rollup cycle completes, the rollup hierarchy is then used to service dashboard requests for hierarchy structure.

Important

Agent Groups for which agent membership is not tracked in the Configuration Server are not dynamically monitored. For example, Virtual Agent Groups whose members are not evaluated by the Configuration Server. Such agent groups, and changes to them, are not part of the hierarchy.

Related Information

See [FA Monitoring Hierarchy](#) for more information about the monitoring hierarchy and the relationship between the hierarchy in the Configuration Server and the hierarchy in FA.

Data Caches

Frontline Advisor maintains three distinct caches:

- Source cache – This represents the current state of source data that the adapters provide for all agents in the hierarchy. It is updated real-time as FA receives new source data.
- Aggregation cache – At the beginning of each rollup cycle, FA makes a copy of the current source cache. The copy is input to the aggregation engine, which generates all computed metrics that are then appended to the aggregation cache.
- Live cache – When a rollup cycle completes, the aggregation cache (along with the corresponding rollup hierarchy) becomes available to dashboards. In this way, the aggregation cache becomes the new live cache; it provides data to clients until the next rollup cycle completes and it is, in turn, replaced.

Additionally, the configuration of default thresholds and overrides is stored in the database. FA caches this *constraint configuration*, including all constraint overrides. The constraint cache loads from the database at startup. You can change constraints using the FA page in the administration module after startup. At the beginning of each rollup cycle, an immutable copy is made and provided to the aggregation engine.

Tip

The Agent Skills metric is a state metric that has no corresponding source metric. When the dashboard requests a value for the Agent Skills metric, the FA server queries the hierarchy in Configuration Server for the skills list, rather than examining a cache generated from rollups.

Aggregation Engine

The FA aggregation engine runs within the FA service process. The aggregation engine executes formulas using the static rollup hierarchy. This means, of course, that hierarchy events received immediately after the current cycle begins will not be visible on the dashboard until the next cycle completes.

Dashboard Clients and Web Services

When the FA dashboard requests updated metrics values, it requests metrics for all nodes currently visible (the set of expanded nodes in the hierarchy pane, as well as the agents for the currently selected team). The FA server responds with metric values for the nodes, and uses the same nested structure. However, you or another administrator might add nodes to or remove nodes from the hierarchy between requests. The dashboard accounts for structural changes between requests as follows:

- A node that was previously visible on the dashboard is no longer in the monitoring hierarchy – The server does not include this node in the returned data set. This indicates to the dashboard that the node is removed, and the dashboard removes that node (and any previously visible sub-nodes) from the dashboard.
- A node that was not previously visible on the dashboard has been added to the monitoring hierarchy within the expanded set of nodes – The dashboard inserts new records in the hierarchy and/or team panes representing these new nodes.

Restrictions and Limitations

Dynamic hierarchy updates do not include the following events:

- name changes: the FA dashboard does not register a change, in Configuration Server, to the name of a node until the overnight refresh or a forced hierarchy reload. The FA dashboard does register the addition or deletion of a node in Configuration Server, however, and reflects the change after the current rollup cycle completes.
- changes in metric group configuration: for metric group changes to be reflected in the FA dashboard, you must wait for the overnight refresh or force a hierarchy reload. For information about metric groups, see [Working with Metric Groups](#) in the *Genesys Performance Management Advisors Contact Center Advisor and Workforce Advisor Administrator User's Guide*.
- permissions changes: changes to permissions settings, stored in the Configuration Server, are updated

on the dashboards once each hour.

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.

LoggedIn Script-based VAGs in the Resource Management Console

Starting with release 8.5.101, be aware that it might take longer to display LoggedIn script-based VAG agents in the Resource Management Console (RMC) than it takes to display agents of another agent group type. An agent who is a member of a VAG defined by a LoggedIn script displays in a supervisor's RMC only if that agent logs in *after* the supervisor has logged in to the RMC. Agents who are members of any such VAG, and who log in before the supervisor logs in to the RMC, do not display in the supervisor's RMC. As a result, if a supervisor logs out and immediately logs in again, he or she might not see the VAG agents until those agents log in again to the appropriate queues. Be aware that it might take longer to display LoggedIn script-based VAG agents in the RMC than it takes to display agents of another agent group type.

Discontinuation of the Advisors Browser

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.

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 Advisors interface, 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 CCAAdv/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 CCAAdv/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 CCAAdv/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>		<p>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.</p>
Oracle Not applicable.		