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 Current

10/3/2022

Table of Contents

Genesys Pulse Advisors Deployment Guide

Welcome to the *Genesys Pulse 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.

Planning

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

Before you begin deployment, you will make a plan to meet your specific needs. See the *Genesys Pulse Advisors 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.

General Information about Advisors

The Advisors dashboards are accessed using a commercial browser, such as Mozilla Firefox. See the Pulse 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.

The Advisors product suite requires 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.

The Advisors product suite requires the Genesys Solution Control Server to be present because 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.

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.

> **Important**
>
> The Advisors Cisco Adapter is available only for Advisors releases prior to release 8.5.2. Support for Cisco data sources is discontinued starting with Advisors release 8.5.2. Advisors Cisco Adapter release 8.5.100.09 was the final release for this Advisors component.

About Advisors Applications

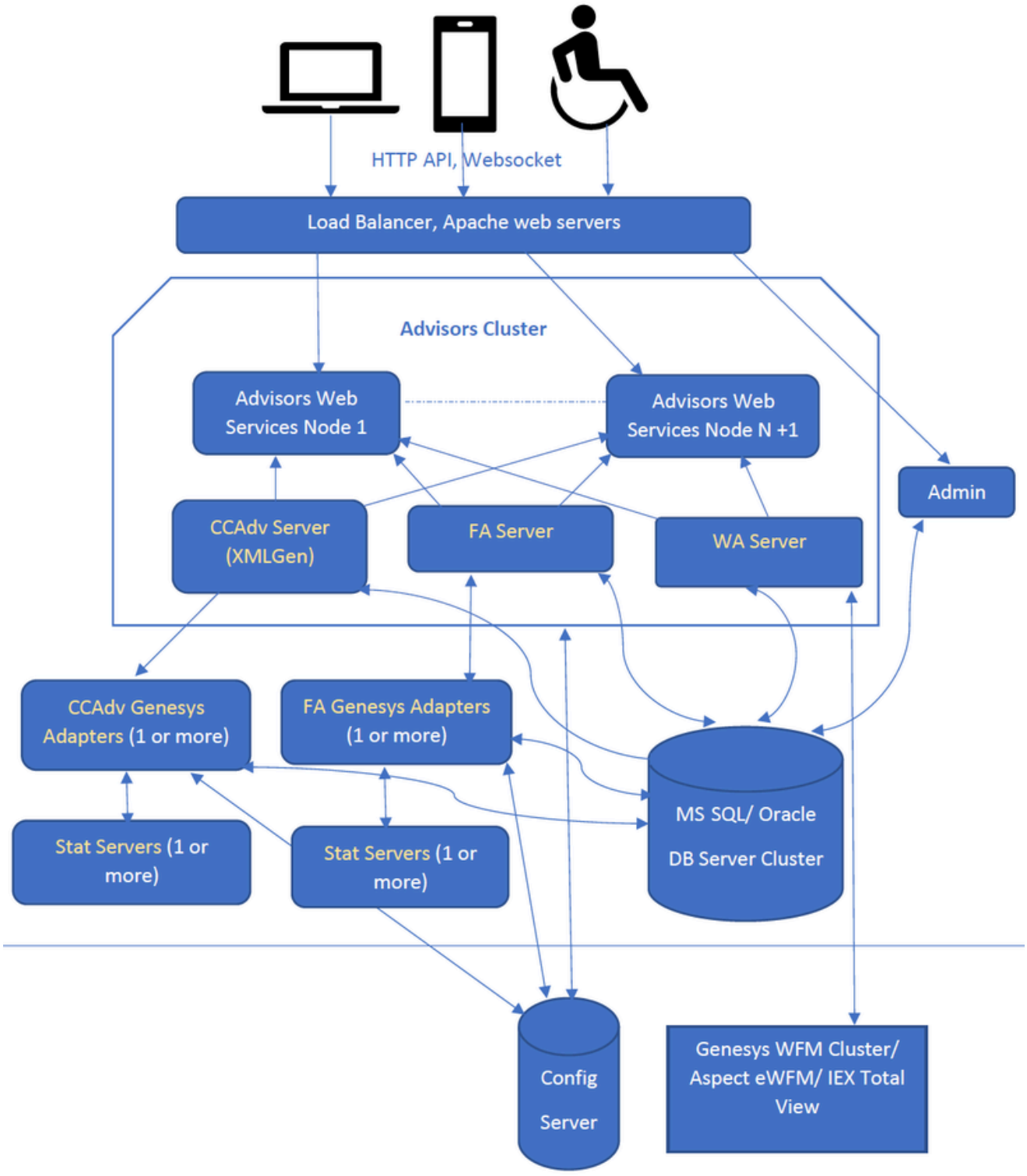
The following Table shows the dependencies amongst Advisors components. For each Advisors product in the Application column, the Table identifies any additional Advisor component that must be installed with it.

Application	Requires these Components on the Same System	Requires these Components within the Same Advisors Deployment
Frontline Advisor	Advisors Platform	Advisors Genesys Adapter
Contact Center Advisor	Advisors Platform	Advisors Genesys Adapter in a Genesys environment
Workforce Advisor	Advisors Platform	Contact Center Advisor
Resource Management Console	Advisors Platform Supervisor Desktop Service	Contact Center Advisor

> **Important**
>
> XML Generator runs independently of Advisors Platform. In other words, the startup of CCAdv XML Generator is not dependent on Advisors Platform startup. XML Generator can be installed on a server with Advisors Platform, but that is not required.

Pulse Advisors Architecture

The following figure shows the Pulse Advisors architecture, including the data flow between Advisors components and other Genesys components. Yellow text in the diagram indicates Advisors components that support primary/backup high availability. Secure connections are supported between the user interfaces and Web servers, and between servers and databases, Genesys Configuration Server, Stat Server, and the Genesys WFM Server.


HTTP API, Websocket
Load Balancer, Apache web servers
Advisors Cluster
Advisors Web Services Node 1
Advisors Web Services Node N +1
Admin
CCAdv Server (XMLGen)
FA Server
WA Server
CCAdv Genesys Adapters (1 or more)
FA Genesys Adapters (1 or more)
MS SQL/ Oracle DB Server Cluster
Stat Servers (1 or more)
Stat Servers (1 or more)
Config Server
Genesys WFM Cluster/ Aspect eWFM/ IEX Total View

Deployment Summary

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

Advisors integrate with the Genesys Management Layer. 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).

You configure Stat Servers as connections to the Advisors Genesys Adapter (AGA) Application object in the Genesys Configuration Server. 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 that you will deploy. In Oracle installations, make sure that Advisors Genesys Adapter (AGA) metrics, metric graphing, and Platform users are created with all of the necessary privileges that are listed in the `advisors-xxxx-<version>_Userxxxx.sql` script that corresponds to your release. Delegate the Users creation task or the whole database creation task to your DBA because the user creation task requires elevated Oracle privileges.

   Perform the database installation in the following order:

   a. AGA metrics database

   b. Grant `select` privileges on all AGA metrics views to the Platform user.

   c. Metric Graphing database

   d. Advisors Platform database

   e. If you want the Advisors applications to run as an application user with least privileges instead of a database user-schema owner, and your installation is with Oracle, ask your DBA to review and apply the `advisors-platform-<version>_UsersAndRoles.sql` script. For MS SQL installations and additional information, see the enhanced security setup.

2. Create the Advisors User account in Genesys Configuration Server.
3. Install the Platform service on servers where it is required for Advisors components. The Platform service is a prerequisite for installing the following components:
   - Advisors Administration
   - Advisors Web Services
   - WA Server
   - FA Server with rollup engine
   - CCAdv/WA/FA Accessibility services
   - CCAdv/WA Resource Management console
4. Install each adapter that you will use and configure the adapter Application objects with Stat Server

connections.

5. Install the Advisors components for your enterprise:
   - Contact Center Advisor server (CCAdv XML Generator)
   - Workforce Advisor server
   - Frontline Advisor server
   - SDS and the CCAdv/WA Resource Management console
6. In installations with Oracle, validate the database by executing the `advisors-platform-<version>_ValidateDatabaseInstall.sql` script as the schema owner after you install XML Generator and before you start it. If you do not see this file in your installation package, see the recommendations for Oracle users.
7. Make any required configuration changes.
8. Run the Advisors Object Migration Utility if necessary.

   Use the Advisors Object Migration Utility when:

   a. You first install Advisors in an environment with a new Configuration Server or when you move an existing Advisors installation to a new Configuration Server.

   b. If any of the required Business Attributes folders that Advisors components use are not already present in the Configuration Server.

   c. If you decide to enable metrics that are not yet present in your Configuration Server.

   d. If you decide to use the Advisors default rollup configuration. Starting with Advisors release 9.0.001.06, a brand new Platform database contains a set of Advisors default hierarchy objects that must be added to the Configuration Server to make the automatic configuration visible on the dashboard. The automatic configuration consists of all base objects mapped to the default hierarchy. For more information, see Contact Center Advisor Default Rollup Configuration in the *Contact Center Advisor and Workforce Advisor Administrator User's Guide*.

   e. If you perform a new installation in an environment that previously had an Advisors release installed that was older than release 8.5.1. In this case, remove all FA metrics that are in the Configuration Server and then run the migration wizard to populate all FA and CCAdv metrics and hierarchy business attributes.

Presentation Nodes

The Platform server nodes on which you install Advisors Web Services are called the *presentation nodes*. These are the nodes to which all user requests will be routed. For example, Apache proxy pass redirects are expected to be routed primarily to these presentation nodes. Installing Advisors Web Services is sufficient to enable all of the Advisors dashboards (that is, the Contact Center Advisor, Workforce Advisor, and Frontline Advisor dashboards).

On these presentation nodes, you can install optional additional services such as the Metric Graphing service, the CCAdv/WA/FA accessible dashboards, or the Resource Management console.

Server Nodes

When you install the WA Server or FA Rollup engine server on the Platform server nodes, the nodes are called *server nodes*.

> **Important**
>
> XML Generator can be installed either on a separate folder or under an existing Platform server installation. In either of those deployments, XML Generator is a separate process from the Platform server process. The only commonality of installing XML Generator on the same folder as the Platform server is sharing of the configuration files between them.

For performance reasons, Genesys recommends that you avoid installing the server components (WA Server or FA rollup engine) and the Advisor Web Services on the same Platform server node.

Prerequisites

This page provides general information about the Genesys Pulse Advisors deployment environment. Also in the **Prerequisites** section is information specific to each Pulse 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
- Contact Center Advisor and Workforce Advisor
- Frontline Advisor and Agent Advisor

Integration with the Genesys Solution Control Server

The following Advisors components are controlled using the Solution Control Server:

- Advisors Genesys 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 Genesys Configuration Server for each system that runs any of the preceding components. See Genesys Administrator Extension Help for information.
- Configure an Application in Genesys Configuration Server for each Advisors server that runs one or more of the preceding components. See 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) or the Genesys configuration interface that you use, such as Genesys Administrator Extension.

For more details, see Integration with Solution Control Server and Warm Standby and Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS.

Importance of Advisors Platform

Most Pulse 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 and Advisors Genesys Adapter, which 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:

- Tomcat
- Mail-Delivery service
- Cache service
- Database resource configuration
- Core components for:
  - High availability
  - Authentication
  - Genesys Management Framework integration

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 Pulse Advisors, ensure you 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 Configuration Interface

You can use Genesys Administrator for much of the post-deployment configuration associated with Genesys Pulse Advisors, however you must have access to the Genesys Configuration Manager to perform some of the administrative functions related to Role-Based Access Control (RBAC). While you can use any Genesys configuration interface (Configuration Manager, Genesys Administrator, or GAX)

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

Operating systems

You can deploy Pulse Advisors on Microsoft Windows or 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 the *Genesys Supported Operating Environment Reference Guide* and *Genesys Interoperability Guide*.

Using Advisors Installation Wizards on Linux Servers

If you install Advisors components on Linux machines, be aware that there are additional security concerns related to Advisors installation. The Advisors installation wizards are graphical installers. To run these installers as they were intended, you require the X Windows System on your Linux machines.

Without the X Windows System, passwords that you enter during the installation process display in plain text; therefore, during installation, Genesys recommends that you take extra precautions to ensure that only users with the correct security permissions are allowed to view the screen where you are running the Advisors installers.

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 can use port 80.
- One of the following Relational Database Management Systems (RDBMS) – for detailed information, see Databases:
  - Microsoft SQL Server
  - Oracle

    If you use Oracle, the appropriate Oracle JDBC driver is also required. You can obtain the driver from the Oracle Web site (www.oracle.com).

    The latest supported Oracle drivers are the following:
  - For Oracle Database 12c Release 1 (12.1.0.1), use ojdbc7.jar
  - For Oracle Database 12c Release 2 (12.2.0.1), use ojdbc8.jar

For information about specific versions of the preceding software components that are compatible

with the Advisors release to which you are migrating, see the *Genesys Supported Operating Environment Reference Guide*.

MS SQL Server Databases/Oracle Schemas

The following MS SQL Server databases/Oracle schemas are required in an Advisors installation:

- Advisors Genesys Adapter metrics database(s)/Oracle schema(s) – Contain transient raw metric data and base object metadata processed by AGA instance(s) and used by CCAdv and WA components.
- Advisors Platform database – Contains various configurations and pre-processed transient metric data. Used by all Advisors components: AGA, FA, CCAdv, and WA.
- Advisors metrics graphing database – Used for storing Contact Center Advisor and Workforce Advisor data for metric graphing. The installation is mandatory even if the metric graphing feature is not used.

Genesys Pulse Advisors applications support Microsoft SQL Server and Oracle RDBMS. You cannot mix database types within an Advisors installation; each installation must be either wholly MS SQL Server or wholly Oracle. See the *Genesys Supported Operating Environment Reference Guide* for supported RDBMS versions and features.

Database Recommendations for MS SQL Server Users

If you use MS SQL Server, 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 Server Enterprise Edition, but you do not want to use partitioning, install the metric graphing database by running the metric graphing database script located in the folder for the Standard MS SQL Server edition. To be precise, in installations prior to Release 8.5.2, use the script(s) located in the `\ip\mssql-standard` directory of your CCAdv/WA installation package; starting with Release 8.5.2, use the script(s) located in the `ip\metric-graphing-database-sql\mssql-standard` directory of your Platform installation package.

Starting with Advisors release 8.5.2, Advisors applications support the MS SQL Server AlwaysOn Availability Groups and AlwaysOn Failover Cluster Instances features. However, for performance reasons, Genesys does not recommend placing Advisors databases in MS SQL Server environments where the simple recovery model is not allowed. Advisors databases are very small in size. The data persisted during application operation is transient and, in case of any failure, there is no danger of any data loss as long as you keep a backup of the Platform database that was made after the Advisors configuration was put in place or updated. Any other data will be re-populated once the application is up and running again. If you decide to install the databases with other than simple recovery model, then a thorough schedule of transaction log back up must be put in place, and tuned to achieve the best database performance.

Database Recommendations for Oracle Users

You achieve the best performance from an Advisors application when it uses an Oracle non-RAC database, ideally dedicated to the Advisors application, or shared with OLTP applications that do not have long-running transactions. Advisors operates with large amounts of data, but all of the data is transient. The data that is permanently saved in an Advisors database is Advisors configuration data, populated during application installation and rarely modified later. Therefore, for recovery purposes, it is sufficient to keep a Data Pump Export of Advisors schemas that includes the latest configuration, as well as all Grants and Roles. In case of a failure, the configuration can be imported from the export files, while all of the operational data will be recovered automatically once the application is up and running again. To improve Advisors application performance, maintain periodic Data Pump Export files and run the database in `NOARCHIVELOG` mode, if possible.

A well-tuned redo log structure is very important for Advisors performance, as well. Issues with the redo log structure, such as frequent log switches, will negatively impact Advisors performance.

Another condition for good application performance is the presence of adequate statistics for the Advisors schemas. The statistics for Advisors schemas need to be gathered during the typical application load, rather than on the weekends when the contact center activity is low, in order to ensure that the optimizer operates with the representative statistics. The preferred method of gathering statistics for Advisors schemas is the following:

```
 exec dbms_stats.gather_schema_stats( ownname => '<PLATFORM SCHEMA OWNER>', estimate_percent => DBMS_STATS.AUTO_SAMPLE_SIZE, method_opt
=> 'FOR ALL COLUMNS SIZE AUTO', cascade => true);
exec dbms_stats.gather_schema_stats( ownname => '<AGA METRICS SCHEMA OWNER' , estimate_percent => DBMS_STATS.AUTO_SAMPLE_SIZE, method_opt
=> 'FOR ALL COLUMNS SIZE AUTO', cascade => true);
exec dbms_stats.gather_schema_stats( ownname => '<METRIC GRAPHING SCHEMA OWNER>', estimate_percent => DBMS_STATS.AUTO_SAMPLE_SIZE,
method_opt => 'FOR ALL COLUMNS SIZE AUTO', cascade => true);
```

Any database maintenance event that involves the removal of optimizer data will require that you gather Advisors statistics the next business day, during the typical call activity.

If you use Oracle databases, 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 does not include the partitioning option or you do not want to use partitioning, use the metric graphing schema scripts contained in the {{oracle-without-partitions}} directory. To be precise, in the installations prior to Release 8.5.2, use the script(s) located in the `\ip\oracle-without-partitions` directory of your CCAdv/WA installation package; starting with Release 8.5.2, use the script(s) located in the `ip\metric-graphing-database-sql\oracle-without-partitions` directory of your Platform installation package. Otherwise, use the script from the `oracle-with-partitions` directory.

Advisors applications support Oracle Real Application Clusters (RAC).

If you use Oracle databases with the Advisors applications, then 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.

Starting with Advisors release 8.5.2, you either need to grant the `execute` privilege on the SYS.DBMS_LOCK package to the Platform schema owner, or you need the Oracle JServer component to be installed in the Oracle database.

Note that there are different scripts for installations with or without JServer. In installations without JServer, use the scripts located in the `/ip/sql/platform-database-sql/oracle/oracleNoJserver` directory of your Platform Installation Package. In installations with JServer, use the scripts from the `ip/sql/platform-database-sql/oracle/` folder.

The Advisors Platform schema owner requires some inter-schema privileges, such as the `select` privilege on all AGA metrics views, the EXECUTE privilege on `SYS.GENADVISORSJOBCLASS`, or, in Oracle installations without JServer, the EXECUTE privilege on `SYS.DBMS_LOCK`, which might disappear after certain operations are applied to Advisors database schemas, such as the restoration of the Platform schema from an export file, or an AGA schema upgrade.

Make sure that all of the privileges that are listed in the `advisors-xxxx-<version>_Userxxxx.sql` script that corresponds to your release are present before you apply the Platform migration script or Platform object creation deployment script.

Genesys recommends that you always run the database validation script as part of the Advisors deployment or migration process. The script is supplied in the installation package starting with release 9.0.001.06 The name of the script is `advisors-platform-<version>_ValidateDatabaseInstall.sql`. For earlier releases, use the script shown below. Execute the script *after* you have performed one of the following actions and *before* you start Advisors components:

- you have manually added or modified a data source (Platform ICM_DATABASE table)

- you have implemented a restore operation of the Advisors Platform schema, such as Data Pump Import
- you have just completed installing or migrating the application

If your installation package does not contain the `advisors-platform-<version_ValidateDatabaseInstall.sql` script, then run the applicable script shown below:

- Script for release 8.5.202.10 and any release before 8.5.202.10
- Script for any release after release 8.5.202.10

Script for release 8.5.202.10 and any release before 8.5.202.10

```
DECLARE v_temp NUMBER;
BEGIN

BEGIN
SPADDSOURCEVIEWS();
END;

BEGIN
SPCOMPILEINVALID();
END;

BEGIN
SELECT 1 INTO v_temp FROM DUAL WHERE EXISTS(SELECT 1 FROM USER_SCHEDULER_JOBS WHERE
                                    JOB_NAME='JOB_R_SPUPDATEDATASOURCESTATUS');
    DBMS_SCHEDULER.DROP_JOB(job_name => 'JOB_R_SPUPDATEDATASOURCESTATUS',
                                defer => false,
                                force => true);
       EXCEPTION WHEN NO_DATA_FOUND THEN NULL;
END;

DECLARE
  M VARCHAR2(4000);
  R NUMBER;
BEGIN
  SPTRUNCATESTAGINGTABLES(
    M => M,
    R => R
  );
END;

BEGIN
SELECT 1 INTO v_temp FROM DUAL WHERE EXISTS(SELECT 1 FROM USER_SCHEDULER_JOBS WHERE
                                    JOB_NAME='JOB_R_SPUPDATEDATASOURCESTATUS');
      DBMS_SCHEDULER.disable(name=>'JOB_R_SPUPDATEDATASOURCESTATUS', force => TRUE);
       EXCEPTION WHEN NO_DATA_FOUND THEN NULL;
END;
END;
```

Script for any release after 8.5.202.10

```
WHENEVER SQLERROR EXIT FAILURE
WHENEVER OSERROR EXIT FAILURE

SET SERVEROUTPUT ON
SET FEEDBACK OFF
```

```
DECLARE m VARCHAR2(4000);r INTEGER;
BEGIN
   BEGIN
    SELECT 1 INTO r FROM DUAL WHERE EXISTS(SELECT 1 FROM USER_SCHEDULER_JOBS WHERE
                                        JOB_NAME='JOB_R_SPUPDATEDATASOURCESTATUS');
        DBMS_SCHEDULER.DROP_JOB(job_name => 'JOB_R_SPUPDATEDATASOURCESTATUS',
                                    defer => false,
                                    force => true);
           EXCEPTION WHEN NO_DATA_FOUND THEN NULL;
   END;
   SELECT 1 INTO r FROM DUAL WHERE EXISTS(SELECT 1 FROM ICM_DATABASE WHERE SOURCE_ID>0);
   spAddSourceMetaDataViews();
   spAddSourceViews();
   spCompileInvalid();
   spTRUNCATESTAGINGTABLES(m => m,r => r);
   SELECT 1 INTO r FROM DUAL WHERE EXISTS(SELECT 1 FROM PATCH_LOG);
     dbms_output.put_line('Successfuly validated the database installation.');
           EXCEPTION
            WHEN NO_DATA_FOUND THEN
            dbms_output.put_line('Schema validation completed with errors.');
            dbms_output.put_line('The schema content is incomplete. Check the output log from
the platform schema creation script.');
            dbms_output.put_line('Check if the ICM_DATABASE table contains at least 1 data
source that has SOURCE_ID other than 0.');
            WHEN OTHERS THEN
            BEGIN
             dbms_output.put_line('Schema creation completed with errors.');
             dbms_output.put_line('Compile each invalid object manually to identify ');
             dbms_output.put_line('the reason of the problem.');
             dbms_output.put_line('Examine the output logs of the schema creation script.');
             dbms_output.put_line(sqlerrm);
              END;

END;
/
EXIT
```

Start all components only if the database validation script is successful. Otherwise, recover/grant the privileges, or fix other problems reported by the script, then re-run the script until it is successful. Contact Genesys support if you cannot achieve a successful script outcome.

If you get the following error, `ORA-28511: lost RPC connection`, then re-run the script immediately after it fails with this error. This error is not related to insufficient privileges. Normally, this is a temporary issue that is caused by a temporary connection loss, which can occur if you have a data source connected through Oracle heterogeneous services. If the problem persists, ask your DBA to verify the related connectivity setup.

See additional details in the Oracle database creation section of this guide, or in the corresponding Readme files in the `ip\platform-database-sql\oracle` folder of your Platform Installation Package.

If any of the Oracle Platform migration scripts that you use in the migration process to release 9.0 issue an error about insufficient privileges (`ORA-20001: spCreateOneSourceView ORA-01031: insufficient privileges`) and you are convinced that the Platform user has been issued all of the privileges listed in the `advisors-platform<version>_User.sql` creation script, then see additional information in the release 9.0 migration procedure.

If the Oracle Platform deployment script issues an error about insufficient privileges (`ORA-20001: spCreateOneSourceView ORA-01031: insufficient privileges`) and you are convinced that the

Platform user has been issued all the privileges listed in the `advisors-platform-<version>_User.sql` creation script, then see additional information in the release 9.0 deployment procedure (open the IMPORTANT INFORMATION notes in the deployment roadmap summary).

Database Connections Secured with TLS 1.2

Starting with release 8.5.2, you can enable TLS 1.2 for encryption and authentication on Advisors MS SQL Server database connections.

The following are prerequisites for TLS 1.2 connections on MS SQL Server installations:

- Java version 8, as a minimum. See the *Genesys Supported Operating Environment Reference Guide* for details about supported Java versions for Advisors releases.
- Any supported version of MS SQL Server starting with MS SQL Server 2008 R2 to MS SQL Server 2014, configured to accept encrypted connections.
- Microsoft JDBC driver 6.2 for SQL Server. This driver is supplied in the Advisors Installation Packages. Advisors installation wizards automatically place the file, `mssql-jdbc-6.2.1.jre8.jar`, in the `lib` folder of each component that requires database access.
- Every machine that hosts Advisors components and that communicates with Oracle over SSL must have a list of trusted certificates installed in a keystore.
- Review all Microsoft recommendations associated with TLS support, as well as descriptions of known issues related to enabling TLS for the database server:
  TLS 1.2 support for Microsoft SQL Server

  SQL Server Release Services

Database Recommendations for Advisors Cluster Installations

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 which Platform server will have the Administration workbench.

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 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 installations. 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?
- Will you use the existing Configuration Server–based authentication system, or the SAML 2.0 Single Sign-On (SSO) login process? If you are planning to use SAML authentication, do you have a SAML 2.0 capable Identity Provider? For example, Microsoft ADFS, Okta, Shibboleth, and so on. Note that the following features are not supported when using the SSO login process:
  - Change password and Forgot password functionality
  - Advisors Resource Management Console (RMC)
- On which server will you install the Advisors Administration module? The Administration module must be installed on at least one system.
- Where will you store log files? Starting with release 9.0.001, you can specify a log file storage location when you run the Advisors Platform installation wizard.
- Will you install the modules of Advisors distributed in a cluster on several systems, or all on one system?
- Each system on which you install Advisors Platform or CCAdv 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 email notification messages? From what address will an application send notifications (for example, `DONOTREPLY@<your enterprise>.com`)? To what email address will an application send notifications?
- Which language(s) will be used for email notifications from the system? (Advisors supports English, German, and French in release 8.5.2.)
- Will you deploy Advisors Web Services on this system? If so, for optimum performance, Genesys recommends that you avoid installing any of the following components on the same system: CCAdv XML Generator, WA Server, or FA Server with rollup engine on the same system.
- Will you later deploy, on this system, one of the following modules?
  - CCAdv XML Generator
  - WA Server
  - FA Server with 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.

    In addition, for optimum performance, Genesys recommends that you avoid installing Advisors Web Services on the same system as any of the preceding components.

- 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 your Genesys configuration interface, such as Genesys Administrator).
  - You must configure Application and Host objects in Genesys Configuration Server 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.
	In a Genesys environment, you have established connection to the Genesys Configuration Server and to its backup if there is one. 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: • CCAdv XML Generator • Workforce Advisor Server • Frontline Advisor Server (with the rollup engine) • Resource Management Console 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 *writes* 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.
	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.

Y or N	Prerequisite

	You have installed JDK on the server on which you will be deploying Advisors Platform. You can use either Oracle JDK or, starting with release 9.0.002, OpenJDK. See the *Genesys Supported Operating Environment Reference Guide* for information about Java versions supported with each Advisors release.
	
	OpenJDK
	
	You can find OpenJDK files at https://openjdk.java.net/install/index.html.
	
	Oracle JDK
	
	You can find Oracle Java files at http://www.oracle.com/technetwork/java/javase/downloads/index.html.
	
	For Advisors installations on a Linux platform, the correct Oracle JDK file to use is the archive binary file (.tar.gz). For installations on a Windows platform, the correct Oracle JDK file is the .zip archive file.
	
	Linux environments
	
	The following procedure is provided as an aid for installing the JDK on a Linux machine and verifying that the installation was successful. The procedure uses JDK 7 in the sample input and output, however Advisors components no longer support JDK 7. Ensure you enter the correct JDK version number that you use in your installation. See the *Genesys Supported Operating Environment Reference Guide* for information about Java versions supported with each Advisors release.
	
	1. As root, navigate to the directory that has the downloaded JDK and copy the JDK archive binary file to the Advisors home directory:
	`cp ./jdk-7u<version>-linux-x64.tar.gz /home/advisors`
	2. Navigate to the Advisors home directory:
	`cd /home/advisors`
	3. As root, unpack the archive and install the JDK:
	`tar zxvf jdk-7u<version>-linux-x64.tar.gz`
	4. As root, change the owner of the installed JDK:
	`chown -R advisors:advisors jdk1.7.0_<version>`
	5. As root, change to the Advisors user and test JDK:
	`su - advisors`
	
	`./jdk1.7.0_<version>/bin/java -version`
	
	You should see output similar to the following:
	`java version "1.7.0_40"`
	
	`Java(TM) SE Runtime Environment (build 1.7.0_40-b43)`
	
	`Java HotSpot(TM) 64-Bit Server VM (build 24.0-b56, mixed mode)`

	If you plan to connect to the Configuration Server using TLS, you have configured a

Y or N	Prerequisite
	secure port for Genesys Configuration Server. For more information, see the Genesys Security Deployment Guide.
	If you plan to connect to the Configuration Server using TLS, you have configured security certificates: • You have configured the security providers and issue security certificates. For more information, see Genesys Platform SDK Developer's Guide. • You have assigned a certificate to the Configuration Server host in Genesys Administrator. For more information, see the Genesys Security Deployment Guide.
	On the system on which you are installing Advisors Platform, you have set the Regional and Language options to the locale for which you want the servers to be deployed.
	If you are going to use two different deployments of Advisors on the same machine, then you have chosen different values for the port numbers that each deployment will use. See Multiple Advisors Deployments on One System.
	You have located the `advisors-platform-installer-<version>.jar` file on the installation CD and have copied it to the local drive of your server. **[+] Show additional information for Linux environments** 1. You can start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled: `ssh -X root@<host>` 2. As root, place the `advisors-platform-installer-<version>.jar` 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 Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS for information.

	If you are deploying Advisors Platform on a Linux system, you must first create the Advisors group and user. The Advisors Platform is run as the *advisors user*, which belongs to the *advisors group*.
	[+] Show Steps
	1. Open the shell.
	2. As root, create the Advisors group:
	`groupadd advisors`
	3. As root, create the Advisors user in the Advisors group:
	`useradd -s /bin/bash -g advisors advisors`
	The preceding command creates the /home/advisors directory. If you want a different directory, you can use

Y or N	Prerequisite

	the following command:
	`useradd -g advisors -d <path to the desired directory> advisors`
	You can optionally set a password for the Advisors user:
	`passwd advisors`
	Genesys recommends that you mount /home as a separate partition.

	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: • the no password change at first login option • the override password expiration option For information about the no password change at first login and override password expiration options, see *Genesys Framework Configuration Options Reference Manual*. Important After you install the Advisors applications, you must also ensure you assign the `Advisors.ChangePassword.canView` privilege to all users. Pulse 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 `Advisors.ChangePassword.canView` privilege to all users.

Collect Information

During deployment of Advisors Platform, the installation wizard prompts you for the information in the following table. The table includes the default values provided by the wizard.

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.	Default on Windows:
	`C:\Program Files\GCTI\Advisors`
	Default on Linux:
	`/opt/gcti/advisors`

Path to the directory in which log files will be written. Starting with release	Default on Windows:

Information	Input

9.0.001, the installation wizard prompts you to provide the log file storage location, and provides a default path.
 	
Specifying the log file directory in the installation wizard will not change the directory that was set for previous installations.
For more information about log files, see Adjust Logging Settings and Configure Administrative Actions Logs.
	`c:\genesys\log\advisors\platform\`
	
	Default on Linux:
	
	`/mnt/log/advisors/platform/`

Location of the Java Development Kit (root directory).	
Port numbers that Tomcat will use. You will typically use the default values that the installation wizard provides, except in the following situations: • You are going to install two different deployments of Advisors on the same machine, so you require two sets of port numbers. For more information, see Multiple Advisors Deployments on One System. • Other software is running on the same host and is already using the ports, in which case you must assign other ports for Tomcat to use.	Default values are: • HTTP port: 8080 • HTTPS port: 8443 • AJP port: 8009 • JMX port: 9999 • Management port: 8005
If you are installing the Administration module, then locate the name, in Configuration Server, of the primary Solution Control Server Application that you will use with Advisors.	Default value is `SCServer`.
If you are installing the Administration module, then you require the following information from the Configuration Server: • the name of the XML Generator application • the port number on which that application listens • the name of the host associated with that application If you are deploying Advisors in a warm standby configuration, then you require this information for both the primary and backup XML Generator applications.	Default value for both port numbers is 8090.
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.
Details to connect to the Genesys Configuration Server: • The name of the Configuration Server (the Application name, obtained	Defaults are: • Configuration server

Information	Input
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* account (see Create the Advisors User Account for information). 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: • CCAdv XML Generator • Workforce Advisor Server • Frontline Advisor Server (with the rollup engine) • Resource Management Console 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 *writes* 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. If you will connect to the Configuration Server using TLS, then you also require the following information: • The TLS port number for the Configuration Server. • The location of the TLS properties file. If you use a backup Configuration Server, you require the following information, as well: • 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.	name: confserv • Configuration server port: 2020 • Application name: default
Will you synchronize user updates between the Configuration Server and the Advisors database? To synchronize user updates, an installation must include the Administration module.	
If you use the SAML 2.0 SSO login process, you require the following information:	

Information	Input
• The authentication endpoint URL. That is, the URL that users will use to access Advisors applications. For more information, see the Authentication Options description on the Deploying Advisors Platform page in this guide. • The precise location of the file that contains the Identity Provider metadata or the URL from which the IdP metadata is served, whichever you use. Note that the following features are not supported when using the SSO login process: • Change password and Forgot password functionality • Advisors Resource Management Console (RMC)	
The name of the default tenant in the Configuration Server under which the Advisors metadata is maintained. 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 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.	
Will you enable **Forgot your password?** functionality (that is, allow password modification)? If you enable it, you can control user access to it with role-based access control.	
Type of database used in your enterprise (MS SQL or Oracle), and connection details for the Advisors Platform database: • 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). • 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 JDBC URL (you should have the freeform JDBC URL in a text file). • For an Oracle installation, the location of the JDBC driver.	Default values for port number: • Oracle: 1521 • MS SQL: 1433 When using numerical IP addresses or names with dots in the installations with MS SQL, enclose the literal in brackets. If the MS SQL database server is a named instance, then omit the port number and use double backslash: <host name>\\<instance name>
If you are installing Advisors Web Services with Platform, then you need the connection details for the Advisors Metric Graphing database: • The host name, IP address, or named instance of the server for the Metric Graphing database. • Port number that the database listens on (you do not require this information if the server is a named instance).	Default values for port number: • Oracle: 1521 • MS SQL: 1433 When using numerical IP addresses or names with dots in the installations

Information	Input
• The Platform database name (the Service name for an Oracle installation). • The Platform database username and password associated with the account that Advisors Web Services will use to access the Metric Graphing database. • For clustered databases, the location of the file that contains the JDBC URL (you should have the freeform JDBC URL in a text file). • For an Oracle installation, the location of the JDBC driver.	with MS SQL, enclose the literal in brackets.If the MS SQL database server is a named instance, then omit the port number and use double backslash: <host name>\\<instance name>
(Optional) If you will send email notifications from the application, such as email about user password–related events, then you require the following details for the SMTP (mail) service that you will use to send the notification messages: • SMTP server host name or IP address • The address from which to send application notification email • The address to which to send application notification email	Important Advisors modules store the email addresses that you enter on the installation wizards and use those addresses to notify support staff about operating issues. The email addresses are stored in the relevant properties file. A user's email address persists in the properties file even after a user's Person object is removed from Configuration Server. An email address that contains an employee's full name can be considered to be personally identifiable information (PII) and therefore, to be compliant with the General Data Protection Regulation (GDPR), you must remove the user's email address from the properties files if the user makes a "forget me" request. The need to update the properties file(s) to remove email addresses can be avoided if you always use an email alias for support staff, rather than user-identifying email addresses. For example, use advisors.support@yourcompany instead of john.doe@yourcompany.com. For more information about PII and the GDPR, see the *Genesys Security Deployment Guide*.

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`.
- Where will you store log files? Starting with release 9.0.001, the default storage location for log files changes.
- 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 intall 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?
- 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.
	You have installed JDK on the server on which you will be deploying AGA. You can use either Oracle JDK or, starting with release 9.0.002, OpenJDK. See the *Genesys Supported Operating Environment Reference Guide* for information about Java versions supported with each Advisors release. **OpenJDK** You can find OpenJDK files at https://openjdk.java.net/install/index.html. **Oracle JDK** You can find Oracle Java files at http://www.oracle.com/technetwork/java/javase/downloads/index.html. For Advisors installations on a Linux platform, the correct Oracle JDK file to use is the archive binary file (.tar.gz). For installations on a Windows platform, the correct Oracle JDK file is the .zip archive file.

Y or N	Prerequisite
	If you are deploying AGA on a Linux platform, you have created the Advisors group and user. This should be done when deploying Advisors Platform on the server.
	You have located the `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. **[+] Show additional information for Linux environments** 1. You can start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled: `ssh -X root@<host>` 2. As root, place the `aga-installer-<version>.jar` file into the Advisors home directory.
	A verified Genesys environment is ready and available. This includes (but is not limited to) Configuration Server, Stat Server, and the T-Server(s) and/or Interaction Servers. All of these services must be running prior to deploying the Genesys Adapter.
	You have 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.
	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 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 Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS for information.
	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. You must also be prepared to configure the Stat Servers as connections to the AGA Application object. For information, see Manage Advisors Stat Server Instances.
	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.
	You have estimated the number of Advisors Genesys Adapters that you require. Depending upon the number of statistics to be served, you might require more than one AGA.

Collect Information

During deployment of Advisors Genesys Adapter, the installation wizard prompts you for the information in the following table. The table includes the default values provided by the wizard.

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.	Default on Windows:
	`C:\Program Files\GCTI\Advisors\`
	Default on Linux:
	`/opt/gcti/advisors`

Path to the directory in which log files will be written. The default location changes starting with release 9.0.001.
Specifying the log file directory in the installation wizard will not change the directory that was set for previous installations.
For more information about log files, see Adjust Logging Settings and Configure Administrative Actions Logs.
	Release 9.0.000:
	• Default on Windows:
	`C:\Program Files\GCTI\Advisors\`
	• Default on Linux:
	`/opt/gcti/advisors`
	Release 9.0.001:
	• Default on Windows (specific default location is dependent on which module you are installing):
	`c:\genesys\log\advisors\`
	• Default on Linux (specific default location is dependent on which module you are installing):
	`/mnt/log/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: • 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	Default values for port number: • Oracle: 1521 • MS SQL: 1433

Information	Input
will use to access the Metrics Graphing database • For clustered databases, the location of the file that contains the JDBC URL (you should have the freeform JDBC URL in a text file).	
Connection details to the Advisors Platform database (use the same database configuration that was specified when the Advisors Platform database was configured): • 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 RAC JDBC URL (you should have the freeform JDBC URL in a text file).	Default values for port number: • Oracle: 1521 • MS SQL: 1433
Connection details to the Genesys Configuration Server: • 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'. If you will connect to the Configuration Server using TLS, then you also require the following information: • The TLS port number for the Configuration Server. • The location of the TLS properties file. If you use a backup Configuration Server, you require the following information, as well: • 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	Default port that the configuration server is listening on is 2020.

Information	Input
Configuration Server. • The port on which the backup Configuration Server listens.	
For integration with the Solution Control Server: • 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.	Default LCA port is 4999. Default SCS application name is SCServer.
For registration with the Platform database: • 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 CCAdv/WA). • In an Oracle environment, the location of the file that contains the RAC JDBC URL (you should have the freeform JDBC URL in a text file). If you do not know the location of the Oracle RAC JDBC URL, contact your database administrator.	Default port number is 7000.

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?
- NEW Where will you store log files? Starting with release 9.0.001, you can specify a storage location for log files when you run the installation wizard.
- Each of the modules associated with a CCAdv/WA installation (CCAdv XML Generator, WA server, Resource Management Console) 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 XML Generator 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 XML Generator 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 email notifications about alerts?
- Where did you install Advisors Platform on this system? When installing WA Server or RMC, the installation directory must be the same as the directory in which 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 Server.

Y or N	Prerequisite
	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 Advisors privileges associated with a Role only in Genesys Configuration Manager. If you need to view the Advisors privileges associated with Roles regularly, then ensure you have access to Genesys Configuration Manager.
	You have configured the Advisors User account in the Genesys Configuration Server. For more information see Creating the Advisors User.
	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: • Contact Center Advisor XML Generator: Platform database and metric graphing database • Workforce Advisor Server: Platform database and metric graphing database • Accessiblity Services, or Resource Management Console: Platform database. You have configured administrator accounts that can be used by applications to access the databases.
	Advisors Platform is successfully installed on each system on which you will install all modules (it is no longer required for CCAdv XML Generator).
	You have located the `ccadv-wa-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 Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS 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 Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS for more information.
	There is a database-level connection between the Advisors Platform database and the datasource database (a Genesys metrics database). To configure the connectivity, see Configure Oracle Metrics Data Sources.
	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.
	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 Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS for more information.

Y or N	Prerequisite
	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 Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS for information.

	Verified workforce management data sources must be ready and available.
	
	For Workforce Advisor installations connecting to Genesys WFM, the server running WA must be able to access your Genesys WFM installation.
	
	To verify this access, ensure you can do all of the following from your WA server machine:
	
	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 Genesys Administrator application.
	
	Your WA server must have access to the WFM server by its associated Genesys Administrator 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.
	
	If you cannot ping or access the Genesys WFM instance using the associated Genesys Administrator 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:
	`# For WA connectivity with WFM`
	`[IP address of WFM server] [Associated Genesys Administrator host name for the WFM instance]`
	
	Example: `192.168.98.229 demosrv.genesyslab.com`
	The hosts file is OS-specific. For example, for Windows 2003, the host file resides in the following location:
	`%SystemRoot%\system32\drivers\etc\`

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	

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.
	Default on Windows:
	
	`C:\Program Files\GCTI\Advisors`
	
	Default on Linux:
	
	`/opt/gcti/advisors`

Location of the Java Development Kit (root directory).	
Contact Center Advisor XML Generator	
NEW Path to the directory in which log files will be written. Starting with release 9.0.001, the installation wizard prompts you to provide the log file	Default on Windows:

Information	Input

storage location, and provides a default path.
 	
Specifying the log file directory in the installation wizard will not change the directory that was set for previous installations.
For more information about log files, see Adjust Logging Settings and Configure Administrative Actions Logs.
	`c:\genesys\log\advisors\ccadv-xmlgen\`
	
	Default on Linux:
	
	`/mnt/log/advisors/ccadv-xmlgen/`

Connection details to the Genesys Configuration Server: • 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'. Important If you are installing CCAdv 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. If you will connect to the Configuration Server using TLS, then you also require the following information: • The TLS port number for the Configuration Server. • The location of the TLS properties file. If you use a backup Configuration Server, you require the following information, as well: • 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.	Defaults are: • Configuration server name: confserv • Configuration server port: 2020 • Application name: default
The name of the default tenant in the Configuration Server under which the Advisors metadata is maintained. 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 tenant. The default tenant configuration is selected when installing the Advisors Platform server.	

Information	Input
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 email: • The host name or IP address of the SMTP server that XML Generator will use to send email. • (Optional) The address from which XML Generator will send notification email about alerts. • The address to which to send notification email for support staff concerning issues with XML Generator. This address will also appear in the `From:` header of these types of email.	Important Advisors modules store the email addresses that you enter on the installation wizards and use those addresses to notify support staff about operating issues. The email addresses are stored in the relevant properties file. A user's email address persists in the properties file even after a user's Person object is removed from Configuration

Information	Input
	Server. An email address that contains an employee's full name can be considered to be personally identifiable information (PII) and therefore, to be compliant with the General Data Protection Regulation (GDPR), you must remove the user's email address from the properties files if the user makes a "forget me" request. The need to update the properties file(s) to remove email addresses can be avoided if you always use an email alias for support staff, rather than user-identifying email addresses. For example, use advisors.support@yourcompany instead of john.doe@yourcompany.com. For more information about PII and the GDPR, see the *Genesys Security Deployment Guide*.
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. 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.	Default is 120 seconds.
The frequency (in seconds) at which snapshots are stored in the metric graphing database. For example, if you enter 60 seconds for this parameter, XML Generator and WA Server store graphable snapshots no more often than that. However, they may store the snapshots less frequently depending upon load and the complexity of the configuration.	Default is 60 seconds.
Should graphs display values from the previous day? Do *not* check the **Start at midnight** box if you want graphs to display values from the previous day.	
What are XML Generator's sources of real-time data? Specify the following: • 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 email. • the Relational Database Management System (RDBMS) type (MS SQL or Oracle)	

Information	Input
Up to five data sources may be added to the deployment of XML Generator.	
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 email 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: • 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: • 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: • The Application name of the WFM server as configured in the Configuration Server. • The URL of the WFM server. • The username WA Server will use to connect to Genesys WFM. • The password WA Server will use to connect to Genesys WFM. • 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: • Application name: WFM_Server • Username and password: no defaults. • Polling interval: 1800000 ms. (30 minutes.) • Number of hours of forecast metric to retrieve: 24 hours.
CCAdv XML Generator and Workforce Advisor Server	
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.
Type of database used in your enterprise (MS SQL or Oracle), and connection details to the Advisors Platform database: • 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	Default values for port number: • Oracle: 1521 • MS SQL: 1433 When using numerical IP

Information	Input
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 JDBC URL (you should have the freeform JDBC URL in a text file). Use the same database configuration that was specified when the Advisors Platform database was configured.	addresses or names with dots in the installations with MS SQL, enclose the literal in brackets. If the MS SQL database server is a named instance, then omit the port number and use double backslash: <host name>\\<instance name>
Connection details to the Metric Graphing database: • 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 JDBC URL (you should have the freeform JDBC URL in a text file).	Default values for port number: • Oracle: 1521 • MS SQL: 1433 When using numerical IP addresses or names with dots in the installations with MS SQL, enclose the literal in brackets. If the MS SQL database server is a named instance, then omit the port number and use double backslash: <host name>\\<instance name>

Prerequisites for FA

Before you deploy Frontline Advisor (FA), 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 email notification messages? From what address will an application send notifications (for example, `DONOTREPLY@<your enterprise>.com`)? To what email address will an application send notifications? What is the subject line for such email 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
	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 Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS 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 Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS 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 the following: • the tenant(s) associated with the hierarchy

Y or N	Prerequisite
	• the path to the hierarchy root folder(s) in Genesys Configuration Server

	You have located the `fa-server-installer-<version>.jar` file on the installation CD and have copied it to the local drive of your server. Copy the installation file to the Advisors home directory.
	[+] Show additional information for Linux environments
	
	1. Ensure the Advisors Platform service has been installed. The Advisors Platform service hosts the FA application.
	2. Open the shell.
	3. Start the installer locally or from a remote desktop. To run the installer remotely, use SSH with X11 forwarding enabled:
	`ssh -X root@<host>`
	4. As root, copy the fa-server-installer-<version>.jar file to the /home/advisors directory.
	`cp ./fa-server-installer-<version>.jar /home/advisors`

	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 Advisors privileges associated with a Role only in Genesys Configuration Manager. If you need to view the Advisors privileges associated with Roles regularly, then ensure you have access to Genesys Configuration Manager.

Collect Information

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

Information	Input

Location and name of the base directory in which you will install Advisors.
(The installation directory for Frontline Advisor server must be the same as the directory where Advisors Platform was installed.)
	Default on Windows:
	`C:\Program Files\GCTI\Advisors`
	Default on Linux:
	`/opt/gcti/advisors`

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 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.	

Information	Input
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): • 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.	Default LCA port is 4999. Default name of the SCS is SCServer.
Information about your hierarchy. You require one of the following: • 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). • The name of a `Person` folder in your Genesys configuration interface (for example, Genesys Administrator), 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).	Default tenant name is Resources. Default path to the hierarchy is Agent Groups\\Enterprise.
Type of database used in your enterprise (MS SQL or Oracle), and connection details to the Advisors Platform database: • 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 JDBC URL (you should have the freeform JDBC URL in a text file).	Default database server name is localhost. Default values for port number: • Oracle: 1521 • MS SQL: 1433
If you will send email notifications from the application, you require the following details for the SMTP (mail) service that you will use to send the notification messages: • The address from which to send application notification email. • The address to which to send application notification email.	Important Advisors modules store the email addresses that you enter on the installation wizards and use those addresses to notify support staff about operating issues. The email addresses are stored in the relevant properties file. A user's email address persists in the properties file even after a user's Person object is removed from Configuration Server. An email address that

Information	Input
	contains an employee's full name can be considered to be personally identifiable information (PII) and therefore, to be compliant with the General Data Protection Regulation (GDPR), you must remove the user's email address from the properties files if the user makes a "forget me" request. The need to update the properties file(s) to remove email addresses can be avoided if you always use an email alias for support staff, rather than user-identifying email addresses. For example, use advisors.support@yourcompany instead of john.doe@yourcompany.com. For more information about PII and the GDPR, see the *Genesys Security Deployment Guide*.

Create the Advisors Databases

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

Deployment Roadmap

The arrow icon in the following roadmap indicates where you are in the Advisors deployment process.

1. Install the databases that correspond to the Advisors products that you will deploy. Perform the database installation in the following order:
   a. AGA metrics database
   b. Grant `select` privileges on all AGA metrics views to the Platform user.
   c. Metric Graphing database
   d. Advisors Platform database
   [+] REVIEW IMPORTANT INFORMATION HERE

   If the Oracle Platform deployment script issues the following error, `ORA-20001: spCreateOneSourceView ORA-01031: insufficient privileges`, and you are sure that the Platform user has been issued all necessary privileges, then you might have role-based Oracle security set for the Platform user by your DBA. Make sure you take the deployment script from the **current_user** sub-folder in the installation package. You can apply the correct script on top of the one that you applied previously, ignoring the exceptions about existing objects and primary key violations. Alternatively, you can ask your DBA to recreate the user and the privileges and apply the correct script.

   If your installation package does not contain a **current_user** folder, edit the following scripts by replacing all entries of `DEFINER` with `CURRENT_USER` and repeat the database deployment process.

   - If initially you used `advisors-platform-<version>_Schema.sql` or `advisors-platform-<version>_ObjectsPlus.sql`, edit these scripts:
     `advisors-platform-<version>_CUSTOM_ROUTINE.sql`
     `advisors-platform-<version>_PIMPORT_xxx.sql`
     `advisors-platform-<version>_Routine1.sql`
   - If initially you used `advisors-platform-<version>_ObjectsCustom.sql` or `advisors-platform-<version>_ObjectsDefault.sql`, this would be the only script to edit.

   If you prefer, you can contact Genesys Support to obtain the edited scripts.

   Alternatively, you can set up the enhanced Oracle security to run Advisors applications as an application user with least privileges. For instructions, see Least Privileges: How to Configure Advisors Database Accounts with Minimal Privileges.

   If necessary, run the Advisors Object Migration utility. You must run the Advisors Object Migration utility when:

   - You first install Advisors in an environment with a new Configuration Server or when you move an existing Advisors installation to a new Configuration Server.
   - If any of the required Business Attributes folders that Advisors components use are not already present in the Configuration Server.
   - If you decide to enable metrics that are not yet present in your Configuration Server.
   - If you decide to use the Advisors default rollup configuration. Starting with Advisors release 9.0.001.06, a brand new Platform database contains a set of Advisors default hierarchy objects that must be added to the Configuration Server to make the automatic configuration visible on the dashboard. The automatic configuration consists of all base objects mapped to the default

hierarchy. For more information, see Contact Center Advisor Default Rollup Configuration in the *Contact Center Advisor and Workforce Advisor Administrator User's Guide*.

- If you perform a new installation in an environment that previously had an Advisors release installed that was older than release 8.5.1. In this case, remove all FA metrics that are in the Configuration Server and then run the migration wizard to populate all FA and CCAdv metrics and hierarchy business attributes.

2. Create the Advisors User account in Genesys Configuration Server.
3. Install the Platform service on servers where it is required for Advisors components. The Platform service is a prerequisite for installing the following components:
   - Advisors Administration
   - Advisors Web Services
   - WA Server
   - FA Server with rollup engine
   - CCAdv/WA/FA Accessibility services
   - CCAdv/WA Resource Management console
4. Install each adapter that you will use and configure the adapter Application objects with Stat Server connections.
5. Install the Advisors components for your enterprise.
   - Contact Center Advisor server (CCAdv XML Generator)
   - Workforce Advisor server
   - Frontline Advisor server
   - SDS and the CCAdv/WA Resource Management console
6. Make any required configuration changes.

Creating a SQL Server Database

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

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 examples of database names.

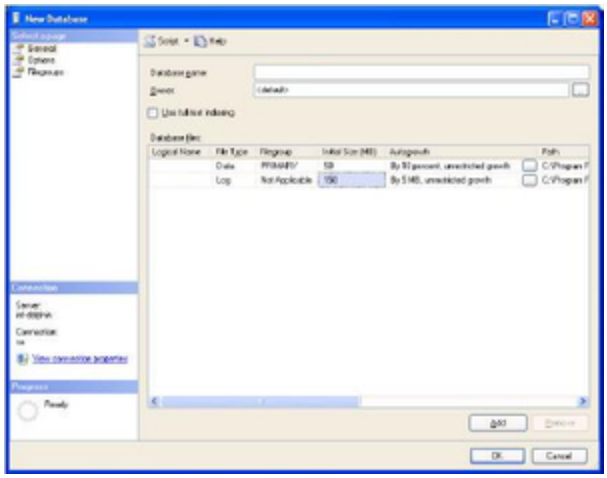
Advisors Component	Recommended DB name	Notes
Platform	advisors_platformdb	Required for Advisors implementations.
CCAdv/WA		Use the Platform and Metric Graphing databases.
FA		Uses the Platform database.
Metric Graphing	advisors_mgdb	Metric Graphing database. Required to run the CCAdv/WA dashboards and CCAdv XML Generator.
Advisors Genesys Adapter	advisors_gametricsdb	AGA metrics database. Used by AGA to transfer Genesys configuration and statistics values to XML Generator for CCAdv/WA. This database includes a table to support calling list statistics. This database is required for CCAdv/WA and WA server installations only.

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.

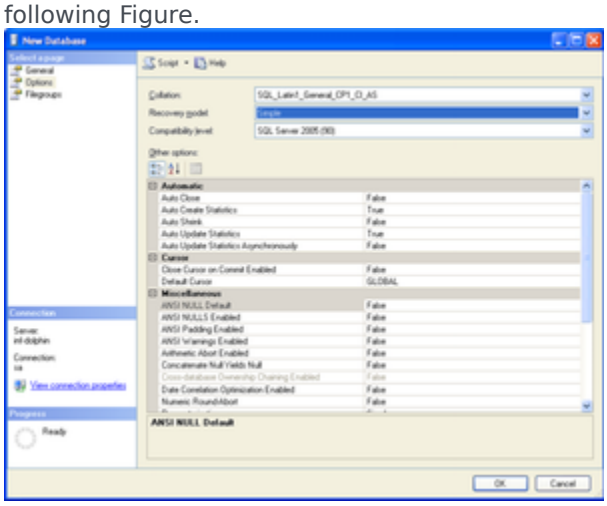
b. In the Recovery model field, select Simple.

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, <*databasename*_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

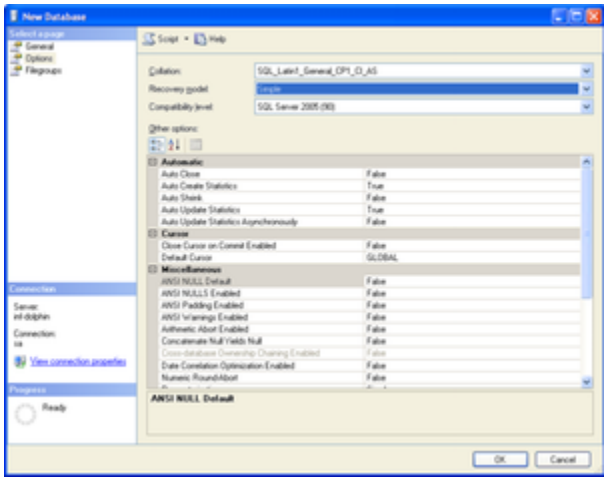
1. In the Microsoft SQL Server Management Studio object explorer, select `Server`, and then `Security`.
2. Right-click `Logins` and choose `New login`. See the Figure that follows—Server-level Security.

a. Specify the login name (in this example, `callcenter01`).

b. Click `SQL Server Authentication`.

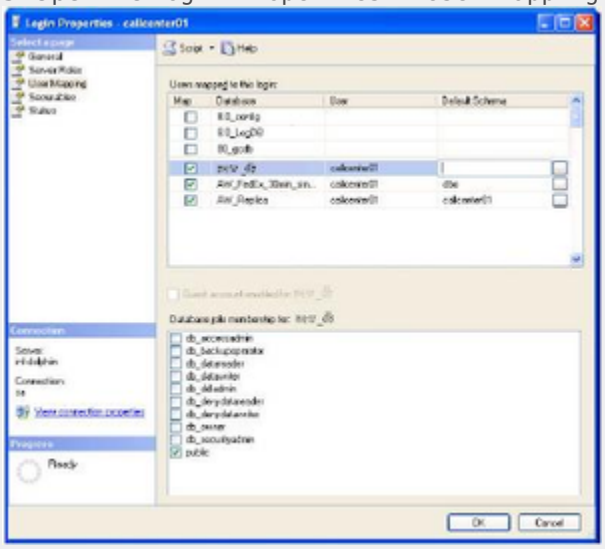
c. Specify a password that complies with your enterprise's security policy.

d. If strong passwords are part of the security policy, check the `Enforce password policy` check box.



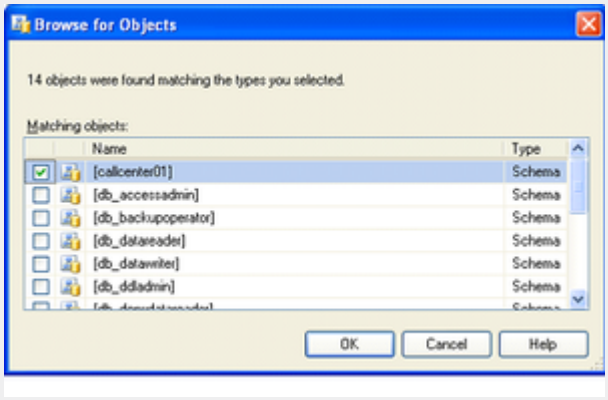
Server-level Security

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

   35px|link= Starting with Advisors release 8.5.202, you have an option to configure the database user with least privileges. See Least Privileges: How to Configure Advisors Database Accounts with Minimal Privileges for more information.

   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 the 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

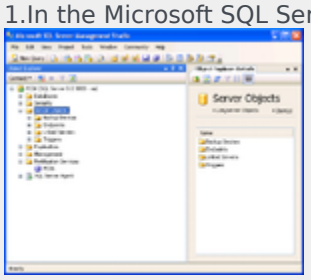
A linked server is normally not required to access the Advisors Genesys Adapter metrics database except in some uncommon cases when the Genesys Adapter metrics database and platform database reside on separate MSSQL Servers. However, each view in the Genesys Adapter metrics database must be accessible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

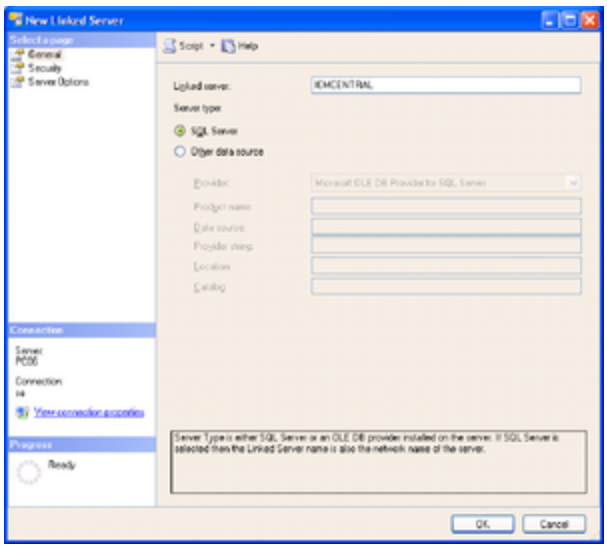
These two views must be accessible by the Platform user, also.

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

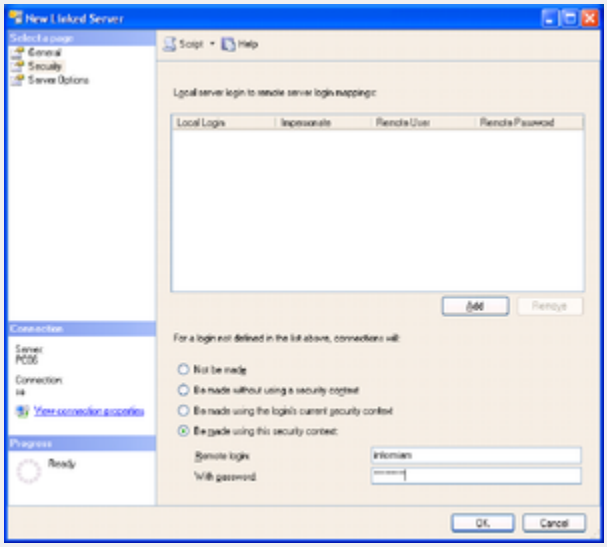
3. Under `Server type`, select `SQL Server`.

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:

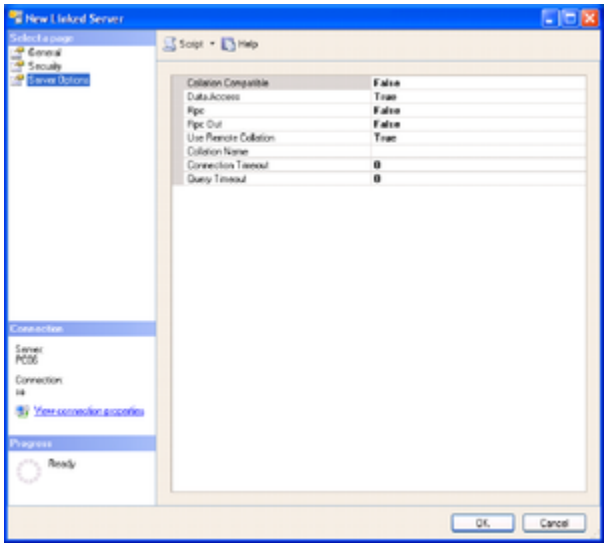
- Select `Be made using this security context`.
- Specify the remote login and password created by the external administrator for access to the external database.



New Linked Server – Security

6. On the `Server Options` screen:

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



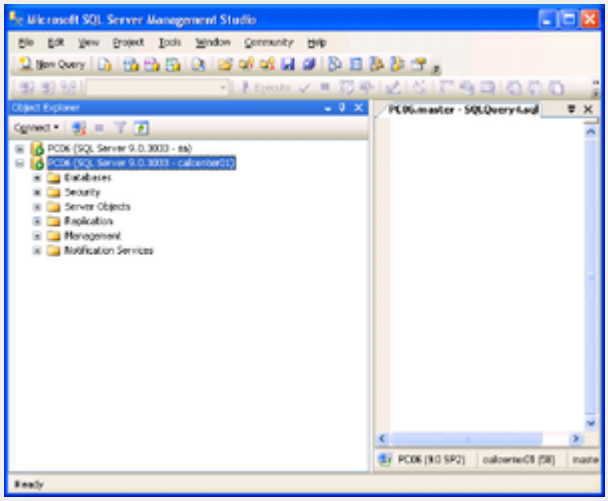
New Linked Server – Server Options

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

a. 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
(nolock)')
```

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

35px|link= Starting with Advisors release 8.5.202, you have an option to configure the database user with least privileges. See Least Privileges: How to Configure Advisors Database Accounts with Minimal Privileges for more information. Otherwise, complete the database user permissions setup as described below.

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, unless a separate migration script is supplied. If present, the separate migration script has to be used for migrations. The script name has the following pattern: `advisors-platform-migrateSchema_<from version>-<to version>.sql`. The script can be applied to any version starting from, and including, the `<from version>` up to, and including, the `<to version>` specified in the script name. Always check the Release Notes and "readme" files for details, specifics, and exceptions to the rules described in the documentation guides.

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.

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. Always review the "readme" files, if supplied, along with the database scripts. The "readme" files can contain important details, specifics, and exceptions related to a particular release, which are not reflected in the general documentation.

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.

Examples of Schema/User Names

Advisors Component	Schema/user name	Notes
Platform	advisors_platformdb	Required for Advisors implementations.
CCAdv/WA		Use the Platform and Metric Graphing schemas.
FA		Uses the Platform schema.
Metric Graphing	advisors_mgdb	Metric Graphing schema. Required to run the CCAdv/WA dashboards and CCAdv XML Generator.
Advisors Genesys Adapter	advisors_gametricsdb	AGA metrics schema. Used by AGA to transfer Genesys real-time statistic values to CCAdv/WA. This schema is required for CCAdv and WA server installations only.

Before You Begin

You must perform all of the steps in the procedure on a machine where you have Oracle client or Oracle instant client installed. The installation scripts require SQL*Plus, which is installed as part of the Oracle client installation or added in addition to the Oracle instant client installation.

Verify that you have your system or session `ORACLE_HOME` or `TNS_ADMIN` environment variable and

`tnsnames.ora` content set properly. If you have full Oracle client installed, you can verify the connectivity to the database by running the following command:
`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 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)
    )
  )
```

On the machine with full Oracle client installation, you can check the connectivity by typing the following command:

```
C:>tnsping wolf
```

The successful message will look as follows:

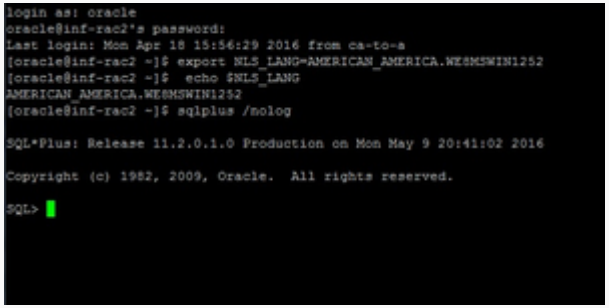
```
Used TNSNAMES adapter to resolve the alias
Attempting to contact (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = inf-wolf.qaslab.com)(PORT = 1521))
(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl.qalab.com)))
OK (0 msec)
```

Procedure

Procedure: Creating the Advisors Oracle Schema

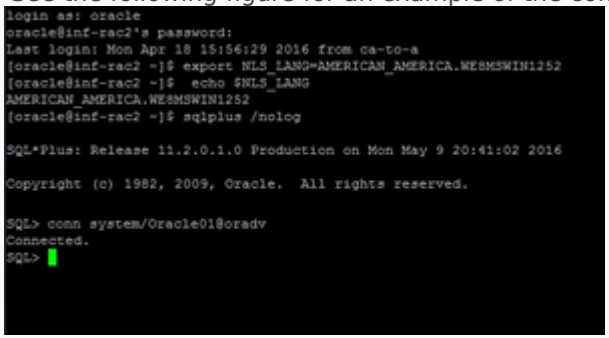
Steps

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.



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.



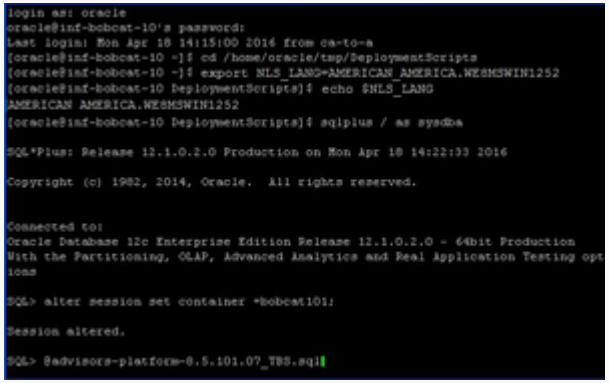
SQL Command Prompt 2

6. 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.

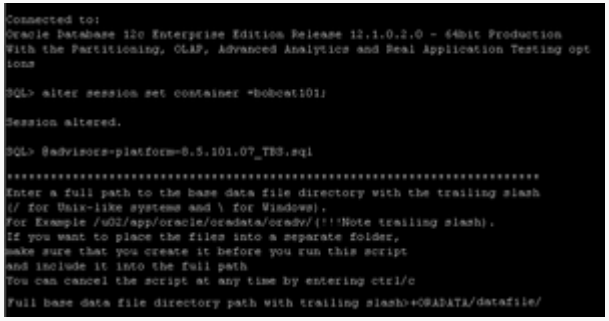


SQL Command Prompt 3

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.



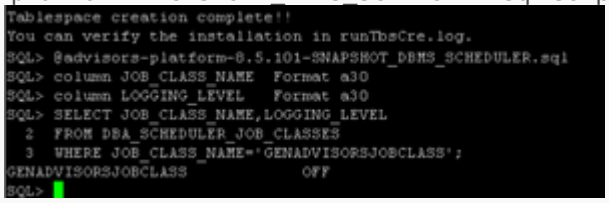
SQL Command Prompt 4

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. 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.



SQL Command Prompt 5

8. Create the user/schema and schema objects.

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

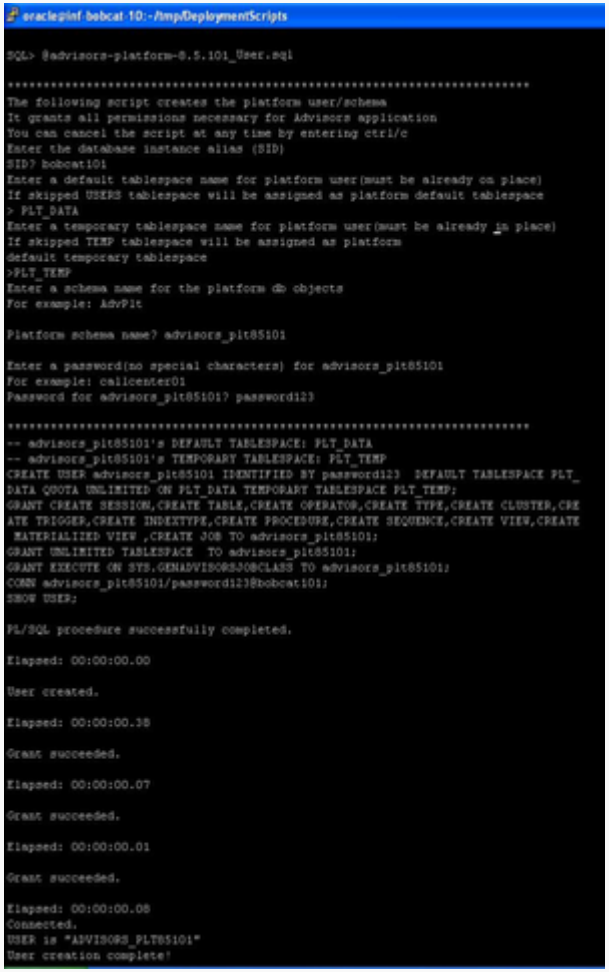
a. You, as a privileged user, or your DBA if you do not have privileged user access, must run the user creation script that is contained in the installation package (the script name ends with `_User.sql`). To run the user creation script, enter @<*script name*> at the prompt. For example:
`@advisors-platform-8.5.xxx_User.sql`, 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@inf-bobcat-10:~/tmp/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 on 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: AdvPlt
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.GENADVISORSJOBCLASS 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.

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.

This concludes a general Oracle schema/user setup where each created user is the owner of the corresponding schema: Platform, AGA metrics, or metric graphing. You can now specify the user in the relevant Advisors installation wizard screens related to database connectivity.

Database access for runtime users with least privileges

Starting with Advisors release 8.5.202, you have the option to configure database access through runtime users with least privileges, rather than through users who are "schema owners" . The procedure to create runtime users is implemented on top of the general Oracle schema/user setup. See Least Privileges: How to Configure Advisors Database Accounts with Minimal Privileges for more information.

Configure Oracle Metrics Data Sources

This page describes how to configure a connection to your Oracle metrics data sources for Pulse Advisors.

Configure a Connection to AGA Metrics Schema on the Same Oracle Instance as the Platform Schema

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

1. Do one of the following:

a. NEW Connect as a privileged user (such as system) and grant the following select permissions to the Platform user-schema owner:

```
grant select on <ADVISORS AGA METRICS SCHEMA>.QUEUE_SET1_REAL_TIME to <ADVISORS
PLATFORM USER> WITH GRANT OPTION;
grant select on <ADVISORS AGA METRICS SCHEMA>.QUEUE_SET2_REAL_TIME to <ADVISORS
PLATFORM USER> WITH GRANT OPTION;
grant select on <ADVISORS AGA METRICS SCHEMA>.SKILL_GROUP_REAL_TIME to <ADVISORS
PLATFORM USER> WITH GRANT OPTION;
grant select on <ADVISORS AGA METRICS SCHEMA>.SERVICE_REAL_TIME to <ADVISORS PLATFORM
USER> WITH GRANT OPTION;
grant select on <ADVISORS AGA METRICS SCHEMA>.SERVICE_MEMBER to <ADVISORS PLATFORM
USER> WITH GRANT OPTION;
grant select on <ADVISORS AGA METRICS SCHEMA>.PERIPHERAL_REAL_TIME to <ADVISORS
PLATFORM USER> WITH GRANT OPTION;
grant select on <ADVISORS AGA METRICS SCHEMA>.INTERACTION_QUEUE_REAL_TIME to
<ADVISORS PLATFORM USER> WITH GRANT OPTION;
grant select on <ADVISORS AGA METRICS SCHEMA>.CONTROLLER_TIME to <ADVISORS PLATFORM
USER> WITH GRANT OPTION;
grant select on <ADVISORS AGA METRICS SCHEMA>.CALL_TYPE_REAL_TIME to <ADVISORS
PLATFORM USER> WITH GRANT OPTION;
grant select on <ADVISORS AGA METRICS SCHEMA>.AGENT_SKILL_GROUP_REAL_TIME to
<ADVISORS PLATFORM USER> WITH GRANT OPTION;
```

b. Connect to the AGA metrics schema as its owner and execute the following statements:

```
grant select on AGENT_SKILL_GROUP_REAL_TIME to <ADVISORS PLATFORM USER> WITH GRANT
OPTION;
grant select on CALL_TYPE_REAL_TIME to <ADVISORS PLATFORM USER> WITH GRANT OPTION;
grant select on CONTROLLER_TIME to <ADVISORS PLATFORM USER> WITH GRANT OPTION;
grant select on INTERACTION_QUEUE_REAL_TIME to <ADVISORS PLATFORM USER> WITH GRANT
OPTION;
grant select on PERIPHERAL_REAL_TIME to <ADVISORS PLATFORM USER> WITH GRANT OPTION;
grant select on QUEUE_SET1_REAL_TIME to <ADVISORS PLATFORM USER> WITH GRANT OPTION;
grant select on QUEUE_SET2_REAL_TIME to <ADVISORS PLATFORM USER> WITH GRANT OPTION;
grant select on SERVICE_MEMBER to <ADVISORS PLATFORM USER> WITH GRANT OPTION;
```

```
grant select on SERVICE_REAL_TIME to <ADVISORS PLATFORM USER> WITH GRANT OPTION;
grant select on SKILL_GROUP_REAL_TIME to <ADVISORS PLATFORM USER> WITH GRANT OPTION;
```

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

```
SELECT * FROM <aga metrics schema>.AGENT_SKILL_GROUP_REAL_TIME;
SELECT * FROM <aga metrics schema>.CALL_TYPE_REAL_TIME;
SELECT * FROM <aga metrics schema>.CONTROLLER_TIME;
SELECT * FROM <aga metrics schema>.INTERACTION_QUEUE_REAL_TIME;
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_MEMBER;
SELECT * FROM <aga metrics schema>.SERVICE_REAL_TIME;
SELECT * FROM <aga metrics schema>.SKILL_GROUP_REAL_TIME;
```

Configure a Connection 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.gcmdb81 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.gcmdb81;
```

Configure a Connection 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 the following 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 'dg4msql2';
```

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.

Least Privileges: How to Configure Advisors Database Accounts with Minimal Privileges

In the general Advisors installation scenario with Oracle, the Oracle schema owners are also used by Advisors components to access the database during runtime.

Starting with Advisors release 8.5.202, access to an Oracle database 12c R2 can be configured in such a way that the Advisors components access the database through low-privileged, runtime users that are not schema owners. The runtime users are granted only DML privileges and the privileges to execute a selected list of stored procedures that operate only within the Advisors database environment.

Advisors installations with MS SQL Server could be configured to access the database through low-privileged runtime users in previous releases. In release 8.5.2, a dedicated security procedure has been added to help further restrict the privileges and allow access only to a minimum set of necessary stored procedures and functions, rather than access to all.

There can be different acceptable scenarios for configuring database accounts with reduced privileges to achieve the same goal. However, this page contains only recommended scenarios that were tested and have passed the evaluation.

This page describes how to configure users with least privileges, which can be used by Advisors components during runtime. You must set up the runtime users before you run the Advisors installation wizards.

The procedures on this page are divided by RDBMS type:

- Microsoft SQL Server
- Oracle

Microsoft SQL Server

This section includes information about the Advisors database users, and the privileges associated with each, for the following setup and installation tasks:

- Creating the Advisors Databases
- Creating the Database Objects
- Creating the Runtime User
- Running the Bulk Configuration Tool
- Running the Advisors Installation Wizards

Creating the Advisors Databases

You require one privileged database user. That user sets up all three Advisors databases. The privileged user requires privileges to create a database, create a login account, create a user, and to back up the database.

Creating Database Objects

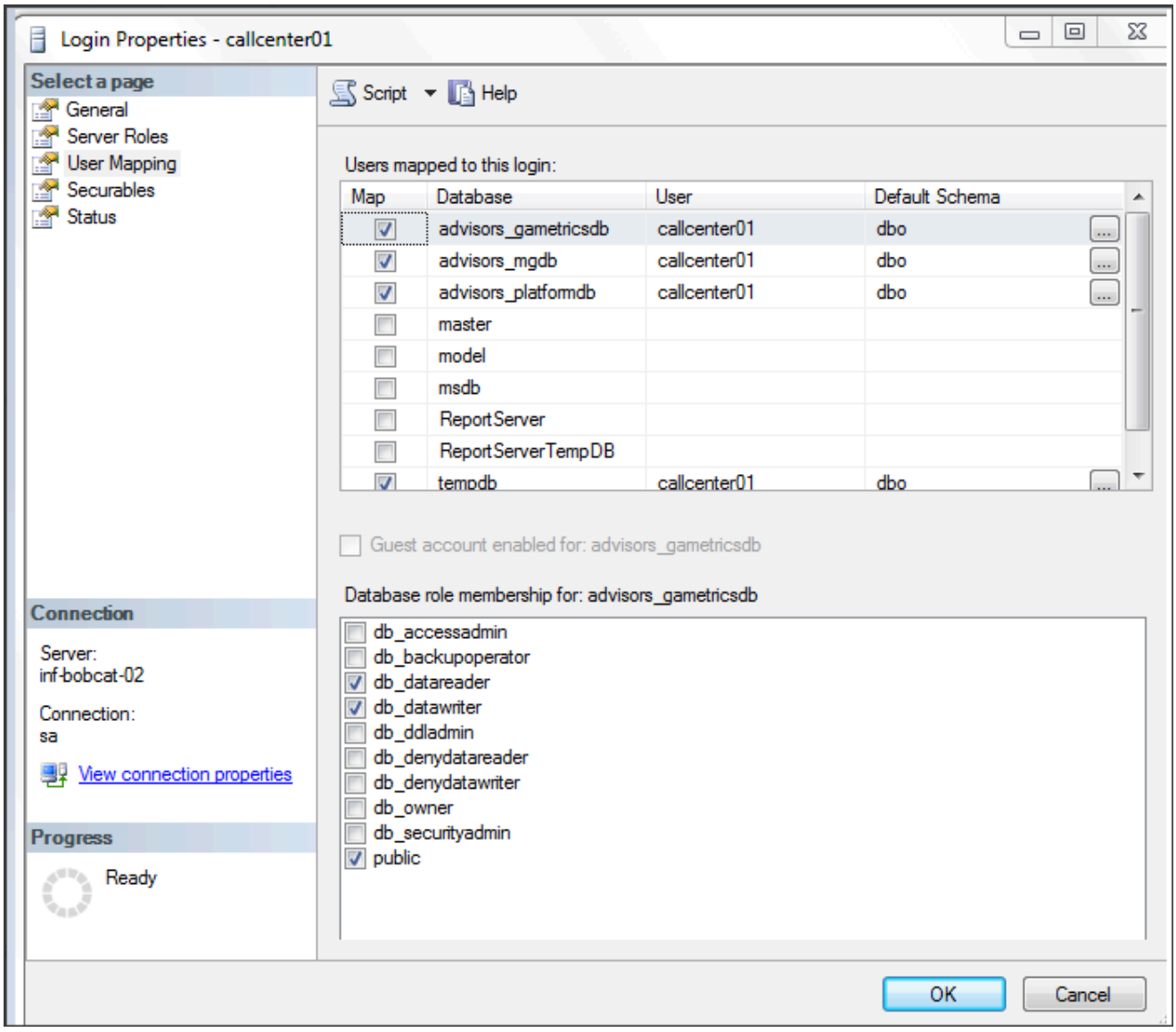
The database owner (db owner) of all three Advisors databases creates the database objects in each database. The db owner executes the "new-database" SQL scripts, which are provided in the Advisors Installation Package (IP) for each database:

- Advisors Genesys Adapter (AGA) metrics database creation script is located in the Advisors Genesys Adapter IP.
- Advisors Platform database creation script is located in the Advisors Platform IP.
- Advisors metric graphing database creation script is located in the Advisors Platform IP starting with Advisors release 8.5.202, and in the Contact Center Advisor/Workforce Advisor IP in earlier releases.

Creating the Runtime User

You must make the low-privileged user, to be used during Advisors application runtime, a member of the [db_datareader] and [db_datawriter] roles in each of the three Advisors databases. The low-privileged user account must have a default schema that holds all objects within each database.

For example, let's say that three databases are created by the "sa" user during the database creation stage. The "sa" user creates a "callcenter01" user login account, which is mapped to each of the three databases and is assigned a default schema, "dbo".



Once the user is added, the db owner must execute the spGrantExecute procedure, located in each of the three Advisors databases. The spGrantExecute procedure has the same name in each database, but has different content depending on the database that holds it. For example:

- AGA metrics database:

```
USE [advisors_gametricsdb]
 GO

 EXEC [dbo].[spGrantExecute]
 @UserName = N'callcenter01'

 GO
```

- Advisors metric graphing database:

```
USE [advisors_mgdb]

GO

EXEC [dbo].[spGrantExecute]
@UserName = N'callcenter01'

GO
```

- Advisors Platform database:

```
USE [advisors_platformdb]

GO

EXEC [dbo].[spGrantExecute]
@UserName = N'callcenter01'

GO
```

It is possible to set up a separate "data reader/data writer" user for each database. However, in that case, the Platform user must also be made a data reader in the Advisors metrics database, or, at a minimum, must be granted a `select` permission on all views contained in the AGA metrics database. A corresponding database user name must be provided in the spGrantExecute procedure and in the Advisors installation wizard prompts.

If a CISCO data source is present, the Platform user must be granted permissions as described elsewhere in guide.

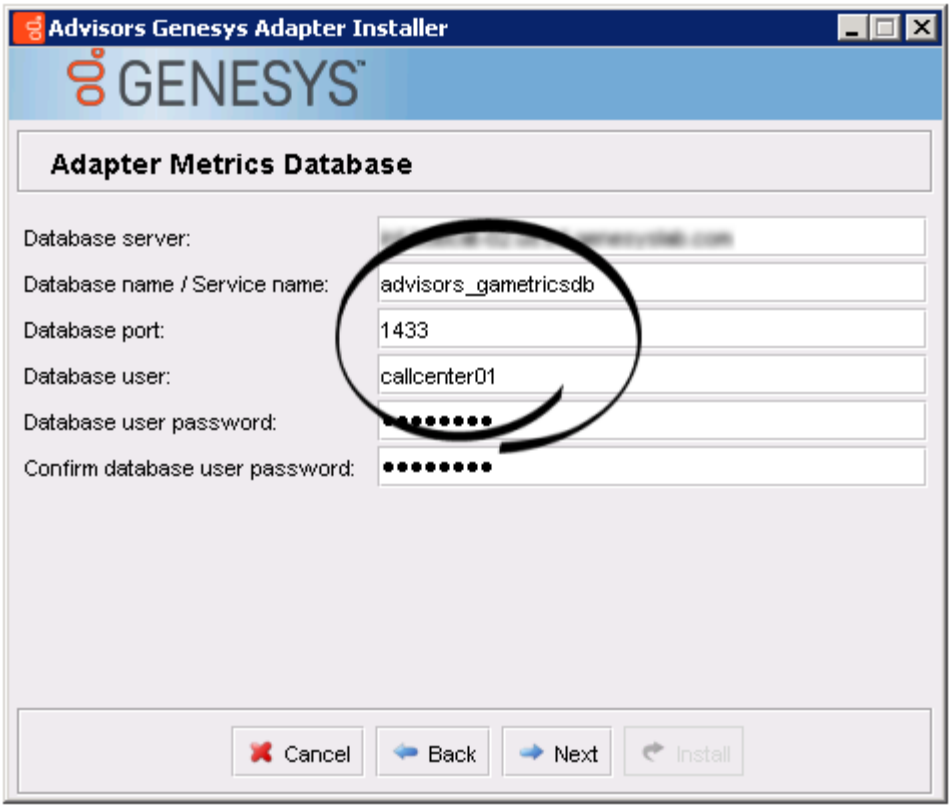
Running the Bulk Configuration Tool

The bulk configuration tool supplied with the Advisors Platform IP is used outside of the applications and is a candidate for a high-privileged user. The spGrantExecute procedure excludes the bulk configuration procedures. Genesys recommends that privileges to execute all procedures with names that start with "spBlk" be temporarily granted to a user when it is necessary to use the bulk configuration tool, and revoked once the Advisors configuration is complete and needs to be frozen. At this point, Genesys also recommends that you back up the Platform database.

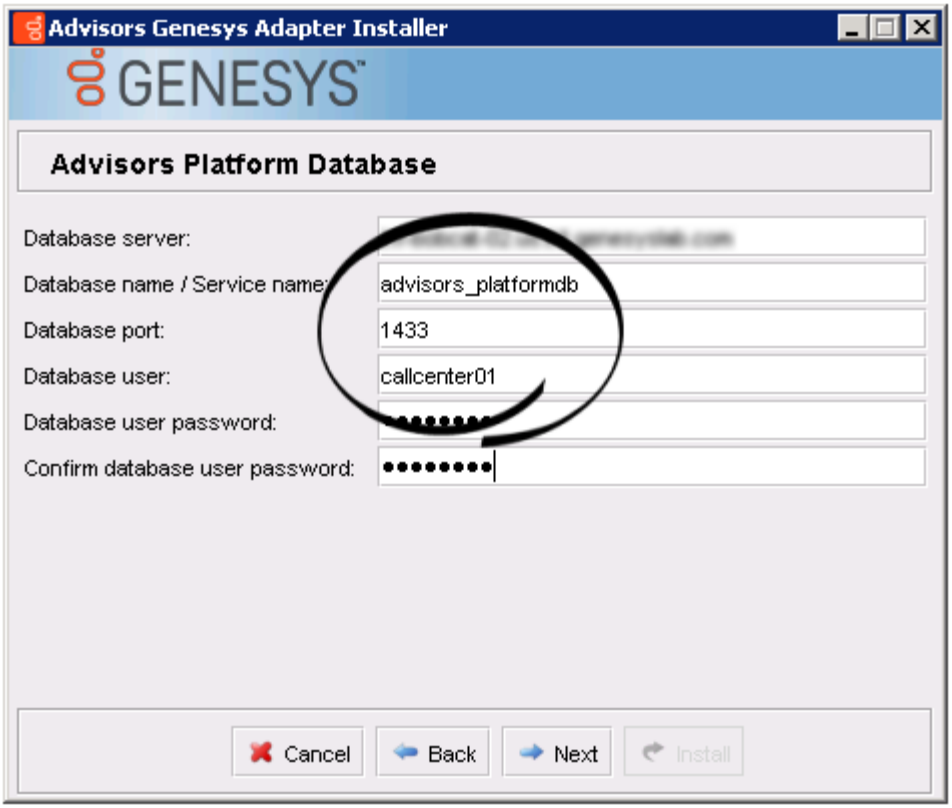
Running the Advisors Installation Wizards

Once the database setup is complete, you can run the Advisors installation wizards. Enter the runtime database user name(s) in the installation wizard prompts for each database. The following examples show the runtime user specified in all of the database user–related fields.

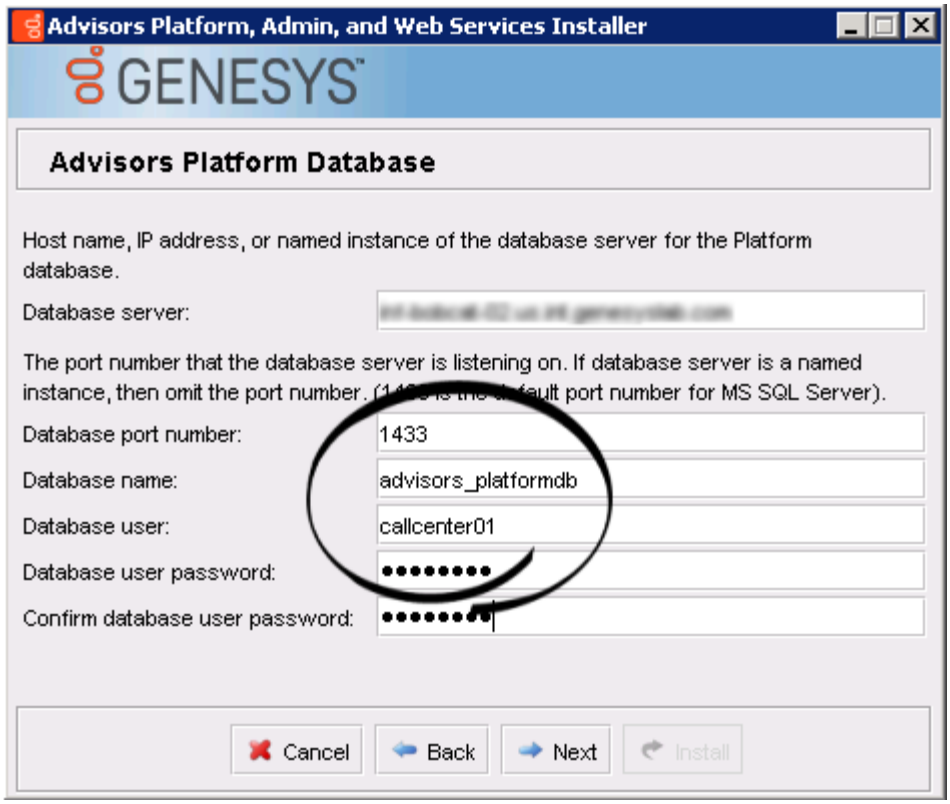
- Advisors Genesys Adapter installation wizard > AGA metrics database



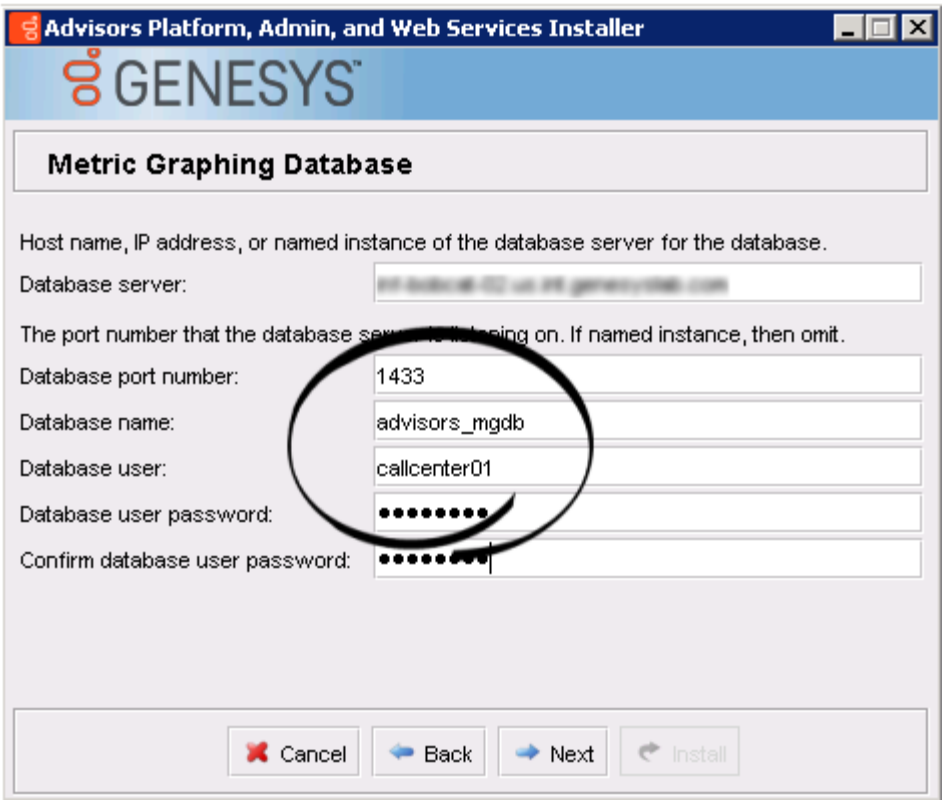
- Advisors Genesys Adapter installation wizard > Platform database



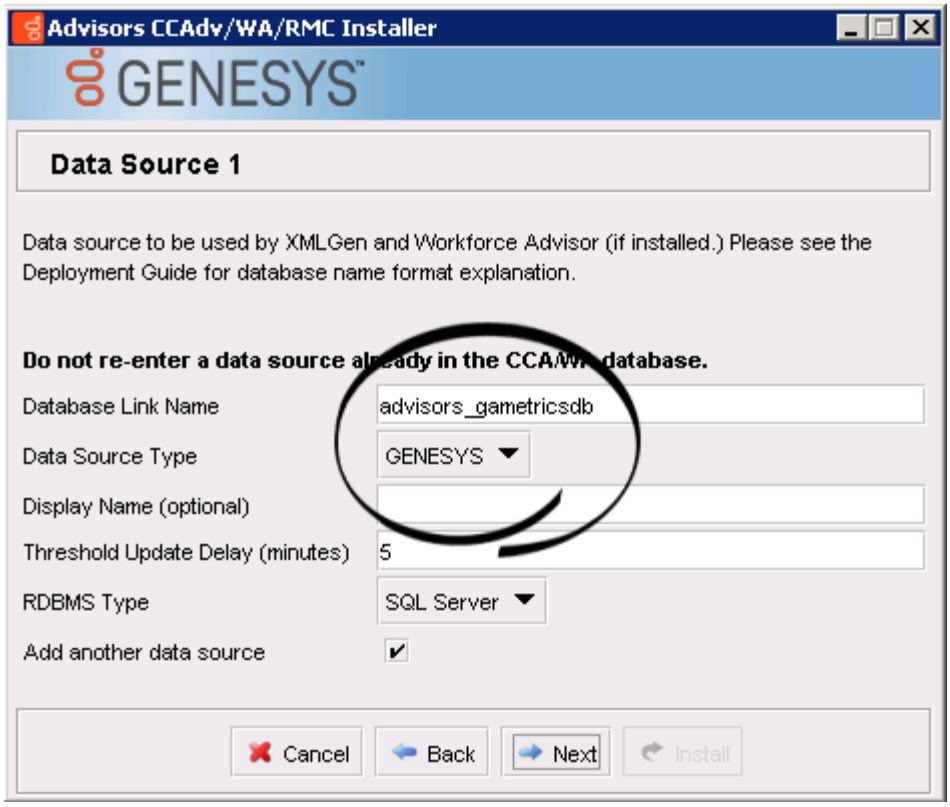
- Platform installation wizard > Platform database



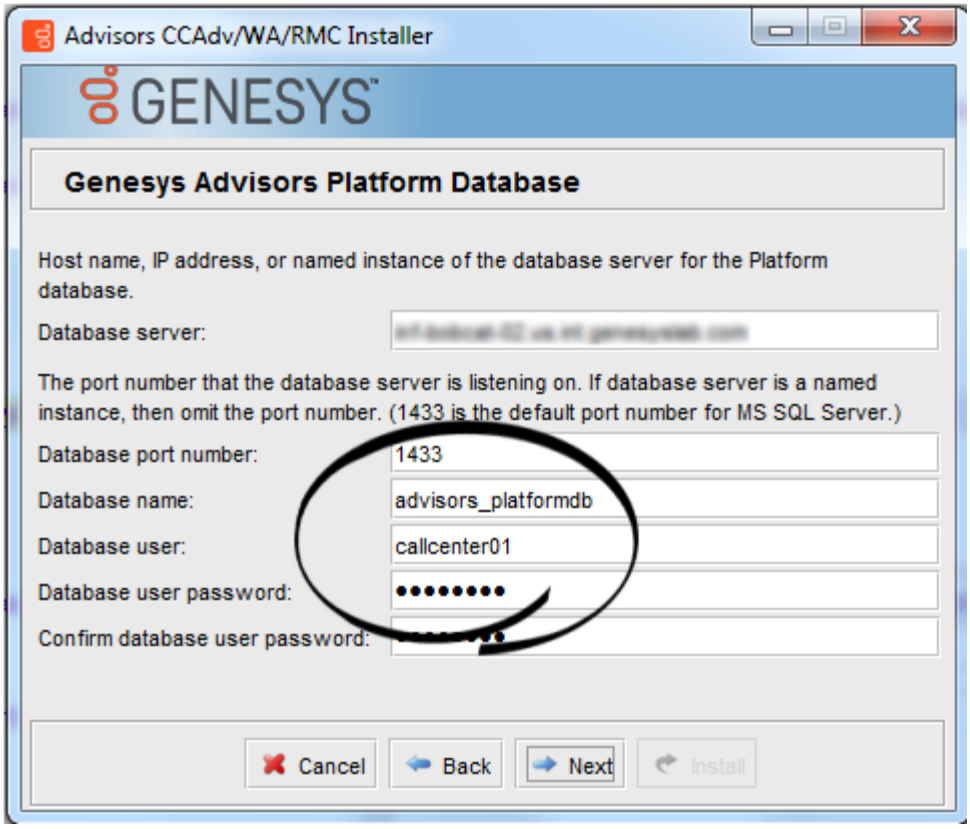
- Platform installation wizard > metric graphing database



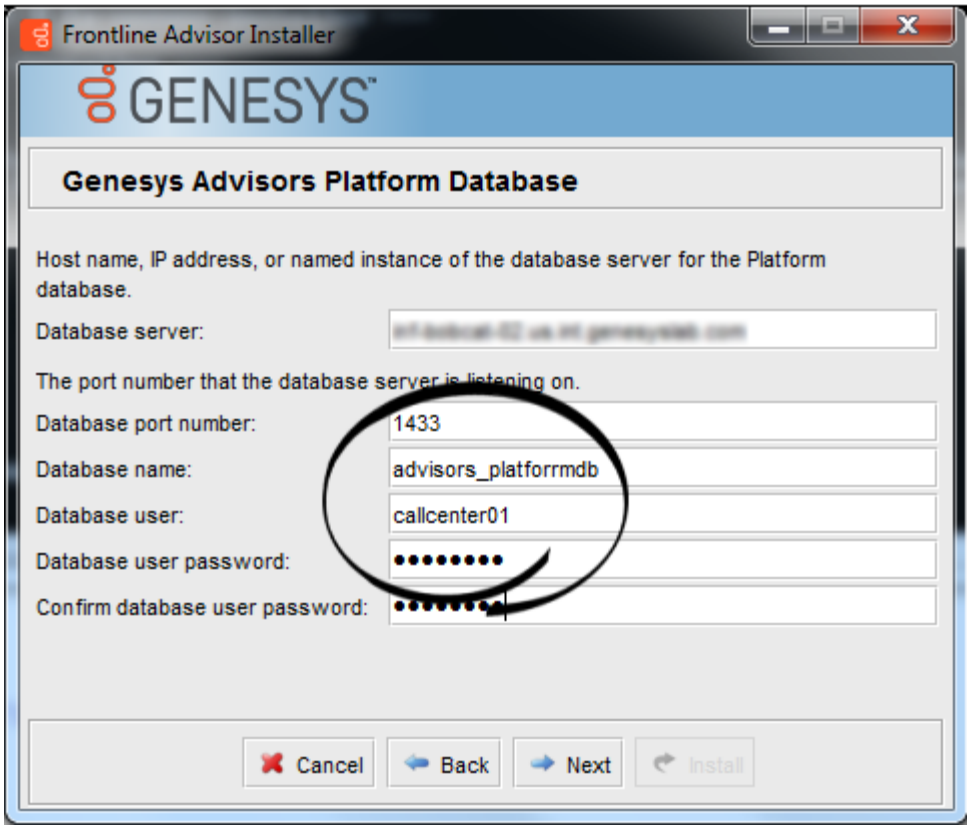
- CCAdv/WA installation wizard > Genesys data source



- CCAdv/WA installation wizard > Platform database



- Frontline Advisor installation wizard > Platform database



Oracle

This section includes the following topics:

- Prerequisites
- Creating the Runtime User
- What to do if something goes wrong
- Running the Advisors Installation Wizards
- Alternative Method to Configure Oracle Runtime Database Access
- Reusing Application and Database Roles

Prerequisites

- Use the Oracle 12c Release 2 RDBMS for your Advisors installation.
- Create three Advisors database users/schemas and the corresponding database objects using the procedures described in the base Oracle Database Installation section of this guide.

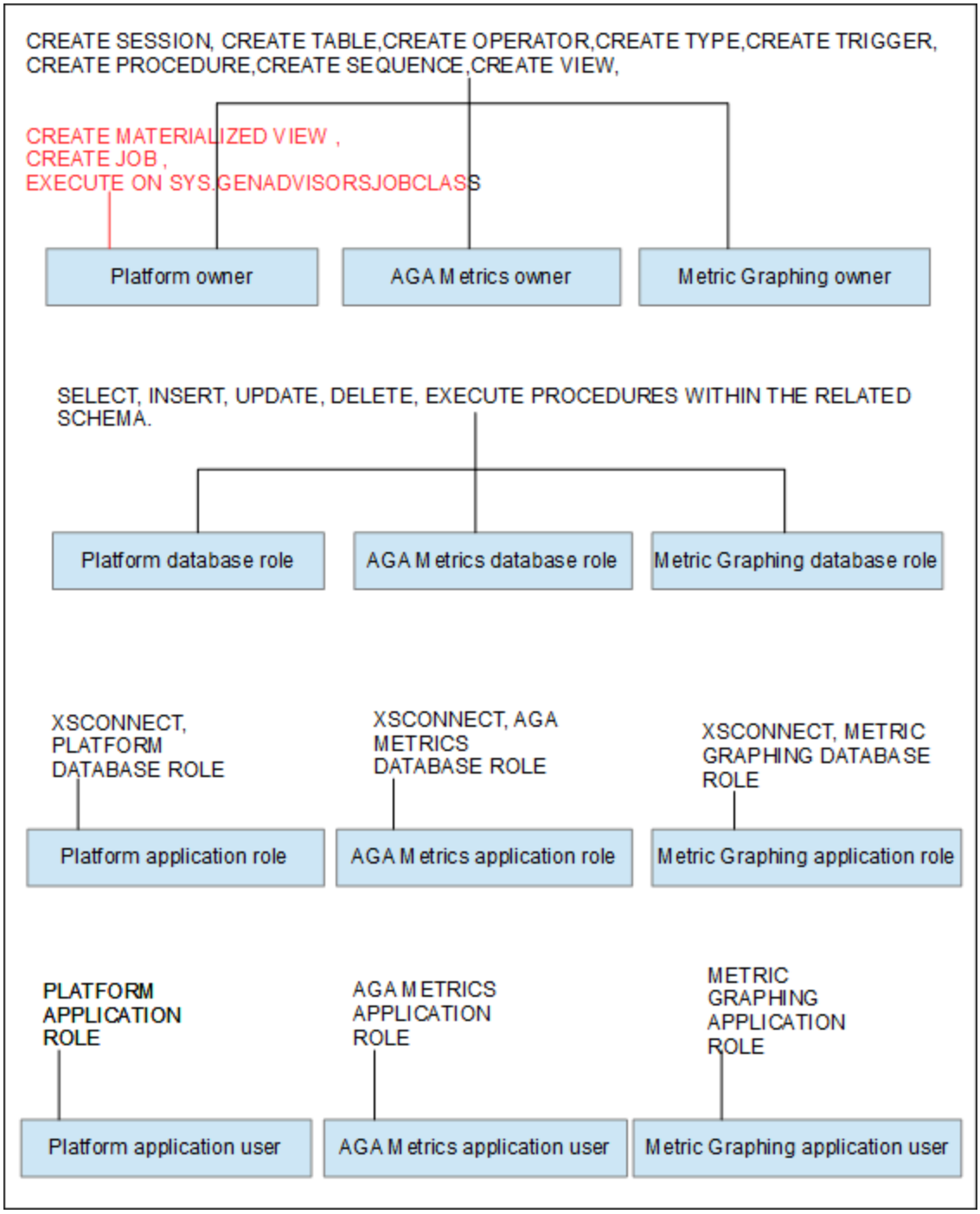
Creating the Runtime User

The solution described on this page is based on the Oracle Database Real Application Security feature and direct-login application users. Application users do not own database schemas by definition, but can create application sessions in the database. Application users can be assigned traditional database schemas owned by other users as their default schemas.

The overall procedure consists of four groups of tasks:

1. Application roles creation and direct-login application users creation with the XS_PRINCIPAL package.
2. Granting roles to direct-login application users with the XS_PRINCIPAL package.
3. Database roles creation and granting a set of restricted object-level privileges to the database roles.
4. Granting database roles to the corresponding application roles.

The following figure is a simplified schema showing the resulting schema owner privileges and the application user privileges.



The Platform schema owner might require an additional privilege if the Advisors application is installed using an Oracle database that does not have the JServer Java Virtual Machine installed.

`EXECUTE ON SYS.DBMS_LOCK` will be required in addition to the three privileges shown in red in the figure above. You must modify the `advisors-platform-<version>_UsersAndRoles.sql` script to accommodate the additional privilege.

Procedure:

Steps

1. Decide what you will use as names for the following entities:

   - The names and passwords for direct-login application users with a restricted set of privileges that Advisors components will use to access the database during runtime.
   - The names for the application roles that will be granted to the direct-login application users.
   - The names for regular database roles that will hold the restricted set of object-level privileges and that will be granted to application roles.

   You will also need to provide the names of schema owners that should have been created already, using the base database creation procedure (these are the Platform, AGA metrics, and Metric Graphing schema owners).

   For this example, we will use the following names:

   - Adv1PltOwner,Adv2AgaOwner,Adv3MgOwner as schema owners.
   - Adv1,Adv2,Adv3 as direct-login application users that will become Advisors runtime users.
   - AdvPlt_approle,AdvAga_approle,AdvMg_approle as application roles.
   - AdvPlt_dbrole,AdvAga_dbrole,AdvMg_dbrole as regular database roles.

2. Connect to SQL*Plus as a privileged user (such as "system") who has access to all three Advisors schemas. Execute the `advisors-platform-<version>_UsersAndRoles.sql` script, providing the names and passwords when prompted:

```
Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production

SQL> @advisors-platform-8.5.202.09_UsersAndRoles.sql
Platform schema owner: Adv1PltOwner
AGA Metrics schema owner: Adv2AgaOwner
MG Metrics schema owner: Adv3MgOwner
Platform runtime user name:  Adv1
AGA Metrics runtime user name:  Adv2
MG runtime user name:  Adv3
Platform application role: AdvPlt_approle
AGA Metrics application role: AdvAga_approle
MG application role: AdvMg_approle
Platform database role: AdvPlt_dbrole
AGA Metrics database role: AdvAga_dbrole
MG database role: AdvMg_dbrole
Enter value for platform_runtime_password: password1
Enter value for aga_runtime_password: password2
Enter value for mg_runtime_password: password3
```

   If you prefer, instead of executing the `advisors-platform-<version>_UsersAndRoles.sql` SQL*Plus script, you can use the Alternative Method to Configure Oracle Runtime Database Access procedure, described below. Using the alternative method, you execute the same commands that are provided in the SQL* Plus script, but in a more controlled way.

3. Once the setup is complete, use the following query to verify the direct-login application users (runtime users) that you have created:

```
SELECT * FROM DBA_XS_USERS;
```

The Name column contains the names of the direct-login application users that you created. The Schema column contains the default schema of the corresponding direct-login application user.

The user name must match the name that you planned for your runtime user. The default schema for the application user must be the name of the Platform, AGA metrics, or Metric Graphing schema that you added during the initial database creation. This will ensure that all of the database objects that the application accesses during runtime through the direct-login application user account will be pulled from the correct schema (Platform, AGA metrics, or Metric Graphing schema), while access control during runtime is restricted to the privileges assigned to the application user.

Considering the sample names used in this procedure, you should see results that are similar to the following:

NAME	SCHEMA
ADV1	ADV1PLTOWNER
ADV1	ADV1AGAOWNER
ADV1	ADV1MGOWNER

4. Verify your "direct login application user - application role" and "application role - db role" mappings using the following query:

   ```
   SELECT GRANTEE, GRANTED_ROLE FROM DBA_XS_ROLE_GRANTS ORDER BY GRANTEE;
   ```

   The application roles must be granted to the corresponding direct-login application users, while the DB roles are granted to the corresponding application roles. Considering the sample names used in this procedure, you should see results that are similar to the following:

GRANTEE	GRANTED_ROLE
ADV1	XSPUBLIC
ADV1	XSCONNECT
ADV1	ADVPLT_APPROLE
ADVPLT_APPROLE	ADVPLT_DBROLE
ADV2	XSPUBLIC
ADV2	XSCONNECT
ADV2	ADVAGA_APPROLE
ADVAGA_APPROLE	ADVAGA_DBROLE
ADV3	XSPUBLIC
ADV3	XSCONNECT
ADV3	ADVPLT_APPROLE
ADV3	ADVMG_APPROLE
ADVMG_APPROLE	ADVMG_DBROLE

What to do if something goes wrong

If it looks like something went wrong during your attempt to add the application users and the application and database roles, then you can remove those users and roles as shown in the samples below. For consistency, the following examples use the same names that were used in the preceding procedure. Removing application users and the application and database roles does not impact the initial database installation or the schema owner permissions.

Sample: Removing application users and application and database roles

```
EXEC SYS.XS_PRINCIPAL.DELETE_PRINCIPAL ('Adv1',xs_admin_util.cascade_option);
EXEC SYS.XS_PRINCIPAL.DELETE_PRINCIPAL ('Adv2',xs_admin_util.cascade_option);
EXEC SYS.XS_PRINCIPAL.DELETE_PRINCIPAL ('Adv3',xs_admin_util.cascade_option);
```

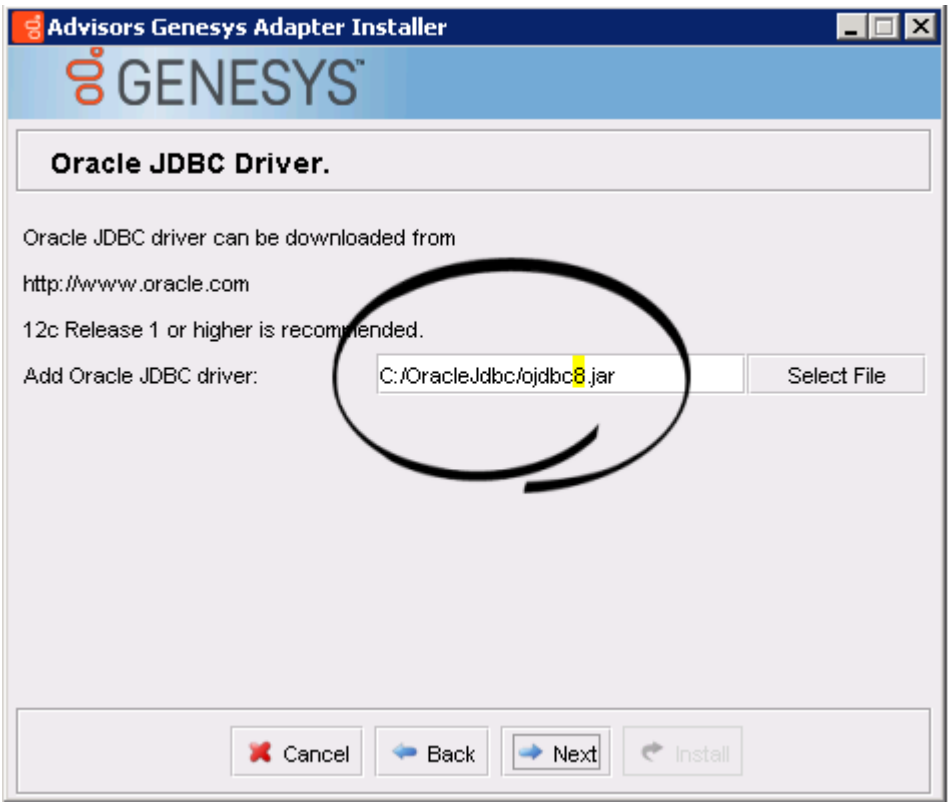
```
EXEC SYS.XS_PRINCIPAL.DELETE_PRINCIPAL('AdvPlt_role');
EXEC SYS.XS_PRINCIPAL.DELETE_PRINCIPAL('AdvAga_role');
EXEC SYS.XS_PRINCIPAL.DELETE_PRINCIPAL('AdvMg_role');

DROP ROLE AdvPlt_dbrole;
DROP ROLE AdvAga_dbrole;
DROP ROLE AdvMg_dbrole;
```

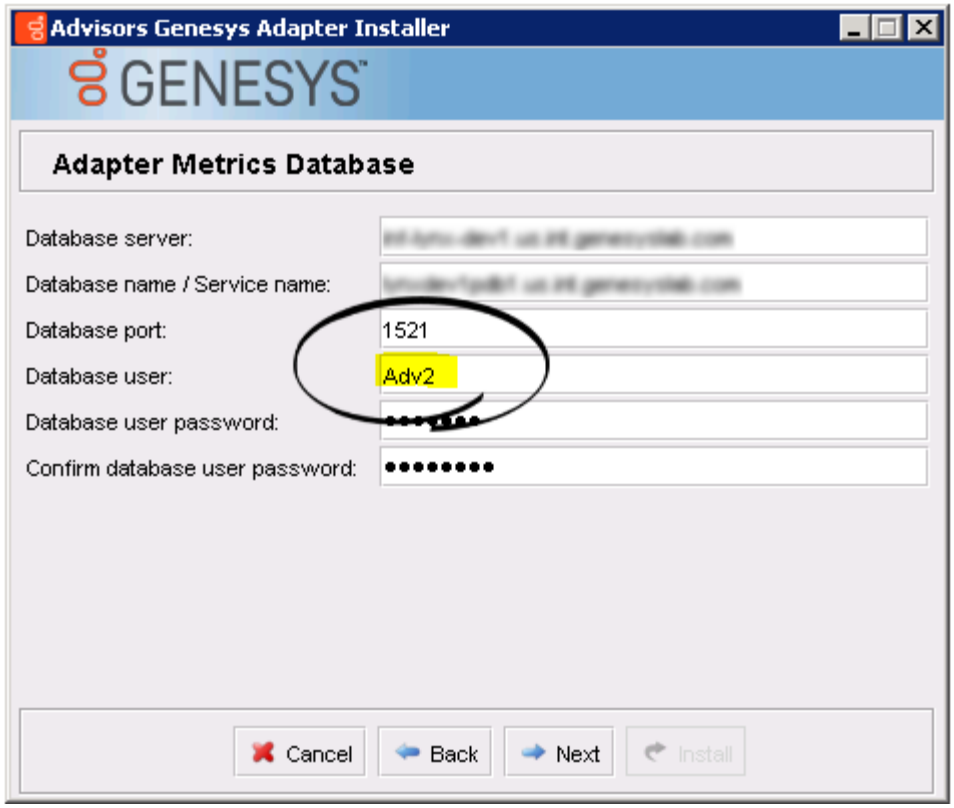
Running the Advisors Installation Wizards

Once the database setup is complete, you can run the Advisors installation wizards. Enter the runtime database user name(s) in the installation wizard prompts for each database. The following examples show the runtime user specified in all of the database user–related fields.

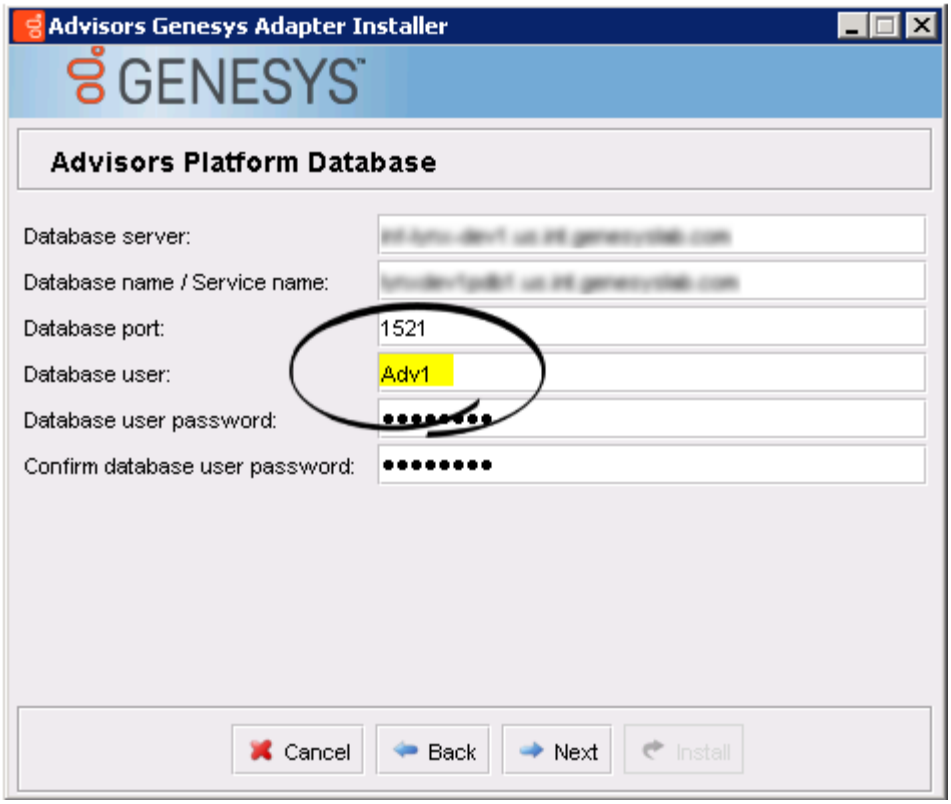
- Advisors Genesys Adapter installation wizard. Make sure you specify `ojdbc8.jar` as the Oracle JDBC driver.



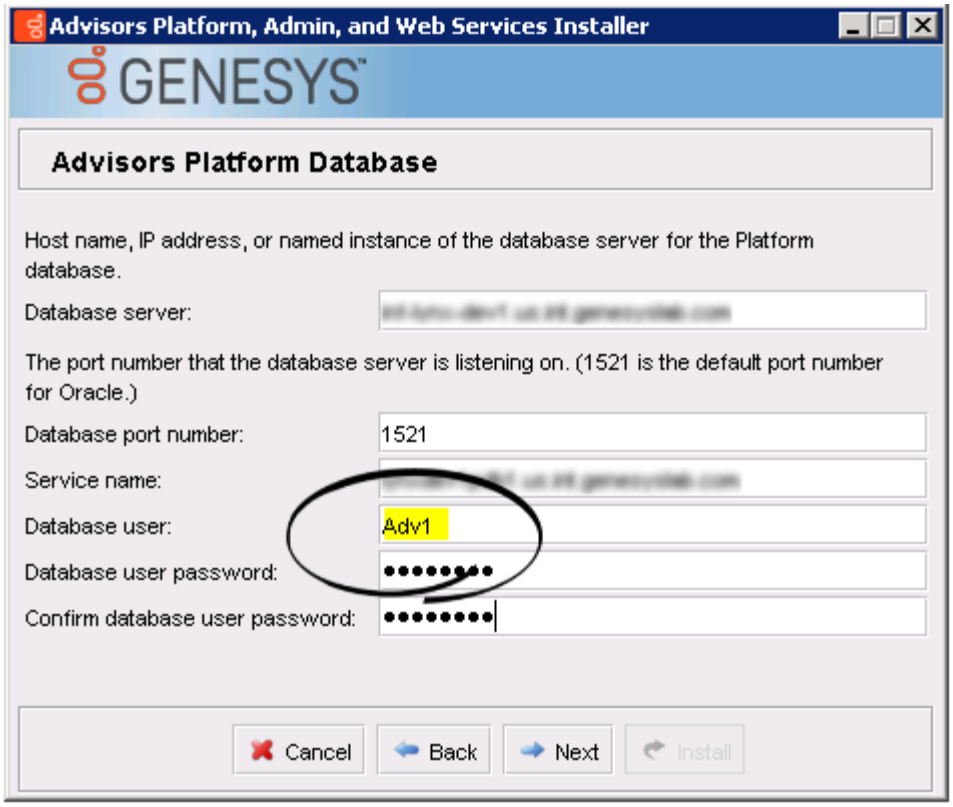
- Advisors Genesys Adapter installation wizard. The AGA runtime user is specified in the **Database user** field.



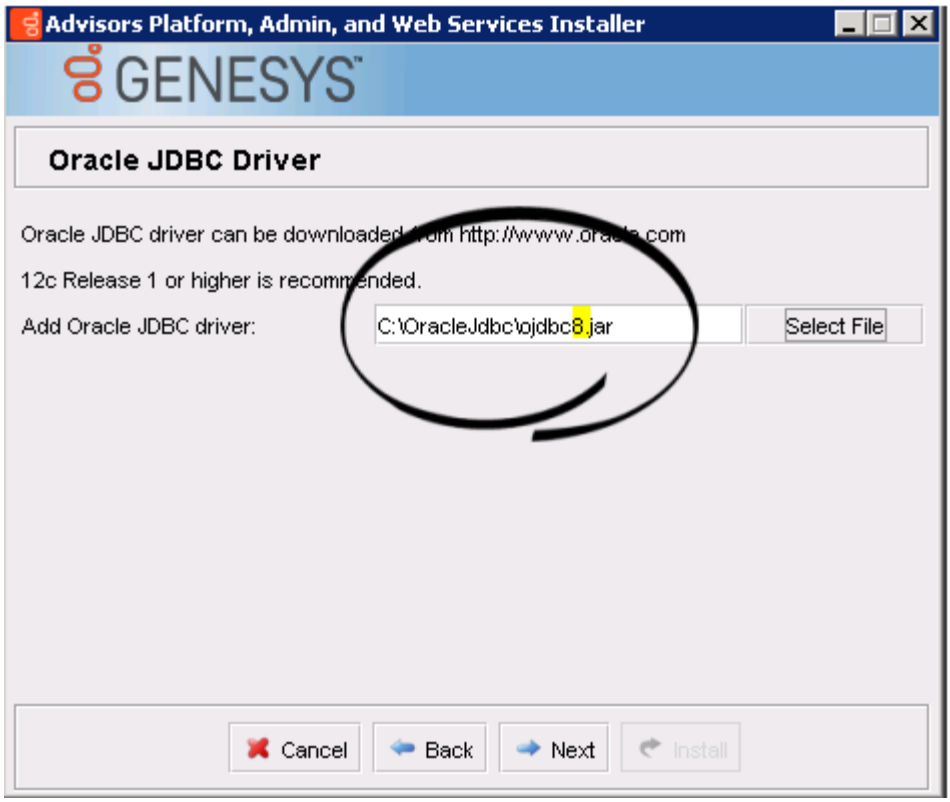
- Advisors Genesys Adapter installation wizard. The Platform runtime user is specified in the **Database user** field.



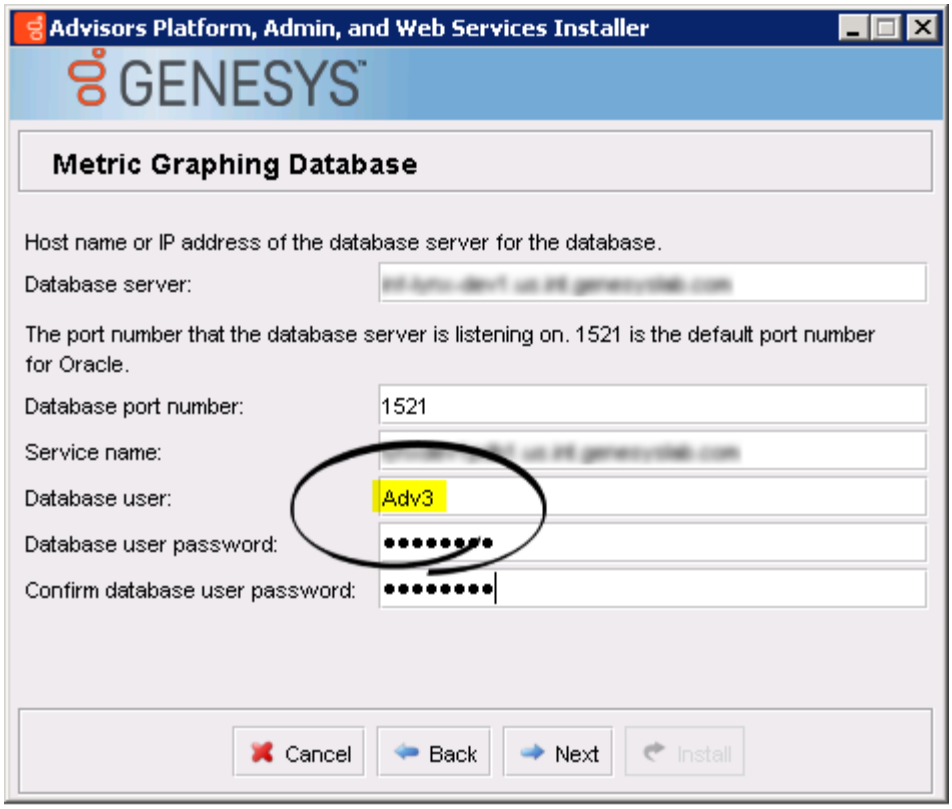
- Platform installation wizard. The Platform runtime user is specified in the **Database user** field.



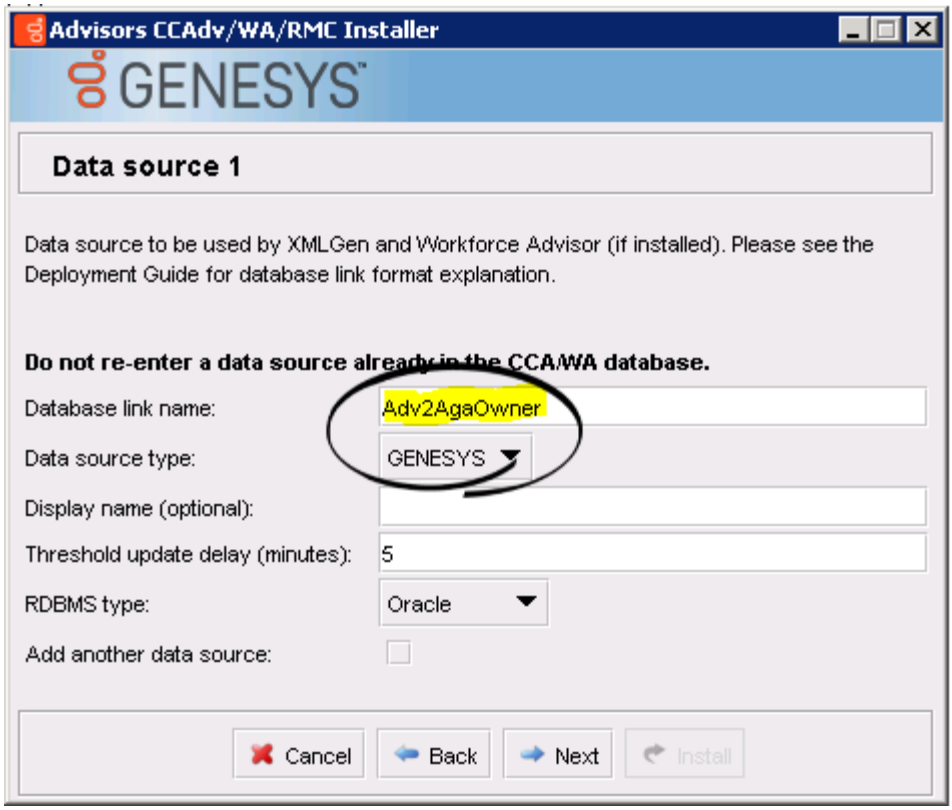
- Platform installation wizard. Make sure you specify `ojdbc8.jar` as the Oracle JDBC driver.



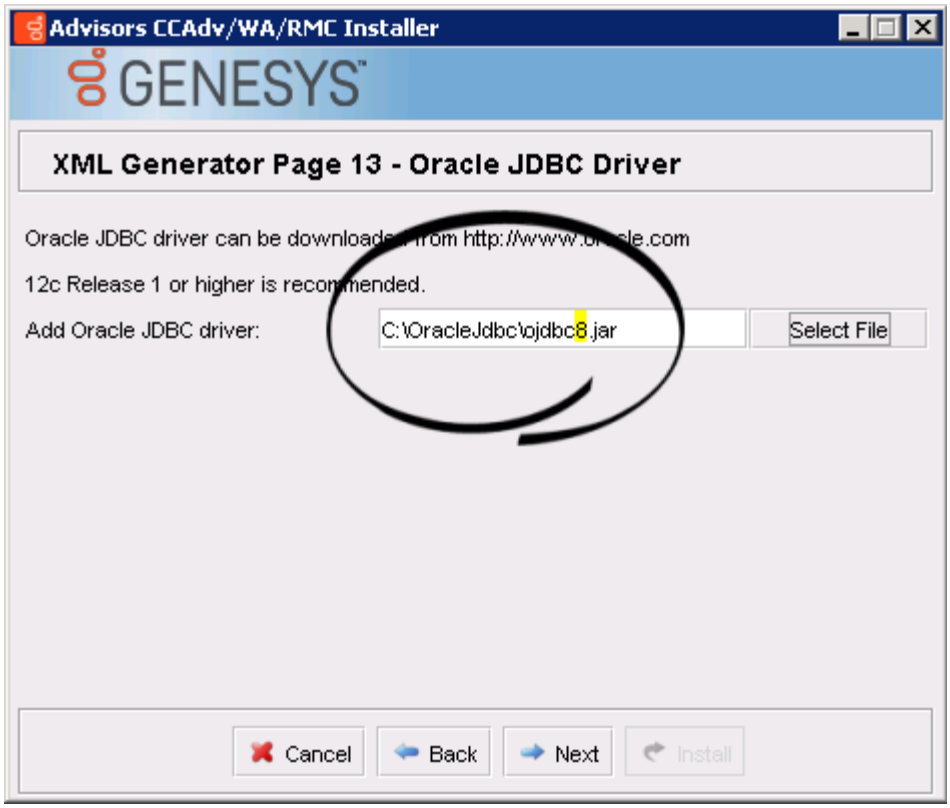
- Platform installation wizard. The metric graphing runtime user is specified in the **Database user** field.



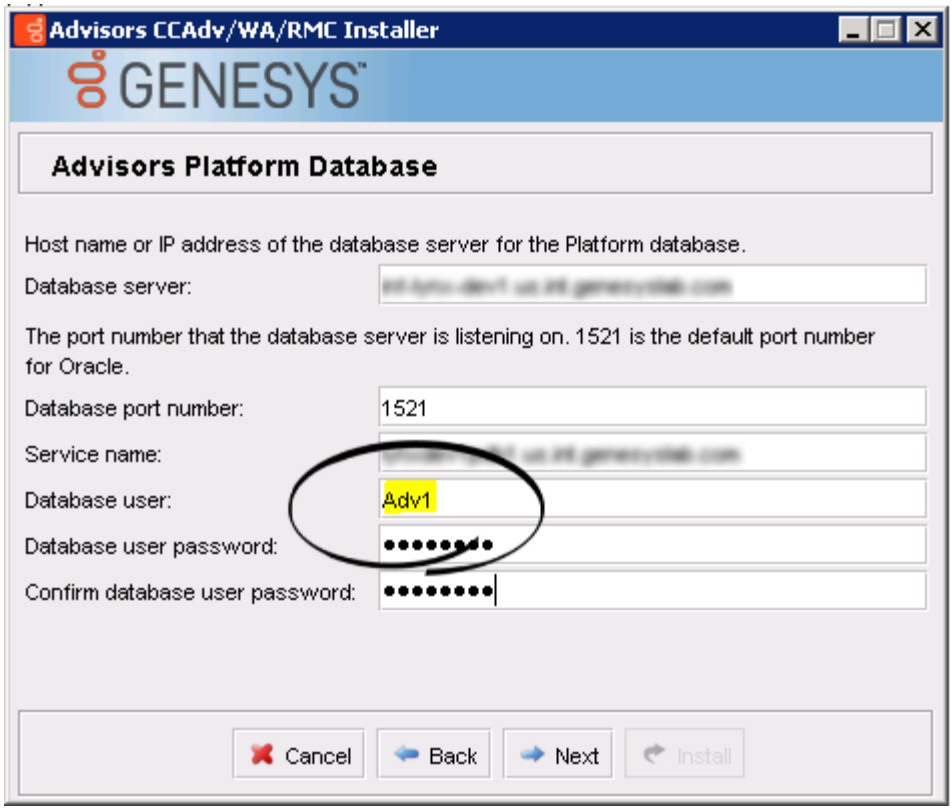
- CCAdv/WA/RMC installation wizard. The AGA schema owner is specified in the **Database link name** field.



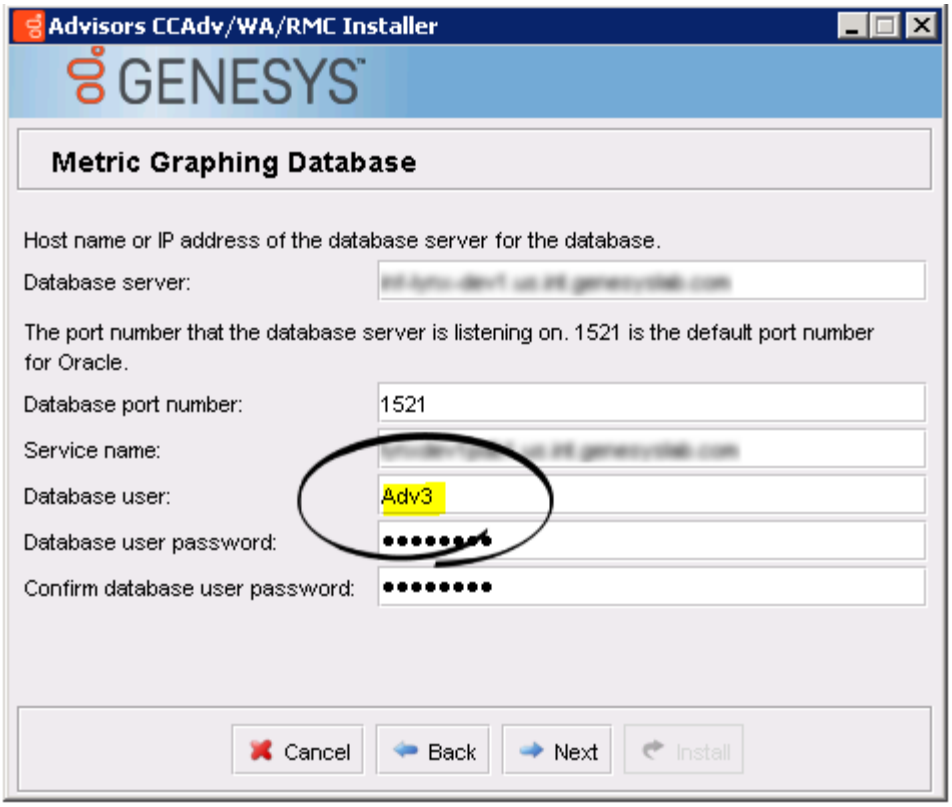
- CCAdv/WA/RMC installation wizard. Make sure you specify `ojdbc8.jar` as the Oracle JDBC driver.



- CCAdv/WA/RMC installation wizard. The Platform runtime user is specified in the **Database user** field.



- CCAdv/WA/RMC installation wizard. The metric graphing runtime user is specified in the **Database user** field.



Alternative Method to Configure Oracle Runtime Database Access

If you prefer to use a more controlled security setup, then instead of executing the SQL*Plus `advisors-platform-<version>_UsersAndRoles.sql` script as described in the procedure above, you can run the script in sections.

1. Connect to Oracle SQL Developer as a privileged user (such as system) who has access to all three Advisors schemas.
2. Copy the entire contents of the script section below and paste it into the Oracle SQL Developer query window. Highlight Section 1 and execute. Answer all 12 prompts. This will provide the substitutions for all variables contained in the next sections of the script, which you will execute later.
   If you make a mistake with the substitute variables, repeat Section 1.

   The scripts from all sections must be executed within the same session; that is, all queries must be run from the same SQL Developer window. The only exception is the object permission script that is generated in Section 3, which can be executed from any session, including your current session.
3. Once you are satisfied with the substitution, execute all of Section 2. Provide passwords, where prompted.
4. Highlight Section 3, and execute. This will generate Section 4.
5. Copy the results that were generated after you executed the Section 3 queries (that is, Section 4), and execute those as a privileged user (such as system).
6. Execute Section 5.

```
--1

SET HEADING OFF
SET LINE 512
SET FEEDBACK OFF
Accept PLATFORM_USERNAME char Prompt 'Platform schema owner: '
Accept AGA_USERNAME char Prompt 'AGA Metrics schema owner: '
Accept MG_USERNAME char Prompt 'MG Metrics schema owner: '
Accept PLATFORM_RUNTIME_USERNAME char Prompt 'Platform runtime user name: '
Accept AGA_RUNTIME_USERNAME char Prompt 'AGA Metrics runtime user name: '
Accept MG_RUNTIME_USERNAME char Prompt 'MG runtime user name: '
Accept PLATFORM_APPLICATION_ROLE char Prompt 'Platform application role: '
Accept AGA_APPLICATION_ROLE char Prompt 'AGA Metrics application role: '
Accept MG_APPLICATION_ROLE char Prompt 'MG application role: '
Accept PLATFORM_DATABASE_ROLE char Prompt 'Platform database role: '
Accept AGA_DATABASE_ROLE char Prompt 'AGA Metrics database role: '
Accept MG_DATABASE_ROLE char Prompt 'MG database role: '

--2

SET VERIFY OFF;
EXEC SYS.XS_PRINCIPAL.CREATE_USER (name => '&&PLATFORM_RUNTIME_USERNAME', schema => '&&PLATFORM_USERNAME');
EXEC SYS.XS_PRINCIPAL.CREATE_USER (name => '&&AGA_RUNTIME_USERNAME', schema => '&&AGA_USERNAME');
EXEC SYS.XS_PRINCIPAL.CREATE_USER (name => '&&MG_RUNTIME_USERNAME', schema => '&&MG_USERNAME');

EXEC SYS.XS_PRINCIPAL.SET_PASSWORD('&&PLATFORM_RUNTIME_USERNAME', '&&PLATFORM_RUNTIME_password');
EXEC SYS.XS_PRINCIPAL.SET_PASSWORD('&&AGA_RUNTIME_USERNAME', '&&AGA_RUNTIME_password');
EXEC SYS.XS_PRINCIPAL.SET_PASSWORD('&&MG_RUNTIME_USERNAME', '&&MG_RUNTIME_password');

EXEC SYS.XS_PRINCIPAL.CREATE_ROLE(NAME => '&&PLATFORM_APPLICATION_ROLE', ENABLED => TRUE);
EXEC SYS.XS_PRINCIPAL.CREATE_ROLE(NAME => '&&AGA_APPLICATION_ROLE', ENABLED => TRUE);
EXEC SYS.XS_PRINCIPAL.CREATE_ROLE(NAME => '&&MG_APPLICATION_ROLE', ENABLED => TRUE);

EXEC SYS.XS_PRINCIPAL.GRANT_ROLES('&&PLATFORM_RUNTIME_USERNAME', 'XSCONNECT');
EXEC SYS.XS_PRINCIPAL.GRANT_ROLES('&&AGA_RUNTIME_USERNAME', 'XSCONNECT');
EXEC SYS.XS_PRINCIPAL.GRANT_ROLES('&&MG_RUNTIME_USERNAME', 'XSCONNECT');

EXEC SYS.XS_PRINCIPAL.GRANT_ROLES('&&PLATFORM_RUNTIME_USERNAME', '&&PLATFORM_APPLICATION_ROLE');
EXEC SYS.XS_PRINCIPAL.GRANT_ROLES('&&AGA_RUNTIME_USERNAME', '&&AGA_APPLICATION_ROLE');
EXEC SYS.XS_PRINCIPAL.GRANT_ROLES('&&MG_RUNTIME_USERNAME', '&&MG_APPLICATION_ROLE');
EXEC SYS.XS_PRINCIPAL.GRANT_ROLES('&&MG_RUNTIME_USERNAME', '&&PLATFORM_APPLICATION_ROLE');
```

```
    CREATE ROLE &&PLATFORM_DATABASE_ROLE;
    CREATE ROLE &&AGA_DATABASE_ROLE;
    CREATE ROLE &&MG_DATABASE_ROLE;

    --3
    --Grant permissions to database objects

    SELECT 'GRANT SELECT, INSERT, UPDATE, DELETE ON '||OWNER||'.'||TABLE_NAME||' TO &&AGA_DATABASE_ROLE;' FROM DBA_TABLES WHERE
OWNER=UPPER('&&AGA_USERNAME')
    UNION
    SELECT 'GRANT SELECT, INSERT, UPDATE, DELETE ON '||OWNER||'.'||VIEW_NAME||' TO &&AGA_DATABASE_ROLE;' FROM DBA_VIEWS WHERE
OWNER=UPPER('&&AGA_USERNAME')
    UNION
    SELECT 'GRANT SELECT ON '||OWNER||'.'||VIEW_NAME||' TO &&PLATFORM_USERNAME;' FROM DBA_VIEWS WHERE OWNER=UPPER('&&AGA_USERNAME')
    UNION
    SELECT 'GRANT SELECT ON '||OWNER||'."'||VIEW_NAME||'" TO &&PLATFORM_USERNAME WITH GRANT OPTION;' FROM DBA_VIEWS WHERE
OWNER='&&AGA_USERNAME'
    UNION
    SELECT 'GRANT EXECUTE ON '||OWNER||'.'||OBJECT_NAME||' TO &&AGA_DATABASE_ROLE;' FROM DBA_PROCEDURES WHERE
OWNER=UPPER('&&AGA_USERNAME') AND OBJECT_TYPE<>'PACKAGE' AND OBJECT_TYPE<>'TYPE' AND OBJECT_TYPE<>'TRIGGER'
    UNION
    SELECT 'GRANT SELECT, INSERT, UPDATE, DELETE ON '||OWNER||'.'||TABLE_NAME||' TO &&MG_DATABASE_ROLE;' FROM DBA_TABLES WHERE
OWNER=UPPER('&&MG_USERNAME')
    UNION
    SELECT 'GRANT SELECT, INSERT, UPDATE, DELETE ON '||OWNER||'.'||VIEW_NAME||' TO &&MG_DATABASE_ROLE;' FROM DBA_VIEWS WHERE
OWNER=UPPER('&&MG_USERNAME')
    UNION
    SELECT 'GRANT EXECUTE ON '||OWNER||'.'||OBJECT_NAME||' TO &&MG_DATABASE_ROLE;' FROM DBA_PROCEDURES WHERE OWNER=UPPER('&&MG_USERNAME')
AND OBJECT_TYPE<>'PACKAGE' AND OBJECT_TYPE<>'TYPE' AND OBJECT_TYPE<>'TRIGGER'
    UNION
    SELECT 'GRANT SELECT ON '||OWNER||'.'||OBJECT_NAME||' TO &&MG_DATABASE_ROLE;' FROM DBA_OBJECTS WHERE OWNER=UPPER('&&MG_USERNAME') AND
OBJECT_TYPE='SEQUENCE'
    UNION
    SELECT 'GRANT SELECT, INSERT, UPDATE, DELETE ON '||OWNER||'."'||TABLE_NAME||'" TO &&PLATFORM_DATABASE_ROLE;' FROM DBA_TABLES WHERE
OWNER=UPPER('&&PLATFORM_USERNAME')
    UNION
    SELECT 'GRANT SELECT, INSERT, UPDATE, DELETE ON '||OWNER||'.'||VIEW_NAME||' TO &&PLATFORM_DATABASE_ROLE;' FROM DBA_VIEWS WHERE
OWNER=UPPER('&&PLATFORM_USERNAME')
    AND VIEW_NAME NOT IN (SELECT VIEW_NAME FROM DBA_VIEWS WHERE OWNER=UPPER('&&AGA_USERNAME')) AND VIEW_NAME NOT LIKE '%REAL_TIME%' AND
VIEW_NAME NOT LIKE '%LOGICAL_CONTROLLER%' AND VIEW_NAME NOT LIKE '%DS_SERVICE_MEMBER%'
    AND VIEW_NAME NOT LIKE 'AGENT_SKILL_GROUP_REAL_TIME%' AND VIEW_NAME NOT LIKE 'INTERACTION_QUEUE_REAL_TIME%' AND VIEW_NAME NOT LIKE
'SKILL_GROUP%' AND VIEW_NAME NOT LIKE 'CALL_TYPE%'
    AND VIEW_NAME NOT LIKE 'SERVICE%' AND VIEW_NAME NOT LIKE 'INTERACTION_QUEUE%' AND VIEW_NAME NOT LIKE 'PERIPHERAL%' AND VIEW_NAME NOT
```

```
LIKE 'CONTROLLER_TIME%'AND VIEW_NAME NOT LIKE 'QUEUE_SET%'
    UNION
    SELECT 'GRANT SELECT ON '||OWNER||'.'||VIEW_NAME||' TO &&PLATFORM_DATABASE_ROLE;' FROM DBA_VIEWS WHERE
OWNER=UPPER('&&PLATFORM_USERNAME')
    AND (VIEW_NAME IN (SELECT VIEW_NAME FROM DBA_VIEWS WHERE OWNER=UPPER('&&AGA_USERNAME')) OR VIEW_NAME LIKE '%REAL_TIME%' OR VIEW_NAME
LIKE '%LOGICAL_CONTROLLER%' OR VIEW_NAME LIKE '%DS_SERVICE_MEMBER%'
    OR VIEW_NAME LIKE 'AGENT_SKILL_GROUP_REAL_TIME%' OR VIEW_NAME LIKE 'INTERACTION_QUEUE_REAL_TIME%' OR VIEW_NAME LIKE 'SKILL_GROUP%' OR
VIEW_NAME LIKE 'CALL_TYPE%'
    OR VIEW_NAME LIKE 'SERVICE%' OR VIEW_NAME LIKE 'INTERACTION_QUEUE%' OR VIEW_NAME LIKE 'PERIPHERAL%' OR VIEW_NAME LIKE
'CONTROLLER_TIME%'OR VIEW_NAME LIKE 'QUEUE_SET%')
    UNION
    SELECT DISTINCT 'GRANT EXECUTE ON '||OWNER||'.'||OBJECT_NAME||' TO &&PLATFORM_DATABASE_ROLE;' FROM DBA_PROCEDURES WHERE
OWNER=UPPER('&&PLATFORM_USERNAME')AND OBJECT_TYPE='PACKAGE'
    UNION
    SELECT 'GRANT EXECUTE ON '||OWNER||'."'||OBJECT_NAME||'" TO &&PLATFORM_DATABASE_ROLE;' FROM DBA_PROCEDURES WHERE
OWNER=UPPER('&&PLATFORM_USERNAME') AND OBJECT_TYPE<>'PACKAGE' AND OBJECT_TYPE<>'TYPE' AND OBJECT_TYPE<>'TRIGGER'
    AND UPPER(OBJECT_NAME) NOT LIKE 'SPBLK%'
    UNION
    SELECT 'GRANT SELECT ON '||OWNER||'.'||OBJECT_NAME||' TO &&PLATFORM_DATABASE_ROLE;' FROM DBA_OBJECTS WHERE
OWNER=UPPER('&&PLATFORM_USERNAME') AND OBJECT_TYPE='SEQUENCE';

    --5

    GRANT &&PLATFORM_DATABASE_ROLE TO &&PLATFORM_APPLICATION_ROLE;
    GRANT &&AGA_DATABASE_ROLE TO &&AGA_APPLICATION_ROLE;
    GRANT &&MG_DATABASE_ROLE TO &&MG_APPLICATION_ROLE;
```

Reusing Application and Database Roles

If you plan to have several Advisors installations that will use the same Oracle database, you can reuse the roles. You can also reuse the roles in application upgrades.

If you reuse the roles, then the following part can be omitted from section 1.

```
EXEC SYS.XS_PRINCIPAL.CREATE_ROLE(NAME => '&&PLATFORM_APPLICATION_ROLE', ENABLED => TRUE);
EXEC SYS.XS_PRINCIPAL.CREATE_ROLE(NAME => '&&AGA_APPLICATION_ROLE', ENABLED => TRUE);
EXEC SYS.XS_PRINCIPAL.CREATE_ROLE(NAME => '&&MG_APPLICATION_ROLE', ENABLED => TRUE);

CREATE ROLE &&PLATFORM_DATABASE_ROLE;
CREATE ROLE &&AGA_DATABASE_ROLE;
CREATE ROLE &&MG_DATABASE_ROLE;
```

Advisors Database Deployment with Data Encryption

This page describes Advisors deployment with data encryption for MS SQL and Oracle database servers.

Secure Deployment for MS SQL Server 2008

For MS SQL Server data encryption, 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, such as READ-ONLY file groups, full text indexes, or filestreams that would prevent the TDE. Users must follow the standard Microsoft documentation related to this topic.

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

Database Deployment with Data Encryption for Oracle

Oracle 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.

Genesys recommends TDE for Oracle tablespaces.

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 ensure 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.

Advanced Tablespace Customization

If a more granular customization is necessary (for instance, changing the table/index grouping or encrypting the data at the column level), you have an advanced option. Do not use this option if you do not have a clear understanding of the script's internals.

You will need to perform 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` script.
4. Save it, and then execute the scripts in the following order:
    a. Run `runUsrCre.sql`
    b. Run `runObjCre.sql`
    c. Run all of the scripts listed in the bottom of the corresponding `<xxx>-<version>_Schema.sql` file after an object creation script.

For example, if you want to customize tablespaces for the Platform schema, you need to determine the additional script set and the script order by opening the `advisors-platform-<version>_Schema.sql` file of the corresponding version. The content will be different in different versions. As an example of a versioned script, let's take `advisors-platform-8.5.202.09_Schema.sql`. The bottom of the file will contain the following:

```
spool off
spool runObjCre.log
@@runObjCre.sql
@@advisors-platform-8.5.202.09_ROUTINE1.sql
@@advisors-platform-8.5.202.09_PIMPORT_J.sql
@@advisors-platform-8.5.202.09_ROUTINE2.sql
@@advisors-platform-8.5.202.09_FA_ROUTINE.sql
@@advisors-platform-8.5.202.09_INIT_DATA.sql
@@advisors-platform-8.5.202.09_CUSTOM_ROUTINE.sql
@@advisors-platform-8.5.202.09_CREATE_JOBS.sql
exec spCompileInvalid();
var r number;
var m varchar2(4000);
exec spAllRelatedMetrics(:r,:m);
@@advisors-platform-8.5.202.09_RECREATE_MV.sql
exec spCompileInvalid();
INSERT INTO PATCH_LOG (PATCH_LOG_ID,PATCH_DESC,PATCH_NAME,PATCH_APPLIED_USER,PATCH_APPLIED_DATE)
VALUES(SEQ_PATCH_LOG.NEXTVAL,'Advisors Platform 8.5.202.09','advisors-platform-8.5.202.09_ObjectsPlus.sql',USER,SYSDATE);
COMMIT;
/
BEGIN
   spCompileInvalid();
   dbms_output.put_line('Schema creation completed. Final compilation was successful.');
   dbms_output.put_line('Previous compilation warnings, if any, can be ignored.');
   EXCEPTION
    WHEN OTHERS THEN
     dbms_output.put_line('Schema creation completed with compilation errors.');
     dbms_output.put_line('Compile each invalid object manually to identify ');
     dbms_output.put_line('the reason of the problem.');
     dbms_output.put_line(sqlerrm);
END;
/
spool off
exit
```

Based on this example, after you execute `runObjCre.sql`, you will also have to execute the following:

```
@advisors-platform-8.5.202.09_ROUTINE1.sql
@advisors-platform-8.5.202.09_PIMPORT_J.sql
@advisors-platform-8.5.202.09_ROUTINE2.sql
@advisors-platform-8.5.202.09_FA_ROUTINE.sql
```

```
@advisors-platform-8.5.202.09_INIT_DATA.sql
@advisors-platform-8.5.202.09_CUSTOM_ROUTINE.sql
@advisors-platform-8.5.202.09_CREATE_JOBS.sql
exec spCompileInvalid();
var r number;
var m varchar2(4000);
exec spAllRelatedMetrics(:r,:m);
@advisors-platform-8.5.202.09_RECREATE_MV.sql
exec spCompileInvalid();
```

To verify that an Advisors schema is secured with TDE encryption, do the following:

1. Run the following query to verify that the tablespaces to which the user has access are created as encrypted:
   `SELECT TABLESPACE_NAME,ENCRYPTED FROM USER_TABLESPACES WHERE ENCRYPTED='YES';`
2. Run the following query to verify that all of the tables are created in the encrypted tablespaces:
   `SELECT DISTINCT TABLESPACE_NAME FROM USER_TABLES;`

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")

Index	Table	Column expression
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

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.

Deployment Roadmap

The arrow icon in the following roadmap indicates where you are in the Advisors deployment process.

1. Install the databases that correspond to the Advisors products that you will deploy. Perform the database installation in the following order:
   a. AGA metrics database
   b. Grant `select` privileges on all AGA metrics views to the Platform user.
   c. Metric Graphing database
   d. Advisors Platform database
   [+] REVIEW IMPORTANT INFORMATION HERE

   If the Oracle Platform deployment script issues the following error, `ORA-20001: spCreateOneSourceView ORA-01031: insufficient privileges`, and you are sure that the Platform user has been issued all necessary privileges, then you might have role-based Oracle security set for the Platform user by your DBA. Make sure you take the deployment script from the **current_user** sub-folder in the installation package. You can apply the correct script on top of the one that you applied previously, ignoring the exceptions about existing objects and primary key violations. Alternatively, you can ask your DBA to recreate the user and the privileges and apply the correct script.

   If your installation package does not contain a **current_user** folder, edit the following scripts by replacing all entries of `DEFINER` with `CURRENT_USER` and repeat the database deployment process.

   - If initially you used `advisors-platform-<version>_Schema.sql` or `advisors-platform-<version>_ObjectsPlus.sql`, edit these scripts:
     `advisors-platform-<version>_CUSTOM_ROUTINE.sql`
     `advisors-platform-<version>_PIMPORT_xxx.sql`
     `advisors-platform-<version>_Routine1.sql`
   - If initially you used `advisors-platform-<version>_ObjectsCustom.sql` or `advisors-platform-<version>_ObjectsDefault.sql`, this would be the only script to edit.

   If you prefer, you can contact Genesys Support to obtain the edited scripts.

   Alternatively, you can set up the enhanced Oracle security to run Advisors applications as an application user with least privileges. For instructions, see Least Privileges: How to Configure Advisors Database Accounts with Minimal Privileges.

   If necessary, run the Advisors Object Migration utility. You must run the Advisors Object Migration utility when:

   - You first install Advisors in an environment with a new Configuration Server or when you move an existing Advisors installation to a new Configuration Server.
   - If any of the required Business Attributes folders that Advisors components use are not already present in the Configuration Server.
   - If you decide to enable metrics that are not yet present in your Configuration Server.
   - If you decide to use the Advisors default rollup configuration. Starting with Advisors release

9.0.001.06, a brand new Platform database contains a set of Advisors default hierarchy objects that must be added to the Configuration Server to make the automatic configuration visible on the dashboard. The automatic configuration consists of all base objects mapped to the default hierarchy. For more information, see Contact Center Advisor Default Rollup Configuration in the *Contact Center Advisor and Workforce Advisor Administrator User's Guide*.

- If you perform a new installation in an environment that previously had an Advisors release installed that was older than release 8.5.1. In this case, remove all FA metrics that are in the Configuration Server and then run the migration wizard to populate all FA and CCAdv metrics and hierarchy business attributes.

2.  Create the Advisors User account in Genesys Configuration Server.
3. Install the Platform service on servers where it is required for Advisors components. The Platform service is a prerequisite for installing the following components:
   - Advisors Administration
   - Advisors Web Services
   - WA Server
   - FA Server with rollup engine
   - CCAdv/WA/FA Accessibility services
   - CCAdv/WA Resource Management console
4. Install each adapter that you will use and configure the adapter Application objects with Stat Server connections.
5. Install the Advisors components for your enterprise.
   - Contact Center Advisor server (CCAdv XML Generator)
   - Workforce Advisor server
   - Frontline Advisor server
   - SDS and the CCAdv/WA Resource Management console
6. Make any required configuration changes.

Tip

You might need to use Configuration Manager to configure some of the permissions described in the following Table; it might not be possible to configure everything listed below in other Genesys configuration interfaces (Genesys Administrator or GAX).

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.

Starting with Advisors release 9.0, the **Base Object Configuration** page no longer exists in the Advisors administration module. Therefore, the following table of Advisors User account permissions has been updated; you no longer require additional permissions related to configuration on the **Base Object Configuration** page.

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. Change permission is required so the installers can update properties of Application objects that correspond to Advisors servers.
Hosts folder	Read	Read permission is required on the **Hosts** folder so that the

Object	Permissions	Notes
		hosts on which Solution Control Server is deployed can be read from the Configuration Server.
Adapter Application object(s)	Read, Change	Starting with release 8.5.2, permissions on the adapter Application object are required for adapter–Stat Server communication. These permissions also allow the migration wizard to update properties in both the adapter Application object and the Stat Server Application object. See Manage

Object	Permissions	Notes
		Stat Server Instances for more information about the Advisors Stat Server configuration.
Stat Server Application object(s)	Read, Change	The Change permission is required starting in release 8.5.2. The migration wizard connects to the Configuration Server in order to update the properties in both the adapter Application object and the Stat Server Application object. See Manage Stat Server Instances for more information

Object	Permissions	Notes
		about the Advisors Stat Server configuration.
Tenants	Read	
*Agent Groups	Read	Required for CCAdv and WA Choose only the sets of objects that you might want to monitor in CCAdv or WA.
Switches	Read	
*DNs (of type ACD Queues and Virtual Queues)	Read	Required for CCAdv and WA
*DN groups	Read	Required for CCAdv and WA
Persons	Read, Read Permissions	
	Change	Required only in the following circumstances: • to allow users to change their password using the

Object	Permissions	Notes
		Change Password functionality • if the Resource Management Console will be used to modify agent skills (the Change permission is required to save the agent skill changes)
Skills	Read	Read permission is required to view skills in the Resource Management Console.
*Objects in the **Scripts** folder (of type Interaction Queue)	Read	Required for CCAdv
Access Groups	Read, Read Permissions	
*Campaigns	Read	Required for CCAdv
*Calling lists	Read	Required for CCAdv
Roles	Read, Read Permissions	Used to determine

Object	Permissions	Notes
		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.
Folders in Persons	Read, Read Permissions	Required for FA. Read `Permissions` is necessary to control end users' permissions to see the agent hierarchy.
Folder in Agent Groups	Read, Read Permissions	Required for FA. The folder content should represent the FA hierarchy. Read `Permissions` is necessary to control the end users'

Object	Permissions	Notes
		agent hierarchy.
SDS Application	Read, Change, Read Permissions	Only required if you deploy Supervisor Desktop Service.

*You may exclude the following Advisors-supported object types from Read access as a whole, or exclude individual objects within any object type, if any of these objects do not need to be monitored in Advisors:

- Agents (Persons)
- Agent Groups
- ACD Queues
- Virtual Queues
- DN Groups
- Calling Lists
- Interaction Queues

In the Configuration Server, under **Agent Groups**, if the folder that you choose for FA does not need to be monitored in CCAdv/WA, then create a separate Advisors account for FA and enter that account when you install the FA component.

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 Pulse Advisors, and include the list of privileges available with Advisors release 8.5.2.

> **Important**
>
> 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 Advisors privileges associated with a Role only in Genesys Configuration Manager.

[+] RBAC and Advisors

Pulse 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.

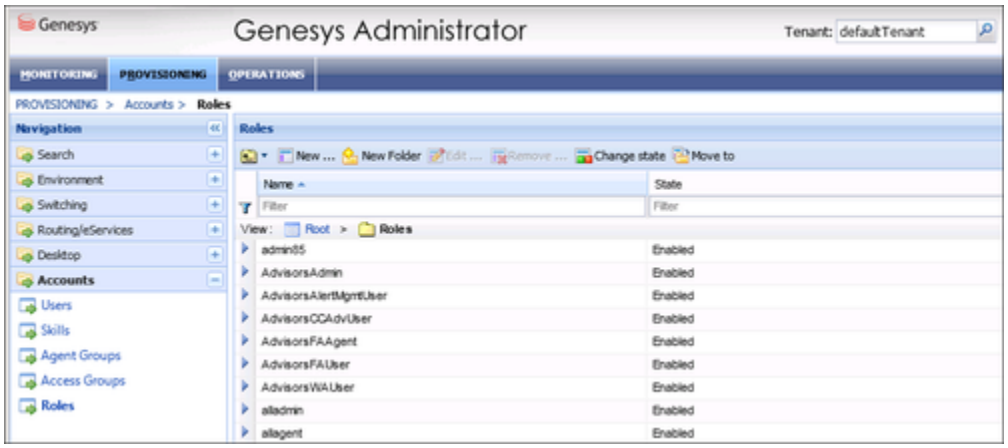
Roles define what facilities are provided to users to review and manipulate various types of data. These include which property controls are available for items permitted by object permissions, what modules are visible, and access control for entities not represented by configuration objects. A Role 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.

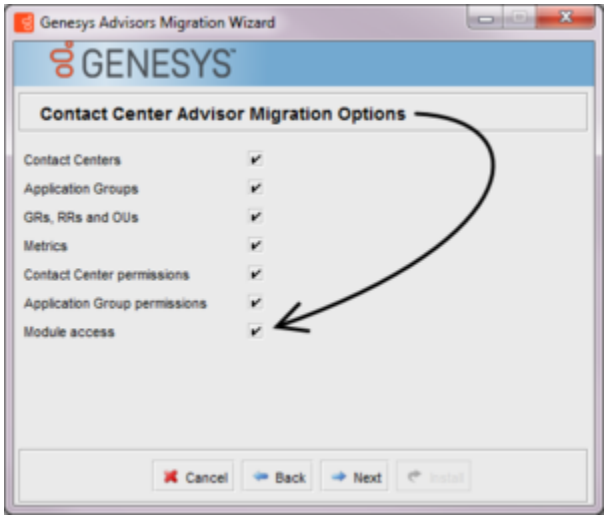
The figure shows an example of Advisors Role configuration.

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 Advisors 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 Advisors 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.

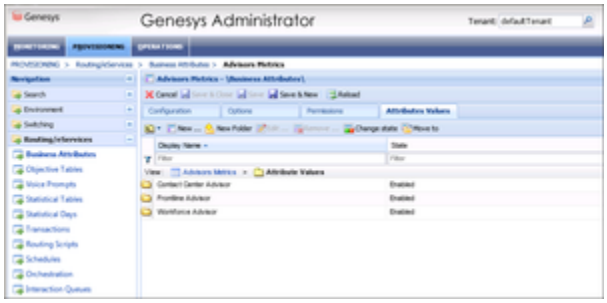
  In this case, user A will be denied access to the metric.
- User A is part of Access Groups X and Y.
  Neither group has defined access to the metric.

  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

You can control access to objects in the Genesys Pulse Advisors Contact Center Advisor (CCAdv) and Workforce Advisor (WA) dashboards and on the Advisors administration module pages using Roles, and associating privileges with each Role. Controlling users' access to data and objects using Roles and associated privileges is called Role-Based Access Control (RBAC).

See the following documents and pages for more information about configuring user profiles:

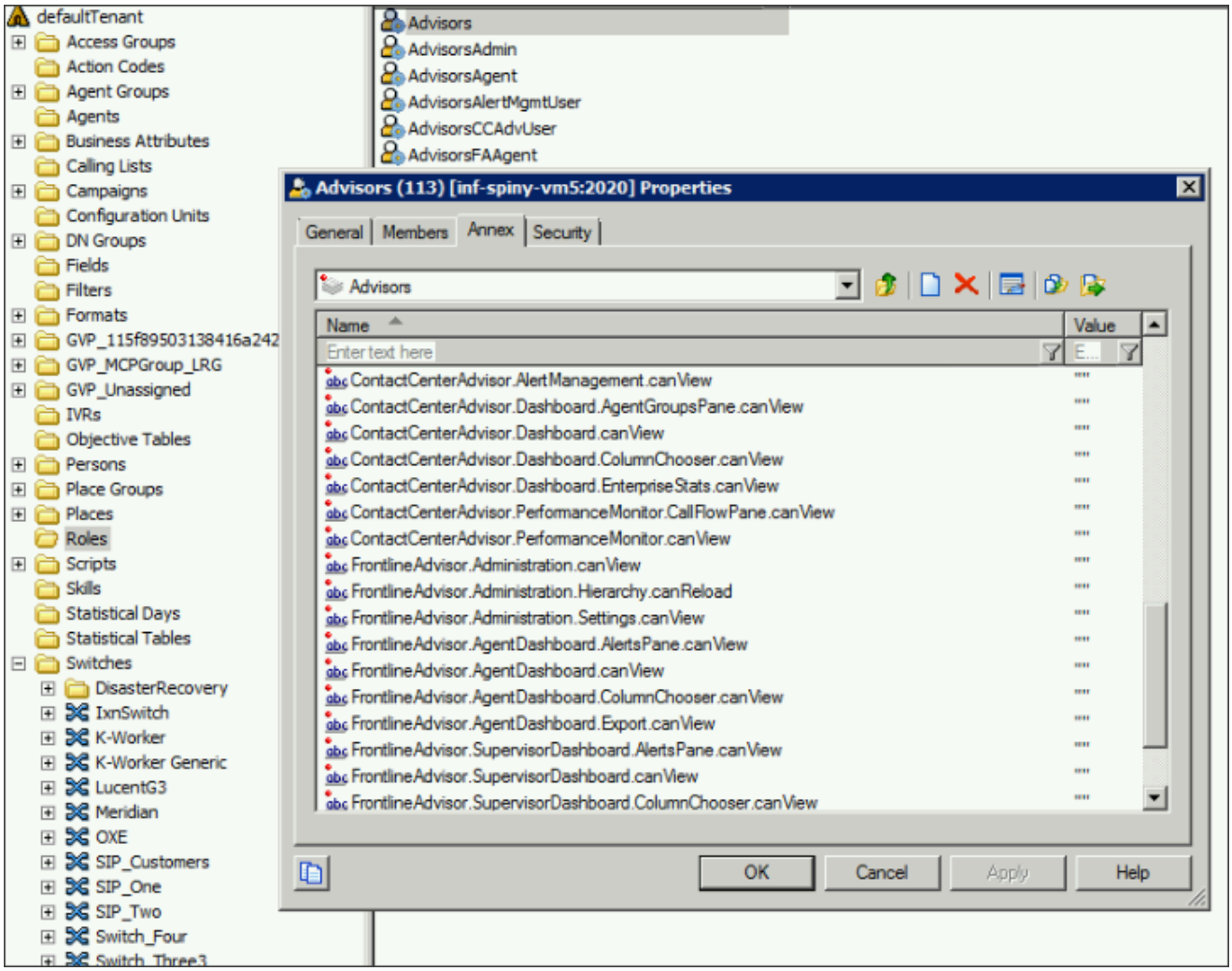
- Authentication and Authorization — This chapter in the *Genesys Security Deployment Guide* provides information about securing access to systems (in whole or in part) with user authentication and authorization. In particular, see User Authentication and User Authorization, Object-Based Access Control, and Role-Based Access Control.
- Framework Configuration Manager Help — How to use Genesys Configuration Manager (this is a .zip file)
- Genesys Administrator Extension Help: Users (Persons) — Configuring Users (Persons) in the GAX interface
- Genesys Administrator Extension Help: Access Groups — Configuring Access Groups in the GAX interface
- Genesys Administrator Extension Help: Roles — Configuring Roles in the GAX interface
- Genesys Administrator Extension Help: Configuration Manager — Working with (GAX) Configuration Manager

> **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 Advisors privileges associated with a Role only in Genesys Configuration Manager.

The following sections provide the lists of available Advisors privileges with which you can secure access to CCAdv, WA, and Advisors administration interface objects:

- Privileges associated with the Advisors Administration module
- Privileges associated with user dashboards
- Privileges associated with Contact Center Advisor
- Privileges associated with Workforce Advisor

The following figure shows a sample of Advisors privileges configuration in Genesys Configuration Manager.



Administration Module

Privilege	Controls Access To:
AdvisorsAdministration.canView * Not specific to Contact Center Advisor/Workforce Advisor. When the privilege is assigned, a Frontline Advisor user has access to the Administration module, as well.	Administration module
AdvisorsAdministration.DeletedObjects.canView	Objects in the Administration module pages that were deleted from the Genesys Administrator server
AdvisorsAdministration.SystemConfiguration.canView	**System Configuration** page in the Administration module

AdvisorsAdministration.Regions.canView	**Regions** page in the Administration menu
AdvisorsAdministration.ApplicationGroups.canView	Application Groups/Thresholds page in the Administration module
AdvisorsAdministration.ContactCenters.canView	**Contact Centers** page in the Administration module
AdvisorsAdministration.ApplicationConfiguration.canView	**Application Configuration** page in the Administration module
AdvisorsAdministration.AgentGroupConfiguration.canView	**Agent Group Configuration** page in the Administration module
AdvisorsAdministration.ContactGroupConfiguration.canView	**Contact Group Configuration** page in the Administration module
AdvisorsAdministration.Metrics.canView	Metric Manager **Report Metrics** page in the Administration module
AdvisorsAdministration.MMW.canCreate	Create and Copy functions in the Metric Manager, which are used to create custom metrics
AdvisorsAdministration.MMW.canEdit	Edit function in the Report Metrics Manager, which is used to edit all metrics
AdvisorsAdministration.MMW.canDelete	Delete function in the Report Metrics Manager, which is used to delete custom metrics
AdvisorsAdministration.MMW.SourceMetrics.canView	Metric Manager **Source Metrics** page in the Administration module
AdvisorsAdministration.MMW.SourceMetrics.canCreate	**Create Source Metrics** button on the **Source Metrics** page
AdvisorsAdministration.MMW.SourceMetrics.canEdit	Edit function on the **Source Metrics** page, which is used to edit source metrics
AdvisorsAdministration.MMW.SourceMetrics.canDelete	Delete function on the **Source Metrics** page, which is used to delete custom source metrics
AdvisorsAdministration.DistributionLists.canView	**Distribution Lists** page in the Administration module
AdvisorsAdministration.ManualAlerts.canView	**Manual Alerts** page in the Administration module
AdvisorsAdministration.RMC.Notifications.canView	User has access to the following pages in the Administration module: • Notification Templates • Notification Lists User can create a new notification template in the **Resource Management** window and use it once, or save the template to use it again. / The **Control Panel** section does not appear in the Administration module's navigation pane and there are no links to the following pages: • Notification Templates • Notification Lists User can create a template in the **Resource Management** window and use it once; there is no option to save a new template for reuse.

Advisors Dashboards

Privilege	Controls Access To:
Advisors.ChangePassword.canView	Change Password function
Advisors.RMC.canView	Resource Management Console (RMC)
Advisors.RMC.ManageAgentSkills.canView	**Manage Skills** pane in the RMC window
Advisors.RMC.ManageAgentStatus.canView	**Manage Status** pane in the RMC window

Contact Center Advisor

Privilege	Controls Access To:
ContactCenterAdvisor.Dashboard.canView	Contact Center Advisor dashboard
ContactCenterAdvisor.Dashboard.AgentGroupsPane.canView	Data in the **Agent Groups** pane
ContactCenterAdvisor.Dashboard.ColumnChooser.canView	Column chooser
ContactCenterAdvisor.Dashboard.EnterpriseStats.canView	The Enterprise row and statistics on the dashboard
ContactCenterAdvisor.Dashboard.PivotSelect.canView	The hierarchy grouping drop-down list on the **Contact Centers** pane.

Workforce Advisor

Privilege	Controls Access To:
WorkforceAdvisor.Dashboard.AgentGroupsPane.canView	Data in the **Agent Groups** pane
WorkforceAdvisor.Dashboard.canView	The WA dashboard
WorkforceAdvisor.Dashboard.ColumnChooser.canView	Column Chooser
WorkforceAdvisor.Dashboard.EnterpriseStats.canView	The Enterprise row 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 use the hierarchy grouping drop-down list if agent group contact centers are configured.	The hierarchy grouping drop-down list on the **Contact Centers** pane.

[+] 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 tables list the RBAC privileges that are available for Frontline Advisor users.

See the following documents for more information about configuring user profiles:

- Framework Configuration Manager Help
- Genesys Administrator Extension Help

> **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 Advisors privileges associated with a Role only in Genesys Configuration Manager.

Administration Module

Privilege	Controls Access To:
AdvisorsAdministration.canView	Administration module

Advisors Dashboards

Privilege	Controls Access To:
Advisors.ChangePassword.canView	Change Password function

Frontline Advisor Dashboard

Privilege	Controls Access To:
AdvisorsAdministration.Metrics.canView	**Report Metrics** page
AdvisorsAdministration.MMW.canCreate	The Create and Copy functions in the Report Metrics Manager. Users require this privilege to create custom metrics.
AdvisorsAdministration.MMW.canEdit	The Edit function in the Report Metrics Manager. Users require this privilege to edit metrics.
AdvisorsAdministration.MMW.canDelete	The Delete function in the Report Metrics Manager. Users require this privilege to delete custom

	metrics.
AdvisorsAdministration.MMW.SourceMetrics.canView	**Source Metrics** page
AdvisorsAdministration.MMW.SourceMetrics.canCreate	The **Create Source Metrics** button on the **Source Metrics** page. Users require this privilege to create custom source metrics.
AdvisorsAdministration.MMW.SourceMetrics.canEdit	The Edit function on the **Source Metrics** page. Users require this privilege to edit source metrics.
AdvisorsAdministration.MMW.SourceMetrics.canDelete	The Delete function does not display on the Source Metrics page. Users require this privilege to delete custom source metrics.
FrontlineAdvisor.SupervisorDashboard.canView	Frontline Advisor supervisor dashboard
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView *The FrontlineAdvisor.SupervisorDashboard.canView privilege must also be present*	**Teams** pane in the FA supervisor dashboard. In addition to the **Teams** pane, the **Alerts** pane is not displayed to users to whom you have not assigned this privilege.
FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView *Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges*	**Alerts** pane. If you have not assigned the FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privilege to a user, the user will not have access to the **Alerts** pane even though the FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privilege is assigned.
FrontlineAdvisor.SupervisorDashboard.ColumnChooser.canView *Requires the FrontlineAdvisor.SupervisorDashboard.canView privilege*	Column Chooser
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canSort *Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges*	The data sorting functionality in the **Teams** pane
FrontlineAdvisor.SupervisorDashboard.TeamAlertsPane.canSort *Requires the FrontlineAdvisor.SupervisorDashboard.canView, FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView and FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privileges*	The data sorting functionality in the **Alerts** pane
FrontlineAdvisor.Administration.canView	Frontline Advisor page in the administration module
FrontlineAdvisor.Administration.Settings.canView *Requires the FrontlineAdvisor.Administration.canView privilege*	The **Settings** tab on the FA administration page in the Administration module.
FrontlineAdvisor.Administration.Hierarchy.canReload *Requires the FrontlineAdvisor.Administration.canView and FrontlineAdvisor.Administration.Settings.canView privileges*	The hierarchy reload action on the **Settings** tab of the FA administration page in the Administration module.

Deploying Advisors

The **Deploying Advisors** section contains topics to assist you when you use the Pulse 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:

Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS

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 Contact Center Advisor or Workforce Advisor

To deploy Contact Center Advisor or Workforce Advisor, see:

General Prerequisites

Prerequisites for CCAdv and WA

Deploying CCAdv and WA

Deploying Frontline Advisor and Agent Advisor

To deploy Frontline Advisor, see:

Deploying Resource Management Console

To deploy the Resource Management Console, see:

Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS

This page provides a summary of the tasks that you must perform in order to deploy the Advisors modules that are controlled by Solution Control Server (SCS). For the list of Advisors modules that are controlled by SCS, see Integration with Solution Control Server.

Related Information

See the following topics for more information:

- Integration with Solution Control Server and Warm Standby

Procedure:

Steps

1. Install a supported version of the Local Control Agent (LCA) on any server that includes, or will include, an Advisors module that SCS will control (some Genesys products install LCA as part of the product deployment, but Advisors do not). See Integration with Solution Control Server for a list of these modules.
   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 module 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 module will run.

c. Create an Application representing this Advisors module.

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 modules ignore these port numbers; therefore, you can enter any port number, but Genesys recommends that you enter the following HTTP port values for servers. Where the Application represents:
  - Tomcat running the WA Server or FA with the rollup engine: Use the default HTTP port number, which is 8080.
  - CCAdv XML Generator: Use the default HTTP port number, which is 8090.
  - AGA: Enter the HTTP port number that will be used for the AGA instance.
- Enter a period (.) as a placeholder in both the **Working Directory** and the **Command Line** fields.
- If this module 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 module 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 before 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 a Genesys configuration interface, such as Genesys Administrator, configure the option on the **Options** tab for your SCS Application. For additional information, see the Genesys Management Framework documentation.

Managing the Start and Stop of Advisors Applications

You can create a Pulse Advisors Solution object that gives you centralized control of the Advisors Application objects. This page describes how to configure the Advisors Solution object, and provides information about managing the automatic restart of Advisors components.

Configuring Advisors Application Objects 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. The procedure can be used in High Availability (HA) configuration, as well.

Procedure: Create an Advisors Solution object

Purpose: To create an Advisors Solution object using existing Advisors Application objects. Once the Advisors suite is configured as a Solution, you can start, stop, and run the Advisors components as a group using either Genesys Administrator or the Solution Control Interface (SCI). You can use an Advisors Solution object if you plan to use the Solution Control Server (SCS) to manage the restart of the Advisors Applications. Genesys recommends that you avoid configuring an Advisors Solution object if you will manage the auto-restart of the Advisors Applications using other external task schedulers, such as the operating system's scheduler (for example, Windows task scheduler). For more information, see Configuring Advisors Applications to Restart Automatically.

Prerequisites

- Ensure the Advisors Application objects exist that will be part of the Solution.
- You will need a "third-party" Application configured for every Advisors Web Services node that

you want to control with 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 Advisors Web services = 4
     e. Workforce Advisor (WA) server = 5

Configuring Advisors Applications to Restart Automatically

Genesys Applications can be configured to restart automatically when the Advisors server machines are restarted. When configuring the Advisors Application objects to restart automatically, Genesys strongly recommends that you use the procedure on this page to configure the Applications as a Solution because it allows you to specify the recommended startup order for the components. However, you can use the Advisors Solution object only if you plan to use SCS to manage the automatic restart of the Advisors Application objects. If you do not use SCS to control the restart of Applications, then an alternative method for automatically restarting the Advisors components is to use your server's OS-based tools for controlling services.

Additional Recommendations for Advisors Automatic Restart

In addition to other recommendations on this page, Genesys also recommends the following when configuring Advisors Applications to restart automatically:

- Use only one tool to manage the restart of Advisors Application objects. When you use SCS to manage the restart of the Advisors Application objects, you might experience conflicts if you also manage Advisors Applications with other external task schedulers, such as the operating system's scheduler (for example, Windows task scheduler).
- Avoid using the **Starting Applications Automatically** procedure in the *Framework Management Layer User's Guide* because it gives you no control over the order in which the Applications restart, which might cause issues when starting up Advisors Applications.

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.

> **Important**
> In release 9.0, there are changes to the installation wizard screens; therefore, you cannot reuse your previous setup for silent installation or any saved `ant.install.properties` file.

Deployment Roadmap

The arrow icon in the following roadmap indicates where you are in the Advisors deployment process. The deployment roadmap on this page is meant to be a summary view. For complete information, see the Deployment Summary page in this guide.

1. Install the databases that correspond to the Advisors products that you will deploy. Perform the database installation in the following order:
   a. AGA metrics database
   b. Grant `select` privileges on all AGA metrics views to the Platform user.
   c. Metric Graphing database
   d. Advisors Platform database
      [+] REVIEW IMPORTANT INFORMATION HERE

      If the Oracle Platform deployment script issues the following error, `ORA-20001: spCreateOneSourceView ORA-01031: insufficient privileges`, and you are sure that the Platform user has been issued all necessary privileges, then you might have role-based Oracle security set for the Platform user by your DBA. Make sure you take the deployment script from the **current_user** sub-folder in the installation package. You can apply the correct script on top of the one that you applied previously, ignoring the exceptions about existing objects and primary key violations. Alternatively, you can ask your DBA to recreate the user and the privileges and apply the correct script.

      If your installation package does not contain a **current_user** folder, edit the following scripts by replacing all entries of `DEFINER` with `CURRENT_USER` and repeat the database deployment process.

      - If initially you used `advisors-platform-<version>_Schema.sql` or `advisors-platform-<version>_ObjectsPlus.sql`, edit these scripts:
        `advisors-platform-<version>_CUSTOM_ROUTINE.sql`
        `advisors-platform-<version>_PIMPORT_xxx.sql`
        `advisors-platform-<version>_Routine1.sql`
      - If initially you used `advisors-platform-<version>_ObjectsCustom.sql` or `advisors-`

`platform-<version>_ObjectsDefault.sql`, this would be the only script to edit.

If you prefer, you can contact Genesys Support to obtain the edited scripts.

Alternatively, you can set up the enhanced Oracle security to run Advisors applications as an application user with least privileges. For instructions, see Least Privileges: How to Configure Advisors Database Accounts with Minimal Privileges.

If necessary, run the Advisors Object Migration utility. You must run the Advisors Object Migration utility when:

- You first install Advisors in an environment with a new Configuration Server or when you move an existing Advisors installation to a new Configuration Server.
- If any of the required Business Attributes folders that Advisors components use are not already present in the Configuration Server.
- If you decide to enable metrics that are not yet present in your Configuration Server.
- If you decide to use the Advisors default rollup configuration. Starting with Advisors release 9.0.001.06, a brand new Platform database contains a set of Advisors default hierarchy objects that must be added to the Configuration Server to make the automatic configuration visible on the dashboard. The automatic configuration consists of all base objects mapped to the default hierarchy. For more information, see Contact Center Advisor Default Rollup Configuration in the *Contact Center Advisor and Workforce Advisor Administrator User's Guide*.
- If you perform a new installation in an environment that previously had an Advisors release installed that was older than release 8.5.1. In this case, remove all FA metrics that are in the Configuration Server and then run the migration wizard to populate all FA and CCAdv metrics and hierarchy business attributes.

2. Create the Advisors User account in Genesys Configuration Server.
3.  Install the Platform service on servers where it is required for Advisors components. The Platform service is a prerequisite for installing the following components:
   - Advisors Administration
   - Advisors Web Services
   - WA Server
   - FA Server with rollup engine
   - CCAdv/WA/FA Accessibility services
   - CCAdv/WA Resource Management Console
4. Install each adapter that you will use and configure the adapter Application objects with Stat Server connections.
5. Install the Advisors components for your enterprise.
   - Contact Center Advisor server (CCAdv XML Generator)
   - Workforce Advisor server
   - Frontline Advisor server
   - SDS and the CCAdv/WA Resource Management Console (RMC)
6. Make any required configuration changes.

Deploying the Advisors Platform Application

Procedure:

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. Navigate to the Advisors home directory:

   ```
   cd /home/advisors
   ```

   b. 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. The following example uses `jdk1.8.0`. When you run the command in your environment, be sure to enter the JDK version number that you use in your installation.

   ```
   ./jdk1.8.0_<version>/bin/java -jar advisors-platform-installer-<version>.jar
   ```

   See the *Genesys Supported Operating Environment Reference Guide* for information about Java versions supported with each Advisors release.

   [+] 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. Use the information provided in the Installer Screens section on this page to complete the remaining deployment screens. 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. Do this only for Advisors servers that are not controlled by Solution Control Server (SCS). For the list of servers that are not controlled by SCS, see Integration with

Solution Control Server.

[+] Show Steps

a. Open a command prompt, and change directory first to your Advisors base directory (for example, `Program Files\GCTI\Advisors`), then to `bin`.

b. On Windows 32-bit machines, run `installService-x86.bat` to install the service.

c. On Windows 64-bit machines, run `installService-x64.bat` to install the service.

d. After installation, you can make changes to the configuration of the service (for example, JVM options) using the `AdvisorsServicew.exe` utility in the `<Advisors directory>/apache-tomcat-<version>/bin` directory, if needed.

If you use a Linux platform, validate that the Advisors Platform component installed successfully, and then configure Advisors Platform to run automatically as a system service. Do this only for Advisors servers that are not controlled by Solution Control Server. For the list of servers that are not controlled by SCS, see Integration with Solution Control Server.

[+] Show Steps

The following example uses `jdk1.8.0`. When you run the commands in your environment, be sure to enter the JDK version number that you use in your installation. See the *Genesys Supported Operating Environment Reference Guide* for information about Java versions supported with each Advisors release.

a. Open the shell.

b. Run the following export command to add the JDK to your path:

```
export PATH=/home/advisors/jdk1.8.0_<version>/bin:$PATH
```

c. Change the owner of the directory in which you installed the Advisors Platform to the Advisors user:

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

d. Test the installation as the Advisors user.

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

```
export JAVA_HOME=/home/advisors/jdk1.8.0_<version>
```

ii. Start Advisors Platform:

```
./<Advisors directory>/apache-tomcat-<version>/bin/catalina.sh run
```

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

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

i. Using the sudo command, create an `/etc/init.d/advisors` file with the following contents; remember to replace `<version>` with the JDK version number that you use 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/jdk1.8.0_<version>
export JAVA_HOME
PATH=$JAVA_HOME/bin:$PATH
export PATH
ADVISORS_BIN=/home/advisors/<Advisors directory>/apache-tomcat-<version>/bin

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

ii. Using the sudo command, make the startup script executable:

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

iii. Using the sudo command, configure the system to start the Advisors process at boot time:

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

iv. Check that the configuration is correct:

```
sudo 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. Using the sudo command, test the service startup script:

```
sudo service advisors start
```

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

vi. Using the sudo command, test the service stop script:

```
sudo service advisors stop
```

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

> **Important**
> To avoid file permission issues, Genesys recommends that you always start the Advisors service with the same user that you used during installation. This user should be a sudoer.

vii. Using the sudo command, test that Advisors Platform starts automatically after a reboot:

> **Warning**
> The following command restarts the whole system.

```
sudo shutdown -r now
```

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

Installation Screens

[+] Authentication Options

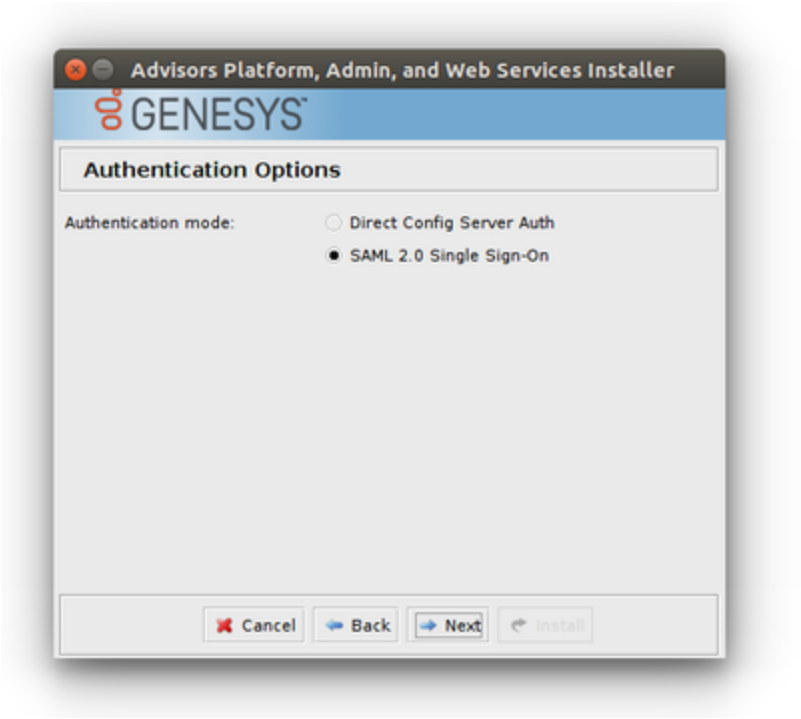
You have two user login options:

- Use the existing Configuration Server–based authentication system
- Use the SAML Single Sign-On (SSO) login process

Note that the following features are not supported when using the Single Sign-On login process:

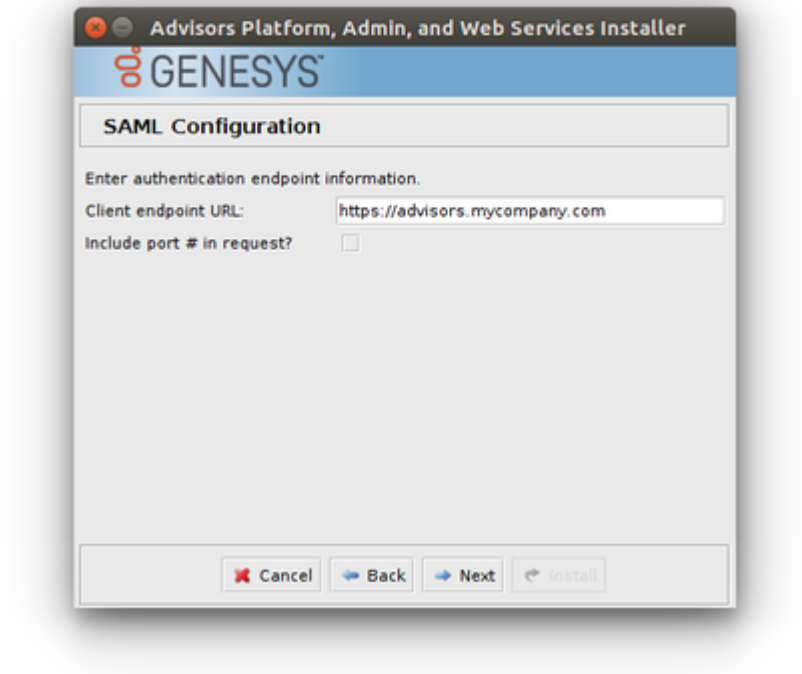
- Change password and Forgot password functionality
- Advisors Resource Management Console (RMC)

To continue to use the Configuration Server–based authentication system, which Advisors applications have used in earlier releases, select the **Direct Configuration Server Auth** authentication mode on the **Authentication Options** installation screen. To use the SAML SSO login system, select the **SAML 2.0 Single Sign-On** option.



If you opt to use the SSO method, the installer will prompt you for additional information. See the descriptions of the following screens for additional information:

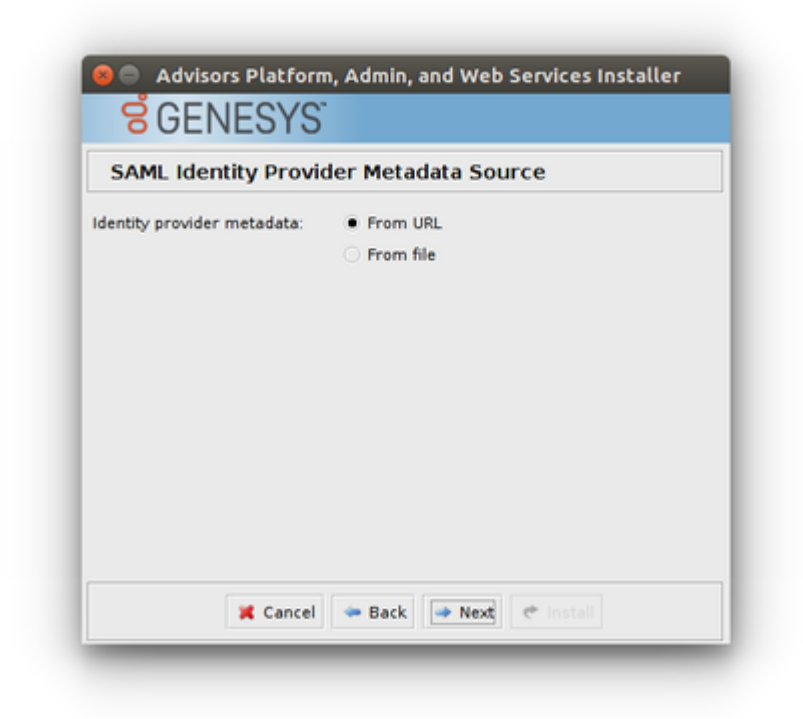
- SAML Configuration



The endpoint URL should be the URL that users will use to access Advisors applications. If Advisors components are deployed in a clustered configuration, this would typically be the single URL to which users are directed and which then load-balances these requests across the cluster. Load balancing with sticky sessions is required when using the SAML SSO login process, and is typically required in clustered Advisors deployment regardless of the authentication process used.

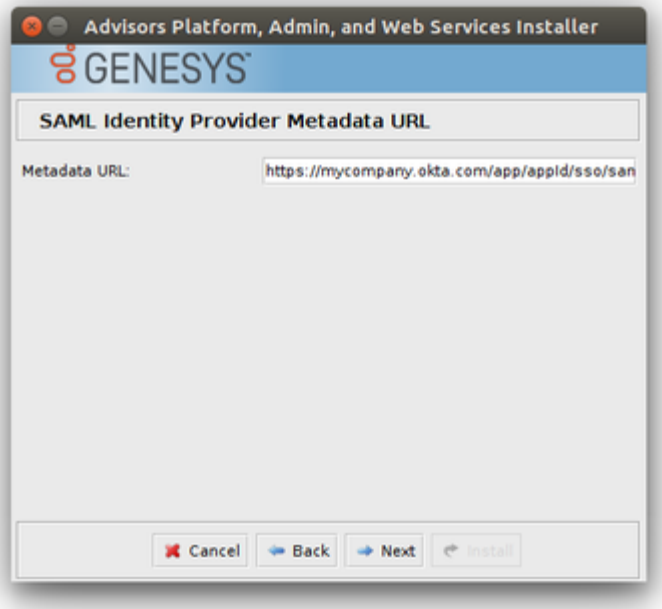
- If your SAML Identity Provider (IdP) asks for an Assertion Consumer URL or "Single Sign-On" URL for IdP-initiated login, this should consist of the endpoint URL, described above, with the added path `/adv/saml/SSO`. For example, `https://advisors.mycompany.com/adv/saml/SSO`.
- If your SAML IdP prompts you for the Advisors Service Provider (SP) "Entity Id" or metadata, this should consist of the endpoint URL, described above, with the added path `/adv/saml/metadata`. For example, `https://advisors.mycompany.com/adv/saml/metadata`.

- SAML Identity Provider Metadata Source

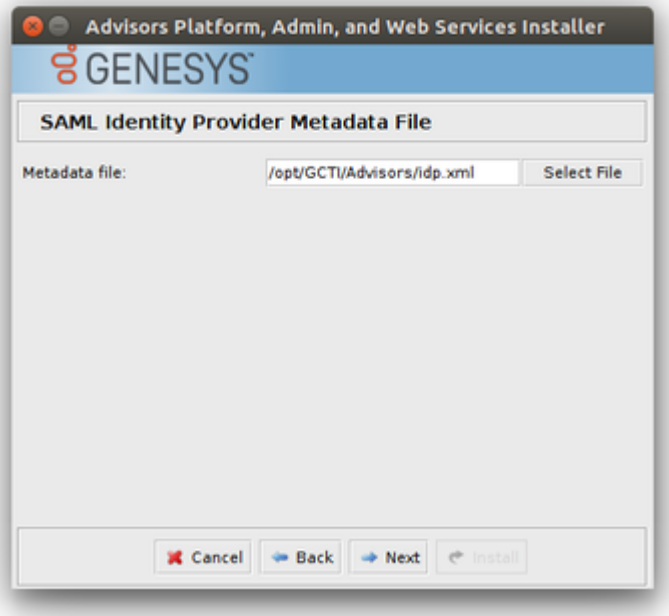


SAML Identity Provider (IdP) metadata can be configured by providing a file containing the metadata or a URL where the IdP metadata is served. This metadata should be provided by your Single Sign-On system. Refer to the documentation for your particular system for information on how to configure an Identity Provider and obtain its metadata. The following two figures show the screens on which you either provide the location of the metadata file or provide the URL from which the IdP metadata is served.

- SAML Identity Provider Metadata URL



- SAML Identity Provider Metadata File



[+] Administration Configuration - CCAdv XMLGen

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

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.

[+] 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.

[+] 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.

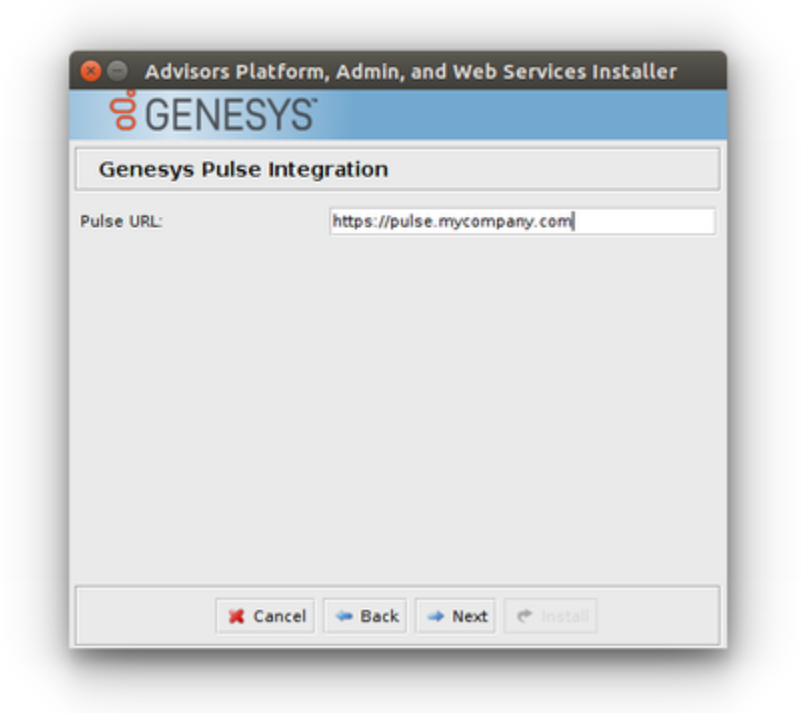
[+] Genesys Config Server Connection Details

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 your Genesys configuration interface (for example, Genesys Administrator) 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`.

[+] Genesys Pulse Integration

Provide a URL to point users to your installation of Genesys Pulse. Entering the Pulse installation URL adds a link to Pulse in the navigation bar of each Advisors dashboard.



[+] 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 email 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.

[+] Log Files Directory

Starting with release 9.0.001, the installation wizard prompts you to provide the log file storage location, and provides a default path. If you plan to use a log file storage location that is not the

default location, then specify the location on the **Log Files Directory** screen. The installation wizard checks that the selected storage directory is present; if not present, then the wizard creates it. The installation wizard stores the selected log file storage location in one of the following files:

- The properties file specific to the module. The log file configuration file picks up the location from the module's properties file.
- The log4j configuration file.

Specifying the log file directory in the installation wizard will not change the directory that was set for previous installations.

For more information about log files, see Adjust Logging Settings and Configure Administrative Actions Logs.

[+] Mail Service Configuration

On the **Mail Service Configuration** screen, specify the email settings that the application will use to send email, including email related to the `Forgot Password` functionality.

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

[+] Metric Graphing Database

On the **Metric Graphing 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 **Metric Graphing Database** screen, specify the parameters for the metric graphing 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 metric graphing database.
- `Database user password`—The password created and used for the metric graphing database.

[+] Metric Graphing Database - Advanced

On the **Metric Graphing Database - 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). 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 **Metric Graphing Database - Advanced** screen, specify the parameters for the metric graphing database:

- `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.

[+] Modules to Install

Select the `Administration workbench` checkbox to install the Administration module. Installing the Administration workbench adds an `Administration.properties` file to the `<advisors>\conf` folder. 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.

Select the `Genesys Pulse Integration` checkbox to configure a link in the Advisors navigation bar pointing to your installation of Genesys Pulse. This option only needs to be installed once per Advisors deployment and applies to all servers. If installed again, the navigation bar will point to the most recently configured link. If not configured, no link to Genesys Pulse will be displayed in the Advisors navigation bar.

Select the `Advisors Web Services` checkbox to install the Web services. This option installs all of the dashboards, as well as the metric graphing services. The Platform installer will prompt you for the Metric Graphing database options when you have selected the `Advisors Web Services` option because metric graphing is not an optional feature; the metric graphing services are always installed with the other Web services.

You must install the Advisors Web services on presentation nodes. If you will later install Contact Center Advisor (CCAdv) XML Generator, Workforce Advisor (WA) Server, or Frontline Advisor (FA) Server with rollup engine on this node, Genesys recommends that you avoid installing the Web Services on the node, for best performance. The Advisors Web Services option does not install the Resource Management Console or the accessible dashboards. For CCAdv/WA, you have the option to select those features when you run the CCAdv/WA installation wizard. The FA accessible dashboard is automatically installed when you run the FA installation wizard.

[+] 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 supported drivers.

[+] Password Management Options

On the **Password Management Options** screen, configure the following.

1. Select the `Allow Password Modification?` checkbox to enable the `Forgot your password?`functionality. If you do not select this option, 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 using a Genesys configuration interface.

> ### Warning
>
> Pulse Advisors do not fully support the password security authentication options available in Management Framework. As a result, it is possible for users to get locked out of the Advisors applications. To avoid lockouts, do one or both of the following:
>
> - Change the following two options in Management Framework to `true`: the **no-change-password-at-first-login** option and the **override-password-expiration** option.
> - Assign the `Advisors.ChangePassword.canView` privilege to all users.
>
> For information about the **no-change-password-at-first-login** and **override-password-expiration** options, see the *Genesys Framework Configuration Options Reference Manual*.

[+] 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.

[+] Tomcat Configuration

On the **Tomcat Configuration** screen, you can configure the port numbers that Tomcat will use, if necessary. You will typically use the default values that the installation wizard provides, except in the following situations:

- You are going to install two different deployments of Advisors on the same machine, so you require two sets of port numbers. For more information, see Multiple Advisors Deployments on One System.
- Other software is running on the same host and is already using the ports, in which case you must assign other ports for Tomcat to use.

[+] User Management Options

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

Add the name of the default Genesys tenant to which new users will be added. The name of the tenant is case sensitive.

Troubleshooting

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

Installation Error Message	Cause

`[echo] Setting up cluster member configuration for this node`
 	
`[java] Connecting to database: inf-wolf.us.int.genesyslab.com;oracle:1521;DatabaseName=orcl;user=yevgeny_plt_81`
`...`
`[java] updating node: KoolNode ipAddress: 138.120.xx.xx localhost: localhost`
`[java] java.sql.SQLException: ORA-01013: user requested cancel of current operation`
`[java] at oracle.jdbc.driver.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.T4C8Oall.receive(T4C8Oall.java:745)`
`[java] at oracle.jdbc.driver.T4CPreparedStatement.doOall8(T4CPreparedStatement.java:219)`
`[java] at oracle.jdbc.driver.T4CPreparedStatement.executeForRows(T4CPreparedStatement.java:970)`
`[java] at oracle.jdbc.driver.OracleStatement.doExecuteWithTimeout(OracleStatement.java:1190)`
`[java] at oracle.jdbc.driver.OraclePreparedStatement.executeInternal(OraclePreparedStatement.java:3370)`
`[java] at oracle.jdbc.driver.OraclePreparedStatement.executeUpdate(OraclePreparedStatement.java:3454)`
`[java] at com.informiam.installer.DAO.executeTimedOutUpdate(DAO.java:214)`
`[java] at com.informiam.installer.ConfigureClusterMember.performActivities(ConfigureClusterMember.java:60)`
`[java] at com.informiam.installer.AbstractDatabaseUtility.doMain(AbstractDatabaseUtility.java:56)`
`[java] at com.informiam.installer.ConfigureClusterMember.main(ConfigureClusterMember.java:34)`
	This type of error may happen when the installer attemp update a table which is locked by a not-committed transaction (usually with Oracle database).
	
	The wording of the error may differ, but the key phrase to look for is `ORA-01013: user requested cancel of current operation`. Typically this could happen with an Oracle database when someone ru query such as `DELETE FROM <TABLE_NAME>` without then executing `CO` and the installer tries to update the same table.
	In this case, the installer will wait for 20 seconds and fail with an error to the above. To correct this, execute `COMMIT;` after the `DELETE` statem and re-run the installer. To prevent this situation, always run `COMMIT;` manually updating tables in Oracle.

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

Installation Error Message	Cause
[java] Failed to connect to the database using connection URL: [java] jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=NotAPlatformDB;selectMethod=cursor; user=sa;password=very_secure_pwd [java] The following exception was thrown: com.microsoft.sqlserver.jdbc.SQLServerException: The TCP/IP connection to the host 192.168.xx.yy, port nnnn has failed. Error: "connect timed out. Verify the connection properties, check that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port, and that no firewall is blocking TCP connections to the port."	Wrong database name
[java] Exception while connecting: Login failed for user 'badUserId'. [java] url used: jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=ys_pldb;selectMethod=cursor; user=badUserId;password=very_secure_password	Wrong database user name or password
[echo] pinging cluster node IP address 138.120.yy.zz... [java] WARNING! Host 138.120.yy.zz is unknown - java.net.UnknownHostException: 138.120.yy.zz. This may be due to a firewall blocking requests or a specific server configuration, e.g.: permissions. [java] ERROR! Host 138.120.yy.zz is unknown - java.net.UnknownHostException: 138.120.yy.zz. This may be due to a firewall blocking requests or a specific server configuration, e.g.: permissions. [java] Exception in thread "main" java.security.InvalidParameterException: Host 138.120.yy.zz is unknown - java.net.UnknownHostException: 138.120.yy.zz. This may be due to a firewall blocking requests or a specific server configuration, e.g.: permissions.	The cluster member node identified by the IP address specified is not reachable. This may be for one of the following reasons: • The host is not online • A firewall is blocking access to the host • The IP address of the host is incorrect • The host is configured to not respond to ICMP ping requests
Apr 11, 2011 3:53:46 PM oracle.jdbc.driver.OracleDriver registerMBeans WARNING: Error while registering Oracle JDBC Diagnosability MBean. java.security.AccessControlException: access denied (javax.management.MBeanTrustPermission register) at java.security.AccessControlContext.checkPermission(Unknown Source) at java.lang.SecurityManager.checkPermission(Unknown Source) at com.sun.jmx.interceptor.DefaultMBeanServerInterceptor.checkMBeanTrustPermission(Unknown Source) at com.sun.jmx.interceptor.DefaultMBeanServerInterceptor.registerMBean(Unknown Source) at com.sun.jmx.mbeanserver.JmxMBeanServer.registerMBean(Unknown Source) at oracle.jdbc.driver.OracleDriver.registerMBeans(OracleDriver.java:360) at oracle.jdbc.driver.OracleDriver$1.run(OracleDriver.java:199) at java.security.AccessController.doPrivileged(Native Method) at oracle.jdbc.driver.OracleDriver.<clinit>(OracleDriver.java:195)	Produced in error and can be ignored. Displays in the Errors tab when installing Platform with Oracle JDBC d ojdbc6-11.2.0.2.0, and accurately reports that installation was success

Installation Error Message	Cause
Exception in thread "AWT-EventQueue-0" java.lang.ArrayIndexOutOfBoundsException: 32 at sun.font.FontDesignMetrics.charsWidth(Unknown Source) at javax.swing.text.Utilities.getTabbedTextOffset(Unknown Source) at javax.swing.text.Utilities.getTabbedTextOffset(Unknown Source) at javax.swing.text.Utilities.getTabbedTextOffset(Unknown Source) at javax.swing.text.PlainView.viewToModel(Unknown Source) at javax.swing.text.FieldView.viewToModel(Unknown Source) at javax.swing.plaf.basic.BasicTextUI$RootView.viewToModel(Unknown Source) at javax.swing.plaf.basic.BasicTextUI.viewToModel(Unknown Source)	Produced in error and can be ignored.
[loadfile] Unable to load file: java.io.FileNotFoundException: C:\ (The system cannot find the path specified)	Produced in error and can be ignored.
java.sql.SQLRecoverableException: IO Error: Connection reset	Related to the operation of the Oracle JDBC driver. Use t following workaround. Edit the <jdk>/jre/lib/security/java.security file: Change securerandom.source=file:/dev/urandom to securerandom.source=file:///dev/urandom.
The installer fails or gives the following error message: Caused by: java.security.AccessControlException: access denied ("javax.management.MBeanTrustPermission" "register")	To correct this error, go to the Java installation that is specified in the path included in the error message, or th Java installation defined as JAVA_HOME. To the java.policy file under jre/lib/security, add the following to granted permissions: permission java.util.PropertyPermission "javax.management.MBeanTrustPermission", "register"
C:\Users\<USERNAME>\AppData\Local\Temp\antinstall\ build.xml:189: The following error occurred while executing this line: C:\Users\<USERNAME>\AppData\Local\Temp\antinstall\ installer-common.xml:468: java.lang.NoClassDefFoundError: javax/xml/bind/DatatypeConverter at com.microsoft.sqlserver.jdbc.SQLServerConnection.sendLogon(SQLServerConnection.java:4061) …	Ensure that you are launching the installer with a suppo version of the Java Development Kit (JDK). You can type --version in a Windows command prompt window or in Linux terminal to see which version is currently configur your system. If you are using a Windows OS, add the Jav folder path to both JAVA_HOME and PATH in environment variables. If you use Red Hat Enterprise Linux, add the Ja JDK folder path to the PATH variable.

Deploying Advisors Genesys Adapter

You run a `.jar` installation file to deploy Advisors Genesys Adapter (AGA). The installation wizard 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 in the **Installer Screens** descriptions, below.

> **Important**
>
> In release 9.0, there are changes to the installation wizard screens; therefore, you cannot reuse your previous setup for silent installation or any saved `ant.install.properties` file.

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

The arrow icon in the following roadmap indicates where you are in the Advisors deployment process.

1. Install the databases that correspond to the Advisors products that you will deploy. Perform the database installation in the following order:

a. AGA metrics database

b. Grant `select` privileges on all AGA metrics views to the Platform user.

c. Metric Graphing database

d. Advisors Platform database
[+] REVIEW IMPORTANT INFORMATION HERE

If the Oracle Platform deployment script issues the following error, `ORA-20001: spCreateOneSourceView ORA-01031: insufficient privileges`, and you are sure that the Platform user has been issued all necessary privileges, then you might have role-based Oracle security set for the Platform user by your DBA. Make sure you take the deployment script from the **current_user** sub-folder in the installation package. You can apply the correct script on top of the one that you applied previously, ignoring the exceptions about existing objects and primary key violations. Alternatively, you can ask your DBA to recreate the user and the privileges and apply the correct script.

If your installation package does not contain a **current_user** folder, edit the following scripts by replacing all entries of `DEFINER` with `CURRENT_USER` and repeat the database deployment process.

- If initially you used `advisors-platform-<version>_Schema.sql` or `advisors-platform-<version>_ObjectsPlus.sql`, edit these scripts:
  `advisors-platform-<version>_CUSTOM_ROUTINE.sql`
  `advisors-platform-<version>_PIMPORT_xxx.sql`
  `advisors-platform-<version>_Routine1.sql`
- If initially you used `advisors-platform-<version>_ObjectsCustom.sql` or `advisors-platform-<version>_ObjectsDefault.sql`, this would be the only script to edit.

If you prefer, you can contact Genesys Support to obtain the edited scripts.

Alternatively, you can set up the enhanced Oracle security to run Advisors applications as an application user with least privileges. For instructions, see Least Privileges: How to Configure Advisors Database Accounts with Minimal Privileges.

If necessary, run the Advisors Object Migration utility. You must run the Advisors Object Migration utility when:

- You first install Advisors in an environment with a new Configuration Server or when you move an existing Advisors installation to a new Configuration Server.
- If any of the required Business Attributes folders that Advisors components use are not already present in the Configuration Server.
- If you decide to enable metrics that are not yet present in your Configuration Server.
- If you decide to use the Advisors default rollup configuration. Starting with Advisors release 9.0.001.06, a brand new Platform database contains a set of Advisors default hierarchy objects that must be added to the Configuration Server to make the automatic configuration visible on the dashboard. The automatic configuration consists of all base objects mapped to the default hierarchy. For more information, see Contact Center Advisor Default Rollup Configuration in the *Contact Center Advisor and Workforce Advisor Administrator User's Guide*.
- If you perform a new installation in an environment that previously had an Advisors release installed that was older than release 8.5.1. In this case, remove all FA metrics that are in the Configuration Server and then run the migration wizard to populate all FA and CCAdv metrics and hierarchy business attributes.

2. Create the Advisors User account in Genesys Configuration Server.
3. Install the Platform service on servers where it is required for Advisors components. The Platform service is a prerequisite for installing the following components:
   - Advisors Administration
   - Advisors Web Services
   - WA Server

- FA Server with rollup engine
- CCAdv/WA/FA Accessibility services
- CCAdv/WA Resource Management console

4.  Install each adapter that you will use and configure the adapter Application objects with Stat Server connections. See additional information for CCAdv/WA installations.
5. Install the Advisors components for your enterprise.
   - Contact Center Advisor server (CCAdv XML Generator)
   - Workforce Advisor server
   - Frontline Advisor server
   - SDS and the CCAdv/WA Resource Management console
6. Make any required configuration changes.

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

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

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`.

Deploying Advisors Genesys Adapter

Procedure:

Prerequisites

- Review the General Prerequisites and prerequisites specific to Advisors Genesys Adapter deployment before beginning deployment.

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. The following example uses `jdk1.8.0`. When you run the command in your environment, be sure to enter the JDK version number that you use in your installation.

   ```
   ./jdk1.8.0_<version>/bin/java -jar aga-installer-<version>.jar
   ```

   See the *Genesys Supported Operating Environment Reference Guide* for information about Java versions supported with each Advisors release.

   [+] 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 **Adapter Server** radio button.
3. Use the **Next** and **Back** buttons on the installer to navigate through the installation screens. Enter your information on each screen. Use the information provided in the Installation Screens section on this page to complete the remaining deployment screens. Ensure you provide complete information on each screen.
4. Click **Show Details** and verify that there were no errors reported during installation.

Installation Screens

[+] Adapter Metrics Database

On the **Adapter Metrics Database** screen, specify the parameters for the metrics database:

- `Database Server`—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 CCAdv/WA metrics database password is encrypted and saved in the `...\GCTI\Advisors\Genesys\Adapter\conf\ inf_genesys_importer.properties` file by default. To change the password, see Change Encrypted Passwords.

[+] Adapter Metrics Database - Advanced

You will see this screen only if you select Oracle as the database type and Advanced as the JDBC connectivity setup type on the RDBMS Type And JDBC Connectivity installer screen. On the **Adapter Metrics Database - 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).

Specify the following parameters for the metrics database:

- `Database user`—The Advisors user that will 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.

[+] 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.

[+] Advisors Platform Database

On the **Advisors Platform Database** 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 **Advisors Platform Database** 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/Service name`—The unique name of the database instance.
- `Database port`—The database server's port number.
- `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.

[+] Advisors Platform Database - Advanced

You will see this screen only if you select Oracle as the database type and Advanced as the JDBC connectivity setup type on the RDBMS Type And JDBC Connectivity installer screen. On the **Advisors Platform Database - 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).

Specify the following parameters for the Advisors Platform database:

- `Database user`—The database user created and used for the Platform 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.

[+] Genesys Config Server Connection Details

On the **Genesys Config Server Connection Details** 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:

- `Config Server name` – The name of the primary configuration server. The name is obtained from your Genesys configuration interface (for example, Genesys Administrator) 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 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.
- `Config Server client name` – 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 the Adapter will use to connect to the Configuration Server.
- `Config Server user 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.

[+] Backup Config Server

You see the **Backup Config Server** screen only if you opted to add a backup Configuration Server on the **Genesys Config Server Connection Details** 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 your Genesys configuration interface (for example, Genesys Administrator) and is case sensitive.
- `Backup server address` – 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 number` – 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.

[+] Log Files Directory

Starting with release 9.0.001, the installation wizard prompts you to provide the log file storage location, and provides a default path. If you plan to use a log file storage location that is not the default location, then specify the location on the **Log Files Directory** screen. The installation wizard checks that the selected storage directory is present; if not present, then the wizard creates it. The installation wizard stores the selected log file storage location in one of the following files:

- The properties file specific to the module that you are installing. The log file configuration file picks up the location from the module's properties file.
- The log4j configuration file.

Specifying the log file directory in the installation wizard will not change the directory that was set for previous installations.

For more information about log files, see Adjust Logging Settings and Configure Administrative Actions Logs.

[+] 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 the current release.

[+] 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 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 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 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

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

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

`[java] Exception while connecting: Login failed for user 'badUserId'.`
 	
`[java] url used: jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=ys_gadb;selectMethod=cursor;user=badUserId;password=very_secure_password`
	Wrong database user name or password

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

`C:\Users\<USERNAME>\AppData\Local\Temp\antinstall\ build.xml:189: The following error occurred while executing this line:`
 	
`C:\Users\<USERNAME>\AppData\Local\Temp\antinstall\ installer-common.xml:468: java.lang.NoClassDefFoundError: javax/xml/bind/DatatypeConverter at com.microsoft.sqlserver.jdbc.SQLServerConnection.terminate(SQLServerConnection.java:4061)`
	Ensure that you are launching the installer with a supported version of the Java Development Kit (JDK). You can type `java --version` in a Windows command prompt window or in the Linux terminal to see which version is currently configured on your system. If you are using a Windows OS, add the JDK folder path to both JAVA_HOME and PATH in environment variables. If you use Red Hat Enterprise Linux, add the JDK folder path to the PATH variable.

Installation Error Message	Cause
...	

Installing Stat Server Java Extensions

Starting with release 9.0, Advisors Genesys Adapter (AGA) supports additional Stat Server Java extensions. Prior to release 9.0, AGA supported the MCR (eServices) extensions only.

Starting with release 9.0, you can create custom metrics using other Stat Server extensions such as Outbound Contact Java Extension (OCCStatExtension) and Orchestration Server Extension (ORSStatExtension). For example, you can create Calling List custom metrics based on the Stat Server Outbound Contact Java Extension.

The eServices extensions are required for the default Interaction queue metrics. If you will create custom metrics that need the OCC and ORS extensions, then you must deploy the corresponding Stat Server extensions on your Advisors Stat Servers.

Use the following procedure to deploy the extensions. For additional information, also see Installing a Stat Server Application and Java Sections in the *Stat Server Deployment Guide*.

Procedure:

Steps

1. Install Stat Server.
2. Install the extension package(s) that you plan to use with Advisors.
3. Follow the instructions on the Java Sections page in the *Stat Server Deployment Guide* to install the Java extensions.
4. If you have installed the eServices extensions, then Genesys recommends that you also perform the following steps:
   - 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.
   - 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.
   - Restart both the Interaction Server and the Stat Server.

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)
- Workforce Advisor (WA)
- Resource Management console (RMC)

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.

> **Important**
>
> In release 9.0, there are changes to the installation wizard screens; therefore, you cannot reuse your previous setup for silent installation or any saved `ant.install.properties` file.

Deployment Roadmap

The arrow icons in the following roadmap indicate where you are in the Advisors deployment process.

1. Install the databases that correspond to the Advisors products that you will deploy. Perform the database installation in the following order:
   a. AGA metrics database
   b. Grant `select` privileges on all AGA metrics views to the Platform user.
   c. Metric Graphing database
   d. Advisors Platform database
      [+] REVIEW IMPORTANT INFORMATION HERE

      If the Oracle Platform deployment script issues the following error, `ORA-20001: spCreateOneSourceView ORA-01031: insufficient privileges`, and you are sure that the Platform user has been issued all necessary privileges, then you might have role-based Oracle security set for the Platform user by your DBA. Make sure you take the deployment script from the **current_user** sub-folder in the installation package. You can apply the correct script on top of the one that you applied previously, ignoring the exceptions about existing objects and primary key violations. Alternatively, you can ask your DBA to recreate the user and the privileges and apply the correct script.

      If your installation package does not contain a **current_user** folder, edit the following scripts by replacing all entries of `DEFINER` with `CURRENT_USER` and repeat the database deployment process.

      - If initially you used `advisors-platform-<version>_Schema.sql` or `advisors-platform-<version>_ObjectsPlus.sql`, edit these scripts: `advisors-platform-<version>_CUSTOM_ROUTINE.sql`

```
advisors-platform-<version>_PIMPORT_xxx.sql
advisors-platform-<version>_Routine1.sql
```

- If initially you used `advisors-platform-<version>_ObjectsCustom.sql` or `advisors-platform-<version>_ObjectsDefault.sql`, this would be the only script to edit.

If you prefer, you can contact Genesys Support to obtain the edited scripts.

Alternatively, you can set up the enhanced Oracle security to run Advisors applications as an application user with least privileges. For instructions, see Least Privileges: How to Configure Advisors Database Accounts with Minimal Privileges.

If necessary, run the Advisors Object Migration utility. You must run the Advisors Object Migration utility when:

- You first install Advisors in an environment with a new Configuration Server or when you move an existing Advisors installation to a new Configuration Server.
- If any of the required Business Attributes folders that Advisors components use are not already present in the Configuration Server.
- If you decide to enable metrics that are not yet present in your Configuration Server.
- If you decide to use the Advisors default rollup configuration. Starting with Advisors release 9.0.001.06, a brand new Platform database contains a set of Advisors default hierarchy objects that must be added to the Configuration Server to make the automatic configuration visible on the dashboard. The automatic configuration consists of all base objects mapped to the default hierarchy. For more information, see Contact Center Advisor Default Rollup Configuration in the *Contact Center Advisor and Workforce Advisor Administrator User's Guide*.
- If you perform a new installation in an environment that previously had an Advisors release installed that was older than release 8.5.1. In this case, remove all FA metrics that are in the Configuration Server and then run the migration wizard to populate all FA and CCAdv metrics and hierarchy business attributes.

2. Create the Advisors User account in Genesys Configuration Server.
3. Install the Platform service on servers where it is required for Advisors components. The Platform service is a prerequisite for installing the following components:
   - Advisors Administration
   - Advisors Web Services
   - WA Server
   - FA Server with rollup engine
   - CCAdv/WA/FA Accessibility services
   - CCAdv/WA Resource Management console
4. Install each adapter that you will use and configure the adapter Application objects with Stat Server connections. See additional information for CCAdv/WA installations.
5. Install the Advisors components for your enterprise:
   - Contact Center Advisor server (CCAdv XML Generator)
   - Workforce Advisor server
   - Frontline Advisor server
   - SDS and the CCAdv/WA Resource Management console
6. Make any required configuration changes.

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

Before starting the XML Generator component

It is necessary to perform this step when deploying Pulse Advisors release 9.0.003.11 with Oracle. After you have deployed all the database schemas and have run the Contact Center Advisor/ Workforce Advisor (CCAd/WA) installer, but before you start the XML Generator component for the first time, you must connect as the Advisors Platform schema owner and apply the `advisors-platform-<version>_ValidateDatabaseInstall.sql` script.

Deploying CCAdv, CCAdv XML Generator, and WA

Procedure:

Prerequisites

- Review the General Prerequisites and prerequisites specific to CCAdv/WA 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 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. The following example uses `jdk1.8.0`. When you run the command in your environment, be sure to enter the JDK version number that you use in your installation.

   ```
   ./jdk1.8.0_<version>/bin/java -jar ccadv-wa-installer-<version>.jar
   ```

   See the *Genesys Supported Operating Environment Reference Guide* for information about Java versions supported with each Advisors release.

[+] Show Step for Windows

Do one of the following:

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

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

For 64-bit systems, if double-clicking to launch the installer, 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 **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. CCAdv XML Generator runs independently of Advisors Platform.
   - CCAdv Accessibility Services—(Optional) If you need the CCAdv accessible dashboard, you can install this on one or more of the presentation nodes.
   - 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 Accessibility Services—(Optional) If you need the WA accessible dashboard, you can install this on one or more of the presentation nodes.
   - Resource Management Console—(Optional) If you need access to the Resource Management console in CCAdv and WA, you can install this on one or more of the presentation nodes.
3. 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.
4. Use the information provided in the Installation Screens section on this page to complete the remaining deployment screens.

Installation Screens

[+] Data Source

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

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

If you have additional data sources to add, select `Add another data source` and repeat this step.

Up to five data sources may be added using the installer.

[+] Database Type

Specify the type of database you use in your enterprise.

[+] Genesys Advisor Platform Database

Enter the database connectivity parameters for the already created or upgraded database (that is, the database must be present and at the current version prior to running the installer).

When using numerical IP addresses or names with dots in the installations with MS SQL, enclose the literal in brackets.

If the MS SQL database server is a named instance, then omit the port number and use double backslash: <host name>\\<instance name>

[+] 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 IP addresses or names with dots in the installations with MS SQL, enclose the literal in brackets.

If the MS SQL database server is a named instance, then omit the port number and use double backslash: <host name>\\<instance name>

[+] 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. To make a secure connection to the WFM Server, the base URL must include:
  - the https:// protocol (instead of http://)
  - the secure port number that is configured on the WFM Server
- Application name—The application name of the WFM server as configured in the Configuration Server or Genesys Administrator.
- User name—The user name with which WA Server will connect to Genesys WFM Server.
- Password—The password with which WA Server will connect to Genesys WFM Server.
- Polling interval (ms)—The interval at which the Genesys WFM Server 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 - Log Files Directory

Starting with release 9.0.001, the installation wizard prompts you to provide the log file storage location, and provides a default path. If you plan to use a log file storage location that is not the default location, then specify the location on the **Log Files Directory** screen. The installation wizard checks that the selected storage directory is present; if not present, then the wizard creates it. The installation wizard stores the selected log file storage location in one of the following files:

- The properties file specific to the module. The log file configuration file pick ups the location from the module's properties file.
- The log4j configuration file.

Specifying the log file directory in the installation wizard will not change the directory that was set for previous installations.

For more information about log files, see Adjust Logging Settings and Configure Administrative Actions Logs.

[+] XML Generator Page 2 - Config Server

CCAdv XML Generator runs independently of Advisors Platform; it is not 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 2 - 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 your Genesys configuration interface (for example, Genesys Administrator) 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`.

[+] XML Generator Page 3 - 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

[+] XML Generator Page 4 - Config Server

Enter the name of the default Genesys tenant.

[+] XML Generator Page 5 - SCS Integration

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

[+] 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 alertsFor 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 and WA Server store graphable snapshots no more often than that. However, they 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 CCAdv 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 Genesys Administrator.

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

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

`[java] Exception while connecting: Login failed for user 'badUserId'.`
 	
`[java] url used: jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=ys_eadb;selectMethod=cursor;user=badUserId; password=very_secure_password`
	Wrong database user name or password

`[loadfile] Unable to load file: java.io.FileNotFoundException: C:\ (The system cannot find the path specified)`	Produced in error and can be ignored.
An error message in the XML Generator log that contains the following string: `datamanager.adapters.MultiAdapterException`	Indicates that there is at least one (there might be more than one) configured Genesys Advisors Adapter (AGA) instance that is either not running or is not reachable. Genesys recommends the following actions to correct the condition: 1. Check all configured AGA instances. Make sure that each one is running and reachable from XML Generator. 2. If you have any AGA instances that are not absolutely

Installation Error Message	Cause
	required for the operation of CCAdv/WA, remove those from the configuration. If a configured adapter is reporting this error condition, and it is running correctly, then you need to look for other problems with the adapter. For example, the adapter Application that is registered in Configuration Server might not have any Stat Servers configured, or the configured Stat Server(s) might not be running.

`C:\Users\<USERNAME>\AppData\Local\Temp\antinstall\ build.xml:189: The following error occurred while executing this line:`
 	
`C:\Users\<USERNAME>\AppData\Local\Temp\antinstall\ installer-common.xml:468: java.lang.NoClassDefFoundError: javax/xml/bind/DatatypeConverter at com.microsoft.sqlserver.jdbc.SQLServerConnection.sendLogon(SQLServerConnection.java:4061) ...`
	Ensure that you are launching the installer with a supported version of the Java Development Kit (JDK). You can type `java --version` in a Windows command prompt window or in the Linux terminal to see which version is currently configured on your system. If you are using a Windows OS, add the JDK folder path to both JAVA_HOME and PATH in environment variables. If you use Red Hat Enterprise Linux, add the JDK folder path to the PATH variable.

Deploying Frontline Advisor

You run a `.jar` installation file to deploy Genesys Frontline Advisor (FA). The `fa-server-installer-<version>.jar` file installs the Frontline Advisor dashboard; you use Role-Based Access Control (RBAC) privileges to control the dashboard features that each user can see and use.

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

> **Important**
>
> In release 9.0, there are changes to the installation wizard screens; therefore, you cannot reuse your previous setup for silent installation or any saved `ant.install.properties` file.

Deployment Roadmap

The arrow icon in the following roadmap indicates where you are in the Advisors deployment process.

1. Install the databases that correspond to the Advisors products that you will deploy. Perform the database installation in the following order:
   a. AGA metrics database
   b. Grant `select` privileges on all AGA metrics views to the Platform user.
   c. Metric Graphing database
   d. Advisors Platform database
      [+] REVIEW IMPORTANT INFORMATION HERE

      If the Oracle Platform deployment script issues the following error, `ORA-20001: spCreateOneSourceView ORA-01031: insufficient privileges`, and you are sure that the Platform user has been issued all necessary privileges, then you might have role-based Oracle security set for the Platform user by your DBA. Make sure you take the deployment script from the **current_user** sub-folder in the installation package. You can apply the correct script on top of the one that you applied previously, ignoring the exceptions about existing objects and primary key violations. Alternatively, you can ask your DBA to recreate the user and the privileges and apply the correct script.

      If your installation package does not contain a **current_user** folder, edit the following scripts by replacing all entries of `DEFINER` with `CURRENT_USER` and repeat the database deployment process.

      - If initially you used `advisors-platform-<version>_Schema.sql` or `advisors-platform-<version>_ObjectsPlus.sql`, edit these scripts:
        `advisors-platform-<version>_CUSTOM_ROUTINE.sql`
        `advisors-platform-<version>_PIMPORT_xxx.sql`
        `advisors-platform-<version>_Routine1.sql`
      - If initially you used `advisors-platform-<version>_ObjectsCustom.sql` or `advisors-platform-<version>_ObjectsDefault.sql`, this would be the only script to edit.

      If you prefer, you can contact Genesys Support to obtain the edited scripts.

      Alternatively, you can set up the enhanced Oracle security to run Advisors applications as an application user with least privileges. For instructions, see Least Privileges: How to Configure Advisors Database Accounts with Minimal Privileges.

      If necessary, run the Advisors Object Migration utility. You must run the Advisors Object Migration utility when:

- You first install Advisors in an environment with a new Configuration Server or when you move an existing Advisors installation to a new Configuration Server.
- If any of the required Business Attributes folders that Advisors components use are not already present in the Configuration Server.
- If you decide to enable metrics that are not yet present in your Configuration Server.
- If you decide to use the Advisors default rollup configuration. Starting with Advisors release 9.0.001.06, a brand new Platform database contains a set of Advisors default hierarchy objects that must be added to the Configuration Server to make the automatic configuration visible on the dashboard. The automatic configuration consists of all base objects mapped to the default hierarchy. For more information, see Contact Center Advisor Default Rollup Configuration in the *Contact Center Advisor and Workforce Advisor Administrator User's Guide*.
- If you perform a new installation in an environment that previously had an Advisors release installed that was older than release 8.5.1. In this case, remove all FA metrics that are in the Configuration Server and then run the migration wizard to populate all FA and CCAdv metrics and hierarchy business attributes.

2. Create the Advisors User account in Genesys Configuration Server.
3. Install the Platform service on servers where it is required for Advisors components. The Platform service is a prerequisite for installing the following components:
   - Advisors Administration
   - Advisors Web Services
   - WA Server
   - FA Server with rollup engine
   - CCAdv/WA/FA Accessibility services
   - CCAdv/WA Resource Management console
4. Install each adapter that you will use and configure the adapter Application objects with Stat Server connections.
5. Install the Advisors components for your enterprise in the following order:
   - Contact Center Advisor server (CCAdv XML Generator)
   - Workforce Advisor server
   -  Frontline Advisor server
   - SDS and the CCAdv/WA Resource Management console
6. Make any required configuration changes.

Deploying the Frontline Advisor Application

Procedure:

Prerequisites

- Review the General Prerequisites and prerequisites specific to Frontline Advisor 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 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. The following example uses `jdk1.8.0`. When you run the command in your environment, be sure to enter the JDK version number that you use in your installation.

   ```
   ./jdk1.8.0_<version>/bin/java -jar fa-server-installer-<version>.jar
   ```

   See the *Genesys Supported Operating Environment Reference Guide* for information about Java versions supported with each Advisors release.

   [+] 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.

2. 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.
3. Use the information provided in the Installation Screens section on this page to complete the remaining deployment screens.
4. After you deploy FA, you must modify the Apache configuration file (`httpd.conf`). See Deploy

and Configure Apache.

Installation Screens

[+] 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 email 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

You will see this screen only if you select `Oracle` as the database type and `Advanced` as the JDBC connectivity setup type on the **RDBMS Type And JDBC Connectivity** installer screen. 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.
- The name of a `Person` folder in your Genesys configuration interface (for example, Genesys Administrator), 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 Advisors Application name exactly as it is configured in Genesys Configuration Server.

Start the FA Service

Procedure:

Steps

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. If you experience problems, check the Platform log file. It may take up to 45 minutes to fully start the FA service, depending on the number of agents and the complexity of the hierarchy.

Troubleshooting

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

Installation Error Message	Cause

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

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

`[java] Exception while connecting: Login failed for user 'badUserId'.`
 	
`[java] url used: jdbc:sqlserver://192.168.xx.yy:nnnn;DatabaseName=ys_fadb;selectMethod=cursor; user=badUserId;password=very_secure_password`
	Wrong database user name or password

`[loadfile] Unable to load file: java.io.FileNotFoundException: C:\ (The system cannot find the path specified)`	Produced in error and can be ignored.
An error message in the FA log that contains the following string: `datamanager.adapters.MultiAdapterException`	Indicates that there is at least one (there might be more than one) configured Genesys Advisors Adapter (AGA) instance that is either not running or is not reachable. Genesys recommends the following actions to correct the condition: 1. Check all configured AGA instances. Make sure that each one is running

Installation Error Message	Cause
	and reachable from FA. 2. If you have any AGA instances that are not absolutely required for the operation of FA, remove those from the configuration. If a configured adapter is reporting this error condition, and it is running correctly, then you need to look for other problems with the adapter. For example, the adapter Application that is registered in Configuration Server might not have any Stat Servers configured, or the configured Stat Server(s) might not be running.
`C:\Users\<USERNAME>\AppData\Local\Temp\antinstall\ build.xml:189: The following error occurred while executing this line:` `C:\Users\<USERNAME>\AppData\Local\Temp\antinstall\ installer-common.xml:468: java.lang.NoClassDefFoundError: javax/xml/bind/DatatypeConverter at com.microsoft.sqlserver.jdbc.SQLServerConnection.sendLogon(SQLServerConnection.java:4061) ...`	Ensure that you are launching the installer with a supported version of the Java Development Kit (JDK). You can type `java --version` in a Windows command prompt window or in the Linux terminal to see which version is currently configured on your system. If you are using a Windows OS, add the JDK folder path to both JAVA_HOME and PATH in environment variables. If you use Red Hat Enterprise Linux, add the JDK folder path to the PATH variable.

Deploying SDS and RMC

Use the procedures on this page to deploy Supervisor Desktop Service (SDS) and the Resource Management console (RMC).

Deployment Roadmap

The arrow icon in the following roadmap indicates where you are in the Advisors deployment process.

1. Install the databases that correspond to the Advisors products that you will deploy. Perform the database installation in the following order:
   a. AGA metrics database
   b. Grant `select` privileges on all AGA metrics views to the Platform user.
   c. Metric Graphing database
   d. Advisors Platform database
   [+] REVIEW IMPORTANT INFORMATION HERE

   If the Oracle Platform deployment script issues the following error, `ORA-20001: spCreateOneSourceView ORA-01031: insufficient privileges`, and you are sure that the Platform user has been issued all necessary privileges, then you might have role-based Oracle security set for the Platform user by your DBA. Make sure you take the deployment script from the **current_user** sub-folder in the installation package. You can apply the correct script on top of the one that you applied previously, ignoring the exceptions about existing objects and primary key violations. Alternatively, you can ask your DBA to recreate the user and the privileges and apply the correct script.

   If your installation package does not contain a **current_user** folder, edit the following scripts by replacing all entries of `DEFINER` with `CURRENT_USER` and repeat the database deployment process.

   - If initially you used `advisors-platform-<version>_Schema.sql` or `advisors-platform-<version>_ObjectsPlus.sql`, edit these scripts:
     `advisors-platform-<version>_CUSTOM_ROUTINE.sql`
     `advisors-platform-<version>_PIMPORT_xxx.sql`
     `advisors-platform-<version>_Routine1.sql`
   - If initially you used `advisors-platform-<version>_ObjectsCustom.sql` or `advisors-platform-<version>_ObjectsDefault.sql`, this would be the only script to edit.

   If you prefer, you can contact Genesys Support to obtain the edited scripts.

   Alternatively, you can set up the enhanced Oracle security to run Advisors applications as an application user with least privileges. For instructions, see Least Privileges: How to Configure Advisors Database Accounts with Minimal Privileges.

   If necessary, run the Advisors Object Migration utility. You must run the Advisors Object Migration utility when:

   - You first install Advisors in an environment with a new Configuration Server or when you move an existing Advisors installation to a new Configuration Server.
   - If any of the required Business Attributes folders that Advisors components use are not already present in the Configuration Server.
   - If you decide to enable metrics that are not yet present in your Configuration Server.
   - If you decide to use the Advisors default rollup configuration. Starting with Advisors release 9.0.001.06, a brand new Platform database contains a set of Advisors default hierarchy objects that must be added to the Configuration Server to make the automatic configuration visible on the dashboard. The automatic configuration consists of all base objects mapped to the default

hierarchy. For more information, see Contact Center Advisor Default Rollup Configuration in the *Contact Center Advisor and Workforce Advisor Administrator User's Guide*.

- If you perform a new installation in an environment that previously had an Advisors release installed that was older than release 8.5.1. In this case, remove all FA metrics that are in the Configuration Server and then run the migration wizard to populate all FA and CCAdv metrics and hierarchy business attributes.

2. Create the Advisors User account in Genesys Configuration Server.
3. Install the Platform service on servers where it is required for Advisors components. The Platform service is a prerequisite for installing the following components:
   - Advisors Administration
   - Advisors Web Services
   - WA Server
   - FA Server with rollup engine
   - CCAdv/WA/FA Accessibility services
   - CCAdv/WA Resource Management console
4. Install each adapter that you will use and configure the adapter Application objects with Stat Server connections.
5. Install the Advisors components for your enterprise:
   - Contact Center Advisor server (CCAdv XML Generator)
   - Workforce Advisor server
   - Frontline Advisor server
   -  SDS and the CCAdv/WA Resource Management console
6. 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.

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:

- When connecting SDS to a Configuration Server proxy, SDS supports a connection only to non-secure ports of the proxy server.
- Supervisor Desktop Service SDS is available in both 32-bit and 64-bit versions.
- When installing Java for SDS, use the following table as a guide. Follow this basic rule: On Windows, if the SDS is 32-bit, use 32-bit Java. If SDS is 64-bit, use 64-bit Java. On Linux, the SDS server for Linux is independent of the distribution of Java in this respect.

Operating System	SDS Version	Java 32 or 64
Linux 32- or 64-bit	7.6.300.11 or 7.6.300.12	Java 1.8.x 32-bit/Java 1.8.x 64-bit
Windows 32-bit	7.6.300.11 32-bit	Java 1.8.x 32-bit

Operating System	SDS Version	Java 32 or 64
Windows 64-bit	7.6.300.11 64-bit, or 7.6.300.12 64-bit	Java 1.8.x 64-bit

- Contact Center Advisor release 9.0 requires SDS release 7.6.300.11 or higher, and is not compatible with earlier SDS releases. See the SDS Release Note for information that can help you to select the SDS release that is right for your environment.
- 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.
- If you use the Resource Management Console in Contact Center Advisor and/or Workforce Advisor, 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.

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.

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. Deploy Supervisor Desktop Service on a supported Windows or Linux operating system. Use one of the following procedures:
   - Procedure: Deploying Supervisor Desktop Service on Windows
   - Procedure: Deploying Supervisor Desktop Service on Linux
3. Complete the Supervisor Desktop Service configuration.

   See Procedure: Completing the Supervisor Desktop Service Configuration.
4. Deploy the Resource Management Console on a supported Windows or Linux operating system.

   See Procedure: Deploying the Resource Management Console.
5. Configure the Resource Management Console. See Procedure: Configuring the Resource Management Console.

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-server.com	The From address used for all Resource Management notification e-mail messages.
email-server	email-server@domainname.com	The mail server name.
email-server-port	25	The default SMTP port.
email-user	sds.email.account	The user account for the e-mail server. Ignored if email-authenticate is set to off.
email-authenticate		Does the e-mail server require authentication? Valid values are on or off.
email-use-SSL		Does the e-mail server use SSL? Valid values are on or off.
password		The password for the e-mail server. Ignored if email-authenticate is set to off.

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.
6. Save the Application.
7. 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

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: 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

Steps

1. If an older version of SDS is already installed, you must uninstall it.
   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. 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 Pulse Advisors Hardware Sizing Guide*.
4. 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 Contact Center Advisor/Workforce Advisor (CCAdv/WA) installation file.
   [+] Show Steps for Linux

   a. Navigate to the Advisors home directory:

   ```
   cd /home/advisors
   ```

   b. 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. The following example uses `jdk1.8.0`. When you run the command in your environment, be sure to enter the JDK version number that you use in your installation.

   ```
   ./jdk1.8.0_<version>/bin/java -jar ccadv-wa-installer-<version>.jar
   ```

   See the *Genesys Supported Operating Environment Reference Guide* for information about Java versions supported with each Advisors release.

   [+] Show Steps for Windows

   Do one of the following:

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

     ```
     java -jar ccadv-wa-installer-<version>.jar
     ```

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

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

   For 64-bit systems, if double-clicking to launch the installer, 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 **Modules to Install** screen, select the `Resource Management Console` checkbox. Genesys recommends that you install RMC after all other Advisors components are installed and working.
3. Enter the following information on subsequent screens:
   - On the **Destination Directory** screen, select the base location of the Advisors installation (that is, the base directory where the Platform components and Tomcat are installed). In most cases, this is `C:\Program Files\GCTI\Advisors`, which is the default location.
   - 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.
   - 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 server`—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 CCAdv/WA 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 JDBC URL (you should have the freeform JDBC URL in a text file). The installer applies the specified freeform JDBC URL when configuring the datasources. If you do not know the location of the JDBC URL, contact your database administrator.

- On the **Resource Management Console** screen, enter the IP address of the SDS server, as well as the port number for the SDS path (the default port number is 8080).

4. After you have entered information on all installer screens, click **Install**.
5. Click **Show Details**. Use the **Errors** tab to verify that no errors were reported during installation.

Next Steps

See Procedure: Configuring the Resource Management Console.

Procedure: Configuring the Resource Management Console

Steps

1. **Configure the RMC properties file**

   After RMC has installed successfully, you can edit the `Advisors\conf\RMC.properties` configuration file. For example, you might want to change the maximum skill level, the refresh interval, and/or the number of concurrent users properties. See Configure Resource Management Console Properties for more information.

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 Platform 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 Platform servers**

   Restart every Platform server for which you changed either the `RMC.properties` properties or the `ActiveMQ.properties` file.
   If the Platform 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 Platform server.
   - On a Linux host machine:
     - If you have not configured Advisors Platform to start as a service, then from the `/bin` folder, execute `./shutdown.sh` and then `./startup.sh` to stop and restart the Platform server.
     - If you have configured Advisors Platform to start as a service, then stop and start the Linux service that controls Advisors Platform.

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.

Post Installation Configuration

You perform initial Pulse 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 Pulse Advisors after the Advisors modules are deployed.

Cold Standby Configuration and Switchover

Pulse 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 (AGA)) 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 (AGA). 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 (AGA) 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 `RMC.properties` file in Advisors/conf to point to the new SDS instance. Instructions are available in the Deploying SDS and RMC section of the *Pulse Advisors Deployment Guide*.

If your Advisors deployment uses RMC, Genesys strongly advises you to install the Advisors 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

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

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/8/docs/technotes/tools/windows/java.html for Windows environments or http://docs.oracle.com/javase/8/docs/technotes/tools/unix/java.html for Linux environments.

Change Memory Allocation for Advisors Platform

The following sections describe changes that you can make to the memory allocation for Advisors Platform:

- Advisors Server Controlled By Solution Control Server
- Advisors Server Controlled By Windows or Linux Service

Advisors Server Controlled by Solution Control Server

This section describes which memory allocation settings to edit 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.

Consider changing the memory allocation for the Advisors Platform server if the `advisors.log` file for the Advisors server is recording an out-of-memory error. Edit the `CATALINA_OPTS= ... -ms` and `-mx` values in one of the following files to increase the heap size:

- On Windows, `apache-tomcat-<version>\bin\setenv.bat`
- On Linux, `apache-tomcat-<version>/bin/setenv.sh`

See the *Genesys Pulse Advisors Hardware Sizing Guide* for memory allocation recommendations.

> **Tip**
> Java out-of-memory errors can also occur due to insufficient operating system (OS) resources or thread stack resources (rather than heap) exhausting available JVM memory. Reviewing the configuration of your JVM and OS resources, and adjusting if necessary to ensure availability of resources, can prevent or fix such errors. For

> example, consider reviewing your ulimit configuration (nproc process limits, file descriptors, and so on) and Java thread stack size.

Advisors Server Controlled by Windows Service

This section describes which memory allocation settings to edit for an Advisors server that is controlled by an OS service (that is, a server that is not controlled by SCS). For a list of the components that are controlled by an OS service, see Integration with Solution Control Server and Warm Standby.

To change memory allocation settings, edit the `<install dir>/bin/service.bat` file. Towards the end of the file, locate the `--JvmMs` and `--JvmMx` settings. Edit the values, particularly the `--JvmMx` value, to increase the heap size.

See the *Genesys Pulse Advisors Hardware Sizing Guide* for memory allocation recommendations.

Change Memory Allocation for Advisors Genesys Adapter

Consider changing the memory allocation for Advisors Genesys Adapter (AGA) if the AGA log file is recording an out-of-memory error. Edit the `JAVA_OPTS=-ms` and `-mx` values in one of the following files to increase the heap size:

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

See the *Genesys Pulse Advisors Hardware Sizing Guide* for memory allocation recommendations.

Change Memory Allocation for CCAdv XML Generator

Consider changing the memory allocation for CCAdv XML Generator if the XML Generator log file is recording an out-of-memory error.

Edit the `.../java" -server -ms` and `-mx` values in one of the following files to increase the heap size:

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

See the *Genesys Pulse Advisors Hardware Sizing Guide* for memory allocation recommendations.

Change Encrypted Passwords

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

Procedure:

Steps

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.

Important

You cannot use this utility to change the password that is used to connect to the WA Server with FTP. To change this password, see Importing Contact Groups into Advisors.

Switching Advisors Oracle database connectivity from JDBC thin driver to Oracle Call Interface (OCI)

If you prefer using Oracle OCI for connectivity between Advisors and Oracle database, you need to perform the standard installation procedure with Oracle JDBC thin driver and then switch to OCI by applying a post-installation procedure presented below.

Genesys recommends that you have deployed (or migrated) your Advisors installation using procedures described in this document and in the *Genesys Pulse Advisors Migration Guide*, and verified that the Advisors installation is working correctly, before proceeding with the procedures described on this page.

Download and Install the Oracle Instant Client

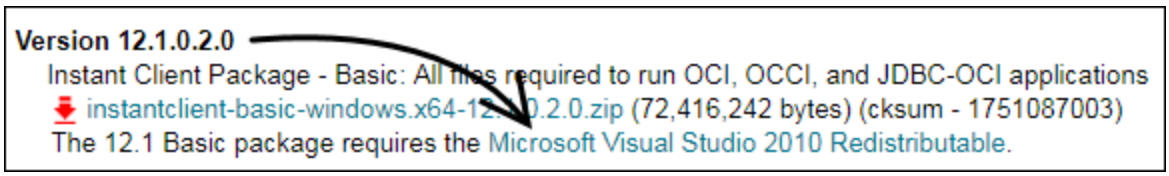
You must install the Oracle Instant Client on each machine in an Advisors installation (that is, all Platform, XML Generator, Frontline Advisor (FA), Workforce Advisor (WA), and Advisors Genesys Adapter (AGA) machines).

Go to the Instant Client Downloads page on the Oracle website. Click the link that matches your system type (for example, Instant Client for Linux x86-64). Choose "Accept License Agreement" at the top of the page, and then download the Instant Client Package (an .rpm file for Linux or a .zip file for Windows) for your target Oracle and operating system version. For example, if your Oracle version is 12.1.x, then select the Instant Client Package that matches the 12.1.x version.

In addition to downloading the Instant Client Package, you can also download the SQL*Plus package that goes with your version of the Instant Client. Downloading the SQL*Plus package is optional, but SQL*Plus is useful for testing the OCI connection to an Oracle database. In fact, using SQL*Plus to test the OCI connections is part of the process described on this page.

Installation on Windows systems

On Windows-based machines, in addition to installing the Oracle Instant Client, you must also download and install the correct version of Microsoft Visual Studio Redistributable. You can find information about the required Microsoft Visual Studio Redistributable under each Instant Client Package on the *Instant Client Downloads for Microsoft Windows* page on the Oracle Web site. For example:



On a Windows server, extract the Instant Client Package zipped files to the desired directory, and then add the path to the PATH system variable. For example:
```
C:\>set PATH=C:\instantclient_12_1;%PATH%
```

Make sure that the path is correct, and that no other PATH variable entry preceding this one ends in a slash (/) character. If one exists, then delete the slash character.

Installation on Linux systems

To install the Oracle Instant Client on a Linux system, navigate to the folder where you downloaded the Instant Client package and execute the .rpm package. This example assumes that you are using a 12.1 version of Oracle; be sure to use the proper version and path for your system:
```
rpm -i oracle-instantclient12.1-basic-12.1.0.2.0-1.x86_64.rpm
```

If you are installing SQL*Plus, then also execute the following command; again, be sure to use the proper version and path for your system:
```
rpm -i oracle-instantclient12.1-sqlplus-12.1.0.2.0-1.x86_64.rpm
```

Run the following two commands to export paths to the PATH variables.Once again, this example assumes that you are using a 12.1 version of Oracle; be sure to use the proper version and path for your system.
```
export LD_LIBRARY_PATH=/usr/lib/oracle/12.1/client64/lib
export PATH=/usr/lib/oracle/12.1/client64/bin:$PATH
```

Alternatively, you can edit profile files to permanently set the OCI path.

Using a TNS alias to connect to an Oracle system

The following example assumes that you are using a 12.1 version of Oracle; be sure to use the proper version and path for your system.

To use a TNS alias to connect from an Advisors application or from SQL*Plus to an Oracle database:

1. On Linux systems, create a `network/admin` directory under `/usr/lib/oracle/12.1/client64/`, or on Windows systems, create a `network\admin` directory under the `\instantclient_12_1` folder.
2. Add your `tnsnames.ora` file to the `admin` folder. The `tnsnames.ora` file must contain your Oracle database connection descriptors that point to the databases to which you intend to connect.

If you intend to use a TNS alias to connect to the database from an Advisors application, then Genesys strongly recommends that you place the tnsnames.ora file in the location mentioned above. Otherwise there is no guarantee that it will be possible to start the application from the Configuration Server Applications list.

The following is an example of a `tnsnames.ora` descriptor entry:

```
sales.example.com =(DESCRIPTION= (CONNECT_TIMEOUT=10)(RETRY_COUNT=3)
(ADDRESS_LIST= (LOAD_BALANCE=on)(FAILOVER=ON)
(ADDRESS=(PROTOCOL=tcp)(HOST=sales1-scan)(PORT=1521))
(ADDRESS=(PROTOCOL=tcp)(HOST=sales2-scan)(PORT=1521)))
(CONNECT_DATA=(SERVICE_NAME= salesservice.example.com)))
```

Test Connectivity Between the Advisors Applications and the Oracle Databases

If you have installed SQL*Plus, then you can now use it to test the client connectivity to the database. Genesys recommends that you verify that the client-database connectivity is successful before you update the Advisors applications to use the OCI instead of the JDBC driver.

Example for Linux systems

The following example assumes that you are using a 12.1 version of Oracle; be sure to use the proper version and path for your system.

```
[root@vce-u0000 tmp]# export LD_LIBRARY_PATH=/usr/lib/oracle/12.1/client64/lib
[root@vce-u0000 tmp]# export PATH=/usr/lib/oracle/12.1/client64/bin:$PATH
[root@vce-u0000 tmp]# sqlplus adv_mg_852/password@'(DESCRIPTION =(ADDRESS_LIST = (ADDRESS =
(PROTOCOL = TCP)(HOST = sales-s.example.com.com)(PORT = 1522)))(CONNECT_DATA =(SERVICE_NAME =
salesservice.example.com)))'
```

Example for Windows systems

```
C:\> sqlplus adv_mg_852/password@sales-s.example.com/salesservice.example.com
```

Adjust the Advisors Database Connection Strings to use the OCI Driver

After you have installed the Advisors applications on servers, using normal procedures, make the following adjustments for each Advisors component:

- Advisors Platform installations:
  - In the `[advisors]\apache-tomcat-<version>\conf` folder, open the `Catalina.properties` file, and edit it. Update all of the JDBC URIs by replacing `:thin:` with `:oci:` in each JDBC string.
  - In the `[advisors]\apache-tomcat-<version>\bin` folder, edit the `setenv.bat` file (Windows systems) or `setenv.sh` file (Linux systems) to add the following string near the top of the file, before the JAVA path command (these are example values – make sure the path is correct for your system):

    Windows systems: `set PATH=C:\instantclient_12_1;%PATH%`

    Linux systems: `export LD_LIBRARY_PATH=/usr/lib/oracle/12.1/client64/lib`

- XML Generator installations:
  - In the `/conf` folder, find the `xmlgen.properties` file, and edit it. Update all of the JDBC URIs by replacing `:thin:` with `:oci:`, as you did for Advisors Platform installations, above.
  - Under the `/xmlgen` folder, edit the `run.bat` file (Windows systems) or `run.sh` file (Linux systems) to add the following string near the top of the file, before the JAVA path command (these are example values – make sure the path is correct for your system):
    Windows systems: `set PATH=C:\instantclient_12_1;%PATH%`

    Linux systems: `export LD_LIBRARY_PATH=/usr/lib/oracle/12.1/client64/lib`
- Advisors Genesys Adapter (AGA) installations:
  - In the `/conf` folder, edit the `inf_genesys_adapter.properties` file to update the JDBC URIs as described above for both Advisors Platform and XML Generator installations (replace `:thin:` with `:oci:`).
  - If the AGA supports Contact Center Advisor (CCAdv), then also in the `/conf` folder, edit the `inf_genesys_importer.properties` file to update the JDBC URIs as described above for both Advisors Platform and XML Generator installations (replace `:thin:` with `:oci:`). This does not apply to an AGA that supports Frontline Advisor (FA).
  - In the `/bin` folder, edit the `run.bat` file (Windows systems) or `setenv.sh` file (Linux systems). Add the OCI path to this file, above the JAVA path command (these are example values – make sure the path is correct for your system):
    Windows systems: `set PATH=C:\instantclient_12_1;%PATH%;`

    Linux systems: `export LD_LIBRARY_PATH=/usr/lib/oracle/12.1/client64/lib`

Deploy and Configure Apache

Use the information on this page to configure an Apache Web Server instance to direct HTTP requests to the appropriate server within your Advisors deployment.

Genesys strongly recommends that you configure Apache to accept HTTP over SSL (HTTPS) connections. The streaming protocols used by Advisors are not required to be encrypted, but this is a more secure form of communication, and helps prevent possible interference from legacy virus scanners, firewalls, proxies, and so on, which don't properly support streaming protocols and might attempt to buffer unencrypted traffic. Using HTTPS connections helps to ensure both the security and reliability of the connection to the Advisors server. Requests between Apache and the Tomcat server running Advisors can also use HTTPS connections if needed.

Configure Apache Modules

The recommended Advisors Apache configuration requires the following modules:

- ssl
- headers
- proxy
- proxy_ajp
- proxy_http
- proxy_wstunnel

To enable Apache modules, edit the relevant file or use the relevant configuration tools for your environment. In many installations, this will involve editing your `httpd.conf` file. For more information on the files used to configure Apache, see the Apache documentation describing the files used to configure Apache.

For example, to use the SSL module, uncomment that line:

Uncomment this line:
```
#LoadModule ssl_module modules/mod_ssl.so
```

It now looks like this:
```
LoadModule ssl_module modules/mod_ssl.so
```

Configure HTTPS

To configure Apache to support HTTPS:

- Obtain or generate the SSL security certificate and private key.
- Configure Apache to use your certificate.

Obtaining a Certificate

An SSL certificate signing request (CSR) can be generated and submitted to a certificate authority using OpenSSL or a similar tool. You can then issue a certificate if you are your own certificate authority, or a certificate can be issued by a third-party certificate authority.

The OpenSSL req command can be used to generate the request, or to generate a self-signed certificate in a single step. For more information, see the OpenSSL documentation.

Configure Apache to use your Certificate

In general, to configure Apache to use your certificate, add the following configuration to the Apache virtual host that is used for Advisors, and for the port on which HTTPS connections are accepted (the default HTTPS port is 443):

```
SSLEngine on
SSLCertificateFile      /path/to/your/certificate.pem
SSLCertificateKeyFile /path/to/your/certificate.key
```

For example, to configure the certificate globally in Apache, use the following configuration:

```
<VirtualHost *:443>
SSLEngine on
SSLCertificateFile      /path/to/your/certificate.pem
SSLCertificateKeyFile /path/to/your/certificate.key
</VirtualHost>
```

For more information about virtual hosts, see the Apache virtual host documentation.

Configure Routing for Advisors Components

Advisors components can be distributed across many servers. The Apache configuration enables proper routing of requests to these components. In some cases, there might be multiple installations of the same component. In these cases, requests can be load-balanced to different Apache servers, each one directing these requests to different servers.

Each Advisors component routing entry in the Apache configuration directs its request to <*hostname*> (see the configuration example below). In your configuration, change <*hostname*> to the host name of the server on which the component is installed. This will vary depending on your particular installation. Note that requests are matched to the first ProxyPass entry in the order in which they are listed within the Apache configuration, so Genesys recommends that you add the routing information in the same order that is outlined in the following configuration example.

Template Configuration Example

In the following template configuration example, the text might wrap to multiple lines, but each ProxyPass directive must be on a single line in the Apache configuration.

Also take care to use the appropriate port for the URL and its protocol being proxied. In this example, requests to Tomcat over AJP use port 8009 while websocket communication uses HTTP port 8080. The specific ports used might vary depending on your Tomcat configuration, if modified from the default.

If you have Pulse Advisors release 9.0.003.09 or higher installed, also see Configuring Tomcat AJP connector.

```
#Route to resource management console
ProxyPass /rmc/ ajp://<hostname>:8009/rmc/

#Route to CCAdv accessibility web services
ProxyPass /ca-xml/ ajp://<hostname>:8009/ca-xml/

#Route to Workforce accessibiltiy web services
ProxyPass /wu/ ajp://<hostname>:8009/wu/

#Route to Advisors metric graphing
ProxyPass /ea-ws/ ajp://<hostname>:8009/ea-ws/
ProxyPass /dashboard/ ajp://<hostname>:8009/dashboard/

#Route to Advisors administration module
ProxyPass /admin ajp://<hostname>:8009/admin

#Route to FA server
ProxyPass /fa/com.informiam.fa.admin.gwt.AdminConsole/ ajp://<hostname>:8009/fa/
com.informiam.fa.admin.gwt.AdminConsole/ timeout=86400
ProxyPass /fa/ ajp://<hostname>:8009/fa/

#Route to Advisors web services
ProxyPass /adv/websocket/wsconnection/info ajp://<hostname>:8009/adv/websocket/wsconnection/
info
ProxyPassMatch /adv/websocket/wsconnection/(.*)/(.*)/websocket ws://<hostname>:8080/adv/
websocket/wsconnection/$1/$2/websocket
ProxyPass /adv/ ajp://<hostname>:8009/adv/

#Route to Advisors platform installation
ProxyPass /base-ws/ ajp://<hostname>:8009/base-ws/
ProxyPass /nav-service/ ajp://<hostname>:8009/nav-service/
ProxyPass /prefs-service/ ajp://<hostname>:8009/prefs-service/
ProxyPass / ajp://<hostname>:8009/
```

Routing With HTTPS Connections From Apache

In addition to configuring HTTPS connections for incoming requests to Apache, as described in the Configure HTTPS section, you can also configure an HTTPS connection between Apache and Tomcat. To do this, you must update the following information in the ProxyPass entries that route requests:

- Use the HTTPS and WSS protocols, which replace AJP and WS.
- Specify the port. By default, the Tomcat HTTPS connector is configured to use port 8443.

The Tomcat HTTPS connector can be used on port 8443 without any additional configuration. If you

will not be using the default configuration, see the documentation that describes how to customize the configuration of the Tomcat HTTPS connector.

[+] Example HTTPS Routing Configuration

```
#Route to resource management console
ProxyPass /rmc/ https://<hostname>:8443/rmc/

#Route to CCAdv accessibility web services
ProxyPass /ca-xml/ https://<hostname>:8443/ca-xml/

#Route to Workforce accessibiltiy web services
ProxyPass /wu/ https://<hostname>:8443/wu/

#Route to Advisors metric graphing
ProxyPass /ea-ws/ https://<hostname>:8443/ea-ws/
ProxyPass /dashboard/ https://<hostname>:8443/dashboard/

#Route to Advisors administration module
ProxyPass /admin https://<hostname>:8443/admin

#Route to FA server
ProxyPass /fa/com.informiam.fa.admin.gwt.AdminConsole/ https://<hostname>:8443/fa/com.informiam.fa.admin.gwt.AdminConsole/ timeout=86400
ProxyPass /fa/ https://<hostname>:8443/fa/

#Route to Advisors web services
ProxyPass /adv/websocket/wsconnection/info https://<hostname>:8443/adv/websocket/wsconnection/info
ProxyPassMatch /adv/websocket/wsconnection/(.*)/(.*)/websocket wss://<hostname>:8443/adv/websocket/wsconnection/$1/$2/websocket
ProxyPass /adv/ https://<hostname>:8443/adv/

#Route to Advisors platform installation
ProxyPass /base-ws/ https://<hostname>:8443/base-ws/
ProxyPass /nav-service/ https://<hostname>:8443/nav-service/
ProxyPass /prefs-service/ https://<hostname>:8443/prefs-service/
ProxyPass / https://<hostname>:8443/
```

Configuring Tomcat AJP connector

Applicable only to release 9.0.003.09 and higher.

Starting with release 9.0.003.09, Advisors Platform includes Tomcat server version 9.0.33 to address a potential security vulnerability with AJP requests. For details, see Injection and potential Remote Code Execution (CVE-2020-1938). As a result of this upgrade, you need to do the following Pulse Advisors configuration:

- On the Platform installation of the Advisors web services, edit the `apache-tomcat-9.0.12/conf/server.xml` file to add the following attribute in the AJP connector section: `secret="your_secret"`. The value of `secret` is a validation key between Apache and Tomcat. For example:

```
<Connector port="${AJPPort}" protocol="AJP/1.3"

      connectionTimeout="${WebConnectorConnTimeout}"

      maxThreads="${MaxThreadPoolSize}" maxConnections="${MaxThreadPoolSize}"
minSpareThreads="${MinThreadPoolSize}"

      redirectPort="${HTTPSPort}" relaxedQueryChars="[,]" secret="your_secret"
address="TOMCAT_HOST_IP"/>
```

- If the Apache HTTP Server and Tomcat are on different hosts, then you must add an attribute of `address="TOMCAT_HOST_IP"` to the AJP connector section as well. See the preceding example. For detailed information, see Tomcat configuration documentation.
- The Apache HTTP Server Proxy configuration needs to be updated to pass the configured secret in each of the ProxyPass directives. For example, here is an updated Proxypass directive (do not enclose the `secret` string in quotation marks):

  ```
  ProxyPass / ajp://<hostname>:8009/ secret=your_secret
  ```

  The addition of the secret to the ProxyPass directive is supported starting with Apache Web Server 2.4.42.

  For details, see Apache mod_proxy_ajp configuration.

Customizing the Tomcat HTTPS Connector

The Tomcat installation includes, by default, a self-signed certificate in the Java keystore file configured for the HTTPS connector. As a result, and without any additional configuration, you can use the HTTPS connector to accept SSL-encrypted HTTP requests from users directly and/or through Apache, as described in the documentation detailing how to configure Apache to use HTTPS when routing requests to the Advisors Tomcat server.

Although it should not be necessary to change this configuration, you might want to change it if you are planning to either use a different port to accept HTTPS connections, or to use a different certificate, such as one signed by a third-party certificate authority or an internal certificate authority.

Procedure: Steps to Replace the Default Keystore for Tomcat HTTPS Connector

Steps

1. Prepare a certificate keystore using the instructions from the Apache Tomcat 8.0 documentation.
2. Edit the HTTPS connector configuration. The connector configuration is found in the installation `apache-tomcat-<version>/conf/` directory `server.xml` file:

```
<Connector port="${HTTPSPort}" protocol="org.apache.coyote.http11.Http11NioProtocol"
                         connectionTimeout="${WebConnectorConnTimeout}"
                         maxThreads="${MaxThreadPoolSize}"
minSpareThreads="${MinThreadPoolSize}" SSLEnabled="true" scheme="https"
secure="true"
                         clientAuth="false" sslProtocol="TLS"
keystoreFile="${informiam.conf.dir}/tomcat-cert" keystorePass="secret"/>
```

3. Set the keystoreFile attribute to the path of your keystore file (generated in Step 1).
4. Set the keystorePass attribute to the password used in your keystore file.
5. After the changes are complete, restart the Advisors Platform server.
6. You can test the HTTPS connection by accessing https://<Tomcat Host>:<HTTPS Port>. The `${HTTPSPort}` property value used in the connector configuration is defined in the installation `apache-tomcat-<version>/conf/` directory `catalina.properties` file and defaults to 8443.

Change a JDBC Data Source Configuration

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

To change the password for connections described on this page, see Change Encrypted Passwords.

Procedure: Changing Database Connection Parameters for Advisors Platform

Steps

1. Edit the following properties in the `Advisors\apache-tomcat-<version>\conf\catalina.properties` file:
   ```
   database.username=
   database.password=
   database.url=
   database.driver=
   ```
2. Restart the Advisors server.

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

Steps

1. Edit the following properties in the `Advisors\apache-tomcat-<version>\conf\catalina.properties` file:
   ```
   dw.database.username=
   dw.database.password=
   dw.database.url=
   ```

```
dw.database.driver=
```

2. Restart the Advisors server.

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`

Browser Console Debug Logging for the Advisors User Interfaces

Starting with Pulse Advisors release 9.0, you can enable and disable the browser console debug logging for the Advisors user interfaces. The debug logging is disabled by default. You can enable the console debug logging for the UI by appending the `?adv.debug.on=true` parameter to the URL. For example:

http://yourdomain.com/adv/contactcenter?adv.debug.on=true

The debug mode is saved in the application cookie on the browser as `adv.debug.on=true`. Therefore, omitting the query parameter from the URL after you have enabled debug logging will not affect the debug mode while you navigate to other modules in the application. The only way to disable the debug mode is to turn it off, which you do by appending the `?adv.debug.off=true` parameter to the URL. For example:

http://yourdomain.com/adv/contactcenter?adv.debug.off=true

When you disable the debug mode, the debug mode cookie is deleted.

Adjust Logging 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
- Workforce Advisor Server running in Tomcat
- Frontline Advisor Server running in Tomcat
- Contact Center Advisor, Workforce Advisor, and Frontline Advisor Web services running in Tomcat
- Contact Center Advisor (CCAdv) XML Generator
- Advisors Genesys Adapter (AGA)

The default setting for rollover of the log files is daily or when the log file size exceeds 10 MB. To change the schedule for log file rollover, see Configuring Rollover of the Log File on this page.

See also Configuring the Audit Logs for more information.

Default Log File Storage Locations

Starting with release 9.0.001, the default storage location for Advisors log files changes. In release 9.0.001, the default log storage location is consistent for all components, with logging content organized by component within the main log directory. That is, there is a subdirectory for each component that produces a log file.

Also starting with release 9.0.001, the installation wizards prompt you to provide the log file storage location for each component that generates a log, and default to the locations listed in the table below. If you plan to use a log file storage location that is not the default location, then specify the location when you install the components.

The installation wizard checks that the selected storage directory is present; if not present, then the wizard creates it. The installation wizard stores the selected log file storage location in one of the following files:

- The properties files specific to each module. The log file configuration file picks up the location from the module's properties file.
- The `log4j` configuration files themselves.

The following table lists the default log file storage locations by release.

> **Tip**
> Any diagnostics files that are produced by Advisors components are treated as log files.

Advisors Component	Advisors Release	Default Storage Location for Logs	
Windows	**Linux**		
Platform Server	9.0.000	<Advisors directory>\apache-tomcat-<version>\logs	/apache-tomcat-<version>/logs
	9.0.001	c:\genesys\log\advisors\platform\	/mnt/log/advisors/platform/
Advisors Genesys Adapter	9.0.000	No default location	No default location
	9.0.001	c:\genesys\log\advisors\ccadv-adapter\ c:\genesys\log\advisors\fa-adapter\	/mnt/log/advisors/ccadv-adapter/ /mnt/log/advisors/fa-adapter/
CCAdv XML Generator	9.0.000	<Advisors directory>\xmlgen\logs	<Advisors directory>/xmlgen/logs
	9.0.001	c:\genesys\log\advisors\ccadv-xmlgen\	/mnt/log/advisors/ccadv-xmlgen/

Log File Naming Conventions

Starting with Advisors release 9.0.001, log file names include the name of the component to ensure uniqueness of file name. For example, in releases prior to release 9.0.001, an Advisors Genesys Adapter (AGA) for Frontline Advisor (FA) and an AGA for Contact Center Advisor (CCAdv) produced log files with the same name. Starting with release 9.0.001, the log file name for AGA identifies the component with which the adapter is associated (FA or CCAdv).

The following table lists the default log file names for Pulse Advisors components.

For additional information, see also Default Log File Storage Locations and Using Properties Files to Change Log Settings on this page.

Advisors Log File Names

Component	Release 9.0.000 Log File Name	Release 9.0.001+ Log File Name	Comments
Advisors Platform	advisors.log	advisors.log	The following modules, which run on Advisors Platform, write content to the `platform.log` file:

Component	Release 9.0.000 Log File Name	Release 9.0.001+ Log File Name	Comments
	wu-server.log	wa-server.log	• Advisors Platform • WA Server • FA Server • Advisors Web Services • Resource Management Console The `wa-server.log` file can be produced, but it is optional. The file contains messages only from Java code with `com.informiam.workforceutilization` in its package name. Note that WA Server also uses code from other packages. That code will not write messages into the `wa-server.log` file.
	AdministrationAudit.log	advisors-admin-audit.log	The `advisors-admin-audit.log` file records Advisors administration module user activity.
	auth.log	advisors-authorization.log	The `advisors-authorization.log` file records users logging in to and out of Advisors.
CCAdv XML Generator	xmlgen.log xmlgen_timing.log	ccadv-xmlgen.log ccadv-xmlgen-timing.log	The `ccadv-xmlgen-timing.log` file can be produced, but it is optional. The file contains only Timing-related messages.
AGA for CCAdv	connector.log memory.log psdk.log timing.log	ccadv-adapter.log ccadv-adapter-memory.log ccadv-adapter-psdk.log ccadv-adapter-timing.log	
AGA for FA	connector.log memory.log psdk.log timing.log	fa-adapter.log fa-adapter-memory.log fa-adapter-psdk.log fa-adapter-timing.log	

Using Properties Files to Change Log Settings

Configuring Rollover of the Log File

You can configure the `log4j.xml` and the `log4j.properties` files to use a rolling file name in this format:
`<Component><Date><Time>.log`
`<Date>` and `<Time>` are configurable parameters. The appropriate component name is automatically added to the log file name.

The current log file does not have a timestamp in the file name. The timestamp is added to the file name when the log file is archived.

A log file has the following rolling attributes:

- `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 file name when the log file rolls over. The parameter supports the Java SimpleDateFormat conventions, such as `'.'yyyy-MM-dd'T'HHmmss'.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, in which case you will need to manually clear the backup copies from the log directory on a periodic basis.

See Using Properties Files to Change Log Settings for procedures to configure the rollover schedule, log file names, 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 the Java 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.2018-02-16` on 2018-02-16 at midnight and logging for 2018-02-17 continues in the `/xxx/yyy.log` file until it rolls over the next day, and so on.

Advisors Platform 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 Advisors base 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.

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 Tomcat application server. Use the following procedure to make changes to the logging properties file for CCAdv XML Generator.

1. Navigate to your Advisors base 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.

Advisors Genesys Adapter

Use the following procedure to make changes to the logging properties file for AGA.

1. Navigate to your AGA base 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.

Specifying the Log File Storage Locations

By default, the Platform server logs are written to the following log folder:

- `<Advisors>\apache-tomcat-<version>\logs` (Release 9.0.000)
- `c:\genesys\log\advisors\platform\` (Release 9.0.001+)

To specify a different directory for the Platform server logs, see Specifying a Location for the Platform Server Log Files.

The AGA log file storage location is specified in a .properties file that is located within the AGA installation directory. Similarly, the CCAdv XML Generator log file storage location is specified in an .xml file, which is located within the XML Generator installation directory. To specify a different location for either the AGA or the CCAdv XML Generator log file, see Specifying a Location for the AGA and CCAdv XML Generator Log Files.

Specifying a Storage Location for the Platform Server Log Files

Procedure:

Steps

1. To change the location of the `advisors.log` file, edit the location in the `<Advisors>/conf/log4j.properties` file:

```
# For 9.0.000
log4j.appender.ADMINISTRATIONAUDIT.file=${catalina.base}/var/log/advisors.log
# For 9.0.001+
log4j.appender.ADMINISTRATIONAUDIT.file=${advisors.logs.dir}/advisors.log
```

2. To change the location of the `advisors-authorization.log` file, edit the location in the `<Advisors>/conf/log4j.properties` file:

```
# For 9.0.000
log4j.appender.ADMINISTRATIONAUDIT.file=${catalina.base}/var/log/auth.log
# For 9.0.001+
log4j.appender.ADMINISTRATIONAUDIT.file=${advisors.logs.dir}/advisors-
authorization.log
```

3. To change the location of the `advisors-admin-audit.log` file, edit the location in the `<Advisors>/conf/log4j.properties` file:

```
# For 9.0.000
log4j.appender.ADMINISTRATIONAUDIT.file=${catalina.base}/var/log/
AdministrationAudit.log
# For 9.0.001+
log4j.appender.ADMINISTRATIONAUDIT.file=${advisors.logs.dir}/advisors-admin-
audit.log
```

4. To change the location of the Tomcat Access log, locate the `directory entry` property in the `<Advisors>\apache-tomcat-<version>\conf\server.xml` file, and edit the value to specify a new location.

   In release 9.0.000, if you do not specify an absolute path, then the location is relative to the Tomcat base folder (`apache-tomcat-<version>`). For example (this is the default setting):

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs" prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %u %t "%r" %s %b" />
```

   In 9.0.001+, the access log is placed in the log directory for Advisors Platform, which was specified during installation. For example, in the `<Advisors>\apache-tomcat-<version>\conf\server.xml` file:

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
directory="${advisors.logs.dir}" prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %u %t "%r" %s %b" />
```

Specifying a Storage Location for the AGA and CCAdv XML Generator Log Files

The default location in which to store the AGA and XML Generator log files is specified in files that reside within the installation directory of each component.

To specify a non-default location for the AGA log file, edit the following file:
`<Adapter>/conf/log4j.properties`

To specify a non-default location for the CCAdv XML Generator log file, edit the following file:
`<XMLGen>/log4j.xml`

Advisors Platform

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

Configure Administrative Actions Logs

All administration actions carried out in the Pulse Advisors environment are logged. The following sections give information about how to configure the logging. 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

You can find logs related to administrative changes in the `AdministrationAudit.log` file. The file records changes to configuration and metrics such as creating/deleting metrics and other configuration changes.

Modules for which Actions are Not Logged

Administrative actions are not logged for the following modules:

- Configuration Server, for actions on objects that are used by Contact Center Advisor and Workforce Advisor
- Frontline Advisor administration
- Resource Management administration

Actions Not Logged by This Functionality

The administrative actions logging functionality does not capture changes made to contact groups when the contact groups are imported from a WFM system.

Information Logged

The following information is logged for each action:

- A timestamp of when the action's data was saved in the format specified by the log configuration properties. For additional information, see Configuring the Audit Logs on this page.

- 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 in a file called:

- `AdministrationAudit.log` (Release 9.0.000)
- `advisors-admin-audit.log` (Release 9.0.001+)

The file is written to the following directory by default:

- `<advisors>\apache-tomcat-<version>\logs` (Release 9.0.000)
- On Windows: `c:\genesys\log\advisors\platform\` (Release 9.0.001+)
- On Linux: `/mnt/log/advisors/platform/` (Release 9.0.001+)

You can configure the audit log using the `log4j` properties in the `log4j.properties` file, which is located in the following directory:
`Advisors\conf`

Sample log4j Appender

The following information is the definition of the appender that configures the audit logs:

```
log4j.appender.ADMINISTRATIONAUDIT.append=true
# For 9.0.000
log4j.appender.ADMINISTRATIONAUDIT.file=${catalina.base}/var/log/
AdministrationAudit.log
# For 9.0.001+
log4j.appender.ADMINISTRATIONAUDIT.file=${advisors.logs.dir}/advisors-admin-audit.log

log4j.appender.ADMINISTRATIONAUDIT.threshold=INFO

log4j.appender.ADMINISTRATIONAUDIT.datePattern=yyyy-MM-dd
# For 9.0.000
log4j.appender.ADMINISTRATIONAUDIT.suffixPattern='.'yyyy-MM-dd_HH-mm-ss'.log'
# For 9.0.001+
log4j.appender.ADMINISTRATIONAUDIT.suffixPattern='.'yyyy-MM-dd'T'HHmmss'.log'
log4j.appender.ADMINISTRATIONAUDIT.maxFileSize=10MB

log4j.appender.ADMINISTRATIONAUDIT.maxRollFileCount=10

log4j.appender.ADMINISTRATIONAUDIT.scavengeInterval=600000
```

```
log4j.appender.ADMINISTRATIONAUDIT.layout=com.informiam.platform.core.logging.StdHeaderPatternLa

log4j.appender.ADMINISTRATIONAUDIT.layout.ConversionPattern=%d{ISO8601} %t %-5p
[%c{1}] %m%n

log4j.appender.ADMINISTRATIONAUDIT.layout.ComponentName=Administration Audit

log4j.appender.ADMINISTRATIONAUDIT.layout.VersionNumber=@platform.version@
```

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, in release 9.0.000:

```
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.
- `MaxBackupIndexOf3`—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.

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

You configure Stat Servers as connections to the Advisors Genesys Adapter (AGA) Application object in the Genesys Configuration Server. You can add a Stat Server primary/backup pair (or more than one) to each adapter's configuration. The Stat Server-to-AGA relationships, as well as the object-to-Stat Server mapping, continues to be stored in the Advisors Platform database.

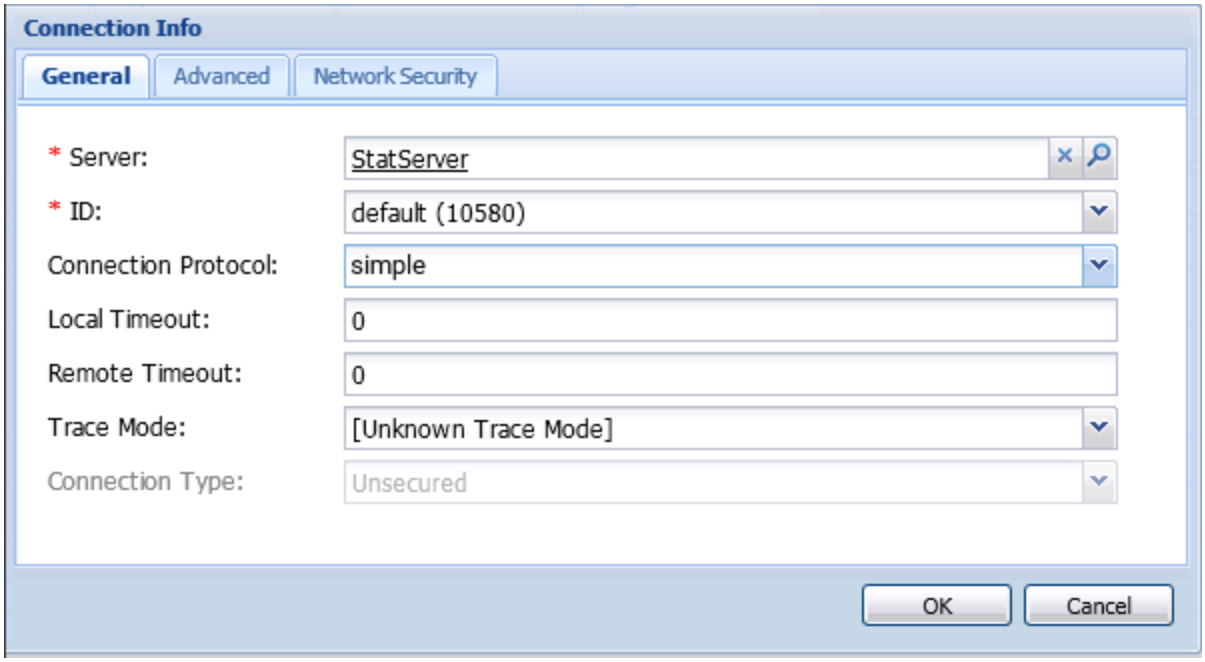
Be sure to review the permissions required by the Advisors User. To perform some of the tasks described on this page, your Advisors User account requires a few permissions that were not previously specified for this account.

Configuring the Connection to Stat Server in the AGA Application Object

Using a Genesys configuration interface, such as Genesys Administrator, configure a Stat Server connection on the AGA Application object. See the Creating Application Objects procedure in the *Genesys Administrator Extension Help* for information about creating and configuring Application objects, which includes steps to configure connections to other Application objects. The following information is specific to configuring a Stat Server connection to the AGA Application:

- The only supported type of connection is to the "default" port. The AGA Application does not support a secure connection.
- The connection protocol type can be either Simple or ADDP. When you specify an ADDP connection mode, AGA uses the ADDP properties that you configure for the connection.

The following figure shows a sample Stat Server connection configured on an AGA Application object, using Genesys Administrator.



Stat Server Connection Configured on an AGA Application Object

Configuring the Backup Stat Server

Advisors Genesys Adapter supports Stat Server primary/backup pairs. Deploy a redundant (backup) Stat Server by configuring a redundancy link on the primary Stat Server Application object, much like you deploy redundant Configuration Servers. An Advisors adapter cannot identify a backup Stat Server if you fail to configure that backup Stat Server as a redundancy link on the primary Stat Server Application object. (Advisors applications do not use the settings for parameters such as redundancy type, timeout, and the number of attempts.)

After the Stat Servers are configured as primary/backup pairs, there are two ways in which you can configure a backup Stat Server connection to an adapter Application object. Use one of the following methods:

1. Add the primary and backup Stat Servers as connections to the adapter Application object in the Configuration Server.

   Using this method has the following implications:

   - An adapter will ignore a backup Stat Server if you fail to add it as a connection to the adapter Application object.
   - You have the option to purposefully remove a backup Stat Server from the Advisors configuration, in cases where you want to use only the primary Stat Server of a pair.

2. If you always use Advisors Stat Servers as redundant pairs in your environment, then you can set the following property in the `inf_genesys_adapter.properties` file to `false`:
   `advisors.genesys_adapter.statserver.backup.configure.as.connections`

   Setting this option to `false` removes the need to manually configure the backup Stat Servers as connections to the adapter Applications.

   Using this method means that any Stat Server that is configured as a backup on a primary Stat Server Application object will automatically be connected to the adapter to which the primary Stat Server is connected.

How the Advisors Adapter Identifies a Backup Stat Server

The Advisors adapter determines which Stat Server connections are to primary Stat Servers and which are to backup Stat Servers based on the configuration of the Stat Server Application. If a Stat Server is configured as a redundancy link to another configured Stat Server connection, then the adapter identifies that Stat Server connection as the connection to a backup Stat Server. If a backup Stat Server is not configured correctly as a redundancy link on the primary Stat Server Application, then the adapter to which the Stat Server pair is connected cannot identify the backup.

How Stat Server Connections Work on a Backup Adapter

When switching over from a primary adapter to the backup, the backup adapter uses the same object distribution that the primary adapter was using. This means that the distribution of objects remains the same even though a failover to the backup adapter occurred.

For this to work, the Stat Server connections configured on the backup adapter need to be the same as those configured on the primary adapter. Genesys Administrator automatically ensures that the connections are added or removed on the backup adapter Application when you modify the connections on the primary adapter Application, provided that a backup adapter is configured on the primary adapter Application.

Configuring the Stat Server Type for Advisors

You can configure an Advisors Stat Server as one or more of the following types:

1. Core (default)
2. Multimedia
3. Thirdpartymedia

The Stat Server type(s) you specify will depend on the purpose of the Stat Server, and what type of statistics it serves.

You configure the Stat Server type on the **Annex** section of the Stat Server Application object, under a new section called **Advisors-StatServerTypes**. The following figure shows the configuration in Genesys Administrator.

Advisors-StatServerTypes (3 Items)		
Advisors-StatServerTypes/CORE	Advisors-StatServerTypes	CORE
Advisors-StatServerTypes/MULTIMEDIA	Advisors-StatServerTypes	MULTIMEDIA
Advisors-StatServerTypes/THIRDPARTYMEDIA	Advisors-StatServerTypes	THIRDPARTYMEDIA

Advisors-StatServerTypes Section in the Stat Server Application Annex

It is the presence or absence of the "type" setting that matters in this configuration; Advisors ignores the "yes" or "no" values. For example, if you add an entry in the Annex for **Advisors-StatServerTypes**, and you enter the type as `MULTIMEDIA`, and set the value to no, then the Stat Server type is configured as `MULTIMEDIA`, regardless of the no value.

An Advisors Stat Server defaults to a type of CORE if you do not explicitly enter a type. In other words, it is necessary to configure the Stat Server types only when non-CORE Stat Server types are required in your configuration.

It is unnecessary to configure the Advisors Stat Server types on the backup Stat Servers because this configuration is only fetched from the primary Stat Servers.

Migrating Stat Server-Adapter Relationships from the Platform Database to Configuration Server

If you have Advisors release 8.5.1 deployed in your enterprise, then you can use the migration wizard to export the existing Stat Server configuration from the Advisors Platform database to the Configuration Server in order to add the connections to the AGA Application object. The migration wizard "Export Stat Server Config to Config Server" option performs the migration operation for all configured adapters in a single pass. Alternatively, you can manually configure the Stat Server connections and the Stat Server types using a Genesys configuration interface, such as Genesys Administrator. You might do this for security reasons, for example.

For more information about using the migration wizard to export your existing Stat Server configuration to the Configuration Server, see the *Genesys Pulse Advisors Migration Guide*.

Configure a TLS Connection Between AGA and Stat Server

To establish a secure Transport Layer Security (TLS) connection between an Advisors Genesys Adapter (AGA) and Stat Server, the following configuration is required:

1. You must configure a secure connection port on Stat Server.
2. You must configure a secure connection between the AGA and Stat Server.
3. You must add the client-side TLS properties on the AGA Application object or AGA connection to the Stat Server.

This page provides additional information about each step, as well as examples of the configuration.

Using TLS with Primary and Backup Stat Servers

If you have more than one Stat Server configured, and you want to enable TLS encryption and security on all of the connections, you have two options:

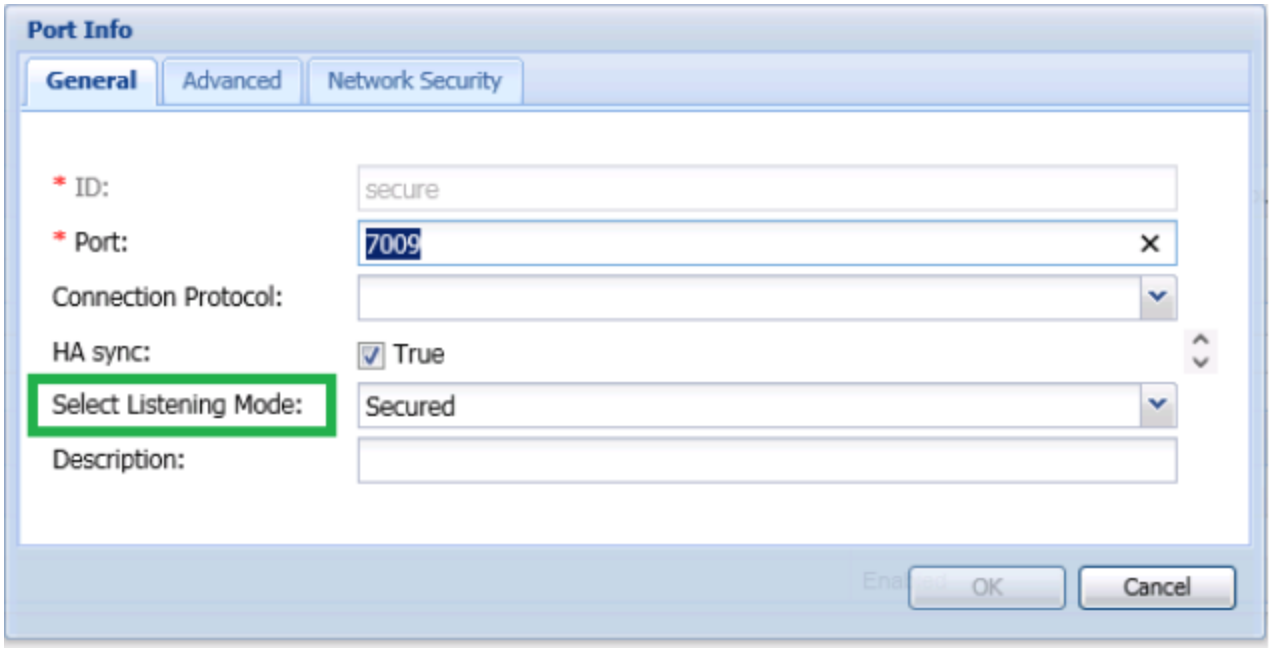
- If all of the Stat Servers connected to an adapter share the same TLS certificates, then you can configure the client-side TLS properties on the AGA Application object.
- If the Stat Servers connected to an adapter do not share TLS certificates (for example, the primary and backup Stat Servers are on different hosts), then you configure the TLS properties on each AGA–Stat Server connection.

Configuring a Secure Connection Port on Stat Server

To configure a secure connection port on each Stat Server Application object, see the instructions in the *Genesys Security Deployment Guide*. You can configure security certificates on the Host application (recommended), on the Application object, or on the connection port.

For additional information, see the Configuring TLS Parameters and the Using and Configuring Security Providers sections of the *Platform SDK* guide.

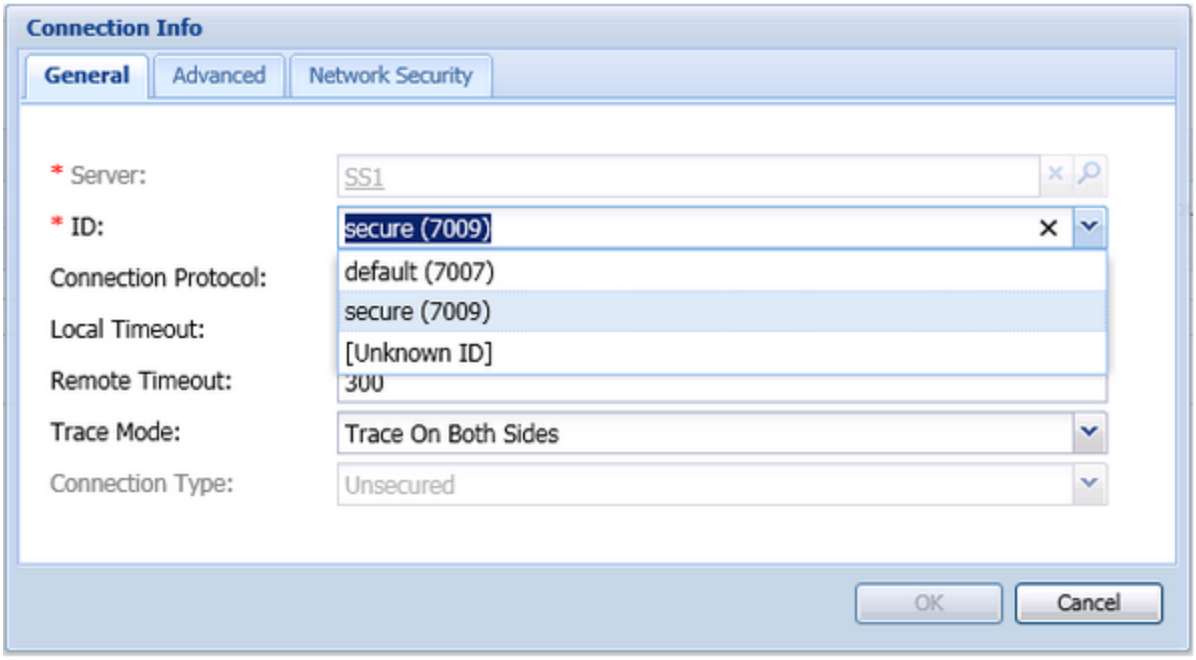
The following figure shows the configuration of a secure port on the Stat Server Application object. In this example, the port ID is called "secure", but it is not necessary to call it that; name it according to the conventions you use in your enterprise.



Configuring Client-side TLS Properties

To configure a secure connection between AGA and each Stat Server, you must configure the connection on a secure Stat Server port. For detailed information, see the Connection Object section of the *Platform SDK* guide.

In the following figure, an existing secure port is used for the connection to AGA. Repeat this configuration for each of the AGA–Stat Server connections.



In general terms, enabling TLS on a secure AGA–Stat Server connection requires the following two actions:

- Configure the certificates.
- Set the `tls=1` configuration option (to enable TLS encryption and security).

In cases where all of the Stat Servers share the same TLS certificates, you can configure the TLS properties on the AGA Application object. In this scenario, the TLS settings are applied to all AGA–Stat Server connections. However, in cases where the Stat Servers do not share TLS certificates, then you cannot apply a "global" TLS configuration. Instead, you must configure the TLS properties on each AGA connection to a Stat Server. For example, when the primary Stat Servers are on one host, and the backup Stat Servers are on another host, then you enable TLS on the connection, and not on the AGA Application object.

If TLS is enabled on the AGA–Stat Server connection, then the Stat Server Application object must have a secure port configured for the connection. If you fail to configure the secure connection port on Stat Server, then an exception message will be written to the log file.

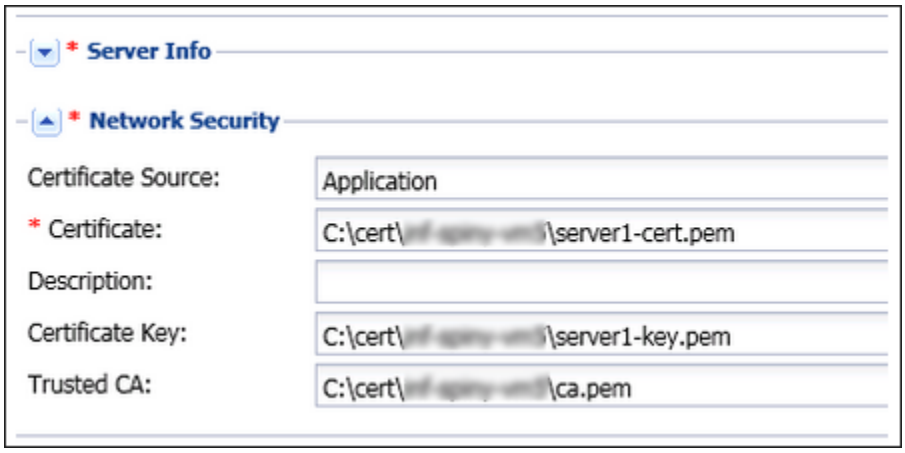
If you will not be using TLS on an AGA–Stat Server connection, then you can either omit the `tls=1` configuration option, or set the option to zero (`tls=0`). You might do the latter if you want to later enable TLS encryption and security on the connection. If you are not using TLS to secure the AGA–Stat Server connection, then you must not use a secure port on Stat Server to connect to AGA. If you do not enable TLS on the AGA–Stat Server connection, but you use a secure Stat Server port to connect to AGA, then an exception message will be written to the log file.

Example: Configuring client-side TLS properties

In this example, the Stat Servers are deployed in such a way that they can share TLS certificates. Therefore, the TLS configuration can be completed on the AGA Application object, and will uniformly apply to all of that adapter's Stat Server connections. In cases where Stat Servers do not and cannot

share TLS properties, then you must configure the TLS properties on the Connection object, rather than the AGA Application object.

The following figure shows the TLS certificate configuration in the **Network Security** section of an AGA Application object:



The following figure shows the TLS option configuration (to enable TLS for connections) in the **security** section of an AGA Application object's **Options** tab:

Mutual TLS Authentication

The Stat Server Application object can enforce mutual TLS authentication on a connection. To configure mutual TLS for the AGA–Stat Server connection, set the `tls-mutual=1` configuration option in the **security** section of the Stat Server Application object's **Options** tab.

Making Changes to the Application Objects

From time to time, you might make changes to your Application object configuration. If you change the Stat Server configuration in the (Stat Server) Application object, then those changes take effect when the Stat Server is restarted. If you change the adapter's configuration in the (AGA) Application object, then those changes take effect when the adapter is restarted.

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
`informiam.genesys_connector.transformer.CCAdv.CCAdvChannel = 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.
`informiam.genesys_connector.ObjectChangeStatRequest.frequency = 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.
`informiam.genesys_connector.statServer.maxOpenReqsPerGroup = 1000` `informiam.genesys_connector.statServer.interGroupDelay = 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.
`informiam.genesys_connector.statServer.allowredistributestats = 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: • informiam.genesys_connector.statServer.reconnect.attempts • informiam.genesys_connector.statServer.reconnect.attempt-interval

Parameter	Description
	If the adapter cannot re-establish the connection before the expiry of the reconnect period, redistribution of the statistics is attempted. 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. This property can be set to `true` for small customers where the total number of statistics requested is small or where the amount of statistics redistributed is small and will not result in overloading of the Stat Servers.
`informiam.genesys_connector.statServer.onstartWaitTimeForAllSSConnections` ToOpen = 20	Time in seconds to wait on Stat Server connection to open before sending statistics requests to all opened Stat Server connections. 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.
`genesys_connector.default_time_profile.oneday = Default,Growing`	Specify the time profile to use in the statistics requests. 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. Ensure you configure the AGA parameter to match the time profile specified on the Stat Server from which AGA is requesting statistics. See Configure the Daily Reset Time for Statistics on a Stat Server for more information.

`informiam.genesys_connector.configServer.reconnect.attempts = 5`
 	
`informiam.genesys_connector.configServer.reconnect.attempt interval = 30`
	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).
	
	This is in addition to – and after – the ADDP time out, if configured.

`informiam.genesys_connector.statServer.reconnect.attempts = 3`
 	
`informiam.genesys_connector.statServer.reconnect.attempt interval = 10`
	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).
	
	This is in addition to – and after – the ADDP timeout, if configured

`informiam.genesys_connector.api.port =`	The port of communication between CCAdv and the Genesys Adapter and between FA and the Genesys Adapter.

Parameter	Description
`informiam.genesys_connector.waitForStatOpenEventsTimeout = 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.
`informiam.genesys_connector.numOfMaxStatRerequestTimes = 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.

`informiam.genesys_connector.configServer.addp.turnon = true`
 	
`informiam.genesys_connector.configServer.addp.tracemode =`
`informiam.genesys_connector.configServer.addp.servertimeout = 300`
`informiam.genesys_connector.configServer.addp.clienttimeout = 120`
`informiam.genesys_connector.configServer.protocol.request.timeout = 180`
	ADDP Settings to be used with the Configuration Server connection.

`informiam.genesys_connector.statServer.addp.turnon = true`
 	
`informiam.genesys_connector.statServer.addp.tracemode =`
`informiam.genesys_connector.statServer.addp.servertimeout = 300`
`informiam.genesys_connector.statServer.addp.clienttimeout = 120`
	ADDP Settings to be used with the Stat Server connections.

`informiam.genesys_connector.transformerjob.pausecheck.limit = 25000`
 	
`informiam.genesys_connector.statsissue.pausechecklimit = 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.

`informiam.genesys_connector.psdk.server.fileEncoding = 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
genesys_connector.configServer.tls.enabled	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). You can set the flag to `true` 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 `genesys_connector.configServer.tls.enabled` 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 (`tls=0` or `tls=1`) in the TLS properties file that you prepare is also ignored.
genesys_connector.configServer.tls.port	Identify the Configuration Server port number for establishing a TLS connection from AGA. 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.
genesys_connector.configServer.tlsproperties.file	When using a TLS connection to the Configuration Server, specify the location of the TLS properties file that you prepared. 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.

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.

Configure Resource Management Console Properties

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 `Advisors\conf\RMC.properties` configuration file.

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 `advisors.resourceManagement.refreshTimeSeconds` 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.

For example, to set the refreshTimeSeconds property value to 60:

```
advisors.resourceManagement.refreshTimeSeconds=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 `Advisors\conf\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 Platform 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 `advisors.resourceManagement.maxSkillLevel` to a different value. To set it to `5`, for example:

```
advisors.resourceManagement.maxSkillLevel=5
```

Number of Concurrent Users of RMC

The default value of the `advisors.resourceManagement.expectedNumberConcurrentUsers=10` 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 should more accurately reflect the maximum number. If the value you use 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 `advisors.resourceManagement.expectedNumberConcurrentUsers=10` to a different value. For example, to set it to `20`:

```
advisors.resourceManagement.expectedNumberConcurrentUsers=20
```

Other RMC Properties

For details about other properties in the RMC.properties file, see Deploying SDS and RMC.

Configure Metric Graphing Properties

Pulse Advisors Contact Center Advisor (CCAdv) and Workforce Advisor (WA) include a metric graphing component, in which you can graph metric values for an object. This page describes configurable metric graphing properties.

You can configure some metric graphing properties during the installation of the CCAdv and WA modules. Other properties are automatically set during installation without you providing an initial value.

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 configurable properties that govern metric graphing in the `CONFIG_PARAMETER` table:

- Duration of the historical values retained for graphing.
  The default value 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, below.
- Duration of the future values displayed for graphing.
  The default value 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, below.
- Minimum interval, in seconds, between graphed values in all graphs for points stored after the change.
  See Change the interval between values, below.
- Whether or not 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, below.
- The number of metric/time profile combinations that can be graphed.
  See Specify the number of metric/time profile combinations, below.
- NEW Batch size based on the number of objects.
  You can configure the number of objects for which to write metrics values to the metric graphing database in one batch.

  The default value is 700. This value is automatically set during installation; you cannot provide an alternate value until after installation is complete.

  To change the batch size, see Specify the number of objects for which to write metrics values to the database in each batch, below.

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. The following calculation shows that one data point will be graphed not more than every 12 minutes: 24 hours * 60 minutes per hour / 120 data points

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.

If you open a graph after CCAdv/WA has been running for 24 hours, the 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.
- when you receive an error message on the **Report Metrics** page of the administration module that says that you cannot configure any more metric/time profile combinations for graphing. You receive that error message when you attempt to configure more than the default maximum number of metric/time profile combinations.

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.

2. Wait at least five minutes until the configuration parameter cache expires, and the value you set is loaded into the cache.

Specify the number of objects for which to write metrics values to the database in each batch

Use this procedure to specify the number of objects for which to include metrics values in each batch written to the metric graphing database.

1. In the Advisors database, execute:

```
UPDATE CONFIG_PARAMETER SET PARAM_VALUE = 'n'
Where
PARAM_NAME = 'waredhoused.metrics.objects.per.batch'
```

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

2. Wait at least five minutes until the configuration parameter cache expires, and the value you set is loaded into the cache.

Importing Contact Groups into Advisors

This page provides the information you need to import Contact Groups into Pulse Advisors.

Data for Contact Groups

Workforce Advisor accepts data from three WFM systems:

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

For information about supported versions, see *Workforce Advisor* in the Genesys 7.x - 9.x Product Availability table in the *Genesys Interoperability Guide*.

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 data sets with forecasts from IEX TotalView are sent by FTP to a port number chosen when installing WA Server. 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.

One data set from IEX TotalView can contain data from more than one contact group.

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 `apache-tomcat-<version>\bin\ftpdir\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 backup 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.

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 data sets until an external FTP server pushes them to WA.

Note that 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.

If you want to use FTP to push data from files on disk to WA, 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.txt` 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 on a Windows system, 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.

Changing the Password Used by WA Server's FTP Server

35px|link= As you can see from the example commands above, the default username to connect to WA Server with FTP is `iex` and the default password is `iex!bat`.

To change this password, update the encrypted password stored in WA Server's `ftpUsers.properties` file.

1. Choose the new password.
2. Use any utility available online to produce an MD5 hash of the password. You cannot use the Advisors password encryption utility for this task.
3. In the hashed result, replace lower-case letters with upper-case ones, if necessary. This makes the new hashed password consistent with existing hashes.
4. Go to the `apache-tomcat-<version>\webapps\wu-server\WEB-INF\classes` directory.
5. Edit `ftpUsers.properties`.
6. Replace ftpserver.user.iex.userpassword with the MD5 hash of your new password.

7. Save the file.
8. Restart WA Server.
9. Update the password in your `SendIEX.txt` file.

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 `advisors.log` file of the Tomcat in which the WA Server is deployed. This log file is in the Advisors deployment directory, in subdirectory `apache-tomcat-<version>/logs`.

This logging is controlled by a category in the `log4j.properties` file in the Advisors/conf directory. 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|schedOp

#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 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 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 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 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 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 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 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 for 30 minutes = ($AdjSCH^1$ * $FNCO^1$ * $FAHT^1$ + $AdjSCH^2$ * $FNCO^2$ *$FAHT^2$) / ($FNCO^1$ * $FAHT^1$ + $FNCO^2$ *$FAHT^2$).
  - If any metric from period 1 is null, then the result is $AdjSCH^2$.
  - If any metric from period 2 is null, then the result is $AdjSCH^1$.
  - If the denominator is 0, then the result is null.

WA combines 15-minute periods as follows:

- Period 1 starting at n:00 and period 2 at n:15 combine to one 30-minute period starting at n:00.
- Period 1 starting at n:30 and period 2 at n:45 combine to one 30-minute period starting at n:30.
- A missing period 1 starting at n:00 and available period 2 starting at n:15 combine to one 30 minute period starting at n:00 that has the metrics from period 2.
- A missing period 1 starting at n:30 and available period 2 starting at n:45 combine to one 30 minute period starting at n:30 that has the metrics from period 2.
- Period 1 starting at n:00 and a missing period 2 starting at n:15 combine to one 30 minute period starting at n:00 that has the metrics from period 1.
- Period 1 starting at n:30 and a missing period 2 starting at n:45 combine to one 30 minute period starting at n:30 that has the metrics from period 1.

Back to Top

Metrics Correspondences among WFM Systems

The Table below shows the relationships among the WFM metrics from different WFM systems. If a metric is not available from a WFM system, then its name in the Table, in the context of that system, is '–'.

Notes:

a. `Name` shows the data in the `NAME` column of the `METRICS` table in the Advisors database.

b. `Display Name` shows the data in the `DISPLAY_NAME` column of the `METRICS` table in the Advisors database.

c. IEXTotalView names are in the headers of files imported from that system.

d. Aspect eWFM names are in the headers of files imported from that system.

e. Genesys WFM's names are constants in `com.genesyslab.wfm7 ... EPerfInfoItems`. They are supplied to `WFMPerformanceService750Soap.getPerformanceData()`. If these parameters are not correct, you can map different ones to WA's canonical names in the `conf/WorkforceUtilization-GenesysMetricsMapping.properties` file.

Name	Display Name	WA Canonical Name	IEX TotalView	Aspect eWFM	Genesys WFM
FNCO	Forecast NCO	fcstContactsReceived	fcstContactsReceived	RVOL	PERF_ITEM_FRC_IV
FAHT	Forecast AHT	fcstAHT	fcstAHT	RAHT	PERF_ITEM_FRC_AHT
FSL	Forecast SL%	fcstSLPct	fcstSLPct	RSL	PERF_ITEM_FRC_CALC_SERVICE
FASA	Forecast ASA	fcstASA	fcstASA	RDELAY SEC	PERF_ITEM_FRC_CALC_ASA
REQ	Required Staff	fcstReq	fcstReq	SGRREQ	PERF_ITEM_FRC_REQ_STAFFING
SCH	Scheduled Staff	schedOpen	schedOpen	SGRSCH	PERF_ITEM_SCH_COVERAGE
AdjREQ	Adjusted Required Staff	fcstReqAdj	–	SGRREQ JU	–
AdjSCH	Adjusted Scheduled Staff	schedOpenAdj	–	SGRSCH J	–
FNCOTotal	Forecast NCO Total	fcstContactsReceivedTotal	–	RVOL_TOTAL	–

Back to Top

Bulk Configuration Overview

The bulk configuration tool allows you to quickly configure Contact Center Advisor (CCAdv), Workforce Advisor (WA), or both outside of the Advisors Administration module. The tool configures CCAdv, WA, or both based on the lists of objects you define and export from other systems and load into temporary structures in the Advisors Platform database. The bulk configuration tool retrieves the data from the temporary structures, validates it, and transforms it into CCAdv, WA, or CCAdv/WA rollup configuration.

You can use spreadsheets or CSV files to collect the configuration information into a simple file structure that can be loaded into `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 the *Contact Center Advisor and Workforce Advisor Administrator User's Guide*. You must select the configuration mode before you perform bulk configuration.

Changes to Bulk Configuration Starting with Release 9.0

The data format for the bulk configuration has changed starting with release 9.0.001.06. You no longer specify the tenant name, switch name, and the filter name as part of the application or agent group name in the bulk configuration structure. If an object has a filter, it needs to be added to the new field that is allocated for that purpose. Adding the content to the fields for the tenant and switch is optional, unless the specified name exists in the Configuration Server as registered under several different tenants or switches. The column names are self-descriptive: `AppFilterName`, `AgntGrFilterName`, `AppTenantName`, `AgntGrTenantName`, `AppSwitchName`.

Starting with release 9.0.001.06, the bulk configuration tool is installed by the deployment script. If you plan to use the bulk configuration tool, you need to set the `ccadv.configuration.method.auto parameter` to `false` and `ccadv.wa.integrated.configuration` to `true`. Both parameters are located in the CONFIG_PARAMETER database table.

> **Important**
>
> The bulk configuration/export tool for independent mode is not available for installations with MS SQL Server starting with release 9.0.001.06.

NEW For Oracle installations, a bulk configuration/export tool for the independent configuration mode is available starting with Advisors release 9.0.002.09, which is a Hot Fix release. The tool is included with the deployment/migration scripts. For earlier 9.0 releases, a separate installation script is available for an independent configuration mode bulk configuration/export tool. Contact Genesys Support to request this script.

The format of bulk configuration structures in the release 9.0.002.09 bulk configuration tool has changed: the concatenated application and agent group names are no longer used and the parts related to tenant name, switch name, and filter are now recorded in separate fields. Moreover, if an object is unique within a switch or tenant, then the switch and tenant details are optional. You can still upload your bulk configuration files that contain data in the old name format, and then use the bulk configuration script to transform the format to the new one. The `advisors-platform-version_BulkConfigurationTool.sql` script will transform the old format to the new if the specified switch names and filter names are already imported into the Platform database. Re-applying the `advisors-platform-version_BulkConfigurationTool.sql` script does not erase any data. It is safe to apply the `advisors-platform-version_BulkConfigurationTool.sql` and `blkCfgExp.sql` scripts while the application is up and running.

For releases 9.0.001.06 and 9.0.002.03, if you are planning to use the Advisors bulk configuration/export tool in your installation with Oracle, execute the `advisors-platform-9.0.002.09_BulkConfigurationTool.sql` script against the Platform schema. The `advisors-platform-9.0.002.09_BulkConfigurationTool.sql` script and the matching `blkCfgExp.sql` script can be requested from your Genesys services representative. There is only one `blkCfgExp.sql` script for any mode. The script detects the configuration mode automatically and populates the corresponding tables. All bulk configuration tables are present in the schema, but only the ones that correspond to the selected configuration mode are considered.

CCAdv/WA Bulk Configuration – Integrated Mode

If you plan to deploy Pulse Advisors release 9.0.001.06 or later and you will use the bulk configuration tool, then see the Changes to Bulk Configuration section on the Bulk Configuration Overview page in this guide before you proceed.

For information about the configuration modes and how to set the mode, see the *Contact Center Advisor and Workforce Advisor Administrator User's Guide*. You must select the configuration mode before you perform bulk configuration. Starting with release 9.0.001, the default configuration mode is the independent configuration mode. Previously, the integrated configuration mode was the default mode.

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.

35px|link= In releases prior to release 8.5.2, the bulk configuration tool required the presence of the business hierarchy objects (regions, operating units, application groups, and contact centers) in the Advisors configuration. You had to first add the business hierarchy data to the Genesys Configuration Server's **Business Attributes** folder, and then manually activate the same objects using the Advisors administration module. Starting with release 8.5.2, none of that is necessary prior to using the bulk configuration tool; the bulk configuration tool now has a business hierarchy bulk configuration feature. All business hierarchy names will be automatically added to the Advisors configuration and activated. All new business attributes can then be added to the Genesys

Configuration Server's **Business Attributes** folder using the migration wizard supplied in the installation package.

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 or by the bulk export utility.

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 export utility to generate a "clean" copy of blk tables from the existing application and contact group configuration before you run the configuration removal procedure. 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

Starting with release 8.5.2, the contact centers, regions, operating units, and application groups that you will use in the bulk configuration structures do not need to be present in the Genesys Configuration Server, nor do they need to be visible in the Advisors configuration pages at the time that you run the bulk configuration procedure. The bulk configuration tool automatically adds all hierarchy objects to the Advisors configuration as long as they are entered in the bulk configuration structures, and if they are not currently present in the Advisors configuration. After the bulk configuration procedure is executed, all new business attributes can be added to the Genesys Configuration Server's **Business Attributes** folder using the migration wizard supplied in the installation package. 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.

Review the following considerations before using the bulk configuration import procedure:

- A contact center will be added to the configuration only if the corresponding Geographic Region name is supplied.
- If a contact center is already present in your configuration, then the bulk configuration import process will make no changes to the existing contact center configuration. 35px|link= Starting with release 9.0, if the geographic region of the existing contact center is "Unknown" while a valid geographic region name is supplied in the bulk configuration structures, the bulk configuration procedure will substitute the "Unknown" geographic region for this contact center accordingly.
- A contact center that is automatically added to the configuration as part of the bulk configuration process will be assigned the default value for opening ("00:00") and the default value for closing time ("23:59"). If you need to change those values, then you must adjust those properties manually using the **Contact Center** page in the administration module.
- A contact center that is automatically added to the configuration as part of the bulk configuration process will be assigned the local time zone if the contact center name does not match any geographic location in the list of time zones. If the matching location is found in the time zone list, then the time zone associated with that geographic location will be assigned to the contact center. An administrator can adjust the time zone property at any time. It is important to adjust this property in accordance with the actual contact center time zone if the open and close times are different than the default values

("00:00"/"23:59").

- A contact center that is automatically added to the configuration as part of the bulk configuration process will always be of the "Network" type. If you need to create a "Site" contact center, then you must manually configure it on the **Contact Center** configuration page of the Advisors administration module *before* you execute the bulk configuration procedure.
- The application server and XML Generator service must be up and successfully running until the required data (see the following two bullet points) 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.

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.

Considerations for SL Threshold Bulk Configuration

The bulk configuration tool accepts the SL Threshold property, which you enter in the `CustomSLThreshold` field. For more information, see Data Preparations below.

Be sure to follow these rules if you use SL Threshold values that are not the default value (20 seconds):

- The CustomSLThreshold field is measured in seconds; enter values accordingly.
- If you do not supply a value in the CustomSLThreshold field before you run the bulk configuration import procedure, the default value of 20 seconds will be assigned to the corresponding application, even if the current value is different.
- Only the predetermined SL Threshold values shown in the THRESHOLD_VALUE column of the database table are allowed:

NAME	THRESHOLD_VALUE
Unknown	0
10 sec	10
20 sec	20
30 sec	30
40 sec	40
45 sec	45
50 sec	50
60 sec	60
70 sec	70
80 sec	80
90 sec	90
5 min	300
8 min	480

If you enter an SL Threshold value in the bulk configuration structure that is not listed in the SL_THRESHOLD database tables, the configuration of the related application will be skipped and an error will be registered in the bulk configuration log file.

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.

Procedure:

Steps

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. 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
6. Connect to the Oracle or MS SQL instance as the platform user.
7. 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.
8. 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.
9. Execute the spblkConfigCCAdvWAIntegrated procedure; for example, use the following string with an Oracle schema:

```
DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkConfigCCAdvWAIntegrated"(
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 spblkConfigCCAdvWAIntegrated
               @m = @m OUTPUT,
               @r = @r OUTPUT

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

GO
```

10. Verify the log stored in the blkAllLog 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 9.

12. Examine all relevant configuration pages in the Advisors administration module to verify the configuration.
13. Examine the dashboards to verify the configuration.
14. Do one of the following:
    a. If you are satisfied with the resulting configuration, connect to the Oracle instance as the 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 11. 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 9.

       To remove the entire configuration in Oracle installations, execute the following:

```
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;
```

       To remove the entire configuration in MS SQL 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, geographic region, reporting region, and operating unit names. 35px|link= Starting with release 9.0, your file must contain 15 columns with headers (headers are mandatory). Bulk configuration application names no longer require the concatenation [tenant name] [base object name or number] / filter name@switch name. Instead the bulk configuration structure contains separate fields for the former parts of object names. The Application Name column should only contain the base object name or number as it appears in the Configuration Server. The tenant name, filter name and switch name can be provided in separate columns where applicable or if necessary. Provide the following information in the file:

- Application Name (35px|link= Starting with release 9.0 provide only the base object name, exclude tenant, filter and switch name)
- Application Display Name
- Contact Center Name
- Geographic Region Name (to allow Contact Center bulk configuration)
- Application Group Name
- Reporting Region Name
- Operating Unit Name

- Contact Group Name
- Contact Group Display Name
- Custom SL Threshold Value (provide this only if you use a value other than the default value of 20 seconds)
- Application Include in Rollup Property
- Contact Group Include in Rollup Property
- 35px|link=Application Switch Name (if applicable, see the Guidelines below)
- 35px|link=Application Tenant Name (if applicable, see the Guidelines below)
- 35px|link=Application Filter Name (if necessary ans applicable, see the Guidelines below)

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, geographic region, 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. If the geographic region is not provided, and the associated contact center is not yet present in the Advisors configuration, the contact center will not be created and the application or contact group configuration will not be added. A corresponding message will be written in the blkAllLog table. If the geographic region is not supplied, but the contact center is already present, no error will be logged and the application or contact group configuration will be added to the Advisors rollup configuration, unless other issues are detected. If a contact center is already present in the Advisors configuration, but the geographic region that is supplied in the bulk configuration data does not match the existing geographic region property, no changes will be made to the existing contact center geographic region property. 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 along with the tenant, switch and filter name) must match the name contained in the tmpImportCallType.PeripheralName, tmpImportInteractionQueue.PeripheralName, or tmpImportApp.PeripheralName column of the Platform database. 35px|link= Starting with release 9.0 each column with application names should contain only the base object names or numbers as they appear in the name or number property of the corresponding object in the Configuration Server or in the Name field of the Platform database table CFG_IMPORTED_OBJECTS.
- 35px|link= Starting with release 9.0 the tenant name is provided in a separate column if applicable. If you know that the name of the object is unique across all tenants in the Configuration Server, the tenant name can be omitted.
- 35px|link= Starting with release 9.0 the application switch name is provided in a separate column if applicable. If you know that the name of the object is unique across all switches within the mentioned tenant or across all switches in the Configuration Server, the switch name can be omitted.
- 35px|link= Starting with release 9.0 the filter name is provided in a separate column if applicable. In this case the object will be configured with the object segmentation filter which will be applied to all filterable metrics applicable to the object. The filter will not be applied to the metrics that have "Exclude from Base Object Filter" property enabled. The filtered object configured by the bulk

configuration tool will be treated as configured with the object segmentation filter even if the filter itself does not have the "ObjectSegmentationFilter" option (35px|link= in release 9.0) set to "true" or "yes". In order to be applied in the statistics requests , the filter must be registered in the Configuration Server as a business attribute under the "Advisors Filters" folder and contain the filter definition under the "Filter" section in the "Filter" option. If you already have filters registered in the "Advisors Filters" folder with the definitions contained in the "Description" property, use the migration wizard to move the existing filter definitions into the "Filter" section.

- If used, each contact group name must match the name contained in the CONTACT_GROUP.NAME column of the Platform database. If the contact group names are unique within each source system, but are not unique across all source systems, append a dot and the source system qualifier to the contact group name in the bulk configuration data, i.e. the name in the bulk configuration will consist of [CONTACT_GROUP.NAME].[CONTACT_GROUP.SOURCE_SYSTEM] .
- 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` (for information about the two `Include in Rollup` columns, see Applications above).
- WA does not support interaction queues. Any contact groups specified and associated with interaction queues are ignored.
- Filters are not applicable to interaction queues and calling lists.

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. 35px|link= Starting with release 9.0, your file must contain 5 additional columns with headers (headers are mandatory). Bulk configuration application and agent group names no longer require the concatenation [tenant name] [base object name or number] / filter name@switch name. Instead the bulk configuration structure contains separate fields for the former parts of object names. The Application Name and the Agent Group Name columns should only contain the base object names or numbers as they appear in the Configuration Server. The tenant name, filter name and switch name can be provided in separate columns where applicable or if necessary.

Your file must contain the following columns with headers and provide 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
- 35px|link=Application Filter Name (if necessary and applicable, see the Guidelines for Applications

above)

- 35px|link=Agent Group Filter Name (if necessary , the guidelines are similar to the ones for Applications)
- 35px|link=Application Tenant Name (if applicable, see the Guidelines for Applications above)
- 35px|link=Agent Group Tenant Name (if necessary, the guidelines are similar to the ones for Applications)
- 35px|link=Application Switch Name (if applicable, see the Guidelines for Applications above)

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

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. 35px|link= Starting with release 9.0 the name must match the Name field content in the Configuration Server or in the Platform database table CFG_IMPORTED_OBJECTS.
- If used, each contact group name must match the name contained in the CONTACT_GROUP.NAME column of the Platform database. If the contact group names are unique within each source system, but are not unique across all source systems, append a dot and the source system qualifier to the contact group name in the bulk configuration data; that is, the name in the bulk configuration will consist of [CONTACT_GROUP.NAME].[CONTACT_GROUP.SOURCE_SYSTEM] .
- 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.

General Data Preparation Guidelines

- If your platform database contains bulk configuration data generated in a previous version, applying the blkObjCre.sql script of the new version in the platform database migrated to the new version will migrate the bulk configuration data to the form required in the new version. If you have bulk configuration data stored outside the database, it can be imported "as is" and then migrated to the form required in the new version by applying the blkObjCre.sql supplied with the new version installation package. It is safe to apply blkObjCre.sql several times. It will migrate the older schema and transform the data as well as preserve the configuration data content.

- If you have a platform database with the existing Advisors configuration but do not have a corresponding copy of the bulk configuration data, you can generate the bulk configuration data in the form required in the new version by applying the bulk export script to the Platform database migrated to the new version. The bulk export script will not remove any existing bulk configuration content. If any, the previous content will be moved to the tables that have identical names with appended

timestamps. You can use the content in tables that have "Exp" in their names to review the validity of your current configuration. You then can address the reported warnings or problems by editing the exported bulk configuration data and then by removing and replacing the configuration by using the bulk removal and then the bulk configuration procedure. You also can address the reported issues by applying the changes in the Administration module and verifying the configuration by applying the bulk export script again. The verification process may require several iterations. You can repeat the process until the bulk export procedure does not report any issues in which case the bulk configuration structures will also contain the valid configuration. If the "Exp" content is large, select only the records that have one or more stars '*' in the "Message" field. These would be the messages that require your attention.

See more information in the "Exporting CCAdv/WA Configuration" section of this guide.

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)

Procedure:

Steps

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 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.

Procedure:

Steps

- Open Microsoft SQL Server Management Studio and register a connection to Advisors Platform database.
- Navigate to the Advisors Platform database and launch the import tool for one of the created tables.
- Follow the import wizard instructions.
- Import the data from each file that contains prepared configuration data.
  Using MS SQL Server, you can load data 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.

MS SQL Server Import is very sensitive to special characters which, if present in the files, can trigger an import failure accompanied by a message that might seem completely unrelated and will not

explain the actual reason. Make sure that the files are clean. Special characters are often invisible; to avoid import failure, check the files for unnecessary empty trailing spaces, as well as 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 might contain such characters.

Bulk Configuration Validation and Logs

The contact group bulk configuration procedure (spblkConfigCCadvWAIntegrated) 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 spblkConfigCCadvWAIntegrated 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, geographic regions, reporting regions, and operating units contained in the associated columns. The applications for which all names are resolved (all objects with those names are found in the Platform database and their IDs can be located through associations and assignments) are added to the existing CCAdv configuration and included in the rollup. The `Include in Rollup` property can be controlled from the utility; that is, the property's value can be supplied in the relevant column in 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 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, geographic region, reporting region, and operating unit specified in the row with the contact group. The procedure also includes the contact group in the rollup. The

`Include in Rollup` property can be controlled from the utility; that is, the property's value can be supplied in the relevant column in 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 then 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.

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. 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 blkAll 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.

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.

If you plan to deploy Pulse Advisors release 9.0.001.06 or later and you will use the bulk configuration tool, then see the Changes to Bulk Configuration section on the Bulk Configuration Overview page in this guide before you proceed.

You can use the bulk configuration 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. Starting with release 9.0.001, the default configuration mode is the independent configuration mode. Previously, the integrated configuration mode was deployed as the default mode.

In releases prior to release 8.5.2, the bulk configuration tool required the presence of the business hierarchy objects (regions, operating units, application groups, and contact centers) in the Advisors configuration. You had to first add the business hierarchy data to the Genesys Configuration Server's **Business Attributes** folder, and then manually activate the same objects using the Advisors administration module. Starting with release 8.5.2, none of that is necessary prior to using the bulk configuration tool; the bulk configuration tool now has a business hierarchy bulk configuration feature. All business hierarchy names will be automatically added to the Advisors configuration and activated. All new business attributes can then be added to the Genesys Configuration Server's **Business Attributes** folder using the migration wizard supplied in the installation package.

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 Database Objects Used in Bulk Configuration Process

The blkObjectsDrop.sql script removes all database objects used in the bulk configuration (such as the tables and procedures 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 or bulk export tables. 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 during the Platform database/schema deployment and which is identical for any configuration mode. 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 export utility to generate a "clean" copy of blk tables from the existing application configuration before you run the configuration removal procedure. 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

Starting with release 8.5.2, the contact centers, regions, operating units, and application groups that you will use in the bulk configuration structures do not need to be present in the Genesys Configuration Server, nor do they need to be visible in the Advisors configuration pages at the time that you run the bulk configuration procedure. The bulk configuration tool automatically adds all hierarchy objects to the Advisors configuration as long as they are entered in the bulk configuration structures, and if they are not currently present in the Advisors configuration. 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.

Review the following considerations before using the bulk configuration import procedure:

- A contact center will be added to the configuration only if the corresponding Geographic Region name is supplied.
- If a contact center is already present in your configuration, then the bulk configuration import process will make no changes to the existing contact center configuration. 35px|link= Starting with release 9.0, if the geographic region of the existing contact center is "Unknown" while a valid geographic region name is supplied in the bulk configuration structures, the bulk configuration procedure will substitute the "Unknown" geographic region for this contact center accordingly.
- A contact center that is automatically added to the configuration as part of the bulk configuration process will be assigned the default value for opening ("00:00") and the default value for closing time ("23:59"). If you need to change those values, then you must adjust those properties manually using the **Contact Center** page in the administration module.
- A contact center that is automatically added to the configuration as part of the bulk configuration process will be assigned the local time zone if the contact center name does not match any geographic location in the list of time zones. If the matching location is found in the time zone list, then the time zone associated with that geographic location will be assigned to the contact center. An administrator can adjust the time zone property at any time. It is important to adjust the time zone property in accordance with the actual contact center time zone if the open and close times are different than the default values ("00:00"/"23:59").
- A contact center that is automatically added to the configuration as part of the bulk configuration process will always be of the "Network" type. If you need to create a "Site" contact center, then you must manually configure it on the **Contact Center** configuration page of the Advisors administration module *before* you execute the bulk configuration procedure.
- The application server and XML Generator service must be up and successfully running until the required data (see the following bullet point) 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 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.

Considerations for SL Threshold Bulk Configuration

The bulk configuration tool accepts the SL Threshold property, which you enter in the `CustomSLThreshold` field. For more information, see Data Preparations below.

Be sure to follow these rules if you use SL Threshold values that are not the default value (20 seconds):

- The CustomSLThreshold field is measured in seconds; enter values accordingly.
- If you do not supply a value in the CustomSLThreshold field before you run the bulk configuration import procedure, the default value of 20 seconds will be assigned to the corresponding application, even if the current value is different.
- Only the predetermined SL Threshold values shown in the THRESHOLD_VALUE column of the database table are allowed:

NAME	THRESHOLD_VALUE
Unknown	0
10 sec	10
20 sec	20
30 sec	30
40 sec	40
45 sec	45
50 sec	50
60 sec	60
70 sec	70
80 sec	80
90 sec	90
5 min	300
8 min	480

If you enter an SL Threshold value in the bulk configuration structure that is not listed in the SL_THRESHOLD database tables, the configuration of the related application will be skipped and an error will be registered in the bulk configuration log file.

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.

Procedure:

Steps

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. 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
6. Connect to the Oracle or SQL Server instance as the platform user.
7. 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.
8. Populate the blk database tables with your application and agent group configuration data.

   For information about preparing your data, see Data Preparations

   For information about importing data from spreadsheets to the database, see Loading Data from Spreadsheets into Temporary Database Structures section.
9. Execute the spblkConfigCCadvIndependent procedure; for example, use the following string with an Oracle schema:

```
DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkConfigCCAdvIndependent"
(
M => M,
R => R
);
END;
```

In an MS SQL Server installation, execute the procedure as follows:

```
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 9.
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 11. 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 9.

       To remove the entire configuration in Oracle installations, execute the following:

       ```
       DECLARE
       M VARCHAR2(200);
       R NUMBER;
       BEGIN
       "spblkRemoveConfigCCAdv"
       (
       M => M,
       R => R
       );
       END;
       ```

       To remove the entire configuration in MS SQL 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
       ```

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, geographic region, reporting region, and operating unit names. 35px|link= Starting with release 9.0, your file must contain three additional columns with headers (headers are mandatory). Bulk configuration application names no longer require the concatenation [tenant name] [base object name or number] / filter name@switch name. Instead the bulk configuration structure contains separate fields for the former parts of object names. The Application Name column should only contain the base object name or number as it appears in the Configuration Server. The tenant name, filter name and switch name can be provided in separate columns where applicable or if necessary. Provide the following information in the file:

- Application Name
- Application Display Name
- Contact Center Name
- Geographic Region Name (to allow Contact Center bulk configuration)
- Application Group Name
- Reporting Region Name
- Operating Unit Name
- Custom SL Threshold Value (provide this only if you use a value other than the default value of 20 seconds)
- Application Include in Rollup Property
- 35px|link=Application Switch Name (if applicable, see the Guidelines below)
- 35px|link=Application Tenant Name (if applicable, see the Guidelines below)
- 35px|link=Application Filter Name (if necessary ans applicable, see the Guidelines below)

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, geographic region, 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. If the geographic region is not provided, and the associated contact center is not yet present in the Advisors configuration, the contact center will not be created and the application configuration will not be added. A corresponding message will be written in the blkAppLog table. If the geographic region is not supplied, but the contact center is already present, no error will be logged, and the application configuration will be added to the Advisors rollup configuration, unless other issues are detected. If a contact center is already present in the Advisors configuration, but the geographic region that is supplied in the bulk configuration data does not match the existing geographic region property, no changes will be made to the existing contact center geographic region property. 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 along with the tenant, switch and filter name) must match the name contained in the tmpImportCallType.PeripheralName, tmpImportInteractionQueue.PeripheralName, or tmpImportApp.PeripheralName column of the Platform database. 35px|link= Starting with release 9.0 each column with application names should contain only the base object names or numbers as they appear in the name or number property of the corresponding object in the Configuration Server or in the Name field of the Platform database table CFG_IMPORTED_OBJECTS.
- 35px|link= Starting with release 9.0 the tenant name is provided in a separate column if applicable. If you know that the name of the object is unique across all tenants in the Configuration Server, the tenant name can be omitted.
- 35px|link= Starting with release 9.0 the application switch name is provided in a separate column if applicable. If you know that the name of the object is unique across all switches within the mentioned tenant or across all switches in the Configuration Server, the switch name can be omitted.
- 35px|link= Starting with release 9.0 the filter name is provided in a separate column if applicable. In this case the object will be configured with the object segmentation filter which will be applied to all filterable metrics applicable to the object. The filter will not be applied to the metrics that have "Exclude from Base Object Filter" property enabled. The filtered object configured by the bulk configuration tool will be treated as configured with the object segmentation filter even if the filter itself does not have the "ObjectSegmentationFilter" option (35px|link= in release 9.0) set to "true" or "yes". In order to be applied in the statistics requests , the filter must be registered in the Configuration Server as a business attribute under the "Advisors Filters" folder and contain the filter definition under the "Filter" section in the "Filter" option. If you already have filters registered in the "Advisors Filters" folder with the definitions contained in the "Description" property, use the migration wizard to move the existing filter definitions into the "Filter" section.
- Filters are not applicable to interaction queues and calling lists.
- An empty cell, or any values in the `Include in Rollup` property that are different from `Y` or `N` are interpreted as `Y` (for information about the `Application Include in Rollup Property` column, 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. 35px|link= Starting with release 9.0, your file must contain 5 additional columns with headers (headers are mandatory). Bulk configuration application and agent group names no longer require the concatenation [tenant name] [base object name or number] / filter name@switch name. Instead the bulk configuration structure contains separate fields for the former parts of object names. The Application Name and the Agent Group Name columns should only contain the base object names or numbers as they appear in the Configuration Server. The tenant name, filter name and switch name can be provided in separate columns where applicable or if necessary.

Your file must contain the following columns with headers and provide the following information:

- Application Name
- Agent Group Name
- Agent Group Contact Center Name
- 35px|link=Application Filter Name (if necessary and applicable, see the Guidelines for Applications above)
- 35px|link=Agent Group Filter Name (if necessary , the guidelines are similar to the ones for Applications)
- 35px|link=Application Tenant Name (if applicable, see the Guidelines for Applications above)
- 35px|link=Agent Group Tenant Name (if necessary, the guidelines are similar to the ones for Applications)
- 35px|link=Application Switch Name (if applicable, see the Guidelines for Applications above)

Add relevant data to the spreadsheet or file under the column headers. You then import this data into the blkAppAgntGr 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. 35px|link= Starting with release 9.0 the name must match the Name field content in the Configuration Server or in the Platform database table CFG_IMPORTED_OBJECTS.

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.

General Data Preparation Guidelines

- If your platform database contains bulk configuration data generated in a previous version, applying the blkObjCre.sql script of the new version in the platform database migrated to the new version will migrate the bulk configuration data to the form required in the new version. If you have bulk configuration data stored outside the database, it can be imported "as is" and then migrated to the

form required in the new version by applying the blkObjCre.sql supplied with the new version installation package. It is safe to apply blkObjCre.sql several times. It will migrate the older schema and transform the data as well as preserve the configuration data content.

- If you have a platform database with the existing Advisors configuration but do not have a corresponding copy of the bulk configuration data, you can generate the bulk configuration data in the form required in the new version by applying the bulk export script to the Platform database migrated to the new version. The bulk export script will not remove any existing bulk configuration content. If any, the previous content will be moved to the tables that have identical names with appended timestamps. You can use the content in tables that have "Exp" in their names to review the validity of your current configuration. You then can address the reported warnings or problems by editing the exported bulk configuration data and then by removing and replacing the configuration by using the bulk removal and then the bulk configuration procedure. You also can address the reported issues by applying the changes in the Administration module and verifying the configuration by applying the bulk export script again. The verification process may require several iterations. You can repeat the process until the bulk export procedure does not report any issues in which case the bulk configuration structures will also contain the valid configuration. If the "Exp" content is large, select only the records that have one or more stars '*' in the "Message" field. These would be the messages that require your attention.

See more information in the "Exporting CCAdv/WA Configuration" section of this guide.

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)

Procedure:

Steps

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.

Procedure:

Steps

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.
   Using 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.

MS SQL 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.

Correct Configuration Validation in Advisors Administration Module

Execution of the spblkConfigCCadvIndependent procedure results in the following configuration, which you can validate in the Advisors Administration module:

- Associates applications contained in the blkAppNames table with contact centers, application groups, geographic regions, reporting regions, and operating units contained in the associated columns. The applications for which all names are resolved (all objects with those names are found in the Platform database and their IDs can be located through associations and assignments) are added to the existing CCAdv configuration and included in the rollup. The `Include in Rollup` property can be controlled from the utility; that is, the property's value can be supplied in the relevant column in the blkAppNames

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 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).

- Establishes relationships between applications and agent groups contained in the blkAppAgntGr table.
- Records the outcome in the blkAppLog table, which you can examine after the procedure exits.

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.

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. 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.

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 Workforce Advisor (WA) contact groups; the bulk configuration tool configures WA rollups outside of the Advisors administration module.

If you plan to deploy Pulse Advisors release 9.0.001.06 or later and you will use the bulk configuration tool, then see the Changes to Bulk Configuration section on the Bulk Configuration Overview page in this guide before you proceed.

You can use the bulk configuration 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. Starting with release 9.0.001, the default configuration mode is the independent configuration mode. Previously, the integrated configuration mode was deployed as the default mode.

In releases prior to release 8.5.2, the bulk configuration tool required the presence of the business hierarchy objects (regions, operating units, application groups, and contact centers) in the Advisors configuration. You had to first add the business hierarchy data to the Genesys Configuration Server's **Business Attributes** folder, and then manually activate the same objects using the Advisors administration module. Starting with release 8.5.2, none of that is necessary prior to using the bulk configuration tool; the bulk configuration tool now has a business hierarchy bulk configuration feature. All business hierarchy names will be automatically added to the Advisors configuration and activated. All new business attributes can then be added to the Genesys Configuration Server's **Business Attributes** folder using the migration wizard supplied in the installation package.

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 Database Objects Used in Bulk Configuration Process

The blkObjectsDrop.sql script removes all database objects used in the bulk configuration (such as the tables and procedures 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 or bulk export tables.

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 WA configuration, run the spblkRemoveConfigWA stored procedure, which is created during the Platform database/schema deployment and which is identical for any configuration mode. 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 export utility to generate a "clean" copy of blk tables from the existing contact group configuration before you run the configuration removal procedure. 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

Starting with release 8.5.2, the contact centers, regions, operating units, and application groups that you will use in the bulk configuration structures do not need to be present in the Genesys Configuration Server, nor do they need to be visible in the Advisors configuration pages at the time that you run the bulk configuration procedure. The bulk configuration tool automatically adds all hierarchy objects to the Advisors configuration as long as they are entered in the bulk configuration structures, and if they are not currently present in the Advisors configuration. 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.

Review the following considerations before using the bulk configuration import procedure:

- A contact center will be added to the configuration only if the corresponding Geographic Region name is supplied.
- If a contact center is already present in your configuration, then the bulk configuration import process will make no changes to the existing contact center configuration. 35px|link= Starting with release 9.0, if the geographic region of the existing contact center is "Unknown" while a valid geographic region name is supplied in the bulk configuration structures, the bulk configuration procedure will substitute the "Unknown" geographic region for this contact center accordingly.
- A contact center that is automatically added to the configuration as part of the bulk configuration

process will be assigned the default value for opening ("00:00") and the default value for closing time ("23:59"). If you need to change those values, then you must adjust those properties manually using the **Contact Center** page in the administration module.

- A contact center that is automatically added to the configuration as part of the bulk configuration process will be assigned the local time zone if the contact center name does not match any geographic location in the list of time zones. If the matching location is found in the time zone list, then the time zone associated with that geographic location will be assigned to the contact center. An administrator can adjust the time zone property at any time. It is important to adjust the time zone property in accordance with the actual contact center time zone if the open and close times are different than the default values ("00:00"/"23:59").
- A contact center that is automatically added to the configuration as part of the bulk configuration process will always be of the "Network" type. If you need to create a "Site" contact center, then you must manually configure it on the **Contact Center** configuration page of the Advisors administration module *before* you execute the bulk configuration procedure.
- The application server and XML Generator service must be up and successfully running until the required data (see the following two bullet points) 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.

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).

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.

Procedure:

Steps

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. 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
6. Connect to the Oracle or SQL Server instance as the platform user.
7. 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.
8. 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.
9. Execute the spblkConfigWAIndependent procedure; for example, use the following string with an Oracle schema:

```
DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkConfigWAIndependent"(
M => M,
R => R
);
END;
```

   In an MS SQL Server installation, execute the procedure as follows:

```
USE <name of Advisors database>
GO
DECLARE @return_value int,
@r int,
@m varchar(255)
EXEC spblkConfigWAIndependent
@r = @r OUTPUT,
@m = @m OUTPUT
SELECT @r as N'@r',
@m as N'@m'
GO
```

10. Verify the log stored in the blkCgLog 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 9. If no correction is necessary, go to the next Step.

12. Examine the Contact Group Configuration page in the Advisors Administration module to verify the configuration.
13. Examine the WA dashboard to verify the configuration.
14. 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 11. 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 9. You can remove the whole configuration by executing the spblkRemoveConfigWA procedure.

       To remove the entire configuration in Oracle installations, execute the following:

```
DECLARE
M VARCHAR2(200);
R NUMBER;
BEGIN
"spblkRemoveConfigWA"
(
M => M,
R => R
);
END;
```

       To remove the entire configuration in MS SQL Server installations, the procedure calls are done 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
```

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, geographic region, reporting region, and operating unit names. Starting with release 8.5.2, your file must contain eight columns with headers (headers are mandatory).

Provide the following information in the file:

- Contact Group Name
- Contact Group Display Name
- Contact Center Name
- Geographic Region Name (to allow Contact Center bulk configuration)
- Application Group Name
- Reporting Region Name
- Operating Unit Name
- Contact Group Include in Rollup Property

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, geographic region, 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. If the geograpic region is not provided, and the associated contact center is not yet present in the Advisors configuration, the contact center will not be created and the application configuration will not be added. A corresponding message will be written in the blkCgLog table. If the geographic region is not supplied, but the contact center is already present, no error will be logged, and the application configuration will be added to Advisors rollup configuration, unless other issues are detected. If a contact center is already present in the Advisors configuration, but the geographic region that is supplied in the bulk configuration data does not match the existing geographic region property, no changes will be made to the existing contact center geographic region property. The whole content of the data row is rejected if any incomplete configuration is detected or there are names that cannot be resolved.
- An empty cell, or any values in the `Include in Rollup` properties that are different from `Y` or `N` are interpreted as `Y` (for information about the `Contact Group Include in Rollup Property` column, 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 the following columns with headers and provide the following information:

- 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

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` (for information about the `Contact Group Include in Rollup Property` column, see Contact Groups mapped to AGCC above).

Contact Groups and Related Applications

The word *application*, as used with Advisors WA component, refers to Advisors objects that originate from the following:

- Genesys ACD and virtual queues

- Genesys DN Groups
- 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. Provide the relationships by supplying the corresponding pairs of contact group and application name. 35px|link= Starting with release 9.0, your file must contain three additional columns with headers (headers are mandatory). Bulk configuration application names no longer require the concatenation [tenant name] [base object name or number] / filter name@switch name. Instead the bulk configuration structure contains separate fields for the former parts of object names. The Application Name column should only contain the base object name or number as it appears in the Configuration Server. The tenant name, filter name and switch name can be provided in separate columns where applicable or if necessary. Your spreadsheet or CSV file for this information contains the following columns:

- Contact Group Name
- Application Name
- 35px|link=Application Switch Name (if applicable, see the Guidelines below)
- 35px|link=Application Tenant Name (if applicable, see the Guidelines below)
- 35px|link=Application Filter Name (if necessary ans applicable, see the Guidelines below)

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 tmpImportCallType.PeripheralName or tmpImportApp.PeripheralName column of the Platform database. 35px|link= Starting with release 9.0 each column with application names should contain only the base object names or numbers as they appear in the name or number property of the corresponding object in the Configuration Server or in the Name field of the Platform database table CFG_IMPORTED_OBJECTS.
- 35px|link= Starting with release 9.0 the tenant name is provided in a separate column if applicable. If you know that the name of the object is unique across all tenants in the Configuration Server, the tenant name can be omitted.
- 35px|link= Starting with release 9.0 the application switch name is provided in a separate column if applicable. If you know that the name of the object is unique across all switches within the mentioned tenant or across all switches in the Configuration Server, the switch name can be omitted.
- 35px|link= Starting with release 9.0 the filter name is provided in a separate column if applicable. In

this case the object will be configured with the object segmentation filter which will be applied to all filterable metrics applicable to the object. The filter will not be applied to the metrics that have "Exclude from Base Object Filter" property enabled. The filtered object configured by the bulk configuration tool will be treated as configured with the object segmentation filter even if the filter itself does not have the "ObjectSegmentationFilter" option (35px|link= in release 9.0) set to "true" or "yes". In order to be applied in the statistics requests , the filter must be registered in the Configuration Server as a business attribute under the "Advisors Filters" folder and contain the filter definition under the "Filter" section in the "Filter" option. If you already have filters registered in the "Advisors Filters" folder with the definitions contained in the "Description" property, use the migration wizard to move the existing filter definitions into the "Filter" section.

Contact Groups and Related Agent Groups

You can associate contact groups that are mapped to network contact centers with agent groups.

Contact groups that are related to AGCC can be mapped only to agent groups that are mapped to AGCC and are identified as agent groups to include in WA.

Your spreadsheet or CSV file for this information contains the relationships between contact groups and agent groups provided as pairs of the related contact group name and agent group name. 35px|link= Starting with release 9.0, your file must contain 2 additional columns with headers (headers are mandatory). Bulk configuration agent group names no longer require the concatenation [tenant name] [base object name or number] / filter name. Instead the bulk configuration structure contains separate fields for the former parts of object names. The Agent Group Name column should only contain the base object names as they appear in the Configuration Server. The tenant name and the filter name can be provided in separate columns where applicable or if necessary.

- Contact Group Name
- Agent Group Name
- AGCC Name
- 35px|link=Agent Group Filter Name (if necessary , the guidelines are similar to the ones for Applications)
- 35px|link=Agent Group Tenant Name (if necessary, the guidelines are similar to the ones for Applications)

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. 35px|link= Starting with release 9.0 the agent group name must match the Name field content in the Configuration Server or in the Platform database table CFG_IMPORTED_OBJECTS.
- 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. 35px|link= Starting with release 9.0, your file must contain 2 additional columns with headers (headers are mandatory). Bulk configuration agent group names no longer require the concatenation [tenant name] [base object name or number] / filter name. Instead the bulk configuration structure contains separate fields for the former parts of object names. The Agent Group Name column should only contain the base object names as they appear in the Configuration Server. The tenant name and the filter name can be provided in separate columns where applicable or if necessary.

Example of content in an blkAgntGrNames file

In releases prior to 9.0:

AGNTGRNAME	AGNTGRDISPLAYNAME
V_THO_PK_TR_EntertainIP_Generalist_KristallRetention_100/F1	KristallRetention_100_cca
[Tenant1] V_IDR_PK_CF_Kundenbindung_120	Kundenbindung_120

35px|link=Starting from release 9.0

AGNTGRNAME	AGNTGRDISPLAYNAME	"AGNTGRFILTERNAME"	"AGNTGROUPTENANTNAME"
V_THO_PK_TR_EntertainIP_Generalist_KristallRetention_100/F1	KristallRetention_100		
V_IDR_PK_CF_Kundenbindung_120	Kundenbindung_120		Tenant1

General Data Preparation Guidelines

- If your platform database contains bulk configuration data generated in a previous version, applying the blkObjCre.sql script of the new version in the platform database migrated to the new version will migrate the bulk configuration data to the form required in the new version. If you have bulk configuration data stored outside the database, it can be imported "as is" and then migrated to the form required in the new version by applying the blkObjCre.sql supplied with the new version installation package. It is safe to apply blkObjCre.sql several times. It will migrate the older schema and transform the data as well as preserve the configuration data content.

- If you have a platform database with the existing Advisors configuration but do not have a corresponding copy of the bulk configuration data, you can generate the bulk configuration data in the form required in the new version by applying the bulk export script to the Platform database migrated to the new version. The bulk export script will not remove any existing bulk configuration content. If any, the previous content will be moved to the tables that have identical names with appended timestamps. You can use the content in tables that have "Exp" in their names to review the validity of your current configuration. You then can address the reported warnings or problems by editing the exported bulk configuration data and then by removing and replacing the configuration by using the bulk removal and then the bulk configuration procedure. You also can address the reported issues by applying the changes in the Administration module and verifying the configuration by applying the bulk export script again. The verification process may require several iterations. You can repeat the process until the bulk export procedure does not report any issues in which case the bulk configuration structures will also contain the valid configuration. If the "Exp" content is large, select only the records that have one or more stars '*' in the "Message" field. These would be the messages that require your attention.

See more information in the "Exporting WA Configuration" section of this guide.

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

Procedure:

Steps

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, geographic regions, 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, geographic regions, 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.

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. 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.

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.

Frontline Advisor

This section contains information and procedures to help you change configuration for Frontline Advisor after you have deployed the module.

Frontline Advisor Configuration Parameters

This page contains information about the Frontline Advisor (FA) configuration properties file (`<Advisors>/conf/FrontlineAdvisor.properties`). Use this information to help you to edit the FA configuration. All of the parameters listed are either specified during installation of Frontline Advisor, or set to an appropriate default, and are generally not expected to need to be changed.

Parameter	Description
__failure_notification_fromAddress	Sender email address used for notifications sent from Frontline Advisor
__failure_notification_toAddress	Email address where notifications from Frontline Advisor should be directed to
plt.database.type	Indicates what RDBMS is being used for the Advisors Platform database: either Oracle or Microsoft SQL Server
link.out.url.template	A legacy parameter of the Frontline Advisor Agent Advisor dashboard which is no longer present in the 8.5.2 release.
__checkDBConnectivity_JobFrequency_inMilliSecs	Frequency (in milliseconds) Frontline Advisor will check for DB connection issues and send notifications to the FA administrator if one is discovered. The impact of this check on the database during normal operation should be negligible and not normally need to be adjusted.
__resetStateMachine_JobFrequency_inMilliSecs	Specifies how often (in milliseconds) the system will check for a High Availability (HA) or connectivity status initiated aggregation process reset. The default (5 sec) is a negligible fraction of the total time required for resetting of the aggregation process, and should not normally need to be adjusted.
__allowed_state_refresh_rates	Specified which time intervals are available for selection in FA administration for state metrics. Note: Do not change these values unless you are sure the values are supported by the Connector
__allowed_performance_rule_refresh_rates	Specified which time intervals are available for selection in FA administration for performance metrics. Note: Do not change these values unless you are sure the values are supported by the Connector
hierarchy.tenantname.{0,1,2}	The Configuration Server Tenant that the corresponding hierarchy path (see hierarchy.root.foldername.{0,1,2}) belongs to.
hierarchy.root.foldername.{0,1,2}	Path(s) to the root(s) of the Frontline Advisor hierarchy in the Configuration Server. If multiple hierarchy roots are configured they will be displayed together under a combined "Enterprise" root element in the Advisors dashboard

Parameter	Description
hierarchy.reload.cronExpression	Specifies a schedule for reloading of the entire FA hierarchy. By default this is configured to run daily at 02:55 based on the system time (generally outside of business hours). If you wish to adjust this schedule refer to documentation on the cron trigger syntax
hierarchy.dynamicUpdate.maxBatchSize	All update events which can be read from the Configuration Server at one time will be batched together for reconciling with FA adapter(s). This parameter allows for specifying a maximum batch size to limit the batch size and ensure that changes are eventually reflected within FA in situations where there is an indefinitely long or continuous stream of updates. Any series of updates smaller in number than this maximum size is of course applied immediately.
hierarchy.dynamicUpdate.subscribe	Toggles subscription to update events from the Configuration Server which are used to update the FA hierarchy. Enabled by default, but can be disabled if the hierarchy is not changed, or changes do not need to be reflected in Frontline Advisor immediately. Scheduled reload of the hierarchy will still take place.
message.listening.port	Port on which FA listens for connections from Adapter for source metric reporting. Set this to a static port, or zero, in which case any available port will be used
is.distributed	Indicates if Frontline Advisor will persist its data in the Advisors distributed cache. Note: This is not intended to be set to false. The new Advisors Web Services serves data for all Advisors modules now. The serving of FA data for single-instance only configurations from a non-distributed cache is no longer supported.
enable.rollup.engine	Specifies if the rollup engine (aggregation process) should run. Note: This is not intended to be changed after installation since installing with the aggregation process enabled also requires high availability (HA) integration with the Genesys Management Framework. Enabling/disabling this process after installation may result in Frontline Advisor failing to start or working incorrectly
rollup.engine.timeout	Timeout in minutes to wait for an actively running aggregation process to complete before initiating high availability (HA) failover
accessibleDashboard.nodeDisplayLimit	Maximum number of teams, agents, folders which can be displayed in the FA accessible dashboard. Note: increasing this limit may negatively impact the performance of Advisors
accessibleDashboard.metricDisplayLimit	Maximum number of metrics which can be displayed in the FA accessible dashboard. Note: increasing this limit may negatively impact the

Parameter	Description
	performance of Advisors

Features Overview

The Features Overview section contains descriptions of the Pulse 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 Advisors 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 Advisors 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

Pulse 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 a Genesys configuration interface, such as Genesys Administrator. LCA, SCS, and the management interface manage the primary/backup pair of applications.

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

Some Advisors modules must integrate with the Solution Control Server, while others do not. 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 Natively Integrated With SCS

The following Advisors modules are integrated with the LCA, SCS, and the Genesys Management Layer user interface (for example, Genesys Administrator) to support warm standby:

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

NEW The following Advisors modules are integrated with the LCA, SCS, and the Genesys Management Layer user interface (for example, Genesys Administrator):

- Advisors Web Services (ADVWS)

  These modules do not support warm standby. They support n+1 high availability. You can start and stop them using the SCS user interface, but you cannot configure them with a backup server to which they fail over.

If deployed in the same Tomcat server with a module that does support warm standby, ADVWS can run in a server that is executing in Backup mode, but ADVWS itself does not have a backup mode. In such a server, ADVWS continues to provide web services as if the server's execution mode were Primary.

Because all of the preceding modules are integrated with the Management Layer, you must proceed as follows:

1. Install and run the LCA on a system that runs any of the preceding modules.
2. Configure a Host for the system in your Genesys configuration interface, such as Genesys Administrator.
3. Configure an Application in your Genesys configuration interface for each Advisors server that runs one or more of the preceding modules.
4. If you have a license for an HA deployment, and the the module supports warm standby, configure a second Application in your Genesys configuration interface for the secondary server. Associate the two Applications as a primary and backup pair for failover.
5. Specify the properties, during installation, that permit the Advisors server to integrate with the LCA, SCS, the Application, and the Host.
6. Do not create a Windows or Linux service to control the module because SCS will control it.

For detailed instructions about carrying out the preceding tasks, see Overview: Configuring Advisors Application Objects and Deploying Modules that are Controlled by SCS.

[+] Advisors Modules that do not Support HA

The following Advisors modules are not automatically highly-available:

- 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.

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

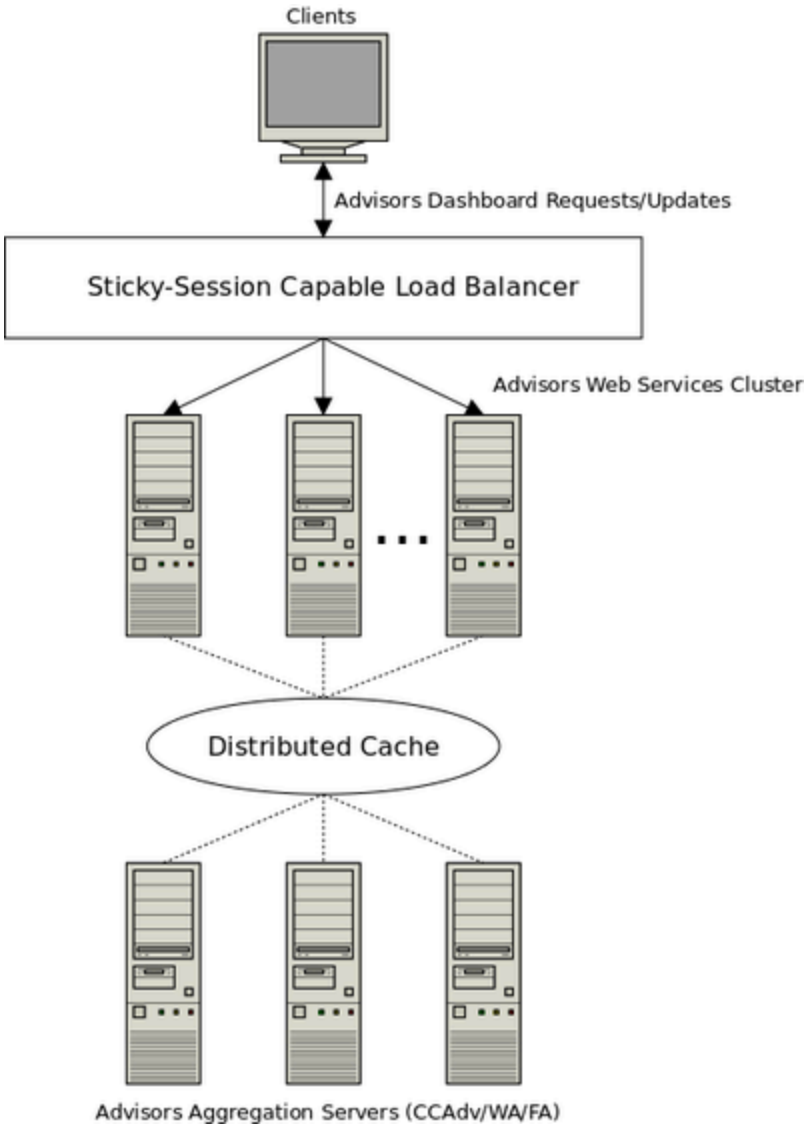
This page provides information about scaling your Pulse Advisors Web Services in order to increase capacity in your environment.

Advisors Web Services Module

The Advisors Web Services module is offered as part of the Platform installation package. It contains the Web services responsible for delivering updates to, and handling requests for, the Contact Center Advisor, Workforce Advisor, and Frontline Advisor dashboards. These Web services retrieve the data produced by the Advisors aggregation servers, and which is held in a shared distributed cache, and deliver it to the Advisors user's dashboards that are running in a Web browser.

Layout

The following diagram provides a high-level view of how a scalable Web services deployment is structured. Note that, for simplicity, other supporting Advisors/Genesys components are not included in the diagram.



Scaling

To serve more Advisors dashboard users, you can deploy additional instances of the Advisors Web Services module. The Web services handle requests and updates for all Advisors modules. When adding additional user capacity, you deploy the same type of instance, regardless of the particular Advisors module that users are planning to use.

Recommendations

- For best performance, the Advisors Web Services module should be deployed to its own server, which is not running any other major Advisors and/or Genesys components. Because the responsiveness of the Advisors dashboards at any given moment depends on the performance of these Web services, it is important to ensure that they have the necessary system resources available at all times. Avoid running resource-intensive jobs, and so on, on these instances for the best experience.

- Users accessing the Web services instances are ideally distributed equally across the cluster. This might be challenging because established, persistent connections cannot be redirected to other servers. Investigating the different load distribution strategies available in your particular load balancer might be helpful in trying to maintain a healthy balance as users connect/disconnect.
- In addition to providing load distribution, many load balancers also offer options to redirect traffic away from unresponsive servers. For availability purposes, consider having additional capacity in your Web services cluster. The Web service instances provide a health check resource that can be accessed without authentication by load balancers and other devices as a means of checking the instance's availability. See the notes on the Health Check API for technical details.

Simplified High Availability Architecture

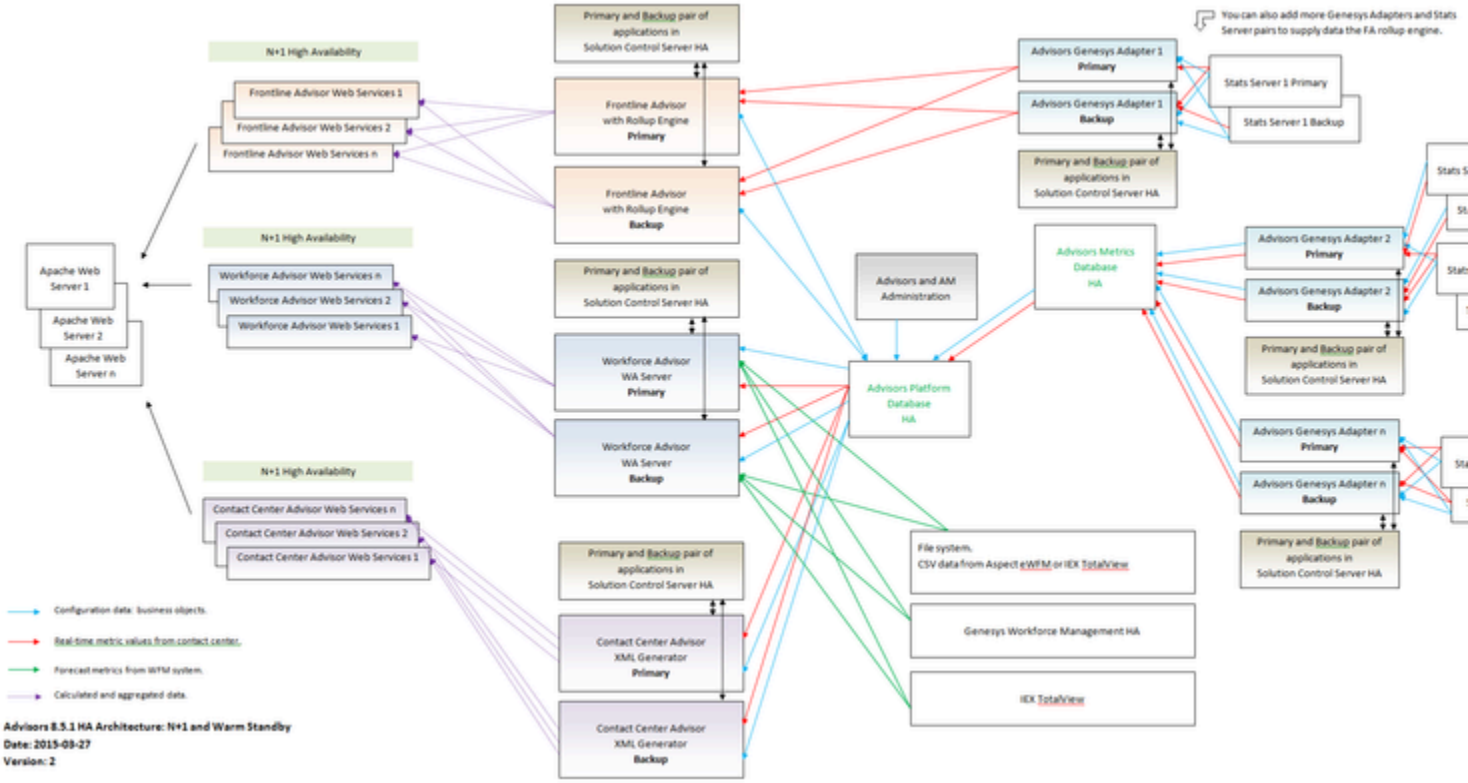
The Figure on this page shows that Advisors supports two kinds of High Availability (HA), by default.

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.

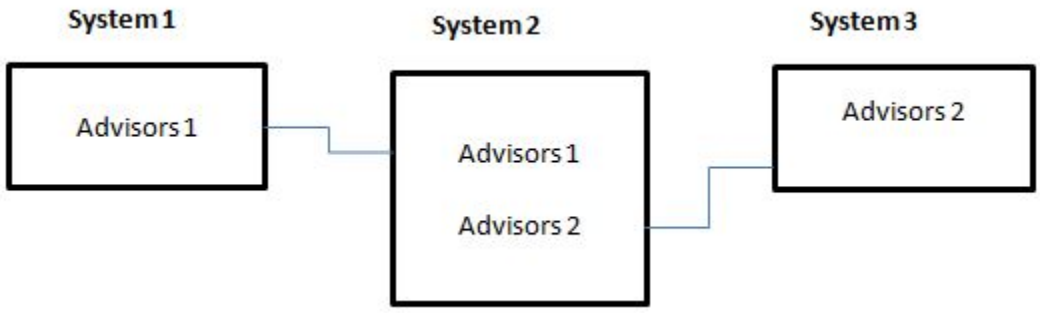
You can also manually configure any Advisors module to offer Cold Standby HA.



Simplified Advisors Architecture in Warm Standby Configuration

Multiple Advisors Deployments on One System

You can deploy more than one distinct Advisors deployment 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 Apache Tomcat configurable ports. The properties of the Apache Tomcat configurable ports are defined in `apache-tomcat-<version>\conf\catalina.properties`.

  The Platform application server will not work correctly if there are ports that are not defined or if there are invalid port numbers.

  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 Apache Tomcat configurable ports are the

following:

- HTTP Port=8080
- HTTPS Port=8443
- AJP Port=8009
- JMX Port=9999
- Management Port=8005

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	apache-tomcat-<version>\conf\catalina.properties	HTTPPort, HTTPSPort, JMXPort, managementPort, 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 Workforce Advisor contains an FTP server that accepts data directly from the IEX TotalView data source.

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
- HTTPSPort=8443
- JMXPort=9999
- AJPPort=8009
- managementPort=8005
- 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
- HTTPSPort=8444
- JMXPort=10000
- AJPPort=8010
- managementPort=8006
- ftpService.port=6022

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.
- 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.

Tenant-based Routing of Advisors Objects Among Multiple Adapters and Stat Servers

You can configure a pool of adapters for both Contact Center Advisor and Frontline Advisor, and each adapter can be configured to use a pool of Stat Servers. Data Manager and the adapters use a round-robin mechanism to determine the selection of Stat Servers from the pool when requesting statistics for a given source object.

In multi-tenant configuration, each object's tenant must be considered for object routing, but not all of the Stat Servers are necessarily connected to all of the tenants. When statistics are requested on a Stat Server that is not connected to the necessary tenant, an error occurs and the Stat Server cannot report on the objects. To avoid the necessity of having to connect all of the Stat Servers to all of the tenants, Advisors applications use tenant-based routing. Tenant-based routing uses the Stat Server-tenant link, which you configure with a Genesys configuration interface such as Genesys Administrator, to determine how Data Manager will route objects to the pool of adapters and how each adapter will route objects to a particular Stat Server within the pool of Stat Servers.

Linked tenants display in the **Server Info** section of a Stat Server Application object. At startup, Data Manager and the adapters read the Stat Server-to-tenant associations that are present in Configuration Server. They use that information to determine to which Stat Server to route the statistics request for a particular source object.

For information about how to create an Application object, including how to add a tenant to the Application, see the Applications page in the *Genesys Administrator Extension Help.*

Carefully plan and configure the Stat Server-tenant links. Tenant-based routing of objects among Stat Servers can sometimes result in an unequal distribution of statistics among the configured pool of Stat Servers, which can, in turn, lead to an unequal distribution of statistics among the adapters. When configuring the tenant connections to Stat Servers, try to take into account the number of source objects that will be served from each linked tenant. If certain tenants have fewer objects for Advisors than others, then consider linking multiple tenants to each Stat Server as a way to avoid overloading some of the Stat Servers with large numbers of objects.

Making Updates to Stat Server-Tenant Links after Initial Configuration

Genesys recommends that you avoid making changes to the Stat Server-tenant links after the Stat Servers are in use in an Advisors deployment. Making changes to the Stat Server-tenant links after the configuration is established and in use can negatively impact performance in the Advisors installation because an existing, stored distribution mapping of objects-to-Stat Servers is always used as long as it is relevant. That means that the mapping is not modified for the sake of equal re-distribution of statistics.

For example, if you add a new tenant to a Stat Server, the Stat Server and the corresponding adapter would be considered only for any *new* source objects from that tenant. No automatic re-routing of

statistics is performed for objects that have been requested previously from other Stat Servers. If, on the other hand, you remove a tenant from a Stat Server, the process of closing the corresponding object's statistics on that Stat Server could take a long time to finish. There is no automated process for closing the statistics in this scenario.

If something changes in your enterprise, and you must make a change to the Stat Server-tenant links, then you can force a re-distribution of statistics among the group of Stat Servers. See the following procedure.

Procedure: Forcing the re-distribution of statistics among an adapter's pool of Stat Servers

Purpose: Use this procedure to force a re-distribution of statistics among the Stat Servers when you add a Stat Server (or more than one) to an adapter's configuration.

Steps

1. Before making any changes, remove all of the existing Stat Server connections from the adapter's Application object.
2. Restart the adapter with no Stat Server connections.
3. Add the new Stat Server connection(s).
4. Restart the adapters, XML Generator, and Frontline Advisor.

Tenant-Based Routing and the Backup Stat Server

If you use redundant Stat Server pairs in your environment, then tenants that are linked to a backup Stat Server must exactly match the list of tenants that are linked to the primary Stat Server. The Stat Server type (CORE, MULTIMEDIA, or THIRDPARTYMEDIA) must also match exactly on the primary and backup Stat Servers of a given pair. The Genesys configuration interface (for example, Genesys Administrator) automatically updates the configuration on the backup Stat Server Application when you modify the tenant or Stat Server type configuration on the primary Stat Server Application, provided that the backup Stat Server is correctly configured on the primary Stat Server Application object.

Migration Information

If you already have an Advisors deployment running, the default behavior is for the existing object-to-Stat Server mapping to be used for the distribution after you migrate to release 8.5.2. Distributing

statistics based on the Stat Server tenant is not used by default, but is used for any new object that you add to configuration. However, after migrating to release 8.5.2, tenant-based statistics routing can be enforced for the existing objects by removing the existing object-Stat Server mappings that are stored in the Advisors Platform database. The procedure for this is the same as the procedure for redistributing the statistics when new Stat Servers are added to the configuration.

Application Monitoring

JMX

There is a variety of application information that can be accessed using the Java Management Extensions (JMX). This information can be accessed in a customized fashion using the JMX API, or more generically using popular JMX clients like jconsole, jvisualvm, and so on.

JMX connections can be made by adding the appropriate Java options in Tomcat. These options have already been added to the `setenv.sh` and `setenv.bat` files in the Advisors installation Tomcat `bin` directory. Uncommenting these options and adding the port and host information for your environment will allow you to establish JMX connections.

MBean Resources

The following is not a comprehensive list of all MBeans in Advisors, but some which might be useful.

Catalina

These MBeans include:

- Tomcat connector statistics. Includes various connection-related statistics
- Server configuration and port information
- Classloader configuration
- Database connection information

com.genesys.advisors.advws.websocket

Exposes information for managed websocket connections:

- Number of users currently connected.
- Number of user-sessions currently established. Individual users may have multiple open connections in separate machines, browsers, tabs, and so on
- Number of users actively using the system within the last x minutes

com.genesys.advisors.datamanager

Advisors Genesys Adapter related information:

- Adapter configuration information. Note that this includes a warning that it should not be invoked for large hierarchies.

com.genesys(lab).advisors.fa.engine

These MBeans are only present when connected to installations that include the FA aggregation server. Includes:

- Various metric aggregation process information
- Activity information for incoming data from adapters configured for FA

Application Profiling

The Java Virtual Machine (JVM) exposes performance and resource utilization information through JMX. This might be useful for monitoring things such as:

- CPU and memory utilization
- Thread activity
- Garbage collection activity

Health Check API for the Platform Web Services Node

The Advisors Web services provide an API to check the health of the Web server nodes. For example, if you have installed Pulse Advisors release 9.0.000, you can configure the load balancer to access the `http://<host:port>/adv/rest/health` URL to check the health of an Advisors Web services node. NEW That URL changes to `http://<host:port>/adv/health` starting with Advisors release 9.0.001. In either case, it is an unauthenticated resource; it can be accessed without first logging in.

The service returns an HTTP status code of `200` when the Web server is up and running. The service returns a non-200 HTTP status code when the Web server is not reachable.

Establishing a TLS Connection to Genesys Configuration Server

Pulse 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. Contact Center Advisor (CCAdv), Workforce Advisor (WA), and Frontline Advisor (FA) have a secure connection to the Configuration Server if you enable a TLS connection on Advisors Platform.

TLS 1.2 is supported on connections to the Configuration Server starting with Advisors release 8.5.2. No additional configuration is required on the Advisors client side to enable TLS 1.2. For information about possible additional configuration on the server side for your environment, see the protocol compatibility section of the *Management Framework Deployment Guide*.

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 the Genesys Security Deployment Guide.
3. Configure security certificates.
4. Configure the security providers and issue security certificates. For more information, see the Genesys Platform SDK Developer's Guide.
5. Assign a certificate to the Configuration Server host. For more information, see the 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.

Data Manager

The Advisors Data Manager provides the following functionality:

- Support for multiple Genesys 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 each AGA for each Advisors module (such as CCAdv or FA).
- Use of a handshake protocol to establish connection with all adapters.

Installation and Configuration

During the installation of any adapter, the installation wizard might prompt you for the following information:

- The connection details for the Platform database.
- A unique name for the adapter and the source environment (the latter is requested only in a Cisco 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 AGAs, although you can choose to bypass Advisors Cisco adapter registration.

Configuration Server Integration

If there are agents, agent groups, calling lists, or queues configured in the Configuration Server when Data Manager starts, then Data Manager immediately issues statistics requests to the configured Advisors Genesys Adapter(s).

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 Genesys Configuration Server

The following changes to object configuration in Configuration Server affect the Contact Center Advisor/Workforce Advisor configuration:

- The addition of an object to the Configuration Server is reflected on the **Application Configuration** page. New agent groups, queues, calling lists, or interaction queues that you add to the Configuration Server are added to the lists of available objects by simply reloading the **Application Configuration** page.
- Any change to the name of an object will be propagated to the **Application Configuration** page when you reload that page in the Advisors administration module.

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 your Genesys configuration interface.

> **Important**
>
> The Advisors Filters business attribute must exist on one—and only one—tenant. Genesys recommends that 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 AGA starts, and the filters are not loaded.

Configuring the Advisors Filters

You can find an Advisors filter expression in your Genesys configuration interface. The Annex of a filter attribute value contains the expression that defines that filter; the expression is entered as an option value. For more information about configuring Advisors filters, see Using Advisors Filters Configuration to Segment Objects and Metrics.

Tip

In a migration scenario, the Migration utility that ships with Advisors release 9.0 includes an option that, when selected, will reconfigure the Advisors Filters Business Attribute configuration for you. Previously, you configured the filter expression in the **Description** field of the Filter Business Attribute value, but starting with release 9.0, the filters are configured as Annex options on the Business Attribute. The new migration utility option automatically updates this configuration for filters that were configured in earlier releases. For more information about filter configuration in release 9.0, see Using Advisors Filters Configuration to Segment Objects and Metrics.

Data Manager uses the filters that are configured as Annex options on objects when it requests statistics. When one or more filter combination is 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. However, as an example, if three filters (Gold, Silver and Platinum) are combined with an ACD Queue object, then three variations of CallsHandled would be requested. The three filters are individually applied to yield three statistics: CallsHanded.Gold, CallsHandled.Silver, and CallsHandled.Platinum.

Filters and Interaction Queues

Filter categorization is not applicable to interaction queue statistics. Available applications do not combine object filter segments with interaction queues because typically interaction queue metrics are not filterable. For more information about application and filter configuration for Contact Center Advisor/Workforce Advisor release 9.0 and later, see Application Configuration in the *Genesys Contact Center Advisor and Workforce Advisor Administrator User's Guide*.

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 AGAs, the source environment is always `GENESYS`.

Load Balancing

When two or more adapters share the same source environment, 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.

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 redistributed among all the adapters, including the ones you added. For the procedure to redistribute the statistics load balancing to include newly-deployed adapters, see Re-distribute Stats Load when Adapters are Added.

Once a statistic is opened with an adapter for a given object, 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.

Troubleshooting Data Manager

If you are experiencing issues with Data Manager, check for the problems described in this section.

The adapter is unavailable

If there is one or more AGA 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 redistribute statistics 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.

Procedure:

Steps

1. Determine which objects are associated with the inactive adapter:
   a. 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
      ```

   b. 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>
   ```

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.
- Ensure that the configured Stat Servers are up and running.

Providing a User Interface for Users with Visual Impairment

Contact Center Advisor, Workforce Advisor, and Frontline Advisor support JAWS Standard software, so you can provide an accessibility interface for users with visual impairment. JAWS software 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.

The CCAdv login page URL uses the following format:
`http(s)://<server>[:port]/ca-xml/accessibleDashboard?language=<en|de|fr>`

The WA login page URL uses the following format:
`http(s)://<server>[:port]/wu/accessibleDashboard?language=<en|de|fr>`

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 FA, CCAdv, and WA accessibility services respectively. Users specify their language preference as part of the URL; again, no additional configuration is required to provide language options.

Advisors Software Distribution Contents

Click the links below to view the software contents that Genesys provides for each Performance Management Advisors product.

[+] Advisors Platform

Starting with release 9.0.002.03, there is no longer a `baseweb-<version>-static-web.zip` file included with the software installation package; baseweb static files are no longer needed. If you are following the Apache configuration recommendations, no files need to be served directly from Apache.

Distribution Artifacts	Contents	Notes
advisors-platform-installer-<version>.jar	The installation file for Advisors Platform.	You use the Advisors Platform installation wizard to install the Advisors Web services and to configure available integration with Genesys Pulse. For detailed information about the Advisors Platform installation wizard, see Deploying Advisors Platform.
... supplement/ advisors-migration-wizard-<version>.jar user-migration-util-<version>.zip	The Advisors migration utilities.	See User Migration Utility and Object Migration Utility in the *Genesys Performance Management Advisors Migration Guide*.
platform-database-sql/mssql/ advisors-platform-new-database-<version>.sql advisors-platform-migrateSchema_<from-versions>_<to-version>.sql	1. `...-new-database-<version>.sql` Creates database objects for the MS SQL Platform database after the Platform database is created. 2. `...-migrateSchema_<from-versions>_<to-version>.sql` The scripts to update an existing MS SQL Platform database.	Always check the Release Notes for additional information.

Distribution Artifacts	Contents	Notes
platform-database-sql/oracle/ advisors-platform-<version>_INMEMORY.sql advisors-platform-<version>_NO_INMEMORY.sql advisors-platform-<version>_ObjectsCustom.sql advisors-platform-<version>_ObjectsDefault.sql advisors-platform-<version>_ObjectsPlus.sql advisors-platform-<version>_Schema.sql advisors-platform-<version>_TBS.sql advisors-platform-<version>_User.sql advisors-platform-migrateSchema_<from-versions>_<to-version>.sql WhatsInThisFolder.txt (Starting with release 9.0.001.06) WhatFolderToUse.txt (Starting with release 9.0.001.06) Any additional files in the folder are not to be executed manually. They are called automatically within the sql*Plus script during runtime.	The creation scripts for the Platform database for Oracle. 1. `..._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 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. 2. `..._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. 3. `..._ObjectsPlus.sql` An SQL*Plus script that creates	The `platform-database-sql/oracle/` directory contains several files and folders. Starting with release 9.0.001.06, see the `WhatsInThisFolder.txt` file, also included in the same location, for information about the folders and scripts as well as instructions about how and why to use them. In addition, also starting with release 9.0.001.06, within the `migration`, `migrationarchive`, `oracleJServer`, and `oracleNoJServer` folders you will find a `WhatFolderToUse.txt` file. Be sure to read the file to understand the differences between the `current_user` and `definer` folders. Always check the Release Notes for additional information.

Distribution Artifacts	Contents	Notes
	all platform database objects. To be executed by the previously-created Platform user and after all planned tablespaces are created. 4. `..._ObjectsCustom.sql` An alternate script that has the same purpose as `...ObjectsPlus.sql`, but can be executed from Oracle 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. 5. `..._ObjectsDefault.sql` An alternate 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. 6. `..._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 alternate script that replaces, and has the same purpose as `...User.sql` and `...ObjectsPlus.sql` combined. 7. `..._INMEMORY.sql` You use this script if you run the Oracle 12C In-Memory option. 8. `..._NO_INMEMORY.sql` You use this script to revert the changes to the metrics schema if you previously executed the `..._INMEMORY.sql` script.	

Distribution Artifacts	Contents	Notes
	9. `advisors-platform-migrateSchema_<from-versions>_<to-version>.sql` The scripts to update an existing Oracle Platform database.	
.../bulkconfig/	The CCAdv and WA bulk configuration tool. To use the bulk configuration tool, see instructions on the following pages in this guide: • CCAdv Bulk Configuration – Independent Mode • WA Bulk Configuration – Independent Mode • CCAdv/WA Bulk Configuration – Integrated Mode	The `bulkconfigarchive` folder contains a corrected bulk configuration tool and bulk export tool. Use the tool in the `bulkconfigarchive` folder if you must export or reconfigure the rollups in earlier-release installations (releases prior to release 9.0) before you export the configuration. For additional information about changes to bulk configuration in release 9.0, see Changes to Bulk Configuration Starting with Release 9.0 in the *Pulse Advisors Deployment Guide*.
metric-graphing-database-sql/mssql-... mg-new-database-<version>.sql	The creation script for the metric graphing database on MS SQL. This script is located in the `metric-graphing-database-sql` directory. The IP includes the following folders: • mssql-standard (for installations that use MS SQL Standard Edition) • mssql-enterprise (for installations that use MS SQL Enterprise Edition) Ensure you use the files from the folder that corresponds to your edition of Microsoft SQL Server.	
metric-graphing-database-sql/oracle-...	The creation scripts for the metric graphing database on Oracle.	Always check the Release Notes for additional

Distribution Artifacts	Contents	Notes
mg-<version>_INMEMORY.sql mg-<version>_NO_INMEMORY.sql mg-<version>_ObjectsCustom.sql mg-<version>_ObjectsDefault.sql mg-<version>_ObjectsPlus.sql mg-<version>_Schema.sql mg-<version>_TBS.sql mg-<version>_User.sql migrate_mg_<from-version>_<to-version>.sql	The scripts are located in the `metric-graphing-database-sql` directory. The IP includes the following folders: • `oracle-without-partitions` (for installations that use Oracle without the partitioning option) • `oracle-with-partitions` (for installations that use Oracle with the partitioning option) Ensure you use the files from the folder that corresponds to your edition of Oracle. 1. `_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 alternate script that replaces, and has the same purpose as `...User.sql` and `...ObjectsPlus.sql` combined. 2. `..._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 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	information.

Distribution Artifacts	Contents	Notes
	among multiple tablespaces. If created by the DBA, the DBA provides the tablespaces information to the engineer who proceeds with the installation. 3. `..._User.sql` Creates the CCAdv/WA metrics graphing user and schema. To be executed by a database user who has permission to create other users. In most cases, users are created by your DBA. The file can be used as is or for DBA information as it shows user permission and tablespace requirements. If the user/ schema is created by the DBA, the DBA provides the relevant information to the engineer who proceeds with the installation. 4. `..._ObjectsPlus.sql` An SQL*Plus script that creates all CCA/WA database objects necessary for metrics graphing. To be executed by the previously-created CCAdv/WA metric graphing user and after all planned tablespaces are created. 5. `..._ObjectsCustom.sql` An alternate script that has the same purpose as `...ObjectsPlus.sql`, but can be executed from Oracle Sql Developer by the previously-created CCAdv/WA metric graphing user and after all planned tablespaces are created. The script allows table and index distribution among multiple tablespaces by issuing pop-up prompts. 6. `..._ObjectsDefault.sql` An alternate 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	

Distribution Artifacts	Contents	Notes
	not issue any pop-up prompts and creates all platform database objects in the Platform user default tablespace assigned during Platform user creation. 7. `..._INMEMORY.sql` You use this script if you run the Oracle 12C In-Memory option. 8. `..._NO_INMEMORY.sql` You use this script to revert the changes to the metrics schema if you previously executed the `..._INMEMORY.sql` script. 9. `migrate_mg_<from-version>_<to-version>.sql` The metric graphing database migration script.	

[+] Advisors Genesys Adapter

Distribution Artifacts	Contents	Notes
aga-installer-<version >.jar		The installer for Genesys Adapter.
configuration-schema/mssql/ gc_metrics_db_<version>.sql		The creation and migration script for an Advisors Genesys Adapter metrics database on MS SQL.
configuration-schema/oracle gc_metrics_<version>_INMEMORY.sql gc_metrics_<version>_NO_INMEMORY.sql gc_metrics_<version>_ObjectsCustom.sql gc_metrics_<version>_ObjectsDefault.sql gc_metrics_<version>_ObjectsPlus.sql gc_metrics_<version>_Schema.sql gc_metrics_<version>_TBS.sql gc_metrics_<version>_User.sql	1. `..._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	The creation and migration scripts for an Advisors Genesys Adapter metrics database on Oracle.

Distribution Artifacts	Contents	Notes
	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. 2. `..._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. 3. `..._ObjectsPlus.sql` An SQL*Plus script that creates all AGA metrics DB objects. To be executed by the previously-created AGA metrics user and after all the planned tablespaces are created. 4. `..._ObjectsCustom.sql` An alternate script that has the same purpose as `...ObjectsPlus.sql`,	

Distribution Artifacts	Contents	Notes
	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. 5. `..._ObjectsDefault.sql` An alternate 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. 6. `..._INMEMORY.sql` You use this script if you run the Oracle 12C In-Memory option. 7. `..._NO_INMEMORY.sql` You use this script to revert the changes to the metrics schema if you previously executed the `..._INMEMORY.sql` script. 8. `..._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 alternate script that replaces, and has the same purpose as, `...User.sql` and	

Distribution Artifacts	Contents	Notes
	`...0bjectsPlus.sql` combined.	

[+] Contact Center Advisor/Workforce Advisor

Distribution Artifacts	Contents	Notes
ccadv-wa-installer-<version>.jar	The installation file for the Contact Center Advisor (CCAdv) XML Generator application, Workforce Advisor (WA) server, CCAdv accessibility services (optional), WA accessibility services (optional), and the Resource Management Console (optional).	For detailed information about the CCAdv/WA installation wizard, see Deploying CCAdv and WA. You deploy the CCAdv and WA dashboards (Advisors Web services) using the Advisors Platform installation wizard; see also Advisors Platform software distribution contents, above.

[+] Frontline Advisor

Distribution Artifacts	Contents	Notes
fa-server-installer-<version>.jar	The installation file for the Frontline Advisor (FA) server.	For detailed information about the FA installation wizard, see Deploying Frontline Advisor. You deploy the Frontline Advisor dashboard (Advisors Web services) using the Advisors Platform installation wizard; see also Advisors Platform software distribution contents, above.