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

Prerequisites for Advisors Platform

5/6/2025

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*.