Performance Management Advisors Deployment Guide

Deploying SDS and RMC

5/9/2025

Deploying SDS and RMC

Contents

Deployment Roadmap

1. **[+] Install the databases that correspond to the Advisors products you will deploy.**
   a. Advisors Genesys Adapter metrics database
   b. Advisors Platform database
   c. Advisors Cisco Adapter database (if you use ACA)
   d. Metric Graphing database
2. Create the Advisors User and the Object Configuration User in Configuration Server.
3. **[+] Install the Platform service (Geronimo) on servers where it is required for Advisors components.**
   - Contact Center Advisor Web services
   - Workforce Advisor
   - Frontline Advisor
   - Contact Center Advisor–Mobile Edition
   - Resource Management Console
4. Install each adapter you will use (AGA and ACA).
5. Register the Stat Servers that you plan to use with Advisors.
6. Install the Advisors components for your enterprise:
   - Contact Center Advisor
   - Workforce Advisor
   - Contact Center Advisor – Mobile Edition
   - Frontline Advisor
   - ⛔ SDS and Resource Management Console
7. Make any required configuration changes.

Resource Management and Resource Management User Configuration

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

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

Related Information

See the following for more information:

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

Important Information about the SDS and RMC Operating Environment

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

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

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

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

- Install SDS and the RMC only after you have installed all other Advisors components that you use in your enterprise. Genesys recommends that you verify the dashboards are working for all installed components (CCAdv, WA, FA), and that the hierarchy in each dashboard rolls up correctly before you install SDS and RMC. After you have verified Advisors is working correctly, install JDK 1.6 (if it is not already installed as your primary JDK version), and then install SDS and RMC.
- If you use the Resource Management Console in Contact Center Advisor and/or Workforce Advisor, note the following:
  - Avoid running Resource Management in Microsoft Internet Explorer 10 or earlier versions; older versions of Internet Explorer can cause serious problems with the Resource Management console.
  - For 8.5.1 releases prior to 8.5.101, deploy Resource Management on a supported Microsoft Windows operating system. Resource Management is not compatible with Red Hat Enterprise Linux until Advisors release 8.5.101. See the *Genesys Supported Operating Environment Reference Guide* for information about supported Windows operating systems.

SDS and RMC Deployment Procedures

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

Task Summary

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

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

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

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

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

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

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

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

   - Procedure: Deploying Supervisor Desktop Service on Windows
   - Procedure: Deploying Supervisor Desktop Service on Linux

4. Complete the Supervisor Desktop Service configuration.

   See Procedure: Completing the Supervisor Desktop Service Configuration.

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

   See Procedure: Deploying the Resource Management Console.

6. Configure the Resource Management Console:

   - For Advisors release 8.5.100, see Procedure: Configuring the Resource Management Console for Advisors release 8.5.100.
   - For Advisors release 8.5.101, see Procedure: Configuring the Resource Management Console for Advisors release 8.5.101.

Procedure: Configuring the SDS Application in the Genesys Configuration Layer

Steps

1. On the Genesys server, launch the Genesys configuration interface (for example, Genesys Administrator).
2. Create a host object, under the `Environment` tenant, for the machine on which you will deploy the SDS, if one does not already exist.
   Genesys recommends that the IP address configured in this host object be the actual IP address of the server, not a loopback address.
3. Import the application template called `Genesys_Supervisor_Desktop_Service_763.adp`. This template is located with the SDS installation files.
4. Create a new Application using the `Genesys_Supervisor_Desktop_Service_763.adp` application template. Configure the Application using the following guidelines:
   a. Specify the name of the application as `Genesys Supervisor Desktop`.

b. Add connections to the T-Servers, Interaction Servers, and the Stat Server to which the SDS will connect.
   SDS can be connected to one primary/backup Stat Server pair.

c. (Multi-tenant environments only) Add the non-`Environment` tenant that SDS will monitor.

d. Select the host object configured in **Step 2** above (that is, the server on which you will install SDS). If necessary, change the port number to `8080`.

e. Enter a single period (.) for the working directory, command line, and command line arguments.

f. Ensure you select a login account that has full control privileges. For example, you can select the option to log in as `System` as long as your `System` user has full control access privileges.

g. Configure options as follows:

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

> **Tip**
>
> The `stat-threads= -1` setting can be used to indicate “use all available processors”.
>
> For smaller customers the following settings can be used to create periodic SDS statistics polling at 30-second intervals:
>
> - `stat-peeking=false`
> - `stat-refresh-rate=30`
>
> The refresh rate can be increased for more frequent updates, at the cost of increased SDS and Stat Server load.
>
> For larger customers the `stat-peeking=true` setting can be used to define on-demand statistics retrieval.

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

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

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

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

- Save the Application.
- Verify that the T-Server(s), Interaction Server(s), and Stat Server(s) are configured with a correct host (that is, they do not use `localhost`).
  The SDS uses the hosts that are configured in the Configuration Server for the T-Servers, Interaction Servers, and the Stat Servers to determine where they are installed and how to reach them. If these servers are configured with the `localhost` host, the SDS tries to connect to the server on which it is installed. This will not work if the SDS and the other servers are installed on different machines.

Next Steps

Do one of the following:

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

For information about supported operating systems for Advisors deployments, see the Advisors section in the *Supported Operating Environment Reference Guide*.

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

Steps

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

- To enable agent maintenance for multiple tenant installations, you must give the Spv user the same subset of permissions that are given to tenant Administrators. You must also give the Spv user Change permission to Person objects (to manage agent skills).
  You might want to create a separate access group for the Spv user that contains these required permissions. If you do not wish to create a separate access group, add the Spv user to the existing tenant's Administrators access group, and grant the group Change permission to `Person` objects.

Next Steps

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

Procedure: Deploying Supervisor Desktop Service on Windows

Steps

1. If an older version of SDS is already installed, you must uninstall it.
   [+] Show Steps for Using Command Line
   a. Stop the SDS service.
   b. In a command prompt, navigate to the `bin` subdirectory for the SDS installation.
   c. Run `service.bat uninstall SupervisorDesktopService`.
   d. Delete all files and subdirectories in the root SDS directory.

   [+] Show Steps for Using SDS Installer
   a. Stop the SDS service.
   b. Run the SDS installer, selecting the option to update an existing installation.
   c. When prompted, select the option to remove the SDS.
   d. Delete all files and subdirectories in the root SDS directory.

2. Ensure that you have either a `JAVA_HOME` or `JRE_HOME` environment variable set, pointing to the JDK or JRE root directory respectively.
3. Copy the installation package to a directory of your choice.
4. Run `setup.exe`.
   You can find the `setup.exe` file in the folder containing the Supervisor Desktop Service installation package.
   The Genesys Installation Wizard for SDS displays and guides you through the rest of the installation.
   [+] See information about installer screens
   a. On the **Connection Parameters to the Configuration Server** screen, enter information in all fields.
   b. On the **Select Application** screen, select the application that you created.
   c. On the **Choose Destination** screen, specify the directory in which to install SDS. Clicking the `Default` button enters `C:\GCTI\GenesysSupervisorDesktopService\Genesys_Supervisor_Desktop`. Click the `Browse` button to navigate to a directory of your choice.

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

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

Next Steps

There are additional steps to complete the SDS configuration. See Procedure: Completing the Supervisor Desktop Service Configuration.

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

Steps

1. If an older version of SDS is already installed, you must uninstall it.
   This should be unnecessary for Advisors release 8.5.1 because Genesys' support for SDS on Linux begins in Advisors release 8.5.101. However, if you must uninstall SDS from a Linux platform for any reason, manually remove the installation directory and delete the web application from the server.
2. Ensure that you have either a `JAVA_HOME` or `JRE_HOME` environment variable set, pointing to the JDK or JRE root directory respectively.
3. Copy the installation package to a directory of your choice.
4. Run `./install.sh`.
   You can find the `./install.sh` file in the folder containing the Supervisor Desktop Service installation package.
   [+] See information about installer screens
   a. On the **Connection Parameters to the Configuration Server** screen, enter information in all fields.
   b. On the **Select Application** screen, select the application that you created.
   c. On the **Choose Destination** screen, specify the directory in which to install SDS. Clicking the `Default` button enters `C:\GCTI\GenesysSupervisorDesktopService\Genesys_Supervisor_Desktop`. Click the `Browse` button to navigate to a directory of your choice.

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

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

Next Steps

There are additional steps to complete the SDS configuration. See Procedure: Completing the Supervisor Desktop Service Configuration.

Procedure: Completing the Supervisor Desktop Service Configuration

Steps

1. On the Genesys server, launch the Genesys configuration interface (for example, Genesys Administrator).
2. Edit the options for your Stat Server application as described below:
   a. Import the `StatServerEntries.cfg` file (found in the Advisors Genesys Adapter installation directory) into the Stat Server application options. If prompted to overwrite the existing options, choose `NO`.
   b. If prompted to overwrite/update any statistics options, do so. The file does not alter any default Stat Server metrics, only ones specific to Advisors. Changing any logging options is optional.
   c. Restart the Stat Server.
3. If you are deploying Advisors release 8.5.101, omit this Step.
   If, however, you are deploying Advisors release 8.5.100, in the Genesys configuration interface, browse to the scripts for the tenant(s) that you use for the SDS installation. Delete all scripts named `User Stat.Spv*`.
4. For performance reasons, Genesys recommends that you update `xms` and `xmx` values for servers that host your SDS. Edit these values based on information in the *Genesys Hardware Sizing Guide*, *Chapter 17: Performance Management Advisors*, in section *Improving Supervisor Desktop Service Performance*.
5. Use Solution Control Server, Genesys Administrator, or the SDS host to start SDS.
   To start SDS from the host machine:
   - On a Windows host machine: Use the Windows service
   - On a Linux host machine: Execute `./startup.sh` in the `/bin` folder

Next Steps

Deploy the Resource Management Console. See Procedure: Deploying the Resource Management Console.

Procedure: Deploying the Resource Management Console

Steps

1. Launch the AGA installation file.
   [+] Show Steps for Linux

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

   ```
   cd /home/advisors
   ```

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

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

   [+] Show Steps for Windows

   Do one of the following:

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

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

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

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

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

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

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

- `Database host`—If requested, enter the host name or IP address of the database server. When using numerical IPv6 addresses, enclose the literal in brackets.
- `Database name/Service name`—If requested, enter the unique name of the database instance.
- `Database port number`—If requested, enter the database server's port number.
- `Database user`—The username to be used by the Adapter to access the database.
- `Database user password`—The password associated with the database user.
- `Locate file`—Enter the location of the file that contains the advanced database connection string. If you do not know how to correctly build the advanced database connection string, contact your database administrator. The installation wizard applies the specified advanced connection string when configuring the data sources.

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

Next Steps

See information about configuring the RMC:

- For Advisors release 8.5.100, see Procedure: Configuring the Resource Management Console for Advisors release 8.5.100.
- For Advisors release 8.5.101, see Procedure: Configuring the Resource Management Console for Advisors release 8.5.101.

Procedure: Configuring the Resource Management Console for Advisors release 8.5.100

Steps

1. **Configure the RMC properties file**

After RMC has installed successfully, you must edit the `RMCInfo.xml` configuration file to provide the information required to make Resource Management function and available to Contact Center Advisor. The `RMCInfo.xml` file is found in the following directory:
`Advisors\geronimo-tomcat6-minimal-2.2.1\repository\com\informiam\genesys\rmc-web\<version>\rmc-web-8.x.xxx_<version>.war\WEB-INF\classes`

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

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

Use the following values:

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

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

   To access the Resource Management Notification administration pages through the Advisors interface (Advisors Administration module), you must add the following entry to the Apache `httpd.conf` file on the web server:

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

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

3. **Restart the Geronimo server**

   Open the Windows Services window and restart the Geronimo server.

Next Steps

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

RMC.

Procedure: Configuring the Resource Management Console for Advisors release 8.5.101

Steps

1. **Configure the RMC properties file**

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

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

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

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

   Use the following values:

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

2. **Enable transmission of login events to RMC**

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

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

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

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

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

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

   To access the Resource Management Notification administration pages through the Advisors interface (Advisors Administration module), you must add the following entry to the Apache `httpd.conf` file on the web server:

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

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

4. **Restart Geronimo servers**

   Restart every Geronimo server for which you changed either the `RMCInfo.xml` properties or the `ActiveMQ.properties` file.
   If the Geronimo server is running an Advisors application that is integrated with Solution Control Server, then restart the Advisors server from the Solution Control Interface.
   If not integrated with Solution Control Server, then:

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

Next Steps

- See Configure Resource Management Console Properties for information about configuring RMC properties for optimal performance.

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