Workspace Desktop Edition Deployment Guide

Configuring the Workspace application object

4/14/2025

Configuring the Workspace application object

[**Modified:** 8.5.111.21]

Contents

Workspace is designed to be used with the Genesys 8 Suite. Before you install Workspace, you must deploy the Genesys 8 Management Framework. You must also be familiar with Genesys Administrator Extension (or Genesys Administrator 8.0.2 or higher). For more information on these products, please consult the following documents:

- Genesys Framework documentation set
- Genesys Administrator Extension Deployment Guide
- Genesys Administrator Extension Help

1. Using Genesys Administrator Extension to create and provision the Workspace application

Purpose:

To create and configure a Workspace Desktop Edition `Application` object in Genesys Administrator Extension to enable you to deploy and provision Workspace.

The Workspace Desktop Edition Application Template and the configuration metadata are included in the standard application-template set that comes with Genesys Suite 8.

Beginning with Workspace 8.5, three templates and their associated XML metadata files are distributed with the application. You can choose to deploy different combinations of templates/XML metadata files to meet the needs of your call center:

- The Core Workspace template with core Workspace options, which does not contain any SIP Endpoint options: `Workspace_Desktop_Edition_850.apd/xml`. Use this option if you already are not planning to use any Genesys SIP Endpoint.
- The core Workspace template with core Workspace options and the Interaction Workspace SIP Endpoint 8.0.2 options: `Workspace_Desktop_Edition_SEP802_850.apd/xml`. Use this option if you are planning to deploy Interaction Workspace SIP Endpoint 8.0.2 (no video channel).
- The core Workspace template with core Workspace options and the Workspace SIP Endpoint 8.5.0 options: `Workspace_Desktop_Edition_SEP850_850.apd/xml`. Use this option if you are planning to use Workspace SIP Endpoint 8.5.0, which implements video channel.

Use the `Options` tab of the Workspace Desktop Edition `Application` object to provision Workspace by setting configuration options. Refer to Provisioning Functionality for more details.
Prerequisites

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension
- A working knowledge of Genesys Administrator Extension

Start

1. In Genesys Administrator Extension, choose the Configuration view.
2. Upload one of the following Application Templates (refer to the Purpose for a description of each

template):

- `Workspace_Desktop_Edition_850.apd`
- `Workspace_Desktop_Edition_SEP802_850.apd`
- `Workspace_Desktop_Edition_SEP850_850.apd`

3. Upload one the following application metadata (refer to the Purpose for a description of each metadata file):

- `Workspace_Desktop_Edition_850.xml`
- `Workspace_Desktop_Edition_SEP802_850.xml`
- `Workspace_Desktop_Edition_SEP850_850.xml`

4. Save the Application Template.

5. Create a new Workspace Desktop Edition application.

6. Set the application name.

7. Save the application.

End

2. Using Genesys Administrator Extension to set up the Workspace application

Purpose:

After you create the Workspace Desktop Edition `Application` object, you must set up connections to various Genesys components.

Prerequisites

- Using Genesys Administrator Extension to create and provision the Workspace application

Start

1. In Genesys Administrator Extension, choose the Configuration/Environment/Application view.

2. Open the Workspace Desktop Edition `Application` object that you created.

3. Add the following connections (**Note**: you can optionally add Advanced Disconnect Detection Protocol (ADDP) for *any* connection):

- T-Server or SIP Server (for Voice and IM features)
- Statistics Server (for Statistics feature and Presence)
- Universal Contact Server (for Contact Management)
- Interaction Server (for eServices)
- Configuration Server/Configuration Server Proxy (if you plan to use Configuration Server Proxy).
  Note: Before setting ADDP with Configuration Server or Configuration Server Proxy, first create a

connection to this server in the Workspace Desktop Edition application object.

4. Grant execution rights to the agents that will log on to this application.

5. Grant read rights to the agents that will log on to this application for the objects listed in Steps 3.

6. (Optional) To use HA functionality, grant Read rights to backup applications of the object that are listed in Step 3 and Configuration Server application, and the associated Host objects.

7. In T-Server environments, you can specify the the time, in seconds, between the two attempts to reconnect to the back-up T-Server by setting the value of the voice.hot-standby.backup-retry-delay option. Genesys recommends that you keep the value of this option above 30 seconds for optimal performance.

End

Next Steps

- (Optional) Procedure: Enabling client-side port definition

- Installing The Deployment Package and Deploying Workspace

3. Enabling client-side port definition

Purpose:

To enhance security by defining a client-side port.

Defining the access ports for each application to which Workspace connects ensures the security of the system. This feature is configured partially on Framework Configuration Server and partially on the Workspace Desktop Edition application in Genesys Administrator Extension.

Start

1. Open the `InteractionWorkspace.exe.config` file. This file is in the Workspace Desktop Edition directory on the Workspace Desktop Edition CD/DVD.

2. In the appSettings section, modify the value of the `transport-port` and `transport-address` keys as follows:

    - For the `transport-address` key, specify the IP address or the host name that Workspace will use to make a TCP/IP connection to Configuration Server. If the value is empty, this parameter is not used.

    - For the `transport-port` key, specify the port number that Workspace will use to make a TCP/IP connection to Configuration Server. If the value is empty, this parameter is not used.

    ```
    <appSettings>
    <add key="login.url" value="tcp://[ToBeChanged config_hostname]:[ToBeChanged
    config_port]<br/>/[ToBeChanged config_ApplicationName]" />
     <add key="login.connections.parameters.isenable" value="true" />
     <add key="options.record-option-locally-only" value="false" />
     <add key="about.view-region.isvisible" value="false"/>
     <add key="transport-address" value="[ToBeChanged transport_address]"/>
     <add key="transport-port" value="[ToBeChanged transport_port]"/>
    </appSettings>
    ```

3. Configure the connection to Statistic Server. For additional information, refer to the Client-Side Port

Definition chapter of the *Genesys Security Deployment Guide*.

a. In Genesys Administrator Extension, open the Workspace Desktop Edition application.

b. Click StatSever in the Connections tab to open the Connection dialog box.

c. In the Transport Protocol Parameters field specify the following parameters:

port=<port number>;address=<IP address>

Where: <port number> is the port number that a client will use for its TCP/IP connection to the server, and <IP address> is the IP address (or host name) that a client will use for its TCP/IP connection to the server.

You can configure one or two parameters. If you configure two parameters, they must be separated by a semicolon.

d. Click OK.

e. In the Workspace Desktop Edition application configuration window, click Save.

4. Configure the connection to T-Server and/or SIP Server. For additional information, refer to the Client-Side Port Definition chapter of the *Genesys Security Deployment Guide*.

a. In Genesys Administrator Extension, open the Workspace Desktop Edition application.

b. In the Connections tab, click your T-Server to open the Connection dialog box. If you have connections to more than one T-Server, repeat Step 3 for each connection.

c. In the Transport Parameters field, specify the following parameters:

port=<port number>;address=<IP address>

Where: <port number> is the port number that a client will use for its TCP/IP connection to the server, and <IP address> is the IP address (or host name) that a client will use for its TCP/IP connection to the server.

You can configure one or two parameters. If you configure two parameters, they must be separated by a semicolon.

d. Click OK.

e. In the Workspace Desktop Edition application configuration window, click Save.

5. Configure the connection to Universal Contact Server. For additional information, refer to the Client-Side Port Definition chapter of the *Genesys Security Deployment Guide*.

a. In Genesys Administrator Extension, open the Workspace Desktop Edition application.

b. Click UCS in the Connections tab to open the Connection dialog box.

c. In the Transport Parameters field, specify the following parameters:

port=<port number>;address=<IP address>

Where: <port number> is the port number that a client will use for its TCP/IP connection to the server, and <IP address> is the IP address (or host name) that a client will use for its TCP/IP connection to the server.

You can configure one or two parameters. If you configure two parameters, they must be separated by a semicolon.

d. Click OK.

e. In the Workspace Desktop Edition application configuration window, click Save.

End

Next Steps

- Installing The Deployment Package

4. Pre-Defining HA for Configuration Server

[**Added:** 8.5.111.21]

Purpose: To enable simple primary/backup HA on the client-side when an agent logs in for the first time.

If you want to setup:

- Business Continuity for Configuration Server go to this page: Business Continuity

- High Availability and Load balancing using a Cluster of Configuration Server Proxies, go to that page: Load Balancing Using Clusters

Prerequisites

- Using Genesys Administrator Extension to set up the Workspace application.

Start

1. Open the `InteractionWorkspace.exe.config` file. This file is in the Workspace Desktop Edition installation directory.

2. To support Primary/backup High Availability configuration for Config Server, you can provide information about the connection to Config Server, both primary and backup, from the `interactionWorkpace.exe.config` configuration file:

```
<appSettings>
 ...
 <add key="login.url" value="tcp://MyConfigurationEnvironment/ApplicationName" />
 <add key="login.nodes.MyConfigurationEnvironment"
value="[PrimaryConfigurationServerHost:PrimaryConfigurationServerPort][BackupConfigurationServerHost:Backup
/>
 ...
</appSettings>
```

- **MyConfigurationEnvironment**: The name of the Configuration Environment that is displayed in the Login window. For example: `'Production'` or `'Staging'`

- **ApplicationName**: The name of the Workspace Desktop application in Management framework

- **[PrimaryConfigurationServerHost:PrimaryConfigurationServerPort][BackupConfigurationServerHost:B** PrimaryConfigurationServerHost:PrimaryConfigurationServerPort is the Primary Configuration Server, BackupConfigurationServerHost:BackupConfigurationServerPort is the Backup Configuration Server. The order indicate the preference for the connection.

- **Timeout**: Specifies the delay, in seconds, that is applied after connections to primary and backup

have been checked and failed. This parameter applies only after initial successful connection has been lost..

End Next Steps

- Deploy the modified package to the Workstation.

5. Configuring Workspace for Business Continuity

Purpose:

To manage server and switch connections to enable Workspace to connect to an alternate (Peer) SIP Server in the event of a disaster at the Preferred agent login site.

Workspace enables you to use SIP Server Business Continuity (disaster recovery) to ensure that your agents can keep working in the event that one of your sites experiences a disaster or other loss of service. You can also configure eServices Business Continuity with UCS 9.1 or eServices Business Continuity with UCS 8.5.
Prerequisites

- Genesys Administrator Extension, configured to show Advanced View.

- A working knowledge of Genesys Administrator Extension.

- A Workspace Desktop Edition `Application` object exists in the Configuration Database.

- Two synchronized sites, each with configured High Availability (HA) pairs.

Start

1. On the SIP Server object at the Preferred site, configure the `disaster-recovery.site` option in the `interaction-workspace` section with a symbolic name, such as `Site X`, for the server. The symbolic name is how the server will be identified to the Business Continuity functionality. The Preferred site for one agent or group of agents will also be the Peer site for another agent or group of agents. The concept of Preferred site and Peer site is then configured agent by agent (or agent group by agent group) as described below.

2. You can also use the optional `disaster-recovery.name` option in the `interaction-workspace` section of both SIP Server objects of an HA pair to identify two SIP Servers as belonging to the same pair. If no name is specified for his option, the value `default` is assumed.

3. On the SIP Server object at the Peer site, configure the `disaster-recovery.site` option in the `interaction-workspace` section with a symbolic name, such as `Site Y`, for the server. The symbolic name is how the server will be identified to the Business Continuity functionality.

4. For each agent, agent group, or tenant, configure the `disaster-recovery.preferred-site` option in the `interaction-workspace` section by specifying the symbolic site name of the SIP Server that you specified with the `disaster-recovery.site` option.

5. For each agent, agent group, or tenant, configure the `disaster-recovery.peer-site` option in the `interaction-workspace` section with the symbolic site name of the SIP Server that you specified with the `disaster-recovery.site` option.

6. Enable Business Continuity for each agent, agent group, or tenant and specify the Business Continuity behavior by configuring the other Business Continuity options that are listed in the Business Continuity

Configuration Options reference.

End