Workspace Desktop Edition Deployment Guide

Workspace And Genesys 8

3/31/2025

Workspace And Genesys 8

[**Modified:** 8.5.148.04]

Contents

Workspace is the key agent interface for Genesys 8. Workspace is built on top of the primary Genesys 8 SDKs. See the Table - **Interoperability between Workspace Desktop Edition 8.5 and other Genesys Products** for a list and description of the components of Workspace and the Table - **Miscellaneous Deliverables of Workspace** for a list of miscellaneous deliverables that ship with Workspace.

Miscellaneous Deliverables of Workspace

Component	Description
Workspace Desktop Edition Deployment Manager	Wizard that is used during deployment to prepare the ClickOnce packages
Workspace Extension Samples	Set of examples that illustrate how to implement extensions for Workspace

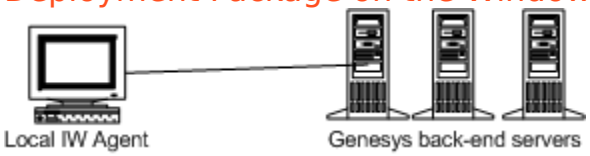
Topology

You can deploy Workspace in two different deployment configurations, depending upon the arrangement of your network; they are:

- Oversimplified deployment with a Client-server in a local setup.
- Client-server with centralized deployment based on ClickOnce

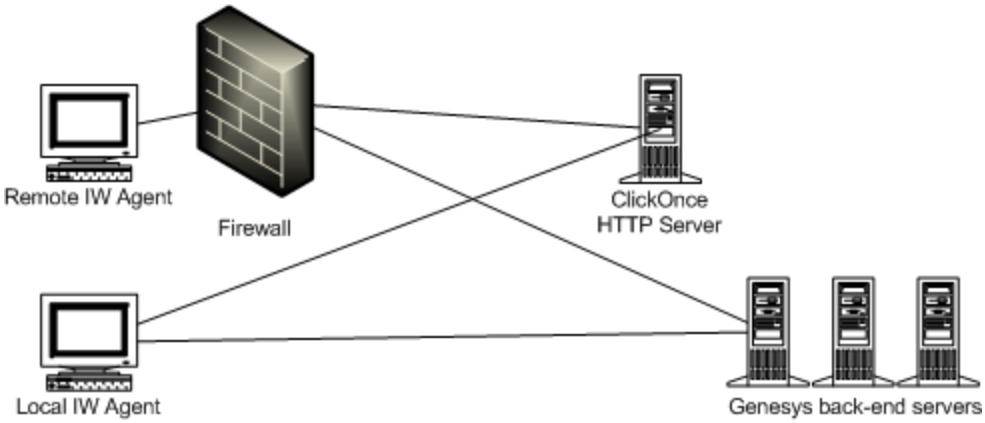
This section shows the key components of the Workspace network topology and indicates how Workspace is related to other Genesys components.

The Figure - **Simple client-server deployment of Workspace** shows a minimal deployment that consists of agent workstations that are connected directly to the Genesys back-end servers. For the procedure on deploying Workspace in this configuration, see the Procedure: Installing Workspace Deployment Package on the Windows operating system.



Simple client-server deployment of Workspace

The Figure - **Standard deployment of Workspace with a ClickOnce server** shows the standard deployment of Workspace in an environment in which the deployment is controlled from a centralized place and in which remote agents can be connected to Genesys back-end through a Virtual Private Network.



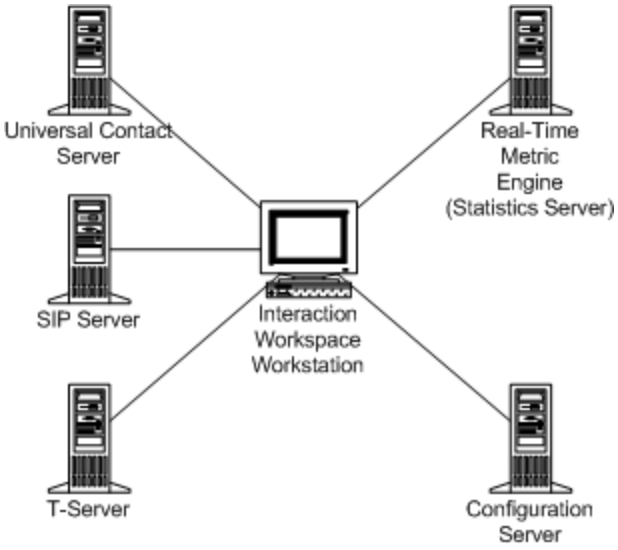
Standard deployment of Workspace with a ClickOnce server

Connections to Genesys components

The Figure - **Workspace connections to the Genesys 8 Suite** shows the connections to various Genesys components. Workspace requires connections to the following Genesys Components for environments that use IPv4:

- Configuration Server: Through Genesys Administrator, provides authentication, the list of connections, Role- Based Access Control, agent and place management, the object hierarchy for team communication, and application hierarchical configuration
- T-Server: Enables voice handling
- SIP Server: Enables voice and IM handling
- Real Time Metric Engine: Maintains statistics and target agent/group presence
- Universal Contact Server: Maintains the contact history
- Interaction Server: Manages interactions

Refer to the documentation that accompanies Genesys Administrator Extension and each of these components for information on setting up connections.



Interaction Workspace connections to the Genesys 8 Suite

IPv6 environments

[**Added:** 8.5.106.19]

Workpace supports IPv6 connections with all Genesys components if your system hardware supports IPv6 and it is implemented in your Framework Layer.

Review the IPv6 provisioning in the Genesys Framework documentation before proceeding:

- Internet Protocol version 6 (IPv6)
- IPv6 vs. IPv4 Overview

Enabling IPv6 in Workspace

You can enable IPv6 at various levels and with various scope.

You can enable IPv6 at the Environment level, which is shared with other Genesys components by configuring the following Environment Variables:

- `GCTI_CONN_IPV6_ON=1`
- `GCTI_CONN_IP_VERSION=6,4`

At the Environment level, the IPv6 settings apply to all connections that Workspace opens, such as Configuration Server, TServer or SIP Server, Stat Server, Universal Contact Server, Interaction Server, and Chat Server, and to SIP or RTP from/to the SIP Endpoint.

The setting of these Environment variables can be overridden by setting the following option in the `interactionworkspace.exe.config` file:

- `enable-ipv6=true`

- `ip-version=6,4`

When IPv6 is set at the Workspace level, the IPv6 settings apply to all connections that Workspace opens, such as Configuration Server, TServer or SIP Server, Stat Server, Universal Contact Server, Interaction Server, and Chat Server, but not for the SIP or RTP from/to the SIP Endpoint.

If Workspace is running in an environment where the IPv6 must be selectively enabled depending on the server to be contacted, you can use the following options to override the IP version that is specified by an Environment Variable or in the `interationworkspace.exe.config` file:

Options to Override the IP Version of Workspace Connections

Connection	Options to make an IPv6 settings specific for this connection
Configuration Server	N/A
Chat Server	Workspace option: • interaction-workspace\chatserver.ip-version=6,4
T-Server, SIP Server, Stat Server, Interaction Server, Universal Contact Server	In the connection object that links Workspace to this server (Connection Info, Advanced tab, Transport Parameters) • ip_version=6,4
SIP/RTP (for Workspace SIP Endpoint 8.5.1)	• interaction-workspace\ sipendpoint.enable_ipv6=true • interaction-workspace\sipendpoint.ip_version= 6,4

IPv6 provisioning reference

[+] Show Workstation Environment Variables

GCTI_CONN_IPV6_ON

- Default Value: `0`
- Valid Values: `0` and any non-zero integer value
- Changes take effect: When the application is started or restarted.
- Description: This environment variable enables IPv6. When set to `0` (false), IPv6 is not enabled. When set to any non-zero integer value (true), IPv6 is enabled.

GCTI_CONN_IP_VERSION

- Default Value: `4,6`

- Valid Values: `4,6`, `6,4`
- Changes take effect: When the application is started or restarted.
- Description: This environment variable specifies whether IPv4 (`4,6`) or IPV6 (`6,4`) is the preferred connection protocol.

[+] Show interactionworkspace.exe.config File Variables

enable-ipv6

- Default Value: `false`
- Valid Values: `true`, `false`
- Changes take effect: When the application is started or restarted.
- Description: Specifies that the `GCTI_CONN_IPV6_ON` environment variable can be overridden (`1`) for all applications connections.

ip-version

- Default Value: `4,6`
- Valid Values: `4,6`, `6,4`
- Changes take effect: When the application is started or restarted.
- Description: Specifies that the `GCTI_CONN_IP_VERSION` environment variable can be overridden (`1`) for all applications connections.

[+] Show Application Template Variables

chatserver.ip-version

- Default Value: `auto`
- Valid Values: `auto`, `4,6`, or `6,4`
- Changes take effect: At the next interaction
- Description: Specifies the Internet Protocol Version of the connection to Chat Server. The value `auto` specifies that the Internet Protocol Version is inherited by the value set for the `ip-version` option or the `GCTI_CONN_IP_VERSION` or environment variable. This option can be overridden by a routing strategy, as described in Overriding Options by Using a Routing Strategy.

sipendpoint.enable-ipv6

- Default Value: `auto`
- Valid Values: `auto`, `false`, or `true`

- Changes take effect: When the application is started or restarted.
- Description: Specifies that the GCTI_CONN_IPV6_ON environment variable can be overridden (1) for connections to SIP Server and RTP. If the value auto and the GCTI_CONN_IPV6_ON variable do not exist, then the value of ip-version is set to 4,6.

sipendpoint.ip-version

- Default Value: auto
- Valid Values: auto, 4,6, or 6,4
- Changes take effect: When the application is started or restarted.
- Description: Specifies the Internet Protocol Version of connections to SIP Server and RTP. The value auto specifies that the Internet Protocol Version is inherited by the value set for the ip-version option or the GCTI_CONN_IP_VERSION environment variable. If the GCTI_CONN_IP_VERSION environment variable does not exist, the value of the ip-version option is set to 4,6.

[+] Show Connection Object Variables

In the Transport Protocol Parameters (Tab Advanced) set the following variable:

ip-version

- Default Value: 4,6
- Valid Values: 4,6, or 6,4
- Changes take effect: When the application is started or restarted.
- Description: Specifies that the GCTI_CONN_IP_VERSION environment variable and the values configured for applications can be overridden for all connection objects.

Architecture

Workspace is integrated with the following Genesys 8 applications:

- Embedded components:
  - Enterprise Services
  - Platform SDK
- Direct connections:

  Genesys back-end servers to which WDE is connecting are listed in the following table:

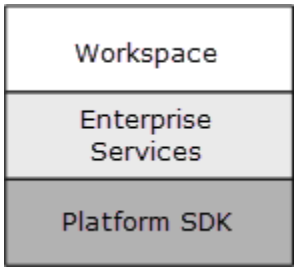
Genesys back-end server	Protocol
Chat Server	TCP/TLS
Configuration Server	TCP/TLS
Genesys Mobile Services	HTTP/HTTPS
Interaction Server	TCP/TLS
Media Control Platform	RTP/RTCP (for Workspace SIP Endpoint or Genesys Softphone)
Statistics Server	TCP/TLS
SIP Server	TCP/TLS SIP (for Workspace SIP Endpoint or Genesys Softphone)
T-Server	TCP/TLS
Universal Contact Server	TCP/TLS

- Miscellaneous Dependencies:
  - Genesys Administrator/Genesys Administrator Extension

- Optional installation:
  - Workspace SIP Endpoint
  - Workspace Compatible Plug-ins

Workspace features a modular design that divides the application into several components that are served out to agents based on their roles. All agents receive common modules such as the Login and Go Ready module and the Main Window module, while other modules, such as the Contact Management module and the Team Communicator module are distributed only to agents whose roles include those modules.

Workspace relies on both Enterprise Services and Platform SDK (refer to the Figure - **Workspace architecture**). This architecture enables developers to build customization for Workspace at any level.



Workspace architecture

Customization support

This architecture supports the following customization:

- Workspace -- User-interface customization
- Enterprise Services -- Business logic customization using a high-level API
- Platform SDK -- Business logic customization using a low-level API

Refer to the Workspace Developer's Guide and .NET API Reference and the Workspace Extension Examples for information on how to customize Workspace. Refer to the Platform SDK 8.0 .NET API Reference and Developer's Guide for information on lower-level customization capabilities.

Common system aspects

The goal of Genesys 8 and Workspace is to provide a consistent, simplified, and comprehensive application that enables each user at every level to be efficient and productive. Genesys 8 and Workspace focus on a set of criteria that deliver a higher level of productivity. Workspace is designed "from the ground up" to have a high degree of usability, with the goal of enhancing agent productivity.

Internationalization

Workspace uses the existing internationalization capabilities of Genesys back-end components, such as Universal Contact Server, that employ Unicode to support multiple languages. Workspace uses the Genesys Platform SDK **ESP** protocol to communicate with Genesys back-end servers that also support the same Unicode protocol.

Any set of Unicode characters is supported; therefore, any language that is supported by Unicode is supported by Workspace; however, to support more than one Unicode language in your environment, you must configure the specific Unicode support for each connection (this is configured in the same way as TLS requires custom encoding).

Workspace is aligned with the existing internationalization capabilities of Genesys back-end components:

- Universal Contact Server uses Unicode to support multiple languages. Therefore, for this connection any combination of locale that is specified in the client configuration, server configuration, and interaction content is supported. This applies to the content of the Notepad, the body of an email and so on.
- Other Genesys back-end servers do not implement Unicode. Therefore, internationalization requires you to configure consistently the locale of the system servers, the client "locale for non Unicode application", and the content of interactions. Each of these items must rely on the same Code Page (several languages can be supported by a single code page). This configuration applies to the user data, configuration data, and so on of each interaction.
- You can configure Workspace to enforce which encoding is used when it communicates with non-Unicode back-end servers. To do this, configure the following options:

  `general.non-unicode-connection-encoding`--The value corresponds to the `.Net Name of Code Page Identifier`. Refer to the following article: http://msdn.microsoft.com/en-us/library/windows/desktop/dd317756(v=vs.85).aspx

  For the Configuration Server connection, the code page identifier must be set in the `general.non-unicode-connection-encoding` key in the `Workspace.exe.config` file.

Accessibility and navigation

Section 508 accessibility

You can use a screen-reader application or the keyboard to navigate the agent desktop interface.

Screen readers

Workspace is designed to maximize content readability for screen-reader applications. Workspace can be configured to be compatible with screen readers that support Microsoft UI Automation API, such as the Freedom Scientific application: Job Access With Speech (JAWS) version 11. Screen readers enable visually impaired (blind and low-vision) agents to use the desktop interface through text-to-speech or text-to-Braille systems. Workspace must be configured in the Configuration Layer to enable this compatibility (see Accessibility). These options can be set in the Configuration Layer as default values that can be overridden in the Agent Annex following the standard hierarchy configuration.

Keyboard navigation of the interface

You can navigate the Workspace interface by using a keyboard or other accessibility device that is enabled by keyboard navigation. This feature improves the accessibility of the interface by not forcing the user to navigate by using the mouse. Navigation works panel to panel and, within a panel, component to component.

In general, you can use the TAB key to set the focus on the next component; use the SHIFT-TAB key combination to set the focus on the previous component. You can use this method to navigate the Menu bar, the interaction interface, the tabs, and so on.

Access keys and keyboard shortcuts

Workspace follows the Microsoft Windows convention of enabling interface navigation by using access keys. Access keys are alphanumeric keys that are employed in combination with the ALT key to replicate a menu command or button click the interface.

Workspace also provides shortcut keys. Shortcut keys, which are intended mostly for advanced users, enable quick access to frequently performed actions. Shortcut keys can be reconfigured by Tenant, Group, and/or User by using Genesys Administrator Extension. These key combinations are documented in the *Workspace 8.5 User's Guide*.

Security

RADIUS

Workspace implements the Remote Authentication Dial-In User Service (RADIUS) security protocol to prevent illegal system access, track system use, and limit the access of authenticated users. To access the system, users must provide their credentials and connection parameters for authentication before they can be granted limited system access.

The user must provide both a user name and a password to gain access to the Configuration Layer, which is used to obtain a list of existing places, privileges that are specified for the user, and configuration of the agent application. A place is mandatory for all Interaction Workspace agent scenarios. A role or roles are assigned to agents upon login. Agents do not have access to system aspects outside of those that are defined by their assigned roles.

Transport Layer Security (TLS)

Workspace supports Transport Layer Security (TLS), which is a cryptographic protocol that provides security and data integrity for communications over networks such as the Internet. TLS encrypts the segments of network connections at the transport layer from end to end. For more information about TLS, refer to the Genesys TLS Configuration chapter of the *Genesys 8.1 Security Deployment Guide*.

FIPS

As of release 8.1.401, Workspace supports Federal Information Processing Standard (FIPS). For information about configuring and using FIPS, refer to *Genesys 8.1 Security Deployment Guide*.

Controlling TLS version

Prior to Interaction Workspace 8.1.4, encrypted communication was used to secure the communication protocol between Workspace and the other Genesys Servers. This method meant that control on certificate expiration and authority was not enforced. Workspace 8.1.4 (and higher) implements full TLS control. If you have migrated from Interaction Workspace 8.1.3 (or lower) to 8.5.0, you might receive warning messages from the system informing you that the security certificate on a particular channel has expired. This renders the channel `Out of Service` until the certificate is updated. Workspace supports a TLS connection to Universal Contact Server (UCS) starting from version 8.1.3 of UCS. For support details for other Genesys servers please refer to the respective product documentation.

Up to version 8.5.118.10, you can use the `ssl-version` option in the `interactionworkspace.exe.config` configuration file to specify the maximum TLS version to be used by Workspace during the handshake of the initialization of a secured connection to one of the Genesys back-end servers such as SIP Server:

- **Name:** ssl-version
- **Valid values:** One label from the following list: `TLS1.0`, `TLS1.1`, `TLS1.2`
- **Default value:** `TLS1.0`

Starting with version 8.5.119.05, the mentioned `ssl-version` option is deprecated and the maximum TLS version that Workspace requires is 1.2.

Configuring Mutual TLS with backend servers

[**Added:** 8.5.148.04]

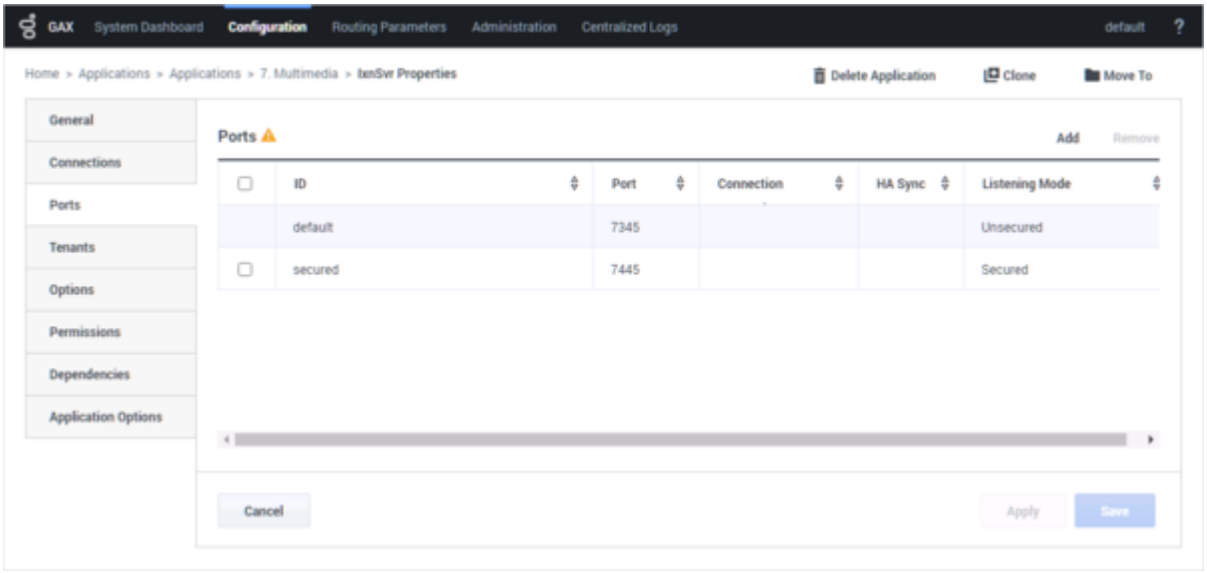
Configuring Mutual TLS between Workspace and the backend servers for which you have set up connections, such as TServer, Interaction Server, Universal Contact Server, Statistics Server, and Configuration Server ensures security of data exchange. Each time Workspace and server initiate a connection, Mutual TLS negotiation occurs, and it is valid until the connection ends. Workspace

notifies the agent if a TLS certificate error occurs for the corresponding media or service and a response is available from the server. Servers may behave differently on TLS connection issues. Therefore, check the server logs to troubleshoot the Mutual TLS connection issues.

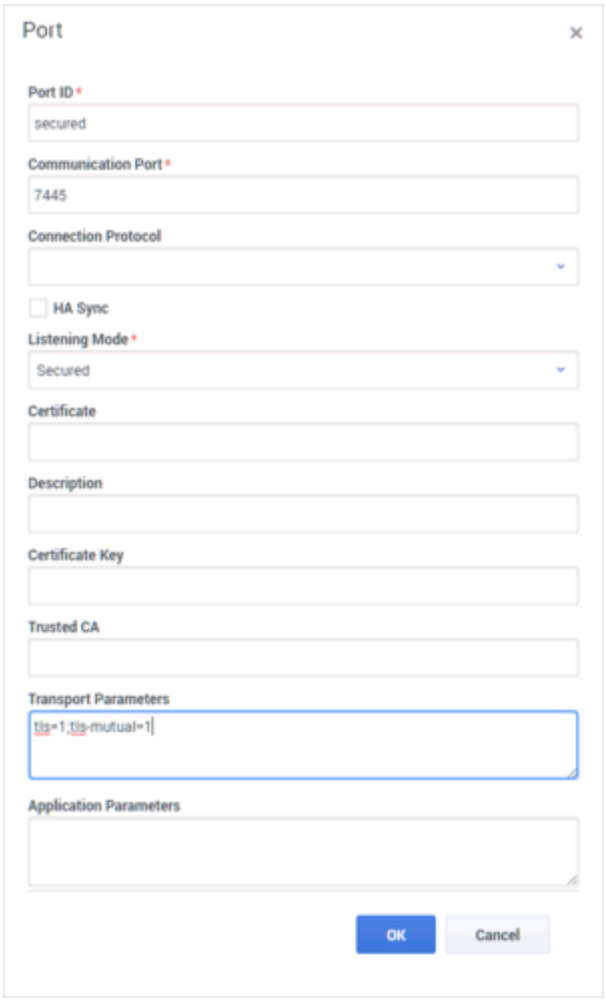
> **Important**
>
> Workspace caches the Configuration Server data. If the Configuration Server connection is down, Workspace can reuse the cached data.

You can configure Mutual TLS only for secured ports. For Configuration Server, you must use upgrade port (refer to the following procedure). To configure Mutual TLS between Workspace and the connected backend servers, follow these steps for each connected backend server to enable Mutual TLS:

1. In Genesys Administrator Extension, open the **Properties** for the Server (for example, Interaction Server):



2. Open the **Ports** tab.
3. Select **Secured**. For Configuration Server, select **Upgrade**.
4. Ensure the **Listening Mode** is set to **Secured**. For Configuration Server, **Listening Mode** can be set to **Secured** or **Auto Detect/Upgrade**.
5. In the **Transport Parameters** field paste the following text: "tls=1;tls-mutual=1"



For Configuration Server, you must paste the following text instead: "upgrade=1;tls-mutual=1"

6. Click **OK** then save your changes.
7. Configure the security.client-authentication-certificate-search-value option. One of the following configurations is available:
   - If you want Mutual TLS to apply to Configuration Server as well as to all other servers with enabled Mutual TLS, in the **InteractionWorkspace.exe.config** configuration file, add the **security.client-authentication-certificate-search-value** option.
   - If you want Mutual TLS to apply to all servers with enabled Mutual TLS except Configuration Server, configure the **security.client-authentication-certificate-search-value** option in Genesys Administrator Extension.

Important

- Backend servers provide different levels of support for TLS connections. For more information, refer to TLS Feature Support Matrix.

- First certificate selected for mutual TLS will be used for all mutual TLS connections before Workspace restart.

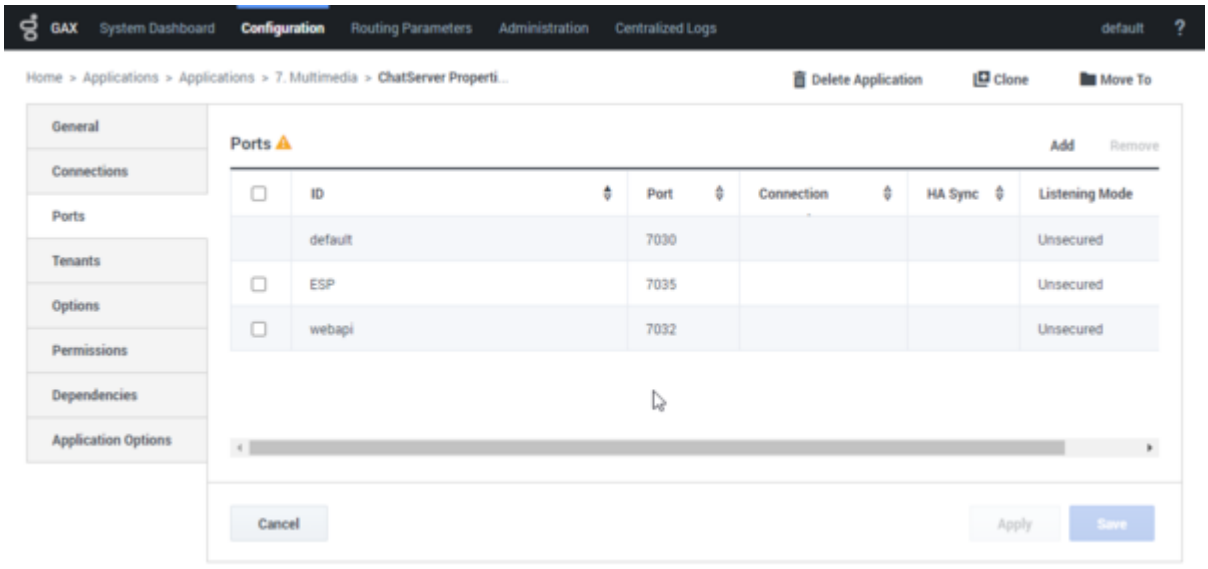
Configuring Mutual TLS with Chat Server

Important

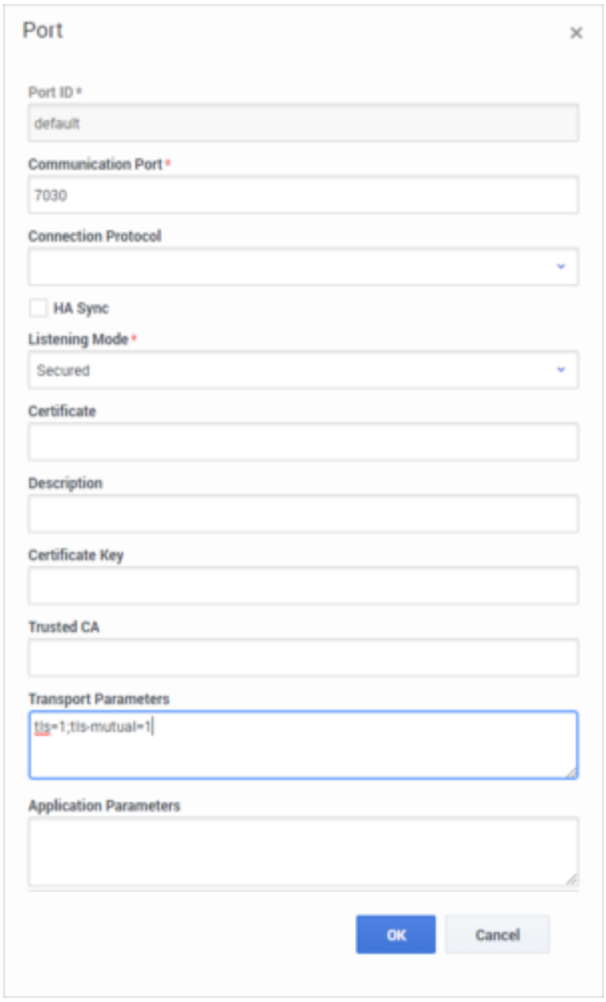
To enable successful Mutual TLS connection between Workspace and Chat Server, besides configuring the security.client-authentication-certificate-search-value option, you must also set the value of the chatserver.tls-mutual option to `true`. This option indicates to Workspace to provide a certificate key in environments where Chat Server works in Mutual TLS mode.

If the agent handles an interaction that is specific to Chat Server, Workspace connects to Chat Server. To configure Mutual TLS between Workspace and Chat Server, follow these steps:

1. In Genesys Administrator Extension, open the **Properties** for Chat Server.



2. Open the **Ports** tab.
3. Select **default**.
4. Ensure the **Listening Mode** is set to **Secured**.
5. In the **Transport Parameters** field paste the following text: "tls=1;tls-mutual=1"



6. Select **ESP**.
7. Repeat from Step 2 to Step 5 to define values in the **Transport Parameters** field.
8. Click **OK** then save your changes.
9. Configure the chatserver.tls-mutualoption.

Workspace SIP Endpoint

Pre-requisites: Workspace 8.5.001 and higher, and Workspace SIP Endpoint 8.5.000 and higher.

The sipendpoint.transport-protocol option enables configuration of the SIP Transport Protocol. For encrypted transport, set the value of this option to TLS.

The *No results* option enables you to configure the RTP Protocol. For encrypted transport, set the value of this option to 1. If Workspace is deployed in a SIP Business Continuity environment, set also the value of the *No results* option to 1 to encrypt the peer SIP connection. For more information about SRTP, refer to *Genesys 8.1 Security Deployment Guide* and *SIP Server 8.1 Deployment Guide*.

If Workspace SIP Endpoint must connect to an SBC or a SIP Proxy instead of an actual SIP Server, then

you must configure the sipendpoint.sbc-register-port configuration option (and sipendpoint.sbc-register-port.peer if you are running Workspace in SIP Business Continuity scenarios) by specifying the UDP/TCP or TLS ports.

Inactivity time-out

Workspace can be configured to become locked after a specific period of time during which neither the agent's mouse nor keyboard are used. This feature protects your system from unwanted system access, should the agent walk away from a workstation without locking it.

When the specified time period of inactivity is reached, all of the open Workspace windows on the agent's desktop are minimized, and the Reauthenticate view is displayed. Interaction notifications such as notification of inbound interaction delivery are still displayed, but business information about them is not, and the **Accept** and **Reject** buttons are disabled.

To unlock Workspace, the agent must enter in the Reauthenticate view the password that was used to log in the locked application, then click Authenticate.

Refer to the *Workspace 8.5.x Help* for details about using the reauthentication feature.

Business Continuity

The *Framework 8.1 SIP Server Deployment Guide* provides detailed information about Business Continuity architecture and configuration. A disaster is defined as the loss of all Genesys components that are running on one or more physical sites. Business Continuity is a set of automated procedures that enable agents that are connected to the site that is experiencing a disaster to connect to an alternate site to continue working normally with minimal data lost. This is known as Geo-redundancy.

In the event of a disaster, Workspace can be configured to maintain a dual connection to a pair of SIP Servers, a pair of Stat Servers, and a pair of Configuration Servers at two different sites.

Two or more switches must be configured in Genesys Administrator Extension to have identical agent extensions and logins. Agents must be able to log in to any synchronized switch at any time. In a typical Business Continuity set up, two pairs of High Availability (HA) SIP Servers are implemented. Each pair of SIP Servers, the Preferred server and the Peer server, use synchronized (not replicated) configuration layer objects. Agents are logged in to the Current Primary server in their Preferred site HA Pair. Each agent has two SIP Channels and two SIP Endpoints registered on each server.

Workspace always tries to connect to the Preferred server. If it is not available it connects to the alternate (Peer) server until the Preferred server becomes available again. The agent state is set to `Not` Ready until a connect with one or the other server is established.

> **Warning**
> The current interaction might be lost.

Refer to the Procedure: Configuring Workspace for Business Continuity to enable Business Continuity for your agents and eServices Business Continuity.

Licensing

There are no technical licensing requirements for Workspace.

Framework and solutions compatibility

Workspace is part of the Genesys 8 suite of products. See Table - **Interoperability between Workspace Desktop Edition 8.5 and other Genesys Products** for a list of key compatibilities. Also see the following system guides for details on compatibility and system requirements:

- *Genesys Hardware Sizing Guide*''
- *Genesys Interoperability Guide*
- *Genesys Licensing Guide*
- *Genesys Supported Media Interfaces Reference Manual*
- *Genesys Supported Operating Environment Reference Guide*