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.

# Workspace Desktop Edition Deployment Guide

Workspace Desktop Edition 8.5.1

6/27/2024

# Table of Contents

# Workspace Desktop Edition 8.5 Deployment Guide

Deployment and Configuration information for **Genesys Workspace Desktop Edition** (Workspace)

These pages introduce you to Workspace Desktop Edition, the Genesys agent desktop interface. Privilege- and role-driven capabilities, as well as features that focus on the needs of the user, make Workspace a total agent solution. The Workspace agent interface enables users to invoke interactions that are related to existing interactions -- thus ensuring a consistent customer experience. Workspace is a modular application that permits expansion and customization.

See the following resources for information about how to customize and extend Workspace:

- Workspace Developer's Guide and .NET API Reference
- Workspace Extension Examples

See the following topic for information about the **Genesys Plug-ins** that are available for Workspace:

- Workspace Plug-ins

## Hybrid Integrations

Some Genesys Cloud services are available for Workspace. You must prepare your environment by provisioning a Genesys Engage Hybrid Integration and Integrating Genesys Predictive Engagement into Genesys Engage on-premises.

### Installation and deployment introduction

Find information about concepts, features, functionality and environment.

Concepts and Features

Workspace Functionality Overview

Supported Systems and Switches

### Deploying Workspace

Find detailed information about planning your Workspace deployment.

Deploying Workspace

Effects of Configuration Options and Privileges on Performance

### Deployment Procedures

Find all of the procedures that you need to install and deploy Workspace.

Deployment Procedures for Workspace

Installing plug-ins for Workspace

### Provisioning Workspace

Find all of the procedures that you need to enable the features of Workspace.

Provisioning Workspace

### Configuration options and privileges

Find detailed descriptions for all of the configuration options and role privileges that are available in Workspace.

Workspace Configuration Options Reference

### Document change history

A list of topics that are new or that have changed since the previous release.

New in Deployment Guide 8.5.1

# What's new in Workspace?

The following pages contain a list of topics that are new or have changed significantly in the specified release of Workspace:

## Workspace 8.5.155.03

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.155.03:

- The new configuration option, **teamcommunicator.person-cache-for-favorites-recents-enabled**, is introducing a new Team Communicator data initialization mode that reduces the number of requests to Configuration Server or Configuration Server Proxy when it prepares the Favorite list and Recent list of records for Team Communicator. To enable this new Team Communicator data initialization mode, the value of this option must be set to `true`.
    - teamcommunicator.person-cache-for-favorites-recents-enabled

## Workspace 8.5.154.05

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.154.05:

- You can specify the list of attachment file types for which agent operations, such as Attach, Open, Save, and Save All, will be blocked. File types are recognized by binary content, unlike the file extension used in chat.restricted-attachment-file-types and email.restricted-attachment-file-types options. Following file formats are supported: Windows/DOS executable file and PKZIP archive file. Microsoft Office document files having extension '.docx', '.xlsx' have format PKZIP. If the file format 'zip' is specified in this option, the file will be rejected. The content type of the attachments added by inserting a Standard Response into an interaction is not validated by the Workspace logic controlled by this option.
    - general.restricted-attachment-file-content-types

## Workspace 8.5.153.05

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.153.05:

- You can define the number of reconnection attempts to the sms session to make in the case of a connection loss. The following configuration option has been added to support this feature:
    - sms.reconnect-attempts
- You can specify the duration, in seconds, between each attempt to reconnect to the sms session in the

case of a connection loss. The following configuration option has been added to support this feature:

  - sms.reconnect-timeout

## Workspace 8.5.150.06

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.150.06:

- Agents can paste formatted text as plain text in HTML emails using `Paste Text Only` format.
- You can specify the time, in seconds, after which an engaging call of Outbound Assured Connection can be released. The following configuration option has been added to support this feature:
  - outbound.assured-connection.allow-release-engaging-call-timeout
- You can specify the width, in pixels, of Rich Media in a chat interaction. The value of this option affects the minimum width of the Chat transcript view. The following configuration option has been added to support this feature:
  - chat.rich-media-widget-width
- You can specify whether the agent must complete the mandatory case data before applying a 'Transfer' and/or 'Conference' action for any Digital Channel interaction other than email. The following configuration option has been added to support this feature:
  - interaction.case-data.<media-type>.mandatory-actions
- You can specify whether the agent must complete the mandatory case data before applying a 'Transfer' or 'Forward as an attachment’ action on an email interaction. The following configuration option has been added to support this feature:
  - interaction.case-data.email.mandatory-actions
- You can specify whether the mandatory disposition code must be completed by the agent before applying a 'Transfer’ and/or 'Conference' action for interactions of any given media type that is different from email. The following configuration option has been added to support this feature:
  - interaction.disposition.<media-type>.mandatory-actions

## Workspace 8.5.149.03

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.149.03:

- In addition to the existing Screen and Classify service support, Workspace now supports the Analyze service of Classification Server to detect suggested responses.

## Workspace 8.5.148.04

- Workspace now supports Mutual TLS connection with the Genesys backend servers. The following options have been added to support this feature:
  - security.client-authentication-certificate-search-value
  - chatserver.tls-mutual

## Workspace 8.5.147.05

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.147.05:

- Workspace Desktop Edition now embeds a WebView2 SDK, which allows Chromium-based web rendering customizations with WebView2 control supported by Microsoft Edge WebView2.

## Workspace 8.5.145.06

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.145.06:

- You can now use the Assured Connection feature in Progressive and Predictive Outbound Campaigns.
- You can now specify the display format of the Chat contact party name by using a string that can contain regular characters and field codes. The following option has been added to support this feature:
  - display-format.chat-customer-name

## Workspace 8.5.144.05

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.144.05:

- You can now mask the contact phone number for contact information stored in Universal Contact Server (UCS). The following options have been added to support this feature:
  - contact.history.voice-detail-attributes
  - contact.multi-value-attribute-display.<contact-attribute>
- The standard-response.categories option has been modified for this release.

## Workspace 8.5.143.08

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.143.08:

- Workspace Desktop Edition Role-based access (RBAC) now supports both the Genesys Administrator Role data storage model, introduced by Management Framework 8, and the Genesys Administrator Extension Role data storage model (as implemented in Genesys Engage cloud). RBAC requires Configuration Server 8.0.2 or higher and either Genesys Administrator 8.0.2 or higher, or Genesys Administrator Extension (9.0.100.56 or higher is recommended).
- You can now specify whether a Business Attribute is used to specify the default 'From' email address of a reply email interaction. The following option has been added to support this feature:
  - email.from-addresses.force-default-on-reply
- The <media-type>.contact-history.enable-combine-interaction-with-current option is replaced by <media-type>.contact-history.enable-combine-ixn-with-current. This change resolves an issue where the length of the name of the media type could cause the length of the option name to exceed the maximum number of allowable characters.
- You can now specify how an Outbound Record from a Record Chain is displayed when presented to an agent. The following option has been added to support this feature:
  - display-format.outbound-record-name

    The following option has been modified to support this feature:
  - display-format.caller-name

    See Masking a contact's phone number on inbound and outbound interaction views for a use case on using the `display-format.*` options to mask caller data in the Workspace agent UI.
- Workspace Desktop Edition now provides a Voluntary Product Accessibility Template (VPAT) report as part of the accessibility and navigation features and accessiblity configuration documentation: Genesys Workspace Desktop Edition Accessibility Conformance Report
- Use the screen-recording.client.address option to specify the IP address or host of the Screen Recording Service. You can use this option to support screen recording in a Genesys Softphone VDI environment.

## Workspace 8.5.142.05

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.142.05:

- Workspace can now display Rich Media elements contained in Chatbot messages sent to a contact who is connected to the Genesys WebChat Widget. This applies to live Chat interactions and the History view.
- You can now specify whether interactions opened from the **Contact History** tab are opened in the same view as the currently active interaction or in a separate case view. The following option has been added to support this feature:
  - <media-type>.contact-history.enable-combine-interaction-with-current

(**Note**: this option is renamed to <media-type>.contact-history.enable-combine-ixn-with-current in 8.5.143.08; however, both options are supported).

## Workspace 8.5.141.04

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.141.04:

- You can specify how the DN-less phone number specified by an agent during login is propagated to the Genesys back-end. Passing as an extension to SIP Server limits the impact of multiple simultaneous login or logout events in the case of a Disaster Recovery/Business Continuity event. SIP Server 8.1.102.93 or higher is required for this feature. Refer to Remote Agents with Non-provisioned DNs for more information. The following option has been added to support this feature:
  - login.voice.use-dn-less-login-extension
- You can have editable case data copied back to the original inbound email from an outgoing reply email interaction when it is sent. The following option has been added to support this feature:
  - email.outbound.copy-editable-case-data-in-inbound
- You can specify a prefix to be used when an agent resends an outgoing or reply email from History (**My History**, **Contact History**, and **Interaction Search**). The following option has been added to support this feature:
  - email.resend-prefix.
- You can specify whether the default Business Attribute value of a drop-down list is automatically populated in the associated contact attribute field of the Contact Information tab. The following option has been added to support this feature:
  - contact.multiple-value-attributes-enable-default-description
- You can pre-load folders of Business Attribute objects containing folders for folder/tree structure display for Disposition Codes and Case Data when an agent logs in to avoid a delay in loading this content when an interaction is first received. The following option has been added to support this feature:
  - general.configuration-business-attribute-folder-cache-preload

## Workspace 8.5.140.08

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.140.08:

- You can specify whether the chat transcript displays interactions as left-to-right or right-to-left reading to support interactions written in a right-to-left reading language. By default, Workspace displays interactions as left-to-right reading. The following option has been added to support this feature:
  - chat.transcript-message-text-direction
- In SIP Server environments, you can specify whether the DN-less phone number stored in the agent's DN is restored to its original value when the agent logs out of this DN. The following option has been added to support this feature:

  - login.voice.restore-dn-less-phone-number-on-logout

- In a Virtual Desktop Infrastructure (VDI) environment, you can specify whether Workspace relies on a DNS resolution to identify the IP Address used to connect to Workspace SIP Endpoint. The following option has been added to support this feature:
  - sipendpoint.standalone.vdi-detection-use-dns
- The `login.kerberos.agent-identification` option has been updated in this release. The following values have been added or modified:
  - `implicitupn`: Workspace 8.5.140.08 and higher uses the Implicit User Principal Name (iUPN), which is a combination of the **samAccountName** and the user's Domain name. [Added: 8.5.140.08]
  - upn: Workspace 8.5.132.05 to 8.5.139.07 uses the User Principal Name (UPN) specified by Windows Administrator in the Windows Active Directory when provisioning the account of an agent. This mode is deprecated and should be substituted by `implicitupn`, but is maintained for compatibility purposes.

## Workspace 8.5.139.06

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.139.06:

- You can configure Workspace to automatically set agent status to Not Ready or Not Ready with a Not Ready Reason when their workstation is locked. The following options have been added to support this feature:
  - security.session-lock-set-agent-not-ready
  - security.session-lock-force-not-ready-state
  - security.session-lock-not-ready-reason
- You can configure Workspace to automatically force the agent state to Not Ready when inactivity timeout occurs. The following option has been added to support this feature:
  - security.inactivity-force-not-ready-state

## Workspace 8.5.138.04

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.138.04:

- You can now enable agents to enter different Places associated with different types of SIP DNs when they log in so that they can login from a Workspace SIP Endpoint/Genesys Softphone workstation one day and from their mobile or home phone through SIP Server, or a 3rd party SIP Endpoint on a different day. The following option has been added to support this feature:
  - voice.device-type

## Workspace 8.5.137.06

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.137.06:

- You can now specify whether Workspace preserves the availability interval of the parent Outbound record when rescheduling an Outbound record with a new phone number. The following option has been added to support this feature:
    - outbound.reschedule-inherit-parent-availability-interval
- In environments where the main toolbar is configured in auto-hide mode, you can now configure the delay between the moment when the mouse cursor reaches the top of the screen and the moment the Workspace toolbar is displayed. The following option has been added to support this feature:
    - main-window.auto-hide-display-delay

## Workspace 8.5.136.07

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.136.07:

- Contact History search has been improved for UCS 9.1 users. The following option has been added to support this feature:
    - contact.history-custom-attributes-search-types
- It is now possible to adjust the timing of the auto-hide/display property of the Main window. The following option has been added to support this feature:
    - main-window.auto-hide-display-delay

## Workspace 8.5.132.05

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.132.05:

- To prevent changes to the case data after a voice or chat interaction has ended, the interaction.case-data.is-read-only-on-idle option has been added.
- To specify whether the Category ID of the reply outbound email is copied to the parent inbound email, the email.reply-copy-category-id option has been added.
- For Chat interactions, to specify that the value specified for the contact.history.filters-<attribute> option is used to filter the history-based part of the chat transcript, the chat.transcript-enable-history-filters option has been added. Keys and values of the option are constructed like those of the `contact.history.filters-<attribute>` option. You can add these options to a routing strategy.
- For SMS interactions, to specify that the value specified for the contact.history.filters-<attribute> option is used to filter the history-based part of the SMS transcript, the sms.transcript-enable-history-filters option has been added. Keys and values of the option are constructed like those of the

`contact.history.filters-<attribute>` option. You can add these options to a routing strategy.

- To support Kerberos in a multi-tenant environment, the `login.kerberos.agent-identification` option in the `interactionworkspace.exe.config` configuration file has been modified. The upn value has been added to enable Workspace to use the User Principal Name (UPN) specified by Windows Administrator in Windows Active Directory when provisioning the account of an agent.
- To specify whether the 'Complete Conference' function requires a consultation call to the Agent to be established first or not, the voice.complete-conference-requires-connected-consultation-call option has been added.

## Workspace 8.5.128.07

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.128.07:

- When contacts disconnect from chat interactions, you can specify that chat interactions are auto marked done immediately or are auto marked done after a configurable time interval. The following configuration options have been added to support this feature:
  - chat.auto-mark-done-owner-agent
  - chat.auto-mark-done-owner-agent.timer
  - chat.auto-mark-done-non-owner-agent
  - chat.auto-mark-done-non-owner-agent.timer
- You can keep chats open after the last agent leaves the session, enabling an agent to rejoin the session until the session is marked Done using the Asynchronous chat function. The following Chat privileges were added to support this feature:
  - Chat - Can Place On Hold
  - Chat - Can Release Async
  - Chat - Can Release

    The following configuration options have been added to support this feature:
  - chat.on-hold-queue
  - keyboard.shortcut.interaction.chat.hold

## Workspace 8.5.127.06

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.127.06:

- Agents can combine left-to-right (LTR) text or right-to-left (RTL) text in the same email message by using the **Right-to-left Text Direction** and **Left-to-right Text Direction** buttons. The following configuration option has been added to support this feature:
  - email.can-change-text-direction

## Workspace 8.5.126.07

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.126.07:

- Supervisors/Team Leads can manually change the state of agents to **Ready**, **Not Ready**, and **Logoff** by using Team Communicator. The following privilege has been added to support this feature:
  - Team Lead - Can Change Agent State

    The following configuration option has been added to specify which state changes a team lead is allowed to make:
  - teamlead.agent-status.enabled-remote-actions
- Support for UCS 9.1.
- You can specify the list of attributes to be displayed in tree view in the **Interaction Search** view. The following configuration option has been added to support this feature:
  - contact.all-interactions-displayed-columns-treeview
- You can specify the date display format for custom attributes that you want to display as dates in the History view.
- Support for Receiving-side Automatic Gain Control (Rx-AGC) for Workspace SIP Endpoint has been added to address the problem with some calls having too low a volume for agent to hear the customer clearly. The following configuration option has been added to support this feature:
  - sipendpoint.policy.session.rx_agc_mode
- Support for specifying the Local IP address or Fully Qualified Domain Name (FQDN) of the machine on which SIP Endpoint is running. This setting can be an explicit setting or a special value that the SIP Endpoint uses to automatically obtain the public address. The following configuration option has been added to support this feature:
  - sipendpoint.policy.endpoint.public_address
- The valid values of the sipendpoint.system.security.use_srtp option have been expanded.

## Workspace 8.5.125.04

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.125.04:

- The `date.time-display-format` option has been added to Case Information to enable you to specify how the `DateTime` variable in attached data are displayed in Workspace views, such as Outbound attached data. You can specify both date and time, just the date, just the time, and so on.

## Workspace 8.5.124.08

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace

Desktop Edition 8.5.124.08:

- For Alcatel 4400/OXE switch environments only, you can specify whether or not the queue that is used on login should be used for the queue on logout. The following configuration option controls this feature:
  - logout.voice.use-login-queue-on-logout
- You can control whether agents are able to extend their After Call Work (ACW) status beyond the wrap-up time that you specified. The following configuration option enables this feature:
  - voice.after-call-work-extension
- In Accessibility mode, you can prevent hyperlinks from being active in email, chat, and SMS interactions. Some screen readers cause Workspace to become unresponsive when processing active hyperlinks. The following option has been added to enable this feature:
  - accessibility.disable-hyperlinks

## Workspace 8.5.122.08

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.122.08:

- You can choose between the original simple text display and the new block style display introduced in this release for the Chat, SMS, and IM transcript views. The following options have been added to support this feature:
  - chat.simple-transcript
  - im.simple-transcript
  - sms.simple-transcript
- You can add an unread message icon to the chat transcript so that your agents know when the chat message they sent has been read. The icon disappears when the message is read. The following option has been added to support this feature:
  - chat.show-unread-notification
- You can specify whether agents can see previous chat sessions with a contact in the current chat session. This reduces the need for agents to open the contact history to find previous chat interactions. Many chat sessions are conducted on mobile devices, meaning that the likelihood of timeout is very high. If a chat is resumed after a timeout, the agent sees the content of the previous sessions. The following option has been added to support this feature:
  - chat.historical.maximum-age
- The default color values have been updated for the following Chat, SMS, and IM options:
  - chat.agent.prompt-color = #FF2E6599
  - chat.agent.text-color = #FF3D464D
  - chat.other-agent.prompt-color = #FF295B00
  - chat.other-agent.text-color = #FF3D464D
  - chat.client.prompt-color = #FFAF4F0B

  - chat.client.text-color = #FF3D464D
  - im.agent.prompt-color = #FF2E6599
  - im.agent.text-color = #FF3D464D
  - im.other-agent.text-color = #FF3D464D
  - im.other-agent.prompt-color = #FF295B00
  - sms.agent.prompt-color = #FF2E6599
  - sms.agent.text-color = #FF3D464D
  - sms.other-agent.prompt-color = #FF295B00
  - sms.other-agent.text-color = #FF3D464D
  - sms.client.prompt-color = #FFAF4F0B
  - sms.client.text-color = #FF3D464D
- You can specify an alert bell when there is a pending chat message to be answered. The following option has been added to support this feature:
  - chat.pending-response-to-customer-bell
- You can configure Workspace to notify agents when there is a change to an interaction property inside a specified workbin. The following option has been added to support this feature:
  - workbin.<media-type>.<nick-name>.notify-property-changed

## Workspace 8.5.120.05, WSEP 8.5.114.05

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.120.05, WSEP 8.5.114.05:

- You can specify the format of the folder structure that is displayed to agents in the Disposition Code view and Case Data view. The following option has been added to support this feature:
  - display-format.folder.name

## Workspace 8.5.119.05

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.119.05:

- You can configure Workspace to specify whether an outgoing email interaction must have a subject before the email can be sent. The following option has been added to support this feature:
  - email.mandatory-subject

## WSEP 8.5.113.02

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition WSEP 8.5.113.02:

- Workspace SIP Endpoint now supports DNS SRV resolution to connect to Genesys SIP Proxies. The following options have been updated to support this feature:
  - sipendpoint.sbc-register-address
  - sipendpoint.sbc-register-port
  - sipendpoint.sbc-register-address.peer
  - sipendpoint.sbc-register-port.peer

## Workspace 8.5.118.10

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.118.10:

- Agents can call and transfer calls to the voice mail of other agents and agent groups. The following configuration options have been added to support this feature:
  - intercommunication.voicemail.enabled-target-types
  - intercommunication.voicemail.routing-points

  ### The following privileges have been added to support this feature:

  - Voice Mail - Can Deposit Message
  - Voice Mail - Can Transfer Message
- Agents can create, manage, and delete hyperlinks in chat and email interactions using hyperlink management tools. Refer to the *Help* and *User's Guide* for more information about this feature.
- You can set up short cut keywords that let agents enter responses into text based interactions by typing a prefix key followed by the keyword. The following configuration options have been added to support this feature:
  - editor.shortcuts.prefix
  - standard-response.shortcuts.<keyword>
- Agents can update case information by searching and selecting categories from a directory tree.
- You can specify attachment types to edit only certain file types preserves the data integrity of files that you do not want agents to modify. For example, you might allow agents to modify .jpg and .png files so that the orientation can be changed, but restrict the modification of .docx, .xlsx, and other file types. Or, you might want to ensure that only .xlsx files can be updated by agents. The following configuration option has been added to support this feature:
  - general.writable-downloaded-attachment-file-types
- You can manage how agents can force close stuck interactions. The following configuration option has

been added to support this feature:

- interaction.unconditional-force-close

## Workspace 8.5.117.18

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.117.18:

- Hybrid voice agent configuration is now supported to let an agent log in on two distinct voice devices and answer or make calls (according to priority rules) from each of them. Skype for Business and Workspace SIP Endpoint hybrid mode support has been added. Contact centers are no longer required to choose between Skype for Business or Workspace SIP Endpoint as their communication media of choice. With hybrid mode, both can be used by the same agent for handling customer interactions and internal communication. This feature significantly expands Skype enabled enterprise/back office users as available resources for assistance to improve first contact resolution. The following configuration options support this feature:
  - expression.callable-phone-number
  - voice.hybrid-switch-preference
  - `spl.switch-policy-label`
  - `display-name or display-name.<language-code>-<country-code>`
- You can control automatic contact assignment by enabling agents to choose from a list of possible matching if there is more than one contact in the contact database to which a new inbound interaction can be assigned. The following configuration options support this feature:
  - contact.lookup.auto-assign-mode
  - contact.lookup.<media-type>.auto-assign-mode
- You can force an Outbound enabled agent to complete the processing of an outbound record prior to transferring or conferencing the call to another agent, and retain the call result in the OCS database. The following configuration options support this feature:
  - outbound.complete-record-before-transfer
  - outbound.call-result-is-mandatory
- You can specify whether the current interaction is highlighted in the Contact History view of the current interaction. If the current interaction is not on the first page of the view, the view is scrolled to the position of the current interaction. The following configuration option has been added to support this feature:
  - contact.history.highlight-current-interaction
- You can specify that it is mandatory for agents to edit case data fields before they can mark an interaction as Done. If the agent tries to close the interaction without editing the case data field, an error message is displayed. Mandatory fields are marked with a red asterisk. This feature is supported by the `interaction-workspace/mandatory` option.

## Workspace 8.5.116.10

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.116.10:

- You can specify how new interaction windows behave after an agent who is working on one or more interactions accepts a new inbound interaction. You can choose to have the new interaction window receive the focus (default behavior), or you can choose to keep the focus on the currently active interaction window. You can also configure this behavior by media channel. The following configuration options have been added to support this feature:
  - interaction.auto-focus
  - interaction.auto-focus.<media-type>
- Screen recording through Genesys Interaction Recording (GIR) has been ehanced to support hot seating (hot desking) environments. The following option has been modified to support this feature:
  - screen-recording.htcc.uri
- The behavior of the email.reply-prefix option has been modified to better handle multiple reply email interaction threads. This option can also be overridden by a routing strategy to handle situations where the locale of the recipient might be different from the locale of the agent.
- Cisco Call Manager environments now support two DNs, one for ACD calling and one extension.

## Workspace 8.5.115.17

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.115.17:

- Agents can save files that they receive through chat interactions and can transfer files either from their workstation or from Standard Responses to contacts in a chat interaction. The following configuration options have been added to support this feature:
  - chat.attachment-download-timeout
  - chat.max-attachments-files
  - chat.max-attachments-size
  - chat.max-file-size
  - chat.restricted-attachment-file-types
  - chat.show-attachment-image-thumbnail

  ### The following privileges have been added to support this feature:

  - Chat - Can Save Attached files
  - Chat - Can Transfer File From File System
  - Chat - Can Transfer File From Standard Response
- You can enable your agents to send emojis as part of chat interactions. The handling of received emojis

has been improved. In Workspace, sent and received emojis are displayed as Unicode characters according to the default Workspace and Windows system fonts, which Workspace uses in the Chat Interaction view. You define which emojis your agents can use by configuring a Business Attribute that populates the emoji item in the chat composition tool bar. The following configuration option has been added to support this feature:

- chat.emojis-business-attribute
- gui.emoji-font-name

### The following privilege has been added to support this feature:

- Chat - Can Use Emojis

- You can control which Chat Server messages are recorded in chat transcripts and SMS Session transcripts in the Contact History.
- For Outbound campaigns, you can specify whether rescheduled calls/callbacks are personal, campaign, or both. The following configuration option has been added to support this feature:
  - outbound.callback-types
- Agents can change the phone number to be dialed in Outbound Campaign calls. This covers both the scenario where a different number than the one in the record must be dialed and the scenario where there is no number in the record. The following privilege has been added to enable this feature:
  - Outbound - Can Dial On New Number

### The following configuration option has been added to support this feature:

- expression.outbound-campaign-phone-number

- You can include Interaction Server and T-Server system properties keys in Case Data (Attached Data).
- You can configure the keyboard.shortcut.hamburger.open option to enable agents to open the Main Menu (Hamburger Menu) to access views such as 'My Workspace' and 'My History'.

## Workspace 8.5.114.08

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.114.08:

- Automatic Place selection using Place Groups is now supported to improve the management of Places by no longer tying a single Place to a single agent. This feature enables you to create a pool of Places that agents can select from whether they are connecting from a workstation, from home, or from a mobile. The Place Group selection feature works only with SIP Server. It is not supported by Workspace SIP Endpoint. The following configuration options have been added to support this feature:
  - login.available-place-groups
  - login.place-selection-type

### The following configuration options have been modified to support this feature:

- login.default-place

    - login.enable-place-completion
    - login.enable-same-agent-place
    - login.prompt-place
    - login.store-recent-place

- You can restrict outgoing email interactions by preventing agents from added or editing the To, Cc, and Bcc fields. The following configuration options have been added to support this feature:
    - email.outbound.editable-to-addresses
    - email.outbound.editable-cc-addresses
    - email.outbound.editable-bcc-addresses

## Workspace 8.5.113.11

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.113.11:

- Embedded images in outgoing email interactions. Agents can paste copied images at the insertion point in the outgoing email interaction view. The following privilege supports this feature:
    - E-Mail - Can Add Embedded Image In Outbound E-Mail
- Agents can forward emails to external resources as a new, in-line, quoted email. The previous Forward to External Resource feature has been renamed Forward as an Attachment.
- Enable or disable inserting TAB characters into outgoing email interactions by using the accessibility.visual-impairment-profile option. The following configuration option supports this feature:
    - email.inline-forward-prefix
    - email.inline-forward-queue
    - keyboard.shortcut.interaction.email.inline-forward

  ### The following privilege supports this feature:

    - E-Mail - Can In-line Forward To External Resource
- Agents are now notified if either party in a chat has timed out due to inactivity.

## Workspace 8.5.112.08

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.112.08:

- You can create custom field codes for Standard Response objects. The following configuration option supports this new feature:
    - standard-response.field.<CustomFieldCode>

- You can store agent profile information on a shared directory instead of in the Configuration layer. The following configuration options support this feature:
    - options.clean-up-former-record-location
    - options.record-location
- You can optimize the way that the most recently used Place is tracked. This feature is beneficial in environments where agents move from workstation to workstation or phone set to phone set. The following configuration option supports this new feature:
    - login.place-location-source
- You can configure how interaction duration information is collected and reported to the Genesys back-end by using the Duration in Focus feature. The following configuration option supports this feature:
    - reporting.case.report-case-in-focus-duration

## Workspace 8.5.111.21

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.111.21:

- For the Voice channel, you can configure Workspace to display the current hold time instead of the total call time when an agent puts a contact on hold; and, you can configure Workspace to display a hold time progress bar as part of the Hold icon. You can also configure Workspace to display the current after call work time instead of the total call time after the agent disconnects a call. The following configuration options support these new behaviors:
    - voice.hold-indicator-timer
    - voice.show-hold-duration
    - voice.show-post-call-duration
- Workspace now supports Genesys Mobile Server (GMS) Callback interactions. The Web Callback feature is being phased out.
    - Use the Callback privileges to enable this feature.
    - Use the Callback options to configure this feature.
- Workspace now supports Load Balancing Using Clusters.

## Workspace 8.5.110.13

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.110.13:

- You can configure agent accounts to enable agents to search/filter Workbins and Interaction Queues. This feature is supported by the following privileges:
    - Workbins - Can Search in Workbins
    - Interaction Management - Can Search In Interaction Queues

This feature is supported by the following configuration options:

  - workbin.<media-type>.<workbin-nickname>.auto-update
  - workbin.<media-type>.<workbin-nickname>.quick-search-attributes
  - workbin.<media-type>.<workbin-nickname>.max-results

- Workspace now supports Multimedia Message Service (MMS) messages that contain images sent in the following formats:
  - Bitmap (image/bmp)
  - GIF (image/gif)
  - JPEG (image/jpeg)
  - Portable Network Graphics (image/png)
  - TIFF (image/tiff)
  - ICO (image/vnd.microsoft.icon)

  This feature is available through the SMS channel. You configure this feature by using the following configuration option:

  - openmedia.bundle.sms

  This feature is supported by the following privilege:

  - SMS - Can Save Attached File

- Agents can mark interactions as Done from the Contact History, My History, and Interaction Search views.
- Agents can delete interactions from the Contact History, My History, and Interaction Search views.
- You can display agent names in the interactive notification for cross site internal calls by using the following option:
  - interaction.evaluate-real-party-for-agent.expression
- Team Communicator can be configured to display different metrics for the availability of Routing Points, Queues, and Interaction Queues. If the corresponding metric from Stat Server is a time, you can use the new `statistic-text` option to specify the format of the time information. You can specify a {0} field code anywhere in this string, and to add time formatting value to this field code, like {0:HH:mm:ss}, following Microsoft reference: https://msdn.microsoft.com/en-us/library/8kb3ddd4(v=vs.110).aspx. Previously, time information in Team Communicator was always displayed in seconds; however, this was inconvenient if the number of seconds was large. This feature is supported by the `statistic-text` configuration option in the following sections:
  - `routing-point-presence`
  - `queue-presence`
  - `interaction-queue-presence`
- Changes to the following configuration options now take effect immediately instead of when the application is started or restarted:
  - kpi.displayed-kpis

  - statistics.displayed-statistics
  - statistics.queues
  - statistics.routing-points

## Workspace 8.5.109.16

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.109.16:

- Stand-alone version of Workspace SIP Endpoint for Virtual Desktop Infrastructure environments. This feature is supported by the following configuration options:
  - sipendpoint.standalone.protocol
  - sipendpoint.standalone.port
  - sipendpoint.standalone.vdi-detection-model
  - sipendpoint.standalone.security-level
  - sipendpoint.standalone.certificate-search-value
  - sipendpoint.standalone.subject-criteria
  - sipendpoint.standalone.subject-matching-properties

  Enable the Standalone Workspace SIP Endpoint by removing the SIP Endpoint - Can Use Embedded SIP Endpoint privilege.

  Install the Standalone Workspace SIP Endpoint by using the Installing the Workspace SIP Endpoint Standalone Application procedure.
- You can add a display name for certain configuration layer objects. This feature enables you to name objects without relying on a local dictionary file. This feature makes localization and centralization more efficient. The following configuration options support the new `$<object-type>.AnnexValue$` key:
  - display-format.acd-queue.name
  - display-format.action-code.name
  - display-format.agent-group.name
  - display-format.business-attribute.name
  - display-format.interaction-queue.name
  - display-format.routing-point.name
  - display-format.skill.name
  - display-format.virtual-queue.name
  - display-format.workbin.name
- You can specify how agents who are part of Push Preview, Pull Preview, and Reschedule Preview outbound campaigns dial campaign calls: manually, immediately, or after a specified time. This feature is enabled by the following configuration option:
  - outbound.timed-preview-auto-dial

- You can enable agents to set the zoom of text editing fields, such as email, chat, and SMS, and transcript areas. This feature applies to the following views:
  - IM (text entry, transcript, and interaction data tooltip)
  - Chat (text entry, transcript, and interaction data tooltip)
  - Email (text entry and inbound email view)
  - SMS (text entry, transcript, and interaction data tooltip)
  - Interaction history (IM, Chat, Email, SMS)
  - Standard responses
  - Social media (text entry only)

  The following topics have been updated to include this feature:

  - Overriding Default Font and Icon Sizes
  - Enabling Accessibility Features

  The following configuration option was added to support this feature:

  - gui.editor-zoom-range
- The Prevent/Allow Listening feature has been modified slightly in the agent interface. The interface now informs agents when a party is suspended from a conference or reinstated to a conference. Conference party Action menu items have been renamed accordingly. This feature is controlled by the Voice - Can Suspend or Reinstate A Conference Party privilege.
- You can control which media Workspace tries to reconnect for active interactions after connection to Interaction Server is reestablished. The following configuration options have been added to support this feature:
  - eservices.session-restore-mediatype
  - eservices.session-restore-timeout
- Changes to the following two options are now taken into effect immediately instead of when the application is started or restarted:
  - gadget-statistics.displayed-call-center-statistics
  - gadget-statistics.displayed-kpis

## Workspace 8.5.108.11

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.108.11:

- The Chat typing feature has been enhanced to enable agents to see what a contact is typing on a web site chat form before the contact clicks **Send**. This feature is enabled by the following privilege:
  - Chat - Can Preview Customer Typing
- You can configure the Disposition tab in the interaction views to display dispositions as a hierarchical tree of folders and dispositions instead of a radio button list. Use the following option to retain the former radio button interface:

  - interaction.disposition.display-mode
- You can optimize the use of eServices licensing by using the following configuration option:
  - eservices.disconnect-on-logoff
- Business Continuity (Disaster Recovery) support has been extended to include StatServer.

## Workspace 8.5.106.19

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.106.19:

- You can configure Workspace for eServices Business Continuity. The following configuration options have been added to support this feature:
  - disaster-recovery.eservices-random-delay-range
  - disaster-recovery.eservices-site
  - warm-standby.retry-delay
  - warm-standby.reconnection-random-delay-range

  As well, some other Business Continuity (Disaster Recovery) options have been modified to support this feature.
- IPv6 Support
- You can use the interaction-bar.quick-access-auto-open.<media-type> configuration options to specify that when an agent accepts an interaction, it is displayed as collapsed to the Interaction Bar. This enables agents to view other content, such as custom or 3rd-party content in the Main View, without the pinned or floating interaction views opening in front of the content.
- The `string.expression` and `string.expression-instructions` options have been added to the string type for editable Case Data. It is used to validate the format for the string data type Key-Value Pairs.
- Screen Recording Client Authentication is added for users of Genesys Interaction Recording (GIR). You must have a login provided by Genesys to access the Genesys Interaction Recording documentation. This feature is supported by the following privilege:
  - Can Use Active Recording

  The following options have been added to configure the behavior of Screen Recording:
  - screen-recording.client.port: Specifies the port on which Screen Recording Client listens for credentials.
  - screen-recording.client.ping-interval: Specifies, in milliseconds, the interval between ping requests to Screen Recording Client.
  - screen-recording.client.max-attempts: : Specifies the maximum number of attempts made to establish communication with Screen Recording Client.
  - screen-recording.client.secure-connection: Specifies whether a secure connection is to be used for communication with Screen Recording Client.
  - screen-recording.htcc.uri: Specifies the URI of HTCC server. This URI is used as as the `Origin` header field for HTTP requests to SRC REST services.

- Several options in the Interaction Options section have been slightly modified.
- Several options in the Display Formats Options section have been slightly modified.

## Workspace 8.5.105.12

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.105.12:

- The mandatory ring before auto-answer feature enables you to configure the auto-answer functionality to display a timer that enables an agent to view case information before the interaction is automatically answered. This feature is configured by media type using the following new options:
  - chat.auto-answer.enable-reject
  - chat.auto-answer.timer
  - email.auto-answer.enable-reject
  - email.auto-answer.timer
  - outbound.push-preview.auto-answer.enable-reject
  - outbound.push-preview.auto-answer.timer
  - sms.auto-answer.enable-reject
  - sms.auto-answer.timer
  - voice.auto-answer.enable-reject
  - voice.auto-answer.timer
  - webcallback.auto-answer.enable-reject
  - webcallback.auto-answer.timer
  - <media-type>.auto-answer.enable-reject
  - <media-type>.auto-answer.timer
- You can specify by media type whether you want agents to be prompted when they send an email message, SMS, or Chat if there are misspelled words in the message by using the spellchecker.<media-type>.prompt-on-send configuration option.
- Agents can double-click to insert a standard response into an email message, SMS, Chat, and other text-based interactions.
- The contact.directory-enabled-modes option is added to enable you to specify which Contact Directory views can be displayed by the agent. Specifies which view(s) of the Contact Directory can be selected by an agent. Genesys recommends that the value is set to `ListView` in environments with a large number of contacts and, in particular, where contact segmentation is used.
- VMWare Horizon (View) 6 is now supported.

# Workspace 8.5.104.15

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.104.15:

- The Forward E-Mail feature has been modified to enable agents to forward email interactions to multiple targets, including **CC** (carbon copy) targets. Agents can also include information or instructions in a dedicated case data field of the Forward view. The following configuration options have been added to support this feature:
  - email.forward.enable-multiple-to-addresses
  - email.forward.enable-cc-addresses
  - email.forward.enable-instructions
- The Interaction Search feature expands on the Contact History/My History search capabilities to enable you to search for email and chat interactions without knowing which agent worked on them, when they were handled, or who the contact is. You must define the search attributes by using the `contact.history` options. The following configuration options have been modified or added to support this feature:
  - contact.all-interactions-default-time-filter-main
  - contact.all-interactions-displayed-columns
  - contact.all-interactions-quick-search-attributes
  - contact.date-search-types
  - contact.directory-permissions.<ContactAttributeName>
  - contact.history-advanced-default
  - contact.history-custom-attribute-values.<attribute-name>
  - contact.history-search-attribute-group.<group-name>
  - contact.history-search-attributes
  - contact.history-quick-search-attributes
  - contact.history.media-filters
  - contact.myhistory-displayed-columns
  - contact.myhistory-quick-search-attributes

    The following privilege is added to enable this feature:

  - Contact - Can Use Interaction Search
- The following configuration options have been added to support Chat Server ADDP:
  - chatserver.addp.local-timeout
  - chatserver.addp.remote-timeout
  - chatserver.addp.trace-mode
- The Active Recording Privileges have been renamed to the following:
  - Recording - Can Use MSML-based Recording

  - Recording - Can Monitor Call Recording
  - Recording - Can Control Call Recording

## Workspace 8.5.103.10

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.103.10:

- In SIP Server environments, you can control whether contacts are automatically taken off hold when an agent ends a consultation call, or whether agents must end the hold manually by using the voice.end-consultation-method option.
- You can specify whether it is mandatory for agents to assign a disposition code when they transfer or forward email interactions by using the interaction.disposition.email.mandatory-actions configuration option.
- You can specify that the After Call Work state is automatically changed to Ready when an agent clicks **Done** by using the voice.cancel-after-call-work-on-done option.
- You can specify whether the most recently used Username is stored locally in the user profile and is used to automatically populate the username field in the login view by using the login.store-username.

## Workspace 8.5.102.06

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.102.06:

- Management Framework 8.5 is now fully supported.
- eServices 8.5 is now fully supported.
- Kerberos User Authentication support.
  - ClickOnce and console deployment
  - Non-ClickOnce deployment
- You can define several formats for displaying queue, routing point and interaction queue presence in the Team Communicator. The following configuration options have been added to support this feature:
  - teamcommunicator.interaction-queue-presence-metrics
  - teamcommunicator.queue-presence-metrics
  - teamcommunicator.routing-point-presence-metrics

    The following options have also been added to the "presence" sections to allow to use a statistic metric of an hidden technical object like a Virtual Queue on behalf of a queue/routingpoint/interactionqueue actually presented in Team Communicator: object-ids, associated-statistic-type, and associated-object-ids. These are supported by the following sections:
  - interaction-queue-presence
  - queue-presence

  - routing-point-presence

- You can control the display size of fonts and icons in the Workspace views by using the gui.magnification-factor configuration option.
- To enable the standardization across all workstations of the Dates that are displayed in Case Information, the following new formats for the `Date` attribute type have been added: `date.time-format` and `date.utc-time-zone`. Refer to the **Editing Case Information** table in the **Displaying and Editing Case Information** section.

## Workspace 8.5.101.14

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.101.14:

- Workspace SIP Endpoint 8.5.0 now supports the `G729` and `H.264` video codecs. The following configuration options have been added to support this feature:
  - sipendpoint.codecs.g729/8000.fmtp
  - sipendpoint.codecs.h264.fmtp
- The following new options have been added to enable you to optimize bandwidth and Configuration Server load when Team Communicator is initialized:
  - general.configuration-agent-collection-loading-method
  - general.configuration-object-collection-cache-timeout
- E-mail printing capability has been extended to the following views:
  - My History
  - Contact History
  - Draft workbin
  - Search results
- Workspace now supports the customizing of display names for configuration objects. The following configuration options have been added to support this feature:
  - display-format.action-code.name
  - display-format.agent-group.name
  - display-format.business-attribute.name
  - display-format.skill.name
  - display-format.workbin.name

  The following configuration options have been modified to support this feature:

  - display-format.acd-queue.name
  - display-format.interaction-queue.name
  - display-format.routing-point.name

  - display-format.virtual-queue.name
- You can specify which contact attributes can be edited by agents. The following configuration option has been added to support this feature:
  - contact.editable-attributes
- You can specify whether agents can reject ClickOnce upgrades when they are presented at login time. Use the **Force the end-user to upgrade to the latest available version** option in the Client Configuration dialog box of the **Workspace Desktop Edition Deployment Manager** to control this feature — refer to 1a. Wizard: Deploy the Workspace downloadable ClickOnce package on your web server procedure.
- Accessibility has been enhanced. You can control whether Interaction Notification views receive the focus in environments that use screen reader applications. The following configuration options have been added to support this feature:
  - accessibility.focus-on-interaction-toast
  - accessibility.<media-type>.focus-on-interaction-toast
- The following configuration options have also been added or modified in this release:
  - sipendpoint.policy.endpoint.video_max_bitrate
  - sipendpoint.policy.device.audio_in_device
  - sipendpoint.policy.device.audio_out_device
  - sipendpoint.policy.device.capture_device

## Workspace 8.5.100.05

The following content has been added to the Workspace 8.5.1 Deployment Guide for Workspace Desktop Edition 8.5.100.05:

- Support for SIP Voicemail
  - Overview
  - Privileges
  - Configuration options:
    - voicemail.access-number
    - voicemail.notification-types
- Support for High Contrast Theme
  - High Contrast Workspace
  - Supporting configuration option:
    - gui.themes
  - Configuration of the High Contrast Theme: Enabling Accessibility Features

The following configuration options were also added or modified in this release:

- application.wiki-help-locale
- display-format.contact-name
- email.include-original-text-in-reply
- log.PSDK.SwitchPolicy
- outbound.call-result-is-mandatory

# Concepts And Features

Workspace features a unified user interface (UI) that empowers contact center employees to make their contact center truly dynamic by enabling them to respond in real time to real-time information from a wide variety of touch points and channels.

## Benefits

Workspace enhances internal communications, user performance, and quality. Workspace features a privilege-driven flow of information based on roles that you assign to your agents.

> **Important**
>
> The functionality that is assigned to agents through their defined role determines the footprint of the Interaction Workspace application that is downloaded to their workstation. Agents who have simple roles assigned to them do not require as much space for the application as agents whose roles contain many privileges.

## Main features

The following is a list of some of the main features of Workspace:

- Role-based application
- Open Framework for integration and extendability
- Support of plug-ins from many Genesys solutions.
- Advanced Multi-Channel Interaction interface
- Accessibility
- Active Call Recording
- Active Screen Recording
- Multiple Channels
  - Inbound Voice for both SIP and TDM
  - Outbound Campaigns
  - Callback/Web Callback
  - Email
    - Print preview
    - QA review
  - eServices

        - Inbound Video
        - Video Chat
        - Chat (including support for Chat High Availability (HA) and nicknames)

          [**Added:** 8.5.153.05]
        - SMS and MMS (including support for SMS High Availability (HA))

          [**Added:** 8.5.153.05]
        - Web Callback
        - Facebook (by an eServices plug-in)
        - Twitter (by an eServices plug-in)
        - RSS (by an eServices plug-in)
    - Voicemail
    - Workbin
    - Workitem
- Team Communicator
- Favorites and Corporate Favorites
- Internal Instant Messaging
- Standard Response Library and suggested responses (including filtering by language or other category)
- Agent and Contact-Center performance tracking
- Contact History Management
- Last-agent routing
- Broadcast Message viewing
- Disposition codes
- Customer context notifications
- Silent Monitoring, coaching, and barge-in (SIP and Chat only; for Team Lead agents or from a 3rd party Supervisor, including monitoring the current interaction)
    - Multi-site support
- Spelling check (including corporate dictionary support)
- Business Continuity (Disaster Recovery)
- Implementation of Language Packs to facilitate the customization of the User Interface in any non-right-reading language.
- Business Data Management and Case Data Management

## High-level architecture

Workspace incorporates Genesys interactions into a multi-modal paradigm that enables agents to invoke interactions within interactions to ensure a consistent customer experience.

Workspace is integrated with Genesys 8 components and applications, including Enterprise Services, Platform SDK, Management Framework, T-Servers, Universal Contact Server, Interaction Server, Configuration Server Data Base, Statistics Server for Reporting, SIP Server, and various specialized plug-in IPs. Workspace is dependent upon Genesys Administrator Extension. See Architecture for a more detailed description of the Workspace architecture.

## Time zones

Workspace displays all dates based on the time zone and the locale of the workstation where the user is logged in.

# Workspace Plug-ins

The following Workspace compatible plug-ins are available from Genesys:

- Genesys Predictive Engagement for Workspace: Genesys Predictive Engagement (formerly Altocloud) is a customer journey analytics platform that analyzes all kinds of customer journey behavior and data. It can be used to observe and analyze visitors on your digital properties, such as websites. Genesys Predictive Engagement can predict what it will take for visitors to achieve a desirable business outcome, and then acts to offer the most appropriate and effective channel to assist them in completing their journey.

> ### Important
>
> Genesys Predictive Engagement requires you to provision a Genesys Engage/Genesys Cloud Hybrid Integration to use this service. Refer to: Provisioning Genesys Engage Hybrid Integrations and Integrating Genesys Predictive Engagement into Genesys Engage on-premises.

- Workspace Plug-ins for LYNC / Skype: Genesys provides a plugin that adds functionality to Workspace Desktop Edition to tightly integrate it with the Skype for Business client on the agent desktop. Through the plugin, agents can handle voice, video, and instant messaging interactions handled by Skype for Business, in addition to accessing their Skype for Business contacts and seeing their presence status.
- Workspace Plug-ins for Social Media: Genesys provides a plugin that adds functionality to Workspace Desktop Edition, enabling agents to handle social media interactions.
- Workspace Plug-in Genesys Agent Scripting: Genesys Agent Scripting provides customized solutions to the agent desktop to guide an agent through each interaction by structuring, enriching, and optimizing agent conversation and workflow.
- Genesys Web Engagement Plug-in for Workspace: Genesys Web Engagement provides the ability to monitor, identify, and proactively engage web visitors in conversations that match business objectives.
- Genesys Co-browse Plug-in for Workspace: Genesys Co-browse provides the ability for an agent and the end customer to browse and navigate the same web page at the same time. In a Genesys Co-browse session, both the agent and the customer share the same instance of the screen, as opposed to a conventional screen sharing application, where one of the parties sees an image of the other party's browser instance.

Refer to Installing plug-ins for Workspace for information about installing Workspace compatible plug-ins.

# Workspace And Genesys 8

[**Modified:** 8.5.148.04]

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 |

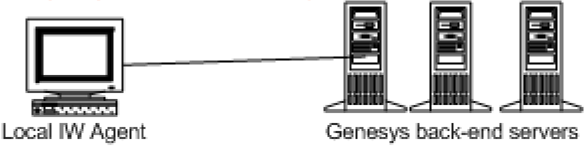
## Topology

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

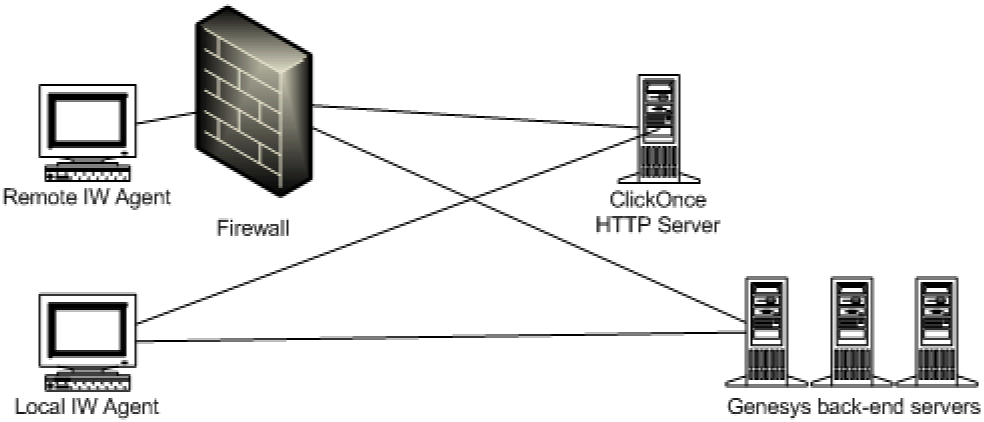
This section shows the key components of the Workspace network topology and indicates how Workspace is related to other Genesys components.

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.



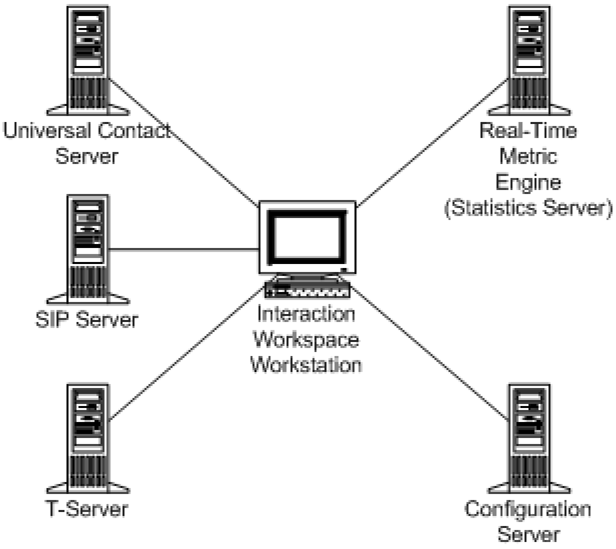
Standard deployment of Workspace with a ClickOnce server

## 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.


Universal Contact Server
Real-Time Metric Engine (Statistics Server)
SIP Server
Interaction Workspace Workstation
T-Server
Configuration Server

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:<br>• 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)<br>• ip_version=6,4 |
| SIP/RTP (for Workspace SIP Endpoint 8.5.1) | • interaction-workspace\sipendpoint.enable_ipv6=true<br>• 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:

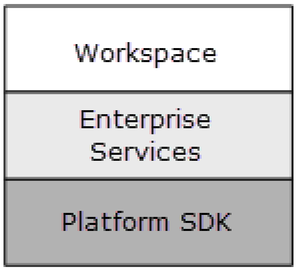
| Genesys back-end server | Protocol |
|---|---|
| Chat Server | TCP/TLS |
| Configuration Server | TCP/TLS |
| Genesys Mobile Services | HTTP/HTTPS |
| Interaction Server | TCP/TLS |
| Media Control Platform | RTP/RTCP (for Workspace SIP Endpoint or Genesys Softphone) |
| Statistics Server | TCP/TLS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

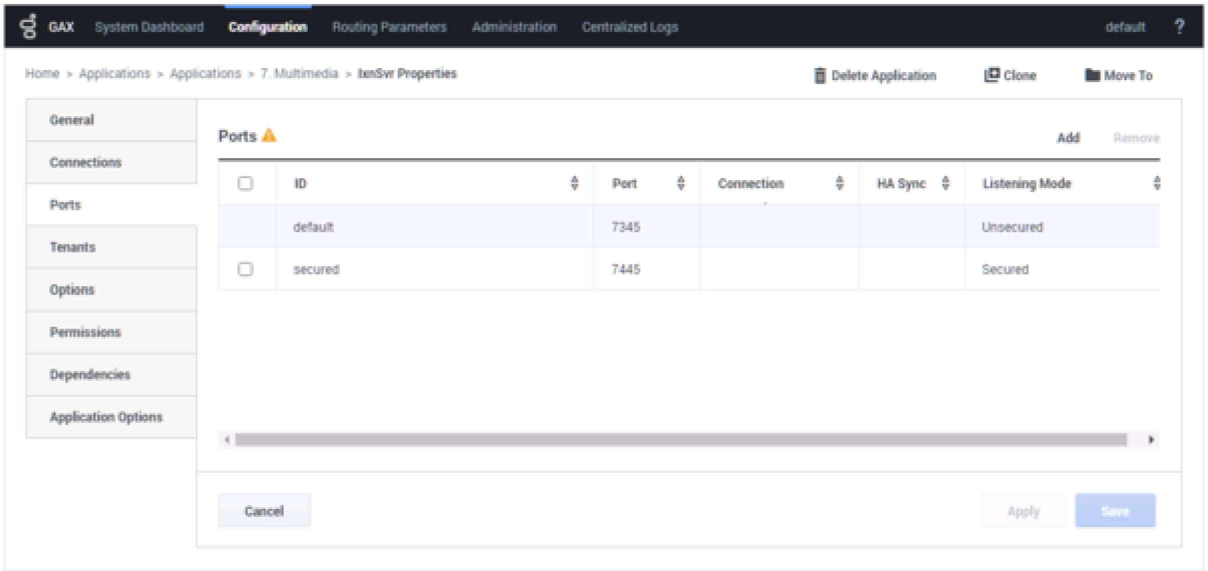
[**Added:** 8.5.148.04]

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.

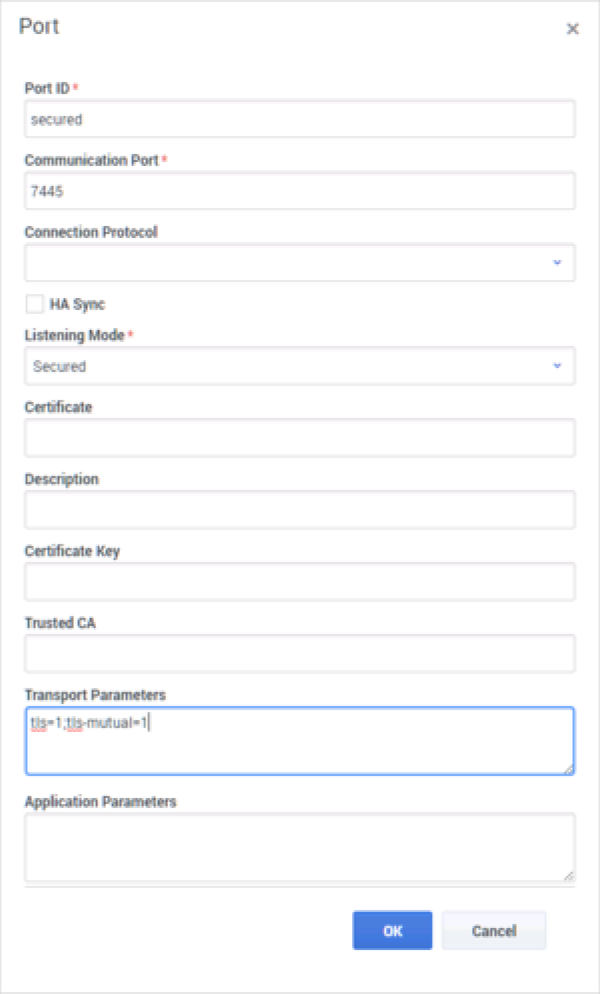
You can configure Mutual TLS only for secured ports. For Configuration Server, you must use upgrade port (refer to the following procedure). To configure Mutual TLS between Workspace and the connected backend servers, follow these steps for each connected backend server to enable Mutual TLS:

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



| | ID | Port | Connection | HA Sync | Listening Mode |
|---|---|---|---|---|---|
| | default | 7345 | | | Unsecured |
| □ | secured | 7445 | | | Secured |

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"



Port

Port ID * secured

Communication Port * 7445

Connection Protocol

□ HA Sync

Listening Mode * Secured

Certificate

Description

Certificate Key

Trusted CA

Transport Parameters tls=1;tls-mutual=1

Application Parameters

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.

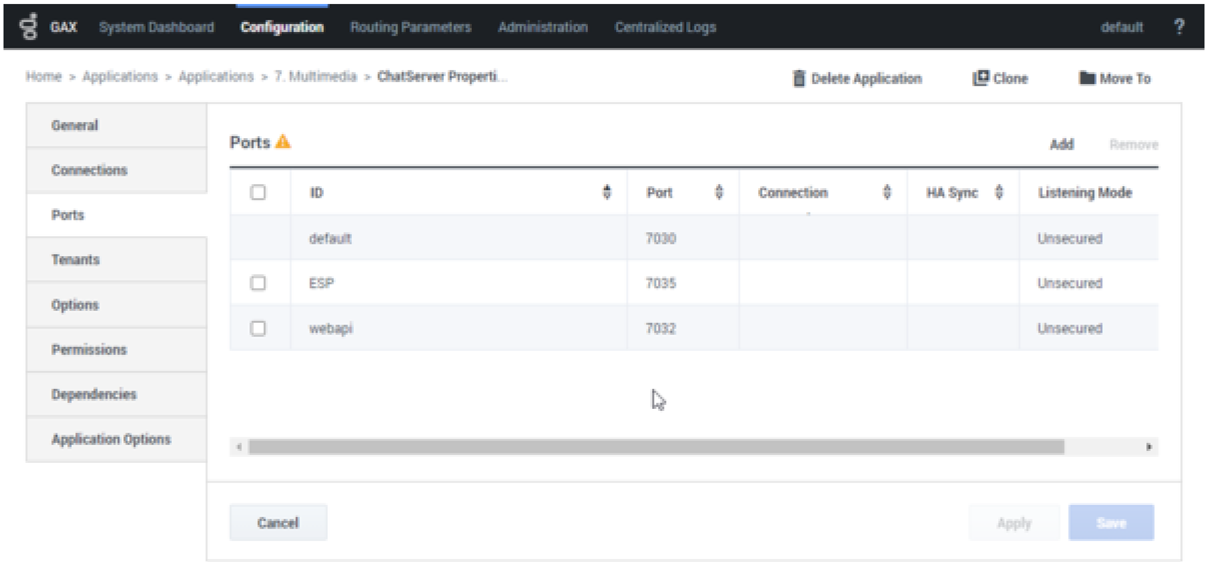
- First certificate selected for mutual TLS will be used for all mutual TLS connections before Workspace restart.

### 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.

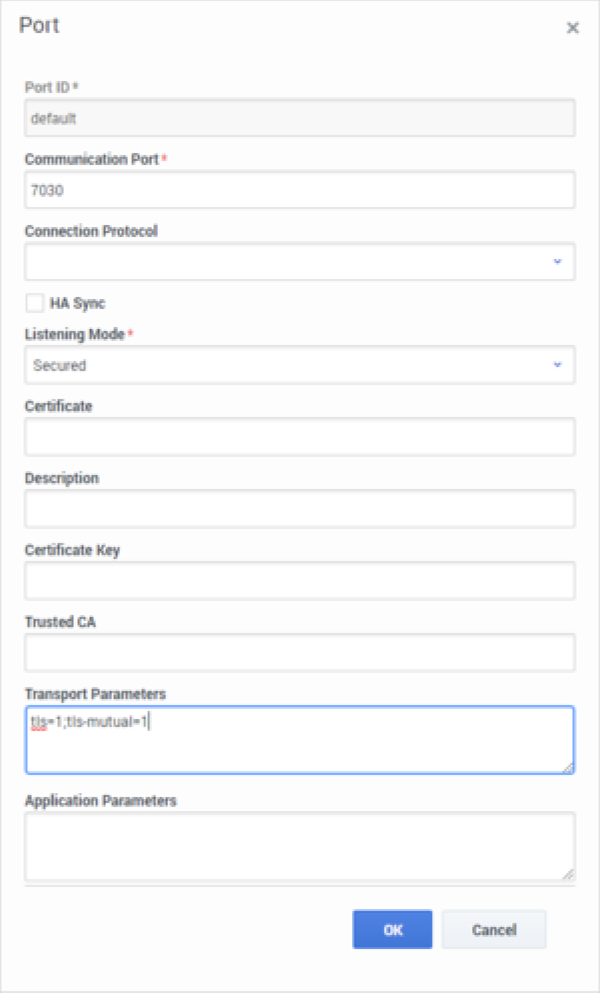
If the agent handles an interaction that is specific to Chat Server, Workspace connects to Chat Server. To configure Mutual TLS between Workspace and Chat Server, follow these steps:

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



| □ | ID | Port | Connection | HA Sync | Listening Mode |
|---|---|---|---|---|---|
| | default | 7030 | | | Unsecured |
| □ | ESP | 7035 | | | Unsecured |
| □ | webapi | 7032 | | | Unsecured |

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"



Port ID *: default

Communication Port *: 7030

Listening Mode *: Secured

Transport Parameters: 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*

# Role-based approach of Genesys 8

[**Modified:** 8.5.143.08]

Tip

You no longer have to use Genesys Administrator to create agent Roles for Workspace Desktop Edition. Workspace also supports the Role storage model of Genesys Administrator Extension 9.0.100.56 or higher. [**Added:** 8.5.143.08]

Genesys Administrator Extension is used to create Roles that contain a list of privileges. Roles are defined as the set of privileges that are either Allowed or Not Assigned. Each agent receives only what is needed to complete the privileges that relate to the Role of that agent; everything else is inaccessible. Genesys Administrator Extension enables the assignment of a Role to an Access Group or a Person.

Tip

Users have no default assigned Role. Roles have no default granted privileges.

Depending on the privileges that are granted to an agent, Workspace enables the following:

- Module activation — Triggering of module download from the ClickOnce server; this modifies the footprint of the agent desktop application.
- User Interface rendering — Includes the display of menu items, toolbar buttons, and views.

Refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group to create or modify a role and assign privileges to an agent or Agent Group.

## Role- and Privilege-Based Models

Workspace implements Role-Based Access Control (RBAC). RBAC enables administrators to limit agents to specific channels, interactions, and so on, based on their permissions.

Important

RBAC requires Configuration Server 8.0.2 or higher. RBAC requires Genesys Administrator 8.0.2 or higher, or Genesys Administrator Extension 9.0.100.56 or higher.

Workspace supports both the Genesys Administrator Role data storage model, introduced by Management Framework 8, and the Genesys Administrator Extension Role data storage model (as implemented in Genesys Engage cloud). The following are the general rules for Roles defined for Workspace:

- In one environment, you can define both Genesys Administrator and Genesys Administrator Extension Roles.
- Each Role is defined and stored either in a Genesys Administrator storage model or a Genesys Administrator Extension storage model.
- The Person (agent) object can be assigned to Roles defined by both Genesys Administrator and Genesys Administrator Extension.

The system administrator defines a Role for each agent. The Role has a series of privileges that are associated with it; in this way, agents do not have access to privileges or functionality that are outside their assigned Roles.

RBAC enhances system security by limiting agent access to the system. This is critical for protecting the system against accidental or intentional damage. Accidental damage can occur if an agent is accessing a part of the system that is outside of the area of responsibility of that agent.

RBAC enables you to update your system easily. If agents change responsibilities or new agents are added, you do not have to assign permissions to those agents based on their username. When you create or modify an agent, all that you have to do is set the Role of that agent; system access is determined automatically. As soon as the agent logs into the system, the identity of that agent determines access. Individual permissions do not have to be set for new or modified users.

To facilitate RBAC, Workspace is constructed as a collection of modules that encompass privileges or related privileges. RBAC selects only those modules that pertain to the Role of the agent and are necessary for the context of the functions that are accessible to the agent.

The security.disable-rbac configuration option in the `interaction-workspace` section determines whether agents have all privileges granted or whether the Role Based Access Control (RBAC) control system is used. You can set this option to `true` when you deploy the application in your testing lab to evaluate and test the application. Refer to Role Privileges for a list of all the privileges.

### Views (Modules and Groups of Privileges)

Modules are assembled into views. Each module, set of modules, or view is related to a privilege or set of privileges. Privileges are implemented by modules. In a ClickOnce environment; when an agent logs in to Workspace, modules are transferred to the client desktop. The modules that are transferred are dependent upon the Role that is assigned to the user with that login.

## Privileges implemented by Workspace

This section introduces the privileges that are implemented by Workspace. The privileges are grouped logically by action and access type:

- Voice actions
- Instant Messaging actions
- Statistics access

- Contact actions
- Team Communicator actions
- eServices actions
- Standard Response Favorites actions

### Voice actions

Voice action privileges enable a variety of capabilities, including the use of the Voice media, transfer, conference, disposition, answering, rejecting, and making calls.

### Instant Messaging actions

Instant Messaging (IM) actions enable agents to use the IM media for internal communication, and to make and release IM sessions.

### Statistics access

Statistics access privileges enable the viewing of Key Performance Indicators (KPIs) and contact center statistics by agents.

### Contact actions

Contact action privileges can be used to enable a wide variety of contact related privileges including marking done interactions, merging contacts and interactions, creating contacts, deleting contacts, and saving changes to contacts. Contact action privileges also enable access to Interaction Workspace features such as Contact history, information, directory, details, notepad, and case data.

### Team Communicator actions

Team Communicator privileges enable contacts to use the Team Communicator feature to contact internal targets, create and use favorites, and view recent contacts.

### eServices actions

eServices privileges for E-Mail, Chat, Video, Web Callback, Workitems, and Workbins. For more information on the privileges implemented by Workspace, refer to Workspace Functionality Overview.

### Standard Response Favorites actions

Standard Response Favorites privileges enable the agents to save a list of favorite responses from the SRL.

# Configuration and administration by using options and annexes

> Tip
>
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

Workspace privileges are assigned to users based on the role that is configured for them in the Configuration Layer. Workspace privileges are associated with modules. Under the terms of RBAC, agents must be configured to have access to Workspace modules. Later, agents may be granted the ability to set preferences that personalize the modules. As with the other Genesys 8 applications, Workspace is first set up and configured through the Genesys Administrator Extension interface. After the initial configuration, the settings of each Workspace module can be assigned hierarchically to:

1. An Application.
2. A Tenant.
3. An Agent Group.
4. A Person.

The option settings are applied to an agent upon login to Workspace in the following override order:

1. Default settings that are defined in the application code, which are overridden by:
2. Settings that are specified in the Application, which are overridden by:
3. Settings that are specified in the Tenant of the agent, which are overridden by:
4. Settings that are specified in the Agent Group(s) to which an agent belongs (**Note:** only Virtual Agent Groups defined with rules that are based on Skills are supported) — in cases in which an agent is a member of more than one group, Workspace considers the union of options that are set in each group; if an option is declared in two different groups, each of which has a different value, Workspace uses built-in rules to resolve the conflict (see Conflict Resolution for Configuration Options for information on how such conflicts are resolved), which are overridden by:
5. Settings that are specified in the Person object that corresponds to the agent.

You can override options only in the `interaction-workspace` section. Therefore, you must replicate the `interaction-workspace` section to the annex of the object level at which you want the override to occur (Tenant, Group, User, or Transaction).

### Other applicable object hierarchies

Some specific Workspace options can be defined in other objects and object hierarchies, such as:

Action Codes -- For example: Not Ready reason codes.

### Overriding options by using a Routing Strategy

A Routing Strategy can be used to override configuration options that you have defined by using the hierarchies that are described in Configuration And Administration By Using Options And Annexes.

Workspace uses Transaction Objects of type `object list`. You can attach a transaction name or list of transaction names to your strategy. The transaction names in the list should be separated by commas. Workspace reads the transaction objects at rendering time to override the static options.

Overriding options enables you to change the appearance of interactions based on a key-value pair that is defined in the annex of each listed transaction object. The attached data contains the name of the transaction object to be used for the interaction. Transaction objects are configured in Genesys Administrator Extension or Composer, by using the standard approach that is used for other object types in the hierarchy.

Use the interaction.override-option-key option to define the key in which the Transaction object(s) are to be listed in attached data. If you set an override value, Workspace will look for the transaction object that corresponds to the key-value pair.

Not all the options in the `interaction-workspace` section can be overridden by transaction objects. Refer to Section: interaction-workspace to determine which options support overriding by transaction objects. To apply this approach, you must replicate in the annex of the transaction object the structure that is used in the `interaction-workspace` section of the Workspace Application object. The option name must be the same key as in the Workspace Application object template.

## Conflict resolution for configuration options

In the hierarchy that is described in the previous sections, conflicts might occur during the resolution of option inheritance. Typically, an agent can be a member of more than one Agent Group. If group options conflict with one another, Workspace considers the conflict to be an administration error. An arbitrary resolution is applied.

### Single value option types

The arbitrary conflict resolution for single-value options proceeds as follows:

1. Agent Groups are sorted into ascending order by the name of the Agent Group.
2. The values of the options for each section are compared.
3. If there is a conflict, the value that is set for the agent corresponds to the value that is set for the group name that comes first in the sort order. For example, values that are set for options in the "Pre-Sales" group take precedence over values that are set for options in the "Support" group.

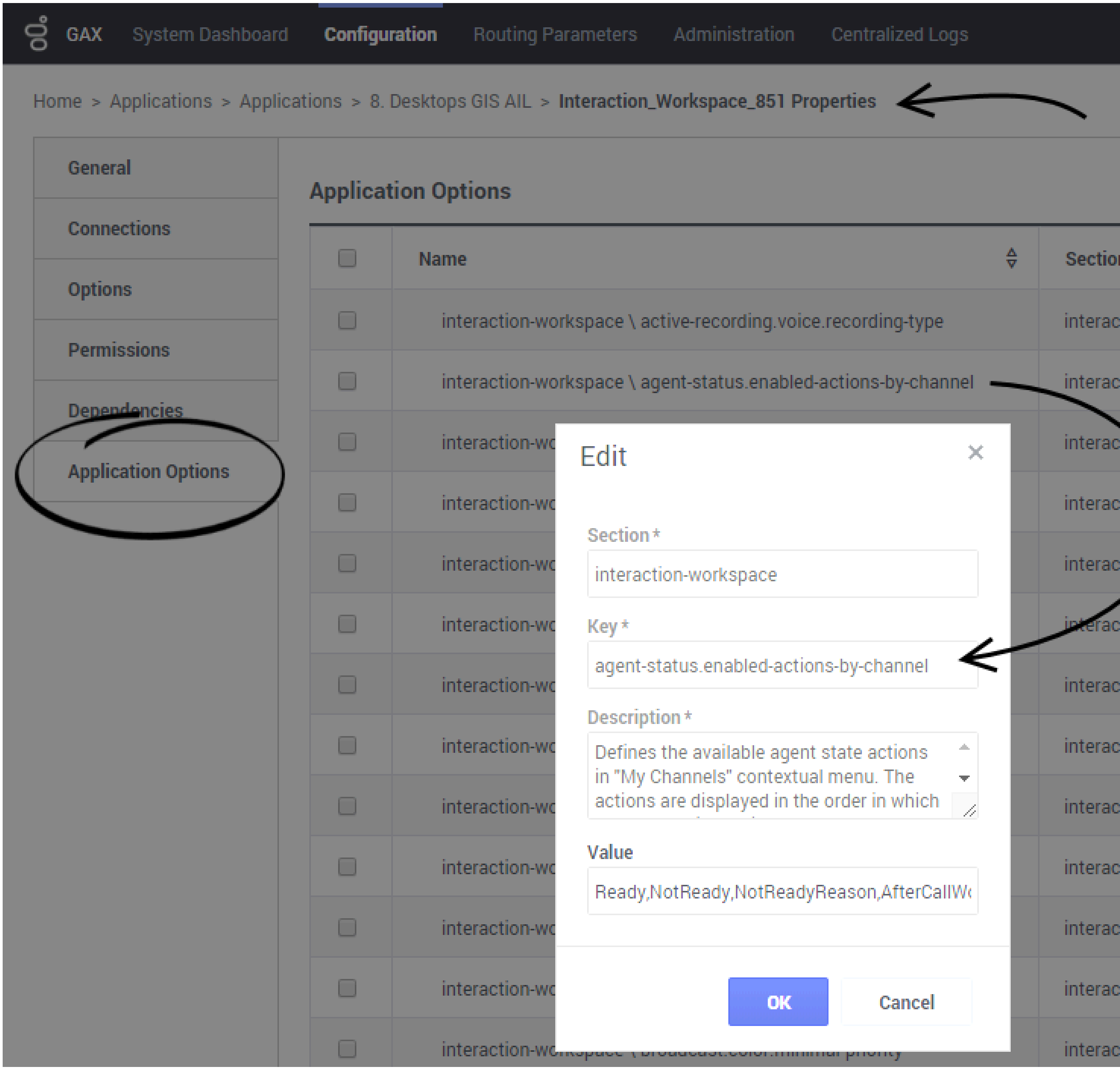
### Transaction object conflicts

If there is a conflict between transaction objects as specified by the list of override options, the first value that is set in a transaction, starting from the beginning of the list, is taken into account. All the subsequent values that are specified for the same option are ignored.

## Using options in Genesys 8 and Workspace

Each object in Genesys Framework, including agents and the Workspace application, can be configured using Genesys Administrator Extension. Refer to *Genesys Administrator Extension Help* and *Genesys Administrator Extension Deployment Guide* for detailed information on how to use Genesys Administrator Extension and Management Framework to set up your contact center and configure objects such as agents, groups, privileges, and applications.

All configuration options in Genesys 8 are divided first into sections. Sections are groups of related configuration options. Within a section, each option is named by its functional area, and then by its name or specific function. The Figure - **Examples of Workspace sections and configuration options, derived from metadata, displayed in the Genesys Administrator Extension interface** shows examples of Workspace options in the `KPIs` and `interaction-workspace` sections, such as `agent-status.not-ready-reasons`. The functional area is `agent-status`, and the option name is `not-ready-reasons`.


GAX
System Dashboard
Configuration
Routing Parameters
Administration
Centralized Logs
Home > Applications > Applications > 8. Desktops GIS AIL > Interaction_Workspace_851 Properties
General
Connections
Options
Permissions
Dependencies
Application Options
Application Options
Name
Sectio
interaction-workspace \ active-recording.voice.recording-type
interaction-workspace \ agent-status.enabled-actions-by-channel
interaction-wo
interac
Edit
OK
Cancel

Section *

interaction-workspace

Key *

agent-status.enabled-actions-by-channel

Description *

Defines the available agent state actions in "My Channels" contextual menu. The actions are displayed in the order in which

Value

Ready,NotReady,NotReadyReason,AfterCallW

Examples of Workspace sections and configuration options, derived from metadata, displayed in the Genesys Administrator Extens

## Option-value yypes

Option values are of the following types:

- String -- Open content or a comma-separated list of valid string or numeric values; some lists may have an open number of members to be determined by the user.
- Numeric -- Specific values or ranges of values.
- Boolean -- Either `true` or `false`.

Workspace Configuration Options Reference contains a list of all the Workspace options. It includes descriptions of their type and use. Refer also to Deploying Workspace, when you are planning your implementation of Workspace.

## Effect of privileges and hierarchical options on the behavior of Workspace

The behavior of Workspace is controlled by a compilation of settings in various systems and components of the Genesys 8 suite. The behavior is controlled by the following components:

- Privileges are assigned to logged-in agents through the Genesys RBAC security system (refer to Role- and Privilege-Based Models).
- Option and Annex settings that are defined in the applicable objects of the configuration layer.

Privileges are part of the security of the Genesys 8 suite; therefore, they have a higher priority than application and user settings. It is important to note that the options that are defined in the configuration layer and the routing strategy will never override any privilege management.

Under this hierarchy of control, options act only on the feature set that is permitted by the privilege that is specified for a given role. For example, a graphical module is configured to be visible by the application settings; however, none of the privileges that are implemented by this module are granted to the agent; therefore the module is not visible for this agent.

## Effects of configuration options and privileges on performance

This content had been moved here.

# Configuring the appearance and content of the user interface

Many of the Workspace views can be configured to display certain elements depending on the context—for example:

- Case data key-value pairs
- The values that are displayed for a Case History
- The title of the Main Toolbar
- The party identifier in Voice Media view
- The information that is displayed in the Preview window

There are three ways to specify the appearance and functionality of Workspace: Administration, Personalization, and Customization.

## Administration

Administration is configuration that is performed by system administrators. It managed through Genesys Administrator Extension by setting configuration options on the Workspace Application object. Administration settings are stored in the Genesys Configuration Layer.

## Views

The View options enable you to configure the sorting order and the default tab selection of tabbed views within each window.

The sort order can be customized by using the `views.<RegionName>.order` options.

The default tab selection can be configured by using the `views.<RegionName>.activate-order` options. The first in the list, if present, is selected by default. If the first in the list is absent, the second in the list is presented by default, and so on. Both options support out-of-the-box view names and names of custom views added to tab areas.

For custom views, use the `ViewName` string in the option; this is the string that is passed as the `ViewName` in the view activator. For the details about how to do this, refer to the Workspace Developer's Guide.

# Personalization

[**Modified:** 8.5.112.08]

Workspace is personalized at the user level by the setting of Personal Preferences. Personalization data are stored in the agent annex, in the personal-data directory on the local workstation (as specified by the options.record-option-locally-only option), or on a common working directory (as specified by the options.record-location option).

For more information on setting preferences, see *Workspace User's Guide* and *Workspace Context-Sensitive Help* (which is available by clicking the Help icon in the Workspace Main Window, or, with the Workspace Main Window open, by pressing F1 on your keyboard).

Agents have control over the display location of various Workspace Windows, as well as the arrangement and appearance of text and fields within the display.

## Keyboard shortcuts

You can configure keyboard shortcuts that control many different features of Workspace. Refer to the keyboard shortcut configuration option reference for a complete list of all configurable keyboard shortcuts.

> ### Important
>
> Whenever the rich text editor is used, for example to edit an outbound email interaction, it is possible that there will be a conflict between shortcuts that you have configured by using the Workspace configuration options and the shortcuts of the Rich Text Editor interface. A list of the default shortcuts of the Rich Text Editor are available on this Microsoft Web Page. Scroll down to the table in the **Remarks** section. Genesys recommends that you do not use any of the keyboard shortcuts that are already in use by the Rich Text Editor.

Workspace also supports accessibility through keyboard navigation.

# Customization

Customization is accomplished through development. Workspace features an open framework that enables developers to add value and extend the capabilities of the application. Workspace employs a modular design that enables you to expand and integrate your application by using multiple data sources and systems. Workspace enables you to customize views and create or customize extensions. For more information on extending Workspace, see the Workspace Developer's Guide and .NET API Reference and the Workspace 8.5 Extension Examples.

# Customization and Rebranding

Workspace can be customized through development. Refer to the Workspace Developer's Guide and .NET API Reference and the Workspace 8.5 Extension Examples for more information.

To customize the Workspace, you must install the Workspace Developer's Kit. For more, information see the Procedure: Installing Workspace Customization on the Windows operating system.

> **Important**
>
> Usage of Enterprise Services that is provided with this release of Workspace is supported only for the purpose of Workspace customization.

Workspace 8.5.0 and higher enables you to completely customize the color (theme), logo (branding), images, and icons of the user interface. Refer to Best Practices for Views for information about this feature.

# Preparing to deploy Workspace

This topic provides an overview of the deployment procedures for Workspace and discusses the prerequisites and other items that should be considered prior to deployment.

This topic contains the following sections:

- Migrating from Interaction Workspace 8.1 to Workspace 8.5
- Planning Your Deployment
- Deployment Overview
- ClickOnce Deployment
- Non-ClickOnce Deployment
- Configuring System-Access Permissions

# Migrating from Workspace 8.1 to 8.5

Migrating from Interaction Workspace 8.1 to Workspace Desktop Edition 8.5 is a simple and straightforward task. It is as simple as when you initially deployed and intalled Workspace.

Refer to the *Genesys Migration Guide* for the complete procedure.

# Planning Your Deployment

[**Modified:** 8.5.102.06, 8.5.141.04]

Before you deploy Workspace, you should take time to define your needs in terms of load, bandwidth, scale, the type of network that you have or want to develop, the number of resources you plan to manage, and the type of deployment that you want:

- ClickOnce
- Non-ClickOnce

## Defining your needs

This section provides items that you should consider when you are planning your deployment.

### Load, IIS vs. Apache

Workspace is designed to be equally compatible with Microsoft Internet Information Services (IIS) or Apache web servers. Your choice depends on the server-side operating system and HTTP server that you are running. Refer to the following system guides for details on compatibility and system requirements:

- *Hardware Sizing*
- *Genesys Interoperability Guide*
- *Genesys Supported Operating Environment Reference Manual*

### Type of network

Refer to the following system guides for details on compatibility and system requirements:

- *Hardware Sizing*
- *Genesys Interoperability Guide*
- *Genesys Supported Operating Environment Reference Manual*

### Single Sign-On (SSO)

[**Added:** 8.5.102.06]

Workspace supports Single Sign-On authentication by using Kerberos User Authentication. This feature must be configured prior to deployment.

## Choosing between a ClickOnce deployment and a Non-ClickOnce deployment

**ClickOnce** A ClickOnce deployment of Workspace automatically handles software updates as you make them available in your environment. If you do not have the ability to push applications, updates, and configurations to your agents, you might want to take advantage of a managed services deployment approach in your environment by using ClickOnce.

**Non-ClickOnce** In a Standard Deployment, you must install the Workspace application on each client workstation. In this scenario, you must push software updates to each workstation in your environment. Refer to the following sections for information about different deployment scenarios:

- Deployment Overview
- ClickOnce Deployment
- Non-ClickOnce Deployment

## Memory usage

This Table represents the Memory Usage range of Interaction Workspace. Minimum value is the out of the box version using voice only interactions Maximum value is the out of the box version using multimedia interactions

| OS Type | Memory used |
|---|---|
| x86 (32-bits) | 180 - 280 MB |
| x64 (64-bits) | 200 - 300 MB |

Interaction Workspace can use more memory if deployed with click-once on compatibility mode with 8.1.2. This mode runs Interaction Workspace in 64-bits native mode and can use up to 450 MB.

If you are using Workspace SIP Endpoint, an additional 60 MB are used.

## Monitor resolution

The minimum supported resolution is 1024 x 768 at 100% appearance display factor.

# Effects of configuration options and privileges on performance

These table list the effects that some configuration options and privileges might have on network bandwidth and also the performance of Configuration Server and Configuration Server proxies.

**Summary of the effects of Workspace options and privileges on network bandwidth**

| Option/Privilege | Default Value | Values that might affect system network bandwidth | Functional impact of using different values |
|---|---|---|---|
| Workbins - Can Use My Team Workbins | Unassigned | Assigned<br>During supervisor/Team Lead | No Team Workbin Supervision |

| Option/Privilege | Default Value | Values that might affect system network bandwidth | Functional impact of using different values |
|---|---|---|---|
| | | login, the Workbin module loads the current state of each of the workbins of the agents on the supervisor's team to provide the supervisor with an overview of the content of each workbin.<br>This action generates a set of requests to Interation Server. The bandwidth that is consumed by those requests is proportional to the following variables:<br>• the number of monitored agents<br>• the number of workbins assigned the supervisor<br>• the number of interactions in each workbin<br>• the size of the interaction properties in each interaction (depends on the Business Process design | |
| teamcommunicator.list-filter-showing | Agent | Agent<br>Affected instance: Configuration Server (Proxy) | Target types are not displayed to agents |
| login.enable-place-completion | true | true: Workspace loads all the Places that are visible to the logged-in agent immediately to enable the process of Place. This might be a large number of Places in a large scale environment.<br>Affected instance: Configuration Server (Proxy) | false: agents must enter their Place name manually and the verification is performed after the Place is submitted. If a default place is assigned to agents, this issue is mitigated. |
| teamcommunicator.load-at-startup | true | true: all configured object lists for team communicator are loaded during agent login and added to the index. | false: all configured object lists for team communicator are loaded at the first time that the Team Communicator is used. |

| Option/Privilege | Default Value | Values that might affect system network bandwidth | Functional impact of using different values |
|---|---|---|---|
| | | Affected instance: Configuration Server (Proxy) | |
| general.configuration-object-collection-cache-timeout | 0 | 0: No local cache of the list of objects is maintained; therefore, every time that the Team Communicator is initialized, the list of objects is requested from Configuration Server. | Any positive integer: Specifies the number of hours between requests for objects from Configuration Server, reducing the number of requests made to Configuration Server. |
| general.configuration-agent-collection-loading-method | read-objects | read-objects: This is the legacy agent-retrieval method. This method returns the list of agents according to the "read" permission of the current agent. For each retrieved agent this method returns the full agent data from Configuration Server, including annex structure, in an uncompressed format. The bandwidth consumed can be much larger than the other retrieval methods.<br>When an agent logs in to Workspace, several collections of configuration objects are loaded from Configuration Server or Configuration Server Proxy to build a Lucene index which enables instant quick search in Team Communicator. Depending on the user profile, this mechanism triggers the download of different types of objects, such as: agents, DNs (Routing Point, Queues), Scripts (Interaction Queue, Workbins), Agent Groups, and/or Skills.<br>In large scale environments where Workspace is configured to enable searching of agents in Team Communicator, Workspace might cause a large load on Configuration Server/Configuration Server Proxy, and on the network. This is particularly true of massive | brief-info: For each retrieved agent, this method returns only a subset of the agent data. This can result in significant network bandwidth optimization, as well as a decrease of the load on Configuration Server.<br>The larger the contact center, the larger the size of the Person collection. Each person object returned by Configuration Server Proxy can be a large data set that contains annex KVCollection where Workspace can store the agent profile and where other custom business applications can also store data. This can result in several megabytes of download for each agent login. |

| Option/Privilege | Default Value | Values that might affect system network bandwidth | Functional impact of using different values |
|---|---|---|---|
| | | concurrent logins, such as at the beginning of a shift or after an infrastructure incident. | |

**Summary of Interaction Workspace options and privileges that can affect Configuration Server (or CS Proxies)**

| Option/Privilege | Default Value | Values that can affect Configuration Server (or CS Proxies) | Functional impact of using different values |
|---|---|---|---|
| teamcommunicator.person-cache-for-favorites-recents-enabled | false | false (default): represents the legacy behavior where the preparation of Favorites and Recents can generate some duplicated requests to Configuration Server. | true: optimizes the usage of local cache when loading Recents and Favorites.<br>The Team Communicator user experience during data loading can be slightly different when this option is set to 'true'. |
| options.record-option-locally-only | false | false and the options.record-location option is absent or left empty: the agent profile is stored in the annex of the corresponding Person object when an agent logs out of the application. Write requests are transmitted by Configuration Server Proxies back to the central Configuration Server and then the Central Configuration Server notifies all proxy instances the update.<br>Affected instance: central Configuration Server and Configuration Server Proxies. | false and options.record-location set to a valid shared directory: there is no functional impact. Refer to Storing the agent profile on a controlled shared host.<br>true: Unless you are using the Windows Roaming Profile approach as part of your IT policy, the personal settings do not follow an agent who is roaming or hot seating. |
| general.configuration-update-notification | All | All or <empty>: Workspace subscribes for notifications about all object types that are read. | None: no notification at all. Any config update is taken into account at next login.<br>ThisApplication, ThisAgent: |

| Option/Privilege | Default Value | Values that can affect Configuration Server (or CS Proxies) | Functional impact of using different values |
|---|---|---|---|
| | | The Agent option might also generate a lot of notifications, depending on Configuration Server operations.<br>Affected instance: Configuration Server (Proxy) | Workspace is informed about modifications to the configuration of the current agent or current Application. Any other changes are taken into account at the next login. |
| teamcommunicator.list-filter-showing | Agent | Agent<br>Affected instance: Configuration Server (Proxy) | Target types are not presented to agent |
| login.enable-place-completion | true | true: Workspace loads all the Places that are visible to the logged-in agent immediately to enable the process of Place. This might be a large number of Places in a large scale environment.<br>Affected instance: Configuration Server (Proxy) | false: agents must enter their Place name manually and the verification is performed after the Place is submitted. If a default place is assigned to agents, this issue is mitigated. |
| • interaction.evaluate-real-party-for-agent<br>• display-format.agent-name | true | true: Workspace accesses Configuration Server and Stat Server before an interactive notification is displayed, to retrieve the display name of internal agents or supervisors who are engaged. The generated load on Config Server Proxy is not large, but it is proportional to the flow of interactions. Use the interaction.evaluate-real-party-for-agent.expression option to use a regular expression to display an agent's name instead of the agent's DN.<br>Affected instance: Workspace client | false: the internal voice interaction parties are displayed as phone numbers instead of a display name. |
| teamcommunicator.load-at-startup | true | true: all lists of configured objects for Team Communicator are loaded at login time and | false: all lists of configured objects for Team Communicator are loaded the first time |

| Option/Privilege | Default Value | Values that can affect Configuration Server (or CS Proxies) | Functional impact of using different values |
|---|---|---|---|
| | | added to the index, which can affect the system in a scenario where there is massively concurrent agent login operations.<br>Affected instance: Configuration Server (Proxy) | that Team Communicator is used, which might make the first activation of Team Communicator slower. |
| - interaction.override-option-key<br>- interaction.disposition.value-business-attribute<br>- interaction.case-data.format-business-attribute | empty | Business Attributes and Transaction objects for Dispositions and Case Data are always loaded the first time that an interaction requiring them is received by an agent. They are then cached for future use. The more possible values that exist, the more accesses are required during interaction notification. The generated load is not large, but in case of slow response time, there might be a delay before the interactive notification is displayed.<br>Affected instance: Workspace client | The general.configuration-business-attribute-cache-preload and general.configuration-business-attribute-folder-cache-preload options enable you to cache a list of Business Attributes up front to avoid a slow response accessing the Business Attributes in scenarios where Config Server has difficulties answering in a timely manner. [**Modified:** 8.5.141.04] |

# Deployment overview

Workspace can be deployed in one of three ways, depending on whether you want a ClickOnce or a non-ClickOnce deployment. Optionally, you can choose to install the developer package to customize and extend the capabilities of Workspace. Refer to Table - **Workspace Install Mode Deployment Packages** for the list and description of items that are installed by the Workspace Deployment Application.

**Workspace Install Mode Deployment Packages**

| Package name | Purpose | Folder contents |
|---|---|---|
| Prepare a ClickOnce package | Enables IT and administrators to install the Workspace ClickOnce package on a WebServer. | The Workspace folder contains the following folders or files:<br>• `Workspace`: Workspace application<br>• `WorkspaceDeploymentManager`: Deployment Manager application<br>• `WebPublication`: `publish.htm` (bootstrap for client side) and `setup.exe` (prerequisites) |
| Install Workspace Developer Toolkit | Intended for developers, testers, or those who are demonstrating the application. It contains all the deliverables, including the API references, Workspace, Deployment Manager, and Samples. | The destination folder contains the following folders or files:<br>• `Bin`: List of assemblies (DLLs) available for customization of Workspace (API)<br>• `Doc`: API Reference documentation<br>• `Workspace`: Workspace application<br>• `WorkspaceDeploymentManager`: Deployment Manager application<br>• `WebPublication`: `publish.htm` (bootstrap for client side) and `setup.exe` (prerequisites)<br>• `Samples`: Samples of extensions for developers |
| Install Workspace application | Intended for agents, testers, or those who are demonstrating the application. It contains only the agent application. | The destination folder contains the following folder: |

| Package name | Purpose | Folder contents |
|---|---|---|
| | | • `Workspace`: Workspace application. |

## ClickOnce deployment

ClickOnce enables a safe and secure workflow that enables agents to be authenticated and then granted access only to specific privileges. Initially, agents are given a URL (through email, a corporate portal, or a desktop shortcut) that links to the ClickOnce server. When they navigate to the server, the Workspace application is downloaded to their workstation. The application automatically starts, and agents are prompted to authenticate through the login window. When upgrades are made available, they are automatically delivered to agents upon login.

The basic steps for a ClickOnce deployment are as follows:

1. Perform the Procedure: Installing Workspace Deployment Package on the Windows operating system, which guides you through the steps for installing Workspace on your Windows web server from the Workspace CD/DVD.
2. Deploy the ClickOnce package on your web server by using the following Procedure: Deploying the Workspace downloadable package (ClickOnce) on your web server.
3. Start the application bootstrap to install, upgrade, or start the application.
4. Test the client application by using the following Procedure: Configuration verification: Testing the client.

## Non-ClickOnce deployment

You can install Workspace on a workstation without a ClickOnce deployment. This installation includes only the agent application. This installation option is used mainly to test Workspace on your system, not for enterprise-wide deployment.

The basic steps for a Non-ClickOnce deployment are as follows:

1. Perform the Procedure: Installing the Workspace application on a client desktop, which guides you through the steps for installing Workspace on an end-user desktop from the Workspace CD/DVD.
2. Start the application.
3. Test the client application by using the following Procedure: Configuration verification: Testing the client.

(Optional) To use Kerberos Single Sign-on (SSO):

1. Install Workspace by using the basic Non-ClickOnce above.
2. Modify the Configuration Server host, port, and application name parameters in the `interactionworkspace.exe.config` property file to conform with your system. This file is in the Workspace directory on the Workspace CD/DVD.

   Workspace requires that you specify the unique Service Principal Name (SPN) that is used in each Configuration Server and Configuration Server Proxy that will handle SSO requests from UI applications. Edit the `login.kerberos.service-principal-name` option in the `interactionworkspace.exe.config` property file to add the following line:

```
<appSettings>
  ...
  <add key="login.kerberos.service-principal-name" value="<SPN Name>"/>
  <add key="login.url" value="tcp://<host><port>/AppName" />
  <add key="login.connections.parameters.isenable" value="false" />
  ...
 </appSettings>
```

3. Add the customization resources that are required for your final installation.
4. Prepare your final package by using the updated file set.
5. Push the package to the agent workstations by using your desktop technology.

### Customization package deployment

You can install the Workspace application, API references, Deployment Manager, and Samples on a development workstation as follows: Perform the Procedure: Installing Workspace Customization on the Windows operating system, which guides you through the steps for installing Workspace Customization on a development workstation from the Workspace CD/DVD.

## ClickOnce deployment principles

ClickOnce provides a smooth experience for both the user and the network administrator. The user launches the application by using either a URL or a desktop icon. The URL can be provided to agents by email, a corporate portal, a desktop shortcut, or other means. This simple method enables you to install the Workspace application on every workstation easily.

When an agent accesses the URL the Interaction Workspace application is downloaded to the agent's workstation; it automatically starts and the login window is displayed.

For subsequent application starts, the agent can reuse the initial URL or execute the application through a desktop icon or through the `Start` menu.

If a hot fix or update is required or made available on the server, Workspace automatically upgrades the next time that the agent starts the application without you having to push-out a fix or update to every user.

> **Important**
>
> During deployment, you can specify whether agents can reject the Workspace upgrade.

ClickOnce enables you to deploy a security-enabled centralized WebService. Microsoft ClickOnce deployment technology that simplifies the privilege of publishing Windows-based applications to a web server or other network file share.

ClickOnce eliminates the need to reinstall the entire application whenever updates occur. Updates are provided automatically when an agent logs in. Only those portions of the application that have changed are downloaded to the client.

ClickOnce applications are entirely self-contained, they do not rely on shared resources. This means that you can update other resources without any impact on Interaction Workspace, or you can update Workspace without breaking other applications.

Another advantage of ClickOnce is that administrative permissions are not required for the update to be installed. The update is installed automatically from the server when an authorized client logs in.

## Scenarios: ClickOnce principles

The following three scenarios demonstrate the utility of the ClickOnce approach to application and system security management:

- Initial installation
- Application patch
- Update of agent privilege permissions

The application patch and permission-update scenarios can occur simultaneously.

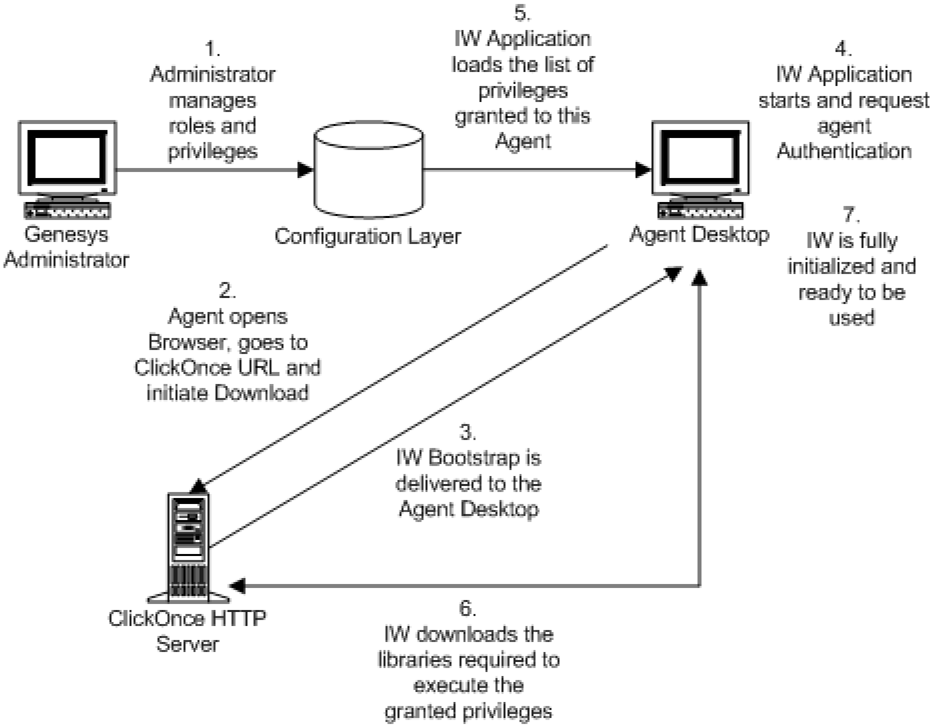
### Initial installation

For the initial installation onto the client workstation, the following prerequisites must be met:

- The Workspace application must be installed as a ClickOnce package on the HTTP Server that enables ClickOnce.
- Microsoft .NET Framework 4.5 must be installed on the client workstation.

The Figure - **Initial ClickOnce installation of the Workspace (IW) application** shows the steps in a typical first installation of Workspace in a ClickOnce environment:

1. The administrator manages the roles and privileges of the contact center agent by using Genesys Administrator Extension and stores the configurations in the Configuration Layer. Through email, the corporate portal, or other notification, agents are provided with the application URL.
2. Agents use the URL to go to the ClickOnce HTTP Server and initiate the download.
3. The Workspace Application Bootstrap is delivered to the agent workstation; then the Workspace application launches and agents are prompted for authentication information. **Note:** Agents provide their credentials and are authenticated on the network.
4. The Workspace application starts and requests agent authentication.
5. The Workspace application loads the list of privileges that are granted to each agent, based on agent authentication.
6. The Workspace application then downloads the libraries that are required to execute the granted privileges.
7. Workspace is fully initialized and ready to be used.


1.
Administrator manages roles and privileges
Genesys Administrator
Configuration Layer
5.
IW Application loads the list of privileges granted to this Agent
4.
IW Application starts and request agent Authentication
Agent Desktop
7.
IW is fully initialized and ready to be used
2.
Agent opens Browser, goes to ClickOnce URL and initiate Download
3.
IW Bootstrap is delivered to the Agent Desktop
ClickOnce HTTP Server
6.
IW downloads the libraries required to execute the granted privileges

Initial ClickOnce installation of the Workspace application

## Applying a patch

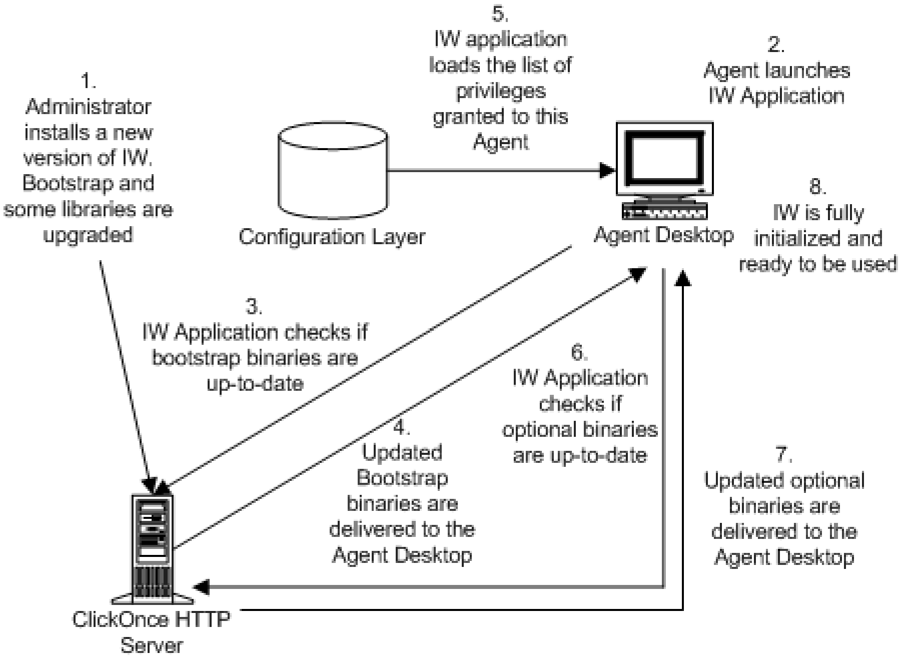
To apply a patch to the installation on the client workstation, the following prerequisites must be met:

- The agent has run Workspace and has been successfully authenticated at least once on the current workstation.
- Privileges that are granted to the agent have not been changed since their previous authentication.

The Figure - **Patching of the Workspace application through ClickOnce** shows the steps in a typical patch installation of Workspace in a ClickOnce environment:

1. The administrator installs a new version of the Workspace Bootstrap and upgrades one or more libraries.
2. Agents launch the Workspace application on their desktop by using the URL or by double-clicking the desktop icon. The agent is authenticated.
3. The Workspace application checks the ClickOnce HTTP Server to determine if the bootstrap binaries are up to date.
4. The updated bootstrap libraries are delivered to the agent workstation.
5. The Workspace application loads the list of privileges that are granted to each agent, based on agent authentication.
6. The Workspace application checks the ClickOnce HTTP Server to determine if the optional binaries are up to date.
7. Updated binaries, if any, are delivered to the agent workstation.

8. The Workspace application is fully initialized and ready for agent use.


1.
Administrator installs a new version of IW. Bootstrap and some libraries are upgraded
5.
IW application loads the list of privileges granted to this Agent
2.
Agent launches IW Application
Configuration Layer
Agent Desktop
8.
IW is fully initialized and ready to be used
3.
IW Application checks if bootstrap binaries are up-to-date
6.
IW Application checks if optional binaries are up-to-date
4.
Updated Bootstrap binaries are delivered to the Agent Desktop
7.
Updated optional binaries are delivered to the Agent Desktop
ClickOnce HTTP Server

Patching of the Workspace application through ClickOnce

## Limitation of patching with ClickOnce

Because of the architecture of Workspace and the underlying Platform SDK and Enterprise Services on which it is built, patches are applied to groups of assemblies, not just to a single assembly. Therefore if one assembly in a group is updated, the whole group must be patched.

## Update agent privilege permissions

To update the Workspace installation on the client workstation with updated privilege permissions, the following prerequisites must be met:

- The agent has run Workspace and has been successfully authenticated at least once on the current workstation.
- The Workspace application has not been upgraded on the ClickOnce server since the previous login.

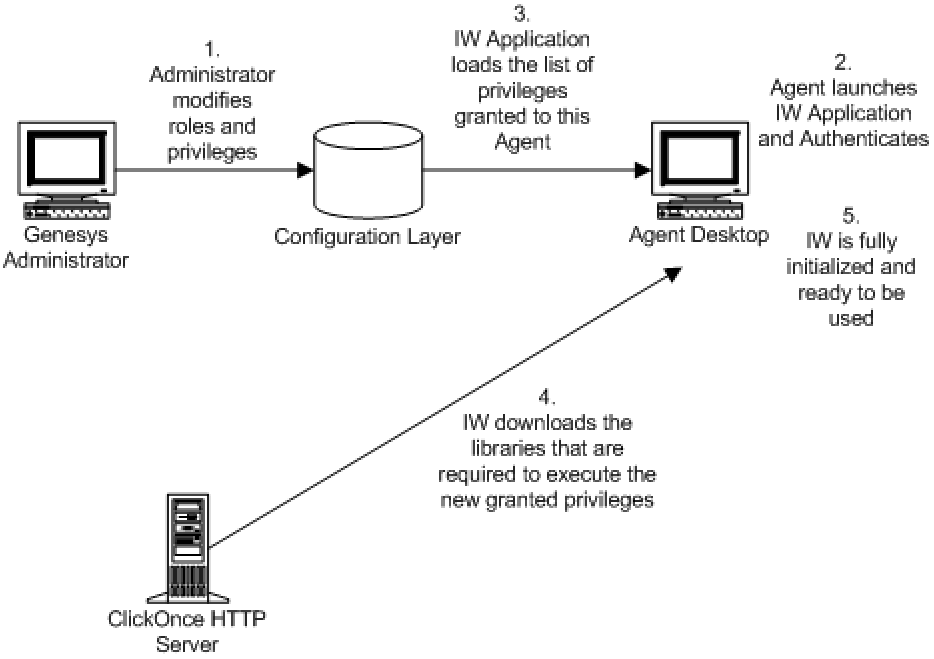
## Privilege updates while the agent is not logged in

The Figure - **Update of the agent's role through ClickOnce** shows the steps in a typical privilege-permission upgrade of Workspace in a ClickOnce environment if the agent is *not* already logged in:

1. The administrator modifies the roles and privileges of the contact center agent by using Genesys Administrator Extension and stores the modified configurations in the Configuration Layer.
2. Agents launch the Workspace application on their desktop by using the URL or by double-clicking the desktop icon. The agents are authenticated.
3. The Workspace application loads the list of privileges that are granted to each agent, based on agent

authentication.

4. The Workspace application then downloads the missing libraries that are required to execute the new granted privileges.
5. Workspace is fully initialized and ready for agent use.


1.
Administrator modifies roles and privileges
3.
IW Application loads the list of privileges granted to this Agent
2.
Agent launches IW Application and Authenticates
Genesys Administrator
Configuration Layer
Agent Desktop
5.
IW is fully initialized and ready to be used
4.
IW downloads the libraries that are required to execute the new granted privileges
ClickOnce HTTP Server

Update of the agent's role through ClickOnce (IW = Workspace)

## Privilege updates while the agent is logged in

If new privileges are granted to the agent while the agent is logged in, the additional libraries will not be downloaded to the agent's workstation; however, if privileges are removed, this change is taken into account immediately to ensure security.

## ClickOnce updates for shared workstations

If multiple users share the same workstation, the download behavior depends on whether each agent has a unique account or whether all agents share the same account.

If each agent has a unique account, then updates are downloaded by account. Therefore, each user will have to download updates. The advantage of this scenario is that multiple agents with different roles can share the same workstation without compromising security.

If all users share a generic account, then only a single instance of the application is downloaded. This means that each user will have the same role as that assigned to the first user to download the application.

## Security constraints

To deploy Workspace, three deliverable subsets are installed on the agent workstation:

- Prerequisites: Microsoft .NET Framework 4.5.
- Mandatory executable: Workspace Application Bootstrap (`.exe` file and mandatory DLL assemblies).
- Optional assemblies: The list of optional assemblies depends on the privileges that are granted to the agent who logs in to the application.

The .NET Framework and service pack are not installed through the ClickOnce system; they are installed by the ClickOnce Bootstrap application (see the Figure - **Initial ClickOnce installation of the Workspace application** and Figure **Patching of the Workspace application through ClickOnce**). Therefore, more rights are required on the target computer to install the prerequisite than to install Workspace.

The Workspace Application Bootstrap and the optional assemblies are pure ClickOnce deliverables; therefore, the full ClickOnce security model applies to these installables. However, the .NET Framework does not have the same security constraints. Therefore, Genesys recommends that you deploy the agent application in two phases:

1. Installation of .NET Framework by the administrator **by using the ClickOnce Bootstrapper**, or **by using the standard network distribution**.
2. Installation of Workspace by the agents at the initial login.

You can find more information about ClickOnce security at this URL: http://msdn.microsoft.com/en-us/library/76e4d2xw(VS.80).aspx

### Code Access Security

Code Access Security (CAS) is a mechanism that limits system access to the permissions that are granted to each code. CAS protects resources and operations and enables you to grant permissions to assemblies — giving a high degree of control over what resources the assemblies can access. For example, restrictions can be applied to file-system locations, the registry, and specific name spaces.

### Setting Code Access Security permissions

You must set CAS permissions for both the Workspace ClickOnce application and the zone from which the application will be installed (for example, your local intranet, the Internet, and so on).

Workspace must be defined as a Full Trust application. A Full Trust application is granted all access to any resource. Granting this level of permission is necessary because some of the embedded DLLs require Full Trust permissions. If Workspace is not defined as a Full Trust application, execution failures will occur when the application tries to access a restricted resource.

### Machine Access Security

The Workspace application, which is deployed by ClickOnce, uses CAS permissions. This means that Workspace might require more permissions than are allowed by your security policy. In this case, ClickOnce will allow an automatic elevation of privileges. However, if the publisher is not trusted, a Machine Access security warning is prompted, but no security warning is prompted if the publisher of

Interaction Workspace is trusted.

> ### Tip
> ClickOnce supports Windows Vista User Account Control (UAC); therefore no additional messages are displayed.

### ClickOnce and installation security

The minimum class privilege for running a ClickOnce application is `User`. A `Guest` account cannot deploy a ClickOnce application through the network. If an agent is logged in with a `User` account, ClickOnce will automatically elevate the privileges for installing the application on the agent's workstation. If the publisher of ClickOnce deployment is Trusted, the installation will run without any prompting; however, if the publisher is not Trusted, the agent will be prompted to Trust the publisher of the deployment.

### ClickOnce and location security

To deploy an application via ClickOnce, the ClickOnce HTTP server must be in a Trusted Zone, such as your local intranet, or be listed in Trusted Sites.

### ClickOnce and publisher security

You must consider two publishers when you are deploying a ClickOnce application: the publisher of the application and the publisher of the deployment.

The Workspace Deployment Wizard updates some application files; therefore, the application manifest must be signed after these updates. The Workspace Deployment Wizard must be enabled to sign both the application and deployment manifests.

To sign the manifests, the Workspace Deployment Wizard requires a security certificate. The same security certificate can be used to sign both manifests.

### Certificate deployment overview

You must provide a permanent certificate that is used to sign the Workspace installer manifest. This certificate is pointed to during installation. You can obtain your own certificate by one of the following methods:

- Generate a self-signed certificate by using the `Makecert.exe` file.
- Purchase a third-party verified certificate
- Generate a certificate by using Windows Certificate Server

> ### Tip
> The certificate can be stored on the client side and the server side in the Windows

> domain. The certificate must be on the target workstation. The certificate can be declared at the Network level.

Refer to the *Genesys 8 Security Deployment Guide* to review a detailed procedure about how to create a certificate.

### Deploying certificates on a workstation

The Workspace Deployment Wizard requires you to do one of the following:

- Provide a security certificate.
- Generate a self-signed security certificate in the Workspace Deployment Wizard.

You must retain the Certificate file for all upcoming updates. If the updated version is signed by a different certificate, ClickOnce will consider it as a new installation, which means that you will have to uninstall the previous version by using `Add/Remove Programs` command *on each client workstation*.

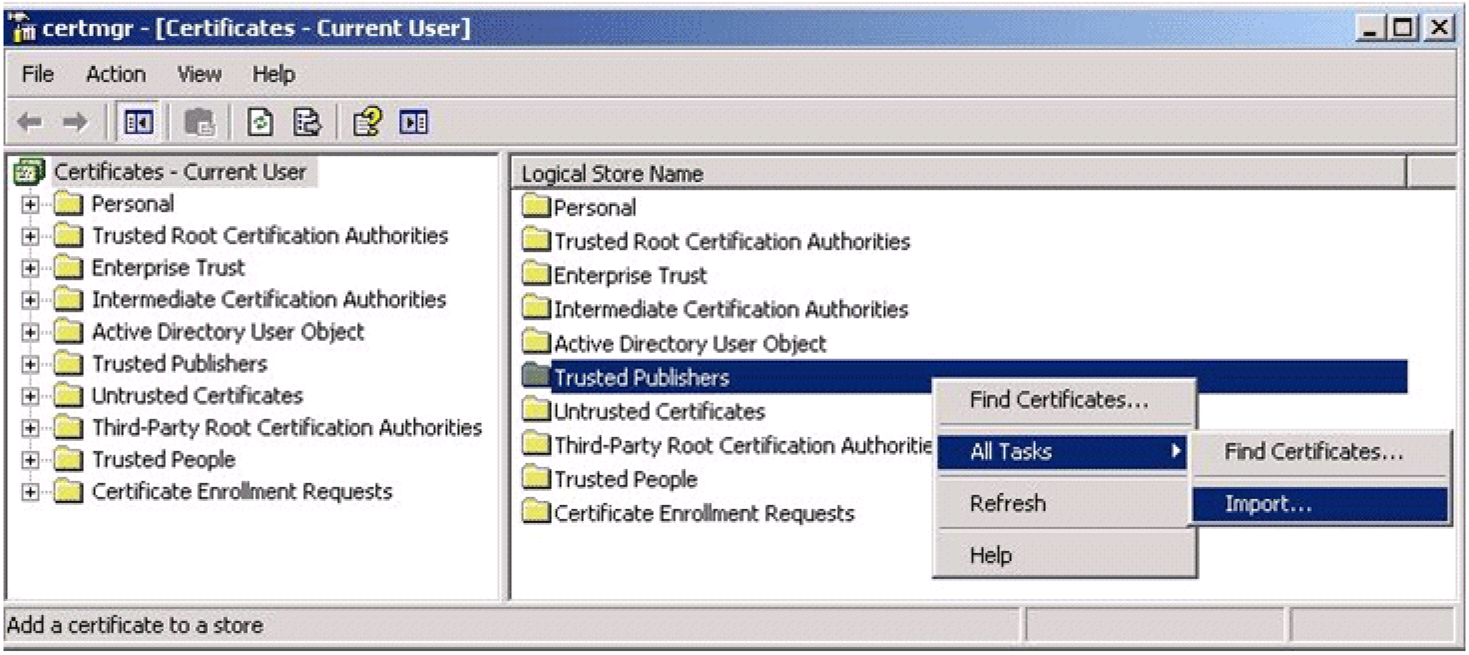
### Application and deployment signing cases

The Table - **Summary of the Cases for Signing the Application and the Deployment for the Integrator and the User** provides a summary of the cases for signing the application and the deployment for the Integrator and the User, along with the impact for the user.

**Summary of the Cases for Signing the Application and the Deployment for the Integrator and the User**

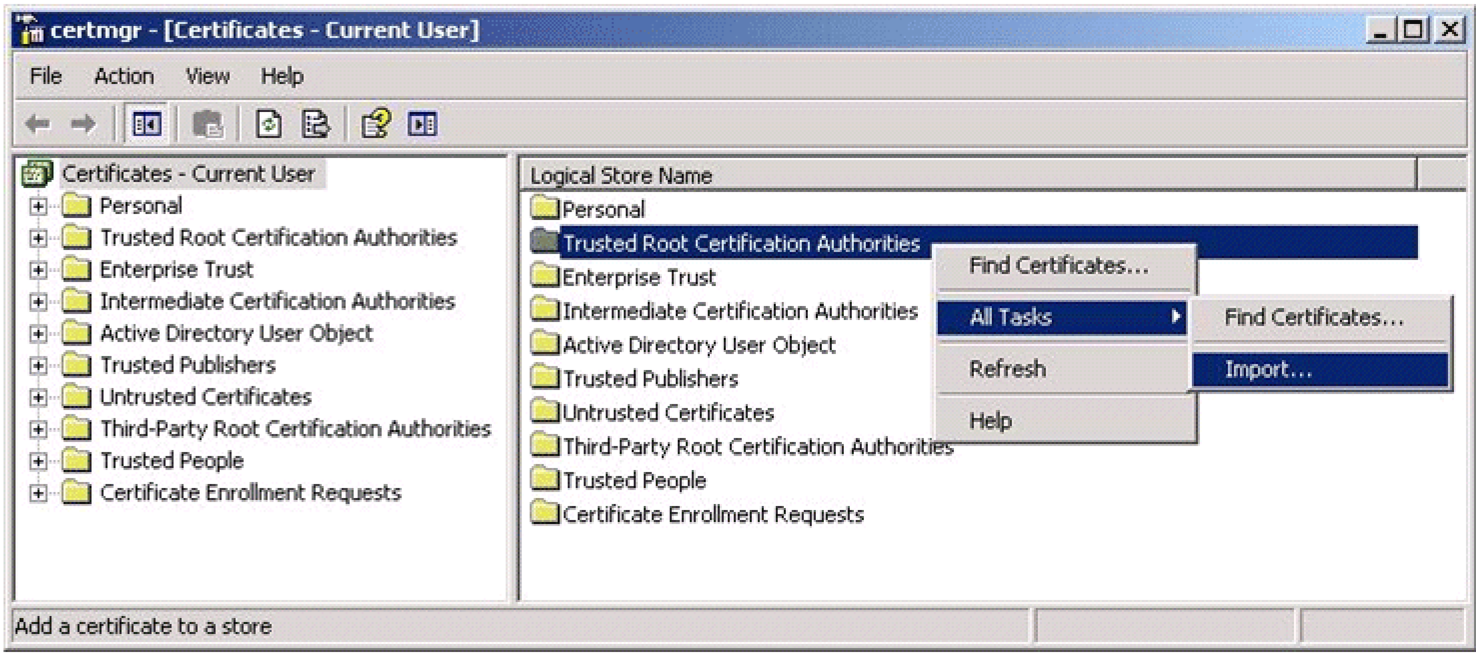
| | Integration | User administration | User impact |
|---|---|---|---|
| **Application Verisign Certificate** | Non-modifiable application | | A prompt to trust the known publisher is displayed. |
| | | Add the certificate in Trusted Publishers store (see Figure - **Importing a Trusted Publisher**). | No warning is displayed. |
| **Application Self-Certification** | Non-modifiable application | | A prompt to trust the unknown publisher is displayed. |
| | | Add the certificate in the Trusted Root Certification Authorities store (see Figure - **Importing a Trusted Root Certification Authority**) and in the Trusted Publishers store (see Figure - **Importing a Trusted Publisher**). | No warning is displayed. |
| **Deployment Verisign Certificate** | N/A | Sign the Deployment. | A prompt to trust the known publisher is |

| | Integration | User administration | User impact |
|---|---|---|---|
| | | | displayed. |
| | | Sign the Deployment and Add the certificate in the Trusted Publishers store (see Figure - **Importing a Trusted Publisher**). | No warning is displayed. |
| **Deployment Self-Certification** | N/A | Sign the Deployment. | A prompt to trust the unknown publisher is displayed. |
| | | Sign the Deployment and Add certificate in the Trusted Root Certification Authorities store (see Figure - **Importing a Trusted Root Certification Authority**) and in the Trusted Publishers store (see Figure - **Importing a Trusted Publisher**). | No warning is displayed. |


certmgr - [Certificates - Current User]
File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
Logical Store Name
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoritie
Trusted People
Certificate Enrollment Requests
Find Certificates...
All Tasks
Refresh
Help
Find Certificates...
Import...

Add a certificate to a store

Importing a Trusted Publisher


certmgr - [Certificates - Current User]
File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
Logical Store Name
Find Certificates...
All Tasks
Refresh
Help
Find Certificates...
Import...

Add a certificate to a store

Importing a Trusted Root Certification Authority

### Trusted publishers

For a publishers to be consider a Trusted Publisher, the following criteria must be met:

- The publisher certificate must be installed in the Trusted Publishers certificate store on the user's computer.
- The issuing authority of the publisher certificate must have its own certificate installed in the Trusted Root Certification Authorities certificate store (This is already included in Verisign).

If the issuer of the certificate is not in the Trusted Root Certification Authorities certificate store, or if the publisher is not in the Trusted Publishers certificate store, the user will be prompted with a dialog box that asks for confirmation. For more information on Trusted Publisher certificates, refer to the following article: http://msdn.microsoft.com/en-us/library/ms996418.aspx

## Deploying certificates on the network

There are two methods for deploying certificates over a network to a large number of client workstations:

1. Active Directory domain
2. `certmgr.exe` tool

### Active Directory domain

If you run in an Active Directory (AD) domain, use the AD Group Policy Objects (GPO) to distribute certificates centrally. For the root Certificate Authorities (CA) certificate, add a GPO to AD, and then link to the appropriate level (usually the domain level).

1. Go to: `Computer Settings>Windows Settings>Security>Public Key Policies`.
2. Add the root CA certificate under `Trusted Root Certification Authorities`.

Next you must distribute the trusted publisher. Add a GPO to AD and link at the appropriate level (usually for the organizational unit that should trust the application).

1. Go to `User Settings>Windows Settings>Internet Explorer Maintenance>Security>Authenticode Settings`.
2. Click `Import`.
3. Click `Modify`.
4. Enable the `Lock down Trusted Publishers` feature to prevent users from modifying their Trusted Publisher certificate store.

After the standard GPO-replication-to-clients occurs, every client trusts your CA and the Trusted Publisher certificate. Users will not receive Trust challenges for applications that are signed with corporate certificates. For more information on this topic, refer to the following technical article: http://msdn.microsoft.com/en-us/library/aa719097.aspx#clickonce_topic6

### certmgr.exe tool

You can use the `certmgr.exe` tool to install the certificate on each client workstation. See the following technical article for more information: http://msdn.microsoft.com/en-us/library/ms996418.aspx#clickoncetrustpub_topic5

## Modifying agent workstations

Installation of Workspace results in the following modifications to your agent workstations:

- Workspace is added to the `Start` menu.
- Workspace is added to the `Add/Remove Programs` group in the Control Panel.
- The Workspace icon is added to the desktop.
- ClickOnce stores the application binaries and associated data files in directories that it creates and manages in the user-profile `Local Settings` folder or other location.

To determine the folder locations at which ClickOnce has stored the application binaries, launch Workspace, and open the `About` dialog box from the `Help` menu. Press `Ctrl-Click` on the Genesys icon to display hidden buttons that enable you to access the `exe`, `data`, `log`, and `GC` folders.

Nothing is added to the `Program Files` folder or the registry. No administrative rights are required for the agent to install the application.

# Deployment prerequisites

## ClickOnce deployment prerequisites

ClickOnce provides a centralized deployment environment that enables you to distribute software and updates from a single server to all agent workstations.

A ClickOnce deployment requires certain conditions to be met both on the client-side and on the server side. This section summarizes the prerequisites for deployment on different web severs and on the client workstation. Refer to the *Genesys Supported Operating Environment Reference Guide* topic for information about the specific environment, system, and operating system versions that are supported by Interaction Workspace.

### Licensing and certificate management

For details on deploying security certificates, refer to Security Constraints.

### Deployment on an Apache server

You must have a Windows server, Linux server, or Solaris server, and Apache Server (refer to *Genesys Supported Operating Environment Reference Guide*). You must also configure Apache by using the following Procedure: Configuring Apache to enable the ClickOnce package.

### Deployment on an IIS server

Your environment must have Windows Server and Microsoft IIS (Refer to the *Genesys Supported Operating Environment Reference Guide*).

The Workspace Deployment Manager is installed on the server along with the application material. To deploy Workspace, launch the Workspace Deployment Manager wizard. The wizard prompts for the required information. You must sign the ClickOnce deployment using a corporate certificate or a test certificate.

> Tip
>
> To avoid an error with Interaction Workspace Deployment Manager, you must log in as Administrator.

### Deployment on the client

Workspace runs on the Window client-side operating system. The workstation must have the .NET Framework installed. The following browsers are supported: Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome. Refer to the *Genesys Supported Operating Environment Reference*

*Guide* for the specific versions that are supported.

## Important

- To use Mozilla Firefox, you must install the following add-on : "`Microsoft .NET Framework Assistant`". This add-on enables you to start the application directly and have Framework .NET detection. This add-on is found here: Microsoft .NET Framework Assistant
- If you have Microsoft .NET Framework Assistant 1.3.0 or higher installed, then the `publish.htm` page might not detect the installed prerequisites and might display a warning. In this case, click the launch link.
- To use Google Chrome, you must install the following add-on "ClickOnce for Google Chrome" from Chrome Web Store : ClickOnce for Google Chrome
- Other browsers, such as Safari and Opera are not officially supported and might not function correctly.
- To properly deploy the Workspace ClickOnce package on agent workstations, the end users must have write access to the `StartMenu` folder of their Windows Users Profile.

### Mass Deployment of .NET Framework

If you do not have the .NET Framework installed on all of your client workstation, you can use the procedures that are found on the Microsoft Developer Network to perform a mass deployment. http://msdn.microsoft.com/en-us/library/ee390831(v=vs.110).aspx

## Non-ClickOnce deployment prerequisites

A non-ClickOnce deployment does not give you the advantages of managing updates to privileges, permissions, or software upgrades. A non-ClickOnce deployment is done typically for testing or development purposes where the agent workstation is not in a production environment. Only the Workspace application is installed on the client workstation.

Refer to the *Genesys Supported Operating Environment Reference Guide* for information about client-side operating system and browsers support in a non-ClickOnce deployment.

## Important

Other browsers, such as Safari and Opera are not officially supported and might not function correctly.

## Mass Deployment of .NET Framework

If you do not have the .NET Framework installed on all of your client workstation, you can use the procedures found on the Microsoft Developer Network to perform a mass deployment. http://msdn.microsoft.com/en-us/library/ee390831(v=vs.110).aspx

# Workspace SIP Endpoint in Virtual Desktop Infrastructure

[**Added:** 8.5.109.16] [**Modified:** 8.5.140.08]

## Important

A direct network connection between the VDI infrastructure (VM or Citrix Server) and Workspace SIP Endpoint host is required. Network Address Translation and home office behind a router without VPN are not supported.

## Tip

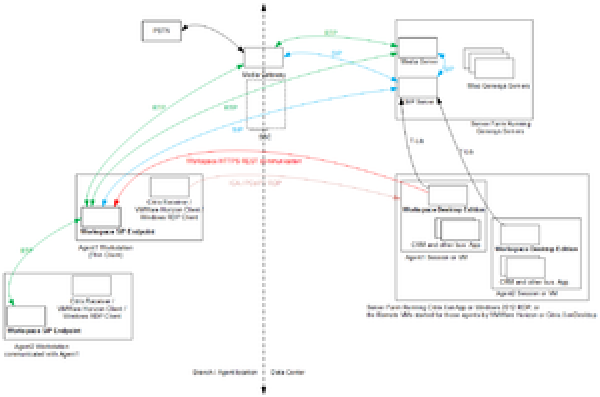
Workspace also supports the Genesys Softphone in place of Workspace SIP Endpoint. To learn about how Genesys Softphone can be deployed in a VDI environment, see Genesys Softphone Deployment Guide.

The standalone version of Workspace SIP Endpoint 8.5.1 enables Workspace and Workspace SIP Endpoint to run in separate user sessions. Workspace manages the UI and interaction control business logic in a virtual desktop infrastructure (VDI, for example: RDP, VMWare, XenApp, XenDesktop) environment and Workspace SIP Endpoint manages voice and video media on the local workstation. This architecture enables you to offload media processing to the agent workstation and reduce the load on your server, leading to better scalability. For information about Virtual Desktop Infrastucture, refer to the Genesys Virtualization Platform Support topics in the *Genesys Supported Operating Environment Reference Guide*.

Workspace SIP Endpoint 8.5.1 can be deployed as a standalone application on agent workstations, either as part of a ClickOnce package or directly installed.

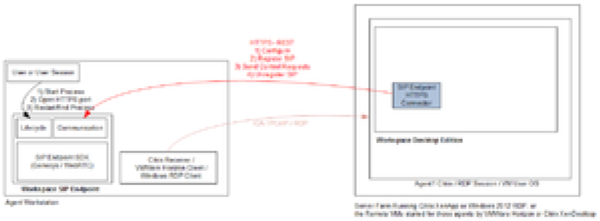
The following figures detail how Workspace and Workspace SIP Endpoint 8.5.1 use HTTPS REST to communicate in a VDI environment. The communication between Workspace and Workspace SIP Endpoint relies on as HTTPS REST connection, independent from the VDI technology.

Network view:



Example of the network connections for Workspace SIP Endpoint Standalone application in a virtualized environment

Component view:



Example of the network connections for Workspace SIP Endpoint Standalone application in a virtualized environment

When Workspace SIP Endpoint is installed as a standalone application on an agent's workstation, its startup and exit are no longer controlled by Workspace. Instead, it is started and stopped as an "auto-start" Windows application and/or manually by the agent.

## Provisioning the Workspace SIP Endpoint Standalone mode

By default, Workspace SIP Endpoint is installed as a standalone application with "protocol"="http" and "port"="8000" set.

First install the Workspace SIP Endpoint Standalone application, then provision it in the `InteractionWorkspaceSIPEndpoint.exe.config` file *and* configure the following options in the `interaction-workspace` section of the Workspace Desktop application:

- sipendpoint.standalone.protocol
- sipendpoint.standalone.port
- sipendpoint.standalone.vdi-detection-model
- sipendpoint.standalone.vdi-detection-use-dns [**Added:** 8.5.140.08]
- sipendpoint.standalone.security-level
- sipendpoint.standalone.certificate-search-value
- sipendpoint.standalone.subject-criteria

- sipendpoint.standalone.subject-matching-properties

To adjust these default settings and make Workspace SIP Endpoint 8.5.1 run in standalone mode as a secured application, you must make the following modifications to the SIP Endpoint settings in the `appSettings` section of the `InteractionWorkspaceSIPEndpoint.exe.config` file:

```
<appSettings>
<!-- This option activates HTTP or HTTPS communication - requires that a port is defined in
port option. -->
<add key="protocol" value="https"/>
<!-- This option gives the level of security if 'protocol' option is set to HTTPS. -->
<!-- 0: check Address IP range, no client certificate required (no check on client
certificate) -->
<!-- 1: check Address IP range, check client certificate -->
<!-- 2: check Address IP range, check client certificate, check client certificate subject -->
<add key="security_level" value="1"/>
<!-- This option gives a string value Workspace uses to select a certificate if 'protocol'
option is set to HTTPS. -->
<!-- Search is done first by thumbprint, then by issuer, then by subject. -->
<add key="certificate_search_value" value="Communications Server"/>
<!-- This option specifies the port to be used when communicating in HTTP or HTTPS -->
<add key="port" value="8000"/>
<!-- This option is only needed if 'security_level' option is 2 for validation of client
certificate subject. -->
<!-- It gives a list of subject fields to validate in the client certificate. -->
<add key="subject_criteria" value="E,CN,OU,OU,OU,DC,DC,DC,DC"/>
<!-- This option is only needed if 'security_level' option is 2 for validation of client
certificate subject. -->
<!-- It gives a list of current user property values to match with the list of criteria
defined by 'subject_criteria' option. -->
<!-- The certificate subject validation process compare the subject criteria values with
current user property values find in its active directory. -->
<add key="subject_matching_properties"
value="mail,cn,distinguishedName.OU,distinguishedName.OU,distinguishedName.OU,distinguishedName.DC,distinguishe
<!-- This option activates the CORS mechanism for the HTTP REST port with the required policy
-->
<!--<add key="cors" value="*"/>-->
<!-- This option specifies if SIP Endpoint can be activated only by an application on the
same local host -->
<!--<add key="localhost" value="true"/>-->
<!-- These options specify a ranges of IP addresses allowed for connection to SIP Endpoint
http services in CIDR format.-->
<!-- Several range can be applied separted with commas "10.20.35.0/24,10.20.39.0/24"-->
<!--<add key="ipv4_address_range" value=""/>-->
<!--<add key="ipv6_address_range" value=""/>-->
<!-- SIP Endpoint dictionary -->
<add key="title" value="Workspace SIP Endpoint"/>
<add key="exit" value="Exit..."/>
</appSettings>
```

## Workspace Standalone SIP Endpoint deployment modes

Workspace Standalone SIP Endpoint can be deployed using one of two modes:

- Standalone Application
- ClickOnce Standalone Package

## Standalone mode

In this mode, executing the `setup.exe` file installs Worksapce SIP Endpoint on the target workstation with no pre-requisites other than .NET Framework version 4.5.

It can be executed in silent mode.

You can repackage the out-of-the-box Workspace SIP Endpoint Standalone setup to meet the specifications of "Microsoft System Center Configuration Manager" and allow it to push this software to workstations in a standard way. The auto-start registry keys instructions can be reused for this purpose.

### SIP Endpoint auto-start

Workspace SIP Endpoint application is deployed as an auto-start application. This enables the Workspace SIP Endpoint to be started automatically as a standalone application each time the agent logs in on the workstation, and stops when he or she logs off. To enable this feature, the following registry key is set when Workspace SIP Endpoint is installed:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\
CurrentVersion\Run\InteractionWorkspaceSIPEndpoint
```

The full path to the Workspace SIP Endpoint application is assigned as the value of the this key, for example:

```
C:\Program Files (x86)\InteractionWorkspaceSIPEndpoint\
InteractionWorkspaceSIPEndpoint.exe
```

When the Workspace SIP Endpoint application is running in this mode, the application waits for a Workspace application to connect to the HTTP port and start a SIP session.

Each time that Workspace exits, it informs the connected standalone SIP Endpoint application to finalize its endpoint activity. Once there are no more active calls, Workspace SIP Endpoint closes itself and then restarts so that it is ready to receive a new connection from a new Workspace instance.

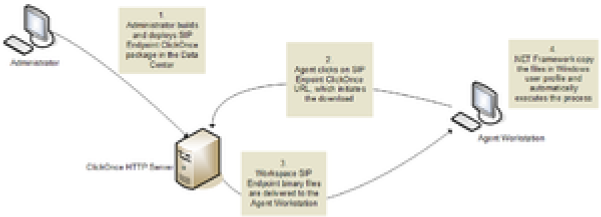
## Click-Once mode

Refer to ClickOnce Deployment and Installation.

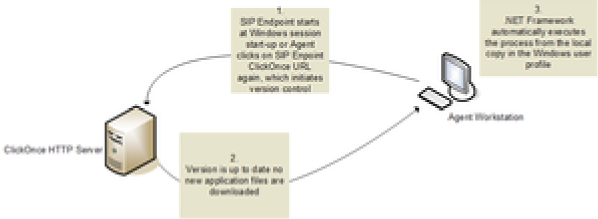
Once Workspace SIP Endpoint is deployed on the HTTP Server, the .NET Framework that is installed as a pre-requisite on Agent Workstation allows a seamless installation as well as execution of the SIP Endpoint process, using only the Microsoft Windows **USER** security model.

The following is a summary of the deployment and upgrade cycle of the Workspace Standalone SIP Endpoint in a ClickOnce deployment:

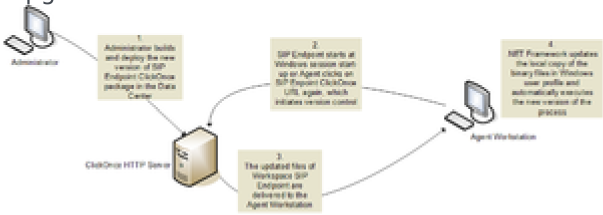
1. First time execution for User X on workstation Y:


Administrator
1. Administrator builds and deploys SIP Endpoint ClickOnce package in the Data Center
2. Agent clicks on SIP Endpoint ClickOnce URL, which initiates the download
4. NET Framework copy the files in Windows user profile and automatically executes the process
Agent Workstation
ClickOnce HTTP Server
3. Workspace SIP Endpoint binary files are delivered to the Agent Workstation

2. Second time execution for User X on workstation Y, with the server version of the software unchanged:


1. SIP Endpoint starts at Windows session start-up or Agent clicks on SIP Enpoint ClickOnce URL again, which initiates version control
3. NET Framework automatically executes the process from the local copy in the Windows user profile
Agent Workstation
ClickOnce HTTP Server
2. Version is up to date no new application files are downloaded

3. Third time execution for User X on workstation Y, after the server version of the software has been upgraded:


Administrator
1. Administrator builds and deploy the new version of SIP Endpoint ClickOnce package in the Data Center
2. SIP Endpoint starts at Windows session start up or Agent clicks on SIP Enpoint ClickOnce URL again, which initiates version control
4. NET Framework updates the local copy of the binary files in Windows user profile and automatically executes the new version of the process
Agent Workstation
ClickOnce HTTP Server
3. The updated files of Workspace SIP Endpoint are delivered to the Agent Workstation

### Auto-upgrade on ClickOnce in Standalone mode

At Workspace SIP Endpoint application restart, the application checks to determine if a new version is available in the ClickOnce repository, and it is downloaded if necessary. The application is then restarted with the new version.

### Auto-start on ClickOnce in Standalone mode

When Workspace SIP Endpoint is installed with ClickOnce as a standalone application, it is then automatically restarted at the beginning of each new Windows session started by the same user on the same workstation.

## Workspace Standalone SIP Endpoint security risks

The following table summarizes the various levels of security versus functionality that can be achieved by different option configuration scenarios. Because a dedicated listening port is opened on agent workstations by Workspace Standalone SIP Endpoint, the workstation is vulnerable to certain security risks. This dedicated port is in addition to listening ports that are opened for SIP and RTP/RTCP.

**Workspace/SIP Endpoint Security Matrix**

| Security Level | SIP Endpoint option values | Workspace option values | IT operational effort |
|---|---|---|---|
| Encryption with Validation level 1:<br>no certificate validation (Lab only) | <add key="ipv4_address_range" value=""/> and/or <add key="ipv6_address_range" value=""/><br><add key="protocol" value="https"/><br><add key="security_level" value="0"/><br><add key="certificate_search_value" value="certificate thumbprint"/> | sipendpoint.standalone.security-level=0 | **Low**:<br>Make any certificate (valid or not) availalble on the Personal Store of the workstations that run Workspace SIP Endpoint |
| Encryption with Validation level 2:<br>Simple certificate validation | <add key="ipv4_address_range" value=""/> and/or <add key="ipv6_address_range" value=""/><br><add key="protocol" value="https"/><br><add key="security_level" value="0"/><br><add key="certificate_search_value" value="certificate thumbprint"/> | sipendpoint.standalone.security-level=1 | **Low**:<br>Make any valid certificate available on the Personal Store of the workstations that run Workspace SIP Endpoint |
| Encryption with Validation level 3:<br>Mutual certificate validation | <add key="ipv4_address_range" value=""/> and/or <add key="ipv6_address_range" value=""/><br><add key="protocol" value="https"/><br><add key="security_level" value="1"/><br><add key="certificate_search_value" value="certificate thumbprint"/> | sipendpoint.standalone.security-level=2<br>sipendpoint.standalone.certificate-search-value=certificate thumbprint | **Medium**:<br>Make any valid certificate available on the Personal Store of the workstations that run Workspace SIP Endpoint and on the Personal Store of the virtual system that runs Workspace Desktop Edition |
| Mutual HTTPS with Personal Identity check | <add key="ipv4_address_range" value=""/> and/or <add key="ipv6_address_range" value=""/><br><add key="protocol" value="https"/> | sipendpoint.standalone.security-level=3<br>sipendpoint.standalone.certificate-search-value=certificate issuer or subject common part<br>sipendpoint.standalone.subject-criteria=certificate subject attribute for validation, | **High**:<br>Make valid personal certificates available on the Personal store of the workstations that run Workspace SIP Endpoint and on the Personal Store of the virtual system that runs Workspace Desktop Edition. |

| Security Level | SIP Endpoint option values | Workspace option values | IT operational effort |
|---|---|---|---|
|  | <add key="security_level" value="2"/><br><add key="certificate_search_value" value="certificate issuer or subject common part"/><br><add key="subject_criteria" value="certificate subject attribute for validation, typically 'E'"/><br><add key="subject_matching_properties" value="Windows account attribute for validation, typically 'mail'"/> | typically 'E'<br>sipendpoint.standalone.subject-matching-properties=Windows account attribute for validation, typically 'mail' | The same domain account should be used in both windows sessions. The attributes of the certificate provided by the remote party are compared to the attributes of the local domain user. |

# Configuring system-access permissions

For Workspace to run correctly, the agent application must be granted permission to access specific system objects. When Workspace is launched, it connects to Configuration Server using the credentials of the agent who is logging in. Therefore, the required permissions to access system objects are typically much higher than those granted to an agent who uses Workspace.

To mitigate this situation you must assign three different kinds of permissions to the agent login:

- Execute permissions
- Read permissions
- Write permissions

The following subsections describe how to configure these permissions in the Permissions tab of the specified object. You can choose to configure agents individually by the Person object, or as a group by Access Group.

Refer to *Genesys Administrator Extension Help* and *Genesys Security Guide* for detailed information on how to use Genesys Administrator Extension and Management Framework to configure access permissions.

## Configuring execute permissions

You must grant execute permissions for the Workspace application to each agent or groups of agents so that Workspace can connect to Configuration Server to start the application.

## Configuring read permissions

Agents might require permissions to read from the Application objects that are referenced in the Connection list of the Workspace application object. They might be required to connect to one of these servers to activate its associated features. The following is a list of items to which an agent might require read access:

- The host of any application objects that are referenced in the Connection list of the Workspace application object.
- The Person object that corresponds to the agent.
- The Place object that corresponds to the voice channel to which the agent is assigned.
- The DN object that determines the capacity of the channel (Voice, IM). This information is stored in annex of the DN.
- The Switch and the T-Server object to determine the possible channel.
- The Tenant object.
- The Person objects of the Tenant to enable Team Communicator to access the firstname, lastname, and username of internal targets.
- The Skills objects of the Tenant to enable Team Communicator to access the names of Skills.

- The Agent Group objects of the Tenant to enable Team Communicator to access the names of Agent Groups.
- The Routing Point objects of the Tenant to enable Team Communicator to access the number, name, and switch.name of Routing Points.
- The ACD Queue objects of the Tenant to enable Team Communicator to access the number, name, and switch.name of ACD Queues.
- The User Properties of the agent's Tenant, logged in application, and agent's Agent Groups, to read corporate favorites for display in Team Communicator.
- The Business Attributes of the Tenant to enable the Contact module to use Business Attributes.
- The transaction object of the Tenant that can be used for overriding options of the strategy.
- The applications used as Backup servers and configuration Server application to have HA.
- Script objects of the tenant Interaction queue and workbins.
- The Calling List, Table Access, DB Access Point Application of Table Access, Format, Field objects reflecting the data structure of the campaigns where the agent will be engaged.

## Configuring write permissions

If you have configured the agent to store preferences in their Person annex instead of on their local desktop or in a shared directory, you must grant that agent write permissions on their Person object.

If you plan to store agent preferences and personal information on a shared directory, refer to Storing the agent profile on a controlled shared host.

If you have configured your system to prompt for a the agent's phone number at login time (this requires SIP Server), you must grant write access to the agent on the SIP DN in which the agent logs in, to set the `request-uri`.

# Genesys Engage/Genesys Cloud Hybrid Integrations

To use the following Genesys Cloud services in Workspace you must first provision a Genesys Engage/Genesys Cloud hybrid integration.

The following Genesys Cloud services are available as Hybrid Integrations:

- Genesys Predictive Engagement (Altocloud). Click here to get started.

# Deployment procedures

This chapter provides the procedures that are required to install and deploy Workspace in a Genesys 8 environment.

The following task table provides an overview of how to set up your Genesys 8 Configuration Layer for Workspace, install and deploy Workspace, and perform additional (optional) installations.

Refer to *Genesys Administrator Extension Help* and *Genesys Security Guide* for detailed information on how to use Genesys Administrator Extension and Management Framework to configure access permissions.

**Preparing the Configuration Layer and Installing Workspace**

| Objective | Related procedures and actions |
|---|---|
| 1. Configuring the Workspace Application Object | • Installing Workspace Deployment Package on the Windows operating system<br>• Using Genesys Administrator Extension to set up the Workspace application<br>• (Optional) Enabling client-side port definition |
| 2. (Optional) Deploying The ClickOnce Application On Your Web Server. Choose this option if you want to deploy Workspace as a ClickOnce application. | 1. Deploying the Workspace downloadable package (ClickOnce) on your web server<br>2. Configuring Apache to enable the ClickOnce package<br>3. Configuration verification--Testing the client<br>4. (Optional) Installing the Workspace SIP Endpoint<br>5. (Optional) Install Language Packs for Workspace |
| 3. (Optional) Installing The Workspace Developer Toolkit. Choose this option if you want to deploy the Workspace developer package. | 1. Installing Workspace Customization on the Windows operating system<br>2. (Optional) Installing the Workspace SIP Endpoint<br>3. (Optional) Install Language Packs for Workspace |
| 4. (Optional) Installing The Workspace Application. Choose this option if you want to deploy a non-ClickOnce version of Workspace. | 1. Installing the Workspace application on a client desktop<br>2. (Optional) Installing the Workspace SIP Endpoint<br>3. (Optional) Installing Plug-ins for Workspace<br>4. (Optional) Install Language Packs for Workspace |

# Configuring the Workspace application object

[**Modified:** 8.5.111.21]

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**

# Choose your deployment

Choose one of the deployment options in the following tabs.

Important

- Some releases of Workspace include Workspace language packs (localized User Interface and Help). These procedures include information about how to install language packs either as part of the Workspace deployment or after you have deployed Workspace.
- Genesys recommends that you always install the release of Workspace for which the language pack was developed rather than installing a language pack on a previously deployed release of Workspace. For example, you should not install an 8.5.1 language pack on top of an 8.5.0 release of Workspace; doing so might result in some UI text being displayed in English or some UI elements being incorrectly labelled.
- If you are not deploying from the Workspace International CD/DVD, you must manually add Language Packs to your deployment package.

Watch video: How to Deploy Languages in Workspace Desktop Edition (International) 8.5.1: Link to video

## Deploying the ClickOnce Application on your web server

### Procedures

1. Install the deployment package

Perform the Procedure: *Installing Workspace Deployment Package on the Windows operating system*, which guides you through the steps for installing Workspace on your Windows web server from the Workspace CD/DVD.

### [+] Procedure: Installing Workspace Deployment Package on the Windows operating system

**Purpose:** To install the deployment files for Workspace on the Windows web server.

Tip

After running one of the Windows installers, inspect the directory tree of your system

> to make sure that the files have been installed in the location that you intended.

### Prerequisites

- Have Administrative rights to the web server
- Framework .NET 4.5 installed

### Start

1. On your desktop, open the Workspace Desktop Edition CD/DVD or the Workspace Desktop Edition IP and double-click the `Setup.exe` file.

   You might be asked to reboot your system to delete or rename certain system files before the Installation Wizard runs.

   The Genesys Installation Wizard launches and the `Welcome` panel is displayed.

2. On the `Welcome` panel, do one of the following:
   - Click `Next` to begin the installation procedure.
   - Click `Cancel` to exit the Genesys Installation Wizard.
   - Click `About` to open the Workspace Desktop Edition ReadMe file in your default browser.

   If you clicked `Next`, the `Genesys License Agreement` panel is displayed.

3. On the `Genesys License Agreement` panel, read the `DEVELOPER SOFTWARE LICENSE AGREEMENT`.

   If you accept the `DEVELOPER SOFTWARE LICENSE AGREEMENT`, check `I accept Genesys License Agreement`; if you do not accept the `DEVELOPER SOFTWARE LICENSE AGREEMENT`, click `Cancel`.

   If you accepted the `DEVELOPER SOFTWARE LICENSE AGREEMENT`, do one of the following:
   - Click `Next` to continue the installation procedure.
   - Click `Back` to return to the `Welcome` panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.

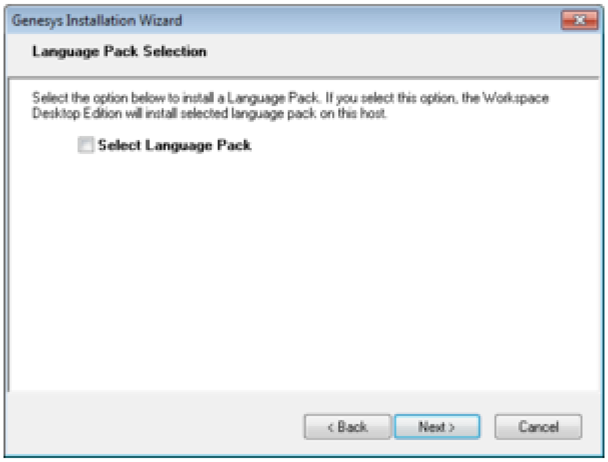
   If you clicked `Next`, the `Select Options` panel is displayed.

4. On the `Select Options` panel, do one of the following:
   - Choose `Prepare a ClickOnce package`, and click `Next`.
   - Click `Back` to return to the `Welcome` panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.

   For more information about installation options, see the Table - **Workspace Install Mode Deployment Packages**.

   If you clicked `Next`, the `Choose Destination Location` panel is displayed (see Figure - **Choose Destination Location panel of the Genesys Installation Wizard**) unless you are installing from the International DVD.

5. (Optional) If you are installing from the International DVD, the `Language Pack Selection` panel is displayed.



Genesys Installation Wizard

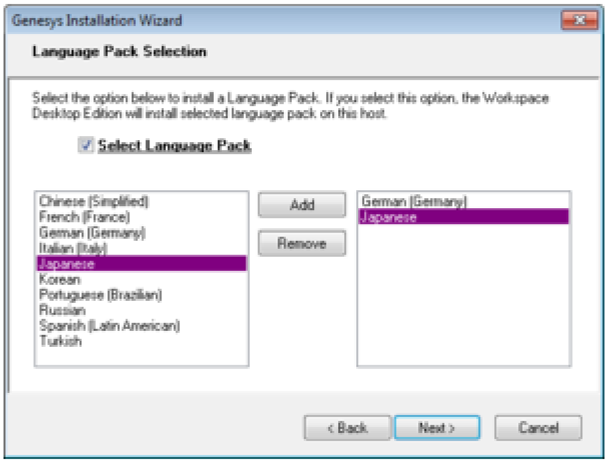
Language Pack Selection

Select the option below to install a Language Pack. If you select this option, the Workspace Desktop Edition will install selected language pack on this host.

□ Select Language Pack

Language Pack Selection panel of the Genesys Installation Wizard

Select `Select Language Pack` to display the list of available language packs.



Genesys Installation Wizard

Language Pack Selection

Select the option below to install a Language Pack. If you select this option, the Workspace Desktop Edition will install selected language pack on this host.

☑ Select Language Pack

Chinese (Simplified)
French (France)
German (Germany)
Italian (Italy)
Japanese
Korean
Portuguese (Brazilian)
Russian
Spanish (Latin American)
Turkish

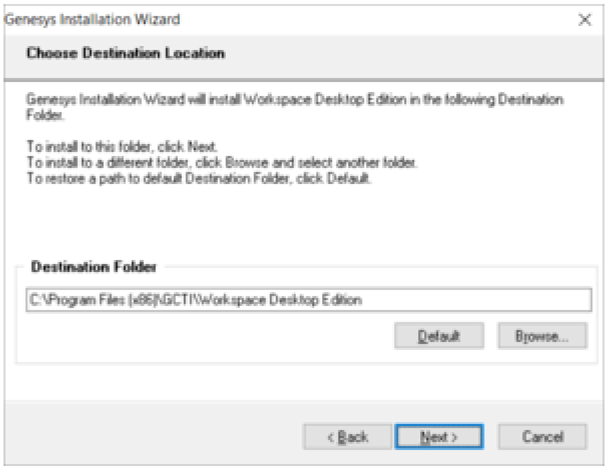
German (Germany)
Japanese

Adding and Removing languages by using the Language Pack Selection panel of the Genesys Installation Wizard

To select a language for installation, select it in the left hand box then click **Add**. The language is moved to the right hand box. To de-select a language for installation, select it and click **Remove**. The language is moved back to the left hand box and will not be installed. After you have added to the right hand box the languages that you want to install, do one of the following:

- Click `Next` to continue the installation procedure.
- Click `Back` to return to the `Select Options` panel.
- Click `Cancel` to exit the Genesys Installation Wizard.

6. On the `Choose Destination Location` panel, specify the location on your web server in which Workspace is to be installed by doing one of the following:
   - Type a location in the `Destination Folder` text box.
   - Click `Default` to reset the location to the default location.
   - Click `Browse` to navigate to a destination folder.



Genesys Installation Wizard

Choose Destination Location

Genesys Installation Wizard will install Workspace Desktop Edition in the following Destination Folder.

To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
To restore a path to default Destination Folder, click Default.

Destination Folder

C:\Program Files (x86)\GCTI\Workspace Desktop Edition

Choose Destination Location panel of the Genesys Installation Wizard

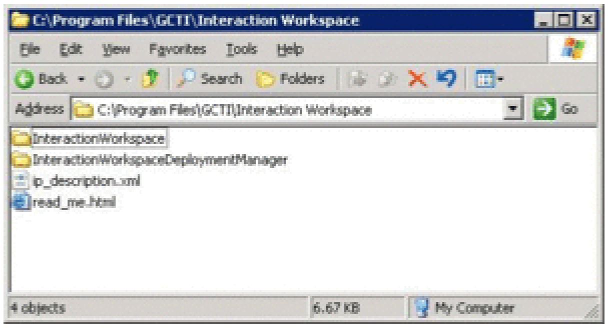
7. With the destination folder specified, do one of the following:
   - Click `Next`.
   - Click `Back` to return to the `Select Options` panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.

   If you clicked `Next`, the `Ready to Install` panel is displayed.
8. On the `Ready to Install` panel, do one of the following:
   - Click `Install` to install Workspace on your web server.
   - Click `Back` to return to the `Choose Destination Location` panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.

If you clicked `Next`, Workspace is installed in the location that you specified. When installation is complete, the `Installation Complete` panel is displayed.

The Figure - **Workspace content installed on the web-server host or workstation** shows the files that are installed by the `Prepare a ClickOnce` package option (for more information about installation options, see the Table - **Workspace Install Mode Deployment Packages**).

- The `Workspace Desktop Edition` folder contains the Interaction Workspace application files.
- The `WorkspaceDeploymentManager` folder contains the application files required for deployment, including the Deployment Manager application: `InteractionWorkspaceDesktop.exe`. This folder contains the following subfolder:
  - `WebPublication`—Contains the `publish.htm` and `setup.exe` (the bootstrap for client-side prerequisites). For more information, see the Procedure: Deploy the Workspace downloadable ClickOnce package on your web server.


C:\Program Files\GCTI\Interaction Workspace
File Edit View Favorites Tools Help
Back Search Folders
Address
Go

C:\Program Files\GCTI\Interaction Workspace

InteractionWorkspace
InteractionWorkspaceDeploymentManager
ip_description.xml
read_me.html

4 objects 6.67 KB My Computer

Workspace content installed on the web-server host or workstation

9. Click `Finish` to exit the Genesys Installation Wizard.

2. Install the optional SIP endpoint and plugins

## [+] (optional) Procedure: Installing the Workspace SIP Endpoint

[**Modified:** 8.5.109.16, 8.5.114.08]

The Workspace SIP Endpoint is an optional plug-in or standalone application for Workspace. It is available as a separate IP that you install from a separate CD/DVD. You can install it in one of two modes, as a plugin that runs with Workspace Desktop Edition on the agent workstation, or as a standalone application that connects to Workspace running in a virtualized environment.

> ### Tip
> Workspace also supports the Genesys Softphone in place of Workspace SIP Endpoint. To learn about the installation of Genesys Softphone, see Deploying Genesys Softphone in the Genesys Softphone Deployment Guide.

If you intend to create a ClickOnce package to install Workspace SIP Endpoint, install the Workspace SIP Endpoint *after* you install the Workspace application on your server, but before you run the Workspace Deployment Manager.

If you deploy Workspace SIP Endpoint as part of a ClickOnce deployment, the behavior of the ClickOnce download depends on the privileges that are assigned to the agent who is logging in. If the agent is granted the privilege to execute a local Workspace SIP Endpoint, the following files are downloaded to the agent workstation:

- The SIP Endpoint Communication plug-in (part of Workspace runtime)
- The Workspace SIP Endpoint executable and associated assemblies.

# Installing Workspace SIP Endpoint as a Workspace Desktop Edition plugin

Use the following procedure to install Workspace SIP Endpoint in environments where the Workspace application and Workspace SIP Endpoint run on the same workstation. Use the Installing the Standalone Workspace SIP Endpoint when you are running Workspace in a virtualized environment.

## Procedure

### Installing the Workspace SIP Endpoint as a Workspace Desktop Edition plugin

**Purpose:** To install the Workspace SIP Endpoint on your web server, an agent workstation, or a development workstation as a plugin.

**Prerequisites**

- .NET Framework 4.5
- The following Microsoft redistributable package(s) is/are required to be installed on the workstation where Workspace SIP Endpoint will execute. They are installed by the Installation Package if they are not already present on the target workstation, but if you are deploying Workspace and Workspace SIP Endpoint by using ClickOnce, you must plan the installation of the following packages on those workstations prior to enabling the ClickOnce deployment:
  - For 8.5.114.xx and higher
    - Visual C++ Redistributable for Visual Studio 2013: http://download.microsoft.com/download/2/E/6/2E61CFA4-993B-4DD4-91DA-3737CD5CD6E3/vcredist_x86.exe
  - For 8.5.104.xx to 8.5.113.xx:
    - Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package MFC Security Update: http://download.microsoft.com/download/8/B/4/8B42259F-5D70-43F4-AC2E-4B208FD8D66A/vcredist_x86.EXE
    - Visual C++ Redistributable for Visual Studio 2013: http://download.microsoft.com/download/2/E/6/2E61CFA4-993B-4DD4-91DA-3737CD5CD6E3/vcredist_x86.exe
  - 8.5.103.xx and lower:
    - Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package MFC Security Update: http://download.microsoft.com/download/8/B/4/8B42259F-5D70-43F4-AC2E-4B208FD8D66A/vcredist_x86.EXE
    - Visual C++ Redistributable for Visual Studio 2012 Update 4, 32-bits package only: http://www.microsoft.com/en-us/download/details.aspx?id=30679
- Install the Workspace application by using one of the following procedures:
  - Deploying The ClickOnce Application On Your Web Server. Choose this option if you want to deploy Workspace as a ClickOnce application.
  - Installing The Workspace Developer Toolkit. Choose this option if you want to deploy the Workspace developer package.
  - Installing The Workspace Application. Choose this option if you want to deploy a non-ClickOnce version of Workspace.

### Start

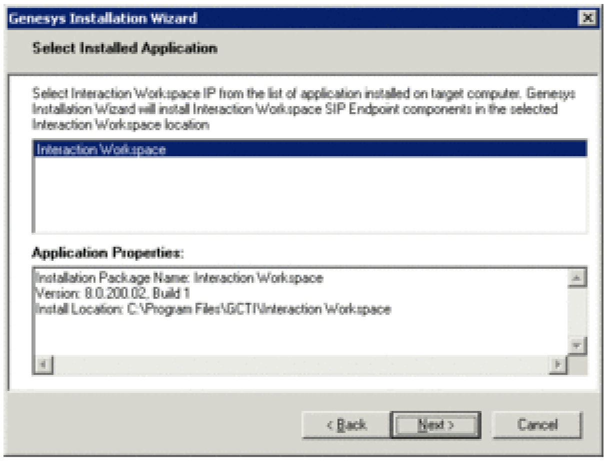
1. On your desktop, open the Workspace SIP Endpoint disc or the Workspace SIP Endpoint IP and double-click the Setup.exe file.

   You might be asked to reboot your system to delete or rename certain system files before the Installation Wizard runs.

   The Genesys Installation Wizard launches and the Welcome panel is displayed.

2. On the Welcome panel, do one of the following:
   - Click Next to begin the installation procedure.
   - Click Cancel to exit the Genesys Installation Wizard.
   - Click About to open the Workspace SIP Endpoint ReadMe in your default browser.

   If you clicked Next, the Select Installed Application panel is displayed (see the Figure - **Select Installed Application Panel of the Genesys Installation Wizard**).

   Genesys Installation Wizard

   Select Installed Application

   Select Interaction Workspace IP from the list of application installed on target computer. Genesys Installation Wizard will install Interaction Workspace SIP Endpoint components in the selected Interaction Workspace location

   Interaction Workspace

   Application Properties:

   Installation Package Name: Interaction Workspace
   Version: 8.0.200.02, Build 1
   Install Location: C:\Program Files\GCTI\Interaction Workspace

   Select Installed Application Panel of the Genesys Installation Wizard

3. The Select Installed Application panel enables you to select the Workspace application instance to which you want to add Workspace SIP Endpoint as a plug-in.

   The Genesys Installation Wizard searches the target computer for an installed version of Workspace. Select the version of Workspace in the location in which you want Workspace SIP Endpoint to be installed.

   The Application Properties pane displays the name, version, and location of the selected Workspace application (see the Figure - **Select Installed Application Panel of the Genesys Installation Wizard**).

4. After you have selected the version of Workspace that you want to use with Workspace SIP Endpoint, do one of the following:
   - Click Next to proceed to the next panel.
   - Click Cancel to exit the Genesys Installation Wizard.
   - Click Back to return to the previous panel.

   If you clicked Next, the Ready to Install panel is displayed.

5. On the Ready to Install panel do one of the following:
   - Click Install to install Workspace SIP Endpoint on your web server, development workstation, or agent workstation.
   - Click Back to return to the Select Installed Application panel.

- Click `Cancel` to exit the Genesys Installation Wizard.

If you clicked `Next`, Workspace SIP Endpoint is installed in the location that you specified. When installation is complete, the `Installation Complete` panel is displayed.

6. Click `Finish` to exit the Genesys Installation Wizard.

   A folder that is named `InteractionWorkspaceSIPEndpoint` is created in the `Workspace` folder. The `InteractionWorkspaceSIPEndpoint` folder contains the Workspace SIP Endpoint application and associated files.

   After the Workspace SIP Endpoint application is installed on the agent or developer workstation, or after it is downloaded by the ClickOnce application (see Deploying The ClickOnce Application On Your Web Server), and after the agent is granted permission to use the application, agents must login Workspace on a Place that is associated with a SIP DN to start the Workspace SIP Endpoint. The Workspace SIP Endpoint process is started automatically when Workspace application is being initialized.

7. To ensure that the supporting programs were installed correctly, check if the following programs are available in the "uninstall programs" view of the Control Panel on your Windows workstation:
   - Genesys Workspace SIP Endpoint <version>
   - Microsoft Visual C++ 2005 Redistributable (8.5.113.xx and lower)
   - Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.60.610

## [+] (optional) Procedure: Installing plugins for Workspace

Workspace enables you to install optional plug-ins for Workspace. Plug-ins, such as eServices Social Media interaction handling, are available as separate IPs that you install from a separate CD/DVD.

If you deploy a plug-in as part of a ClickOnce deployment, the behavior of the ClickOnce download depends on the privileges that are assigned to the agent who is logging in. If the agent is granted the privilege to execute a plug-in, the plug-in is downloaded as part of the deployment.

The Procedure: Installing plug-ins for Workspace is a general procedure that describes how to install plug-ins for Workspace. The documentation for your plug-in provides specific information about how to install and deploy your plug-in.

**Consult the documentation that comes with your plug-in for specific information about how to install and provision your plug-in.**

Before you install your plug-in, you must provision it in Genesys Administrator Extension (refer to the Genesys Administrator Extension documentation for more information) in the same way that you provision Workspace.

Workspace plug-ins come with `<Plug-In Name>.apd` and `<Plug-In Name>.xml` (privileges) files, both of type `Workspace`. Upload the `<Plug-In Name>.apd` file and attach the `<Plug-In Name>.xml` file to create the `<Plug-In Name> Template`.

The Workspace application object is created based on the `Workspace Template`.

When you provision the Privileges that are assigned to a Role, the list of Privileges that are available for the `Workspace` application type combine the privileges that are specified in the `Workspace.xml` and `<Plug-In Name>.xml` files.

## Important

Ensure that you do not use the template and metadata files "Workspace (Agent desktop).apd" and "Workspace (Agent desktop).xml" when working with plug-ins.

## Procedure

### Installing plug-ins for Interaction Workspace

**Purpose:**

To install plug-ins for Workspace on your web server, an agent workstation, or a development workstation.

**Prerequisites**

- .NET Framework 4.5
- Installation of the Workspace application by using one of the following procedures:
  - Deploying The ClickOnce Application On Your Web Server. Choose this option if you want to deploy Workspace as a ClickOnce application. Install the plug-ins after you install the Workspace application on your server, but before you run the Workspace Deployment Manager.
  - Installing The Developer Toolkit. Choose this option if you want to deploy the Workspace developer package. Refer to About Workspace Extension Samples and Deploying and Executing the Extension Samples for information about reorganizing files to enable the debugging of samples with plug-ins.
  - Installing The Workspace Application. Choose this option if you want to deploy a non-ClickOnce version of Workspace.

**Start**

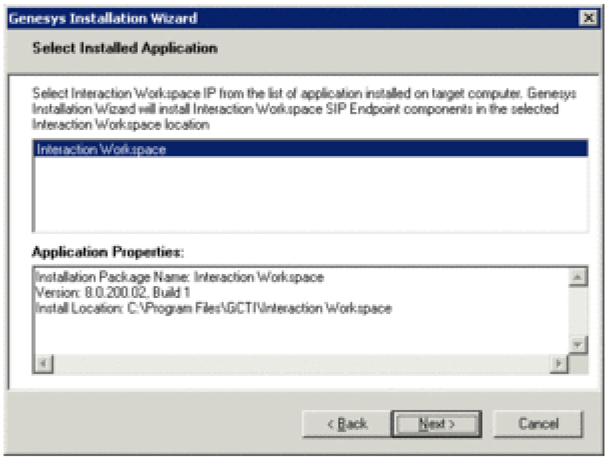
1. On your desktop, open the disc that contains the plug-in IP or the plug-in IP and double-click the `Setup.exe` file.

   You might be asked to reboot your system to delete or rename certain system files before the Installation Wizard runs.

   The Genesys Installation Wizard launches and the `Welcome` panel is displayed.

2. On the `Welcome` panel, do one of the following:
   - Click `Next` to begin the installation procedure.
   - Click `Cancel` to exit the Genesys Installation Wizard.
   - Click `About` to open the plug-in ReadMe in your default browser.

   If you clicked `Next`, the `Select Installed Application` panel is displayed (see the Figure - **Select Installed Application Panel of the Genesys Installation Wizard**).



Select Installed Application

Select Interaction Workspace IP from the list of application installed on target computer. Genesys Installation Wizard will install Interaction Workspace SIP Endpoint components in the selected Interaction Workspace location

Interaction Workspace

Application Properties:

Installation Package Name: Interaction Workspace
Version: 8.0.200.02, Build 1
Install Location: C:\Program Files\GCTI\Interaction Workspace

Select Installed Application Panel of the Genesys Installation Wizard

3. The `Select Installed Application` panel enables you to select the Workspace application instance to which you want to add the plug-in.

   The Genesys Installation Wizard searches the target computer for an installed version of Workspace. Select the version of Workspace in the location in which you want plug-in to be installed.

   The `Application Properties` pane displays the name, version, and location of the selected Workspace application (see the Figure - **Select Installed Application Panel of the Genesys Installation Wizard**).

4. After you have selected the version of Workspace that you want to use with the plug-in, do one of the following:

   - Click `Next` to proceed to the next panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.
   - Click `Back` to return to the previous panel.

   If you clicked `Next`, the `Ready to Install` panel is displayed.

5. On the `Ready to Install` panel do one of the following:

   - Click `Install` to install the plug-in on your web server, development workstation, or agent workstation.
   - Click `Back` to return to the `Select Installed Application` panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.

   If you clicked `Next`, plug-in is installed in the location that you specified. When installation is complete, the `Installation Complete` panel is displayed.

6. Click `Finish` to exit the Genesys Installation Wizard.

   Plug-in files are copied into the target installation directory of the original Workspace deployment.

   After the plug-in application is installed on the agent or developer workstation, or after it is downloaded by the ClickOnce application (see Deploying The ClickOnce Application On Your Web Server), and after the agent is granted permission to use the application, agents must login Workspace on a Place that is associated with a SIP DN to use the plug-in with Workspace. The plug-in process is started automatically when Workspace application is being initialized.

**End**

> Tip
>
> If you did not add Language Packs in the previous step, you can perform a manual installation at this point by using the manual procedure.

### 3. Deploy the ClickOnce application on your web server

Use the Workspace Deployment Manager wizard or console to generate the file hierarchy that is required by the ClickOnce application on your web server.

During the deployment of the ClickOnce application, you are required to enter the following information in the Deployment Manager wizard (this information also has to be added to the `silent.xml` file to be used by the console):

- The deployment URL
- The deployment version
- The deployment certificate:
  - If you do have a deployment certificate, select the `Sign with a provided certificate` option, and then browse to select the certificate. You must also input the password in the dedicated text box.
  - If you do not have a deployment certificate, do not select the `Sign with a provided certificate` option. Without a signed package, a security warning is displayed whenever the client downloads the package.

Be sure to have this information ready before you begin.

The first two procedures: *Wizard: Deploy the Workspace downloadable ClickOnce package on your web server* or *Console: Deploy the Workspace downloadable ClickOnce package on your web server* contain the deployment steps for deploying Workspace on your web server. Choose which procedure you want to use.

> Tip
>
> You can put the Workspace downloadable package in a shared directory instead of on your web server, and then install Workspace from a shared directory.

Choose one of the following two ways to deploy the ClickOnce application on your Web Server:

## [+] 3a. Wizard: Deploy the Workspace downloadable ClickOnce package on your web server

[**Modified:** 8.5.102.06]

**Purpose:** Deploy the Workspace downloadable package on your web server by using the Workspace Deployment Manager Wizard

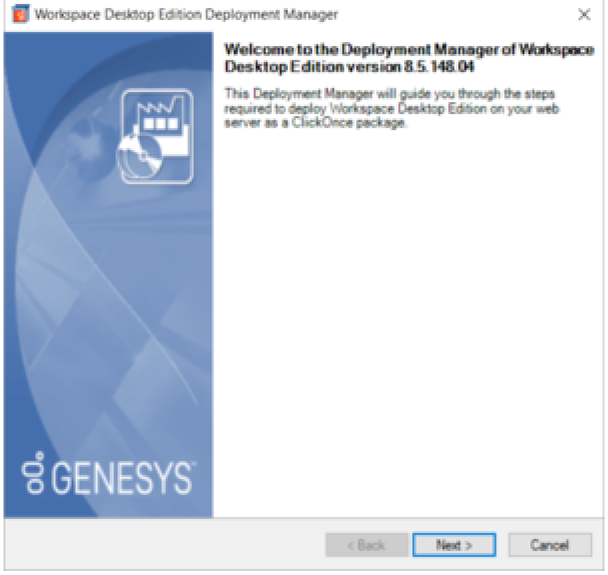
> ### Important
> The following procedure employs a Windows-based Deployment Wizard. If your HTTP server is running on a Solaris or Linux server, you must first build the deployment package on a computer that is running the Windows Operating System, and then copy the package to a compatible location on your Solaris or Linux HTTP server.

### Prerequisites

- Install the Deployment Manager and associated files from the Genesys Workspace disc or download image. See the Procedure: Installing Workspace Deployment Package on the Windows operating system.
- Create an `Application` object of type `Workspace` from the Workspace Application template.
- Microsoft .NET Framework 4.5 installed on the computer on which you run the wizard. This can be the computer on which you run your web server.

### Start

1. Open the `InteractionWorkspaceDeploymentManager` folder. This folder contains the application files required for deployment, including: `InteractionWorkspaceDeploymentManager.exe`.
2. Launch the `InteractionWorkspaceDeploymentManager.exe` application by double-clicking the file or selecting it from the Start menu. The Deployment Manager installs the ClickOnce files on your web server. The `Welcome` pane of the Deployment Manager is displayed (refer to Figure - **The Workspace Deployment Manager splash page**).



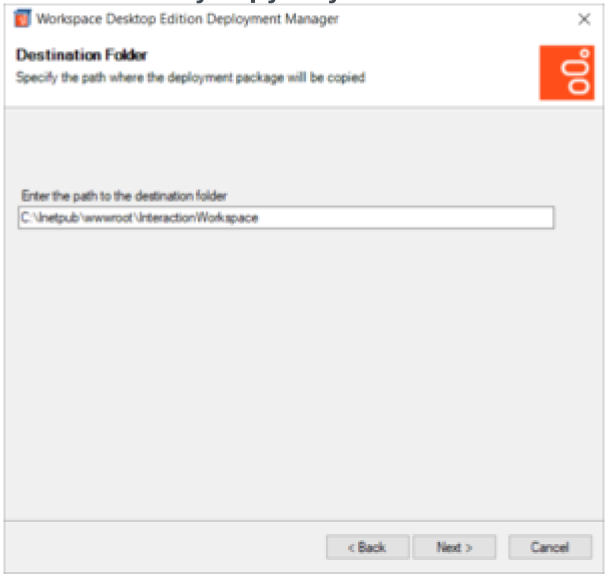
**Welcome to the Deployment Manager of Workspace Desktop Edition version 8.5.148.04**

This Deployment Manager will guide you through the steps required to deploy Workspace Desktop Edition on your web server as a ClickOnce package.

The Workspace Deployment Manager splash page

3. Click `Next` to proceed with the installation. Click `Cancel` to cancel the deployment.
4. If you clicked `Next`, the `Deployment Folder` pane is displayed (refer to Figure - Workspace Deployment Manager Deployment Folder pane**). Specify the location on your server in which you want the ClickOnce files to be deployed. If you are deploying to a Solaris server or a Linux server, specify a local folder on the Windows-based computer on which you are running the**

**Deployment Wizard. From this location, you will build the deployment package that you must manually copy to your Solaris or Linux HTTP server.**



Workspace Desktop Edition Deployment Manager

**Destination Folder**

Specify the path where the deployment package will be copied

Enter the path to the destination folder

C:\Inetpub\wwwroot\InteractionWorkspace

Workspace Deployment Manager Deployment Folder pane

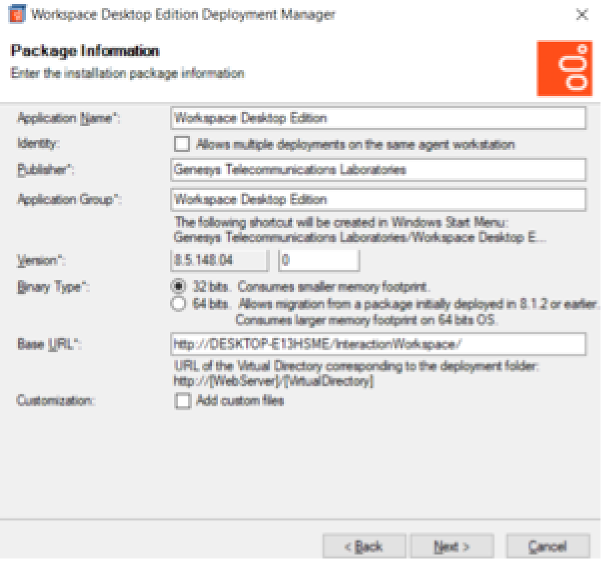
5. Click `Next` to proceed with the installation. Click `Cancel` to cancel the deployment. Click `Back` to return to the previous panel.
6. If you clicked `Next`, the `Package Information` pane is displayed (refer to Figure - Workspace Deployment Manager Package Information pane**). This pane is filled-in automatically. Modify these parameters only if necessary.**

   You can change the application name, the publisher (which is displayed in the `publish.htm` page), and the base URL, which is the URL that corresponds with the virtual directory that is linked to the deployment folder.

   There are one or more optional check boxes that you can use to add plug-ins to the Workspace application:

   - `Add custom files`: Select to add custom content such as simple data files, including rebranding icons or sound files, or file assemblies that implement your Interaction Workspace Customization API.
   - `<plug-in name>`: Select this option to use your installed plug-in, such as Workspace SIP Endpoint, Social Engagement plug-in, Localization Packs, and so on.

   Click `Next` to proceed with the installation. Click `Cancel` to cancel the deployment. Click `Back` to return to the previous panel.



Workspace Desktop Edition Deployment Manager

**Package Information**

Enter the installation package information

Application Name*: Workspace Desktop Edition

Identity: □ Allows multiple deployments on the same agent workstation

Publisher*: Genesys Telecommunications Laboratories

Application Group*: Workspace Desktop Edition

The following shortcut will be created in Windows Start Menu:
Genesys Telecommunications Laboratories/Workspace Desktop E...

Version*: 8.5.148.04 | 0

Binary Type*: ● 32 bits. Consumes smaller memory footprint.
○ 64 bits. Allows migration from a package initially deployed in 8.1.2 or earlier. Consumes larger memory footprint on 64 bits OS.

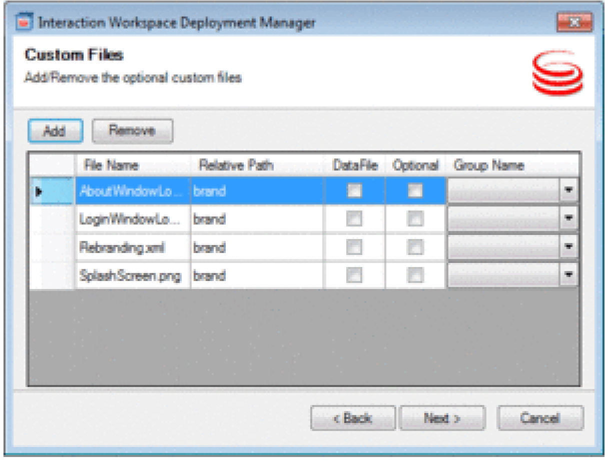
Base URL*: http://DESKTOP-E13HSME/InteractionWorkspace/

URL of the Virtual Directory corresponding to the deployment folder:
http://[WebServer]/[VirtualDirectory]

Customization: □ Add custom files

Workspace Deployment Manager Package Information pane

7. If you clicked Next, and if you selected Add Custom Files in the previous view, the Custom Files panel is displayed (refer to Figure - **Interaction Workspace Deployment Manager Custom Files pane**). This window enables you to add custom content to the out-of-the-box Interaction Workspace.



Interaction Workspace Deployment Manager

**Custom Files**

Add/Remove the optional custom files

| File Name | Relative Path | DataFile | Optional | Group Name |
|---|---|---|---|---|
| AboutWindowLo... | brand | □ | □ | |
| LoginWindowLo... | brand | □ | □ | |
| Rebranding.xml | brand | □ | □ | |
| SplashScreen.png | brand | □ | □ | |

Interaction Workspace Deployment Manager Custom Files pane

- Relative Path: The path where the file will be copied relative to the core Workspace installation directory.
- Data File: Not used — This should be left unchecked.
- Optional: *Must* be checked if the file is part of an optional module that is loaded according to user privileges. A module is considered as optional if the value of the startupLoaded attribute is set to false in the .module.config file, and the same module is associated to a task in the same file.

> ## Important
>
> The .module-config file that core Workspace uses for module declaration, as well as any language dictionary file required by the module, must be specified as NOT optional so that they are loaded unconditionally at Workspace start-up.

- Group Name: For mandatory files (files that have Optional unchecked), always specify Core. For optional files, specify the group name that is assigned to the module description in the .module-config file by the clickOnceGroupsToDownload attribute. For example:

```
<task name="InteractionWorkspace.Custom.ThePrivilege"
 clickOnceGroupsToDownload="TheGroup"
 modulesToLoad="TheModule" />
```

The following table provides examples of settings for a typical optional module comprising a DLL, a dictionary file, and a .module-config file:

| File Name | Relative Path | Data File | Optional | Group Name |
|---|---|---|---|---|
| .module-config file | <empty> | unchecked | unchecked | Core |
| .dll file | <empty> | unchecked | checked | <custom group> |
| language file (.language-code.country-code.xml) | languages | unchecked | unchecked | Core |

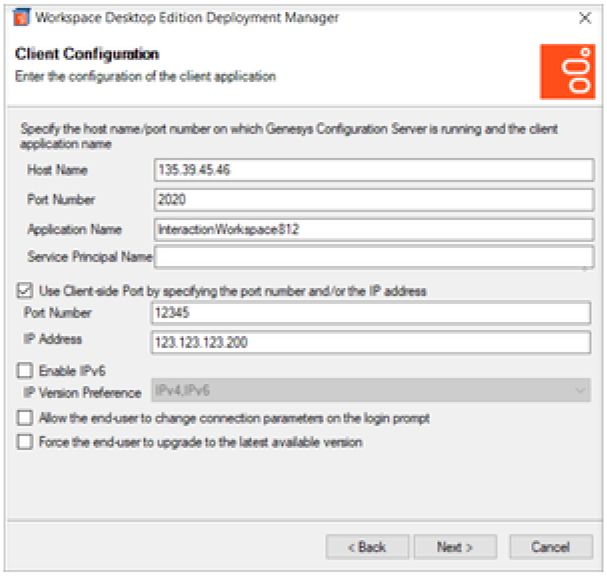
8. Click Next to proceed with the installation. Click Cancel to cancel the deployment. Click Back to return to the previous panel.
9. If you clicked Next, the Client Configuration pane is displayed (refer to Figure - **Workspace Deployment Manager Client Configuration pane**). In this pane, provide the following information:

- The address and port number of your local Genesys Configuration Server
- The name of the Interaction Workspace (client) application that you created in the Configuration Layer by using Genesys Administrator Extension
- (optional) To use Kerberos Single Sign-on (SSO), specify the Service Principal Name (SPN) **Enabling Client-side Port Definition:** To define the client-side port functionality, check Use Client-side Port by specifying the port number and/or the IP address. Checking this option enables the following two text fields: [**Modified:** 8.5.101.14]
- Port Number: The port number that a client will use to make a TCP/IP connection to Configuration Server. If the value is empty, this parameter is not used.
- IP Address: The IP address or the host name that a client will use to make a TCP/IP connection to Configuration Server. If the value is empty, this parameter is not used.

If you specify one or both values, they will be set in the InteractionWorkspace.exe.config file.

There are two additional options in this dialog box:

- Allow the end-user to change connection parameters on the login prompt: Enables agents to change their connection parameters when they log in.
- Force the end-user to upgrade to the latest available version: Disables the ability for agents to reject application updates that are pushed to agents.



**Client Configuration**

Enter the configuration of the client application

Specify the host name/port number on which Genesys Configuration Server is running and the client application name

Host Name: 135.39.45.46

Port Number: 2020

Application Name: InteractionWorkspace812

Service Principal Name:

☑ Use Client-side Port by specifying the port number and/or the IP address

Port Number: 12345

IP Address: 123.123.123.200

□ Enable IPv6

IP Version Preference: IPv4,IPv6

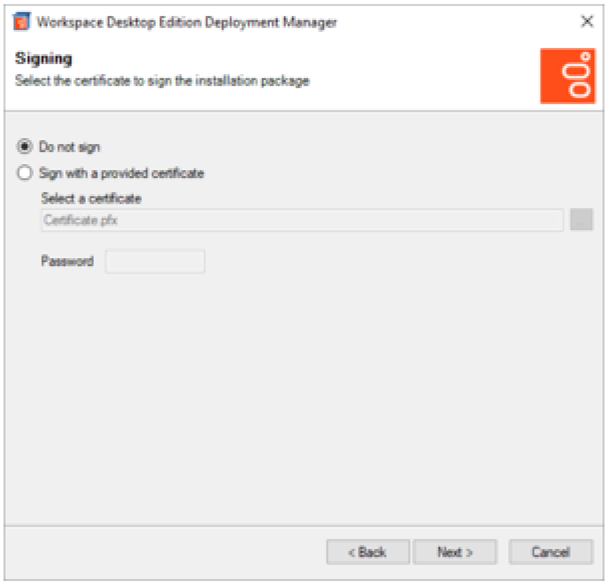
□ Allow the end-user to change connection parameters on the login prompt

□ Force the end-user to upgrade to the latest available version

Workspace Deployment Manager Client Configuration pane

10. Click Next to proceed with the installation. Click Cancel to cancel the deployment. Click Back to return to the previous panel.
11. If you clicked Next, the Signing pane is displayed (refer to Figure - **Workspace Deployment Manager Signing pane**). For more information about how to create or obtain a signing certificate, refer to the "ClickOnce Deployment and Authenticode" page on the Microsoft Developer Network web site:

    http://msdn.microsoft.com/en-us/library/ms172240.aspx



**Signing**

Select the certificate to sign the installation package

● Do not sign

○ Sign with a provided certificate

Select a certificate

Certificate.pfx

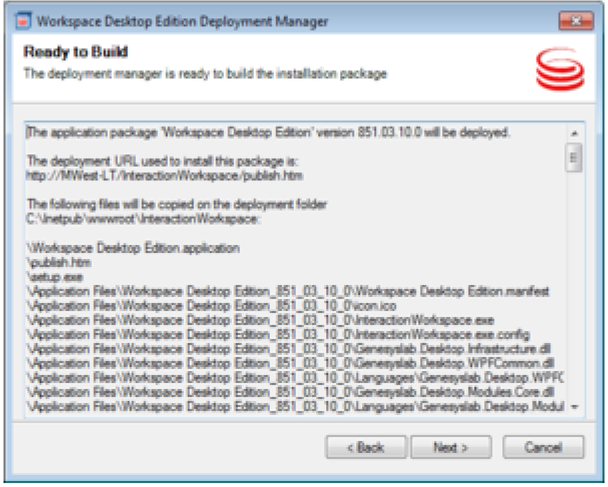
Password

Workspace Deployment Manager Signing pane

12. Choose the type of signing certificate that you are using:
    - Click Do not Sign. If you do not provide a certificate, a security warning is displayed whenever the client downloads the package.

- Click Sign with a provided certificate to enable the Selects a certificate field.

13. Click the browse button to navigate to the certificate.
14. Enter the password for the certificate in the Password field.
15. Click Next to proceed with the installation. Click Cancel to cancel the deployment. Click Back to return to the previous panel.
16. If you clicked Next, the Ready to Build pane is displayed (refer to Figure - **Workspace Deployment Manager Ready to Build pane**). This pane contains a summary of the files that will be deployed on your web server and a confirmation of the deployment URL.



Ready to Build

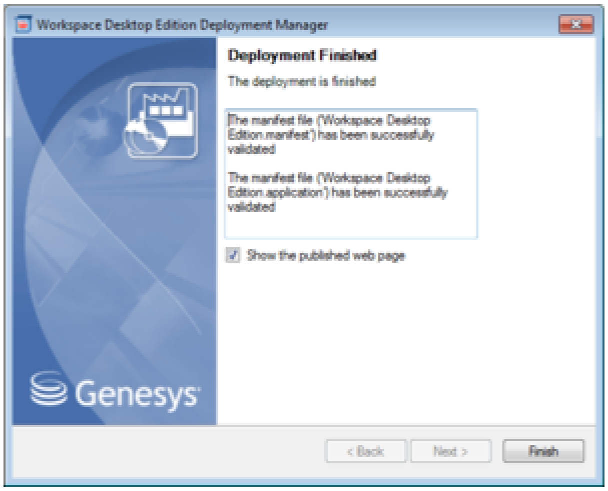
The deployment manager is ready to build the installation package

```
The application package 'Workspace Desktop Edition' version 851.03.10.0 will be deployed.

The deployment URL used to install this package is:
http://MWest-LT/InteractionWorkspace/publish.htm

The following files will be copied on the deployment folder
C:\inetpub\wwwroot\InteractionWorkspace:

\Workspace Desktop Edition.application
\publish.htm
\setup.exe
\Application Files\Workspace Desktop Edition_851_03_10_0\Workspace Desktop Edition.manifest
\Application Files\Workspace Desktop Edition_851_03_10_0\icon.ico
\Application Files\Workspace Desktop Edition_851_03_10_0\InteractionWorkspace.exe
\Application Files\Workspace Desktop Edition_851_03_10_0\InteractionWorkspace.exe.config
\Application Files\Workspace Desktop Edition_851_03_10_0\Genesyslab.Desktop.Infrastructure.dll
\Application Files\Workspace Desktop Edition_851_03_10_0\Genesyslab.Desktop.WPFCommon.dll
\Application Files\Workspace Desktop Edition_851_03_10_0\Languages\Genesyslab.Desktop.WPFC
\Application Files\Workspace Desktop Edition_851_03_10_0\Genesyslab.Desktop.Modules.Core.dll
\Application Files\Workspace Desktop Edition_851_03_10_0\Languages\Genesyslab.Desktop.Modul
```

Interaction Workspace Deployment Manager Ready to Build pane

17. Click Next to complete the deployment. Click Cancel to cancel the deployment. Click Back to modify any of the previous panes.
18. If you clicked Next, the Deployment Manager deploys the Workspace ClickOnce application in the path that you specified at the beginning of the wizard execution. This can be the appropriate place on your web server.

When the deployment is complete, the Deployment Finished pane is displayed (refer to Figure - **Workspace Deployment Manager Deployment Finished pane**). This pane contains messages that relate to the success of the deployment.



Deployment Finished

The deployment is finished

The manifest file ('Workspace Desktop Edition.manifest') has been successfully validated

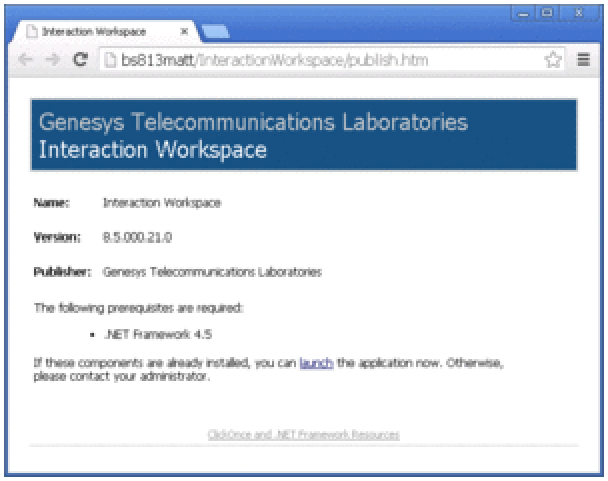
The manifest file ('Workspace Desktop Edition.application') has been successfully validated

☑ Show the published web page

Interaction Workspace Deployment Manager Deployment Finished pane

19. Click Finish to close the Workspace Deployment Manager.

    Deployment proceeds. When deployment is complete, the publish.htm web page is opened in your default browser automatically (refer to Figure - **Workspace pubish.htm web page viewed through Microsoft Internet Explorer**).

    Genesys Telecommunications Laboratories
    Interaction Workspace

    **Name:** Interaction Workspace

    **Version:** 8.5.000.21.0

    **Publisher:** Genesys Telecommunications Laboratories

    The following prerequisites are required:

    - .NET Framework 4.5

    If these components are already installed, you can launch the application now. Otherwise, please contact your administrator.

    ClickOnce and .NET Framework Resources

    Interaction Workspace pubish.htm web page viewed through Microsoft Internet Explorer

    The publish.htm web page confirms that the Workspace package is published and provides you with the version number.

    If you have not installed the prerequisites, the page contains a link to the prerequisite installers.

20. If you are deploying on a Solaris or Linux HTTP server, copy the collection of files that was created by the Deployment Wizard on your Windows-based computer to your HTTP server.

**End**

**Next Steps**

- If you have not installed the prerequisites, in the publish.htm web page, click Install to launch setup.exe to install the prerequisite installers.
- If you already have installed the prerequisites, the application bootstrap either installs a new version automatically, upgrades your existing version, if necessary, or starts the application, if it is installed and up to date.

## [+] 3b. Console: Deploy the Workspace downloadable ClickOnce package on your web server

**Purpose:** Deploy the Workspace downloadable package on your web server by using the Workspace Deployment Manager Console (silent deployment).

> Important
>
> The console mode enables administrators and solution designers to create a script-based ClickOnce deployment to automate deployment.

### Prerequisites

- Install the Deployment Manager and associated files from the Genesys Workspace disc or download image. See the Procedure: Installing Workspace Deployment Package on the Windows operating system.
- Create an `Application` object of type `Workspace` from the Workspace Application template.
- Microsoft .NET Framework 4.5 installed on the computer on which you run the wizard. This can be the computer on which you run your web server.

### Start

1. Open the `WorkspaceDeploymentManager` folder. This folder contains the application files required for deployment.
2. Edit the `silent.xml` file (refer to an example below) to include the deployment parameters that you require, including any custom files (custom plugins) you want to install. The **Table - The deployment attributes that are contained in silent.xml file** describes the parameters that you can specify.
3. Launch the `InteractionWorkspaceDeploymentManager.exe` application by using a command line like the following:

   ```
   start /wait interactionworkspacedeploymentmanager.exe -s silent.xml
   ```

   The following Command Line Arguments are supported:

   - `-s <silent_file_name>`: (mandatory for console execution) This attribute specifies that the deployment manager will execute in console mode, and specifies the configuration file used for execution.
   - `-f <log_file>`: (optional) This attribute specifies the path and the name of the log file printed during the deployment manager execution.

   Use the command `start /wait` if you want the script to wait for end of process execution.
4. If you are deploying on a Solaris or Linux HTTP server, copy the collection of files that was created by the Deployment Wizard on your Windows-based computer to your HTTP server.

### End

### Next Steps

- If you have not installed the prerequisites, in the `publish.htm` web page, click `Install` to launch `setup.exe` to install the prerequisite installers.
- If you already have installed the prerequisites, the application bootstrap either installs a new version automatically, upgrades your existing version, if necessary, or starts the application, if it is installed and up to date.

## The deployment attributes that are contained in silent.xml file

**XML Key Name**: ApplicationToDeploy
Description: The application that Workspace Desktop Edition Deployment Manager will deploy.
If the value is empty or `WorkspaceDesktopEdition`, deployment of Workspace Desktop Edition with or without plug-ins (Workspace SIP Endpoint can be a plug-in in this mode)
If the value is `WorkspaceSIPEndpoint`, deployment of Workspace SIP Endpoint in standalone mode
Default Value:

Example: `WorkspaceSIPEndpoint`

**XML Key Name**: DeploymentDestinationFolder
Description: The path where the Deployment Manager console will copy the built ClickOnce package. This path can be the Production Web Site path or an interim storage from where another utility will have to push the package to the Production Web Site.
Default Value:
Example: c:\temp\depmgr

**XML Key Name**: EndUserConfigureClientSidePort
Description: When set to `true`, the Deployment Manager Console populates the client-side port/address in the property file that is deployed with Workspace on the destination workstation.
Default Value: false
Example:

**XML Key Name**: EndUserClientSideTransportAddress
Description: The Client-Side Address that the deployed Workspace application will use to connect to Configuration Server.
Default Value:
Example: 123.123.123.200

**XML Key Name**: EndUserClientSideTransportPort
Description: The Client-Side Port that the deployed Workspace application will use to connect to Configuration Server.
Default Value:
Example: 12345

**XML Key Name**: EndUserConfigAllowUserToChangeConnectionParameters
Description: When set to `true`, the Configuration Server Host, Port, and Application Name can be edited in the login window of the deployed Workspace application (if the user clicks `More`).
When set to `false`, the application will always use the parameters that are configured in this file.
Default Value: false
Example:

**XML Key Name**: EndUserConfigApplicationName
Description: The Application Name that the deployed Workspace application will use to connect to Configuration Server.
Default Value:
Example: InteractionWorkspace850

**XML Key Name**: EndUserConfigHost
Description: The Host Name that the deployed Workspace application will use to connect to Configuration Server.
Default Value:
Example: <your host name>

**XML Key Name**: EndUserConfigPort
Description: The Port that the deployed Workspace application will use to connect to Configuration Server.
Default Value:
Example: 2021

**XML Key Name**: InformationApplicationName
Description: Name of the ClickOnce package.
The name of the `.application` file to be downloaded on the target workstation.

The icon on the target workstation desktop will have this name.
Default Value: Workspace
Example:

**XML Key Name**: InformationPublisher
Description: The name of the company that delivers the ClickOnce package.
Default Value:
Example: Genesys Telecommunications Laboratories, Inc

**XML Key Name**: InformationURL
Description: The URL Root from which the final ClickOnce package will be downloaded by end users.
Default Value:
Example: http://<your host name>/InteractionWorkspace

**XML Key Name**: OptionsAllowsMultiDeployment
Description: When set to `true`, the ClickOnce package is built to allow distinct ClickOnce packages instances to be installed on the same target destination.
Default Value: false
Example:

**XML Key Name**: OptionsAllowUpgradeFrom812VersionsEndEarlier
Description: When set to `false`, the ClickOnce package includes a 32-bit version of the Workspace executable. This is the default mode when using a regular IP, and this is the recommended mode to optimize the memory footprint on an agent workstation.
The value `true` is required only if you deployed the ClickOnce packages with 8.1.2 versions or earlier and want to ensure a smooth upgrade without first uninstalling old versions. This deploys a 64-bit enabled .NET executable, which can run on a 32-bit OS, and which consumes a significantly higher memory footprint than a 32-bit-only executable when running on a 64 bits OS.
Default Value: false
Example:

**XML Key Name**: PackagesToDeploy
Description: The list of optional file packages ("plug-ins") to be included in the ClickOnce package.
Default Value:
Example: Sip Endpoint;Language Pack for French (France)

**XML Key Name**: SigningCertificateFileName
Description: The path to the certificate to be used to sign the package.
Default Value:
Example: c:\inetpub\InteractionWorkspace

**XML Key Name**: SigningPassword
Description: The password that is required to sign the ClickOnce package with the selected certificate.
Default Value:
Example: abcd

**XML Key Name**: SigningSignsWithProvidedCertificate
Description: When set to `true`, the Deployment Manager Console attempts to sign the ClickOnce package with the provided signing data.
Default Value: false
Example:

[**Added:** 8.5.102.06]

**XML Key Name**: EndUserConfigServicePrincipalName
Description: Specifies the Service Principal Name to support Kerberos Single Sign On.
Default Value: ""
Example:

[**Added:** 8.5.101.14]

**XML Key Name**: EndUserConfigForceUpgrade
Description: Specify whether agents can reject ClickOnce upgrades when they are presented at login time. When set to `true`, agents are forced to upgrade to this new version of the application at next application start. When set to `false`, agents are prompted with the choice to upgrade immediately or later.
Default Value:`false`
Example:

The following is an example of a `silent.xml` file (refer to procedure 1b):

```
<?xml version="1.0" encoding="windows-1250"?>

<configuration>

 <InformationApplicationName>Interaction Workspace</InformationApplicationName>

 <InformationURL>http://BLSHGS1/InteractionWorkspace</InformationURL>

 <InformationPublisher>Genesys Telecommunications Laboratories</InformationPublisher>

 <DeploymentDestinationFolder>c:\temp\depmgr</DeploymentDestinationFolder>

 <SigningSignsWithProvidedCertificate>false</SigningSignsWithProvidedCertificate>

 <SigningCertificateFileName></SigningCertificateFileName>

 <SigningPassword></SigningPassword>

 <EndUserConfigHost>bsgenbruno811</EndUserConfigHost>

 <EndUserConfigPort>2021</EndUserConfigPort>

 <EndUserConfigApplicationName>InteractionWorkspace850</EndUserConfigApplicationName>

 <EndUserConfigureClientSidePort>true</EndUserConfigureClientSidePort>

 <EndUserClientSideTransportAddress>123.123.123.200</EndUserClientSideTransportAddress>

 <EndUserClientSideTransportPort>12345</EndUserClientSideTransportPort>


<EndUserConfigAllowUserToChangeConnectionParameters>false</EndUserConfigAllowUserToChangeConnectionParameters>

 <EndUserConfigAllowFrameworkInstall>false</EndUserConfigAllowFrameworkInstall>

 <EndUserConfigServicePrincipalName>confserv/host:port</EndUserConfigServicePrincipalName>

 <PackagesToDeploy>Sip Endpoint;Language Pack for French (France)</PackagesToDeploy>

 <OptionsAllowsMultiDeployment>false</OptionsAllowsMultiDeployment>


<OptionsAllowUpgradeFrom812VersionsEndEarlier>false</OptionsAllowUpgradeFrom812VersionsEndEarlier>
```

```
 <EndUserConfigForceUpgrade>false</EndUserConfigForceUpgrade>

</configuration>
```

## Adding Custom Files to a console deployment

If you want to add custom files to your Workspace console deployment, such as a custom Workspace plugin, you can edit the `silent.xml` to specify the reference to the plugin deployment file, which describes the list of custom files of the plugin. The deployment file name can be anything, but it must have the file extension `.deployment-config'`.

In step 2 of the **3b. Console: Deploy the Workspace downloadable ClickOnce package on your web server** procedure, edit the **PackagesToDeploy** XML Key Name to specify the `DeploymentName` specified in the `.deployment-config` file that represents your plugin.

Create the `.deployment-config` file of your plugin using code which is similar to the following:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>

    <sectionGroup name="applicationSettings"
type="System.Configuration.ApplicationSettingsGroup, System, Version=2.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089" >
      <section name="DeploymentManager.ApplicationSettings"
type="System.Configuration.ClientSettingsSection, System, Version=2.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089" requirePermission="false" />
    </sectionGroup>
  </configSections>

  <applicationSettings>
    <DeploymentManager.ApplicationSettings>

      <setting name="DeploymentName" serializeAs="String">

<value>theNameOfThePackageThatShowsUpAsPluginInInteractiveModeOrToBePopulatedInPackageToDeployInConsoleMode</va
      </setting>

      <setting name="MandatoryFiles" serializeAs="Xml">
        <value>
          <ArrayOfApplicationFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
            <ApplicationFile FileName="PluginFile1"
RelativePath="emptyForInstallRootOrSubdirectoryName" DataFile="false" EntryPoint="false"
IsMainConfigFile="false" Optional="falseForConditionalByPrivilege"
GroupName="clickOnceGroupsToDownload" />
            <ApplicationFile FileName="PluginFile2AndSoOn"
RelativePath="emptyForInstallRootOrSubdirectoryName" DataFile="false" EntryPoint="false"
IsMainConfigFile="false" Optional="true" GroupName="clickOnceGroupsToDownload" />
          </ArrayOfApplicationFile>
        </value>
      </setting>

    </DeploymentManager.ApplicationSettings>
  </applicationSettings>
</configuration>
```

Change the following placeholders in the code to reflect your specific requirements:

- DeploymentName: The name of the module/plugin as reported in deployment manager (Wizard interface or in silent.xml file)
- ApplicationFile: Must be repeated for each file composing the plugin
  - FileName: Name of the file
  - RelativePath: Relative path of the file inside the plugin. Empty if located with the other core WDE files.
  - Optional: Set to `true` if the plugin should be downloaded only if a specific privilege is required.
  - GroupName: A group name that matches with the one defined in the `.module-config` file of the custom plugin

### 4. Enable the ClickOnce Package on your web server

Choose one of the following procedures depending on the web server in your environment:

## [+] 4a. (For Apache deployments) Configuring Apache to enable the ClickOnce package

**Purpose:**

By default, the Apache web server does not permit the download of documents of specific MIME types. Apache must be configured to enable the ClickOnce package.

**Prerequisites**

- Apache Server 2.x on any Operating System it supports.

**Start**

1. In the `conf/mime.types` file (in the Apache install folder), add the following lines:

   ```
   application/x-ms-application application

   application/x-ms-application manifest

   application/octet-stream deploy
   ```
2. Save the file.

**End**

## [+] 4b. (For IIS Deployments) Configuring Microsoft IIS6 to enable the ClickOnce package

**Purpose:** Microsoft IIS must be configured to enable the ClickOnce package.

**Prerequisites**

- Microsoft IIS on any Operating System it supports

**Start**

1. From Administrative Tools, start Internet Information Services Manager.
2. Right click the tree leaf that represents your server.
3. Select `Properties` from the contextual menu.
4. In the Properties dialog box, click `Mime Types`.
5. Click `New` to add each of the following configuration pairs:

   `.application => application/x-ms-application`

   `.manifest => application/x-ms-application`

   `.deploy => application/octet-stream`
6. Click `OK`.
7. Click `OK` to validate the new MIME types list.

**End**

## 5. Verify your configuration

Verify that Workspace was correctly deployed on your web server and client workstation.

### [+] Procedure: Configuration verification (Testing the client)

**Purpose:**

To ensure that the Workspace application was correctly deployed on your web server and client workstation.

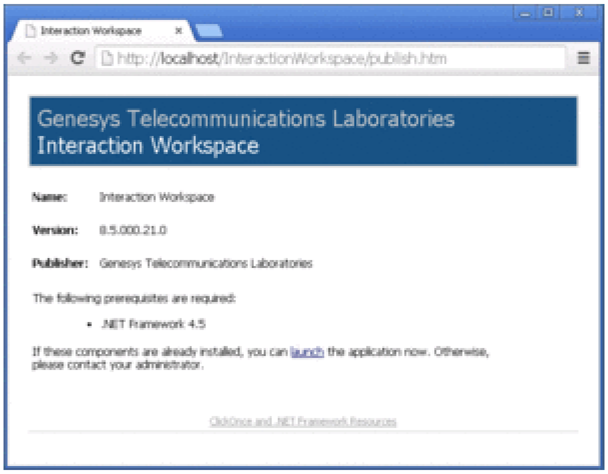
**Start**

1. On a client workstation, open a new Internet browser window.
2. In the `Address` field, enter the URL of the Workspace web application:

   `http://<host>/<application name>/publish.htm`

   For example:

   `http://SUITE80/Workspace/publish.htm`
3. Press `Enter` on your keyboard. The Workspace ClickOnce publish window opens (see the Figure - Workspace publish window).



Genesys Telecommunications Laboratories
Interaction Workspace

**Name:** Interaction Workspace

**Version:** 8.5.000.21.0

**Publisher:** Genesys Telecommunications Laboratories

The following prerequisites are required:

- .NET Framework 4.5

If these components are already installed, you can launch the application now. Otherwise, please contact your administrator.

ClickOnce and .NET Framework Resources

Workspace publish window

This window lists all of the prerequisites that should be installed before you launch Workspace for the first time.

4. If all prerequisites are installed, click `launch` to launch the Workspace installer application.
5. If a security-warning dialog box appears, click `Install`.

   When installation is complete, a shortcut is placed on the desktop, after which the application launches. The Workspace agent-login window is displayed.
6. Enter the following information into the agent-login panel and the connection-parameters panel:
   - `User Name`: A valid user name that is configured in the Configuration Layer
   - `Password`: The valid password for the specified user name
7. Click `Login` to continue logging in to Workspace; click `Cancel` to close the agent-login window without logging in.

   Refer to Workspace User's Guide for more information about how to log in to Workspace and use the application.

**End**

### Next Steps

Installation is complete. You can provision Interaction Workspace functionality:

- Workspace Functionality Overview
- Provisioning Functionality

# Rollback to a previous release of Workspace

## [+] Rollback to a previous release of Workspace by using ClickOnce

**Purpose**:

Rollback the software version installed on the end user (agent) workstation to the previously deployed release of your Workspace package after you have deployed a new version of your Workspace package by using ClickOnce. Here, 'Workspace package' defines the combination of the core Workspace product and the associated customization files.

**Pre-requisites**:

- Identify the out-of-the-box Workspace version that will host the downgrade package (refer to Restriction below).
- Identify the list of custom files (`.dll`, `.module-config`, `.properties`, `.xml` and so on) that comprise the downgrade package.

**Restriction**:

When you activate the **Force upgrade** option of the Deployment Manager, any package version that is downloaded to an end user (agent) workstation requires that the new package version has a version greater than the currently installed one. This means that the procedure above does not allow you to rollback installation on workstations to a version of the out-of-the-box Workspace product that is lower than the currently installed version (as the core Workspace version is used to build the ClickOnce package version). It only allows you to rollback to a previous version of the custom files associated to same of more recent version of out-of-the-box Workspace. To downgrade to an older version of out-of-the-box Workspace, when the **Force upgrade** option has been enabled, an explicit uninstall of the former package on the workstation is required before downloading the older version.

**Start**

1. Navigate to the location where the target out-of-the-box version comprising the downgrade package is available.
2. Execute the Workspace Deployment Manager (console or UI) of the Workspace version that must be part of this rollback.
3. Specify in the wizard execution or in the console configuration file, the list of custom files that must compose the rollback package.
4. Run the Deployment Manager to increment the package build number.
5. After the rollback package is created, push it to the web server.
6. Restart the agent application or, from the **Main Menu** select **Check and Update**. The agent is prompted to update to the new version.

**End**

## Deploying the Developer Toolkit on your development workstation

Use the Procedure: *Installing Workspace Customization on the Windows operating system* to install the Workspace application and Developer's Kit on your development workstation. This procedure installs everything that is required to build and test a Workspace extension. For information about how to build a custom extension or customize Workspace, see the *Workspace 8.5 .NET Developer's Guide & API Reference*.

## Procedure

### Installing Workspace Customization on the Windows operating system

**Purpose:** To install the deployment files for Workspace Customization on your development workstation.

**Prerequisites**

- Preparing The Configuration Layer
- Microsoft Visual Studio 2012, or higher, Express/Community Edition, or above
- .NET Framework 4.5

**Start**

1. On your desktop, open the Workspace disc or the Workspace IP and double-click the Setup.exe file.

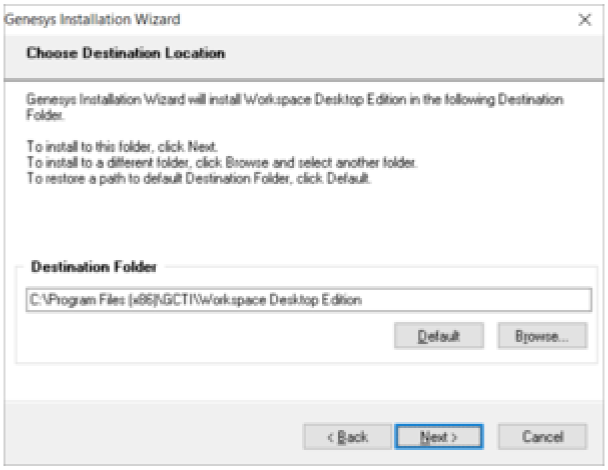
   You might be asked to reboot your system to delete or rename certain system files before the Installation Wizard runs.

   The Genesys Installation Wizard launches and the Welcome panel is displayed.
2. On the Welcome panel, do one of the following:
   - Click Next to begin the installation procedure.
   - Click Cancel to exit the Genesys Installation Wizard.
   - Click About to open the Workspace ReadMe file in your default browser.

   If you clicked Next, the Select Options panel is displayed.
3. On the Select Options panel, do one of the following:
   - Choose Install Interaction Workspace Developer Toolkit, and click Next.
   - Click Back to return to the Welcome panel.
   - Click Cancel to exit the Genesys Installation Wizard.

   For more information on installation options, see the Table - **Workspace Install Mode Deployment Packages**.

   If you clicked Next, the Choose Destination Location panel is displayed (see the Figure - **Choose Destination Location panel of the Genesys Installation Wizard**).



Genesys Installation Wizard

**Choose Destination Location**

Genesys Installation Wizard will install Workspace Desktop Edition in the following Destination Folder.

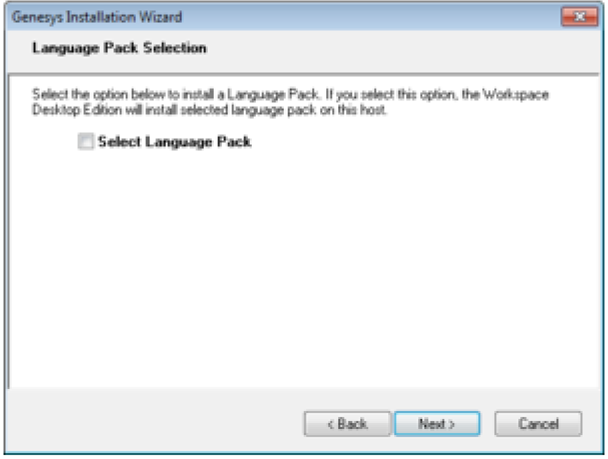
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
To restore a path to default Destination Folder, click Default.

**Destination Folder**

C:\Program Files (x86)\GCTI\Workspace Desktop Edition

Choose Destination Location panel of the Genesys Installation Wizard

4. (Optional) If you are installing from the International DVD, the `Language Pack Selection` panel is displayed.



Genesys Installation Wizard

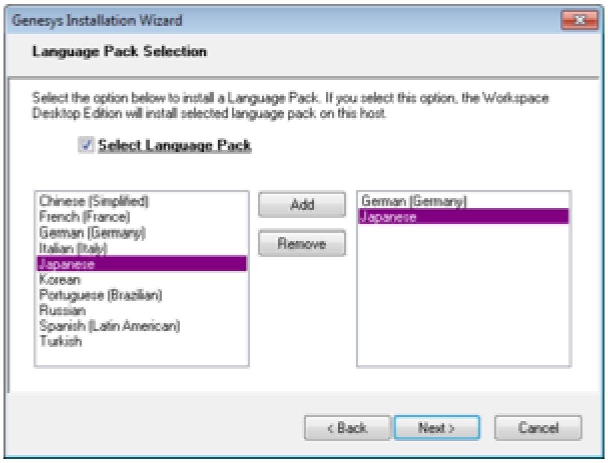
**Language Pack Selection**

Select the option below to install a Language Pack. If you select this option, the Workspace Desktop Edition will install selected language pack on this host.

□ **Select Language Pack**

Language Pack Selection panel of the Genesys Installation Wizard

Select `Select Language Pack` to display the list of available language packs.



Genesys Installation Wizard

**Language Pack Selection**

Select the option below to install a Language Pack. If you select this option, the Workspace Desktop Edition will install selected language pack on this host.

☑ **Select Language Pack**

Chinese (Simplified)
French (France)
German (Germany)
Italian (Italy)
Japanese
Korean
Portuguese (Brazilian)
Russian
Spanish (Latin American)
Turkish

German (Germany)
Japanese

Adding and Removing languages by using the Language Pack Selection panel of the Genesys Installation Wizard

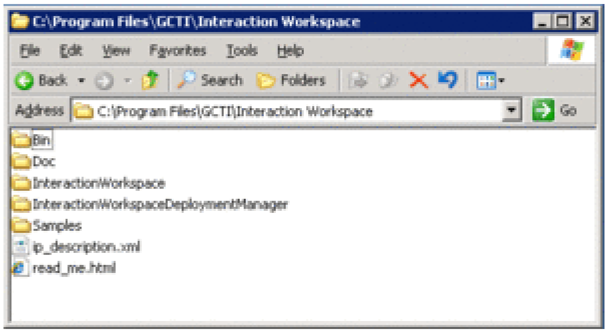
To select a language for installation, select it in the left hand box then click **Add**. The language is moved to the right hand box. To de-select a language for installation, select it and click **Remove**. The language is moved back to the left hand box and will not be installed. After you have added to the right hand box the languages that you want to install, do one of the following:

- Click `Next` to continue the installation procedure.
- Click `Back` to return to the `Select Options` panel.
- Click `Cancel` to exit the Genesys Installation Wizard.

5. On the `Choose Destination Location` panel, specify the location on your development workstation in which the Workspace customization files are to be installed by doing one of the following:
   - Type a location in the `Destination Folder` text box.
   - Click `Default` to reset the location to the default location.
   - Click `Browse` to navigate to a destination folder.
6. With the destination folder specified, do one of the following:
   - Click `Next`.
   - Click `Back` to return to the `Select Options` panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.

   If you clicked `Next`, the `Ready to Install` panel is displayed.
7. On the `Ready to Install` panel do one of the following:
   - Click `Install` to install the Interaction Workspace customization files.
   - Click `Back` to return to the `Choose Destination Location` panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.

If you clicked `Install`, the Workspace customization files are installed in the location that you specified (see the Figure - **Contents of the Workspace install disc or image copied onto the web-server host**).



C:\Program Files\GCTI\Interaction Workspace

Bin
Doc
InteractionWorkspace
InteractionWorkspaceDeploymentManager
Samples
ip_description.xml
read_me.html

Contents of the Workspace install disc or image copied onto the web-server host

The Workspace folder contains the following:

- The `Bin` folder, which contains the Workspace API
- The `Doc` directory, which contains the *Workspace 8.5 .NET Developer's Guide & API Reference* (`WorkspaceSDKNet.chm`)
- The `Workspace` folder, which contains Workspace application files
- The `WorkspaceDeploymentManager` folder, which contains the application files that are required to deploy customized code, including the Deployment Manager application

(InteractionWorkspaceDeploymentManager.exe), and the following subfolder:

  - WebPublication"Contains the publish.htm file.

- The Samples directory, which contains code samples that demonstrate Genesys best-practices recommendations for developers

8. When installation is complete, the Installation Complete panel is displayed.
    - Click Finish to exit the Genesys Installation Wizard.

**End**

**Next Steps**

- (optional) The Procedure: Installing the Workspace SIP Endpoint.
- Refer to the *Workspace 8.5 .NET Developer's Guide & API Reference* for information about how to use the toolkit and samples to customize Workspace.

# Non-ClickOnce deployment

## Installing the Workspace application

Install the out-of-the-box Workspace application on an end-user desktop. The installation contains only the agent application. Use this procedure if you are not going to use the ClickOnce centralized deployment.

## Procedure

### Installing the Workspace application on a client desktop

**Purpose:** To install the Workspace client application on your local agent workstation or virtual machine to test the Workspace application.

**Prerequisites**

- .NET Framework 4.5

**Start**

1. On your desktop, open the Workspace disc or the Workspace IP and double-click the Setup.exe file.

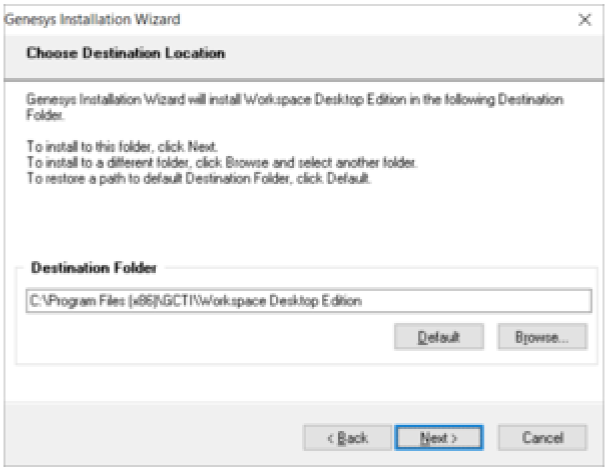
    You might be asked to reboot your system to delete or rename certain system files before the Installation Wizard runs.

    The Genesys Installation Wizard launches, and the Welcome panel is displayed.
2. On the Welcome panel, do one of the following:
    - Click Next to begin the installation procedure.
    - Click Cancel to exit the Genesys Installation Wizard.
    - Click About to open the Workspace ReadMe in your default browser.

If you clicked Next, the Select Options panel is displayed.

3. On the Select Options panel, do one of the following:
    - Choose Install Workspace application, and click Next.
    - Click Back to return to the Welcome panel.
    - Click Cancel to exit the Genesys Installation Wizard.

If you clicked Next, the Choose Destination Location panel is displayed (see the Figure - **Choose Destination Location panel of the Genesys Installation Wizard**).



Genesys Installation Wizard

Choose Destination Location

Genesys Installation Wizard will install Workspace Desktop Edition in the following Destination Folder.

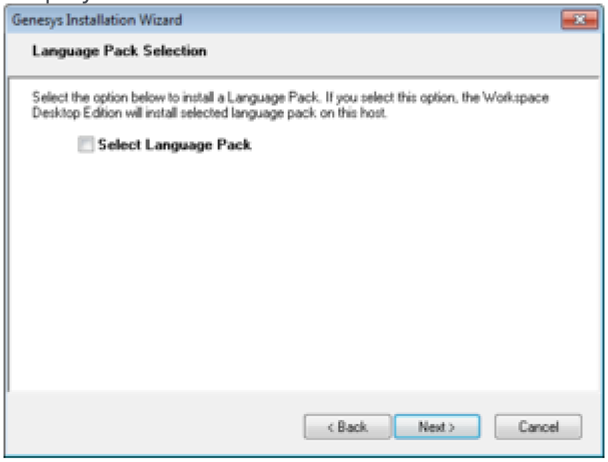
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
To restore a path to default Destination Folder, click Default.

Destination Folder

C:\Program Files (x86)\GCTI\Workspace Desktop Edition

Choose Destination Location panel of the Genesys Installation Wizard

4. (Optional) If you are installing from the International DVD, the Language Pack Selection panel is displayed.



Genesys Installation Wizard

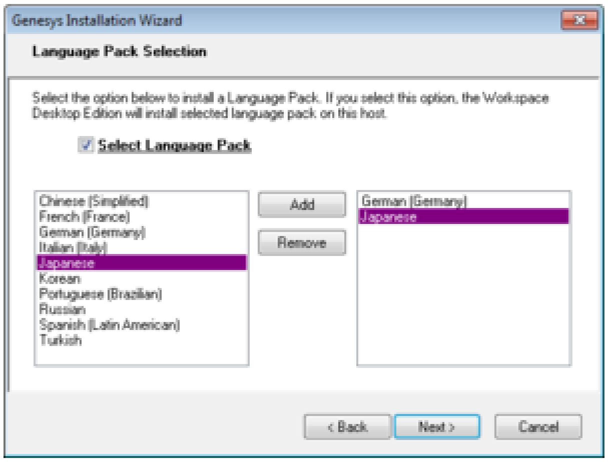
Language Pack Selection

Select the option below to install a Language Pack. If you select this option, the Workspace Desktop Edition will install selected language pack on this host.

□ Select Language Pack

Language Pack Selection panel of the Genesys Installation Wizard

Select Select Language Pack to display the list of available language packs.



Language Pack Selection

Select the option below to install a Language Pack. If you select this option, the Workspace Desktop Edition will install selected language pack on this host.

☑ Select Language Pack

Chinese (Simplified)
French (France)
German (Germany)
Italian (Italy)
Japanese
Korean
Portuguese (Brazilian)
Russian
Spanish (Latin American)
Turkish

German (Germany)
Japanese

Adding and Removing languages by using the Language Pack Selection panel of the Genesys Installation Wizard

To select a language for installation, select it in the left hand box then click **Add**. The language is moved to the right hand box. To de-select a language for installation, select it and click **Remove**. The language is moved back to the left hand box and will not be installed. After you have added to the right hand box the languages that you want to install, do one of the following:

- Click `Next` to continue the installation procedure.
- Click `Back` to return to the `Select Options` panel.
- Click `Cancel` to exit the Genesys Installation Wizard.

5. On the `Choose Destination Location` panel, specify the location on your agent workstation in which Workspace is to be installed by doing one of the following:
   - Enter a location in the `Destination Folder` text box.
   - Click `Default` to reset the location to the default location.
   - Click `Browse` to navigate to a destination folder.
6. With the destination folder specified, do one of the following:
   - Click `Next`.
   - Click `Back` to return to the `Select Options` panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.

   If you clicked `Next`, the `Ready to Install` panel is displayed.
7. On the `Ready to Install` panel, do one of the following:
   - Click `Install` to install Workspace on the client desktop.
   - Click `Back` to return to the `Choose Destination Location` panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.

   If you clicked `Next`, the Workspace client application is installed in the location that you specified. When installation is complete, the `Installation Complete` panel is displayed.

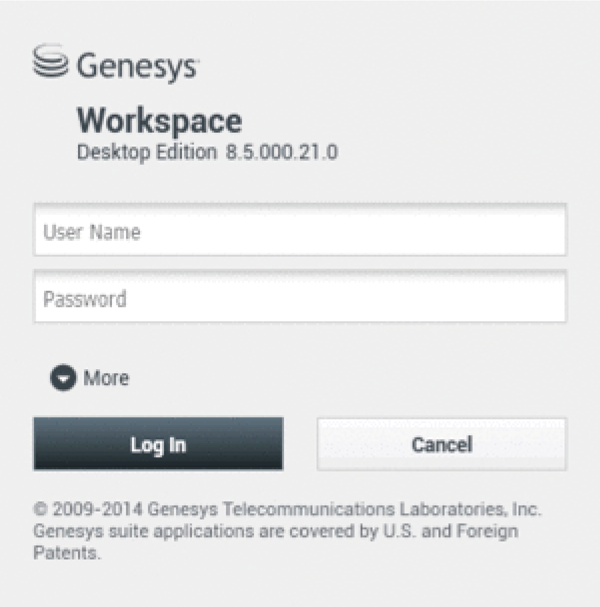
   The Workspace agent application is installed by the `Install Workspace application` option into the folder that you specified (for more information about installation options, see the Table - **Workspace Install Mode Deployment Packages**).
8. Click `Finish` to exit the Genesys Installation Wizard.
9. (optional) Procedure: Installing the Workspace SIP Endpoint.

10. (optional) To use Kerberos Single Sign-on (SSO), edit the `login.kerberos.service-principal-name` option in the `interactionworkspace.exe.config` property file to add the following line:

```
<appSettings>
  ...
  <add key="login.kerberos.service-principal-name" value="<SPN Name"/>
  <add key="login.url" value="tcp://<host><port>/AppName" />
  <add key="login.connections.parameters.isenable" value="false" />
  ...
 </appSettings>
```

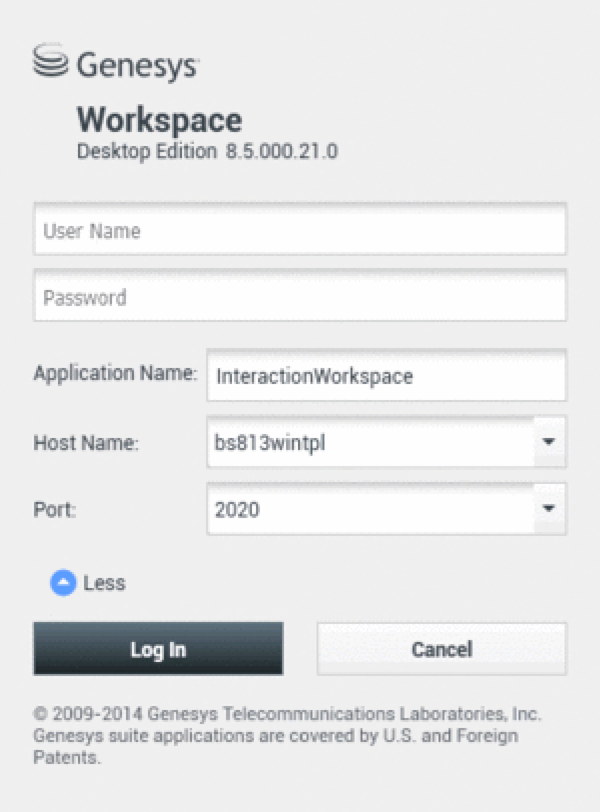
11. (optional) To include custom packages, add the customization resources that are required for your final installation.
12. If you executed at least one of the steps 9 to 11:
    a. Prepare your final package by using the updated file set.
    b. Push your custom package to the agent workstations.
13. To launch the Workspace client application on the client desktop, select it from the `Start` menu or navigate to the installation folder that you specified and double-click the `InteractionWorkspace.exe` file .

The Workspace login window is displayed on the client desktop (see the Figure - **Workspace agent Login window with no connection parameters**). The connection panel of the login window indicates that no connection has been specified. Before the agent can log in, you must connect to the Workspace application in your Genesys Framework.


Genesys
Workspace
Desktop Edition 8.5.000.21.0
User Name
Password
More
Log In
Cancel
© 2009-2014 Genesys Telecommunications Laboratories, Inc. Genesys suite applications are covered by U.S. and Foreign Patents.

Workspace agent Login window with no connection parameters

14. Click the `More Options` drop-down list to open the connection options panel (see the Figure - **Workspace agent Login window with the connection-parameters panel displayed**).



Application Name: InteractionWorkspace

Host Name: bs813wintpl

Port: 2020

© 2009-2014 Genesys Telecommunications Laboratories, Inc. Genesys suite applications are covered by U.S. and Foreign Patents.

Workspace agent Login window with the connection-parameters panel displayed

15. Enter the following information into the agent-login panel and the connection-parameters panel:
    - `User Name`: A valid user name that is configured in the Configuration Layer
    - `Password`: The valid password for the specified user name
    - `Application Name`: The name that is specified for the Workspace `application` object to which you want to connect
    - `Host Name`: The name of the web server.
    - `Port`: The port that is configured for your web-server application

    See the Figure - **Workspace agent Login window with the connection-parameters panel displayed** for an example of how to populate the fields in the Workspace login window.
16. Click `Login` to continue logging in to Workspace; click `Cancel` to close the agent-login window without logging in.

    Refer to *Workspace User's Guide* for more information about how to log in to Workspace and use the application.

**End**

**Next Steps**

- Workspace Functionality Overview and Provisioning Workspace

## Installing Workspace Desktop Edition in Silent mode for Windows

To install Workspace Desktop Edition in Silent mode:

1. Update the **genesys_silent.ini** file by making the following modifications:
   - Agree with license agreement by setting required option: **LicenseAgreement=Accepted**.
   - Add the path to the Workspace Desktop Edition directory. For example, **InstallPath=C:\Program Files (x86)\GCTI\Workspace Desktop Edition.**.
   - Choose installation mode option from one of the following supported values:
     - **INTEGRATOR -** Prepare a ClickOnce package.
     - **DEVELOPER -** Install Developer Toolkit.
     - **USER -** Install application.

     **InstallMode = <INTEGRATOR, DEVELOPER or USER installation mode of Workspace Desktop Edition on this box>**
   - If you are *installing/upgrading* Workspace Desktop Edition, specify the version, build number before the installation:
   - Specify whether Workspace Desktop Edition can dynamically modify the Genesys Softphone configuration by using the **Connector=<Disable or Enable>** parameter.
     - **Mode= <FirstInstall or Upgrade of Workspace Desktop Edition on this box>**
     - **IPVersion= <current (before upgrade) version of Workspace Desktop Edition on this box>**
     - **IPBuildNumber= <current (before upgrade) build number of Workspace Desktop Edition on this box>**
2. Execute the following command:
   `setup.exe /s /z"-s 'FullPathToGenesysSilentConfigurationFile' -sl 'FullPathToGenesysSilentResultFile' -t 'FullPathToGenesysSilentInstallationListingFile'"` where:
   - `/s` specifies that the installation is running in InstallShield Silent Mode.
   - `/z` passes the Genesys Silent mode silent parameters to the installation.
     - `-s` specifies the full path to the silent configuration file. The **<Full path to Genesys Silent Configuration file>** is optional. If the **<Full path to Genesys Silent Configuration file>** parameter is not specified, the installation uses the **genesys_silent.ini** file in the same directory where the **setup.exe** file is located.

       > **Important**
       >
       > Enclose the value of the **<Full path to Genesys Silent Configuration file>** parameter by apostrophes (') if the parameter contains white symbols.
     - `-sl` specifies the full path to the installation results file. If the **<Full path to Genesys Installation Result file>** parameter is not specified, the installation creates the **genesys_install_result.log** file in the **<System TEMP folder>** directory.

> ## Important
> Enclose the value of the **<Full path to Genesys Installation Result file>** parameter in apostrophes (') if the parameter contains white space characters.

- `-t` specifies the full path to the installation listing file for debugging. The **<Full path to Genesys Installation listing file>** parameter is optional and should be used for silent installation debugging purposes.

> ## Important
> Enclose the value of the **<Full path to Genesys Installation listing file>** parameter in apostrophes (') if the parameter contains white space characters.

The **InstallShield setup.exe** installer requires that:

- There is *no* space between the `/z` argument and quotation mark. For example, `/z"-s"` is valid, while `/z "-s"` is not valid.
- There *is* a space between the -s,-sl parameters and quotation mark. For example, `/z"-s c:\temp\genesys_silent.ini"` is valid, while `/z "-sc:\temp\genesys_silent.ini"` is not valid. For example,
`setup.exe /s /z"-s 'C:\8.5.151.01\windows\b1\ip\genesys_silent.ini' -sl 'C:\temp\silent_setup.log' -t 'C:\temp\Genesys_LP_Installation.log'"`.

3. After executing this command, verify that Workspace Desktop Edition is installed in the **C:\<Workspace Desktop Edition Directory>**, and that the **silent_setup.log** file has been created in the **C:\temp\** directory.

For information about silent language pack installation, see the Adding and removing Language Packs.

# Adding and removing Language Packs

Use the following procedures to manually add and remove Workspace Language Packs after you have deployed Workspace.

> ### Important
>
> Notes about upgrading Language Packs when you upgrade Workspace:
>
> **Upgrade from DVD**
>
> - When you upgrade Workspace from DVD, only the application is upgraded
> - All language packs that were install using an older version will not be upgraded—You must manually upgrade each language pack by using the same procedure that was used to install the original language packs; during install, the wizard will detect the older language packs and enable you to choose which ones to upgrade
>
> **Upgrade from Language Pack IP**
>
> - Open the folder containing the language pack
> - Follow the standard procedure to add a language pack to workspace

## Adding a Language Pack to Workspace using Interactive mode

Language packs (localized content for Workspace) are not always released at the same time as the English version of Workspace, and new language packs are added as demanded by Genesys' customers.

Language packs are available as part of the Genesys International DVD/IP. If you are installing a new release of Workspace from an International DVD/IP, use the standard ClickOnce, Developer, and Non-ClickOnce procedures in the other tabs of this topic.

Watch video: How to add a language pack to an already deployed Workspace Desktop Edition 8.5.1: Link to video

Use the following procedure to add a language pack to your existing Workspace deployment.

### Procedure

Installing a Workspace Language Pack on an existing Workspace deployment or ClickOnce package

**Purpose:** To install a Workspace language pack on your existing Workspace deployment on a client desktop or on an existing ClickOnce package.

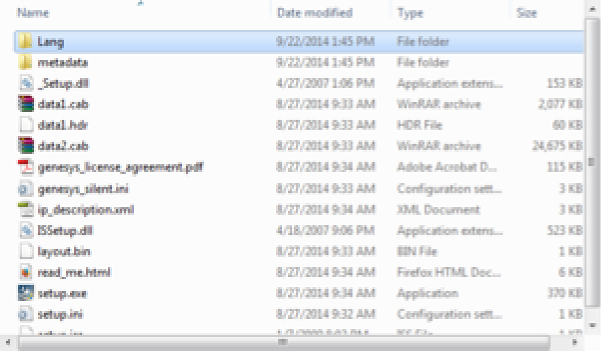
### Prerequisites

Workspace must already be installed using one of the following deployment types:

- ClickOnce Deployment
- Developer Deployment
- Non-ClickOnce Deployment

### Start

1. If you are deploying from the Workspace Desktop Edition DVD, open the **Lang** folder (refer to the **Lang (Language) folder in the Workspace Install Package** figure).

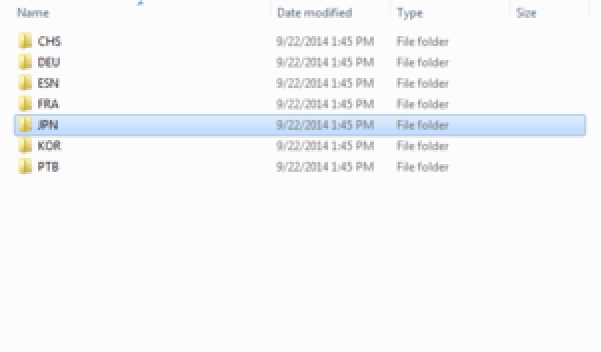


| Name | Date modified | Type | Size |
|---|---|---|---|
| Lang | 9/22/2014 1:45 PM | File folder | |
| metadata | 9/22/2014 1:45 PM | File folder | |
| _Setup.dll | 4/27/2007 1:06 PM | Application extens... | 153 KB |
| data1.cab | 8/27/2014 9:33 AM | WinRAR archive | 2,077 KB |
| data1.hdr | 8/27/2014 9:33 AM | HDR File | 60 KB |
| data2.cab | 8/27/2014 9:33 AM | WinRAR archive | 24,675 KB |
| genesys_license_agreement.pdf | 8/27/2014 9:34 AM | Adobe Acrobat D... | 115 KB |
| genesys_silent.ini | 8/27/2014 9:33 AM | Configuration sett... | 3 KB |
| ip_description.xml | 8/27/2014 9:34 AM | XML Document | 3 KB |
| ISSetup.dll | 4/18/2007 9:06 PM | Application extens... | 523 KB |
| layout.bin | 8/27/2014 9:33 AM | BIN File | 1 KB |
| read_me.html | 8/27/2014 9:34 AM | Firefox HTML Doc... | 6 KB |
| setup.exe | 8/27/2014 9:34 AM | Application | 370 KB |
| setup.ini | 8/27/2014 9:32 AM | Configuration sett... | 1 KB |

Lang (Language) folder in the Workspace Install Package

If you are installing from a language specific IP, go to Step 3.

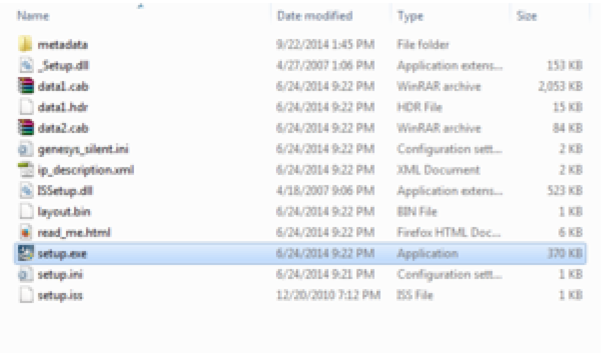
2. The **Lang** folder contains folders named with three-letter language codes. These folders contain the language specific language pack installers (refer to the **Three letter language-code folders in the Lang folder** figure). Open the folder that contains the language installer that you want to use.



| Name | Date modified | Type | Size |
|---|---|---|---|
| CHS | 9/22/2014 1:45 PM | File folder | |
| DEU | 9/22/2014 1:45 PM | File folder | |
| ESN | 9/22/2014 1:45 PM | File folder | |
| FRA | 9/22/2014 1:45 PM | File folder | |
| JPN | 9/22/2014 1:45 PM | File folder | |
| KOR | 9/22/2014 1:45 PM | File folder | |
| PTB | 9/22/2014 1:45 PM | File folder | |

Three letter language-code folders in the Lang folder

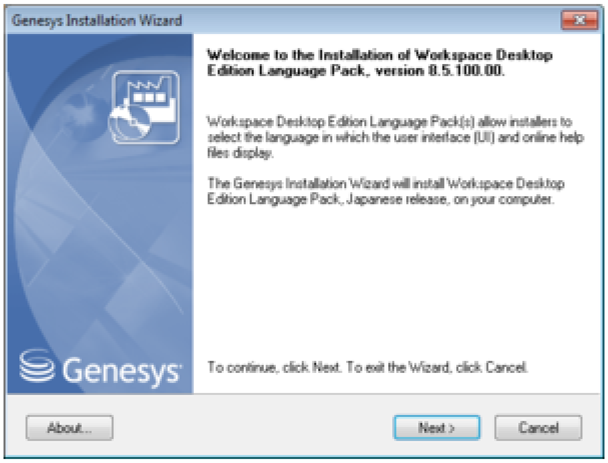
3. Double-click the `setup.exe` file to launch the language pack installer.



| Name | Date modified | Type | Size |
|---|---|---|---|
| metadata | 9/22/2014 1:45 PM | File folder | |
| _Setup.dll | 4/27/2007 1:06 PM | Application extens... | 153 KB |
| data1.cab | 6/24/2014 9:22 PM | WinRAR archive | 2,053 KB |
| data1.hdr | 6/24/2014 9:22 PM | HDR File | 15 KB |
| data2.cab | 6/24/2014 9:22 PM | WinRAR archive | 84 KB |
| genesys_silent.ini | 6/24/2014 9:22 PM | Configuration sett... | 2 KB |
| ip_description.xml | 6/24/2014 9:22 PM | XML Document | 2 KB |
| ISSetup.dll | 4/18/2007 9:06 PM | Application extens... | 523 KB |
| layout.bin | 6/24/2014 9:22 PM | BIN File | 1 KB |
| read_me.html | 6/24/2014 9:22 PM | Firefox HTML Doc... | 6 KB |
| setup.exe | 6/24/2014 9:22 PM | Application | 370 KB |
| setup.ini | 6/24/2014 9:21 PM | Configuration sett... | 1 KB |
| setup.iss | 12/20/2010 7:12 PM | ISS File | 1 KB |

Language pack specific installer setup.exe

The Genesys Installation Wizard launches and the Welcome panel is displayed.



Genesys Installation Wizard

**Welcome to the Installation of Workspace Desktop Edition Language Pack, version 8.5.100.00.**

Workspace Desktop Edition Language Pack(s) allow installers to select the language in which the user interface (UI) and online help files display.

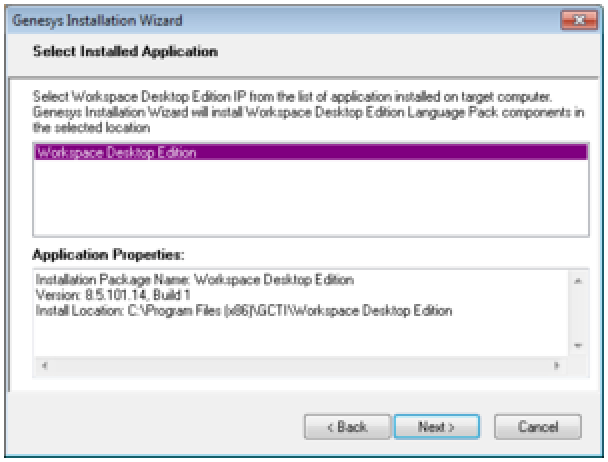
The Genesys Installation Wizard will install Workspace Desktop Edition Language Pack, Japanese release, on your computer.

To continue, click Next. To exit the Wizard, click Cancel.

Genesys Installation Wizard language pack splash screen panel

4. On the Welcome panel, do one of the following:
   - Click Next to begin the installation procedure.
   - Click Cancel to exit the Genesys Installation Wizard.
   - Click About to open the Workspace Desktop Edition ReadMe file in your default browser.

If you clicked Next, the installer searches for instances of the Workspace application installed on your computer and displays a list of installations in the Select Installed Application panel from which you can choose.



Genesys Installation Wizard

Select Installed Application

Select Workspace Desktop Edition IP from the list of application installed on target computer. Genesys Installation Wizard will install Workspace Desktop Edition Language Pack components in the selected location

Workspace Desktop Edition

Application Properties:

Installation Package Name: Workspace Desktop Edition
Version: 8.5.101.14, Build 1
Install Location: C:\Program Files (x86)\GCTI\Workspace Desktop Edition

Genesys Installation Wizard Select Installed Application panel

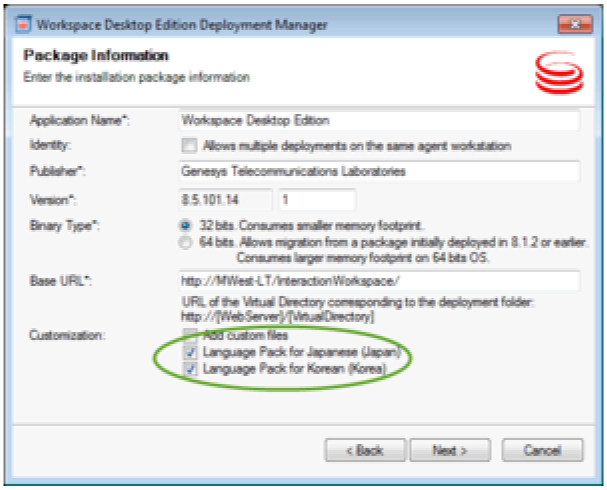
5. On the `Select Installed Application` panel, do one of the following:
   - Select the application to which you want to add a language pack and click `Next` to begin the installation procedure.
   - Click `Cancel` to exit the Genesys Installation Wizard.
   - Click `Back` to return to the splash screen.

   If you clicked `Next`, the `Ready to Install` panel is displayed.

6. In the `Ready to Install` panel, do one of the following:
   - Click `Install` to install the language pack.
   - Click `Cancel` to exit the Genesys Installation Wizard.
   - Click `Back` to return to the `Select Installed Application` panel.

   If you clicked `Next` the update is installed and the `Installation Complete` panel is displayed.

7. Click `Finish` to close the `Installation Complete` panel and complete the installation.
8. Depending on whether you are updating an existing installation or adding a language pack to a ClickOnce package, do one of the following:
   - If you are adding a language to an existing non-ClickOnce installation, launch Workspace and select the new language from the Login view Language drop-down menu.
   - If you are adding a language pack to a ClickOnce installation, launch Workspace Desktop Edition Deployment Manager (`InteractionWorkspaceDeploymentManager.exe`). In the `Package Information` panel, select the installed language packs that you want to add to your ClickOnce package, then complete the deployment.



Workspace Desktop Edition Deployment Manager

**Package Information**

Enter the installation package information

Application Name*: Workspace Desktop Edition

Identity: □ Allows multiple deployments on the same agent workstation

Publisher*: Genesys Telecommunications Laboratories

Version*: 8.5.101.14 1

Binary Type*: ● 32 bits. Consumes smaller memory footprint.
○ 64 bits. Allows migration from a package initially deployed in 8.1.2 or earlier. Consumes larger memory footprint on 64 bits OS.

Base URL*: http://MWest-LT/InteractionWorkspace/

URL of the Virtual Directory corresponding to the deployment folder: http://[WebServer]/[VirtualDirectory]

Customization: □ Add custom files
☑ Language Pack for Japanese (Japan)
☑ Language Pack for Korean (Korea)

Genesys Installation Wizard Package Information panel

**End**

## Adding Language Pack to Workspace using Silent mode

To install Language Pack to Workspace in Silent mode, use the Installation Wizard **Silent** arguments as follows:

1. Update the **genesys_silent.ini** file by making the following modifications:
    - Add the path to the Workspace Desktop Edition directory. For example, **InstallPath=C:\Program Files (x86)\GCTI\Workspace Desktop Edition**.
    - If you are *installing/upgrading* Language Pack for Workspace, specify the version, build number before the installation:
    - Specify whether Genesys Softphone starts automatically when Windows starts by using the **Startup=<Std or Auto>** parameter.
        - **Mode= <FirstInstall or Upgrade of Language Pack on this box>**
        - **IPVersion= <current (before upgrade) version of Language Pack on this box>**
        - **IPBuildNumber= <current (before upgrade) build number of Language Pack on this box>**
2. Execute the following command:
   `setup.exe /s /z"-s 'FullPathToGenesysSilentConfigurationFile' -sl 'FullPathToGenesysSilentResultFile' -t 'FullPathToGenesysSilentInstallationListingFile'"` where:
    - `/s` specifies that the installation is running in InstallShield Silent Mode.
    - `/z` passes the Genesys Silent mode silent parameters to the installation.
    - `-s` specifies the full path to the silent configuration file. The **<Full path to Genesys Silent Configuration file>** is optional. If the **<Full path to Genesys Silent Configuration file>** parameter is not specified, the installation uses the **genesys_silent.ini** file in the same directory where the **setup.exe** file is located.

> ### Important
> Enclose the value of the **<Full path to Genesys Silent Configuration file>** parameter by apostrophes (') if the parameter contains white symbols.

- `-sl` specifies the full path to the installation results file. If the **<Full path to Genesys Installation Result file>** parameter is not specified, the installation creates the **genesys_install_result.log** file in the **<System TEMP folder>** directory.

> ### Important
> Enclose the value of the **<Full path to Genesys Installation Result file>** parameter in apostrophes (') if the parameter contains white space characters.

- `-t` specifies the full path to the installation listing file for debugging. The **<Full path to Genesys Installation listing file>** parameter is optional and should be used for silent installation debugging purposes.

> ### Important
> Enclose the value of the **<Full path to Genesys Installation listing file>** parameter in apostrophes (') if the parameter contains white space characters.

The **InstallShield setup.exe** installer requires that:

- There is *no* space between the `/z` argument and quotation mark. For example, `/z"-s"` is valid, while `/z "-s"` is not valid.
- There *is* a space between the -s,-sl parameters and quotation mark. For example, `/z"-s c:\temp\genesys_silent.ini"` is valid, while `/z "-sc:\temp\genesys_silent.ini"` is not valid. For example,
  `setup.exe /s /z"-s 'C:\8.5.144.00\windows\b1\ip\genesys_silent.ini' -sl 'C:\temp\silent_setup.log' -t 'C:\temp\Genesys_LP_Installation.log'"`.

3. After executing this command, verify that Language Pack to Workspace is installed in the **C:\<Workspace Desktop Edition Directory>**, and that the **silent_setup.log** file has been created in the **C:\temp\** directory.

### Troubleshooting

If you see that error message in silent_setup.log:

```
[Result]
ResultCode=-1
Error=Required parameter <Parent IP GUID parameter is not defined.> is wrong.\nError
was detected by lpScenarioFirstBeforeBegin().
```

Please check that **InstallPath** parameter is correct in silent configuration file.

### Important

No backslash (\) symbol should be in the end of the full path to the installation directory. For example, **InstallPath=C:\Program Files (x86)\GCTI\Workspace Desktop Edition**

For information about silent language pack installation, see the Installing Workspace Desktop Edition in Silent mode for Windows.

## Removing a Language Pack From Workspace after Deployment

For non-ClickOnce deployments, use **Add/Remove Programs** to select which Language Packs you want to remove from your workstation.

For ClickOnce deployments, run **Workspace Deployment Manager** and de-select language packs in the Package Information panel and push new ClickOnce package to your web server.

# Installing the Workspace SIP Endpoint

[**Modified:** 8.5.109.16, 8.5.114.08]

The Workspace SIP Endpoint is an optional plug-in or standalone application for Workspace. It is available as a separate IP that you install from a separate CD/DVD. You can install it in one of two modes, as a plugin that runs with Workspace Desktop Edition on the agent workstation, or as a standalone application that connects to Workspace running in a virtualized environment.

> Tip
>
> Workspace also supports the Genesys Softphone in place of Workspace SIP Endpoint. To learn about the installation of Genesys Softphone, see Deploying Genesys Softphone in the Genesys Softphone Deployment Guide.

If you intend to create a ClickOnce package to install Workspace SIP Endpoint, install the Workspace SIP Endpoint *after* you install the Workspace application on your server, but before you run the Workspace Deployment Manager.

If you deploy Workspace SIP Endpoint as part of a ClickOnce deployment, the behavior of the ClickOnce download depends on the privileges that are assigned to the agent who is logging in. If the agent is granted the privilege to execute a local Workspace SIP Endpoint, the following files are downloaded to the agent workstation:

- The SIP Endpoint Communication plug-in (part of Workspace runtime)
- The Workspace SIP Endpoint executable and associated assemblies.

## Installing Workspace SIP Endpoint as a Workspace Desktop Edition plugin

Use the following procedure to install Workspace SIP Endpoint in environments where the Workspace application and Workspace SIP Endpoint run on the same workstation. Use the Installing the Standalone Workspace SIP Endpoint when you are running Workspace in a virtualized environment.

### Procedure

Installing the Workspace SIP Endpoint as a Workspace Desktop Edition plugin

**Purpose:** To install the Workspace SIP Endpoint on your web server, an agent workstation, or a development workstation as a plugin.

**Prerequisites**

- .NET Framework 4.5
- The following Microsoft redistributable package(s) is/are required to be installed on the workstation where Workspace SIP Endpoint will execute. They are installed by the Installation Package if they are not already present on the target workstation, but if you are deploying Workspace and Workspace SIP Endpoint by using ClickOnce, you must plan the installation of the following packages on those workstations prior to enabling the ClickOnce deployment:
    - For 8.5.114.xx and higher
        - Visual C++ Redistributable for Visual Studio 2013: http://download.microsoft.com/download/2/E/6/2E61CFA4-993B-4DD4-91DA-3737CD5CD6E3/vcredist_x86.exe
    - For 8.5.104.xx to 8.5.113.xx:
        - Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package MFC Security Update: http://download.microsoft.com/download/8/B/4/8B42259F-5D70-43F4-AC2E-4B208FD8D66A/vcredist_x86.EXE
        - Visual C++ Redistributable for Visual Studio 2013: http://download.microsoft.com/download/2/E/6/2E61CFA4-993B-4DD4-91DA-3737CD5CD6E3/vcredist_x86.exe
    - 8.5.103.xx and lower:
        - Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package MFC Security Update: http://download.microsoft.com/download/8/B/4/8B42259F-5D70-43F4-AC2E-4B208FD8D66A/vcredist_x86.EXE
        - Visual C++ Redistributable for Visual Studio 2012 Update 4, 32-bits package only: http://www.microsoft.com/en-us/download/details.aspx?id=30679
- Install the Workspace application by using one of the following procedures:
    - Deploying The ClickOnce Application On Your Web Server. Choose this option if you want to deploy Workspace as a ClickOnce application.
    - Installing The Workspace Developer Toolkit. Choose this option if you want to deploy the Workspace developer package.
    - Installing The Workspace Application. Choose this option if you want to deploy a non-ClickOnce version of Workspace.

### Start

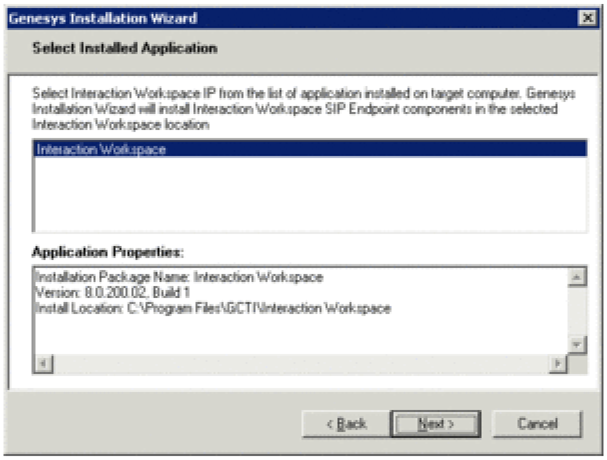
1. On your desktop, open the Workspace SIP Endpoint disc or the Workspace SIP Endpoint IP and double-click the `Setup.exe` file.

   You might be asked to reboot your system to delete or rename certain system files before the Installation Wizard runs.

   The Genesys Installation Wizard launches and the `Welcome` panel is displayed.

2. On the `Welcome` panel, do one of the following:
    - Click `Next` to begin the installation procedure.
    - Click `Cancel` to exit the Genesys Installation Wizard.
    - Click `About` to open the Workspace SIP Endpoint ReadMe in your default browser.

      If you clicked `Next`, the `Select Installed Application` panel is displayed (see the Figure - **Select Installed Application Panel of the Genesys Installation Wizard**).



Genesys Installation Wizard

Select Installed Application

Select Interaction Workspace IP from the list of application installed on target computer. Genesys Installation Wizard will install Interaction Workspace SIP Endpoint components in the selected Interaction Workspace location

Interaction Workspace

Application Properties:

Installation Package Name: Interaction Workspace
Version: 8.0.200.02, Build 1
Install Location: C:\Program Files\GCTI\Interaction Workspace

Select Installed Application Panel of the Genesys Installation Wizard

3. The `Select Installed Application` panel enables you to select the Workspace application instance to which you want to add Workspace SIP Endpoint as a plug-in.

   The Genesys Installation Wizard searches the target computer for an installed version of Workspace. Select the version of Workspace in the location in which you want Workspace SIP Endpoint to be installed.

   The `Application Properties` pane displays the name, version, and location of the selected Workspace application (see the Figure - **Select Installed Application Panel of the Genesys Installation Wizard**).

4. After you have selected the version of Workspace that you want to use with Workspace SIP Endpoint, do one of the following:

   - Click `Next` to proceed to the next panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.
   - Click `Back` to return to the previous panel.

     If you clicked `Next`, the `Ready to Install` panel is displayed.

5. On the `Ready to Install` panel do one of the following:

   - Click `Install` to install Workspace SIP Endpoint on your web server, development workstation, or agent workstation.
   - Click `Back` to return to the `Select Installed Application` panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.

   If you clicked `Next`, Workspace SIP Endpoint is installed in the location that you specified. When installation is complete, the `Installation Complete` panel is displayed.

6. Click `Finish` to exit the Genesys Installation Wizard.

   A folder that is named `InteractionWorkspaceSIPEndpoint` is created in the `Workspace` folder. The `InteractionWorkspaceSIPEndpoint` folder contains the Workspace SIP Endpoint application and associated files.

   After the Workspace SIP Endpoint application is installed on the agent or developer workstation, or after it is downloaded by the ClickOnce application (see Deploying The ClickOnce Application On Your Web Server), and after the agent is granted permission to use the application, agents must login Workspace on a Place that is associated with a SIP DN to start the Workspace SIP Endpoint. The Workspace SIP Endpoint process is started automatically when Workspace application is being initialized.

7. To ensure that the supporting programs were installed correctly, check if the following programs are available in the "uninstall programs" view of the Control Panel on your Windows workstation:

   - Genesys Workspace SIP Endpoint <version>

- Microsoft Visual C++ 2005 Redistributable (8.5.113.xx and lower)
- Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.60.610

**End**

**Next Steps**

- (Optional) If you are deploying Workspace as a ClickOnce application on your web server, go to Deploying The ClickOnce Application On Your Web Server.
- Installation is complete. You can provision Workspace SIP Endpoint functionality. Refer to:
  - Provisioning Functionality.

# Installing the standalone Workspace SIP Endpoint

[**Added:** 8.5.109.16]

Use the following procedure to install Workspace SIP Endpoint in environments where the Workspace application is running in a virtualized environment and Workspace SIP Endpoint runs as a standalone application on the agent workstation.

## Procedure

### Installing the standalone Workspace SIP Endpoint as a ClickOnce package

**Purpose:** To install the Workspace SIP Endpoint on your web server so that it can be deployed on an agent workstation or a development workstation.

**Prerequisites**

- .NET Framework 4.5
- Workspace Desktop Edition is installed on the host machine as a ClickOnce package.
- The following Microsoft redistributable package(s) is/are required to be installed on the workstation where Workspace SIP Endpoint will execute. They are installed by the Installation Package if they are not already present on the target workstation, but if you are deploying Workspace and Workspace SIP Endpoint by using ClickOnce, you must plan the installation of the following packages on those workstations prior to enabling the ClickOnce deployment:
  - Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package MFC Security Update: http://download.microsoft.com/download/8/B/4/8B42259F-5D70-43F4-AC2E-4B208FD8D66A/vcredist_x86.EXE
  - Visual C++ Redistributable for Visual Studio 2013: http://download.microsoft.com/download/2/E/6/2E61CFA4-993B-4DD4-91DA-3737CD5CD6E3/vcredist_x86.exe
- Install the Workspace application in a virtualized environment by using one of the following procedures:
  - Deploying The ClickOnce Application On Your Web Server. Choose this option if you want to deploy Workspace as a ClickOnce application.
  - Installing The Workspace Developer Toolkit. Choose this option if you want to deploy the Workspace

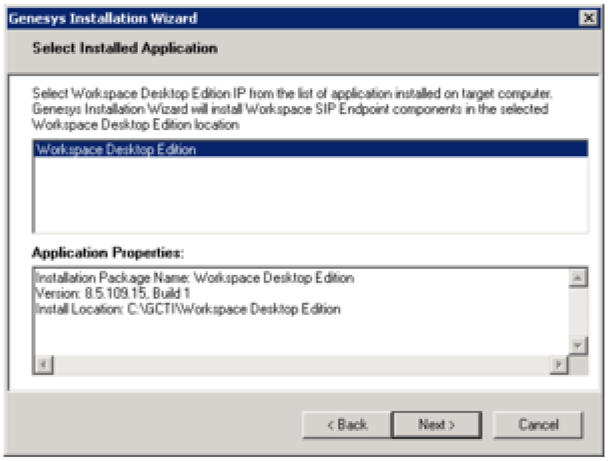
developer package.

- Installing The Workspace Application. Choose this option if you want to deploy a non-ClickOnce version of Workspace.

## Start

1. Open the Workspace SIP Endpoint disc or the Workspace SIP Endpoint IP and double-click the `Setup.exe` file. You might be asked to reboot your system to delete or rename certain system files before the Installation Wizard runs. The Genesys Installation Wizard launches and the Welcome panel is displayed.
2. On the `Welcome` panel, do one of the following:
   - Click `Next` to begin the installation procedure.
   - Click `Cancel` to exit the Genesys Installation Wizard.

   If you clicked `Next`, the `Select Installed Application` panel is displayed (see the Figure - **Select Installed Application Panel of the Genesys Installation Wizard**).



Genesys Installation Wizard

Select Installed Application

Select Workspace Desktop Edition IP from the list of application installed on target computer. Genesys Installation Wizard will install Workspace SIP Endpoint components in the selected Workspace Desktop Edition location

Workspace Desktop Edition

Application Properties:

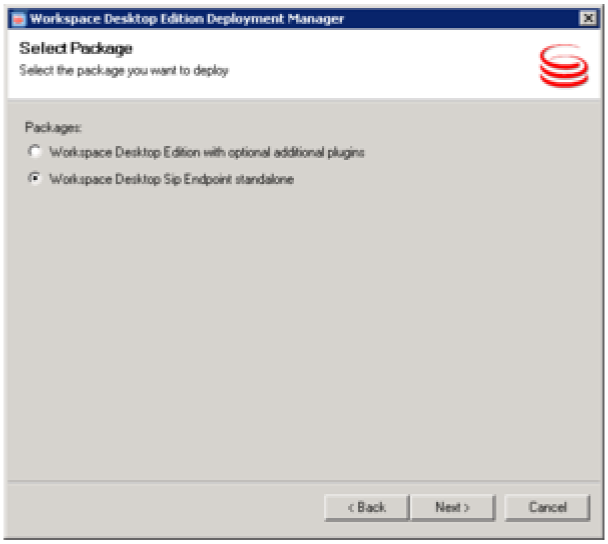
Installation Package Name: Workspace Desktop Edition
Version: 8.5.109.15, Build 1
Install Location: C:\GCTI\Workspace Desktop Edition

Select Installed Application Panel of the Genesys Installation Wizard

3. Ensure that **Workspace Desktop Edition** is selected, then click `Next` to proceed to the `Ready to Install` panel.
4. On the `Ready to Install` panel, click `Install` to install Workspace SIP Endpoint on your web server.

   Workspace SIP Endpoint is installed in the location that you specified. When installation is complete, the `Installation Complete` panel is displayed.
5. Click `Finish` to exit the Genesys Installation Wizard.

   A folder that is named `InteractionWorkspaceSIPEndpoint` is created in the `Workspace Desktop Edition` folder. The `InteractionWorkspaceSIPEndpoint` folder contains the Workspace SIP Endpoint application and associated files.
6. From the **Start** menu of your web server host, use the application shortcut to launch the Workspace Desktop Edition Deployment Manager. The Deployment Manager can also be launched from the location where you installed it. The **Welcome** panel is displayed on the desktop of your web server.
7. On the `Welcome` panel, click `Next` to begin the installation procedure. The **Select Package** panel is displayed.


Workspace Desktop Edition Deployment Manager

Select Package

Select the package you want to deploy

Packages:

○ Workspace Desktop Edition with optional additional plugins

● Workspace Desktop Sip Endpoint standalone

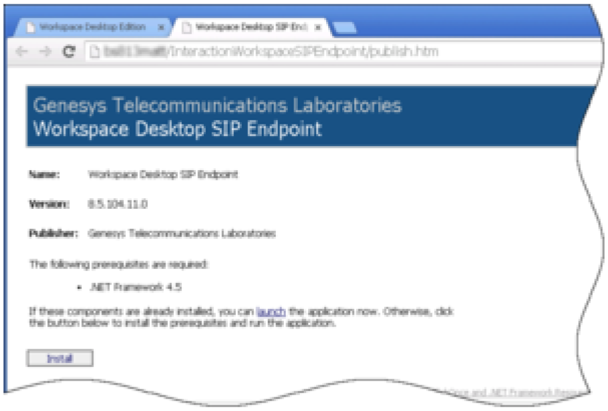
Select Package Panel of the Workspace Desktop Edition Deployment Manager

8. Click the **Workspace Desktop Sip Endpoint standalone** option, then click **Next**. The **Destination Folder** panel is displayed.
9. Specify the path to the destination folder for the ClickOnce package, then click **Next**. The **Package Information** panel is displayed.
10. Specify the following information:
    - **Application Name**—The default name is **Workspace Desktop SIP Endpoint**
    - **Publisher**—The default name is **Genesys Telecommunications Laboratories**
    - **Base URL**—Specify the host URL that will be provided to agents to download the ClickOnce package

    Click **Next**. The **Signing** panel is displayed. For more information about how to create or obtain a signing certificate, refer to the "ClickOnce Deployment and Authenticode" page on the Microsoft Developer Network web site:

    http://msdn.microsoft.com/en-us/library/ms172240.aspx
11. Choose the type of signing certificate that you are using:
    - Click **Do not Sign** if you do not provide a certificate, a security warning is displayed whenever the client downloads the package.
    - Click **Sign with a provided certificate** to enable the **Selects a certificate** field.
        1. Click the browse button to navigate to the certificate.
        2. Enter the password for the certificate in the Password field.
12. Click Next to proceed with the installation. The **Ready to Build** pane is displayed. This pane contains a summary of the files that will be deployed on your web server and a confirmation of the deployment URL.
13. Click **Next** to complete the deployment. The Deployment Manager deploys the Workspace Standalone SIP Endpoint ClickOnce application in the path that you specified at the beginning of the wizard execution. When the deployment is complete, the **Deployment Finished** pane is displayed. This pane contains messages that relate to the success of the deployment.
14. Click **Finish** to close the Workspace Deployment Manager.

    Deployment proceeds. When deployment is complete, the `publish.htm` web page is opened in your default browser automatically for testing purposes.



Workspace Desktop Edition ×  Workspace Desktop SIP End ×

[redacted]/InteractionWorkspaceSIPEndpoint/publish.htm

Genesys Telecommunications Laboratories
Workspace Desktop SIP Endpoint

**Name:** Workspace Desktop SIP Endpoint

**Version:** 8.5.104.11.0

**Publisher:** Genesys Telecommunications Laboratories

The following prerequisites are required:

- .NET Framework 4.5

If these components are already installed, you can launch the application now. Otherwise, click the button below to install the prerequisites and run the application.

Install

The Workspace Standalone SIP Endpoint publish.htm page

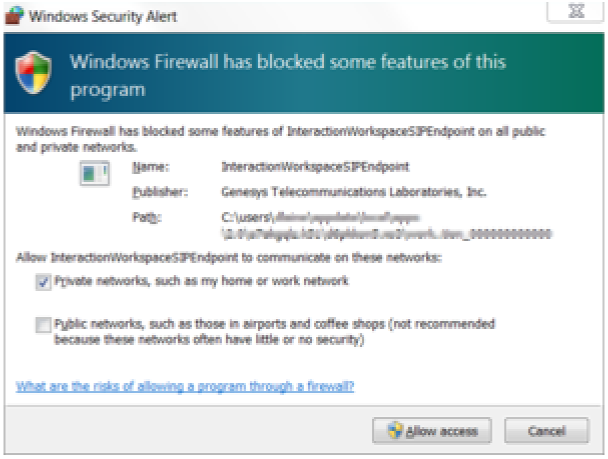
15. Provide the URL for the `publish.htm` page to your agents to enable them to install the Workspace Standalone SIP Endpoint on their workstations and receive automatic updates when the application is updated on the web server.

16. When an agent navigates to the `publish.htm` page, the ClickOnce package deployment automatically starts, or she or he should click the **Launch** hyperlink to start the deployment on his or her workstation.

17. Instruct your agent to click **Install**. When the installation is complete, the Workspace Standalone SIP Endpoint launches automatically. The application icon is displayed in the system tray (). The icon is grey when the SIP Endpoint is not connected to a Workspace application running in a virtualized environment, and red when it has an active connection.

Agents can exit the SIP Endpoint by right clicking on the icon and selecting **Exit**. If Agents have to relaunch the application, they can do so by using the shortcut in the **Start** menu.

**Note:** When Workspace SIP Endpoint is started for the first time on a workstation with an active Windows Firewall, the Windows Operating System displays a security message requesting the user to approve the selection of a private or enterprise network.



Windows Security Alert

Windows Firewall has blocked some features of this program

Windows Firewall has blocked some features of InteractionWorkspaceSIPEndpoint on all public and private networks.

Name: InteractionWorkspaceSIPEndpoint
Publisher: Genesys Telecommunications Laboratories, Inc.
Path: C:\users\[redacted]

Allow InteractionWorkspaceSIPEndpoint to communicate on these networks:

☑ Private networks, such as my home or work network

☐ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing a program through a firewall?

Allow access Cancel

Agents running Workspace SIP Endpoint on Workstations using Windows Firewall might have to grant access to run the application for the first time

**End**

**Next Steps**

- Installation is complete. You can provision Workspace SIP Endpoint functionality. Refer to:
    - Provisioning Functionality.

## Procedure

### Installing the Standalone Workspace SIP Endpoint on a workstation

**Purpose:** To install the Workspace SIP Endpoint on an agent workstation or a development workstation.

**Prerequisites**

- Ensure that Workspace Desktop Edition was not installed on this workstation by an Installation Package from Genesys.
- .NET Framework 4.5
- The following Microsoft redistributable package(s) is/are required to be installed on the workstation where Workspace SIP Endpoint will execute. They are installed by the Installation Package if they are not already present on the target workstation, but if you are deploying Workspace and Workspace SIP Endpoint by using ClickOnce, you must plan the installation of the following packages on those workstations prior to enabling the ClickOnce deployment:
    - Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package MFC Security Update: http://download.microsoft.com/download/8/B/4/8B42259F-5D70-43F4-AC2E-4B208FD8D66A/vcredist_x86.EXE
    - Visual C++ Redistributable for Visual Studio 2013: http://download.microsoft.com/download/2/E/6/2E61CFA4-993B-4DD4-91DA-3737CD5CD6E3/vcredist_x86.exe
- Install the Workspace application in a virtualized environment by using one of the following procedures:
    - Deploying The ClickOnce Application On Your Web Server. Choose this option if you want to deploy Workspace as a ClickOnce application.
    - Installing The Workspace Developer Toolkit. Choose this option if you want to deploy the Workspace developer package.
    - Installing The Workspace Application. Choose this option if you want to deploy a non-ClickOnce version of Workspace.

**Start**

1. On your workstation, open the Workspace SIP Endpoint disc or the Workspace SIP Endpoint IP and double-click the `Setup.exe` file. You might be asked to reboot your system to delete or rename certain system files before the Installation Wizard runs. The Genesys Installation Wizard launches and the Welcome panel is displayed.
2. On the `Welcome` panel, do one of the following:
    - Click `Next` to begin the installation procedure.
    - Click `Cancel` to exit the Genesys Installation Wizard.

   If you clicked `Next`, the `Choose Destination Location` panel is displayed.
3. Specify the **Destination Folder** for the Workspace SIP Endpoint application, then click **Next** to proceed to the `Ready to Install` panel.

4. On the `Ready to Install` panel, click `Install` to install Workspace SIP Endpoint on your workstation.

   Workspace SIP Endpoint is installed in the location that you specified. When installation is complete, the `Installation Complete` panel is displayed.

5. Click `Finish` to exit the Genesys Installation Wizard.
6. When the installation is complete, the Workspace Standalone SIP Endpoint can be launched for the first time by using the shortcut in the **Start** menu (or it will start automatically when any Windows user session is started). The application icon is displayed in the system tray ().

   The icon is grey when the SIP Endpoint is not connected to a Workspace application running in a virtualized environment, and red when it has an active connection.

   Agents can exit the SIP Endpoint by right clicking on the icon and selecting **Exit**. If Agents have to relaunch the application, they can do so by using the shortcut in the **Start** menu.

**End**

### Next Steps

- Installation is complete. You can provision Workspace SIP Endpoint functionality. Refer to:
  - Provisioning Functionality.

## Deployment Manager in Console mode

You can build a Workspace Standalone SIP Endpoint ClickOnce package using Workspace Desktop Edition Deployment Manager in Console mode. This can be done by setting the `ApplicationToDeploy` attribute in the `silent.xml` file:

```
<ApplicationToDeploy>WorkspaceSipEndpoint</ApplicationToDeploy>
```

For more information, refer to 3b. Console: Deploy the Workspace downloadable ClickOnce package on your web server.

The following is an example of a `silent.xml` file with supported options for Workspace SIP Endpoint:

```
<?xml version="1.0" encoding="windows-1250"?>
<configuration>
<ApplicationToDeploy>WorkspaceSipEndpoint</ApplicationToDeploy>
<InformationApplicationName>Workspace SIP Endpoint</InformationApplicationName>
<InformationURL>http://WebServerHost/WorkspaceSipEndpoint</InformationURL>
<InformationPublisher>Genesys Telecommunications Laboratories</InformationPublisher>
<DeploymentDestinationFolder>c:\inetpub\wwwroot\
WorkspaceSipEndpoint</DeploymentDestinationFolder>
<SigningSignsWithProvidedCertificate>false</SigningSignsWithProvidedCertificate>
<SigningCertificateFileName></SigningCertificateFileName>
<SigningPassword></SigningPassword>
</configuration>
```

# Installing plug-ins for workspace

Workspace enables you to install optional plug-ins for Workspace. Plug-ins, such as eServices Social Media interaction handling, are available as separate IPs that you install from a separate CD/DVD.

If you deploy a plug-in as part of a ClickOnce deployment, the behavior of the ClickOnce download depends on the privileges that are assigned to the agent who is logging in. If the agent is granted the privilege to execute a plug-in, the plug-in is downloaded as part of the deployment.

The Procedure: Installing plug-ins for Workspace is a general procedure that describes how to install plug-ins for Workspace. The documentation for your plug-in provides specific information about how to install and deploy your plug-in.

**Consult the documentation that comes with your plug-in for specific information about how to install and provision your plug-in.**

Before you install your plug-in, you must provision it in Genesys Administrator Extension (refer to the Genesys Administrator Extension documentation for more information) in the same way that you provision Workspace.

Workspace plug-ins come with `<Plug-In Name>.apd` and `<Plug-In Name>.xml` (privileges) files, both of type `Workspace`. Upload the `<Plug-In Name>.apd` file and attach the `<Plug-In Name>.xml` file to create the `<Plug-In Name> Template`.

The Workspace application object is created based on the `Workspace Template`.

When you provision the Privileges that are assigned to a Role, the list of Privileges that are available for the `Workspace` application type combine the privileges that are specified in the `Workspace.xml` and `<Plug-In Name>.xml` files.

> ### Important
> Ensure that you do not use the template and metadata files "Workspace (Agent desktop).apd" and "Workspace (Agent desktop).xml" when working with plug-ins.

## Procedure

### Installing plug-ins for Interaction Workspace

**Purpose:**

To install plug-ins for Workspace on your web server, an agent workstation, or a development workstation.

**Prerequisites**

- .NET Framework 4.5
- Installation of the Workspace application by using one of the following procedures:
  - Deploying The ClickOnce Application On Your Web Server. Choose this option if you want to deploy Workspace as a ClickOnce application. Install the plug-ins after you install the Workspace application on your server, but before you run the Workspace Deployment Manager.
  - Installing The Developer Toolkit. Choose this option if you want to deploy the Workspace developer package. Refer to About Workspace Extension Samples and Deploying and Executing the Extension Samples for information about reorganizing files to enable the debugging of samples with plug-ins.
  - Installing The Workspace Application. Choose this option if you want to deploy a non-ClickOnce version of Workspace.

### Start

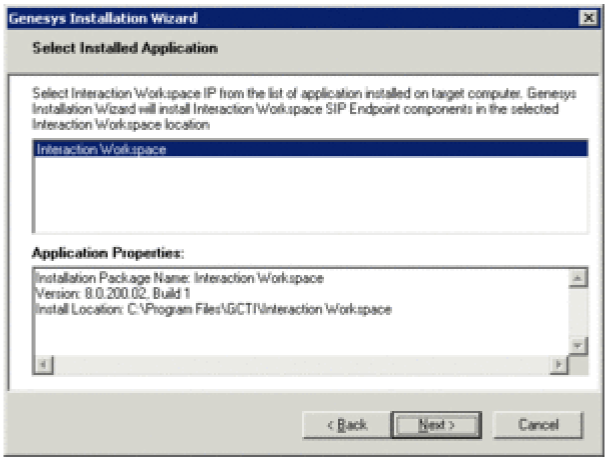
1. On your desktop, open the disc that contains the plug-in IP or the plug-in IP and double-click the `Setup.exe` file.

   You might be asked to reboot your system to delete or rename certain system files before the Installation Wizard runs.

   The Genesys Installation Wizard launches and the `Welcome` panel is displayed.

2. On the `Welcome` panel, do one of the following:
   - Click `Next` to begin the installation procedure.
   - Click `Cancel` to exit the Genesys Installation Wizard.
   - Click `About` to open the plug-in ReadMe in your default browser.

   If you clicked `Next`, the `Select Installed Application` panel is displayed (see the Figure - **Select Installed Application Panel of the Genesys Installation Wizard**).



Select Interaction Workspace IP from the list of application installed on target computer. Genesys Installation Wizard will install Interaction Workspace SIP Endpoint components in the selected Interaction Workspace location

Installation Package Name: Interaction Workspace
Version: 8.0.200.02, Build 1
Install Location: C:\Program Files\GCTI\Interaction Workspace

Select Installed Application Panel of the Genesys Installation Wizard

3. The `Select Installed Application` panel enables you to select the Workspace application instance to which you want to add the plug-in.

   The Genesys Installation Wizard searches the target computer for an installed version of Workspace. Select the version of Workspace in the location in which you want plug-in to be installed.

   The `Application Properties` pane displays the name, version, and location of the selected Workspace application (see the Figure - **Select Installed Application Panel of the Genesys Installation Wizard**).

4. After you have selected the version of Workspace that you want to use with the plug-in, do one of the

following:

- Click `Next` to proceed to the next panel.
- Click `Cancel` to exit the Genesys Installation Wizard.
- Click `Back` to return to the previous panel.

If you clicked `Next`, the `Ready to Install` panel is displayed.

5. On the `Ready to Install` panel do one of the following:
   - Click `Install` to install the plug-in on your web server, development workstation, or agent workstation.
   - Click `Back` to return to the `Select Installed Application` panel.
   - Click `Cancel` to exit the Genesys Installation Wizard.

   If you clicked `Next`, plug-in is installed in the location that you specified. When installation is complete, the `Installation Complete` panel is displayed.
6. Click `Finish` to exit the Genesys Installation Wizard.

   Plug-in files are copied into the target installation directory of the original Workspace deployment.

   After the plug-in application is installed on the agent or developer workstation, or after it is downloaded by the ClickOnce application (see Deploying The ClickOnce Application On Your Web Server), and after the agent is granted permission to use the application, agents must login Workspace on a Place that is associated with a SIP DN to use the plug-in with Workspace. The plug-in process is started automatically when Workspace application is being initialized.

**End**

**Next Steps**

- (Optional) If you are deploying Workspace as a ClickOnce application on your web server, go to the Procedure: Deploying The ClickOnce Application On Your Web Server. When the **Workspace Deployment Manager Package Information** pane is displayed, you can specify that your plug-in is installed with the ClickOnce package.
- (Optional) If you are deploying Workspace for development purposes, go to About Workspace Extension Samples.
- Installation is complete. You can provision the plug-in functionality. Refer to the documentation that accompanies your plug-in IP.

# Installing the Screen Capture application

Screen Capture is not currently available for Workspace.

# Provisioning functionality

These topics introduce the functionality of Workspace and provide information about provisioning the functionality to suite the needs of your contact center. For details about using the functionality, refer to the *Workspace 8.5 User's Guide* and *Workspace Context-Sensitive Help*.

For details about how to use Genesys Administrator Extension to provision Genesys applications, refer to *Genesys Administrator Extension Help* and *Genesys Administrator Extension Deployment Guide*.

Workspace provides a secure agent interface to the Genesys 8 Suite. The functionality of Workspace is controlled for each agent by Role Based Access Control (RBAC). This section describes the functionality in general terms. Refer to the *Workspace 8.5 User's Guide* and *Workspace Context-Sensitive Help* for detailed explanations of the functionality and interface use.

### Basic agent configuration

Find information about how to get an agent's account ready for the agent to login and start using Workspace.

Setting Up Agents On The System

Overriding Workspace Options

Accessibility And Navigation

Agent Login And Authentication

### Set up interaction channels

Find detailed information about how to configure communication channels like voice, outbound, email, and chat.

Configuring the Behavior of Incoming Interactions

Channels and Interaction Handling

Enabling Internal And External

### Additional agent configuration

Find additional procedures for enabling reporting, KPIs, and contact management.

Managing Contacts

KPIs and Contact Center Statistics

Reporting

### System security and customization

Find all of the procedures that you need to protect your system, ensure business continuity, and balance interaction loads.

Hiding Selected Data In Logs

Client-side Port Security

Business Continuity for SIP Server, Configuration Server, and Statistic Server eServices Load Balancing Business Continuity

Load Balancing Using Clusters

Customizing Display Names for Configuration Objects

# Setting up agents on the system

[**Modified:** 8.5.112.08, 8.5.117.18, 8.5.143.08]

Refer to *Genesys Administrator Extension Help* and *Genesys Administrator Extension Deployment Guide* for detailed information on how to use Genesys Administrator Extension and Management Framework to configure access permissions.

## 1. Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group

**Purpose:**

To restrict the privileges that are assigned to an agent or agent group.

The security.disable-rbac configuration option in the `interaction-workspace` section determines whether agents have all privileges granted or whether the Role-Based Access Control (RBAC) control system is used.

> Important
>
> RBAC requires Configuration Server 8.0.2 or higher. RBAC requires Genesys Administrator 8.0.2 or higher, or Genesys Administrator Extension (9.0.100.56 or higher is recommended).

If security.disable-rbac is set to `true`, RBAC is disabled and all privileges are assigned to all agents and Agent Groups. If security.disable-rbac is set to `false`, RBAC is enabled and you must assign roles to agents and Access Groups.

> Important
>
> Beginning with Workspace 8.5.143.08, Workspace supports both the Genesys Administrator Role storage model and the Genesys Administrator Extension Role storage model. Before you create a Role, refer to Role-Based Approach of Genesys 8 for more information about using these different storage models.

**Prerequisites**

- Genesys Administrator 8.0.200.29 or higher or Genesys Administrator Extension (9.0.100.56 or higher is recommended), configured to show Advanced View.

- Configuration Server 8.0.2 or higher.
- A working knowledge of Genesys Administrator Extension.
- Workspace Application Template in the Configuration Layer.

**Start**

1. Create the Workspace `Application` object from the Workspace Application Template.
2. From the `Tenant` drop-down list, select the Tenant for which you want to create the role.
3. In the Genesys Administrator Extension `Provisioning` view, select `Accounts` in the `Navigation` column.
4. Select the `Roles` view.
5. In the `Roles` view, click `New`.
6. In the `Configuration` tab, specify the following `General` parameters:
    - A name for the role.
    - A description of the role (optional).
    - Whether or not the role is enabled.
7. In the `Configuration` tab, specify a list of users or access groups in the `Members` view.
8. In the `Role Privileges` tab, click `Workspace privileges`.
9. Initially, all privileges are unassigned. To assign a privilege, click the drop-down list in the `Value` column that is associated with the privilege and select `Allowed`. Refer to Role Privileges for a list of all the privileges.
10. To save the new role, click `Save and Close`. The new role is now applied to the specified agents and Agent Groups. For information on privilege conflicts, refer to Conflict Resolution for Configuration Options.

    To discard the new role without saving your changes, click `Cancel`.

**End**

## 2. Optimizing the Login window

[**Modified:** 8.5.114.08]

> **Important**
>
> Refer to Agent login, authentication, and logout for detailed information about configuring agent accounts and Places for login and authentication.

**Purpose:**

To control the behavior of the Workspace Agent Login Window.

> ### Tip
>
> - Agent login can be configured as either a one-step or a two-step process depending on whether you want to prompt the agent for connection parameters in the secondary login window or specify the parameters for the agent.
> - For a list of configuration options that are related to login, refer to Login.
> - You can specify whether agents login to a Place or Place Group.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.

**Start**

1. Configure the agent for two-step login by setting the options that control Password, Queue, Switch, and Place.
   a. If the agent must enter a phone-set Password, set the login.voice.prompt-dn-password option to `true`. The second login window is displayed after the agent is authenticated. A phone-set Password prompt will be displayed in the secondary login window.
   b. If the agent must enter a Queue at login, set the login.voice.prompt-queue option to `true`. A Queue prompt will be displayed in the secondary login window.

      If the switch has multiple logins for the agent, the agent will be prompted to enter the particular login that they want to use.
   c. For details about setting up Places or Place Groups, refer to Place Selection. Several options control Place login:
      i. If the agent must enter a Place at each login, set the login.prompt-place option to `true`.
      ii. If the agent always logs in to a default Place at each login, do the following:
         - Assign a default Place in the Agent `Advanced` tab.
         - Set the login.prompt-place option to `false`.
         - Set the login.default-place option to `true`.
      iii. If the agent must specify a Place only the first time that the agent logs in (**Note:** The Place is stored in the local settings of the agent):
         - Set the login.default-place option to `false`.
         - Set the login.prompt-place option to `false`.

4. Configure the agent for one-step login by using the following configuration-option settings:

- Set the login.voice.prompt-dn-password option to `false`.
- Set the login.voice.prompt-queue option to `false`.
- Set the login.prompt-place option to `false`.

**Note:** If the default Place in the Agent Advanced tab is blank, the agent will have to perform a two-step login the first time that the agent logs in to a particular workstation.

**End**

## 3. Provisioning Workspace for the Voice channel

**Purpose:**

To enable an agent to log in to the Voice channel.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.
- T-Server with associated switch and switching office.
- A Switch that is configured with DNs that correspond to agent devices in the switch.
- Agent logins that are configured in the Switch that can be referred by agents.
- A Place that contains one or more DNs from the Switch.

**Start**

### For each agent that you want to configure to use the Voice channel, do the following:

1. Reference at least one `AgentLogin` from the Switch.
2. Check the `isAgent` flag.
3. Set a default Place. (Optional)
4. Allow the voice media privilege (see Voice Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role, allowing an Interaction Workspace privilege, and assigning a Role to an agent or agent group).
5. Allow the voice media privileges that you want the agent to use (see Voice Privileges).
6. Configure the voice options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Voice configuration option reference for a list of Voice options and a description of how to configure them).

**End**

> **Tip**
>
> Agents sometimes click **Hang up** by accident while handling a call. Use the voice.prompt-for-end option to ensure that a confirmation dialog box is displayed so that the call is not ended accidentally.

## 4. Provisioning a hybrid voice agent

### Example: Provisioning a hybrid Skype for Business and Workspace SIP Endpoint agent

[**Added:** 8.5.117.18]

In the past, Workspace has supported a single Voice channel represented by a softphone (Workspace SIP Endpoint, Skype for Business, and so on) or a hard phone during an agent session. Beginning with 8.5.117.18, you can set up agents to have multiple voice devices on the same Place so that they can be hybrid agents with typically at least one voice device, being a softphone, and the second one a hard phone or another softphone. Typical device combinations include:

- Skype for Business DN + SIP Server Voice DN (embedded SIP Endpoint or hard/soft SIP Phone)
- Skype for Business DN + Voice DN of a non-SIP Server system
- Voice DNs from any two voice systems (such as a third party vendor and SIP Server)

> **Important**
>
> In hybrid mode, two voice channels are supported, but only one IM channel can be supported. If hybrid mode agents are set up to use IM, all IM interactions should be handled by the same T-Server (SIP Server or T-Server for Skype for Business) to avoid functional issues. Furthermore, it is not possible to send IMs between SIP Server and Skype for Business Server.

With this configuration, agents can make calls and Workspace selects the best device to use according to configuration and internal rules to select the best way.

During login, the agent chooses a Place that is set up to support multiple devices.

While logged in, the agent can independently control and view the status of the two devices in the **My Channels** tab.

Supervisors can monitor any device for silent monitoring, coaching, and barge-in of hybrid agents as soon as Workspace supports the supervision capability of the corresponding voice channel.

## Important

- If both voice channels are software devices running on an agent workstation, this solution supports a single headset for both devices.
- The two devices cannot be used simultaneously. One call must be on hold while the other is active. If an agent accepts a call on another device, the first device is automatically put on hold.

**Purpose:**

To enable an agent to log in to two separate Voice channels, one for Skype for Business and one for Workspace SIP Endpoint.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- T-Server with associated switch and switching office.
- A Switch that is configured with DNs that correspond to agent devices on the switch.
- Agent logins that are configured on the Switch that can be referred by agents.
- An environment that contains one T-Server for Skype for Business and one SIP Server and associated Switches.
- (optional) ISCC connection between SIP Server and T-Server for Skype for Business, using **cast-type**=`route`.
- A Trunk between SIP Server and Skype for Business Server.
- A Place that contains one voice DN from SIP Server and one DN from the Skype for Business Switch.

**Start** For each agent that you want to configure to be a hybrid Voice agent, do the following:

1. Reference at least one `AgentLogin` from the Switch.
2. Check the `isAgent` flag.
3. Set a default Place. (Optional)
4. Allow the voice media privilege (see Voice Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role, allowing an Interaction Workspace privilege, and assigning a Role to an agent or agent group).
5. Allow the voice media privileges that you want the agent to use (see Voice Privileges).
6. Configure the voice options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Voice configuration option reference for a list of Voice options and a description of how to configure them).

7. In the `interaction-workspace` section, set the value of the `spl.switch-policy-label` on the Skype for Business Switch annex to `SIPSwitch::Lync`.
8. In the `interaction-workspace` section, set the value of the `display-name` or `display-name.<language-code>-<country-code>` option on the Switch annex to the display name of the switch object as you want it to appear in Team Communicator and the **My Channels** tab. The value of this option overrides the `name` property of the switch.
9. In the `interaction-workspace` section, set the value of the expression.callable-phone-number on the Switch or DN annex to the pattern of phone numbers that can be dialed from this switch or DN. You can use this option to limit the numbers that can be called from each switch or DN in a hybrid environment.

   Examples:

   a. You could configure the SIP Server to dial only outgoing calls and Skype for Business only for internal calls.

   b. If you have Skype for Business urls like these:

      - `sip:lync-user13_qa95@lyncdco13.lab`
      - `sip:lyncuser13_qa95@lyncdco13.lab`

      You could set the regular expression value of the `expression.callable-phone-number` option to `sip:\w+-?\w+@\w+\.\w+`.
10. Set the value of the voice.hybrid-switch-preference option to a comma-separated list of switch names in your hybrid environment. The order of the names specifies the preferred switch when the call policy does not favor either switch.

**End**

# 5. Enabling Workspace to play ring tones

**Purpose:** To enable Workspace to play ring tones for inbound interactions on one or more devices.

In Interaction Workspace 8.0 and 8.1, tones were played through the embedded Windows Media Player application on a single audio device that was configured as the default console sound device in the Windows Sound configuration panel. Starting from 8.5.0, the sounds are played through the Direct Sound API, which enables more flexibility on the device(s) that are used to play the sound.

The following procedure enables you to specify whether tones are played on the default audio device, a secondary audio device, or both.

A secondary audio device can be defined as either a specific audio device or all of the non-default audio devices. You can individually each configure sound (ringing bells, state changes, and so on).

All file formats that are playable by Windows DirectShow are usable (*.wav; *.mpa; *.mp2; *.mp3; *.au; *.aif; *.aiff; *.snd).

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.

**Start**

1. Enable the secondary audio device(s) by specifying the value of the new application.secondary-audio-out-device configuration option to the name of the secondary audio device or by specifying the value `$AllNonDefault$` to enable all non-default audio divices.
2. The following existing configuration options have been modified in Workspace 8.5, and higher, to enable a tone to be played on the default audio device, a secondary audio device, or both.
   - webcallback.ringing-bell
   - chat.ringing-bell
   - chat.new-message-bell
   - email.ringing-bell
   - im.new-message-bell
   - im.ringing-bell
   - outbound-callback.ringing-bell
   - outbound.sound.campaign-updated
   - sms.ringing-bell
   - voice.ringing-bell
   - <media-type>.ringing-bell
   - accessibility.agent-state-change-bell
   - accessibility.interaction-state-change-bell
   - accessibility.warning-message-bell
   - broadcast.sound.minimal-priority
   - broadcast.sound.low-priority
   - broadcast.sound.normal-priority
   - broadcast.sound.high-priority
   - broadcast.sound.important-priority

   For each of these options, you can add an additional parameter to the end of the ringing sound configuration string:

   - `|primary`—Play the sound on the default audio output device
   - `|secondary`—Play the sound on the secondary audio device, as defined by the application.secondary-audio-out-device configuration option
   - `|both`—Play the sound on the default and secondary (application.secondary-audio-out-device configuration option) audio devices
3. You can restrict which sound files are pre-loaded when an agent logs in by using the sounds.preloadfiles option. Pre-loading only selected sound files at login can improve bandwidth performance at the start of

a shift when many agents log in simultaneously.

**End**

## 6. Declaring and using new Not-Ready Reason codes

**Purpose:**

To enable an agent to use custom Not-Ready Reason codes and to support the `aux work` mode.

The only Not-Ready Reasons that Workspace supports by default are `Unknown` and `After Call Work`. Custom Not-Ready Reason codes are defined in the `Action Codes` folder of the `Desktop` folder in the `Provisioning` view of Genesys Administrator Extension.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.

**Start**

1. Create a new Action Code in the following Genesys Administrator Extension view: `Provisioning > Desktop > Action Code`.
2. Enable the new Action Code so that it can be used in the Configuration Layer.
3. To enable the Action Code to display in the Agent Interface, configure the agent-status.enabled-actions-global option in the `interaction-workspace` section of the Workspace `Application` object (refer to the Agent status configuration option reference for a list of agent status options and a description of how to configure them).
4. Configure the Workspace agent-status.not-ready-reasons option to include the value that is specified in the Action Code (refer to the Agent status configuration option reference). Not-Ready Reasons are displayed in the order that is defined by the value of the agent-status.not-ready-reasons option. If no value is specified for the agent-status.not-ready-reasons option, the default behavior is to display all Not-Ready Reasons that are defined and enabled in the Action Code folder.

**End**

## 7. Storing the agent profile on a controlled shared host

[**Added:** 8.5.112.08]

**Purpose:**

To enable agents to store preferences and configuration information on a common directory instead of in the Configuration Database or their local workstation.

Genesys recommends using this feature in contact centers that have a large number of agents. The goal of this feature is to reduce the amount of information being sent back and forth between Workspace and Configuration Server. Workspace stores many agents specific preferences and other information both locally (on the agent's workstation) and in the Configuration Database. In some environments, this means that a large amount of configuration data is sent from Configuration Server to Configuration Server Proxy (CSP) and then from CSP to Workspace.

This feature also supports contact center where agents are not required to log in to Workspace from the same workstation each time. This feature supports agent roaming to different workstations. In environments where agents do not always use the same workstation, locally stored configuration data and personalized information is available only on the workstation where the agent first logged in. Use the following procedure to set up your environment to enable agents to roam by storing agent configuration, preferences, and personalized information in a common shared directory.

To set up your environment to support this feature, administrators should work with IT to set up a host where agent information is stored so that it does not have to be stored on Configuration Server or locally on the agent workstation.

Genesys recommends the following best practices that you can discuss with IT.

## Security

When you create a directory on the host, the agent windows user must have write access. Workspace will write encrypted files that only Workspace running on the agent account can read. You do not have to create explicit permissions for the files. The files should inherit their permissions from the user's folder on the host. You can choose to set up a personal or a global shared directory.

When you implement the procedure below, agent information on Config Server will be merged with the new file location. Once that is complete, it will no longer be necessary for agents to have write access to the agent annex in the Configuration Layer; however, if you remove write access, you must grant it each time that that you need to change record location.

## Recommendations about external storage selection

When you create the user profile storage on a network share, follow the Microsoft Windows Group Policy Object Management practices for the redirection of User Profile Folder, following the principles of the definition of the Network Share.

Genesys recommends one of two approaches; however, your IT might have other approaches that they might want to employ.

1. Personal Network Space

   Configure the agent workstations with a login script that assigns a Drive letter to a personal network space for the agent. In this scenario, the profile configuration can explicitly refer to this area. Security is ensured by the design of the Personal network share.

   For example: `G:\WDE\Profile`

2. Dedicated User Profile storage

   Microsoft recommends this approach to administrate the sharing of Roaming Profiles.

In this scenario, the IT administrator must define the first level of security when the share is configured. For example, refer to How to enable Roaming Profiles on Windows Server 2012 R2

A second level of security is implemented at run time by the capability for Workspace to restrict access permissions to the created folder and files. In Microsoft Windows, use the following optional setting for Folder Redirection configuration: **Grant the user exclusive rights**. This setting is enabled by default. This setting specifies that the administrator and other users do not have permissions to access this folder.

### Share sizing suggestions

Use the following guidelines for *minimum* sizing requirements for each agent when setting up the storage folders.

- `externalUserSettings.conf`: Contains about 100 options and requires at least 10 KB
- Peronsal Favorites: 10 favorites is about 7 KB; 100 favorites is about 70 KB
- List of pushed-url: 10 items is about 3 KB; 100 items is about 30 KB
- List of Recents (recent contacts): 10 contacts is about 8 KB; 100 contacts is about 80 KB

## Migration considerations

When Workspace starts, it checks to determine whether a value is specified for the options.record-location option. If no value is specified, Workspace does nothing. If a directory is specified, Workspace checks to determine if the directory exists a the location. If it does not exist, Workspace tries to create it; therefore, Workspace must have permission (*read/write access) to create directories and file on the specified location.

Workspace then compares the location specified by the `options.record-location` option with the last location where personal information was stored. If these locations are different, Workspace attempts to migrate the data from the previous location to the specified location.

If the migration fails, Workspace will attempt to complete the migration again the next time that the application is started; and, if the value of the options.clean-up-former-record-location option is set to `true`, Workspace will not remove data from the former location.

If the migration is successful and the value of the `options.clean-up-former-record-location` option is set to `true`, Workspace will remove data from the former location.

### Migration use case 1

The User Profile was previously configured to be stored in Person's annex and is then configured to be stored in a shared directory. The content of the annex in the configuration layer is copied to the shared directory. Workspace will no longer access the Configuration Layer to store personal information.

### Migration use case 2

The User Profile was previously configured to be stored in a shared directory and is then configured to be stored in Person's annex in the Configuration Layer. The content of the shared directory is copied to the Person's annex in the configuration layer. Workspace will no longer access the personal directory to store personal information.

### Migration use case 3

The User Profile storage location is modified from one shared directory to another shared directory. The content of the first shared directory is copied to the second shared directory. Workspace will no longer access the first shared directory to store personal information.

> **Warning**
>
> Profile data that is stored on a workstation cannot be migrated.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.
- Agent objects created in the Configuration Database.

**Start**

1. Create a shared directory on a host for your agents.
2. If you you have previously configured the value of the options.record-option-locally-only option to `true` to store the agent profile information locally instead of in the Configuration Database, set the value to `false`.
3. Use the options.record-location option to specify the path to the shared directory on the host that you created. The full path can also contain the following field codes: `$Agent.UserName$`, `$Agent.LastName$`,`$Agent.FirstName$`,`$Agent.EmployeeId$`,`$Env.X$` (where X is the name of the environment variable). Genesys recommends that you append the agent's `Username` to the specified path as shown above.

**End**

## 8. Enabling accessibility features

[**Modified:** 8.5.102.06, 8.5.109.16, 8.5.143.08]

**Purpose:**

To enable agents to use the accessibility and navigation features of Workspace.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator

Extension.

- A working knowledge of Genesys Administrator Extension.
- A Workspace Application object exists in the Configuration Database.

**Start**

1. In Genesys Administrator Extension, open the Workspace Application.
2. Select the Application Options tab.
3. In the interaction-workspace section, configure the following option value:
    - accessibility.visual-impairment-profile: Specify true to optimize Workspace for keyboard navigation and screen reader applications.
    - In the interaction-workspace section, configure the following option values to specify whether or not the Interaction Preview should receive the focus when it is displayed on the desktop:
        - accessibility.focus-on-interaction-toast: Specifies whether all Interaction Notification views receive the focus when they are displayed. This option does not rely on accessibility.visual-impairment-profile; therefore, it applies to all configured agents, not just visually impaired agents. By default, the Interaction Notification views do not receive then focus automatically; agents must click the view to make it active.
        - accessibility.<media-type>.focus-on-interaction-toast: Specifies that all Interaction Notification views for the <media-type> receives the focus when they are displayed. When specified, this option overrides the value specified for accessibility.focus-on-interaction-toast. This option does not rely on accessibility.visual-impairment-profile; therefore, it applies to all configured agents, not just visually impaired agents.
4. In the interaction-workspace section, configure the following option values to add sounds to specific interface events:
    - accessibility.agent-state-change-bell: Specify the name of the sound file that you want to play to the agent when the agent changes state.
    - accessibility.interaction-state-change-bell: Specify the name of the sound file that you want to play when an interaction changes state.
    - accessibility.warning-message-bell: Specify the name of the sound file that you want to play when a warning message is displayed to the agent.
    - <media-type>.ringing-bell: Specify the name of the sound file that you want to play to the agent when an interaction of <media-type> is received.
    - chat.new-message-bell: Specify the name of the sound file that you want to play to the agent when a new chat message is received.
    - im.new-message-bell: Specify the name of the sound file that you want to play to the agent when a new IM message is received.
5. To enable the high contrast theme for visually impaired agents, in the interaction-workspace section, configure the following option value:
    - gui.themes : Specify only the value HighContrast.
6. To change the default display size of interface elements in Workspace views, use the gui.magnification-factor.

> **Important**
>
> This feature functions only with the default Workspace 8.5 GUI themes, and to custom themes that are developed according to the documentation and samples of the *Workspace Developer's Guide*. If the blue, royale, and fancy legacy themes are used, the magnification is forced to normal.

7. To enable agents to set the zoom of text editing fields, such as email, chat, and SMS, and transcript areas, use the gui.editor-zoom-range option to specify minimum and maximum text zoom. This feature applies to the following views:
   - IM (text entry, transcript, and interaction data tooltip)
   - Chat (text entry, transcript, and interaction data tooltip)
   - Email (text entry and inbound email view)
   - SMS (text entry, transcript, and interaction data tooltip)
   - Interaction history
     - IM
     - Chat
     - Email
     - SMS
   - Standard responses
   - Social media (text entry only)
8. To specify how long contextual warning messages are displayed to agents, set the number of seconds by using the alert.timeout option. You can specify that message notifications must be manually closed by setting the value to `0`.

**End**

# 9. Enabling security features

**Purpose:**

To enable the security features of Workspace.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.

**Start**

1. In Genesys Administrator Extension, open the Workspace Application.
2. Select the Application Options tab.
3. Configure any of the following options in the `Security` section:
    - security.disable-rbac: Specify whether Role Based Access is applied to agents to control access to Workspace features and functionality.
    - security.inactivity-timeout: Specify whether the agent workstation locks after a certain period of inactivity.
    - security.inactivity-set-agent-not-ready: Specify whether the agent is automatically set to `Not Ready` when agent inactivity is detected.
    - security.inactivity-not-ready-reason: Specify the default Not Ready Reason if the agent's workstation times out.
4. Configure any of the following options to control appearance of sensitive data in logs:
    - log.default-filter-type: Specify the default filter type for logging.
    - log.filter-data.<keyName>: Specify the treatment of log data. Enables you to filter for specific attached data keys, by specifying the key name in the option name.
    - sipendpoint.system.diagnostics.log_filter: Specifies the list of keys of SIP Messages for which the value should be hidden in the log files.

**End**

## 10. Creating Corporate Favorites

**Purpose:**

To enable the use of corporate favorites in the Team Communicator.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.

**Start**

1. In Genesys Administrator Extension, open the Workspace Application.
2. Select the Application Options tab.
3. Create a new section and name it with the name of the Corporate Favorite that you want to create.
4. Configure the new Corporate Favorite section to be one of the following types:
    - `Agent`
    - `Agent Group`

- `Skill`
- `Queue`
- `Interaction Queue`
- `Routing Point`
- `Custom Contact`

The Table **Corporate Favorite Options by Type** defines the Corporate Favorite types and the mandatory options.

**Corporate Favorite Options by Type**

| Type | Options | Mandatory | Valid values | Example |
|---|---|---|---|---|
| Agent | type | Yes | Agent | Agent |
| | id | Yes | <user name of the agent> | User123 |
| | category | Yes | <a semicolon-separated list of category names> | CorporateCategory1;FavoriteAger |
| Agent Group | type | Yes | AgentGroup | AgentGroup |
| | id | Yes | <name of the agent group> | Agent Group Meridian |
| | category | Yes | <a semicolon-separated list of category names> | CorporateCategory1;FavoriteAger |
| Skill | type | Yes | Skill | Skill |
| | id | Yes | <name of the skill> | French |
| | category | Yes | <a semicolon-separated list of category names> | French Speaking Agents; Mandarin Speaking Agents |
| Queue | type | Yes | Queue | Queue |
| | id | Yes | DN number in the following format <DN>@<SwitchName> | 123@MySwitch |
| | category | Yes | <a semicolon-separated list of category names> | CorporateCategory1;FavoriteAger |
| Interaction Queue | type | Yes | InteractionQueue | InteractionQueue |
| | id | Yes | <script name of the interaction queue> | queue_email_inbound |
| | category | Yes | <a semicolon-separated list of category names> | CorporateCategory1;FavoriteAger |
| Routing Point | type | Yes | RoutingPoint | RoutingPoint |
| | id | Yes | DN number in the following format | 123@MySwitch |

| Type | Options | Mandatory | Valid values | Example |
|---|---|---|---|---|
| | | | <DN>@<SwitchName> | |
| | category | Yes | <a semicolon-separated list of category names> | CorpRoutingPoint |
| Custom Contact | type | Yes | CustomContact | CustomContact |
| | category | Yes | <a semicolon-separated list of category names> | External Resources |
| | firstname | No | <any string> | First |
| | lastname | No | <any string> | External |
| | phonenumber | Yes (one or both) | <a semicolon-separated list of phone numbers> | +1555234567890;+5551234543 |
| | emailaddress | | <a semicolon-separated list of email addresses> | external1@mail.dom; external2@mail.dom |

5. The list of corporate favorites can be defined by the teamcommunicator.corporate-favorites options or by using the `teamcommunicator.corporate-favorites` field in an XML file.

   Configure one or both of the following options in the `interaction-workspace` section of agent, agent group, tenant, and/or application annexes:

   - teamcommunicator.corporate-favorites: The list of corporate favorites (quick dial favorites) that are configured in the Configuration Layer in GAX or in a XML file containing corporate favorites for an Agent, Agent Group, Skill, Routing Point, Queue, Interaction Queue, or Custom Contact in the same tenant as the agent. Favorites that are configured at the agent level take precedence over those that are configured at the agent group level, which take precedence over the tenant level, which takes precedence over the application level.
   - teamcommunicator.corporate-favorites-file: The name and the path to an XML file that contains a list and definition of each corporate favorite. The path can be relative to the Workspace working directory (for example: `Favorites\CorporateFavorites.xml`) or an absolute path (for example: `C:\PathToFavorites\CorporateFavorites.xml`).

   The corporate favorites functionality works in one of **three** ways, depending on how you choose to configure the two options and whether corporate favorites are specified in the Configuration Layer or in an XML file:

   - If teamcommunicator.corporate-favorites-file is *not* configured and corporate favorites are specified in the Configuration Layer.
     - Workspace selects corporate favorites only from the list of favorites specified by the teamcommunicator.corporate-favorites option for the Main Window Team Communicator and the Interaction Window Team Communicator.
     - Corporate Favorites in the Interaction Window Team Communicator, for operations such as transfer and conference, can be overridden by favorites specified by a transaction object override.
   - If teamcommunicator.corporate-favorites-file *is* configured, an XML file is present, the XML file *does not* include the **<teamcommunicator.corporate-favorites>** parameter, and the teamcommunicator.corporate-favorites option *is* configured in the Configuration Layer.
     - Workspace searches for corporate favorites from the list of favorites in the XML file that are specified by the teamcommunicator.corporate-favorites option.

  - Corporate Favorites in the Interaction Window Team Communicator, for operations such as transfer and conference, can be overridden by favorites specified by a transaction object override *only if* those favorites are included in the XML file.

- If teamcommunicator.corporate-favorites-file *is* configured, an XML file is present, and the XML file *includes* the **<teamcommunicator.corporate-favorites>** parameter, for example:

```
 <interaction-workspace>
  <teamcommunicator.corporate-favorites>fav2;fav3</teamcommunicator.corporate-
favorites>
  </interaction-workspace>
```

  - Workspace selects only corporate favorites from the XML file specified by the **<teamcommunicator.corporate-favorites>** parameter for the Main Window Team Communicator and the Interaction Window Team Communicator.
  - Workspace ignores the teamcommunicator.corporate-favorites option in the Configuration Layer.
  - For operations such as transfer and conference, corporate favorites *cannot* be overridden by a transaction object.

6. To enable each interaction to have an independent list of corporate favorites that are dynamically loaded into the corporate favorites in the team communicator view of the current interaction, configure the following options:

   a. Configure a Transaction object of type `list`. For example, you could configure a Transaction object that is named: `IW_CorporateFavoritesOverrideOptions`.

   b. In the `interaction-workspace` section configure the `teamcommunicator.corporate-favorites` option to a value such as `fav1` as described in the previous steps.

   c. To the `interaction.override-option-key` option in the `interaction-workspace` section, set a valid key name, for example `IW_OverrideOptions`.

   d. Add the Transaction object name to the `AttachedData` in your strategy. In this example, set the value of `IW_OverrideOptions` to `IW_CorporateFavoritesOverrideOptions`.

   Refer to the Modifying a Routing Strategy to Override Workspace Options, Based on Attached Data section for a general description of this mechanism.

**End**

## Corporate Favorites sample XML

The following is an example of an XML file that is used to define corporate favorites:

```
<?xml version="1.0" encoding="utf-8"?>
<options>
<interaction-workspace>
<teamcommunicator.corporate-favorites>fav2;fav3</teamcommunicator.corporate-favorites>
</interaction-workspace>
<fav3>
<category>Partners</category>
<type>Agent</type>
<id>Jim</id>
</fav3>
<fav2>
<category>CorporatePartners;Partners2</category>
<type>Agent</type>
<id>John</id>
```

```
</fav2>
<fav4CustomContact>
<category>CorporatePartners</category>
<type>CustomContact</type>
<firstname>Bob</firstname>
<lastname>Davis</lastname>
<phonenumber>+12121231234;+18001231234</phonenumber>
<emailaddress>bob@genesys.com;sales@genesys.ca</emailaddress>
</fav4CustomContact>
<fav5RoutingPt>
<type>RoutingPoint</type>
<category>RoutingPoint</category>
<id>122@LucentG3</id>
</fav5RoutingPt>
<fav6AgentGroup>
<category>CorpAgentGroup</category>
<type>AgentGroup</type>
<id>Agent Group Meridian</id>
</fav6AgentGroup>
<fav7Skill>
<category>CorpSkill</category>
<type>Skill</type>
<id>Email-QualityConfidencePercentageSkill</id>
</fav7Skill>
<fav8ACDQueue>
<category>CorpACDQueue</category>
<type>Queue</type>
<id>8000@1LucentG3</id>
</fav8ACDQueue>
<fav9IxnQueue>
<category>CorpIxnQueues</category>
<type>InteractionQueue</type>
<id>route-to-agent-group-8002</id>
</fav9IxnQueue>
</options>
```

# Overriding Workspace options

## Modifying A Routing Strategy to override Workspace options based on attached data

Refer to *Genesys Administrator Extension Help* and *Genesys Administrator Extension Deployment Guide* for detailed information about how to use Genesys Administrator Extension and Management Framework to configure access permissions.

### Procedure

Modifying a Routing Strategy to override a Workspace option based on attached data

**Purpose:** To override previously defined configuration options by using a Routing Strategy.
A Routing Strategy can be used to override configuration options that you have defined by using the hierarchies described in Configuration And Administration By Using Options And Annexes.
Workspace uses Transaction Objects of type `object list`. Attach a transaction name or list of transaction names to the interaction in your strategy. The transaction names in the list should be separated by commas. Workspace reads the transaction objects at rendering time to override the static options.
Overriding options enables you to change the appearance of interactions per line of business based on a key-value pair that is defined in the annex of Transaction objects. The attached data contains the name of the transaction object(s) to be used for the interaction.
**Prerequisites**

- Deploying Workspace
- Strategy that routes to your Workspace agent workstations.

**Start**

1. Configure one or more Transaction objects, of type `list`, in Genesys Administrator Extension or Composer, by using the standard approach that is used for other object types in the hierarchy (these rely on the option reference to determine if a particular option can be overridden in a Transaction).
   You can only override options in the `interaction-workspace` section. Therefore, you must replicate the `interaction-workspace` section to the annex of the object level where you want the override to occur (Tenant, Group, User, or Transaction).
2. Configure the option interaction.override-option-key to define the key where the Transaction object(s) are to be listed in attached data (refer to the Interaction configuration option reference for a list of Interaction options and a description of how to configure them).
3. Using either IRD or Composer, edit your routing strategy by adding an "Attach" or "Multi-attach" block that attaches the key value pair that is defined below:
   - key: The name of the key that you defined in the option set in Step 2.
   - `value`: One or several comma-separated Transaction objects, as defined in Step 1.

**End**

# Accessibility and navigation

[**Modified:** 8.5.113.11, 8.5.124.08, 8.5.143.08]

Workspace enables you to navigate the user interface by using the keyboard and keyboard shortcuts instead of the mouse to enhance your productivity. Navigation works panel to panel, and within a panel, component to component. Keyboard navigability enables users who are using a device for accessibility that relies on keyboard navigation to manipulate the desktop components.

## Accessibility overview

[**Added:** 8.5.143.08]

Genesys provides a Voluntary Product Accessibility Template® - VPAT® report from ITI, to document conformance of Genesys Workspace Desktop Edition to WCAG 2.1 Level A specification. The VPAT® report is a standardized template for documenting conformance to various accessibility specifications. VPAT® report provided by Genesys follows the W3C/WAI's WCAG 2.1 specification, as this is an international standard adopted and recognized by our customers worldwide. The Genesys VPAT® can be downloaded here: Genesys Workspace Desktop Edition Accessibility Conformance Report.

### What is WCAG?

Web Content Accessibility Guidelines (WCAG) 2.1 covers a wide range of recommendations for making Web content more accessible. Following these guidelines will make content more accessible to a wider range of people with disabilities, including accommodations for blindness and low vision, deafness and hearing loss, limited movement, speech disabilities, photosensitivity, and combinations of these, and some accommodation for learning disabilities and cognitive limitations; but will not address every user need for people with these disabilities. These guidelines address accessibility of web content on desktops, laptops, tablets, and mobile devices. Following these guidelines will also often make Web content more usable to users in general.

## Screen reader compatibility

Workspace employs a visual impairment profile feature. This feature enables more elements in the Main Window and the Interaction window to have the focus, enhancing step-wise navigation for screen-reading applications such as Job Access With Speech (JAWS) screen reader from Freedom Scientific. Screen readers enable visually impaired (blind and low vision) agents to use the desktop interface through text-to-speech or text-to-braille. Workspace must be configured in the Configuration Layer to enable this compatibility. These options can be set in the Configuration Layer as default values that can be overwritten in the Agent Annex. The Workspace windows are designed to maximize content readability for screen-reader applications.

## JAWS compatibility

[**Added:** 8.5.124.08]

Use the following two options to ensure compatibility with the JAWS screen reader:

- accessibility.visual-impairment-profile: Specifies whether the profile for visually impaired users is active. This option enables more interface elements to be focusable (accessible from keyboard navigation and mouse-over) so that they can be navigated from Screen Reader applications. [**Added:** 8.5.113.11]
- accessibility.disable-hyperlinks: Specifies whether processing and presenting hyperlinks in email, chat, and SMS as active elements are disabled or enabled. [**Added:** 8.5.124.08]

## Controlling interaction notifications

[**Added:** 8.5.101.14]

By default, the Interaction Notification views do not receive then focus automatically; agents must click the view to make it active. To ensure that screen reader applications can read the content of the Interaction Notification views, you must specify whether or not the text content of Interaction Notification views will receive the focus. In screen reader environments, any window that has the focus is read by the screen reader to the agent. Use the following two configuration options to automatically assign the focus to the Interaction Notification view when it is displayed:

- accessibility.focus-on-interaction-toast—Specifies whether all Interaction Notification views receive the focus when they are displayed. This option does not rely on the accessibility.visual-impairment-profile option; therefore, it applies to all configured agents, not just visually impaired agents.
- accessibility.<media-type>.focus-on-interaction-toast—Specifies that all Interaction Notification views for the <media-type> receives the focus when they are displayed. When specified, this option overrides the value specified for `accessibility.focus-on-interaction-toast`. This option does not rely on accessibility.visual-impairment-profile; therefore, it applies to all configured agents, not just visually impaired agents.

> **Important**
>
> If these options are not specified, then the user must use ALT+TAB to navigate to the Interaction Notification view when it is displayed.

# High contrast Workspace

[**Added:** 8.5.100.05]

Workspace enables visually impaired agents to use a high contrast theme to compliment the Windows high contrast themes that are available from the Windows Personalization control panel. The Workspace high contrast theme follows Web Content Accessibility Guidelines (WCAG) 2.0, with some limitations. The Workspace high contrast theme was tested against red/green and blue/yellow color deficit vision.

> **Tip**
>
> The Workspace high contrast theme functions whether or not one of the Windows high contrast themes are in use.

Enable the Workspace high contrast theme by setting the value of the gui.themes configuration option. To direct the user to the High Contrast theme by default, specify only the value `HighContrast`, removing the other values (`Default,Blue,Royale,Fancy`).

The `gui.themes` option can be configured at the application, skill, group, and agent levels. You can configure `gui.themes` so that specific agents or agent groups have only the high contrast theme available. This ensures that the high contrast theme is the default theme when those agents login.

To make the login window displayed in high contrast, you must make the following edit to the `interactionworkspace.exe.properties` file, which is part of the Workspace package that is pushed to the workstation of the agent who requires the high contrast theme:

1. In the section `<appsettings>` uncomment the line that contains `gui.theme`.
2. Set the following value: `<add key="gui.theme" value="HighContrast" />`

## Overriding default font and icon sizes

[**Added:** 8.5.102.06] [**Modified:** 8.5.109.16]

Workspace specifies the size at which interface elements are displayed so that no matter what magnification or reduction a user specifies for their browser or operating system, these items are displayed consistently. However, some agents might change the browser or operating system settings to increase font size and improve readability. To enable agents to change the size at which interface elements, including fonts and icons, are displayed, use the gui.magnification-factor configuration option to specify the ratio that is applied to the Workspace interface.

> **Important**
>
> This feature functions only with the default Workspace 8.5 GUI themes, and to custom themes that are developed according to the documentation and samples of the *Workspace Developer's Guide*. If the blue, royale, and fancy legacy themes are used, the magnification is forced to normal.

Use the gui.editor-zoom-range option to enable agents to set the zoom of text editing fields, such as email, chat, and SMS, and transcript areas. The gui.editor-zoom-range option is used to specify the minimum and maximum text zoom. This feature applies to the following views:

- IM (text entry, transcript, and interaction data tooltip)
- Chat (text entry, transcript, and interaction data tooltip)

- Email (text entry and inbound email view)
- SMS (text entry, transcript, and interaction data tooltip)
- Interaction history
    - IM
    - Chat
    - Email
    - SMS
- Standard responses
- Social media (text entry only)

To ensure that the login dialog box is also displayed at the same ratio, configure the `gui.magnification-factor` option in the `..\Interaction Workspace\InteractionWorkspace.exe.config` file after you install Workspace on the workstation of an agent who requires a different display size.

## Configuring accessibility features

[**Modified:** 8.5.100.05, 8.5.113.11]

Use the Procedure: Enabling Accessibility Features to enable the Accessibility features for your agents.

Use the following options in the `interaction-workspace` section to configure Accessibility:

- accessibility.agent-state-change-bell: Specifies the agent state change sound configuration string.
- accessibility.interaction-state-change-bell: Specifies the interaction state change sound configuration string.
- accessibility.warning-message-bell: Specifies the warning message sound configuration string.
- accessibility.visual-impairment-profile: Specifies whether the profile for visually impaired users is active. This option enables more interface elements to be focusable (accessible from keyboard navigation and mouse-over). Beginning with version 8.5.113.11, Workspace enables agents to enter TABs in the email composition area of outgoing email interactions by pressing the **TAB** key if the value of this option is set to `false`; to use the **TAB** key to step to the next control or field, agents must first press **Ctrl-TAB** to step out of the text composition area. To disable this feature, set the value of this option to `true`; agents will not be able to enter TABS in the email composition area, but they can use the **TAB** key to move to the next control in the tab order.
- chat.new-message-bell: Specifies the path to the alert sound file for new chat messages.
- email.ringing-bell: Specifies the path to the alert sound file for new email interactions.
- im.new-message-bell: Specifies the path to the alert sound file for new SMS messages.
- chat.new-message-bell: Specifies the path to the alert sound file for new chat messages. [**Added:** 8.5.124.08]
- sms.ringing-bell: Specifies the path to the alert sound file for new SMS Session messages.

- voice.ringing-bell: Specifies the path to the alert sound file for new voice interactions.
- <media-type>.ringing-bell: Specifies the path to the alert sound file for new workitems.
- gui.themes: Specifies that the high contrast theme is avalaible to agents.
- gui.magnification-factor: Specifies the default display size of fonts and icons in the Workspace views.

# Agent login, authentication, and logout

[**Modified:** 8.5.112.08, 8.5.124.08, 8.5.138.04, 8.5.140.08, 8.5.141.04]

Agent login is a two-step process:

1. User authentication and selection of Place in the primary login dialog box
2. Selection of advanced parameters in the secondary login dialog box. Workspace enhances the security of your system by limiting agent login to basic authentication. Workspace further enhances security by enabling you to limit the choices that are presented to an agent at login.

> **Important**
>
> When an agent logs in to Workspace, the application creates a list of headsets that are plugged in to the workstation. If an agent wants to use a different headset, he or she should exit Workspace, plug in the new headset, then relaunch Workspace.

## User authentication

When Workspace is launched by an agent, the agent must provide a user name and password as authentication. After authentication the Configuration Layer is accessed by Workspace to obtain the list of existing places and privileges that are granted to the agent, as well as the configuration of the Workspace application for that agent.

You can specify whether the username is stored locally in the user profile so that the next time the agent logs in the username is populated automatically. [**Added:** 8.5.103.10]

> **Important**
>
> If Workspace is started from the silent command line, the username is never stored.

### Changing passwords

You can require agents to automatically change their password the first time that they log in to the system. You can assign temporary passwords to new agent objects when you create them, and then specify that the password must be changed before the new agent is able to log in to Workspace for the first time.

You can also enable agents to change their passwords by selecting the `Change Password` action from the Interaction Workspace Main Menu.

Use the following Security privilege to enable the password change feature:

- Can Change Password

Refer to the *Genesys Security Guide* for a complete description of password policies and how to configure them.

## Kerberos user authentication

[**Added:** 8.5.102.06] [**Modified:** 8.5.132.05, 8.5.135.05]

Workspace supports Kerberos single sign-on (SSO) authentication. This means that agents only have to authenticate once on their workstations to start using Workspace. If Kerberos authentication is not used, agents must still login to Workspace after authenticating on their workstations.

You must configure your Genesys Management Framework to support Kerberos (refer to Chapter 4: Kerberos External Authentication of the *Framework External Authentication Reference Manual* and the *Genesys Security Guide*).

Workspace requires that you specify the unique Service Principal Name (SPN) that is used in each Configuration Server and Configuration Server Proxy that handles SSO requests from UI applications.

To specify the Service Principal Name in the software package:

- **ClickOnce deployment:** You can specify the Service Principal Name parameter in the **Deployment Manager Wizard** if you are installing Workspace as a ClickOnce application or by using Console Mode.
- **Non-ClickOnce deployment:** Edit the login.kerberos.service-principal-name option in the interactionworkspace.exe.config property file, which is located in the Workspace Installation Package (IP), and add the following line:

```
<appSettings>
  ...
  <add key="login.kerberos.service-principal-name" value="<SPN Name>"/>
  <add key="login.url" value="tcp://<host><port>/AppName" />
  <add key="login.connections.parameters.isenable" value="false" />
  ...
 </appSettings>
```

- To specify how Workspace retrieves agent identity using the Windows API set the login.kerberos.agent-identification option in the interactionworkspace.exe.config configuration file. The value should also match the way agent usernames are synchronized in the Genesys Configuration Layer. See the description of the authentication/enable-upn option in the the **Configuration Option** section of the *Framework External Authentication Reference Manual*. The valid values are:
  - implicitupn: Workspace uses the Implicit User Principal Name (iUPN), which is a combination of the **samAccountName** and the user's Domain. [**Added:** 8.5.140.08]
  - samaccountname: (default value) Workspace uses the SAM Account Name attribute specified by Windows Administrator in Windows Active Directory when provisioning the account of an agent (8.5.110.13 and higher).
  - upn: Workspace uses the User Principal Name (UPN) specified by Windows Administrator in Windows Active Directory when provisioning the account of an agent (8.5.132.05 and higher). **This mode is deprecated and should be substituted by** implicitupn, but is maintained for compatibility

purposes.

    - windowsidentity: Workspace uses the information entered by the agent when opening the Windows session. Depending on the Windows authentication mechanism, this method can return the exact case typed by the agent in the login dialog, which might not match the user name configured in Genesys Configuration Layer. This is the API used in Workspace versions up to 8.5.109.25.

- For environments using Kerberos authentication, set the value of the login.kerberos.enable-case-insensitive-agent-identification option to true to specify that the matching of the username stored in the Genesys Configuration layer and the username specified by the login.kerberos.agent-identification option is *not* case-sensitive (the case of the letters is ignored). [**Added:** 8.5.135.05]

If Kerberos is configured, the agent login process works as follows:

If the Workspace property file is defined to enable Kerberos authentication, Workspace tries to acquire a Kerberos ticket. If the Kerberos ticket is found, Workspace tries to open a connection to Configuration Server using this ticket.

- If the connection attempt is successful, Workspace bypasses the first Workspace Login view and displays the second Login view or immediately displays the Main Toolbar. For more information about launching and logging in to Workspace, refer to the *Workspace Desktop Edition 8.5.1 Help*.
- If connection is not successful because of an invalid Kerberos ticket, a warning message is displayed to the agent, and the application start-up is interrupted.

You can override the error message that is displayed to agents if Workspace is unable to obtain a Kerberos ticket by using the methodology to customize a dictionary to specify an alternative message string for the Windows.login.Kerberos.Retry key.

# Place selection

[**Modified:** 8.5.114.08, 8.5.112.08, 8.5.138.04]

Genesys 8 requires that each agent connect to a unique Place. Depending on your environmental constraints, you can adjust the Place selection process to make it completely invisible to the agents or to minimize the effort required to select the correct Place where the agent logs in.

## Fine-tuning Place selection

You can control or improve the way that agent Place selection is handled. This section describes optional Place selection fine-tunings that are available.

### Static Place

To assign a static Place to an agent and make Place selection invisible during login, in Genesys Administrator Extension you must assign a Default Place to the Agent in the **Advanced** tab of the Agent object Properties section and set the value of the login.default-place option to $Agent.DefaultPlace$, and set the value of the login.prompt-place option to false.

### Auto-complete

You can configure the agent account using the login.prompt-place option so that during authentication the agent must specify a Place in the `Place` field of the secondary login dialog box. If the value of the login.enable-place-completion is `true`, a list of Places is displayed to agents according to the text entered in the **Place** field; this feature enables agents to choose the appropriate Place without typing the entire Place name.

### Last used Place

To optimize the Place selection process, you can configure Workspace to store the last used Place in the Windows User Profile by setting the value of the login.store-recent-place option to `true`. If this information is available in the Windows User Profile the next time the agent logs in, this *recent* Place is proposed to the agent for confirmation during login. If the agent confirms that the recent Place is the correct one, the agent will be able to proceed with the connection to this Place without having to select it in the second login screen.

### Hot seating

The Windows User Profile can be fully or partially set up for roaming/hot seating depending on how your environment is set up and the available infrastructure.

This means that in environments where the Windows User Profile of the agent stored from Workstation A, corresponding to Place 1 where the agent sits on Day 1, can be available on Workstation B, corresponding to Place 2 where agent sits on Day 2. However, in this scenario, the Place restored from the Windows User Profile and proposed as the *recent* Place might be incorrect.

Beginning with Workspace **8.5.112.08**, you can configure the environment so that the stored Place is associated with information that corresponds to the workstation where the agent sits when an agent selects the Place. This Place is then presented to the agent as the *recent* Place during login only if it was previously stored with the current workstation as an associated identifier.

Use the login.place-location-source option to specify how Workspace stores the last selected login Place in the Windows User Profile when the value of the login.store-recent-place option is set to `true`. The following values (modes) are supported:

- `standard`: The most recently used Place is stored in the Windows User Profile without any information about the workstation. This is the legacy recent place storage mode.
- `machine-name`: The most recently used Place is stored in the Windows User Profile, along with the name of the machine where the Workspace application is running. Use this value when Workspace is installed on the physical workstation where the agent logs in.
- `vdi`: The most recently used Place is stored in the Windows User Profile, along with the name of the physical workstation from which the agent executes a virtual session (for example, in Citrix XenApp/XenDesktop, VMWare Horizon, and Windows Terminal Server environments). Use this value when Workspace is installed in a Virtual Desktop Environment. If the machine name of the VDI client is not found, for example because agents are running Workspace on a physical workstation, the `machine-name` mode is used instead. This setting is appropriate for hybrid environments where agents are running Workspace alternatively in physical workstations and in virtual sessions. [**Added:** 8.5.112.08]

## SIP DN type selection

[**Added:** 8.5.138.04]

You can create multiple Places associated with different types of SIP DNs for each agent to enable them to login from different devices, such as Workspace SIP Endpoint and Genesys Softphone when they are in the office, and their mobile through SIP Server or a 3rd party SIP Endpoint when they are working at home or outside the office. Alternately, you might want a hard phone back up for your soft phone in case there are issues with an agent's endpoint.

Use the voice.device-type option in the `interaction-workspace` section of the Annex of the DN object to specify whether the DN associated with a Place is Workspace SIP Endpoint or Genesys Softphone (`auto`), or whether it is a hard phone or 3rd party SIP Endpoint (`separate`).

Genesys recommends that you name your Places in a way that it will make it easy for agents to figure out which one to choose. For example, in the office you might have a desk associated with a soft phone labeled with "SIP-abc123". When the agent sits at the desk associated with the "SIP-abc123" Place, the agent specifies "SIP-abc123" in the Place field of the login screen. For an agent calling in from their mobile or home phone, you might name the Place that the agent should enter when they log in as "Agent XYZ Mobile". It is up to you to train your agents on which Place to enter when they log in.

## Automatic Place selection using Place Groups

[**Added:** 8.5.114.08]

In traditional voice contact centers, a Place contains a DN that represents a hard or a soft phone and agents select it (manually or automatically) according to the location where they work. As contact centers evolve, some individuals that handle calls might be back office workers who login intermittently, while others are workers answering from home or on a mobile device. In each of these situations, the phone that is used is not directly monitored by the Contact Center infrastructure. Creating a static Place/DN pair for each one of these worker/phone combinations is a management issue because of the large number of Places that might be unused at any given time.

To solve this issue, you can enable agents to automatically select a Place using Place Groups. A Place Group makes a small number of Places available to any agent that selects the Place Group when they log in.

Depending on which approach you choose, during login, either your agents either select a Place or a Place Group, or you can assign them a specific default Place Group.

> ### Warning
>
> The *Automatic place selection using Place Groups* feature currently works only with SIP Server for DNs that are provisioned to support the remote login capability, which is enabled by the login.voice.prompt-dn-less-phone-number option.
>
> The feature is *not* supported for:
>
> - DNs that are used with Workspace SIP Endpoint

- Places that also support eServices channels

A Place Group is a preconfigured collection of Places, each containing a preconfigured Extension DN. When an agent logs in, Workspace selects a free Place from the group based on information provided by Statistic Server and assigns it to the agent.

The physical phone number typed by the agent, according to the capability enabled by the login.voice.prompt-dn-less-phone-number option in the `PlaceGroup` option, is stored in the settings of the DN contained in the selected Place.

To use this capability, complete the following steps:

1. Create one or more Place Group objects and add to it all the Places that you want to include in the group.
2. At the Agent, Agent Group, Application, or Tenant level, use the login.place-selection-type option to specify whether agents can select within a list of Places and/or a Place Groups when they log in.
3. At the Agent, Agent Group, Application, or Tenant level, use the login.available-place-groups option to specify the list of Place Groups that is presented to the agent. You can specify a list of Place Group names, or use the `$All$` keyword to enable agents to select from all the Place Groups to which they have read access.
4. Check that the login.voice.prompt-dn-less-phone-number option is enabled, to ensure that the Login on Place Group capability has access to the agent's phone number. You can either specify the option in the traditional Application, Tenant, AgentGroup, Agent hierarchy, or specify it in the PlaceGroup object so that it is taken into account only when this Place Group is selected.

You can also use the login.default-place option at the Agent, Agent Group, Application, or Tenant level to specify a default Place Group for an Agent or a group of Agents.

### Important

The following options treat Place Groups as Places:

- login.enable-place-completion
- login.prompt-place
- login.store-recent-place

## Optimizing the use of eServices Interaction Server licenses

[**Added:** 8.5.108.11]

To enable the operational engagement of Agents in an eServices workflow, the eServices system relies on the following technical license scheme:

- **Seat licenses:** Agents or supervisors require one seat license to:
  - handle interactions of one or more eServices media type
  - access the content of workins or interaction queues.
- **Media Channel licenses:** One media license of the corresponding type is required for each media type that is enabled for an agent to handle interactions.

Refer to Genesys Licensing Guide for details about the different types of eServices licenses.

Workspace does not directly manage eServices licenses; however, the way that it interacts with Interaction Server or Interaction Server Proxy has a direct influence on the way that licenses are checked out or checked in by Interaction Server.

Workspace enables you to manage (optimize) the checkout of eServices licenses by your agents and supervisors by using the eservices.disconnect-on-logoff. You can choose either the legacy behavior (pre-8.5.108.11) or the optimized behavior (8.5.108.11 and higher).

## Legacy seat license and media checkout

The legacy behavior of license checkout when the value of the eservices.disconnect-on-logoff option is set to `false` is as follows:

1. A seat license is checked out when:
   - an agent logs in Workspace and this agent is granted the privilege to use at least one eServices channel (email, chat, social, and so on), or,
   - an agent logs in Workspace and this agent is granted the privilege to use Team Workbin or Interaction Management privilege, or,
   - an agent is notified that he or she is part of a push preview campaign and this agent is granted the privilege to use Outbound.

   In all these cases, the seat license is checked-in when the agent exits the application. Agents can access the content of their Personal or Shared Workbins at any time during the session, independently from media channel status.
2. One media license of a specific type (email, chat, custom, and so on) is checked-out as soon as the agent logs on the corresponding media channel. This can be done automatically at application start-up by implicit or explicit selection of media, or manually during an application session by global or selective media Log On. The media license is checked-in when the corresponding media is logged off manually, or when the agent exists the application.

   The custom media license that corresponds with the ‘outboundpreview’ media login is checked out the first time the agent is notified that he or she is assigned to a push preview campaign, and is checked in when the agent logs off voice channel or exists the application.

## Optimized seat and media license checkout

The optimized seat and media license checkout feature is particularly applicable to environments where the license distribution between Voice and eServices seats is asymmetric, for example in systems where the number of Chat seats represent 20% of the total number of Voice seats, and all the agents are granted the privilege to handle voice and chat interactions.

To configure the optimized license and media checkout behavior, set the value of the eservices.disconnect-on-logoff option to `true`. The license checkout behavior is as follows:

1. A seat license is checked out when:
    - an agent logs on at least one eServices channel in Workspace, either at login time by implicit or explicit selection of media, or manually during an application session by global or selective media Log On. The seat license is checked-in when the last eServices media is logged off manually, or when the agent exists the application (**Warning:** The Agent cannot access the content of his or her Personal or Shared Workbins when no eServices media is logged on), or,
    - when an agent logs in Workspace while this agent is granted the privilege to use Team Workbin or Interaction Management. In this case the seat license is checked in when the agent exits Workspace, or,
    - when an agent is notified that he or she is part of a push preview campaign and this agent is granted the privilege to use Outbound. In this case the seat license is checked in when the agent logs off the voice channel (it will be checked out again when voice channel is logged on again) or when he or she exits Workspace.
2. The media license checkout/checkin life cycle in the optimized license model is the same as in legacy license model.

> **Important**
>
> For both the legacy and optimized licensing model, the opening of the connection to Interaction Server or Interaction Server Proxy is synchronous with the seat license check-out and its closing is synchronous with the seat license is check-in.

## Specification of advanced login parameters

Advanced login parameters are defined by the privileges, such as channel privileges, that are assigned to a particular agent. The privileges assigned to a particular agent, therefore, determine which advanced parameters, if any, are displayed in the secondary login dialog box.

The Place that is specified by an agent also determines the advanced login parameters that is available to be specified by the agent. For example, if the Place is associated with a voice channel, the agent must also provide login and queue information for each assigned DN. Other advanced parameters that might be required include SIP phone numbers.

Advanced parameters can be preset for agents—making it unnecessary for the agent to specify advanced parameters.

### Application options that control login

The following are the most commonly used application options in the `interaction-workspace` section to control agent login (more options can be found here):

- login.default-place—Specifies the default Place that is proposed to the authenticated agent at login.
- login.enable-place-completion—Enables the name of the Place to be completed as the agent types.
- login.im.can-unactivate-channel—Specifies whether the agent can select and deselect (activate and deactivate) IM channels.
- login.im.prompt-agent-login-id—Specifies whether the agent can select a login id from the configured ones for the IM channel in the login window.
- login.im.prompt-dn-password—If applicable, prompts for the IM channel password in the secondary login dialog box.
- login.im.prompt-queue—If applicable, prompts for the ACD Queue in the secondary login dialog box.
- login.place-location-source—Specifies how Workspace stores the last selected login Place in the Windows User Profile when the value of the login.store-recent-place option is set to `true`. [**Added:** 8.5.112.08]
- login.prompt-place—Specifies whether the agent must enter a place in the login window.
- login.store-recent-place—Specifies whether the most recently used Place on the workstation is stored and displayed for the agent at the next login.
- login.store-username—Specifies whether the most recently used Username is stored locally in the user profile. If the value is `false`, the previous value is cleared. [**Added:** 8.5.103.10]
- login.voice.can-unactivate-channel—Specifies whether the agent can select and deselect (activate and deactivate) voice channels.
- login.voice.prompt-agent-login-id—Specifies whether the agent can select a login id from those configured for the voice channel in the login window.
- login.voice.prompt-dn-password—If applicable, prompts for the DN password in the secondary login dialog box.
- login.voice.prompt-queue—If applicable, prompts for the ACD Queue in the secondary login dialog box.
- login.workmode—Specifies the work mode that is applied when the user of the voice DN logs in. If set to `auto-in`, the agent is automatically in Ready state. If set to `manual-in`, the agent must manually activate the Ready state. To determine whether your switch supports the work mode, refer to the Deployment Guide of the relevant T-Server.
- login.<media-type>.can-unactivate-channel—Specifies whether the agent can select and deselect (activate and deactivate) particular channels.
- login.<media-type>.is-auto-ready—Specifies whether the indicated workitem channel is automatically set to the Ready state at login.

## DN-less login configuration options

- login.voice.prompt-dn-less-phone-number—Specifies whether a DN-less phone number is prompted for in the login window. This option is specific to the SIP Server environment.
- login.voice.use-dn-less-login-extension—Specifies how the DN-less phone number specified by an agent during login is propagated to the Genesys back-end. Passing as an extension to SIP Server limits the impact of multiple simultaneous login or logout events in the case of a Disaster Recovery/Business Continuity event. SIP Server 8.1.102.93 or higher is required for this feature. Refer to Remote Agents with Non-provisioned DNs for more information. [**Added: 8.5.141.04**]

## Using the command line to start Workspace

You can pass certain Workspace login information through the command line when you start the Workspace application:

```
interactionworkspace.exe -url tcp://<host>:<port>/<appli> -u <user> -p <password> -place
<place>
where:
<host>: host name or IP Address of Configuration Server
<port>: port of Configuration Server
<appli>: Interaction Worksapce application name in Management Framework
<user> Username of the agent
<password> Password of the agent (optional)
<place> Place where the agent log to (optional)
```

### Important

You must pass all of the parameters on the command line. For example, you cannot pass only the `host`, `port`, `appli` and `place`, and then prompt for the username and password, for example.

If parameters are typed manually in the first login window, they are stored in the local user profile and restored to the login window at the next login session. If the parameters of the first login window are passed by the command line, thereby bypassing the first login window, then the parameters are not saved in the local user profile.

### Warning

When the command-line is used to run Workspace Desktop Edition there is no way to prompt any login parameter, neither in the first nor in the second login screen. The purpose of running from the command-line is to by-pass the login screens and to immediately display the Workspace toolbar. As a consequence the following `login.*` options are by-passed by the command-line start:

- login.<media-type>.can-unactivate-channel = false
- `login.<media-type>.available-queues` = `ACDQueue`
- `login.<media-type>.prompt-queue` = `true`
- `login.<media-type>.prompt-agent-login-id` = `false`
- `login.<media-type>.prompt-dn-password` = `false`
- login.voice.prompt-dn-less-phone-number = `false`
- login.voice.use-dn-less-login-extension = `false`
- login.store-username = `true`
- login.place-location-source = `standard`

> - login.store-recent-place = `true`
> - login.default-place = <any value>
> - login.prompt-place = `false`
> - login.enable-place-completion = `true`

### Kerberos Single Sign-on

(Optional) To use Kerberos Single Sign-on (SSO) you must omit the user name and password. The URL is mandatory. Place is optional when the agent is configured with a “default place” in Management Framework:

```
interactionworkspace.exe -url tcp://<host>:<port>/<appli> -place <place>
where:
<host>: host name or IP Address of Configuration Server
<port>: port of Configuration Server
<appli>: Interaction Workspace application name in Management Framework
<place> Place where the agent log to (optional)
```

## Logout

[**Added:** 8.5.124.08]

Agents log out by selecting **Exit** from the **Main Menu** in the Workspace Window. Agents cannot log out if they have active interactions on their desktop.

You can modify logout behavior by using the following two options:

- logout.enable-exit-on-logoff-error
- login.voice.restore-dn-less-phone-number-on-logout [**Added:** 8.5.140.08]
- logout.voice.use-login-queue-on-logout

# Managing agent status

[**Modified:** 8.5.124.08]

Workspace provides options that enable agents to control their status. Use these options to populate the Workspace status menu with one or more of the following privileges:

- Global Ready
- Global Not Ready (with reason code)
- Global DND (Do Not Disturb)
- Global After Call Work
- Global Log Off
- Global Login

The options enable the following agent states:

- Logged off
- DND (Do Not Disturb)
- After Call Work
- Not Ready - Full (Multiple Reasons)
- Not Ready - Full (Single Reason)
- Ready - Partial (for example, ready on one channel)
- Ready - Full

Workspace also enables detailed agent and place status management through options. Agents can set individual channels to the following states:

- Ready
- Not Ready
- Do Not Disturb
- After Call Work
- Logged off
- Call Forwarded (for voice)

Other configurable agent privileges include the following:

- Refine advanced login parameters, when applicable (for example, Place, and Queue)

You can use the following options in the `interaction-workspace` section to control the contents of the command menu in the Workspace Main Window.

- agent-status.enabled-actions-by-channel: Defines the available agent state actions in the My Channels contextual menu. The actions are displayed in the order in which they appear in the list.
- agent-status.enabled-actions-global: Defines the available agent states in the global Status menu. The agent state commands are displayed in the order in which they appear in the list.

You can set automatic not-ready reasons for individual channels by media-type at login time.

- login.<media-type>.auto-not-ready-reason: Specifies the Not Ready Reason code that is displayed for the specified channel. If the login.<media-type>.is-auto-ready option is set to `true`, the login.<media-type>.auto-not-ready-reason is ignored.

## Voice Channel status

[**Modified:** 8.5.124.08]

You can configure Workspace to automatically set the agent status to the former status when an agent clicks **Done**. This enables an agent to return to their former status as soon as he or she has completed after call work, instead of having to manually change their status. [**Added:** 8.5.103.10]

- voice.cancel-after-call-work-on-done: Specifies that the After Call Work state is changed to the former status when an agent clicks **Done**.

For SIP Server environments, you can control whether agents can request an extension to After Call Work by using the following option: [**Added:** 8.5.124.08]

- voice.after-call-work-extension: Specifies that the After Call Work state is unrestricted, can be extended, or is restricted to the interval specified in the SIP Server *Emulated Agents* configuration, pps. 251-252; Wrap-up time configuration is also explained on p. 546.

> ### Important
>
> If an agent manually changes status while still engaged in a voice interaction, their status will display the change, but the time in status is suspended until the call is ended.

# Managing agent inactivity

[**Modified:** 8.5.139.06]

For security purposes, Workspace can be configured to lock the application, if an agent has not used the keyboard or mouse for a period that you specify. All user input is blocked until the agent provides login information to unlock the application.

When Workspace is locked, the following conditions occur:

- The following windows are minimized or hidden when the application is locked:
  - Main window
  - Statistics Gadget
  - Interaction window
  - My Channels
  - My History
  - My Statistics
  - My Contact Center Statistics
  - My Messages
- The following windows/controls remain visible, but are disabled:
  - Interaction notifications (case information is not displayed)
  - System tray icon
- An authentication dialog window is displayed.
- A notification that the agent should authenticate to unlock Workspace is displayed.
- System notices are not locked.

## Inactivity timeout

[**Modified:** 8.5.139.06]

You can use the following option in the `interaction-workspace` section to control the inactivity timeout.

- security.inactivity-timeout: Specifies the amount of time in minutes of agent inactivity (no mouse or keyboard usage) that triggers application locking. If the agent has been inactive longer than the number of minutes that are specified by the inactivity timeout, the agent must reauthenticate to be able to use the Interaction Workspace application. A value of `0` disables this functionality.
- security.inactivity-set-agent-not-ready: Specifies whether the agent is automatically set to Not Ready

when agent inactivity is detected.

- security.inactivity-not-ready-reason: Specifies the Not Ready Reason if the security.inactivity-set-agent-not-ready option is set to `true`.
- security.inactivity-force-not-ready-state: Specifies whether channels that are already in Not Ready status (with or without a Not Ready Reason) are switched to the Not Ready Reason specified by the security.inactivity-not-ready-reason option when the agent is set to Not Ready when their workstation is locked. Depends on security.inactivity-set-agent-not-ready. If the value of this option is set to `false`, only the status of channels in the Ready and After Call Work statuses are updated. [**Added:** 8.5.140.08]

## Managing workstation screen lock

[**Added:** 8.5.139.06]

Sometimes agents lock their workstation without first setting their status to Not Ready. If this happens, the agent will still be the target of Voice and Digital Channels interactions. You can configure Workspace to automatically set agent status to Not Ready or Not Ready with a Reason when their workstation is locked by using the following configuration options:

- security.session-lock-set-agent-not-ready: Specifies whether the agent channels status is switched to Not Ready automatically when the Windows session is locked while the agent state is Ready, After Call Work, and optionally Not Ready.
- security.session-lock-not-ready-reason: Specifies the Not Ready Reason to be used when the agent status is forced to the Not Ready with a Reason status. Depends on security.session-lock-set-agent-not-ready.
- security.session-lock-force-not-ready-state: Specifies whether channels that are already in a Not Ready status (with or without a Not Ready Reason) are switched to the Not Ready Reason specified by the security.session-lock-not-ready-reason option when the agent is set to Not Ready when their workstation is locked. Depends on security.session-lock-set-agent-not-ready. If the value of this option is set to `false`, only the status of channels in the Ready and After Call Work statuses are updated.

# Configuring the behavior of incoming interactions

[**Modified:** 8.5.116.10]

(Formerly: **Previewing Incoming Interactions**)

For information about automatic contact assignment for incoming interactions, see Contact Management.

## Configuring the Interaction Preview window

Interaction Preview is rendered through an Interactive Notification pop-up from the System Tray from the Workspace icon. The Interactive Notification pop-up preview handles inbound notification for ringing voice interactions (SIP or TDM) or SIP interaction preview or incoming eServices interactions (email, chat, or workitem). The preview contains sufficient information to enable agents to determine whether to accept or reject an interaction. The following privileges enable these actions:

- Accept Interaction or Accept Preview
- Reject Interaction or Decline Preview

In a Voice environment, if the `Reject` privilege is granted to an agent, the Reject function is available only for an incoming voice call if T-Server provides information about the queue or Routing Point that is used to deliver the call to the agent.

> Tip
>
> You can control the behavior of the Voice Reject function by using the interaction.reject-route configuration option.

You can use the following options in the `interaction-workspace` section to configure the Interaction preview:

- interaction.case-data.format-business-attribute: Specifies the case-data format.
- interaction.case-data.frame-color: Specifies the color of the border of the Case Data view frame. Examples: #FFFFBA00 for a Gold color, #FF6F7074 for a Silver color, and #FFB8400B for a Bronze color. This option can be overridden by a routing strategy.
- voice.ringing-bell: Specifies the voice channel ringing sound configuration string.
- interaction.override-option-key.

To configure an agent for SIP Preview, see the Procedure: Enabling an agent to use the SIP Preview feature.

## Configuring the behavior of new interactions

[**Added:** 8.5.116.10]

You can specify how new interaction windows behave after an agent who is working on one or more interactions accepts a new inbound interaction. You can choose to have the new interaction window receive the focus (default behavior), or you can choose to keep the focus on the currently active interaction window. You can also configure this behavior by media channel. For example, you might choose to have newly accepted email interactions appear in the background and newly accepted voice interactions to receive the focus.

Use the following new configuration options to control the behavior of new interaction windows:

- interaction.auto-focus: Specifies whether a new inbound interaction should be in focus automatically when it is accepted.
- interaction.auto-focus.<media-type>: Specifies whether a new inbound interaction of the specified media type should be in focus automatically when is accepted. When this option is defined it overrides the `interaction.auto-focus` option.

### Outbound/outgoing interactions

Newly created outbound/outgoing interactions always receive the focus. These options do not affect them.

### Inbound interactions

If there are no other active interactions, newly accepted (or auto-accepted) inbound interactions always receives focus.

If active interaction(s) exist in Workspace, and option is set for the media type of newly accepted inbound interaction to not automatically receive focus, the new interaction will not be in focus when it is accepted or auto-accepted.

### Focus Time calculations

When interactions are accepted, but are displayed in the background, focus time calculations do not begin until the agent selects the interactions window and gives it the focus.

# Channels and interaction handling

[**Modified:** 8.5.110.13, 8.5.111.21, 8.5.115.17, 8.5.117.18, 8.5.118.10]

The following media types are supported by Workspace:

- Voice and SIP Voice
- Voicemail
- Outbound Campaigns
- E-Mail
- Chat
- Video
- SMS and MMS
- Callback [**Added:** 8.5.111.21]
- Web Callback
- Workitems
- Social Media:
  - Facebook (by using an eServices plug-in)
  - Twitter (by using an eServices plug-in)
  - RSS (by using an eServices plug-in)

## Force close stuck interactions

[**Modified:** 8.5.118.10]

Since 8.0, Workspace has enabled agents to force-close stuck interactions (at the case level) by using the **Force Close This Case** feature. Prior to 8.5.118.10, this capability was unconditional and could result in a real active interaction becoming uncontrollable by agents.

Beginning with 8.5.118.10, you can use the interaction.unconditional-force-close option to control the behavior of this feature. When this option is set to `false` (the *new* default value), Workspace disables the Force Close feature, but enables it only when the following conditions are detected:

- T-Server reports that the voice or IM call on which an operation is requested is no longer under agent control
- Interaction Server reports that the eServices interaction on which an operation is requested is no longer under agent control

## Common interaction functionality

[**Modified:** 8.5.110.13, 8.5.115.17, 8.5.117.18, 8.5.118.10]

Workspace also supports the following functionality for various interaction types:

- Case Data (also called: Customer Case or Case Information)
- Interaction Bar
- Workbins
- Standard Response Library
- Spelling Check

# Case Data

[**Modified:** 8.5.115.17, 8.5.117.18, 8.5.118.10, 8.5.125.04, 8.5.141.04]

This topic is part of a set of topics related to setting up channels and interaction handling.

Customer Case Data, also called Case Information, is the grouping in one location of all the information (Attached Data) about active interactions of all types for a single customer. The Customer Case facilities enable agents to store all information about the following actions in one location, as well as:

- Handle two voice calls simultaneously.
- Toggle between two calls.
- Transfer/conference one or all interaction(s).

## Evolution and behavior of Attached Data or Case Data

Attached data, or Customer Case information, that is relevant to a call evolves and changes as a call progresses through the system in a contact center. For example, during a Transfer or Conference, information about who transferred a call and when, is attached to the Customer Case as case data. Not all agents in the chain will see the same case data. This information can be retrieved through the contact database by agents who have the following privileges assigned:

- Contact - Can Use Contact History Case Data
- Contact - Can Use Contact My History

## Displaying and editing Case Information

### Important

The following section assumes that you are familiar with the use of Genesys Administrator Extention, Genesys Administrator, and/or Genesys Configuration Manager, and that you are familiar with the creation of Business Attribute objects and Business Attribute Values.

Refer to:

- Business Attribute Values
- Universal Routing 8.1 Business Process User's Guide
- Universal Routing 8.1 Reference Manual

## 1. Basic attached data display

[**Modified:** 8.5.141.04]

To display attached data key-values in Workspace, you must first define a Business Attribute that contains a list of Business Attribute Values.

- The Names of Business Attribute Values correspond to the names of the attached data keys that you want to display.
- The Display Names of the Business Attribute Values display the key in the User Interface.

You must then assign the name of this Business Attribute to the interaction.case-data.format-business-attribute option.

To pre-load case data Business Attribute objects when an agent logs in, configure the value of the general.configuration-business-attribute-cache-preload option with a list of Business Attributes to pre-load. Business Attributes and Transaction objects are otherwise loaded the first time that an interaction requiring them is received by an agent. They are then cached for future use. If there is a large number of possible attribute values, such as a large list of case data, there could be a delay in the display of the Interaction Notification while the case data loads. Pre-loading Business Attributes related to disposition and case data when an agent logs in ensures that there is no delay in displaying Interaction Notifications.

## 2. Translated attached data values

To display a value of attached data by using a *display name* instead of *raw data*, in addition to what is described in step #1, you must define an additional Business Attribute in which each Business Attribute Value represents a way to display this value in the User Interface:

- The name of the Business Attribute Value is the raw attached value that is contained in the interaction.
- The Display Name of the Business Attribute Value is the label that is used for rendering in the User Interface.

Next, you must define the annex of the Business Attribute Value that was defined in step #1 to represent this attached data, such as the following:

- `interaction-workspace/enum.business-attribute` = the name of the Business Attribute that is defined to translated attached data value
- `interaction-workspace/read-only` = `true`
- `interaction-workspace/display-type` = `enum`

Example:

To display a key-value pair in the Case Information area of an interaction in Workspace, such as `"CallQuality = "0"` (which is stored in attached data), perform the following steps:

### In Genesys Administrator Extension/Genesys Administrator:

### 1. Create a Business Attribute that is named "`CaseData`".

2. In this Business Attribute, create a Business Attribute Value that has the name `Name="CallQuality"` and `Display Name = "Call Quality"`.

3. In the Workspace application object, set the value of the `interaction-workspace`/interaction.case-data.format-business-attribute to `"CaseData"`

Workspace can display the attached data, but the value "0" will be displayed.

4. In Genesys Administrator Extension/Genesys Administrator:
   a) Create a Business Attribute that is named `enumCallQuality`

   b) In this Business Attribute, create the following Business Attribute Values:
      Name = '0' and display name = '0 - Good'

      Name = '1' and display name '1 - Poor'

      Name = '2' and display name '2 - No audio'

5. In the `"CallQuality"` Business Attribute Value of the `"CaseData"` Business Attribute, set the following annex:
   - `interaction-workspace/enum.business-attribute = enumCallQuality`
   - `interaction-workspace/read-only = true`
   - `interaction-workspace/display-type = enum`

## Enabling attached data editing

[**Modified:** 8.5.117.18, 8.5.118.10]

You can configure Workspace to give agents the ability to edit the case and interaction information that is attached to an interaction. You can also make it mandatory that an agent edits the attached data prior to marking the interaction as Done. You can make editable case data display as a field, a calendar, a list or a folder tree in a drop-down list, or a checkbox.

To make case data editable, you specify which key-value pairs are editable by an agent by adding a new section called `interaction-workspace` to the attribute in Genesys Administrator Extension/Genesys Administrator, and then defining its properties.

When you define the properties of an attribute in a Business Attribute, you can also specify whether it has the property `read-only` or not. Attributes that are *not* `read-only` *can be edited by agents* who have the `Contact - Can Use Contact History Case Data` privilege allowed.

When you set the key-value pair to be editable (read-write enabled), agents can perform the following actions:

- edit plain strings (with format and length control)

- edit integer values (within a valid interval)
- edit float values (within a valid interval)
- edit date/time (by using a calendar control)
- edit enum (by using a drop-down control)
- edit enum-tree (by using a drop-down control containing a folder tree) [**Added:** 8.5.118.10]
- edit boolean (by using a check box control)

## Tip

An agent can only edit case information key-value pairs of those attributes that are displayed to the agent.

To make it mandatory that an agent edit an attribute before marking the interaction as Done, in the Business Attribute Value, create the `interaction-workspace/mandatory` option and set the value to `true`. [**Added:** 8.5.117.18]

## Warning

Genesys recommends that you set the value of the interaction.case-data.is-read-only-on-idle option to `false` to ensure that mandatory case data fields do not become read-only by default after the agent ends a call or a chat.

Some interaction actions such as 'Transfer', 'Forward as an attachment', and 'Transfer' and/or 'Conference', have an uncertain final status. By configuring the following options, you can specify whether the agent must complete the mandatory case data:

- interaction.case-data.email.mandatory-actions - Specifies whether the agent must complete the mandatory case data before applying a 'Transfer' or 'Forward as an attachment’ action on an email interaction. If you specify `Transfer` and/or `Forward` for this option, agents must complete the mandatory case data before completing one of these actions. [**Added:** 8.5.150.06]
- interaction.case-data.<media-type>.mandatory-actions - Specifies whether the agent must complete the mandatory case data before applying a ‘Transfer’ and/or ‘Conference’ action for any Digital Channel interaction other than email. If you specify `Transfer` and/or `Conference` for this option, agents must complete the mandatory case data before completing one of these actions. Agents can apply the Conference action only for the media types that support the functionality. [**Added:** 8.5.150.06]

These options can be overridden by a routing strategy as described in Overriding Options by Using a Routing Strategy.

The *Editing Case Information* table lists the case information Business Attribute keys that can be configured to be editable. For each attribute, add a new section named `interaction-workspace`, then define the options according to the type (boolean, string, integer, list, enum, enum-tree, float, and date) of the attribute.

## Tip

To view the table below, hover your mouse over it until the expand table icon appears. Click the icon to display the table in a separate window.

**Editing Case Information**

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| boolean | display-type | bool (for this type) | (none) | |
| | read-only | true, false | true | Specifies whether this key name can be modified |
| | mandatory<br>[**Added:** 8.5.117.18] | true, false | false | Specifies whether it is mandatory for an agent to edit the value of this key before marking the interaction as done. The value `true` is ignored if the `read-only` option is set to `true` or the interaction.case-data.is-read-only-on-idle Workspace option is set to `true`. |
| | bool.false-value | | false | Value accepted for false |
| | bool.true-value | | true | Value accepted for true |
| string | display-type | string (for this type) | (none) | |
| | read-only | true, false | true | Specifies whether this key name can be modified |
| | mandatory<br>[**Added:** 8.5.117.18] | true, false | false | Specifies whether it is mandatory for an agent to edit the value of this |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | | | | key before marking the interaction as done. The value `true` is ignored if the `read-only` option is set to `true` or the interaction.case-data.is-read-only-on-idle Workspace option is set to `true`. |
| | string.max-length | 0 to max length | 255 | Maximum number of characters that are accepted for this option |
| | string.expression<br>[**Added:** 8.5.106.19] | A string defining a valid regular expression | (none) | Specifies what the agent is permitted to enter in the field. If the characters that are entered are not part of the expected input, the character is displayed, but an error icon appears and the entry will not be committed to the backend until the string matches the configured format. When the entered string is corrected, the error icon disappears. For example, the regular expression for an AMEX credit card number is: "^3[47][0-9]{13}$" (American Express card numbers start with 34 or 37 and have 15 digits). It is possible to use this option with string.max-length; however, string.expression makes this option redundant. |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | string.expression-instructions<br>[**Added:** 8.5.106.19] | Any string | (none) | Specifies the instructions and/or examples that represent how the value configured by the 'string.expression' are populated. This string is displayed as a tooltip on top of the icon that informs the agent about incorrect formatting. |
| integer | display-type | int (for this type) | (none) | |
| | read-only | true, false | true | Specifies whether this key name can be modified |
| | mandatory<br>[**Added:** 8.5.117.18] | true, false | false | Specifies whether it is mandatory for an agent to edit the value of this key before marking the interaction as done. The value `true` is ignored if the `read-only` option is set to `true` or the interaction.case-data.is-read-only-on-idle Workspace option is set to `true`. |
| | int.min-value | integer | 0 | Minimum value accepted. If the value that is entered is not part of the expected input, the value is displayed, but an error icon appears and the entry will not be committed to the backend until the value matches the configured format. When the entered string is corrected, the error icon disappears. |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | int.max-value | integer | 9223372036854775807 | Maximum value accepted. If the value that is entered is not part of the expected input, the value is displayed, but an error icon appears and the entry will not be committed to the backend until the value matches the configured format. When the entered string is corrected, the error icon disappears. |
| | int.storage-type | int or string | string | Type storage of the value |
| enum | display-type | enum (for this type) | (none) | |
| | read-only | true, false | true | Specifies whether this key name can be modified |
| | mandatory<br>[**Added:** 8.5.117.18] | true, false | false | Specifies whether it is mandatory for an agent to edit the value of this key before marking the interaction as done. The value `true` is ignored if the `read-only` option is set to `true` or the interaction.case-data.is-read-only-on-idle Workspace option is set to `true`. |
| | enum.business-attribute | (link to business attributes) | (none) | Link to business attributes that define the enum value. By default the items in this list are sorted alphabetically. To move some or all of the fields to the top of the list, use the `order` option. |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | | | | This option must be created in the annex of the Business Attribute object that contains the list of values:<br>• Section: `interaction-workspace`<br>• Option: `Order`<br>• Default value: `""`<br>• Valid values: A comma-separated list of Business Attribute Value names. |
| enum-tree<br>[**Added:** 8.5.118.10] | display-type | enum-tree (for this type) | (none) | |
| | read-only | true, false | true | Specifies whether this key name can be modified |
| | mandatory | true, false | false | Specifies whether it is mandatory for an agent to edit the value of this key before marking the interaction as done. The value `true` is ignored if the `read-only` option is set to `true` or the interaction.case-data.is-read-only-on-idle Workspace option is set to `true`. |
| | enum.business-attribute | (link to business attributes) | (none) | Name of the Business Attribute object that defines the tree structure and enum values presented in the tree view. Agents can fold or unfold the treeview. |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | | | | Agents can search for values inside the tree structure. |
| float | display-type | float (for this type) | (none) | |
| | read-only | true, false | true | Specifies whether this key name can be modified |
| | mandatory<br>[**Added:** 8.5.117.18] | true, false | false | Specifies whether it is mandatory for an agent to edit the value of this key before marking the interaction as done. The value `true` is ignored if the `read-only` option is set to `true` or the interaction.case-data.is-read-only-on-idle Workspace option is set to `true`. |
| | float.min-value | float | 0 | Minimum value accepted. If the value that is entered is not part of the expected input, the value is displayed, but an error icon appears and the entry will not be committed to the backend until the value matches the configured format. When the entered string is corrected, the error icon disappears. |
| | float.max-value | float | 3.40282347E+38 | Maximum value accepted. If the value that is entered is not part of the expected input, the value is displayed, but an error icon appears and the entry will not be committed to the backend |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | | | | until the value matches the configured format. When the entered string is corrected, the error icon disappears. |
| date | display-type | date (for this type) | (none) | |
| | read-only | true, false | true | Specifies whether this key name can be modified |
| | mandatory<br>[**Added:** 8.5.117.18] | true, false | false | Specifies whether it is mandatory for an agent to edit the value of this key before marking the interaction as done. The value `true` is ignored if the `read-only` option is set to `true` or the interaction.case-data.is-read-only-on-idle Workspace option is set to `true`. |
| | date.time-format<br>[**Added:** 8.5.102.06] | The value of this option must be specified according to Windows Standards: http://msdn.microsoft.com/en-us/library/8kb3ddd4.aspx | "" | Specifies the format in which time values in attached data are stored or parsed, for example, `yyyy-MM-dd HH:mm:ss`. Use this key-value pair to make the time format consistent across users and workstations. When this option is not specified, the Workspace date and time format is inherited from the local system setting, which can cause inconsistencies for global deployments. Genesys recommends that |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | | | | you configure a date/time format that contains both date and time-of-day information. |
| | date.time-display-format<br>[**Added:** 8.5.125.04] | The value of this option must be specified according to Windows Standards: http://msdn.microsoft.com/en-us/library/8kb3ddd4.aspx | "" | Specifies the format in which time values for the DateTime variable in attached data are displayed in Workspace views. You can specify date and time, just date, or just time. |
| | date.utc-time-zone<br>[**Added:** 8.5.102.06] | true, false | false | Specifies whether the local time zone or UTC time zone is used to store data and time information for case information. If the value `false` is specified, the time is saved as local time. If the value `true` is specified, the time is saved as UTC time and the following time zone information is added to the formatted time in case no time zone information is specified as part of the value of the `date.time-format` option: `"+00:00"`. |

## Using enum-tree to display folders in Case Data

[**Added:** 8.5.118.10][**Modified:** 8.5.141.04]

The `enum-tree` option is intended to enable you to create a complex tree structure of categories in a drop-down list that presents all potential outcomes (dispositions) for an interaction. This is a supplement to the Disposition feature in each interaction. Agents can both browse and search the category tree.

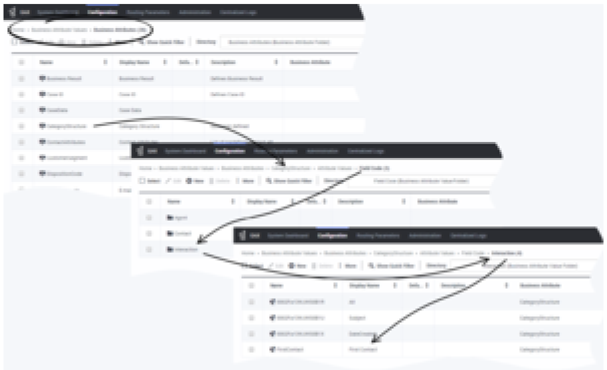
The enum-tree value selected by an agent while handling an interaction can be used to improve routing or suggested responses for the interaction.

You can specify more than one enum-tree for each interaction.

You can specify that the agent must edit the case data (select a category) before marking the iteraction Done.

To support this feature, you must create multiple categories in a folder structure.

1. Using Genesys Administrator Extension, create a Business Attribute (for example `Category Structure>`).
2. In the `Attribute Values` folder, add a series of folders that represent the categories that you want to use for your business outcomes or dispositions.
3. In each category folder, create one or more new Attribute Values.



For case data that employ the folder/tree structure, you can choose to pre-load the folder structure when a agent logs in by using the general.configuration-business-attribute-folder-cache-preload option to specify the list of Business Attributes containing the folders that you want to pre-load.

> ### Important
>
> You must specify the Business Attributes containing folders in both the general.configuration-business-attribute-folder-cache-preload and general.configuration-business-attribute-cache-preload options for the Business Attributes containing folders to be pre-loaded.

## Interaction Server and T-Server system properties keys

[**Added:** 8.5.115.17]

You can access Interaction Server system properties keys and T-Server system properties keys to be used in case information.

When you use the system properties keys that are listed in the *Supported Interaction Server System Properties*' and *Supported T-Server System Properties* tables. Only the `ScheduledAt` property can be modified to be read-only or read-write, the other properties are read-only.

When you use system properties keys to display a system property in the Attached Data, create a Case Data object that uses the system property name. Since system properties keys have a predefined configuration, you can only specify the `display-name` parameter in the `interaction-workspace` section that you create in the object.

The *Supported Interaction Server System Properties* table lists the Interaction Server system properties that you can use in Attached Data.

**Supported Interaction Server System Properties**

| System Properties Key | Predefined Display Type | Notes |
|---|---|---|
| AbandonedAt | date | |
| DeliveredAt | date | |
| MovedToQueueAt | date | |
| PlacedInQueueAt | date | |
| ReceivedAt | date | |
| ScheduledAt | date | This property can be changed by agents if `read-only` parameter is set to false. |
| SubmittedAt | date | |
| HeldAt | date | |
| CompletedAt | date | |
| AssignedAt | date | |
| ExternalId | string | |
| InteractionId | string | |
| InteractionSubtype | string | |
| InteractionType | string | |
| MediaType | string | |
| OutQueues | string | |
| ParentId | string | |
| Queue | string | |
| SubmittedBy | string | |
| Workbin | string | |
| WorkbinAgentGroupId | string | |
| WorkbinAgentId | string | |
| WorkbinPlaceGroupId | string | |
| WorkbinPlaceId | string | |
| AssignedTo | string | |
| InteractionState | integer | |
| IsLocked | integer | |
| IsOnline | integer | |
| PlaceInQueueSeq | integer | |
| SubmitSeq | integer | |
| TenantId | integer | |

The *Supported T-Server System Properties* table lists the T-Server system properties that you can use in Attached Data. All properties are read-only.

**Supported T-Server System Properties**

| System Properties Key | Predefined Display Type |
|---|---|
| ANI | string |
| CallID | integer |
| ConnID | string |
| CustomerID | string |
| DNIS | string |
| NetworkCallID | string |
| NetworkNodeID | integer |
| PreviousConnID | string |
| Server | string |
| ThisDN | string |

### Important

- All system attributes can be displayed in the following views: Case Information, Workbins Case Data tab, and Interaction Queues Case Data tab.
- Some system attributes are not available in the History and Interaction Search views depending on the media type of interaction.
- There might be some display issues between Interaction Server System Properties and T-Server System Properties in Case Information during the following times:
    - after the preview phase of a Push Preview interaction
    - after the preview phase and after call work phase of a Web Callback interaction
    - after adding a multimedia channel to a voice interaction and vice versa

## Displaying active URLs in Case Information

You can configure Workspace to render some key-values as clickable hyperlinks in the Case Information area and also enable previewing of web pages by tooltip on the clickable hyperlinks.

Use the following configuration options to control the way that hyperlinks are displayed, whether they are active or not, and to enable the display of a tooltip that displays a preview of the web page.

- expression.url—The option is configured by default to display most valid URLs as clickable hyperlinks.
- interaction.case-data.enable-url-preview—If this option is set to `true`, the tooltip-preview of linked web pages is enabled.

To control the display of hyperlinks in the Case Information area, format the attached data:

- If the attached data contains a raw URL, the hyperlink will be displayed as a raw URL (for example, http://<your web site>).
- If the attached data is formatted in the following way, the TITLE is displayed as a clickable hyperlink, and the target is the URL:
    - <a href="URL" title="TITLE" />
    - <a href="URL">TITLE<a/>

The Business Attribute Value of the key that contains the URL must contain the following key value: `[interaction-workspace]/display-type=string`

## Add key-value pair to the Case Information

You can enable the ability to edit the case information to add Key-Values that are missing from the case information. For example, the country or region contact information might be missing. If the agent obtains this information, the agent can edit the Case Information view to add the data value.

Pre-requisites:

- Enable the following privilege to allow editing of case information: Case Information - Can Add
- To enable a key to be added, the key must be configured as editable (refer to Enabling Attached Data Editing).

## Sharing case information between conversation participant and making it persistent in UCS

Case information structure is dependent on the context. For example, it will vary according to the agent configuration and any interaction overrides. Workspace attaches dedicated data to the interaction, in the form of key-value pairs, that is shared by anyone accessing the interaction, whether it is during live handling, from a workbin, or from the history. Workspace maintains these key-value pairs in a sub-list stored in the `IWAttachedDataInformation` key in the interaction.

# Interaction Bar

This topic is part of a set of topics related to setting up channels and interaction handling.

Workspace supports multiple simultaneous contact interactions. This means that agents can have more than one interaction open and active on their desktop simultaneously. The Interaction Bar is a feature of the Main Window that enables agents to track and access all their current interactions. Each interaction is represented by a block in the Interaction Bar view. The block contains contact information and interaction types to enable an agent to distinguish one interaction from another.

When an agent has one or more active interactions, each one can be displayed in one of three ways:

- As a toolbar in the Interaction Bar
- As a floating interaction window that is attached to the Interaction Bar
- As an interaction window that is pinned to the Interaction Bar

For more information about the Interaction Bar, refer to the *Workspace 8.5 Help* and the *Workspace 8.5 User's Guide.*

To use the Interaction Bar, allow the Interaction Bar Privileges and set the Interaction Bar options.

You can use the interaction-bar.quick-access-auto-open and interaction-bar.quick-access-auto-open.<media-type> configuration options to specify that when an agent creates or accepts an interaction, it is displayed as collapsed to the Interaction Bar. This enables agents to view other content, such as custom or 3rd-party content in the Main View, without the pinned or floating interaction views opening in front of the content. [**Added:** 8.5.106.19]

# Workbin and Interaction Queue management

[**Modified:** 8.5.110.13]

This topic is part of a set of topics related to setting up channels and interaction handling.

A *workbin* is like a shared queue for Agents, Places, Agent Groups, and Place Groups, in which an agent, supervisor, or manager can store email and other multimedia interactions that are to be handled later. However, unlike with a queue, interactions that are stored in a workbin can be accessed in any order; and can be assigned to Agents, Places, Agent Groups, or Place Groups. Items that are stored in a workbin are owned by the owner of the workbin.

Open interactions can be added to a workbin and saved for future processing or collaborative processing by the agent, place, agent group, or place group. Interactions can also be distributed to workbins by Universal Routing Server.

For information about configuring Workbins, refer to *Universal Routing 8.1 Interaction Routing Designer Help*.

The **desktop-draft-workbin** workbin object is normally configured by the Multimedia Configuration Wizard. However, you might have to create your workbins. Refer to *Genesys Administrator Extension Help* and the *eServices User's Guide* for information about defining Scripts in Configuration Server.

Workspace employs the following privileges for all workbin interactions:

- Can Use Workbins

You can use configuration options in each section that defines a workbin to configure the behavior of each workbin in Workspace (refer to Section: interaction-workspace).

## Workbin and Queue management

You can configure an agent who is specified as a Supervisor (Team Lead) for an Agent Group to read and manage the contents of the workbins of the other Agent Group members. A Supervisor can also manage the contents of queues. This functionality is enabled by granting the following privileges according to the functionality that you want to enable:

- Can Use My Team Workbins (`InteractionWorkspace.Workbins.canUseMyTeamWorkbins`)—Enables the Team Lead to see the workbins of the agents who are members of the Agent Group for which the Team Lead is specified as a Supervisor.
- Can Use Interaction Management (`InteractionWorkspace.InteractionManagement.canUse`)—Enables the Team Lead to see interactions that are filtered by predefined criteria.
- Can Use Interaction Management Move to Queue (`InteractionWorkspace.InteractionManagement.canMoveToQueue`)—Enables the Team Lead who can

use Interaction Management to move items from displayed workbins or from an Interaction Filter to an available Queue.

- Can Use Interaction Management Move to Workbin (`InteractionWorkspace.InteractionManagement.canMoveToWorkbin`)—Enables the Team Lead who can use Interaction Management to move items from displayed workbins or from an Interaction Filter to another workbin.
- Interaction Management - Can Search in Interaction Queues (`InteractionWorkspace.InteractionManagement.canSearchInInteractionQueues`)—Enables the Team Lead to further refine an assigned Interaction Queue Filter. [**Added:** 8.5.110.13]

Team Leads who are provisioned for Interaction Management can select single or multiple interactions in a workbin or a Queue and reassign them by moving them to other workbins or queues or mark them as Done.

## Creating interaction filters for Team Leads

[**Modified:** 8.5.110.13, 8.5.117.18]

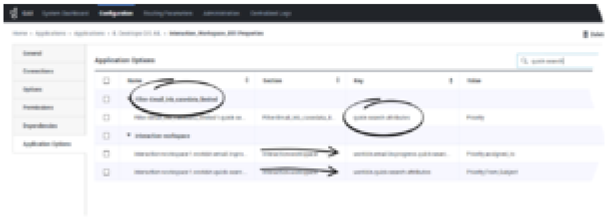
Agents who are granted the `InteractionWorkspace.InteractionManagement.canUse` privilege can view "snapshots" from the Interaction Server database of all the interactions that belong to specified queues. System administrators use Genesys Administrator Extension to build interaction filters, and then use the interaction-management.filters option to assign the filters to Team Lead (Supervisor) agents.

An *interaction filter* is a database request that is sent to the Interaction Server database. The following are examples of criteria that can be used to create a filter:

- `mediaType`—The media type, for example `email`, of the interactions to be extracted.
- age—The age of the interactions to be extracted. You can use this criteria to find interactions received in the last 4 hours, or the interactions that are older than 1 day, and so on.
- `Priority`—The *priority* of the interactions to be extracted.
- `Queue`—The name of the queue or a comma-separated list of queues in which the interactions to be extracted are stored.
- `Time in Queue`—The duration that the interactions to be extracted have been in the queue.
- `Received At`—The date and time at which the interaction was received. The query can specify that the filter returns either all the interactions created on, before, or after this date, or in a range of two dates.

To create and use a filter in Workspace and make it searchable in workbins and interaction queues, do the following:

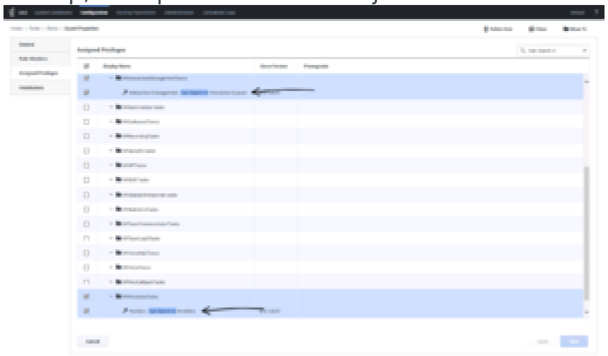
1. Create a new Section for the Workspace application object that is the name of the filter (for example: `FilterEmailAge`).



Sample Workspace Interaction Queue configuration in Genesys Administrator Extension.

[**Added:** 8.5.110.13]

2. Allow the Interaction Management - Can Search In Interaction Queues privilege on the Role, Agent Group, Group or other user objects.



Interaction Queue Search Privilege.

3. Configure options for the filter by using the names of fields in the Interaction Server database. The options correspond to the criteria for the interactions to be extracted from the database. The filter section must contain the following options:

   - `category`: The name of the category that contains the filter—for example: `Email`
   - `condition`: The complete filter—for example: `(priority >= 2) AND (MediaType='email') AND (_age() > 172800)`. Refer to Specifying Filter Conditions for information about how to define the conditions of a filter.
   - `display-name`: The display name of the filter—for example: `Older Than Two Days`
   - `displayed-columns`: (Optional) The list of columns that are displayed for this interaction filter—for example: `From,To,Subject,Received`. If this option is not set, the displayed columns are taken from the interaction-management.interactions-filter.displayed-columns option.
   - `queues`: (Optional) The list of queues to which this filter applies—for example: `email-routing-queue-inbound,email-default-queue`.
   - `case-data.business-attribute`: Specifies the name of the Business Attribute that contains the Business Attribute Values that are used to filter and render attached data for an interaction displayed in this filter. Use the `case-data.business-attribute` option to enable agents who are configured to be supervisors to view different interaction content than the agents whom they supervise. This option is not mandatory; however, when it is used, it is impacted by the `mandatory` option of a Business Attribute Value ([**Added:** 8.5.117.18]). If it is not specified, Workspace displays the case data that is specified by the interaction.case-data.format-business-attribute option.
   - `quick-search-attributes`: This key specifies the list of interaction attributes that are used when applying a quick search in this Interaction Queue Filter. The quick search criteria is applied like an AND logical operation combination, with the default criteria defined for this Filter (keys 'condition'

and 'queues'). The quick search part of the query is built to match any attributes that start with the criteria specified by the agent. If this option is not configured or is left empty, the **Search** field is not displayed for the corresponding Interaction Queue filter. The valid values are the interaction properties ("System" and "Custom" properties) defined in the "Specifying Filter Conditions" section of this same topic.

4. For the Application object, Agent Group, or Agent, configure the value of the interaction-management.filters option to specify a comma-separated list of filters by the section name that you configured. For example: `interaction-workspace\interaction-management.filters=FilterEmailAge`.

## Specifying filter conditions

A filter in Workspace is defined by specifying different property filters and linking them together by using `AND` and `OR` logical operators. A property filter is composed of a property name (for example: MediaType, Queue, or SubmittedBy) and a property value, for example, `MediaType='email'`. Refer to the Interaction Properties chapter of the *eServices 8.1 User's Guide* for detailed information about keywords, operators, and properties that can be used to query the Interaction Server database.

You can use System properties and Interaction Custom properties to define interaction filters. These are the System properties:

- `AbandonedAt`
- `AssignedAt`
- `AssignedTo`—The Employee ID of the agent to whom the interaction was last delivered
- `CompletedAt`
- `DeliveredAt`
- `ExternalId`—The External interaction identifier (for example, the chat session ID)
- `HeldAt`
- `InQueues`—The suggested destination for the interaction (provided by Universal Routing Server(URS))
- `InteractionId`
- `InteractionState` (0=queued, 1=cached, 2=being processed by URS, 3=being handled by agent)
- `InteractionSubtype`—The list of values comes from the Interaction Subtype business attribute
- `InteractionType`—The list of values comes from the Interaction Type business attribute
- `IsLocked` (0=unlocked, 1=locked)
- `IsOnline` (0=offline, 1=online)
- `MediaType`—The list of values comes from the Media Type business attribute
- `MovedToQueueAt`
- `OutQueues`—The suggested destinations for a reply
- `ParentId`
- `PlacedInQueueAt`
- `PlaceInQueueSeq`

- Queue
- ReceivedAt
- ScheduledAt
- SubmittedAt
- SubmittedBy—The name of the client application that submitted the interaction
- SubmitSeq
- TenantId
- Workbin
- WorkbinAgentGroupId
- WorkbinAgentId
- WorkbinPlaceGroupId
- WorkbinPlacedId

Custom properties are defined in the Configuration Layer in the **Interaction Custom Properties** Business Attribute. Each Custom Property annex must have a section that is named translation. The translation section contains the translate-to option that has a value corresponding to the name of a column in the interactions table of the Interaction Server database. The following property types for System and Custom are supported: Integer, String and Timestamp.

The name of the custom property (name of the Business Attribute value) can be used to define the interaction filter.

Property values have different types:

- string—Strings are enclosed by single quote characters, for example: 'email'
- date—Use the _timestamp keyword from Interaction Server for the value, for example: _timestamp('2013-11-21 14:12:00')
- integer

Filter conditions use comparators and logical operators to test the value of a property against the value that is stored in the database field. The following operators are supported:

- > (greater than)
- < (less than)
- >= (greater than or equal)
- <= (less than or equal)
- = (equal)
- != OR <> (different from/not equal)
- LIKE (contains the string)—for example, MediaType LIKE '%a%' finds all of the media types that contain the letter a. The % character acts as a wildcard. If MediaType LIKE 'ema%' is used, then media types that begin with ema are found. If MediaType LIKE '%at' is used, then media types that end with at are found.
- NOT LIKE (does not contain the string)

For interaction properties that have the `String` type, use the `_empty` and `_not_empty` keywords to avoid the problem of database formatting differences for empty strings. For example, to filter all the interactions that have a `ExternalId` property that is non-null, use: `_not_empty(ExternalId)`

For Interaction properties that have the `Timestamp` type, use the keywords that are described in the Translations section of the *eServices 8.1 User's Guide*. Use the following `Timestamp` properties for filtering based on the Timestamps of interactions:

- `_age()`—For example, `_age() >= 86400` returns all interactions that are older than 1 day (86400 seconds)
- `_time_in_queue()`
- `_current_time()`
- `_timestamp()`
- `_timestampdiff()`
- `_timestampadd()`
- `_time_in_same_queue()`

To find all interactions that were received between November 24 and November 29, 2013, use the following conditions: `ReceivedAt >=_timestamp('2013-11-23 00:00:00') AND ReceivedAt <= _timestamp('2012-11-29 00:00:00')`

## Important

To make the columns of the Interactions Table sortable, in the **Interaction Custom Properties** Business Attribute, you must explicitly declare the attribute as a column of the 'interactions' table of Interation Server Database.

## Tip

You can perform a bulk disposition code application followed by a bulk "Mark Done" operation on email interactions by performing a bulk "place in queue" operation to an Interaction Queue that is configured with a strategy that edits the **Disposition KVP** and then **Terminates** the email.

# Standard Responses Library

This topic is part of a set of topics related to setting up channels and interaction handling.

The Standard Responses Library (SRL) enables you to access a database of pre-written standard responses for interactions. Agents can insert these responses as replies into any email, chat message, or instant message, or they can read them to the contact during a voice interaction.

Agents can modify the contents of a standard response after inserting it into an email, chat message, or instant message.

The following information about the usage of standard responses is provided automatically to the Universal Contact Server by Workspace:

- `0`—The agent received suggested responses on the desktop but chose to ignore them and chose another response from the SRL.
- 2—The agent received suggested responses on the desktop, chose one of them, and replied.
- 3—The agent did not receive a suggested response from the content analyzer and chose a standard response from the SRL.

Interaction Workspace employs the following privilege for the Standard Responses Library (SRL):

- Can Use Standard Response Library

You use the following options in the `interaction-workspace` section to configure the SRL:

- standard-response.default-search-type: Specifies the default search type that is used to search for text in Standard Response Library. If empty, the default search type `AllKeywords` is used.
- standard-response.suggested-responses-min-relevancy: Specifies the minimum level of relevancy above which Suggested Responses will be shown from the Standard Response Library.
- standard-response.categories—Specifies the Standard Response category names to which the agent is restricted. Only standard responses and sub-category trees of the specified categories are displayed to the agent.
- standard-response.languages—Specifies the Standard Response languages to which the agent is restricted. Only standard responses of the specified languages are displayed to the agent. Languages are defined as Business Attributes in the Configuration Layer.

The `standard-response.categories` and `standard-response.languages` options can be overridden by a routing strategy. For example:

1. Configure a Transaction object of type `list`. For example, the object could be named: `IW_StandardResponseOverrideOptions`.
2. In the `interaction-workspace` section of the Agent configure the following options:
   - `standard-response.languages` = `French`
   - `standard-response.categories` = `Financial Service,HTML,English/Email/Loan`

3. To the override options add the name of the key to be used in the Routing Strategy to the `interaction-workspace` section: `interaction.override-option-key = IW_OverrideOptions` (default).
4. To the `AttachedData` in the strategy, add the following object name: `IW_OverrideOptions = IW_StandardResponseOverrideOptions`

For more information, refer to Modifying a Routing Strategy to Override Workspace Options, Based on Attached Data.

# Setting up Spelling Check

This topic is part of a set of topics related to setting up channels and interaction handling.

The spelling-check feature enables agents to verify the spelling of text that they have entered in an email, chat, or SMS interaction. The spelling of the contents of an outgoing email or chat interaction is verified against the default language dictionary.

The spelling-check feature steps through the text of replies, and underlines in red potentially misspelled words one by one. Agents can replace the underlined word with another word from a list of suggestions, add it to a custom dictionary, or ignore it.

The following languages are supported by default: English (US), English (UK), French, German, Spanish, Czech, Russian, Portuguese, and Italian.

Use the spellchecker.<media-type>.prompt-on-send configuration option to specify by media type whether you want agents to be prompted when they click **Send** if there are misspelled words in an email, chat, or SMS message. [**Added:** 8.5.105.12]

## Corporate Dictionary

There are two ways to add a corporate dictionary to the spelling-check feature. You can choose to combine these methods in the following execution order:

1. Configure the spellchecker.corporate-dictionary option with a list of comma-separated corporate dictionary words. Words in this list are limited to 7-bit ASCII characters. For words that require a different character set, us the spellchecker.corporate-dictionary-file option. The file can handle any type of encoded characters.
2. Configure the spellchecker.corporate-dictionary-file option with the absolute or relative path to your corporate dictionary text file. Each entry in the file should be on a separate line.

## Procedure

### Adding a new language dictionary to Workspace

**Purpose:**

To add a new spelling check language dictionary to Workspace.

**Start**

1. Find the appropriate dictionary from the Open Office web site: http://extensions.services.openoffice.org/en/dictionaries
2. Download the `.oxt` file and save it.

3. Rename the `.oxt` file by using the following naming convention, which follows the ISO 639-1 and ISO 3166 standard codes:
   `<language-code>-<country-code>.oxt`
4. Copy this file to `[IW install location]/Dictionaries`.
5. Restart Interaction Workspace.
6. The new language is then available in the dictionary language selection available in rich edit toolbar or by right-clicking in text areas.
   The following languages are supported by default: English (US), English (UK), French, German, Spanish, Czech, Russian, Portuguese, and Italian.

**End**

The Spelling Check *Interaction Workspace User*'s *Guide* lesson demonstrates how to select a language in the E-Mail Interaction interface (it applies to the interfaces of other interaction types as well.

The above procedure implements two "`spellchecker`" configuration options. You can use these options to configure the behavior of the Spelling Check feature. Use the spellchecker.corporate-dictionary-file option to point to a text file that contains a list of spelling words.

You can also customize the language pack for Workspace.

# Enabling internal and external communications

Refer to *Genesys Administrator Extension Help* and *Genesys Administrator Extension Deployment Guide* for detailed information on how to use Genesys Administrator Extension and Management Framework to configure access permissions.

### Setting up Voice and Outbound

Find information about setting up your agents' voice channel, universal look up tool (Team Communicator), voice mail, and voice call monitoring.

Communicating Inside Your Business

Voice

Enabling Team Communicator Calling

### Setting up eServices channels

Find information about setting up your agents' email, chat, video, and SMS/MMS channels.

Email

Email Quality Assurance

Chat

Chat Monitoring

### Setting up Callback

Find information about setting up your agents for Web Callback and Callback.

Web Callback

Callback

### Miscellaneous set up

Find information about enabling your agents to handle workitems, manage interactions in workbins, exchange IM's with coworkers. Agents can also be set up to specify call outcomes (disposition), access contact history, edit case information, use standard responses, read broadcast messages, and be team leads/supervisors.

Workitems

Workbins

Instant Messaging

Disposition Codes

Contact History

Case Information Editing

Standard Responses

Broadcast Messages

Team Leads and Supervisors

# Communicating inside your business

Workspace supports internal communication through Voice, Instant Messaging, and eServices Chat. The various interaction interfaces, such as Interactive Notifications, Interaction Window title bars, and lists of parties involved in an interaction, support the display of internal parties.

## Employing internal communication for Coaching and Barge-in

Workspace is an agent-only application that supports supervision in many different ways, including separate interactions integrated into one interaction window. Supervisors can silently monitor agents, and agents can be aware when they are being silently monitored.

Agents can consult with internal targets (supervisors and others) about their voice, chat, and email interactions, by starting a consultation interaction in the same window as their contact interaction. Agents can also communicate with a supervisor who has initiated coaching with the agent, or barge-in with the agent and the contact.

## Voice communication

Workspace provides many facilities for voice communication between agents, between agents and supervisors, and between agents and internal experts. The following functionality is available:

- Starting a consultation call
- One-step transfer
- Two-step transfer
- One-step conference
- Two-step conference
- Sending DTMF from a consultation call
- Holding a call
- Retrieving a call
- Alternating (toggling) between calls — holding and retrieving a call while on a consultation call
- Ending a consultation call

Voice call functionality is enabled for agent by using the Voice privileges.

You can use the following options in the `interaction-workspace` section to configure internal voice communications:

- voice.one-step-trsf-mode: Specifies the type of one-step transfer. If you specify default, the default one step transfer type for your switch is applied. For a Lucent G3 switch, the default type is `mute-transfer`; for a SIP switch, the default type is `single-step-transfer`; for an Alcatel A4400 switch, the default type is `single-step-transfer`.

Use the Enabling an agent to use Team Communicator to call/transfer to an agent group, skill, or

Voicemail procedure to enable agents to call or transfer a call to the voicemail box of another agent or agent group.

## Voice Conference functions

Workspace supports four-way conferencing. Agents can mute and parties can drop out without ending the call. The following functionality is available:

- Prevent a party from listening to the conversation
- Re-allow a party to listen to the conversation
- Remove a party from the conference

Use the following privileges to enable these voice conferencing functions:

- Can Delete From Conference
- Can Prevent a Conferenced Party From Listening
- Can ReAllow Conferenced Party To Listen

## Instant Messaging communication

Workspace provides many facilities for instant-messaging communication between agents, between agents and supervisors, and between agents and internal experts. The following functionality is available:

- Invite an internal target to join an Instant Messaging session
- Accept or Reject an invitation to join an Instant Messaging session
- Time-out if the internal target does not respond to an invitation

Use the following option in the `interaction-workspace` section to configure internal instant-messaging conferences:

- im.toast-timeout: Defines the duration, in seconds, of Interactive Notification for interaction instant messaging in the Information area of the Main Window. The value `0` means the Interactive Notification is not displayed.

## eServices Chat consultation

Workspace supports integrated chat consultation in the Chat Interaction window. A chat consultation enables an internal target to view the chat transcript between an agent and contact, and to chat with the agent privately in a second chat session in the same Chat Interaction window.

The internal target can see the messages that are exchanged with the contact, but the contact does not see the messages that are exchanged with the internal target.

## eServices Chat conference

The Workspace Chat Interaction window enables agents to instant-conference the current chat interaction with an internal target. In an instant conference, the conference starts as soon as the other party accepts the interaction. All parties in a chat conference can read all messages that are sent by each party.

## Transitioning to a different channel

During a collaboration with an agent or a knowledge worker, agents can perform the following tasks:

- Change from an Instant Message consultation to a Voice consultation
- Change from a Voice consultation to an Instant Message consultation
- Change from an Chat consultation to a Voice consultation
- Change from an Chat consultation to an Instant Message consultation

> **Tip**
>
> When an IM is transferred or conferenced to a different agent, or if an internal IM consultation is transitioned to a Voice consultation, or vice versa, all the information about the transferring agent is included with the interaction.

# Voice

[**Modified:** 8.5.144.05]

Workspace employs the following privileges for all voice interactions:

- Answer Call
- Delete from conference
- End Consultation Call
- Forward Call
- Hold/Retrieve Call
- Make Call
- One Step Conference
- Two Step Conference
- One Step Transfer
- Two Step Transfer
- Reject Call
- Release Call
- Set Interaction Disposition
- Send DTMF
- Suspend or Reinstate a Conference Party
- Show Silent Monitoring
- Use Voice Channel

Use the Voice and Interaction options in the `interaction-workspace` section to configure the handling of voice interactions. The following options are critical for configuring the behavior of the Voice channel:

- voice.mark-done-on-release: Specifies whether the Mark Done function is required to complete the release of the call.
- voice.auto-answer: Specifies whether a voice interaction is automatically answered when a TServer Ringing event is received. This feature is disabled if the voice media that handles the interaction is in Logged Off state (**Modified:** 8.5.117.18). This option can be overridden by a routing strategy. You can also configure auto-answer to display a timer that enables an agent to view case information before the interaction is automatically answered by using the voice.auto-answer.timer and voice.auto-answer.enable-reject options (**Added:** 8.5.105.12).
- interaction.disposition.is-mandatory: Specifies whether it is mandatory for the agent to set a disposition code before Marking Done an interaction. This option can be overridden by a routing strategy.
- interaction.disposition.is-read-only-on-idle: Prevents changes to the disposition code after the interaction has been released. This option can be overridden by a routing strategy.

- interaction.disposition.key-name: The key that is used to populate attached data or a user event when a disposition code is submitted to the back-end system, such as T-Server, Interaction Server, and Contact Server. This option can be overridden by a routing strategy.
- interaction.disposition.use-attached-data: Enables the adding of attached data from the interaction in UserEvent. This option can be overridden by a routing strategy.
- interaction.disposition.use-connection-id: Specifies whether the connection id is sent as part of the user event that is sent for disposition code. This option can be overridden by a routing strategy.
- interaction.disposition.value-business-attribute: A character string that specifies the name of the Business Attribute that contains the Attribute Values that are used as an enumerated value for a disposition code. This option can be overridden by a routing strategy.

## SIP Calls

In environments that use SIP Server, in the SIP Server application object, use the `sip-enable-call-info` option to control the user experience.

- Set the value to `true` to improve the display of call parties and enable blended interactions such as creating an email to the contact of voice interaction. This setting also ensures that caller information remains consistent when calls are transferred, conferenced, or routed between switches, for example in multi-site environments and business continuity environments.
- Set the value to `false` to maintain the default behavior; however, caller identification might not be displayed consistently in the interaction notification and the interaction view.

## Controlling Hold behavior

[**Modified:** 8.5.111.21]

### During Consultation calls

[**Added:** 8.5.103.10]

Workspace supports two different call hold behaviors during consultation calls in SIP Server environments. During consultation call, the contact is put on hold automatically when an agent initiates the consultation. You can control whether after the consultation call is ended the hold ends automatically or whether agents must end the hold manually by using the voice.end-consultation-method option.

Forcing agents to end the hold manually enables them to make other consultation calls or perform other actions prior to reconnecting with the contact, rather than reconnecting and then immediately putting the contact back on hold.

### Hold Indicator thresholds

[**Added:** 8.5.111.21]

Use the following configuration options to control the behavior of the Hold icon timer and progress indicator:

- voice.show-hold-duration: Specifies if the current hold duration is displayed instead of the total call time timer in the Interaction Bar when a voice call is placed on hold. The total call duration is accessible by using the Interaction Bar tooltip.
- voice.show-post-call-duration: Specifies if the current post call duration is displayed as the call timer in the Interaction Bar when a voice call is disconnected. The previous total call duration is accessible by using the Interaction Bar tooltip.
- voice.hold-indicator-timer: Specifies two alarm thresholds, in seconds, that warn agents that a voice call is on hold for a long time. Three levels are displayed: before the warning time, between the warning time and the maximum time, and after the maximum time. This option can be enabled only if the value of the voice.show-hold-duration is set to `true`.

## Dial Plan prefix management

The Dial Plan feature enables you to define the rules that Workspace applies to the dialed digits. The rules enable Workspace to transform the digits that it receives into the actual digits that are used to make the call.

Workspace receives digits from chat and SMS interactions when an agent uses the click-to-dial feature.

The Dial Plan Call Flow feature is applied to the following events:

- TMakeCall
- TInitiateTransfer
- TInitiateConference
- TSingleStepTransfer
- TMuteTransfer
- TSingleStepConference

### Pattern matching

The table *Dial plan pattern matching values* provides the list of special characters that you can use to define dialed number patterns to be matched.

**Dial plan pattern matching values**

| Special Character | Pattern Matching |
|---|---|
| X | Matches any single digit from 0-9. |
| Z | Matches any single digit from 1-9. |
| N | Matches any single digit from 2-9. |
| [...] | Matches any one of the digits that are found in the square brackets. For example, using the special characters [12345], Workspace can match any of |

| Special Character | Pattern Matching |
|---|---|
| | the digits: 1, 2, 3, 4, or 5. |
| [a-b] | The hyphen inside square brackets acts as a range indicator. Matches any one digit that falls in a range of digits. For example, [125-8] matches any of the digits 1, 2, 5, 6, 7, 8. |

The following are some examples of the use of special characters to match the patterns for dialed number Pattern Matching:

- `9NXXXXXXXXX`: Matches any 11-digit number that begins with 9, where the second digit is between 2 and 9.
- `9[54]10XXXXXX`: Matches any 11-digit number that begins with either 9510 or 9410.
- `[45]XXX`: Matches any 4-digit number that begins with either 4 or 5.

## Digit translation

After the number to be dialed is matched to the pattern that is defined in the dial-plan rule, Workspace uses the `digits` parameter to determine which number to use to make the call. These digits can be any alphanumeric string. The string must be terminated with a semicolon. This parameter can also use the `{DIGITS}` variable, which provides flexibility in defining the digits to be dialed. `{DIGITS}` Variable: The digits variable in the dial-plan rule must take one of the following formats:

- `${DIGITS}`
- `${DIGITS:x}`
- `${DIGITS:x:y}`

Where:

- `DIGITS` defines the actual digits dialed from the endpoint.
- `X` defines the starting position of the variable, identified by the character position in the digit string. The value `0` represents the first character in the string (starting from the left). This value can be negative, which indicates a character position that starts from the right instead of left. For example, `-1` indicates the right-most character. The default value is `0`.
- `Y` specifies the number of characters to be included, starting from the position that is defined by `X`. By default, all characters in the string are included.

For example, if the number `96501235678` is dialed, here are some examples of how the {DIGITS} translate:

- `${DIGITS}` translates to `96501235678`.
- `${DIGITS:1}` translates to `6501235678`.
- `${DIGITS:-4:4}` translates to `5678`.
- `${DIGITS:0:4}` translates to `9650`.

You must configure a Dial-Plan Rule in the `dial-plan-rule-<name> option` that uses the following format: `pattern => digit translation \# comment` For example:

- `5XXX=>4351707${DIGITS}` # This rule matches any 4-digit number starting with 5 and translates it to the number 43517075XXX
- `5002=>43517075002` # This rule matches the dialed number 5002 and translates it to the number 43517075002

## Formatting and masking the contact phone number

[**Added:** 8.5.144.05]

Workspace enables you to control how contact information is displayed to agents in the following user interface elements. Controlling the display of contact information can be helpful if your organization has policies regarding the masking of specific contact information, such as a phone number, from agents. You can mask contact information in the following interface elements by using the options described in this section:

- Call details in the **Contact History**.
- Interaction creation menu options in the **Interaction Party** view **Party Action** menu.
- **Team Communicator** tooltip.
- Call Party List tooltip.
- Callback reschedule **Phone Number** menu.
- Interaction **Action** menu items in the **Contact Directory**.

The following options enable you to specify how the contact information is displayed:

- display-format.caller-name
- display-format.case-name-format
- display-format.customer-name-format
- display-format.interaction-callback-name
- display-format.interaction-voice-name
- display-format.party-name-format
- interaction.window-title
- contact.history.voice-detail-attributes
- contact.multi-value-attribute-display.<contact-attribute>

The **display-format.*** option method enables you to hide information in specific interface elements. To mask contact information, such as the contact's phone number, using these options, you can include a text string in the option value instead of specifying a field code. In the following example, the default value will show the contact full name and will fallback to only the contact phone number if there is no first name, last name for this contact; the alternative option value will change the fallback to the configured string "Hidden Phone Number" when there is no first name, and last name.

| Default value |
|---|
| $Contact.FirstName$ $Contact.LastName$\|$Interaction.MainParty$ |
| **Masking value** |
| $Contact.FirstName$ $Contact.LastName$\|Hidden Phone Number |

Use the contact.history.voice-detail-attributes option to specify which of the following contact attributes are displayed in the History views: `Date`, `Contact`, `PhoneNumber`, `Duration`.

Use the contact.multi-value-attribute-display.<contact-attribute> option to specify how a contact attribute, which might have multiple values is displayed. To use this option, substitute **<contact-attribute>** with the name of a contact attribute, such as **PhoneNumber** (**contact.multi-value-attribute-display.PhoneNumber** is the only supported option at this time). Specify `Description` and/or `value` (see the tables below for information on reformatting the phone number display).

Attributes that support multiple values often have a **Description** property to distinguish among the multiple values. Here are some examples of **PhoneNumber** attributes that might have multiple values.

| Attribute format | Attribute description and value |
|---|---|
| Description (Value) | Home (+15555555555) |
| | Office (+15666666666) |
| | (+15555555555) |
| Description | Office |
| | Primary |
| Value | +15555555555 |

# Enabling Team Communicator calling features

[**Modified:** 8.5.102.06, 8.5.118.10]

The following procedures enable calling and presence features in Team Communicator.

## Enabling an agent to use Team Communicator to call/transfer to an agent group, skill, or Voicemail

[**Modified:** 8.5.118.10]

**Purpose:**

To enable an agent to use Team Communicator to call or transfer a voice call to an agent group or a skill.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.

**Start**

1. In the `Configuration` tab of the Workspace application, add a connection to Statistics Server.
2. In the connection, add a reference to the T-Server in which the agent logs in.
3. Allow any applicable privileges from the following list of Voice privileges for the role to which the agent is assigned:
   - Voice - Can Use
   - Voice - Can Make Call
   - Voice - Can One Step Transfer
   - Voice - Can Two Step Transfer
4. Allow the Team Communicator privileges (see Team Communicator Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group).
5. Configure the Team Communicator options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Team Communicator configuration option reference for a list of Team Communicator options and a description of how to configure them). The value of the teamcommunicator.list-filter-showing option must at least contain `AgentGroup` and `Skill`.

6. Configure the values of the intercommunication options as follows:
    - intercommunication.voice.routing-points: a valid routing point name that will be used to load the strategy to be used for call and transfer
    - intercommunication.voice.routing-based-actions: at least one of the following values: MakeCall, OneStepTransfer,InitTransfer
7. In your routing configuration, configure a routing strategy that uses the routing targets that are connected to Workspace (see intercommunication.voice.routing-points, which describes the list of keys than can be used in the routing strategy).
8. Load the routing strategy on the Routing Point that is defined by the intercommunication.voice.routing-points option.
9. You can enable agents to call or transfer calls to the voicemail of another agent by using the Team Communicator. [**Added:** 8.5.118.10]
    a. Set up voicemail for the target agent and/or agent group.
    b. Configure the values of the intercommunication options as follows:
        - intercommunication.voicemail.routing-points: a valid routing point name that will be used to load the strategy to be used for call and transfer.
        - intercommunication.voicemail.enabled-target-types: the list of targets, Agent and/or Agent Group, that are contacted through the routing based strategy mechanism for requests.
    c. Allow the following privileges from the following list of Voicemail privileges for the role to which the agent is assigned:
        - Voicemail - Can Deposit Message
        - Voicemail - Can Transfer Message

**End**

## Enabling an agent to use Team Communicator to call a contact

**Purpose:**

To enable an agent to use Team Communicator to call a contact that is stored in the Universal Contact Server (UCS).

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace Application object exists in the Configuration Database.
- Workspace has a connection to Universal Contact Server.
- Procedure: Enabling agents to manage contacts.
- The Procedure: Provisioning Workspace for the Voice channel.

**Start**

1. Allow the Team Communicator privileges (see Team Communicator Privileges) for the role to which the agent is assigned (refer to the Team Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group).
2. Configure the Team Communicator options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Team Communicator configuration option reference for a list of Team Communicator options and a description of how to configure them).
3. Ensure that the UCS application to which Workspace is connected is configured to support index searches on Contact database:
   - Set the `index\enabled` option to `true`.
   - Set the `index.contact\enabled` option to `true`.

   For more details about these settings, refer to the *eServices (Multimedia) 8.0 Reference Manual*.
4. Allow the following Voice privileges for the role to which the agent is assigned:
   - Can Hold/Retrieve Call
   - Can Make Call
   - Can Release Call
5. Allow the following contact management privileges for the role to which the agent is assigned:
   - Can Use Contact Directory
   - Can Use Contact Information
   - Contact Module

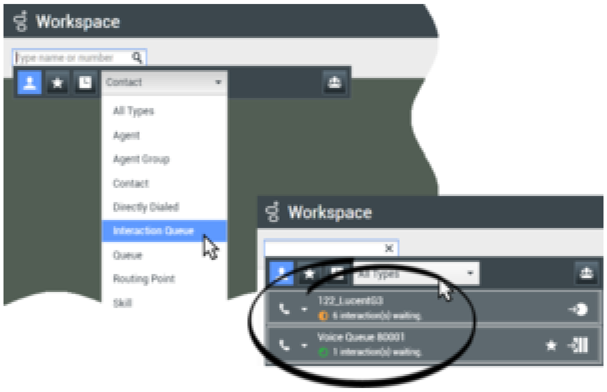
**End**

## Enabling an agent to view queue, interaction queue, and routing point presence information in Team Communicator

[**Added:** 8.5.102.06]

This section describes how you can configure Workspace to display presence information, including warning and error levels, in the Team Communicator for Interaction Queue, Queue, or Routing Point Objects.

Each object or group of objects for which you want to define presence must have its own section defined in the Workspace Application object in the Configuration Database.



## Defining a Presence Object section

Use Genesys Administrator Extension to define a new section in the options of Workspace Application object. Use any string representing the type of object (Interaction Queue, Queue, or Routing Point) concatenated with any logical identifier as the name of the section. Define the values that are to be displayed for the Interaction Queue, Queue, or Routing Point as the Options and Values of the section. The following options are used in the "presence" sections to enable you to display interaction queue, queue and routing point presence in the Team Communicator: object-ids, associated-statistic-type, associated-object-ids... Refer to the Table **- Mandatory and Optional Options for Presence Sections** for a complete list of the mandatory and optional options that you can define for each presence Object.

Workspace application template includes three default sections that can be used as the default generic presence metric definition respectively for Interaction Queues, Queues, and Routing Points:

- Section: interaction-queue-presence
- Section: queue-presence
- Section: routing-point-presence

**Mandatory and Optional Options for Presence Sections**

| Key | Default Value | Valid Values | Description | Mandatory |
|---|---|---|---|---|
| Key: statistic-name | "" | A valid statistic name according to what is configured in Stat Server | Name of the Stat Server metric used to compute the presence status | Yes |
| Key: statistic-text | "" | A String | Display name of the presence information presented in Team Communicator below the name of the object | Yes |
| Key: warning-level | 0.0 | A decimal value greater than or equal to 0 | First availability threshold according to the Unit of the Stat Server metric | No |

| Key | Default Value | Valid Values | Description | Mandatory |
|---|---|---|---|---|
| Key: error-level | 0.0 | A decimal value greater than or equal to 0 | Second availability threshold according to the Unit of the Stat Server metric | No |
| Key: object-ids | "" | A comma separated list of object ids of the same type | A comma separated list of object identifiers that represent the objects displayed in Team Communicator for which this presence metric is applicable. This key is optional. If it is absent from the section, the presence metric applies to all objects of the type for which this section is defined that do not have an explicit presence metric assignment. The Object identifier format is:<br>• For Queues and Routing Points: <DN Number>@<Switch_Name><br>• For Interaction Queues: <Script_Name> | No |
| Key: associated-statistic-type | "" | A valid statistic type | The statistic type, as referenced in Stat Server, that is requested to show the presence metric when this metric is not calculated directly on the object that is displayed in Team Communicator, but instead on the objects that are referenced in the `associated-` | No |

| Key | Default Value | Valid Values | Description | Mandatory |
|---|---|---|---|---|
| | | | `object-ids` option. This option is applicable only if the `associated-object-ids` option is also set. For example 'Queue' or 'RoutingPoint'. | |
| Key: associated-object-ids | "" | A comma separated list of object ids of the same type | A comma separated list of object identifiers that represent the objects that hold the statistic requested from Stat Server that is displayed in Team Communicator as the "presence metric" of the object. The type of those objects must match the type specified by the `associated-statistic-type` option. If multiple values are defined by the `object-ids` option, this option must contain the same number of objects in the order specified by `object-ids`. This option is applicable only if the `associated-statistic-type` option is also set. The Object identifier format is:<br>• For Queues and Routing Points: <DN Number>@<Switch_Name><br>• For Interaction Queues: <Script_Name> | No |

### Displaying object statistics

Workspace enables you to assign the Object presence statistics that you have defined on the Application object at one or more of the following levels:

- **Application level** -- Display Object Statistic to all agents
- **Tenant level** -- Display Object Statistic to all the agents of the Tenant
- **Agent Group level** -- Display Object Statistic to all the agents of the Agent Group
- **Agent level** -- Display Object Statistic to the agent

To assign an Object presence statistic to a specific configuration hierarchy level, define and configure the option corresponding to the object type in the `interaction-workspace` section of the level. The value of this option is a comma-separated list of Presence Object sections that are to be interpreted.

Use the following Team Communicator options to assign interaction queue, queue and routing point object presence to Team Communicator:

- teamcommunicator.interaction-queue-presence-metrics
- teamcommunicator.queue-presence-metrics
- teamcommunicator.routing-point-presence-metrics

Display precedence rules:

- When there is a presence section that does not have a specified `object-ids` key and a presence section which applies to object "queue 1", the second section will apply to "queue 1"; the presence of all other objects is defined by the first section.
- When there are multiple presence sections that do not have `object-ids`, only the first presence section in the list is taken into account.
- When an object is listed in multiple presence sections, only the first one in the list is taken into account.
- When all presence sections have explicit `object-ids` keys, the objects that are not explicitly listed in any presence section are displayed without presence information.

### Example

The following is an example of a contact center that displays routing points in Team Communicator and also uses virtual queues to calculate statistics for presence on routing points.

- Routing Points RP1, RP2, RP3 are available in Team Communicator as target for voice call transfers.
- Virtual Queues VQ1, VQ2 are not available in Team Communicator, but are technical objects that are available for background operations.
- The availability of RP1 is based on the "Number of Waiting Calls" on RP1.
- The availability of RP2 is based on the "Estimated Waiting Time" of VQ1.
- The availability of RP3 is based on the "Estimated Waiting Time" of VQ2.

Use the following configuration to get the expected presence metric of the routing points described above:

- **Section:** `routing-point-presence1`
  - `statistic-name=CurrNumberWaitingCalls`
  - `statistic-text=interaction(s) waiting.`
  - `warning-level=5`
  - `error-level=10`
  - `object-ids=RP1@Switch1`
- **Section:** `routing-point-presence2`
  - `statistic-name=ExpectedWaitTime`
  - `statistic-text=second(s) to wait`
  - `warning-level=30`
  - `error-level=60`
  - `object-ids=RP2@Switch1,RP3@Switch1`
  - `associated-statistic-type=Queue`
  - `associated-object-ids=VQ1@Switch1,VQ2@Switch1`
- **Section:** `interaction-workspace`
  - `teamcommunicator.routing-point-presence-metrics=routing-point-presence1,routing-point-presence2`

In this configuration, any routing point apart from RP1, RP2, and RP3 will not display presence in Team Communicator.

# Voicemail

[**Added:** 8.5.100.05]

Workspace enables SIP agents to access their voicemail boxes through the agent interface by using their hard-phone or soft-phone to dial their voicemail box. When this feature is enabled, a Message Waiting Indicator, a red circle that displays the total number of unread messages, including system messages, in all voicemail boxes that are configured to be connected to Workspace.

Refer to the following Genesys documentation for information about setting up voicemail boxes in your Genesys system:

- Genesys SIP Voicemail (Voicemail deployment, administration, and use)
- Feature Server Deployment Guide (mailbox configuration)

Workspace employs the following privilege for voicemail support:

- Voice Mail - Can Use

You use the following option in the `interaction-workspace` section to configure the number to dial to access the voicemail system:

- voicemail.access-number: Specifies the number to call to access your voicemail system.
- voicemail.notification-types: Specifies the types of voicemail boxes, personal and/or group (public) to be included in the count of unread voicemail messages in the Main Window.
- broadcast.system-messages-auto-mark-read: Specifies whether system messages are automatically marked as read so that they are not included in the total messages displayed in the Message Waiting Indicator.

Use the Enabling an agent to use Team Communicator to call/transfer to an agent group, skill, or Voicemail procedure to enable agents to call or transfer a call to the voicemail box of another agent or agent group.

## Related Resources

The following pages provide more information about managing voicemail boxes:

- Accessing voicemail from the web
- Provisioning mailboxes

# Workspace SIP Endpoint

[**Modified:** WSEP 8.5.113.02]

Workspace Desktop Edition supports two different SIP Endpoints: Interaction Workspace SIP Endpoint 8.0.2 and Workspace SIP Endpoint 8.5.0. If you want to continue to use SIP Endpoint 8.0.2, use the configuration options that are described in the *Interaction Workspace 8.1.4 Deployment Guide*.

> ## Tip
> Workspace also supports the Genesys Softphone in place of Workspace SIP Endpoint. To learn about Genesys Softphone, see Configuring Workspace Desktop Edition to use Genesys Softphone in the Genesys Softphone Deployment Guide.

Workspace provides three templates from which you can choose when you deploy, one for the application, and two optional ones for the Workspace SIP Endpoint. This means that there are three possible deployment configuration scenarios, depending on your environment, and whether you want to use the new Workspace SIP Endpoint video features.

1. `Workspace_Desktop_Edition_850.apd`: Deploy only this template if you want to use a different SIP Endpoint.
2. `Workspace_Desktop_Edition_SEP802_850.apd`: Deploy this template to use Workspace and the Workspace SIP Endpoint 8.0.2.
3. `Workspace_Desktop_Edition_SEP850_850.apd`: Deploy this template to use Workspace and the Workspace SIP Endpoint 8.5.0.

You can install an optional SIP Endpoint that can be added as a privilege to enable the agent workstation to handle SIP Voice-over-IP calls. The Workspace SIP Endpoint does not have an interface; instead, it adds interface elements to the Voice Interaction window, including muting and volume control for both the microphone channel and the speaker channel of the selected audio device(s) on the agent workstation.

> ## Tip
> Any USB headset that is supported by the Windows Operating System should work normally with Workspace SIP Endpoint.

Other SIP Voice features include: automatic gain control, beep tone, auto-answer, unavailable headset detection, log-level support, Real-time Transport Protocol (RTP) support, and speaking detection.

Workspace SIP Endpoint is started and stopped by Workspace. Both applications employ a keep-alive mechanism that allows each to detect when the other is no longer running. If the SIP Endpoint detects that Workspace is no longer running, it waits for any active calls to end, and then exits. If

Workspace detects that the SIP Endpoint is no longer running, it starts a new instance of Workspace SIP Endpoint.

The Workspace SIP Endpoint can be configured at any level of the configuration-layer hierarchy, from Tenant to agent. Workspace employs the following privilege for activating the Interaction Workspace SIP Endpoint:

- Can Use Embedded SIP Endpoint

Refer to the *SIP Endpoint SDK for .NET Developer's Guide* for a list of supported codecs for the Workspace SIP Endpoint.

> **Important**
>
> QoS policies are managed by the operating system. To configure a QoS policy in Windows, refer to Quality of Service (QoS) Policy in the Microsoft documentation.

## USB headset configuration

You can use the following options to configure Workspace to use a headset:

- sipendpoint.policy.device.use_headset: Specifies whether a USB head set is used for voice calls.
- sipendpoint.policy.device.headset_name: Specifies what type of USB headsets are supported in your environment. Use the "|" character to separate the names of different headsets if more than one type is supported. For example: 'Plantro|Jabra'.

If these options are set, and the corresponding USB headset is connected to the agent workstation at start-up time, the headset is selected automatically.

If the configured USB headset is not connected to the agent workstation, then the behavior depends on the following configuration option in the `interaction-workspace` section of the Workspace Application object:

- sipendpoint.headset-enforce-configured-usage

This option specifies whether the agent must plug in the specified USB headset to complete logging in. By default, when it is set to `false`, and if the headset is not plugged in at start-up time, the default audio devices that are available on the workstation, if any, are selected. When it is set to `true`, and if the headset is not plugged in when the agent logs in, Workspace waits for the headset to be plugged in before finalizing the login of the voice channel. The behavior of other medias, such as email and chat, are not affected by this option.

Workspace SIP Endpoint enables agents to switch to a pre-configured Not Ready state if the USB headset becomes unplugged after the agent has logged in to the SIP Voice Media. The agent will remain logged in to other eServices media such as email and chat.

Use the following configuration options in the `interaction-workspace` section of the Workspace Application object to control the behavior of this feature:

- sipendpoint.headset-unplugged.not-ready-reason—Specifies the Not Ready reason to be set to the SIP DN if the USB headset that is used by the agent becomes unplugged.
- sipendpoint.headset-unplugged-set-not-ready—Specifies whether the SIP DN of the agent is set automatically to `Not Ready` if the USB Headset that is used by the agent becomes unplugged.
- sipendpoint.headset-replugged-set-ready—Specifies whether the SIP DN of the agent is set automatically to Ready if the USB Headset that is used by the agent is plugged back in.

Workspace SIP Endpoint can be configured to retain volume setting of the USB headset between agent sessions.

Use the following configuration options in the `interaction-workspace` section of the Workspace Application object to control the behavior of this feature:

- sipendpoint.retain-volume-settings-between-sessions—Specifies whether the volume settings are saved for both microphone and speaker, when the agent logs out.

> **Important**
>
> When an agent logs in to Workspace, the application creates a list of headsets that are plugged in to the workstation. If an agent wants to use a different headset, he or she should exit Workspace, plug in the new headset, then relaunch Workspace.

## Session Border Controller

Interaction Workspace SIP Endpoint supports connecting to SIP Server through a Session Border Controller (SBC) (refer to *Server 8.1 Deployment Guide*). You must configure Interaction Workspace to connect to SIP Server through an SBC instead of directly to SIP Server.

If you do not configure Interaction Workspace to connect to SIP Server by using an SBC, Interaction Workspace SIP Endpoint connects directly to SIP Sever to register the agent SIP Endpoint by using the `TServer/sip-address` and `TServer/sip-port` options of the corresponding SIP Server application. When you configure Interaction Workspace to connect by using an SBC you decouple the address and port information that is sent to the SIP REGISTER from SIP Server and Interaction Workspace obtains the host address and port from the configuration.

Configure the following two options in the `interaction-workspace` section of the Application, Tenant, Agent Group, or User object.

- sipendpoint.sbc-register-address—Specifies the address of your SBC to which Interaction Workspace SIP Endpoint connects.
- sipendpoint.sbc-register-port—Specifies the port on your SBC to which Interaction Workspace SIP Endpoint connects.

To set the Domain/Realm of your contact center instead of an IP when Workspace SIP Endpoint tries to register through a session border controller (SBC) device, set the value of the following two options to represent valid SIP domain names to specify a 'request-uri' in the SIP REGISTER request that is decoupled from the SIP Proxy address that is contacted:

- sipendpoint.proxies.proxy0.domain
- sipendpoint.proxies.proxy1.domain

## Genesys SIP Proxy configuration

[**Modified:** WSEP 8.5.113.02]

Workspace Desktop Edition supports Genesys SIP Proxy. This feature enables SIP high availability (HA) without requiring a virtual IP address. Refer to the SIP Proxy 8.1 Deployment Guide for information about deploying and using SIP Proxy.

### DNS SRV

[**Added:** WSEP 8.5.113.02]

You can configure the Workspace SIP Endpoint with either:

- a standard DNS A-Records. Final URI form is: `sip:user@<host_fqdn>:<port>` where `<host_fqdn>` can be virtual and can represent multiple physical addresses behind the scenes, but the `:<port>` is mandatory, or
- a DNS SRV (Service record) as specified in the Genesys SIP Proxy Architecture. Final URI form is: `sip:user@<host_fqdn>`

### Limitations

- Genesys SIP Proxy currently does not support scenarios with switchover mid-transaction; therefore, call ANSWER and CANCEL probably will not work, but BYE is fully supported.

### Provisioning

The connection to the SIP Proxy is configured by using the following Workspace configuration options:

- sipendpoint.sbc-register-address—Specifies the IP Address, Host Name of the SIP Proxy or the FQDN of the SIP Proxy farm.
- sipendpoint.sbc-register-port—Specifies the port of the SIP Proxy. In case of a SIP Proxy farm, all SIP Proxy instances must have the same SIP Port. In case of DNS SRV, set this option to '0'.
- sipendpoint.sbc-register-address.peer— Specifies the IP Address, Host Name of the DR peer SIP Proxy or the FQDN of the DR peer SIP Proxy farm.
- sipendpoint.sbc-register-port.peer—Specifies the port of the DR peer SIP Proxy. In case of DNS SRV, set this option to '0'.

Tip

- These options were introduced in Interaction Workspace 8.1 to support Session Border Controller; therefore, they are not specific to SIP Proxy.
- Genesys recommends that you set the value of the sipendpoint.policy.endpoint.rtp_inactivity_timeout option to the default value of 30.

## Video configuration

Use the procedure: Enable an agent to use the SIP video interactions to set up agents to receive inbound video interactions. The following configuration options support this feature:

- sipendpoint.policy.session.auto_accept_video
- sipendpoint.video.auto-activate
- sipendpoint.video.always-on-top
- sipendpoint.video.thumbnail-ratio
- sipendpoint.video.camera-frame-rate
- sipendpoint.video.camera-frame-size
- sipendpoint.video.camera-render-format

## Changes to Workspace SIP Endpoint configuration options in Workspace 8.5.x

The **Workspace SIP Endpoint 8.0.2 versus Interaction Workspace SIP Endpoint 8.5.x options** table lists the changes that have been made to the Workspace SIP Endpoint configuration options with the introduction of Workspace SIP Endpoint 8.5.x. If you want to continue to use Interaction Workspace SIP Endpoint 8.0.2, use the configuration options that are described in the *Interaction Workspace 8.1.4 Deployment Guide*.

**Interaction Workspace SIP Endpoint 8.0.2 versus Workspace SIP Endpoint 8.5.x options**

| Interaction Workspace SIP Endpoint 8.0.2 Option Name | Workspace SIP Endpoint 8.5.x Option Name |
|---|---|
| sipendpoint.audio.headset.audio_in_agc_enabled | sipendpoint.policy.session.agc_mode |
| sipendpoint.audio.incoming.use_agc | N/A |
| sipendpoint.genesys.beeptone.beeptone_timeout | N/A |
| sipendpoint.genesys.beeptone.enable_beeptone | N/A |
| sipendpoint.genesys.beeptone.play_locally | N/A |
| sipendpoint.genesys.control.auto_answer | sipendpoint.policy.session.auto_answer |

| Interaction Workspace SIP Endpoint 8.0.2 Option Name | Workspace SIP Endpoint 8.5.x Option Name |
|---|---|
| sipendpoint.genesys.device.audio_in_device | sipendpoint.policy.device.audio_in_device |
| sipendpoint.genesys.device.audio_out_device | sipendpoint.policy.device.audio_out_device |
| sipendpoint.genesys.device.error_code_when_headset_na | sipendpoint.policy.session.sip_code_when_headset_na |
| sipendpoint.genesys.device.headset_name | sipendpoint.policy.device.headset_name |
| sipendpoint.genesys.device.manual_audio_devices_configure | N/A |
| sipendpoint.genesys.device.reject_call_when_headset_na | sipendpoint.policy.session.reject_session_when_headset_na |
| sipendpoint.genesys.device.use_headset | sipendpoint.policy.device.use_headset |
| sipendpoint.genesys.dtmf.pause_start_stop_dtmf | N/A |
| sipendpoint.genesys.dtmf.play_locally | N/A |
| sipendpoint.genesys.system.log_level_AbstractPhone | N/A |
| sipendpoint.genesys.system.log_level_Audio | N/A |
| sipendpoint.genesys.system.log_level_Auto Configuration | N/A |
| sipendpoint.genesys.system.log_level_CCM | N/A |
| sipendpoint.genesys.system.log_level_Conferencing | N/A |
| sipendpoint.genesys.system.log_level_Contacts | N/A |
| sipendpoint.genesys.system.log_level_DNS | N/A |
| sipendpoint.genesys.system.log_level_Endpoint | N/A |
| sipendpoint.genesys.system.log_level_Jitter | N/A |
| sipendpoint.genesys.system.log_level_Licensing | N/A |
| sipendpoint.genesys.system.log_level_Media | N/A |
| sipendpoint.genesys.system.log_level_Privacy | N/A |
| sipendpoint.genesys.system.log_level_RTP | N/A |
| sipendpoint.genesys.system.log_level_Security | N/A |
| sipendpoint.genesys.system.log_level_Storage | N/A |
| sipendpoint.genesys.system.log_level_STUN | N/A |
| sipendpoint.genesys.system.log_level_Transport | N/A |
| sipendpoint.genesys.system.log_level_USB Devices | N/A |
| sipendpoint.genesys.system.log_level_Utilities | N/A |
| sipendpoint.genesys.system.log_level_Voice Quality | N/A |
| sipendpoint.genesys.system.log_level_XMPP | N/A |
| sipendpoint.proxies.proxy0.reregister_in_seconds | sipendpoint.proxies.proxy0.reg_timeout |
| sipendpoint.rtp.2833.enabled | sipendpoint.policy.session.dtmf_method |
| sipendpoint.rtp.2833.hold_over_time_in_ms | N/A |
| sipendpoint.rtp.2833.packet_time_in_ms | N/A |
| sipendpoint.rtp.2833.payload_number | N/A |
| sipendpoint.rtp.inactivity.timer_enabled | sipendpoint.policy.endpoint.rtp_inactivity_timeout |

| Interaction Workspace SIP Endpoint 8.0.2 Option Name | Workspace SIP Endpoint 8.5.x Option Name |
|---|---|
| sipendpoint.system.diagnostics.enable_logging | sipendpoint.system.diagnostics.enable_logging (Unchanged) |
| sipendpoint.system.diagnostics.log_level | sipendpoint.system.diagnostics.log_level (key unchanged; Warning: value format has been changed) |
| sipendpoint.system.dtmf.force_send_in_band | sipendpoint.policy.session.dtmf_method |
| sipendpoint.system.dtmf.minimum_rfc2833_play_time | N/A |
| sipendpoint.system.indialog_notify.enable_indialognotify | N/A |
| sipendpoint.system.network.dtx_enabled | sipendpoint.policy.session.dtx_mode |
| sipendpoint.system.qos.audio | N/A |
| sipendpoint.tuning.mixer.allow_master_volume_change | N/A |

# Provisioning procedures

## 1. Enabling an agent to use the Workspace SIP Endpoint

**Purpose:** To enable an agent to use the Workspace SIP Endpoint to send and receive SIP-based interactions.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.

**Start**

1. Allow the SIP Endpoint privileges (see SIP Endpoint Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group).
2. If required, configure the SIP Endpoint options in the `interaction-workspace` section of the Workspace `Application` object (refer to the SIP Endpoint configuration option reference for a list of SIP Endpoint options and a description of how to configure them).
3. If required, configure SIP Endpoint for SIP Proxy support.
4. Set the following `TServer` section options for the DNs of the Place to which the agent is logging in:
   - `sip-cti-control = talk,hold`
   - voice = `true`
5. Install Workspace SIP Endpoint (refer to Procedure: Installing the Workspace SIP Endpoint).

**End**

## 2. Enabling an agent to use the SIP Preview feature

**Purpose:**

To enable an agent to view a display that contains a preview of an inbound SIP interaction.
**Prerequisites**

- Target agents are using an internal or external SIP endpoint.
- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.

**Start**

1. Configure a SIP DN for an agent with the preview feature by setting the value of the `preview-interaction` option to `true` in the `TServer` section of the annex of the DN.
2. To test the configuration, log the agent in to Workspace on the place that contains the DN that you configured in Step 1.
3. Use a SipEndpoint sample application to connect to a different SIP DN.
4. Make a call to a queue (Call to `sip:<QueueNumber>@<SIPServerHost>`) that routes interactions to the agent's Place Group that contains the agent.
5. The SIP Preview Interactive Notification is displayed on the agent's desktop.

**End**

## 3. Enabling an agent to use the SIP Video interactions

**Purpose:**

To enable an agent to receive inbound SIP video interactions.
**Prerequisites**

- Target agents are using Workspace SIP Endpoint 8.5.0.
- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- A webcam connected to the agent workstation.

> Important

> Workspace SIP Endpoint 8.5.0 supports only the VP8 and H.264 video codecs.

**Start**

1. Configure the values of the following SIP Server options:
   - TServer\default-music: Specify the path to an audio or video file to be played when the video call is on hold. The path is relative to the **MCP** root directory (for example: video/on_hold.avi). Video files must be .AVI file format with VP8 encoding. The frame rate must be 8000/16000 Hz for audio. 30 fps is recommended for video.
   - TServer\info-pass-through Specify the value true.
2. Configure the values of the Media Control Platform (MCP) 8.1.7+ options:
   - mcp\codec: Specify the list of codecs known by MCP and presented to SIP Endpoints. This list must include the vp8 codec to enable video hold, transfer, and conference.
   - mcp\transcoders: Specify the list of transcoders used by MCP. This list must include the vp8 codec to enable video hold, transfer, and conference.
   - conference\video_output_type: Specify the type of video output for conferences to be single (mixed mode is not supported).
3. Allow the following SIP Endpoint privilege (see SIP Endpoint Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group).
4. Activate the Workspace video capability by specifying 1 for the sipendpoint.policy.session.auto_accept_video configuration option.
5. For the sipendpoint.video.auto-activate configuration option, specify true to automatically connect to the video stream or false to require agents to manually connect to the video stream.
6. To control the size of the thumbnail of the local video stream specify a value for the sipendpoint.video.thumbnail-ratio configuration option.
7. For the sipendpoint.video.always-on-top configuration option, specify true to display the Video window always on top of all the other windows of the agent workstation or false to allow other windows to be on top of the Video window when they are made the active window.
8. If you are using H.264 codec, use the following configuration option to specify additional advanced parameters: sipendpoint.codecs.h264.fmtp

**End**

### High definition video requirements

> Important
>
> If you plan on supporting High Definition (HD) video, please take the following requirements into account.

Due to the complex processing required for High Definition video, all of the endpoints that are involved in a video conversation must run on computers that meet a certain minimum hardware performance level. As the actual CPU performance can no longer be accurately measured in MHz and since video processing performance depends on a wide variety of factors, Genesys recommends that you use the free benchmarking tool NovaBench to assess whether your hardware meets the requirements for successful HD video processing.

For 720p HD video, the **minimum** requirements are (in addition to what the camera manufacturer requires):

- A total NovaBench score of at least 500 (with a Graphic Test sub-score of at least 12), with recommended scores of at least 800 and 20, respectively
- 2 GB RAM
- 1 Mbps upload and download speed (for a total bandwidth of 2 Mpbs)

Workspace SIP Endpoint does not currently support video resolutions higher than 720p.

# Monitoring SIP, Cisco UCM, or Skype for Business voice interactions

Workspace supports two approaches to monitoring, built-in Team Lead capabilities and support for 3rd-party Supervisor applications.

> **Important**
>
> Depending on the technical environment of your voice channel, some voice specific supervisor switch-modes might not be available:
>
> - Switching from coaching to barge-in is not possible for agents or supervisors who are logged in to an environment that uses SIP Server or Multimedia Connector for Skype for Business.
> - Switching from coaching to barge-in is not possible for agents or supervisors who are logged in to an environment that uses T-Server for Cisco UCM.
> - Switching from monitoring to barge-in is not possible for agents or supervisors who are logged in to an environment that uses T-Server for Cisco UCM.
> - Only Interaction Workspace 8.1.3 and higher and Workspace Desktop Edition 8.5.0 and higher are compatible with T-Server for Cisco UCM.
> - To use Skype for Business with Workspace, you must install the Workspace Plugin for Skype for Business.

## Team Lead functionality

You can configure an agent role to have the Team Lead capability. Team Leads have capabilities that extend beyond the coaching and barge-in abilities that are enabled by internal communications. Interaction Workspace supports auto-monitoring of agents in an agent group by a team lead that is configured as the Supervisor of this Agent Group.

A Team Lead can perform the following functions:

- Monitor the next interaction or the currently active interaction.
- Select an agent and monitor all the voice interactions of this agent in one of two modes:
  - silent—neither the agent nor the contact is aware of the monitoring
  - coaching—only the agent can hear the Team Lead
- Silently monitor voice interactions
- Start a coaching monitoring session from a silent session

- Start a barge-in (all parties on the call can hear the Team Lead) monitoring session from silent or coaching session
- Start a silent monitoring session from coaching or barge-in session

Enable Team Lead functionality by allowing the Team Lead Privileges.

To support the monitoring of currently active voice interactions, you must also configure the SIP Server or T-Server for Cisco UCM application object by setting the `intrusion-enabled` option in the `TServer` section to the value `true`.

> **Important**
>
> There are no options in the `interaction-workspace` section to control the Team Lead functionality; however, Genesys strongly recommends that you use different DNs for the `voice` and `multimedia` channels to ensure that voice and IM channels can be monitored independently.

## Third-party supervision

You can enable agents to be monitored by a supervisor that is using a Supervisor application, such as Genesys 7.6 Supervisor Desktop, if you are running a Genesys Suite that include Genesys SIP Server or T-Server for Cisco UCM and Genesys Media Server. The monitoring feature is implemented as a hidden conference with the SIP DN or Cisco UCM DN of a supervisor.

If configured, the agent is notified through the Workspace interface during supervisor monitoring. All monitoring is conducted through the supervisor application. If the supervisor is using whisper coaching or barge-in, an "eye" icon is displayed within the voice interaction window to indicate that the call is monitored. When the supervisor leaves the call, the icon disappears.

# Outbound campaigns

[**Modified:** 8.5.115.17, 8.5.109.16, 8.5.106.19, 8.5.105.12, 8.5.102.06, 8.5.117.18, 8.5.125.04, 8.5.137.06, 8.5.145.06]

Workspace supports the following campaign types:

- **Preview**: Contacts are retrieved manually by the agent and dialed manually by the agent. These are low volume/high value campaigns, in which campaign calls are made by using a preset calling list for a specific campaign.
- **Push Preview**: Contacts are retrieved automatically by the campaign, but the agent dials the call manually. These are low volume/high value value campaigns, in which campaign calls are made by using a preset calling list. Agents are provided with a preview of the call, and then can either have the opportunity to accept it, or to reject it and return it to the top of the queue or discard the record.
- **Progressive**: Contacts are retrieved and dialed automatically by the campaign. These are low volume/high value campaigns, in which outbound calls are directed to the agent desktop.
- **Predictive**: Contacts are retrieved and dialed automatically by the campaign. These are high volume/low value campaigns, in which outbound calls are directed to the agent desktop.
- **Assured Connection**: This is a dialing mode for certain records in Progressive and Predictive campaigns. In this mode, an agent is engaged (connected) to the call prior to dialing the contact. For information about using Assured Connection in your campaigns, refer to the *Outbound Contact 8.1 Deployment Guide*. This mode is supported for SIP Campaigns only. [**Added:** 8.5.145.06]
- **Active Switching Matrix (ASM)**: Contacts are retrieved and dialed automatically by the campaign, like Progressive and Predictive, but the agent is connected immediately to the contact.

> ### Warning
>
> If you grant an agent voice capabilities and Instant Messaging (IM) capabilities on two different DNs, the agent does not get Outbound Campaign notifications and experiences other issue when handling Outbound Campaign interactions.
>
> **Workaround**: Configure the **Log On As Person** feature of the Outbound Contact Server so that it does not "see" the IM DNs that are configured in the Places of the agent.

## Provisioning Outbound Campaigns

Workspace employs the following Outbound privileges for all outbound campaign voice interactions:

- Can Use: Enables access to the Outbound Campaign functions
- Can Cancel Record: Enables agents to decline a preview record so that it is not processed during the current campaign.

- Can Dial Alternative Chained Record: Enables agents to dial a number from the preview record chain that is different from the number selected by the system.
- Can Edit Record Data: Enables agents to edit the outbound record fields that are configured as editable.
- Can Get Next Preview Record: Enables agents to request a new preview record while terminating the processing of the previous record.
- Can Mark Do Not Call: Enables agents to mark a contact as `Do Not Call`.
- Can Reject Record: Enables agents to decline a preview record and redirect it back to the queue to be processed by another agent in the campaign.
- Can Reschedule: Enables agents to reschedule an outbound record of an active call for callback at a different date and/or time.
- Can Reschedule Before Call: Enables agents to reschedule an outbound record of an Outbound Preview for callback at a different date and/or time. The Can Reschedule privilege must be enabled for this privilege to be active.
- Can Reschedule On New Number: Enables agents to reschedule an outbound record using a new number. This action results in a new record being added to the chain.
- Can Set Call Result: Enables agents to set a call result for the outbound record.
- Can Set Interaction Disposition: Enables agent to set a disposition code for Outbound interactions.

> ### Important
> The **Dispositions** tab does not become available until the call is established.

Interaction Workspace also enables privileges for Outbound Push Preview campaigns interactions:

- Can Use Push Preview: Enables agents to actively participate in Outbound Push Preview campaigns.

To ensure that this feature behaves correctly in Workspace, you must configure the `send_attribute` key-value pair as specified in the *Outbound Reference Guide*. For example, where the *Outbound Reference Guide* recommends that you set the field name to `GSW_UNTIL` or `GSW_FROM`, consider setting those values to `GSW_UNTIL` or `GSW_FROM` only. To set an alternative display name in the agent facing interface, you can use the `display-name` key-value as described in the table below.

There are two ways to specify the attribute type of outbound field:

- To create an attribute of the `string`, `integer`, `float`, or `date` type, specify this type in the data type of the outbound field.
- To create an attribute of the `boolean` or `enum` type, follow these two steps:
  1. Specify the type `char` or `varchar` for the data type of the outbound field.
  2. Set the value of `display-type` to `bool` for Boolean, or `enum` for enum.

## Configuration of the interaction-workspace section in the objects of type ‘Field’ in Genesys Administrator Extension

**Configuration of the interaction-workspace section in the objects of type ‘Field’ in Genesys Administrator Extension**

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| boolean | display-type | bool | (none) | Specifies the type of the outbound field to be displayed on the Workspace side. The outbound field value is displayed as a checkbox. `bool` display type is taken into account only if the outbound field data type is `char` or `varchar` |
| | display | true, false | true | Specifies if the outbound field is displayed or not on the Workspace side. This option is used in addition to the creation of the `send_attribute`. If the `send_attribute` is defined, use this option to hide the outbound field. |
| | display-name | any string | (none) | Specifies the name that is displayed for this outbound field on the Workspace side. If this option is not set, the outbound field is displayed by using the `send_attribute` value. |
| | read-only | true, false | true (for system fields),<br>false (for user-defined fields) | Specifies whether this outbound field can be modified |
| | bool.false-value | any string | false | Defines the string that corresponds to 'false'. |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | bool.true-value | any string | true | Defines the string that corresponds to 'true'. |
| string | display | true, false | true | Specifies if the outbound field is displayed or not on the Workspace side. This option is used in addition to the creation of the `send_attribute`. If the `send_attribute` is defined, use this option to hide the outbound field. |
| | display-name | any string | (none) | Specifies the name that is displayed for this outbound field on the Workspace side. If this option is not set, the outbound field is displayed by using the `send_attribute` value. |
| | read-only | true, false | true (for system fields), false (for user-defined fields) | Specifies whether this outbound field can be modified |
| | string.expression<br>[**Added:** 8.5.106.19] | A string defining a valid regular expression | (none) | Specifies what the agent is permitted to enter in the field. If the characters that are entered are not part of the expected input, the character is displayed, but an error icon appears and the entry will not be committed to the backend until the string matches the configured format. When the entered string is corrected, the error icon disappears. For example, the regular expression for an AMEX credit |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | | | | card number is: "^3[47][0-9]{13}$" (American Express card numbers start with 34 or 37 and have 15 digits). |
| | string.expression-instructions<br>[**Added:** 8.5.106.19] | Any string | (none) | Specifies the instructions and/or examples that represent how the value configured by the 'string.expression' are populated. This string is displayed as a tooltip on top of the icon that informs the agent about incorrect formatting. |
| enum | display-type | enum | (none) | Specifies the type of the outbound field to be displayed on the Workspace side. The outbound field possible values are displayed in a combo box. In this case, the list of possible values is defined in the `enum.business-attribute` option. `enum` display type is taken into account only if the outbound field data type is `char` or `varchar` |
| | display | true, false | true | Specifies if the outbound field is displayed or not on the Workspace side. This option is used in addition to the creation of the `send_attribute`. If the `send_attribute` is defined, use this option to hide the outbound field. |
| | display-name | any string | (none) | Specifies the name |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | | | | that is displayed for this outbound field on the Workspace side. If this option is not set, the outbound field is displayed by using the `send_attribute` value. |
| | read-only | true, false | true (for system fields)<br>false (for user-defined fields) | Specifies whether this outbound field can be modified |
| | enum.business-attribute | (link to business attribute) | (none) | Link to business attribute that define the enum value. By default the items are sorted alphabetically in this list. To move some or all of these fields to the top of the list, you can use the `order` option. Create this option in the annex of the Business Attribute object that contains the list of values:<br>• Section: `interaction-workspace`<br>• Option: `order`<br>• Default value: `""`<br>• Valid values: A comma-separated list of Business Attribute Value names. |
| integer | display | true, false | true | Specifies if the outbound field is displayed or not on the Workspace |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | | | | side. This option is used in addition to the creation of the `send_attribute`. If the `send_attribute` is defined, use this option to hide the outbound field. |
| | display-name | any string | (none) | Specifies the name that is displayed for this outbound field on the Workspace side. If this option is not set, the outbound field is displayed by using the `send_attribute` value. |
| | read-only | true, false | true (for system fields),<br>false (for user-defined fields) | Specifies whether this outbound field can be modified |
| | int.max-value | integer | 9223372036854775807 | Maximum value accepted. |
| | int.min-value | integer | 0 | Minimum value accepted. |
| float | display | true, false | true | Specifies if the outbound field is displayed or not on the Workspace side. This option is used in addition to the creation of the `send_attribute`. If the `send_attribute` is defined, use this option to hide the outbound field. |
| | display-name | any string | (none) | Specifies the name that is displayed for this outbound field on the Workspace side. If this option is not set, the outbound field is displayed by using the `send_attribute` value. |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | read-only | true, false | true (for system fields), false (for user-defined fields) | Specifies whether this outbound field can be modified |
| | float.max-value | float | 3.40282347E+38 | Maximum value accepted. |
| | float.min-value | float | 0 | Minimum value accepted. |
| date | display | true, false | true | Specifies if the outbound field is displayed or not on the Workspace side. This option is used in addition to the creation of the `send_attribute`. If the `send_attribute` is defined, use this option to hide the outbound field. |
| | display-name | any string | (none) | Specifies the name that is displayed for this outbound field on the Workspace side. If this option is not set, the outbound field is displayed by using the `send_attribute` value. |
| | display-type | date | date | Specifies that the display type of the `date.utc-time-zone` and/or the `date.time-format` options in the corresponding date format outbound field is `date`. **Note:** for Workspace 8.5.105.xx and earlier, if this option is not specified, the `date.utc-time-zone` and `date.time-format` options are not taken into account. |
| | read-only | true, false | true (for system fields), | Specifies whether this outbound field |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | | | false (for user-defined fields) | can be modified |
| | date.time-format<br>[**Added:** 8.5.102.06] | The value of this option must be specified according to Windows Standards: http://msdn.microsoft.com/en-us/library/8kb3ddd4.aspx | "" | Specifies the format in which time values in attached data are stored or parsed, for example, `yyyy-MM-dd HH:mm:ss`. Use this key-value pair to make the time format consistent across users and workstations. When this option is not specified, the Workspace date and time format is inherited from the local system setting which can cause inconsistencies for global deployments. Genesys recommends that you configure a date/time format that contains both date and time-of-day information. |
| | date.time-display-format<br>[**Added:** 8.5.125.04] | The value of this option must be specified according to Windows Standards: http://msdn.microsoft.com/en-us/library/8kb3ddd4.aspx | "" | Specifies the format in which time values for the DateTime variable in attached data are displayed in Workspace views. You can specify date and time, just date, or just time. |
| | date.utc-time-zone<br>[**Added:** 8.5.102.06] | true, false | false | Specifies whether the local time zone or UTC time zone is used to store data and time information for case information. If the value `false` is specified, the time is saved as |

| Attribute type | Option | Valid Values | Default Value | Description |
|---|---|---|---|---|
| | | | | local time. If the value `true` is specified, the time is saved as UTC time and the following time zone information is added to the formatted time in case no time zone information is specified as part of the value of the `date.time-format` option: `"+00:00"`. |

Next, you must configure the `send_attribute` key-value pair as specified in the *Outbound Reference Guide* for the calling list. To set an alternative display name in the agent facing interface, you can use the `outbound.fields.order` key-value as described in the table below.

**Configuration of the interaction-workspace section in the objects of type 'Calling List' in Genesys Administrator Extension**

| Option | Valid Values | Default Value | Description |
|---|---|---|---|
| outbound.fields.order | A comma-separated list of Outbound fields, identified by the value of the key `send_attribute` that is configured in section `OCServer` or `default` in the annex of the `Field` object. | `""` | Defines the order in which the outbound fields are sorted in the outbound data area. The fields that are not listed in this option are listed after the sorted fields, retaining their default sorting as specified by OCS. |

You use the following options in the `interaction-workspace` section to configure voice interactions:

- outbound.record-information.frame-color: Specifies the color of the border of the Case Data view frame. This option can be overridden by a routing strategy.
- outbound.record-information.header-foreground-color: Specifies the color of the foreground of the Case Data view header. This option can be overridden by a routing strategy.
- outbound.call-result-values: Specifies the list of call results that are available for the agent to use for an outbound interaction. The call results are displayed in the order in which they appear in the list. For example: `Answered,NoAnswer,AnsweringMachine,Busy,WrongNumber`
- outbound.push-preview.auto-answer: Specifies whether a push-preview outbound interaction is automatically accepted and joined when an Interaction Server Invite event is received. This option can be overridden by a routing strategy. You can also configure auto-answer to display a timer that enables an agent to view case information before the interaction is automatically answered by using the outbound.push-preview.auto-answer.timer and outbound.push-preview.auto-answer.enable-reject options [**Added:** 8.5.105.12].
- outbound.push-preview.use-combined-channel: Specifies whether the outbound push-preview channel is combined with the voice channel.

- outbound.assured-connection.allow-release-engaging-call-timeout Specifies the time, in seconds, after which an engaging call of Outbound Assured Connection can be released. If the value -1 is specified, an engaging call is not allowed to release [**Added:** 8.5.150.06].
- outbound.reschedule-inherit-parent-availability-interval: Specifies whether Workspace preserves the availability interval of the parent Outbound record when rescheduling an Outbound record with a new phone number.
- display-format.interaction-outbound-pull-preview-name: Defines the display format of outbound pull-preview (preview) interactions by specifying a string of field codes.
- display-format.interaction-outbound-push-preview-name: Defines the display format of outbound push-preview interactions by specifying a string of field codes.
- outboundpreview.ringing-bell: Specifies the Outbound preview ringing sound configuration string of an Outbound preview interaction pushed to the agent as a preview.

## Procedure

### Enabling an agent to use Outbound Campaign functionality call to a contact

**Purpose:**

To enable an agent to join an Outbound Campaign call to a contact that is stored in Outbound Contact Server (OCS).
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- Workspace `Application` object exists in the Configuration Database.

**Start**

1. Allow the Outbound privileges (see Outbound Campaign Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group).
   - Can Use
   - Can Reject Record
   - Can Cancel Record
   - Can Dial Alternative Chained Record
   - Can Get Next Preview Record
   - Can Use Push Preview
   - Can Mark Do Not Call
   - Can Set Call Result
   - Can Reschedule
   - Can Reschedule On New Number
   - Can Edit Record Data

2. Configure the Outbound options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Outbound configuration option reference for a list of Outbound options and a description of how to configure them).

**End**

> ### Important
>
> Workspace does not support OCS Recall Record. To allow for Recall, Genesys recommends that you create an OCS treatment capacity based on the the **Call Result** specified by the agent after the first call attempt.

## Dialing an alternate number in Outbound Preview Mode

You can configure an alternate dialing number for an Outbound call that has a `NoAnswer` or `Busy` result, or some other result than `Answered`.

To enable this functionality, you must create a new Treatment object in the Outbound Contact Server (OCS) application in the Genesys Configuration layer. The Treatment object specifies that the next number in the dialing chain for the contact is dialed. The Treatment ensures that each number in the dialing chain is tried until the agent applies a different disposition to the call.

1. In Genesys Administrator Extension, open `PROVISIONING > Outbound Contact > Treatments`.
2. Click `New`.
3. In the New Treatment view, set the following field values:
   - **Name:** ReDial_NoAnswer
   - **Call Result:** No Answer
   - **Apply to Record:** Next in chain
   - **Number in Sequence:** 1
   - **State:** Enabled
   - **Cycle Attempt:** 10
   - **Interval, minutes:** 1
4. Assign the new Treatment to the calling list. Open one or more of your Calling List objects in Genesys Administrator Extension and select the Treatments tab.
5. Click `Add`.
6. In the Browse dialog box, select the treatment that you just created.
7. Click `OK`.
8. Click `Save & Close`.
9. In Genesys Administrator Extension, open the Workspace Application object and configure it to use the Treatment.

10. In the interaction-workspace section assign the value personal to the outbound.treatment-mode option. Setting this option to personal adds the GSW_TREATMENT = RecordTreatPersonal attached data to the EventUserEvent that is generated when the record is marked as processed. This attached data informs OCS that a treatment should be applied to the outbound record if the call result matches the result that is set for the record. This ensures that the callback is assigned to the agent who set the No Answer disposition for the call and not to the next available agent who is working on the same campaign. Refer to the scenario that is described below.

## Scenario

1. Your Outbound campaign is started in Preview mode.
2. An agent logs in to Interaction Workspace.
3. The agent clicks Get Record to retrieve an Outbound Record from the Outbound Campaign on which they are working.
4. The agent receives an Outbound Record and selects the number to be dialed from the list of available phone numbers in the Outbound Chain.
5. The agent calls the selected number.
6. When the call is over, the agent sets the Call Result to No Answer and then clicks Done, closing the interaction.
7. OCS applies the ReDial_NoAnswer call treatment that you created to handle the No Answer call result.
8. An immediate callback for the Outbound Record is triggered (refer to the "Call Handling/Treatments" section in the *Outbound Contact 8.1 Deployment Guide*).
9. The agent immediately receives a *personal* callback for this outbound record because the value of the outbound.treatment-mode option is set to personal.
10. The agent accepts the personal callback.
11. The preview record is displayed and the agent is able to dial one of the available numbers from the outbound chain.

# Timed Auto-dial in Outbound Preview campaigns

[**Added:** 8.5.109.16]

You can specify how agents who are part of Push Preview, Pull Preview, and Reschedule Preview outbound campaigns dial campaign calls. Use the outbound.timed-preview-auto-dial option to specify one of the following dial scenarios:

- Manual dialing (-1, default value)—Agents manually dial calls after viewing the call preview.
- Auto-dial (0)—The call is automatically dialed when agents get or accept a new record.
- Timed auto-dial (any value greater than 0)—Calls are automatically dialed the specified number of seconds after agents get or accept a new record. A countdown is displayed on the record preview to inform agents of how long they have before the call is dialed.

## Push Preview campaign pre-requisites

[**Added:** 8.5.109.16]

To ensure that Workspace properly handles scenarios where a call that is generated from a Push Preview Campaign record is transferred to another agent who is also engaged in the same Push Preview Campaign, use the following configuration:

Configure a Routing Point or ACD Queue belonging to the TServer/SIPServer to the Voice Transfer Destination of the Campaign Group object that assigns agents as transfer targets.

## Personal versus campaign callbacks

[**Added:** 8.5.115.17]

To specify whether rescheduled calls/callback are personal (the agent who created the callback), campaign (any agent active in the campaign), or both, use the outbound.callback-types

## Forcing agents to complete Outbound Record processing before transferring a call

[**Added:** 8.5.117.18]

By default, if an outbound campaign call is transferred from an Outbound enabled agent to an agent who is not enabled to handle outbound campaign calls, the call result set by the Outbound agent is lost because the ownership of the record is transferred from an Outbound agent to another agent.

Use the outbound.complete-record-before-transfer option to control whether or not the call result is retained. Setting the value of this option to `true` forces Workspace to complete the processing of the Outbound record before the call is transferred or conferenced to another agent, and makes the Outbound record read-only.

Use the outbound.call-result-is-mandatory option to ensure that the transferring agent is forced to set a call result prior to transferring an Outbound record.

## Setting up manual dialing of alternate numbers

[**Added:** 8.5.115.17]

There are many scenarios where an agent has to reject an Outbound Record because the provided phone number or phone numbers are incorrect or empty. For example, the phone number might have been entered incorrectly into the record and is missing a digit. A blank record might be intentional. Perhaps the requirements of the state are that all campaign calls must be manually dialed. In both of these scenarios, the agent needs a way to enter a phone number for the chain.

Make the following configurations to enable agents to enter a new phone number from the active Outbound Interaction toolbar:

1. Grant the Outbound - Can Dial On New Number privilege.
2. Set the value of the expression.outbound-campaign-phone-number option to a valid regular expression that confirms to the dialing requirements of the campaign. This option validates the number that an agent enters into the **New Phone Number** dialog box.

# Email

[**Modified:** 8.5.116.10, 8.5.113.11, 8.5.118.10, 8.5.127.06, 8.5.141.04, 8.5.143.08]

## Features

Workspace enables agents to handle email interactions, including the following functionality:

- Reply to inbound emails (with or without the original text).
- Create new outbound emails
- Validate the format of email addresses enter by agents into the To, Cc, and Bcc fields and provide feedback to agents prior to sending an email with an improperly formatted address [**Modified:** 8.5.114.08]
- Check the spelling of an outbound email
- Insert, edit, or delete hyperlinks dynamically, by context menu, or by a toolbar button into outgoing email interactions [**Added:** 8.5.118.10]
- Apply a signature to an outbound email
- Store emails in a workbin
- Transfer an email to an internal target such as another agent or an interaction queue
- Forward or forward as an attachment an email to someone outside of the Genesys system
- Set a disposition code
- Mark the interaction as Done
- Quality Assurance (QA) review of emails
- View and copy links to non-embedded images in inbound and outbound email interactions
- View and insert Standard Responses
- Paste content from browsers and other applications that display HTML
- Paste formatted text as plain text in HTML emails using `Paste Text Only` format. [**Added:** 8.5.150.06]
- Paste images from browsers and other applications that display HTML
- Print emails

### Tip

If you are using Interaction Routing Designer to create a Business Process to route your email interactions, refer to "Multimedia Objects" in the Universal Routing 8.1 Reference Manual.

# Enabling Email

This section describes the privileges and configuration options that you use to enable Workspace email.

## Privileges

Workspace employs the following privileges for all E-mail interactions:

- Can Use E-mail media
- Can Decline
- Can Move to Workbin
- Can Reply
- Can Reply All
- Can Add Attachments
- Can Send
- Can Save
- Can Delete
- Can Transfer
- Can Forward
- Can Forward As An Attachment
- Can Set Interaction Disposition
- Can Interim Send
- Can Print E-mail
- Can Change Format In New E-mail
- Can Change Format In Reply E-mail
- Can Mark Done

## Basic Configuration

You can find all of the email configuration options here. Use the following configuration options for correct email interaction handling:

- email.default-queue: Specifies the default queue for email interactions.
- email.outbound-queue: Specifies the default queue for email interactions.
- workbin.email.draft: Specifies the name of the Workbin to be used to store draft email interactionss
- workbin.email.in-progress: Specifies the workbin to be used to store email interactions which are in the `In Progress` state.
- email.auto-answer: Specifies whether an email interaction is automatically answered when it is routed

to an agent. This option can be overridden by a routing strategy. You can also configure auto-answer to display a timer that enables an agent to view case information before the interaction is automatically answered by using the email.auto-answer.timer and email.auto-answer.enable-reject options [**Added:** 8.5.105.12].

- Reply to inbound emails (with or without the original text). The behavior of the email.reply-prefix option can be overridden by a routing strategy to conform to locale requirements [**Added:** 8.5.116.10].
- email.resend-prefix: Specifies a prefix to be used for resending an email. Agents who are granted the "Email - Can Reply" privilege to reply to emails can use the Resend feature in the History (**My History**, **Contact History**, and **Interaction Search**) to resend an outgoing or reply email. [**Added:** 8.5.141.04].
- accessibility.visual-impairment-profile: Beginning with version 8.5.113.11, Workspace enables agents to enter TABs in the email composition area of outgoing email interactions by pressing the **TAB** key if the value of this option is set to `false`; to use the **TAB** key to step to the next control or field, agents must first press **Ctrl-TAB** to step out of the text composition area. To disable this feature, set the value of this option to `true`; agents will not be able to enter TABS in the email composition area, but they can use the **TAB** key to move to the next control in the tab order.
- expression.url: Specify a regular expression that defines a valid URL.
- email.can-change-text-direction: Specifies whether the Right-to-left Text Direction and Left-to-right Text Direction buttons are enabled in the outbound email editor. Agents can use these buttons to change the text field to left-to-right (LTR) script or right-to-left (RTL) script. This means that an email can have a mix of both LTR and RTL scripts. Enabling the option is not mandatory if agents are working exclusively in LTR or RTL scripts.

## Controlling attachment read-only behavior

[**Added:** 8.5.118.10]

By default, all attachments opened by agents in an external program are read-only. This means that agents cannot update them and save the changes to their hard drive.

Use the general.writable-downloaded-attachment-file-types option to override this behavior for specific file types. Allowing agents to edit only certain file types preserves the data integrity of files that you do not want agents to modify. For example, you might allow agents to modify `.jpg` and `.png` files so that the orientation can be changed, but restrict the modification of `.docx`, `.xlsx`, and other file types. Or, you might want to ensure that only `.xlsx` files can be updated by agents.

## Linked images

Workspace handles linked images in the HTML content of inbound and outbound email interactions. Images are loaded from their respective web servers in the background so that display of the email interaction does not block the application. For environments where Internet proxies require user authentication, the following options have been added to the template:

- webproxy.address—Specifies the the web proxy address.
- webproxy.username—Specifies the the web proxy username.
- webproxy.password—Specifies the the web proxy password.

## Provisioning the Email channel

[**Modified:** 8.5.115.17]

### 1. Enabling an agent to use Email to correspond with a contact

**Purpose:**

To enable an agent to use Email to correspond with a contact that is stored in Universal Contact Server (UCS).

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to Universal Contact Server and Interaction Server.
- The Procedure: Enabling agents to manage contacts.

**Start**

1. Allow the Email privileges (see Email Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group).
   - Can Use E-mail media
   - Can Decline E-mail
   - Can Release E-mail
   - Can Reply
   - Can Send
   - Can One Step Transfer
   - Can Set Interaction Disposition
2. Configure the Email options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Email configuration option reference for a list of Email options and a description of how to configure them).
3. Configure the email queue options in the `email` section that are mandatory for basic email processing: email.default-queue and email.outbound-queue.
4. (Optional for transfer or email to queues) Configure the queue options in the `interaction-queue-presence`, `queue-presence`, `routing-point-presence` sections of the Workspace `Application` object (refer to Section: interaction-queue-presence, Section: queue-presence, Section: routing-point-presence in the configuration option reference for a list of queue options and a description of how to configure them).
5. Configure the workbins options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Workbin configuration option reference for a list of workbin options and a description of how to configure them), in particular: workbin.email.in-progress and workbin.email.draft.

6. To add an email signature, configure the email.signature template option in the `interaction-workspace` section to enable automatic insertion of a signature in all new and reply outbound emails.
7. To limit the 'From' addresses that are available to agents to select in the outbound Email Interaction view to an address or addresses that are based on the inbound service used, or to specify a default address for each service rather than a fixed list, configure the email.from-addresses option. [**Added:** 8.5.115.17]

   If you use a Business Attribute with a value containing the 'From' address that you want agents to use by default, you can use the email.from-addresses.force-default-on-reply option to specify whether the 'From' address of a reply email interaction is the value configured in the Business Attribute (`true`) or the target inbound mailbox of the parent inbound email interaction (`false`). [**Added:** 8.5.143.08]
8. To have editable case data copied back to the original inbound email from an outgoing reply email interaction when it is sent, set the value of the email.outbound.copy-editable-case-data-in-inbound option to `true`.

> Tip
>
> For information about configuring Load Balancing and Business Continuity, refer to Runtime Connection Logic in the eServices Load Balancing Business Continuity section of the *Business Continuity and Disaster Recovery* topic. **Added:** 8.5.109.16

**End**

## 2. Configuring filtered email From Address functionality

**Purpose:**

To enable an agent to access a configured list of Contact Center "From" email addresses.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace can handle email interactions.

**Start**

The list of "From" email addresses that can be used in outbound emails can be populated from two mutually exclusive sources, based on options that you configure:

- Email Server POP addresses. Configure the `email.from-addresses` option with the value `$EMAILSERVER$`.
- An option that references a Business Attribute. Each Business Attribute Value corresponds to a "From" Address, where `Name` is the actual address, `Display name` is the human-readable name displayed to the agent, and `Default tag` is used to display a default value in the combo box that is used by the agent to select an address.

**End**

## Displaying Suggested Responses

Suggested responses are relevant standard responses to an email interaction that the agents can use. These responses are associated with an email interaction as part of the routing process before the email is displayed to the agent. Workspace supports the following Classification Server services to detect suggested responses:

- Analyze (starting with 8.5.149.03) - Refer to the Analyze Block documentation based on the routing application you use, for more information on screening rules.
- Screen and Classify - Refer to the topic Screening Rules in eServices Digital Administration for more information on these services.

Workspace automatically detects the type of suggested response delivered to it.

> ### Important
> If you are designing a business process that leverages the Analyze service, ensure that the nested KVPair structure that is returned by the Analyze service is preserved once it is attached to the user data of the email interaction.

## Restricting the editing of addresses in outgoing email

You can prevent your agents from adding or editing the To, Cc, and Bcc fields of outgoing email interactions. This feature enhances email security and other business strategies. Use the following configuration options to implement this email control feature:

- email.outbound.editable-to-addresses
- email.outbound.editable-cc-addresses
- email.outbound.editable-bcc-addresses

By default, these options are set to `true`, meaning that, by default, there are no email address editing restrictions applied. The behavior of these options can be overridden by a routing strategy, as described in Overriding Options by Using a Routing Strategy.

## Signatures

Workspace enables you to assign default signature templates to outbound email interactions. E-mail signatures allow the insertion of tagged-data fields with data that is related to the agent, such as name, job title, department, phone number, email address, and so on. Refer to "Using UCS Data in

Standard Responses: System Variables" in the "Genesys Knowledge Management: Basics" chapter of the eServices User's Guide for more information about the tagged data field. Signatures also support linked image(s) and hyperlinks.

Use the email.signature configuration option in the `interaction-workspace` section to specify the path and name of the signature file or the location of the Response in the Standard Response Library that is to be used as the default signature.

> Tip
>
> This option can be overridden by a routing strategy based on the attached data of the interaction.

## Attaching files to outgoing emails

You can enable agents to attach files to outgoing email interactions by allowing the `Can Add Attachments` privilege. Control the behavior of this feature by using the following configuration options:

- email.attachment-download-timeout
- email.max-attachments-size
- email.restricted-attachment-file-types

## Inserting images into outgoing emails

[**Added:** 8.5.113.11]

Beginning with Workspace 8.5.113.11, embedded in-line images are supported for both inbound and outgoing email interactions. If a contact inserts an image in an HTML formatted email interactions, agents see the image displayed where the contact inserted it.

You can enable agents to paste copied images at the insertion point in an outgoing email interaction or to click the **Insert Image** button and browse to find an image to insert by granting the `Can Add Embedded Image In Outbound Email` privilege. If this privilege is not granted, agents can only include images as attachments.

In Workspace 8.5.112.12 and lower, inserted images were handled as attachments; this did not allow images to be inserted next to the text that provided context for the image.

> Important

> Embedded in-line images are only supported by Genesys Email Server Java version 8.5.102.02 or Higher

## Inbound email forwarding

[**Modified:** 8.5.113.11, 8.5.104.15]

Workspace supports two different email forwarding modes:

1. Forward [**Added:** 8.5.113.11]
2. Forward as an Attachment (Formerly: *Inbound Email Forward to External Resource*)

## Forward

[**Added:** 8.5.113.11]

Agents can send a commented copy of an email interaction to an external resource (someone in your company directory that is outside of the control of the Genesys environment — for example, your back office). This is sometimes referred to as in-line forwarding. A forwarded inbound email interaction is copied into a new email interaction with a note indicating the date and contact name of the inbound email interaction, and the contents of the original email at the bottom of the email body. Agents remain responsible for responding to the original inbound email interaction. Agents may or may not wait for an answer to this forward, depending upon your corporate policies and processes.

When an agent selects **Forward**, a new outbound email is created as a child of the original email. The email subject is initialized to the subject of the parent email, and, if configured, a forward prefix (email.inline-forward-prefix). The body contains the agent's signature, if configured, and a quote header followed by the content of the parent email content . Attachments and attached data of the parent email, if any, are copied to the new email. The interaction is assigned to the same contact, if any, as the parent email. Agents can edit the body before completing the forward. The new outbound email is then placed in the email.inline-forward-queue. The agent **EmployeeId** is attached to that new outbound email to enable business processess to distribute the possible reply back to the same agent. The original inbound email is placed in the in-progress workbin of the agent while it is being forwarded, and then removed from the in-progress workbin when the forward is completed.

The typical use case is that agents use the answer received from the person to whom they forward email interactions to elaborate their responses.

Agents can use Forward to forward emails from the following locations:

- Active inbound email interaction
- Inbound and outbound email interactions in the Contact History
- Inbound and outbound email interactions in My History

- Inbound and outbound email interactions in the Interaction Search

Use the following privilege to enable Forwarding:

- E-Mail - Can Forward

If only this privilege is granted, then the **Forward** (✉) button has no drop-down menu. Clicking it launches the forward process described above. If the `E-Mail - Can Forward As An Attachment` privilege is also granted, then the button activiates a drop-down menu that enables agents to choose between forwarding (in-line) or forwarding as an attachment.

Use the following configuration options to control the behavior of the Forward feature:

- email.inline-forward-prefix—Specifies the prefix that is added at the beginning of the subject of the original email when it is forwarded to an external resource.
- email.inline-forward-queue—Specifies the Interaction Queue in which outbound emails created for in-line forwarding are placed when agents click 'Complete Forward'.
- keyboard.shortcut.interaction.email.inline-forward—Specifies the combination of keys that can be used as a keyboard shortcut to forward an active inbound email to an external resource.

## Forward as an attachment

[**Modified:** 8.5.113.11]

(Formerly: *Inbound Email Forward to External Resource*)

Workspace enables agents to forward active inbound email interactions to an external resource (someone in your company directory that is outside of the control of the Genesys environment — for example, your back office) by selecting a valid email address in Team Communicator, either by manually entering the address or by selecting it from a searched Contact or a Corporate or Personal Favorite. Forward as an Attachment supports both **To** and **CC** (carbon copy) addressing and multiple recipient targets. You can configure agents to be able to add additional information about the forwarded interaction in a dedicated text box.

The typical use case is that agents delegate the writing of an answer to the external resource.

A set of key-value pairs that include the destination email address and other information is added to the inbound email before it is placed in the Forward queue so that they can be used in a Business Process:

- `GD_ExternalAgentAddress`—The same content as `IW_ExternalAgentAddress`. This is added only if the general.gad.attached-data option is set to `true`.
- `GD_OriginalAgentEmployeeId`—The same content as `IW_OriginalAgentEmployeeId`. This is added only if the general.gad.attached-data option is set to `true`.
- `GD_TransferrerUserName`—The same content as `IW_TransferrerUserName`. This is added only if the general.gad.attached-data option is set to `true`.
- `IW_OriginalAgentEmployeeId`—The Empoyee Id of the agent.
- `IW_TransferrerUserName`—The UserName of the agent.

- `IW_EmailNotepad`—The current notepad text of the email view.
- `IW_ExternalAgentAddress`—The **To** email address destination. If the value of the email.forward.enable-multiple-to-addresses option is set to `true`, the value of `IW_ExternalAgentAddress` is a comma separated list of **To** addresses. This list has to be parsed in the Business Process. For each extracted address, the Business Process has to do the following:
  1. Assign the extracted address to a variable.
  2. Use this variable in the Forward Email block.
- `IW_ExternalAgentCcAddress`—The **CC** email address destination. This is added only if the value of the email.forward.enable-cc-addresses option is set to `true` (Enable the CC address field where agents can specify one or several CC addresses). The value is a comma separated list of **CC** addresses. With this list, the Business Process has to do the following:
  1. Assign the list to a variable.
  2. Use this variable in the Forward Email block.
- `IW_ExternalAgentInstructions`—The text provided by the agent who is forwarding the email interaction. This is added only if the value of the email.forward.enable-instructions option is set to `true` (Enable the forward instructions field). This value can be used as a Field Code in the Standard Response that is contained in the Forward Email block to give forward instructions to an external resource.

Refer to EServices email workflow samples for more information about forwarding email interactions to external resources.

The following privilege controls the use of the forwarding feature:

- E-Mail - Can Forward to External Resource

Use the following configuration options in the `interaction-workspace` section to configure this feature:

- email.forward-queue: Specifies the Interaction Queue in which the inbound email is placed when an agent forwards it to an external resource.
- email.forward.enable-multiple-to-addresses: Enable agents to specify more than one target in the **To** address field.
- email.forward.enable-cc-addresses: Enable agents to specify one or more target in the **CC** address field.
- email.forward.enable-instructions: Enable the forward instructions field.
- keyboard.shortcut.interaction.email.forward: Specifies the shortcut that forwards an active inbound email.

## Email Can Mark Done privilege

The `Can Mark Done` privilege controls how emails are marked as done.

When this privilege is allowed, the Done button is displayed in the toolbar when an inbound email is presented. If an agent clicks Done, the inbound email is terminated (removed from the Business Process). It will then not be possible to submit any corresponding outbound reply from the interaction view. It can only be reopened from the Contact History.

When this privilege is not allowed, the Done button is not displayed in the toolbar when an inbound email is displayed. The agent must handle the email by replying to it, transferring it, or placing it in a workbin.

## Email interaction history

An agent can take ownership of email interactions that are in-progress if you grant the permissions that are listed in the table **Agent Privileges that Control Email Interaction History Functionality** lists the privileges that can be used to enable the Interaction History for agents. The E-mail Interaction History feature displays the status of the interaction to agents by using the detailed status information that is provided by Interaction Server. The in-progress status of an email enables agents to find and process inbound email interactions that are in a queue but are not assigned, or are in the process of being routed. The in-progress status can also be used to restrict which agents can handle an in-progress interaction.

**Agent Privileges that Control Email Interaction History Functionality**

| Privilege | Agent Functionality |
|---|---|
| Workbin - Can Use | Agents can open any email that is present in the agent's personal workbins or in shared workbins to which the agent has access from the Workbin view. |
| Contact - Can Pull From Other Personal Workbins | Agents can select an email that is currently in the workbin of another agent. |
| Contact - Can Pull From unasigned shared workbin | Agents can select an email from a shared workbin to which the agent is not assigned or is in the scope of a group to which the agent is not a member. |
| Contact - Can Pull Queued Emails | Agents can select an email that is in a queue or that is currently being delivered. |

## Printing

[**Modified:** 8.5.101.14]

From the following views, agents can display and use the Print Preview window:

- Email Interaction window
- My History
- Contact History
- Draft workbin

The Print Preview window provides the following functionality:

- Print preview
- Printer selection

- Page range
- Page layout
- Configurable page margins
- Page numbers

Enable the following privilege to allow agents to print email interactions:

- Can Print Email

Configure the following option to specify whether the Print Preview window is displayed to the agent:

- printing.use-print-preview

# Email Quality Assurance

Workspace supports Quality Assurance (QA) review of outbound email interactions. Team Leads (supervisors) or other individuals can approve or reject email interactions or email interactions in workbins. You can design your routing strategy to send all email interactions from and agent or agent group to a reviewer; you can design your routing strategy to enable an agent to request a review; you can direct email interactions for review to a reviewer or a group or to a workbin. You can design your routing strategy to send rejected email interaction back to the originating agent or to a workbin.

## Designing a Routing Strategy for an email quality assurance review

The email QA Review process is managed by a Routing Strategy and Business Process design. You must configure specific keys that are set in the interaction by Workspace; these keys are used by the Routing Strategy to route the interaction based on its review state, as defined by the keys. In the following example, the keys prefixed by "BP_" are exclusively under the responsibility of the Routing Strategy or Business Process. The keys that do not have this prefix are keys that are defined by Workspace. The values of the keys are interpreted and/or updated by the core product implementation and can also be interpreted/edited by the Routing Strategy or Business Process.

Prerequisites to enable the "QA Review Disposition" feature:

- Create a Business Attribute in Genesys Administrator Extension that defines all possible QA review dispositions. The following example uses the `Rejected` and `Accepted` dispositions as samples. You should use values that suit your business purposes.
- Assign the name of this Business Attribute as the value of the email.qa-review-dispositions-business-attribute option.
- The QA Review disposition that is selected by a Team Lead (supervisor) is assigned to the attached data `Ixn.UserData.QAReviewDisposition`, described in the following section. Your Business Process must apply rules that are based on this disposition— for example, redistributing to the writer.

The following is an example of a Strategy workflow:

1. An inbound email is received by the Business Process
2. The inbound email is distributed to an agent
3. The agent writes a reply email and clicks Send
4. Workspace makes the following updates to the attached data of the reply email
   - In the UCS interaction record, `OwnerID` is set to the DBID of the agent.
   - In the UserData of the Interaction Server interaction record, `OriginalAgentEmployeeID` is set to the EmployeeID of the agent.
   - In the UserData of the Interaction Server interaction record, `OriginalAgentUserName` is set to the username of the agent.

5. The email is then directed to the Business Process, and the Business Process should make the following updates to the reply email and distribute it to the reviewer target:
   - In the UserData of the Interaction Server interaction record, QAReviewFlag is set to 1
   - In the UserData of the Interaction Server interaction record, QAReviewDisposition is set to Unknown
   - In the UserData of the Interaction Server interaction record, BP_QAReview_Status is set to Review
   - In the UserData of the Interaction Server interaction record, BP_QAReview_Cycle# is set to 1
6. The reviewer reviews the email and edits it or provides feedback. If the reviewer sets the disposition to Rejected, it is sent back to the originating agent.
7. Workspace makes the following updates to the attached data of the rejected reply email:
   - In the UCS interaction record, ReviewerID is set to the DBID of the reviewer.
   - In the UserData of the Interaction Server interaction record, QAReviewerEmployeeId is set to the employee ID of the reviewer.
   - In the UserData of the Interaction Server interaction record, QAReviewerUserName is set to the username of the reviewer.
   - In the UserData of the Interaction Server interaction record, QAReviewDisposition is set to Rejected
8. The email is then directed to the Business Process, and the Business Process should make the following updates to the reply email and distribute it to the original agent:
   - In the UserData of the Interaction Server interaction record, QAReviewFlag is set to 0
9. The agent makes the required changes and then clicks Send.
10. Workspace makes the following updates to the attached data of the reply email and directs it the the Business Process:
    - In the UCS interaction record, OwnerID is set to the DBID of the agent.
    - In the UserData of the Interaction Server interaction record, OriginalAgentEmployeeID is set to the employee ID of the agent.
    - In the UserData of the Interaction Server interaction record, OriginalAgentUserName is set to the username of the agent.
11. The Business Process should make the following updates to the reply email and distribute it to the Reviewer Target:
    - In the UserData of the Interaction Server interaction record, QAReviewFlag is set to 1
    - In the UserData of the Interaction Server interaction record, QAReviewDisposition is set to Unknown
    - In the UserData of the Interaction Server interaction record, BP_QAReview_Status is set to Review
    - In the UserData of the Interaction Server interaction record, BP_QAReview_Cycle# is set to 2
12. The reviewer reviews the email reply again and sets the disposition to Accepted and clicks Send
13. Workspace makes the following updates to the attached data of the accepted reply email and directs it to the Business Process:
    - In the UCS interaction record, ReviewerID is set to the DBID of the reviewer.
    - In the UserData of the Interaction Server interaction record, QAReviewerEmployeeId is set to the employee ID of the reviewer.

- In the UserData of the Interaction Server interaction record, `QAReviewerUserName` is set to the username of the reviewer.
- In the UserData of the Interaction Server interaction record, `QAReviewDisposition` is set to `Accepted`

14. The Business Process should make the following updates to the reply email and then distribute it to the Final 'Send Email' Business Process:
    - In the UserData of the Interaction Server interaction record, clear key: `QAReviewFlag`
    - In the UserData of the Interaction Server interaction record, clear key: `BP_QAReview_Status`
15. The email reply is sent to the contact.

## Outbound email quality assurance review

The Workspace outbound email review feature enables you to redirect outbound email interactions to an internal target for review. The Quality Assurance Review function has the following features:

- Outbound email interactions can be redirected to a reviewer or workbin
- Reviewers can accept and send the outbound email to the recipient
- Reviewers can reject the outbound email interaction and send it back to the author to be reworked
- Review of outbound email interactions can be configured to be handled through a workbin folder
- Rejected outbound email interactions can be configured to be handled through a workbin folder

The following is a sample of the outbound email review process workflow:

1. E-mail interaction is received from a contact and is routed to an agent who, by a business process is identified as an agent whose outbound email interactions are to be sent for review before the email is sent to the contact.
2. The agent creates a reply to the inbound email interaction, or the agent creates a new outbound email interaction, and clicks **Send**.
3. Workspace tags the email interaction with the `EmployeeID` and `UserName` of the agent, and stores the `OwnerID` of the author in the email interaction history in Universal Contact Server.
4. The outbound business process for the agent is activated and the email interaction is flagged for review. The review flag is a count of the number of review iterations which the interaction has undergone. The business process might also be configured to attach other key/value pairs to the interaction.
5. The email interaction is redirected to the agent, agent group, role, or workbin who/that is defined by the business process as the reviewer. The reviewer either receives the email interaction directly or retrieves it from a workbin.
6. The email interaction reviewer can modify the interaction, add information to the Notepad, and then accept or reject the email interaction.
    - If the reviewer accepts the interaction, the email interaction is sent to the contact.
    - If the reviewer rejects the interaction, the email interaction is sent back to the agent who created the email.
7. If the email interaction is returned to the agent, the agent can change the email according to the

comments that are provided by the reviewer or view the changes that were made by the reviewer.

8. The agent finishes updating the email interaction and then clicks **Send**.
9. The outbound business process for the agent is activated and the email interaction is flagged for second review.
10. The email interaction is redirected to the agent or agent group or roles who is defined by the business process as the reviewer.
11. The email interaction reviewer can modify the interaction, add information to the Notepad, and then accept or reject the email interaction, or apply some other disposition that is specific to the design of your business process or routing strategy. Workspace tags the email interaction with the `EmployeeID` and `UserName` of the reviewer, and stores the `ReviewerID` of the author in the email interaction history in Universal Contact Server.
    - If the reviewer accepts the interaction, the email interaction is sent to the contact.
    - If the reviewer rejects the interaction, the email interaction is sent back to the agent who created the email, either directly, or placed in a special workbin for rejected email interactions, and the process begins again. The review count is incremented by one.

## Creating a For-Review workbin

If you want to direct to a workbin outbound emails that require review, you must create the workbin in the eServices Business Process (script name="review_outbound_emails").

Configure a group or user and make it available only to agents, agent groups, tenants, or roles whom you want to be email interaction reviewers by specifying the value `review_outbound_emails` for the workbin.<media-type>.<workbin-nickname> (workbin.email.review) option in the `interaction-workspace` section.

## Displaying review information in the Case Information area

You can create Business Attributes to populate the interaction Case Information area with information about the review process that informs the reviewer and the author of the email about the status of the review. For example, you could create keys for Review Status and Review Cycle Count.

You can create an editable Case Information attribute that is displayed as a drop-down list of disposition types. Refer to the interaction.case-data.format-business-attribute option for information about creating new attributes for case data.

## Creating a Rejected Outbound Email workbin

If you want to direct to a workbin outbound emails that were rejected by a reviewer, you must create the workbin in the eServices Business Process (script name="rejected_outbound_emails").

Configure a group or user and make it available only to agents, agent groups, tenants, or roles whom you want to be email interaction reviewers by specifying the value `rejected_outbound_emails` for the workbin.<media-type>.<workbin-nickname> (workbin.email.rejected) option in the `interaction-workspace` section.

# Chat

[**Modified:** 8.5.108.11, 8.5.113.11, 8.5.115.17, 8.5.118.10, 8.5.122.08, 8.5.128.07, 8.5.132.05, 8.5.140.08, 8.5.142.05, 8.5.145.06]

Workspace employs the following Chat privileges for all Chat interactions:

- Can Use Chat Media
- Can Decline Chat
- Can Release
- Can One Step Transfer
- Can One Step Conference
- Can Push Url
- Can Set Interaction Disposition
- Show Silent Monitoring
- Can Preview Customer Typing [**Added:** 8.5.108.11]
- Chat - Can Transfer File From File System [**Added:** 8.5.115.17]
- Chat - Can Transfer File From Standard Response [**Added:** 8.5.115.17]
- Chat - Can Save Attached files [**Added:** 8.5.115.17]

> **Warning**
>
> If the Chat - Can Preview Customer Typing privilege is also granted, and you have configured eServices to hide sensitive personal information that is entered by the contact during the chat, agents will be able to see the information as it is entered, but not after the contact sends it.
> [**Added:** 8.5.108.11]

Workspace displays a "Contact is typing a message" notice when the contact begins to type a reply message in your web site chat interface. The Chat - Can Preview Customer Typing privilege enables agents to see what the contact is typing before the contact clicks **Send**. This feature enables agents to anticipate their reply and therefore respond more quickly. However, Genesys recommends that you train your agents to wait until the contact has sent their message before responding to it. The text that is being typed by the contact is updated according to the updates that the web site sends to the Web API and Chat Server; therefore, your web site designer is responsible of the refresh rate of the content.

Chat server can be configured to disconnect a chat upon inactivity of engaged parties. Workspace warns the agents when a chat is about to expire due to inactivity and notifies when the session is automatically closed because of inactivity. [**Added:** 8.5.109.25]

### Workspace notifies the agent through an audio alert or a visual alert when

another party is leaving (automatically, due to inactivity, or manually) or joining the chat session while the focus is not on the Workspace application or is on another area of Workspace.
**Visual notification added:** 8.5.113.11

The Chat feature supports spelling check. Refer to Spelling tab for information about configuring Spelling Check.

For Genesys Widget customers, Workspace supports Rich Messaging. [**Added: 8.5.142.05**]

You use the following options in the `interaction-workspace` section to configure Chat interactions:

- chat.simple-transcript: Specifies whether the chat transcript is displayed as simple lines of text or as colored blocks of text. [**Added:** 8.5.122.08]
- options.record-option-locally-only: Specifies whether the display settings for the agent are stored locally or in the agent annex.
- chat.pending-response-to-customer: Defines two alarm thresholds, in seconds, that warn agents that they have a pending response to a chat. Three levels are displayed: below the warning time, between the warning time and the maximum time, and above the maximum time. Agents are warned by the flashing of various elements in the user interface, including the taskbar, collapse/expand button, the interaction bar, and the pending response timer. If the agent places his or her mouse pointer on any of these flashing elements, a preview of the last received message from the contact is displayed.
- chat.show-unread-notification: Specifies whether the unread message notification is displayed in the chat transcript. When the message is read, the notification icon disappears. [**Added:** 8.5.122.08]
- chat.toast-information-key: Specifies whether the Information area is displayed in the Chat interaction notification. The option specifies the name of the attached data key that contains the information.
- chat.typing-isenabled: Specifies whether typing notification is enabled. It should be disabled for Chat Server lower than 8.0.1.
- chat.typing-timeout: Specifies the duration, in seconds, that the typing notification is displayed after the last keystroke and before the agent or contact sends their message.
- chat.new-message-bell: Specifies the new Chat sound configuration string.
- chat.reconnect-attempts—Defines the number of attempts to reconnect to the chat session. This applies to environments that implement Chat High Availability (HA) but also to simple environments if network disconnection occurs during a chat session.
- chat.reconnect-timeout—Defines the interval between each attempt to reconnect to the chat session. This applies to environments that implement Chat High Availability (HA) but also to simple environments if network disconnection occurs during a chat session.
- chat.nickname—Specifies that a nickname (pseudonym) is used in chat sessions instead of the agent's user name, and defines the nickname.
- display-format.chat-agent-name—Specifies the display format of agent identifiers in agent and team supervisor views.
- display-format.chat-customer-name—Specifies the display format of contact identifiers in agent and team supervisor views. [**Added:** 8.5.145.06]
- chat.auto-answer: Specifies whether a chat interaction is automatically answered when it is routed to an agent. This option can be overridden by a routing strategy. You can also configure auto-answer to display a timer that enables an agent to view case information before the interaction is automatically answered by using the chat.auto-answer.timer and chat.auto-answer.enable-reject options [**Added:**

8.5.105.12].

- chat.historical.maximum-age: Specifies the number of days of previous chat sessions with the current contact are to be displayed in the Chat interaction view before the current chat session. This reduces the need for agents to open the contact history to find previous chat interactions. Many chat sessions are conducted on mobile devices, meaning that the likelihood of timeout is very high. If a chat is resumed after a timeout, the agent sees the content of the previous sessions. [**Added:** 8.5.122.08]
- chat.rich-media-widget-width: Specifies the width, in pixels, of Rich Media in a chat interaction. The value of this option affects the minimum width of the Chat transcript view [**Added:** 8.5.150.06].
- chat.transcript-enable-history-filters: Specifies that the value specified for the contact.history.filters-<attribute> option is used to filter the history-based part of the chat transcript. Keys and values of the option are constructed like those of the `contact.history.filters-<attribute>` option. You can add these options to a routing strategy [**Added:** 8.5.132.05].
- chat.transcript-message-text-direction: Specifies whether messages in the chat transcript are displayed with a left-to-right (default) or a right-to-left reading layout. Use this option for chat interactions where contacts are using a right-to-left reading language [**Added:** 8.5.140.08].

## Provisioning the Chat channel

[**Modified:** 8.5.115.17, 8.5.128.07]

### 1. Enabling an agent to chat with a contact

**Purpose:**

To enable an agent to use the Chat channel to chat with a contact whose information is stored in Universal Contact Server (UCS).
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View.
- A working knowledge of Genesys Administrator 8.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to Universal Contact Server, Chat Server, and Interaction Server.
- The Procedure: Enabling agents to manage contacts.

**Start**

1. Allow the Chat privileges (see Chat Access Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group):
    - Can Use Chat Media
    - Can Decline Chat
    - Can Release
    - Can One Step Transfer

- Can Two Step Transfer
- Can One Step Conference
- Can Two Step Conference
- Can Set Interaction Disposition
- Can Preview Customer Typing [**Added:** 8.5.108.11]

2. Configure the Chat options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Chat configuration option reference for a list of Chat options and a description of how to configure them).

3. [**Added:** 8.5.128.07] Configure the Chat options that control how Chat interactions are marked as done. When an agent manually marks a Chat interaction as done, a new Chat interaction can be directed to the agent. Sometimes agents do not mark interactions done to avoid getting new interactions, which affects the focus time. To have Workspace automatically mark a Chat as done, use the following configuration options:

   - chat.auto-mark-done-owner-agent: When set to `true`, the Chat interaction is automatically closed and marked as done as soon as the last agent (the owner) ends the Chat session or the contact disconnects. To prevent the Chat interaction from closing immediately — for example to allow for after-call work — you can specify how long the interaction window stays open by using the chat.auto-mark-done-owner-agent.timer option.
   - chat.auto-mark-done-non-owner-agent: When set to `true`, the Chat interaction on the non-owner's desktop is automatically closed and marked as done as soon as the non-owner leaves the Chat session or the contact disconnects. To prevent the Chat interaction from closing immediately, for example to allow for after-call work, specify how long the interaction window stays open by using the chat.auto-mark-done-non-owner-agent.timer option.

   If the value of the interaction.disposition.is-mandatory option is `true`, then an agent must specify an outcome for the interaction before it can be closed. In this case, the auto-close options are overridden and the agent must click **Done** to close the interaction.

   If the value of the `interaction-workspace/mandatory` option is set to `true`, then an agent must edit the case data for the interaction before it can be closed. In this case, the auto-close options are overridden and the agent must click **Done** to close the interaction.

4. To keep chats open after the last agent leaves the session, which enables an agent to rejoin the session until the session is marked as done, set up Asynchronous chat [**Added:** 8.5.128.07]. Allow the following Chat privileges:

   - Chat - Can Place On Hold
   - Chat - Can Release Async
   - Chat - Can Release

   Configure the following options according to your environment:

   - chat.on-hold-queue
   - keyboard.shortcut.interaction.chat.hold

5. You can specify which Chat Server messages are included as part of the chat transcript in the interaction history. To include notices about inactivity timeout:

   - Set up the Chat Server inactivity control configuration options.
   - Set the value of the transcript-save-notices Chat Server option to `selective2`. [**Added:** 8.5.115.17]

**End**

## 2. Enabling Chat HA

**Purpose:**

To enable Chat for High Availability (HA).
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View.
- A working knowledge of Genesys Administrator 8.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to Universal Contact Server and Interaction Server.
- Chat Server 8.1.0 or higher.
- The Procedure: Enabling agents to manage contacts.

> ### Important
> Chat Server 8.1.0 Limitation: Do not use the application cluster to connect the Web API Server Application to Chat Server.

**Start**

1. Configure Chat Server for Warm Stand-by. Set the following values for the following Chat Server options for both the primary and backup Chat Servers:
   - `session-restoration-mode = simple`
   - `transcript-auto-save = 2`
   - `transcript-resend-attempts = 10`
   - `transcript-resend-delay = 15`
   - `transcript-save-on-error = continue`

   Refer to the EServices documentation for more information on setting up Chat Server.
2. For the Web API Server application, add a connection to the primary Chat Server.
3. Configure the following options in the `interaction-workspace` section of the Workspace Application object:
   - `chat.reconnect-attempts`--Defines the number of attempts to reconnect to the chat session.
   - `chat.reconnect-timeout`--Defines the interval between each attempt to reconnect to the chat session.

   Refer to the Chat configuration option reference for information about how to configure these options.

> **Tip**
>
> For information about configuring Load Balancing and Business Continuity, refer to Runtime Connection Logic in the eServices Load Balancing Business Continuity section of the *Business Continuity and Disaster Recovery* topic. [**Added:** 8.5.109.16]

**End**

## Configuring Chat Conference and Consultation with a Skill, Group, or Interaction Queue

Agents can use the Team Communicator to find an "Instant Chat Conference" and "Start Chat Consultation" target based on a skill, group, or interaction queue instead of searching for a specific individual or DN. The system router finds the next available target from a list of targets based on the skill, group, or interaction queue that is selected by the agent. A Business Process tries to route the call based on attached data. You can configure the contact attempt interval and the number of attempts to find an available target with the specified skill or in the specified agent group or interaction queue before the request times out. The requesting agent is informed if the request has timed out.

The following attached data keys are populated by Workspace:

- InternalConferenceInviteOwnerId—The `employeeId` of the agent who is requesting the conference or consultation.
- InternalConferenceInviteOwnerInteractionId—The `Interaction Id` of parent Interaction.

To enable this feature, allow the following privilege:

- Can One Step Conference

To configure the features of the Chat conference or consultation with a skill, an agent group, or an interaction queue, set the following configuration options:

- Set the value of the intercommunication.chat.conference.invite-timeout to specify the length of the interval before the conference invitation times out.
- Set the value of the intercommunication.chat.queue to the name of the interaction queue that is used by the routing based feature for chat.

## Receiving Files from Contacts

[**Added:** 8.5.115.17]

Workspace lets your agents handled files that have been sent by contacts in chat interactions. By default, agents enabled for chat can receive files, open them in an appropriate application, and print them (if applicable). You can configure Workspace to enable agents to save files on their local workstation that have been sent through chat by a contact. To enable this feature, allow the following privilege:

- Chat - Can Save Attached files

Configure the chat.show-attachment-image-thumbnail option to specify whether to display the icon of an attached image file in chat transcript as image thumbnail or as generic file) in the online session, the interaction history, or both.

Files are stored in the Contact History, so attached files can also be opened or saved from the Contact History view.

> **Warning**
>
> Workspace does not provide virus checking of files sent to your agents. You should have anti-virus software running on agent workstations to prevent infection from opening or saving infected files.

### Controlling attachment read-only behavior

[**Added:** 8.5.118.10]

By default, all attachments opened by agents in an external program are read-only. This means that agents cannot update them and save the changes to their hard drive.

Use the general.writable-downloaded-attachment-file-types option to override this behavior for specific file types. Allowing agents to edit only certain file types preserves the data integrity of files that you do not want agents to modify. For example, you might allow agents to modify `.jpg` and `.png` files so that the orientation can be changed, but restrict the modification of `.docx`, `.xlsx`, and other file types. Or, you might want to ensure that only `.xlsx` files can be updated by agents.

## Transferring files to contacts

[**Added:** 8.5.115.17]

You can enable your agents to transfer files to contacts in a chat interaction. You can specify whether agents can transfer files from their local workstation, from the Standard Response Library, or both. To enable this feature, allow one or more of the following privileges:

- Chat - Can Transfer File From File System
- Chat - Can Transfer File From Standard Response

A toolbar in the chat composition field enables agents to choose files from their local workstation.

Files that are transferred to a contact are also stored in the Contact History, so attached files can also be opened or saved from the Contact History view.

Use the following configuration options to control the behavior of this feature:

- chat.max-file-size: Specifies the maximum size of the file, in kilobytes, that an agent can attach to a chat interaction.
- chat.max-attachments-size: Specifies the total number of megabytes of files that an agent can attach to a chat interaction.
- chat.max-attachments-files: Specifies the maximum number of files that an agent can attach to a chat interaction.
- chat.restricted-attachment-file-types: Specifies the list of file types (for example: exe, `bat`, and so on) that agents cannot attach to a chat interaction.
- chat.attachment-download-timeout: Specifies the time to wait for Universal Contact Server to download a chat attachment.
- chat.show-attachment-image-thumbnail: Specifies whether to display the icon of an attached image file in chat transcript (as image thumbnail or as generic file) in the online session, the interaction history, or both.

## Enabling emojis

[**Added:** 8.5.115.17]

**Prerequisites:**

- Chat Server deployed in UTF-8 mode
- Interaction Server to handle attached data
- Universal Contact Server deployed in UTF-8 mode

If you want your agents to be able to send and receive *emojis* during chat interactions you must perform the following actions:

1. Allow the Chat - Can Use Emojis privilege.
2. Set the value of the chat.emojis-business-attribute option to the name of a Business Attribute that defines the emojis that you want to support.
3. Set the value of the gui.emoji-font-name option to specify which font should be used to display received emojis.

In chat interactions, emojis are handled as Unicode characters, which systems recognize and translate into an image. On computers, the image that is displayed is dependent on the font being used. Not all fonts support emojis and not all fonts support all emojis. On mobile devices, the image that is displayed is depending on the image set of the platform. Each mobile device substitutes the Unicode character with an image.

The list of emojis can be found at http://unicode-table.com/en/blocks/emoticons/. Click a Unicode character in the table to view how it looks on different platforms. For example: 1F601. Another resource for emojis can be found at http://unicode.org/emoji/charts/full-emoji-list.html.

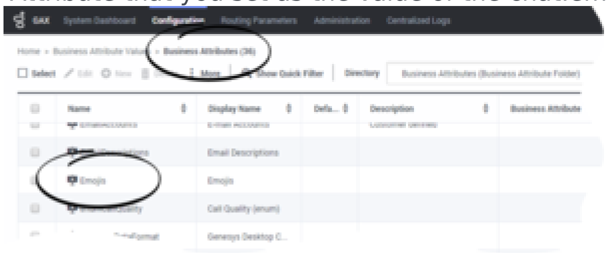
If an emoji is not supported by the font that you are using in your environment, it will be replaced by a rectangle in the chat transcript.

> ### Tip
> For more information about emojis in Genesys solutions, see this article.

## Creating the Business Attribute

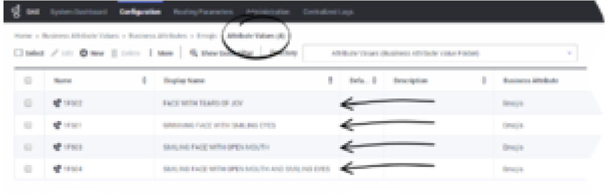
Use the following steps to create a Business Attribute that defines the emojis that your agent can send:

1. Create a new Business Attribute of type `Custom` with a name such as `Emojis`. This is the Business Attribute that you set as the value of the chat.emojis-business-attribute option.



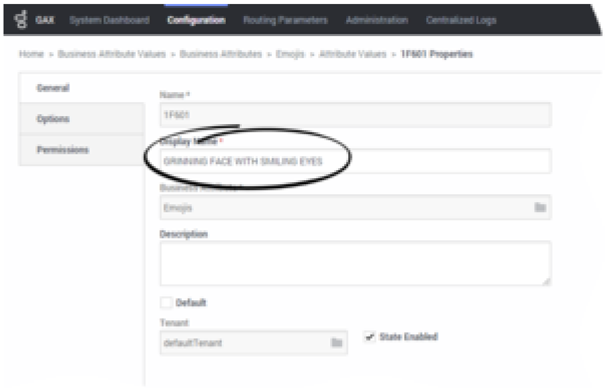
| Name | Display Name | Defa... | Description | Business Attribute |
|---|---|---|---|---|
| [illegible] | E-mail Accounts | | Customer Defined | |
| [illegible] | Email Descriptions | | | |
| Emojis | Emojis | | | |
| [illegible] | Call Quality (enum) | | | |
| [illegible]Format | Genesys Desktop C... | | | |

2. In the **Attribute Value** tab of the Business Attribute, create one value for each emoji Unicode character that you want to support.


GAX
System Dashboard
Configuration
Routing Parameters
Administration
Centralized Logs
Home › Business Attribute Values › Business Attributes › Emojis › Attribute Values (4)
Select
Edit
New
Delete
More
Show Quick Filter
Directory
Attribute Values (Business Attribute Value Folder)

| Name | Display Name | Defa... | Description | Business Attribute |
|---|---|---|---|---|
| 1F602 | FACE WITH TEARS OF JOY | | | Emojis |
| 1F601 | GRINNING FACE WITH SMILING EYES | | | Emojis |
| 1F603 | SMILING FACE WITH OPEN MOUTH | | | Emojis |
| 1F604 | SMILING FACE WITH OPEN MOUTH AND SMILING EYES | | | Emojis |

3. Name each value with a unique name, such as the code value of the Unicode character that you want to support. The `Display Name` that you define is displayed in a tooltip when an agent hovers their mouse pointer over an emoji before selecting it from the chat text field tools.



Name * 1F601

Display Name * GRINNING FACE WITH SMILING EYES

Business Attribute * Emojis

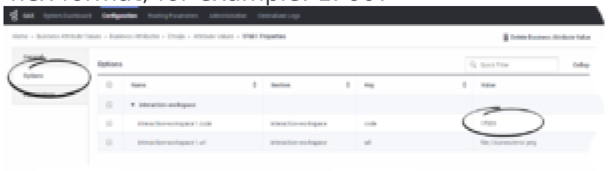
Description

□ Default

Tenant defaultTenant

☑ State Enabled

4. For each attribute value, configure the `interaction-workspace\code` option and assign to it the value of the emoji Unicode character. The value of the Unicode emoji format is 1F6nn where nn are digits in hex format; for example: 1F607



Options

| Name | Section | Key | Value |
|---|---|---|---|
| interaction-workspace | | | |
| interaction-workspace\code | interaction-workspace | code | 1F601 |
| interaction-workspace\url | interaction-workspace | url | [illegible].png |

# Chat monitoring

Workspace supports two approaches to monitoring, built-in Team Lead capabilities and support for 3rd-party Supervisor applications, such as Genesys 7.6 Supervisor Desktop.

## Team Lead functionality

You can configure an agent role to have the Team Lead capability. Team Leads (supervisors) have capabilities that extend beyond the coaching and barge-in abilities that are enabled by internal communications. Workspace supports auto-monitoring of agents in an agent group by a team lead that is configured as the Supervisor of this Agent Group.

A Team Lead can perform the following functions:

- Monitor the next interaction or the currently active interaction.
- Select an agent and monitor all the chat interactions of this agent in one of two modes:
    - silent—neither the agent nor the contact is aware of the monitoring
    - coaching—only the agent can see the messages from the Team Lead
- Silently monitor chat interactions
- Start a coaching monitoring session from a silent session
- Start a barge-in (all parties on the chat can see the Team Lead) monitoring session from silent or coaching session
- Start a silent monitoring session from coaching or barge-in session

Enable Team Lead functionality by allowing the Team Lead Privileges.

## Third-party supervision

You can enable agents that are assigned the chat task to be monitored by a supervisor who is using a Supervisor application, such as Genesys Supervisor Desktop 7.6.

If the agent is configured for notification, the agent is notified through the Workspace interface during supervisor monitoring. All monitoring is conducted through the supervisor application. An "eye" icon is displayed in the chat interaction window to indicate that the chat interaction is monitored. When the supervisor leaves the call, the icon disappears.

Workspace employs the following privilege for activating the Workspace supervisor monitoring:

- Chat - Show Silent Monitoring

# Video

Workspace enables agents to handle video interactions, including the following functionality:

- Accept, Reject, or Ignore an inbound Video Call by using the interactive Interaction Notification view.
- Auto-accept an inbound Video Call
- End Call
- Instant Transfer
- Instant Conference
- Add video to a SIP Voice call
- Hold the Video Call and display a splash screen
- Toggle the agent's camera on and off
- Store and view Video interactions in the Interaction History
- Control the size of the video display of each party during a Video Call
- Set an interaction disposition

The following limitations apply to video transfer and conference:

- For video conferences, the video stream is limited to single mode. Mixed mode is not supported.
- Two-Step conference of a video call results in a pure voice conference engaging the video call initiator, the agent making the conference, and the new party of the conference.
- Two-Step transfer of a video call results in a pure voice call between the video call initiator and the target of the transfer.
- Consultation video calls are not supported. If a consultation is started in the context of a video call, this will be a pure voice consultation.

Refer to the following resources for details about video conference settings:

- SIP Server Deployment Guide
- Chapter 3 in the GVP 8.1 User's Guide has numerous references to MCP, including: Configuring MCP, MRCPv2, CCP, CTIC, and RM for Secure SIP Transport
- VP Solution 8.1 Integration Guide
- GVP 8.5 Deployment Guide
- Media Server 8.5 Deployment Guide

Workspace employs the following privileges for all video interactions:

SIP Endpoint - Can Use Embedded SIP Endpoint

> **Important**
>
> Workspace SIP Endpoint 8.5.0 is required to support video functionality. Only the `VP8` and `H.264` video codecs are supported.

You use the following options in the interaction-workspace section to configure video interactions:

- sipendpoint.policy.session.auto_accept_video—Specifies whether video calls are accepted automatically or manually.
- sipendpoint.video.auto-activate—Specifies whether a video stream is automatically or manually added to a voice call.
- sipendpoint.video.always-on-top—Specifies the video capture rate, in frame per second, of the local video camera.
- sipendpoint.video.thumbnail-ratio—Specifies the size of the video thumbnail that displays on the agent desktop the video stream that the agent is sending to the contact.
- sipendpoint.video.camera-frame-rate—Specifies the video capture rate, in frame per second, of the local video camera.
- sipendpoint.video.camera-frame-size—Specifies the frame size capture of the local video camera.
- sipendpoint.video.camera-render-format—Specifies the size ratio of the thumbnail to the video in the SIP video window when both local and remote video are displayed.
- sipendpoint.codecs.h264.fmtp—Specifies the profile of the `H.264` codec. This option is applicable only if the value of the sipendpoint.policy.session.auto_accept_video option is set to 1.

Refer to the Procedure: Enabling an agent to use SIP Video interactions for information on enabling the video feature.

The following are examples of two scenarios that you might choose to use:

## 1. Inbound with auto-accept

To configure the video channel to automatically accept inbound interactions, set the values of the following two options like this:

- `sipendpoint.policy.session.auto_accept_video = 1`
- `sipendpoint.video.auto-activate = true`

With this configuration, inbound video calls are distributed to the agent from an endpoint that enables video by using the `VP8` or `H.264` codec. When an agent accepts the incoming call, the video window is also displayed. The contact is displayed in the main video window and the local video is displayed in the main video window as a thumbnail.

## 2. Inbound without auto-accept

To configure the video channel to automatically accept inbound interactions, set the values of the following two options like this:

- `sipendpoint.policy.session.auto_accept_video = 1`
- `sipendpoint.video.auto-activate = false`

With this configuration, inbound video calls are distributed to the agent from an endpoint that enables video by using the VP8 or `H.264` codec. When the agent accepts the incoming call, it is handled by agents as voice-only calls.

Agents can use the **Start Video** control of the interaction bar to activate the video component of the call and display the video window. The contact is displayed in the main video window and the local video is displayed in the main video window as a thumbnail (reduced size image).

# SMS and MMS

[**Modified:** 8.5.110.13, 8.5.115.17, 8.5.122.08, 8.5.132.05]

There are three media types that you can configure in the Configuration Server Manager `Media Type` business attribute. You can set the following media types:

- `sms`: Use this media type to enable page mode (single message inbound and reply).
- `smssession`: Use this media type to enable session mode (multiple message "chat"-like session).
- `mms`: Use this media type to enable the attachment of images as Multimedia Message Service (MMS) to an SMS interaction. MMS is a separate media channel that appears as part of the SMS channel in the agent interface. [**Added:** 8.5.110.13]

In page mode, messages are handled individually. A contact sends a message, the agent handles the message (replies or forwards it), and the SMS interaction view is closed.

In session mode, a keyword is sent by the contact that indicates that the SMS is to be part of a chat-like session. Multiple SMS messages are exchanged between an agent and a contact in a single interface. In addition to the keyword, session mode also functions when the SMS is sent to a specific, pre-configured inbound phone number.

In MMS mode [**Added:** 8.5.110.13], an image is sent by a contact as an inbound MMS in page mode. Images are displayed in the transcript as thumbnails. To view the images full size, an agent must click the thumbnail. The image opens in the application that is configured as the Windows default for that media type. The following MIME-types are supported for MMS:

- Bitmap (image/bmp)
- GIF (image/gif)
- JPEG (image/jpeg)
- Portable Network Graphics (image/png)
- TIFF (image/tiff)
- ICO (image/vnd.microsoft.icon)

## Warning

When MMS interactions are selected in the Contact History view of an interaction window, the full-sized MMS image is loaded when the MMS message is selected.

Workspace employs the following privileges for all SMS and MMS interactions:

- SMS - Can Use SMS: Enables access to the SMS channel.
- SMS - Can Decline SMS: Enables the agent to decline an SMS interaction.

- SMS - Can One Step Transfer: Enables the agent to transfer an SMS interaction.
- SMS - Can Set Interaction Disposition: Enables the agent to set a disposition for an SMS interaction.
- SMS - Can Create SMS: Enbles the agent to create a new SMS interaction.
- SMS - Can Save Attached File: Enbles the agent to save an MMS [**Added:** 8.5.110.13]

Refer to Spelling tab for information about configuring spelling check.

You use the following options in the `interaction-workspace` section to configure the channel to handle SMS interactions:

- sms.simple-transcript: Specifies whether the SMS transcript is displayed as simple lines of text or as colored blocks of text. [**Added:** 8.5.122.08]
- openmedia.bundle.sms: Specifies the list of media-types (SMS page mode, SMS Session mode, and MMS) that are used to implement the SMS channel. [**Modified:** 8.5.110.13]
- login.sms.can-unactivate-channel: Specifies whether the agent can select and unselect (activate and deactivate) the SMS channel.
- login.sms.is-auto-ready: Specifies whether the SMS channel is automatically in the ready state at login.
- sms.ringing-bell: Specifies the path to the sound file that is played when an sms message is received.

You can use the following `intercommunication` options in the `interaction-workspace` section to configure the routing of SMS interactions:

- intercommunication.sms.routing-based-targets: Specifies the list of targets that are contacted through the Routing Base feature mechanism for the requests that are defined in the option intercommunication.sms.routing-based-actions.
- intercommunication.sms.routing-based-actions: Specifies the list of routing-based actions that an agent may perform.
- intercommunication.sms.queue: Specifies the name of the queue that is used by the Routing Base feature.
- sms.transcript-enable-history-filters: Specifies that the value specified for the contact.history.filters-<attribute> option is used to filter the history-based part of the SMS transcript. Keys and values of the option are constructed like those of the `contact.history.filters-<attribute>` option. You can add these options to a routing strategy. [**Added:** 8.5.132.05]

You can use the following options in the `interaction-workspace` section to configure SMS interactions:

- sms.max-message-number: Specifies the maximum number of SMS that are considered to be part of a single message.
- sms.agent.text-color: Specifies the color of the text of the messages that are entered by an agent in the SMS interaction view.
- sms.agent.prompt-color: Specifies the color of the prompt for the messages that are entered by an agent in the SMS interaction view.
- sms.other-agent.text-color: Specifies the color of the text entered by another agent in the SMS interaction view.
- sms.other-agent.prompt-color: Specifies the color of the prompt for the messages that are entered by the target agent in the SMS interaction view.

- sms.client.text-color: Specifies the color of the text received by a contact in the SMS interaction view.
- sms.client.prompt-color: Specifies the color of the prompt for the messages entered by a contact in the SMS interaction view.
- sms.time-stamp: Specifies whether the time stamp is displayed in the SMS transcript area.
- sms.auto-answer: Specifies whether an SMS interaction is accepted automatically when an Interaction Server `Invite` event is received. This option can be overridden by a routing strategy. You can also configure auto-answer to display a timer that enables an agent to view case information before the interaction is automatically answered by using the sms.auto-answer.timer and sms.auto-answer.enable-reject options (**Added:** 8.5.105.12).
- sms.default-queue: Specifies the Interaction Queue to which a new or reply outbound SMS is submitted.
- sms.outbound-queue: Specifies the Interaction Queue to which outbound SMS are moved when an agent clicks Send. This option is used only when the Interaction Workflow does not specify the `Queue for New Interactions` when Inbound SMS are being routed to an agent.
- sms.from-numbers-business-attribute: Specifies the business attributes that contain the attribute values that are used as an enumerated value for the From number of an SMS interaction.
- sms.transcript-time-frame: Specifies the range of time in which to search for previous interactions by the same contact.
- sms.subject-max-chars: Specifies the maximum number of characters from an SMS message that are used to create the message subject if the SMS does not contain a subject.
- sms.reconnect-attempts: Defines the number of attempts to reconnect to the sms session. This applies to environments that implement SMS High Availability (HA) but also to simple environments if network disconnection occurs during an sms session. For more details see DMS High Availability configuration. [**Added:** 8.5.153.05]
- sms.reconnect-timeout: Defines the interval between each attempt to reconnect to the sms session. This applies to environments that implement SMS High Availability (HA) but also to simple environments if network disconnection occurs during an sms session. For more details see DMS High Availability configuration. [**Added:** 8.5.153.05]

## Provisioning the SMS Channel

[**Modified:** 8.5.110.13, 8.5.115.17]

### Procedure

Enabling an agent to use SMS to exchange SMS with a contact

**Purpose:**

To enable an agent to use the SMS channel to exchange SMS with a contact that is stored in Universal Contact Server (UCS) and to receive MMS.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.

- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to Universal Contact Server and Interaction Server.
- The Procedure: Enabling agents to manage contacts.

**Start**

1. Allow the SMS privileges (see SMS Access Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group).
   - SMS - Can Use SMS: Enables access to the SMS channel.
   - SMS - Can Decline Chat: Enables the agent to decline an SMS interaction.
   - SMS - Can One Step Transfer: Enables the agent to transfer an SMS interaction.
   - SMS - Can Set Interaction Disposition: Enables the agent to set a disposition for an SMS interaction.
   - SMS - Can Create SMS: Enbles the agent to create a new SMS interaction.
   - SMS - Can Save Attached File: Enbles the agent to save an MMS [**Added:** 8.5.110.13]
2. Configure the openmedia.bundle.sms option to specifies the list of media-types (SMS page mode, SMS Session mode, and MMS) that are used to implement the SMS channel. [**Modified:** 8.5.110.13]
3. Configure the SMS options in the `interaction-workspace` section of the Workspace `Application` object (refer to the SMS configuration option reference for a list of SMS options and a description of how to configure them, and to SMS and MMS Interactions for a list of other configuration options).

   > Tip
   >
   > For information about configuring Load Balancing and Business Continuity, refer to Runtime Connection Logic in the eServices Load Balancing Business Continuity section of the *Business Continuity and Disaster Recovery* topic. **Added:** 8.5.109.16

4. You can specify which Chat Server messages are included as part of the SMS Session transcript in the interaction history. To include notices about inactivity timeout:
   - Set up the Chat Server inactivity control configuration options.
   - Set the value of the transcript-save-notices

   Chat Server option to `selective2`. [**Added:** 8.5.115.17]

**End**

# Web Callback

Workspace supports agent processing of Web Callbacks. Contacts can schedule a callback through your website. Workspace employs the following privileges for all Web Callback interactions:

- Can Use Web Callback Channel: Enables access to the Web Callback channel. All other Web Callback privileges are dependent on this one.
- Can Decline: Enables agents to decline incoming Web Callback interactions.
- Can Set Interaction Disposition: Enables agents to set disposition codes for Web Callback interactions.
- Can Reschedule: Enables agents to reschedule a Web Callback interaction.
- Can Reschedule Before Call: Enables agents to reschedule a Web Callback Preview at a different date and/or time. The Can Reschedule privilege must be enabled for this privilege to be active. If Can Reschedule is enabled but Can Reschedule Before Call is disabled, agents can still reschedule the Web Callback Preview after they have connected and disconnected the call.
- Can Reschedule On New Number: Enables agents to reschedule a Web Callback interaction by using a new phone number.
- Can Mark Done: Enables agents to mark inbound Web Callback interactions as Done without processing them further.

You must also allow the voice privileges since the Workspace Voice channel is used to complete Web Callback interactions. To function correctly, the Web Callback feature requires Interaction Server to be available in the environment (refer to the eServices documentation), as well as either a Voice TServer or SIP Server. To support the transfer of corresponding Voice calls, configure the webcallback.park-queue option. To automatically dial the call when the web Callback interaction is accepted, configure the webcallback.auto-dial. You use the following options in the `interaction-workspace` section to configure the channel to handle Web Callback interactions:

- login.webcallback.auto-not-ready-reason: Specifies whether the channel is set to Not Ready Reason automatically when the agent logs in.
- login.webcallback.can-unactivate-channel: Specifies whether the agent can unactivate the Web Callback Channel.
- login.webcallback.is-auto-ready: Specifies whether the channel is set to Ready automatically when the agent logs in.
- webcallback.auto-answer: Specifies whether a Web Callback interaction is automatically accepted when an Interaction Server `Invite` event is received. This option can be overridden by a routing strategy, as described in Overriding Options by Using a Routing Strategy. You can also configure auto-answer to display a timer that enables an agent to view case information before the interaction is automatically answered by using the webcallback.auto-answer.timer and webcallback.auto-answer.enable-reject options (**Added:** 8.5.105.12).
- webcallback.auto-dial: Specifies whether Callback Phone Number is automatically dialed when an Interaction Web Callback is accepted.
- webcallback.callback-information.content: Specifies the callback data that is displayed in the Callback Information Area. The callback data entries are displayed in the order in which they appear in the list.
- webcallback.complete-queue: Specifies the Interaction Queue in which Web Callback interactions are placed when an agent marks it as `Processed`.

- webcallback.park-queue: Specifies the Interaction Queue in which the parent Web Callback interaction is placed when an agent transfers a voice call that is created from a Web Callback interaction.
- webcallback.ringing-bell: Specify the web callback ringing sound configuration string of a web callback is delivered to the agent.
- webcallback.callback-information.frame-color: Specifies the color of the border of the Web Callback Information view frame of Web Callback interactions. This option can be overridden by a routing strategy, as described in Overriding Options by Using a Routing Strategy.
- webcallback.callback-information.header-foreground-color: Specifies the color of the foreground of the Web Callback Information view frame of Web Callback interactions. This option can be overridden by a routing strategy, as described in Overriding Options by Using a Routing Strategy.
- webcallback.reschedule-queue: Specifies the Interaction Queue in which Web Callback interactions are placed when an agent reschedules it.

# Callback

[**Added:** 8.5.111.21]

Workspace supports agent processing of Voice Callback interactions through Genesys Callback is provided as an integrated service through Genesys Mobile Services (GMS) component. Contacts can request a callback through your website and these are routed to available agents according to your routing strategy. For information about setting up **Genesys Callback**, refer to the *Genesys Callback Online Documentation* and the *Genesys Callback User's Guide*.

The following user callback request scenarios are supported:

- **Immediate**: The contact requests an immediate callback, to be routed to the agent as soon as the agent is available. The contact is called and a treatment is played until the agent is available.
- **Delayed**: The contact requests a delayed callback, to be called back when the request reaches the top of the queue.
- **Delayed (Agent Preview)**: The contact requests a delayed callback based on available times. At the designated time, when the agent is available, a callback preview is directed to the agent and the agent connects the call to the contact. Configure five different key-value pairs or whole list.
- **Scheduled**: The contact requests a callback to be scheduled for a desired time based on available time slots.

Workspace employs the following privileges for all Callback interactions:

- Can Use Callback: The agent is permitted to use the Callback media.
- Can Reject Invitation: The agent is permitted to decline a Callback so that it can be processed by a different agent. Depends on 'Callback - Can Use Callback Channel'.
- Can Reschedule Current Callback: The agent is permitted to reschedule the current Callback interaction. Depends on 'Callback - Can Use Callback Channel'.
- Can Reschedule Or Submit On New Number: The agent is permitted to reschedule a Callback interaction or submit a new Callback by using a new phone number. Depends on 'Callback - Can Use Callback' and 'Callback - Can Reschedule Current Callback' or 'Callback - Can Submit New Callback'.
- Can Submit New Callback: The agent is permitted to create a new Callback interaction from another interaction or by using the Team Communicator. Depends on 'Callback - Can Use Callback Channel'.

You must also allow the voice privileges since the Workspace Voice channel is used to complete Callback interactions.

Use the Callback options in the `interaction-workspace` section to configure the channel to handle Callback interactions and to configure the appearance and content of the Callback information view. You must specify the URL of the Genesys Mobile Server (GMS) that is used for Callback requests by using the callback.gms-url option.

## Configuring a callback type for the Schedule Callback window

You use a Business Attribute of type `Interaction Operational Attribute` to define the callback types that are specified by the callback.callback-types-business-attribute option in the `interaction-workspace` section. A callback type is a combination of the following:

- A Callback Service defined in Genesys Mobile Services (GMS)
- A time slot duration
- A set of Key-Value Pairs.

The callback types that are available to an Agent or a Group of Agents are defined by using Business Attribute Values. Specify the Business Attribute name as the value of the callback.callback-types-business-attribute option.

> ### Warning
>
> Configure the Callback type data in the annex of the Business Attribute Value objects, not in the annex of the Business Attribute object that contains it.

This is the recommended workflow for specifying Callback types:

1. Create a **Business Attribute** and give it a name.
2. In the **Business Attribute**, create as many **Business Attribute Values** as there are Callback Types to be exposed to Agents.
3. In the annex of each **Business Attribute Value**, specify the keys described below under *Business Attribute Value Annex*.
4. Set the value of the callback.callback-types-business-attribute Workspace option to the name of the Business Attribute that you created in step 1.

**Business Attribute Values** should be configured as follows:

- Business Attribute Value Name: (Mandatory) The unique technical name for this callback type
- Business Attribute Value Display Name: The name that is shown in the **Callback Type** drop-down list of the Schedule Callback window. To specify that a particular Business Attribute value is default, set `Default` to `True` when you create the attribute value.The default callback type is selected by default in the Reschedule Callback and New Callback dialog boxes. If no default is specified, the callback types are displayed alphabetically and the first callback type is selected by default.
- Business Attribute Value Annex:
    - `interaction-workspace/callback.service-name`: The Callback Service name defined in GMS to be associated with this callback type
    - `interaction-workspace/callback.time-slot-duration`: Specifies the duration, in minutes, of the time slots to be displayed in the time picker of the **Reschedule Callback** and **New Callback** dialog boxes. It must be a multiple of the "bucket" duration that is specified in the corresponding Callback Service ('_request_time_bucket') option defined in GMS. Valid values are `15`, `20`, `30`, `60`. Default value is `15`.

- interaction-workspace/callback.keys.<business-key>=<business-value>: The Key-Value pairs to be attached to the (re-)schedule request as the business context of this callback type.

## Personalizing the content of the Callback Preview notification

The business data that is distributed as part of the Callback Preview notification has a static key structure:

```
1=Value1
2=Value2
3=Value3
etc...
```

To display agent-facing labels instead of the keys "1", "2",and so on, use Business Attributes, specified by the toast.case-data.format-business-attribute.

As this option can be overwritten by a routing strategy, if the Callback business process is able to assign to the notification UserEvent a Key-Value Pair that points at a Transaction object name, this can provide even more flexibility.

The localization model of Configuration Objects can also be used to transform the display name of the configured Business Attribute Values into labels in the language of the logged in agent.

To make callback Key-Value pairs ready to be displayed in the case data of the interaction notification and the interaction view, you should configure the corresponding GMS Service by setting the value of the _attach_udata option to separate_keys. Next, you can configure Case Data to show these as any regular interaction key-value pair.

## Configuring callback availability

- Opening hours configured in solution.
- Not available: slot capacity full

# Workitems

Workitems are custom media types or tasks that are processed by the intelligent Workload Distribution (iWD) solution. iWD is an application that works with the Genesys Customer Interaction Management (CIM) Platform to distribute tasks to the resources that are best suited to handle them. It is a collection of software components for:

- Capturing tasks from various enterprise work sources.
- Applying business rules to classify, prioritize, and reprioritize the tasks.
- Routing the tasks to agents or knowledge workers in the enterprise.
- Monitoring and reporting on the intraday and historical status of the tasks and the task handling.

Refer to the *intelligent Workload Distribution Deployment Guide* for more information.

You must define workitems in Configuration Server (refer to *Genesys Administrator Extension Help* and the *eServices (Multimedia) documentation* for information about defining Business Attributes (Media Type) in Configuration Server).

Workspace employs the following privileges for all Workitem interactions:

- Can Use WorkItem Channel
- Can One Step Transfer
- Can Set Interaction Disposition

You use the following options in the `interaction-workspace` section to configure Workitem interactions:

- intercommunication.<media-type>.queue: Specifies the name of the queue to be used by the Routing Base feature. The following attached data are added by Workspace:

```
IW_RoutingBasedOriginalEmployeeId, IW_RoutingBasedTargetId,
IW_RoutingBasedTargetType, IW_RoutingBasedActionType.
```

- intercommunication.<media-type>.routing-based-targets: Specifies the list of targets (`Agent` and/or `Queue`) that are contacted through the routing-based mechanism, for the requests that are defined in the intercommunication.<media-type>.routing-based-actions option. The `AgentGroup` and `Skill` targets are always addressed by routing; therefore, they are not affected by this option.
- login.<media-type>.can-unactivate-channel: Specifies whether an agent is allowed to select and unselect (activate and deactivate) a workitem channel during login, for example: `login.myworkitem.can-unactivate-channel=true`
- login.<media-type>.is-auto-ready: Specifies whether the Workitem channel is in the `auto-ready` state at agent login.
- openmedia.workitem-channels: Specifies a list of Workitem channels that an agent can be enabled to use, for example: `openmedia.workitem-channels=myworkitem`
- <media-type>.auto-answer: Specifies whether a Workitem interaction is accepted automatically when an `Invite` event is received from Interaction Server. This option can be overridden by a routing

strategy. You can also configure auto-answer to display a timer that enables an agent to view case information before the interaction is automatically answered by using the <media-type>.auto-answer.timer and <media-type>.auto-answer.enable-reject options (**Added:** 8.5.105.12).

## Provisioning the Workitems feature

### Procedure

Enabling an agent to use Workitems to handle custom media types

**Purpose:**

To enable an agent to use custom media types as Workitem interactions.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to Universal Contact Server (optional, depending on the workitem type).
- Workspace has a connection to Interaction Server.
- The Procedure: Enabling agents to manage contacts.

**Start**

1. In Genesys Administrator Extension, add the Workitem media in the `Media Type` Business Attribute. (refer to *Genesys Administrator Extension Help* and *Genesys Administrator Extension Deployment Guide* for information about defining Business Attributes in Configuration Server ).
2. Update the capacity rules for the Workitem (refer to *Genesys 8 Resource Capacity Planning Guide*).
3. Allow the Workitem privileges (see Workitem Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group).
   - Can Use Workbins
   - Can One Step Transfer
4. Configure the Workitem options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Workitem configuration option reference for a list of Workitem options and a description of how to configure them).

> Tip
>
> For information about configuring Load Balancing and Business Continuity, refer to Runtime Connection Logic in the eServices Load Balancing Business Continuity section of the *Business Continuity and Disaster Recovery* topic. **Added:** 8.5.109.16

5. Configure the options that support Workitems (refer to Workitems).

**End**

## Workitem Can Mark Done privilege

The Can Mark Done privilege controls how workitems are marked as done.

When this privilege is allowed, the Done button is displayed in the toolbar when an inbound workitem is presented. If an agent clicks Done, the inbound workitem is terminated (removed from the Business Process). It will then not be possible to submit any corresponding outbound reply from the interaction view. It can only be reopened from the Contact History.

When this privilege is not allowed, the Done button is not displayed when an inbound workitem is displayed. The agent must handle the workitem by replying to it, transferring it, or placing it in a workbin.

## Open In-progress Workitems from History

You can enable agents to open a workitem of a specified media type that is in progress and in a workbin or a queue and is not assigned to any agent that is listed in the contact history for that interaction. This feature enables an agent to immediately work on the workitem before it is assigned. This feature is useful for an agent who is interacting with a contact on another media channel.

To enable this feature, for the agent, agent group, or application object, allow the following privileges and set the value of the <media-type>.pull-from-history-isenabled option to true:

- Contact - Can Pull From Queue
- Contact - Can Pull Interactions In Shared Workbins
- Contact - Can Pull Interactions In Workbins Not Owned By The User

# Setting up agents to use workbins

[**Modified:** 8.5.110.13, 8.5.122.08, 8.5.126.07]

## Procedure

### Enabling an agent to use and search agent, place, agent group, or place group workbins

**Purpose:**

To enable an agent to use agent, place, agent group, or place group workbins to receive and/or store contact interactions for future processing.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to Universal Contact Server and Interaction Server.
- The Procedure: Enabling agents to manage contacts.

**Start**

1. Use Genesys Interaction Routing Designer (IRD) or Genesys Composer to create a workbin.
2. In Genesys Administrator Extension, create a reference to the workbin in the Workspace `Application` object, following the generic rule: `workbin.<media-type>.<workbin-nick-name>=<workbin-script-name>`
   Refer to the Section: interaction-workspace and workbin configuration option reference for a list of Workbin options and a description of how to configure them.
3. Allow the workbin privileges (see Workbin Access Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group).
   - Workbin - Can Use Workbins
4. To enable agents to use Interaction Search in workbins, allow the following privilege on the agent, role, agent group, or other User object: [**Added:** 8.5.110.13]
   - Workbin - Can search in Workbins

Interaction Queue Search Privilege.

5. To specify how the workbin content is displayed and updated, use the following configuration options: [**Added:** 8.5.110.13]

   - workbin.<media-type>.<workbin-nickname>.auto-update: Specifies whether the list of interactions in a workbin is updated automatically or manually by the agent. When set to `true`, Workspace registers for workbin notifications from Interaction Server so that the workbin content is always up to date. When set to `false`, the content of the workbin is refreshed only when the user explicitly requests it by selecting the workbin in the selection pane or by clicking the **Refresh** button. When set to `false`, the maximum size of the displayed workbin content is defined by the value of the workbin.<media-type>.<workbin-nickname>.max-results option, if Interaction Server 8.5.104.00 or higher is used, or by the value of the Interaction Server `max-workbin-interactions` option with lower releases.
   - workbin.<media-type>.<workbin-nickname>.max-results: Specifies the maximum number of interactions to display in a workbin. This option requires Interaction Server 8.5.104.00 or higher.

6. To specify how the workbin search feature works, use the following configuration options: [**Added:** 8.5.110.13]

   - workbin.<media-type>.<workbin-nickname>.quick-search-attributes: Specifies the list of interaction attributes that are used when applying a quick search in this workbin. The query is built to match any attributes that start with the criteria specified by the agent. This option requires Interaction Server 8.5.104.00 or higher. The maximum size of the result set is defined by the workbin.<media-type>.<workbin-nickname>.max-results option. Once a search result set is displayed, the auto-update no longer applies until the search criteria are cleared. Refer to Specifying Filter Conditions. If this option is not configured, or if the value is left blank, then the Search field is not displayed.

7. To enable agent notification of changes to interaction properties in a workbin, set the value of the workbin.<media-type>.<nick-name>.notify-property-changed to `true`. [**Added:** 8.5.122.08]

8. You can choose to sort custom columns numerically or chronologically instead of alpha-numerically. By default, custom columns that are included in a workbin that has been provisioned for `auto-update` are sorted in alpha-numeric order. To specify that the custom column sorting should be in numerical or date order, you must configure the Business Attribute Value representing this custom column in the 'Interaction Custom Properties' Business Attribute as follows:

   a. Create a section named `interaction-workspace`.

   b. In this section, create the `display-type` key and set the value to `int` (for numerical order) or `date` (for chronological order).

> Tip
>
> When a workbin is not provisioned as 'auto-update', sorting is handled by the Interaction Server database, and so relies on the type assigned in the database table schema.

[**Added:** 8.5.126.07]

**End**

# Instant Messaging

[**Modified:** 8.5.122.08]

You use the following options in the `interaction-workspace` section to configure the channel to handle IM interactions:

- im.simple-transcript: Specifies whether the IM transcript is displayed as simple lines of text or as colored blocks of text. [**Added:** 8.5.122.08]

> ## Warning
>
> If you grant an agent voice capabilities and Instant Messaging (IM) capabilities on two different DNs, the agent does not get Outbound Campaign notifications and experiences other issue when handling Outbound Campaign interactions.
>
> **Workaround**: Configure the **Log On As Person** feature of the Outbound Contact Server so that it does not "see" the IM DNs that are configured in the Places of the agent.

## Procedure

### Enabling agents to use Instant Messaging

**Purpose:**

To enable an agent to use Instant Messaging (IM) to send and receive text messages with an internal target.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to SIP Server.

**Start**

1. Allow the Team Communicator privileges (see Team Communicator Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group).
2. Configure the Team Communicator options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Team Communicator configuration option reference for a list of Team Communicator options and a description of how to configure them).
3. Allow the following IM privileges for the role to which the agent is assigned:

- Can Release IM
- Can Make IM
- Can Use IM

4. Configure the IM options in the `interaction-workspace` section of the Workspace `Application` object (refer to the IM configuration option reference for a list of IM options and a description of how to configure them).
5. Ensure that the SIP DN of the Place used for Instant Messaging has the following options defined in the `TServer` section:
    - `sip-signaling-chat` = `none`
    - `multimedia` = `true`
    - `voice` =
        - `false`: The DN will handle only IM
        - `true`: The DN will handle IM and voice
        - `""`: Option not set (Default = true; therefore, the DN will handle IM and voice)

> ### Important
>
> - The DN that holds the IM channel does not support the **ACDPosition** type. It must be of type **Extension**.
> - If the `voice` key is not included in the `Tserver` Section, the DN handles both IM and voice.

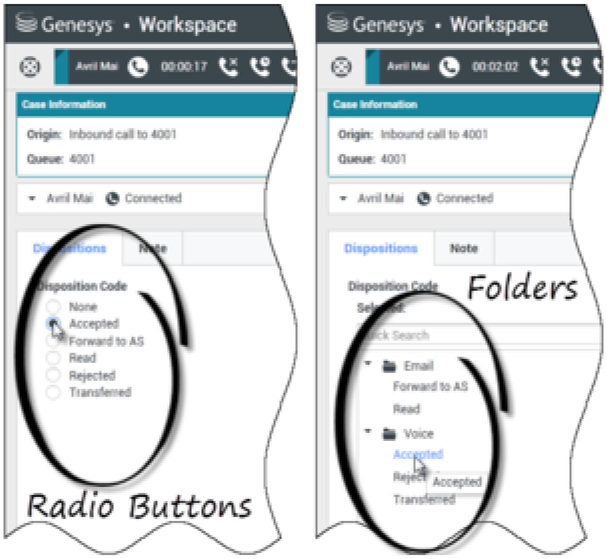
**End**

# Disposition codes

[**Modified:** 8.5.108.11, 8.5.141.04]

The Disposition Code feature enables agents to specify outcomes for interactions that they are handling. Disposition Codes are handled as Business Attributes in Genesys Framework. The interaction disposition is part of the attached data for the interaction.

Workspace supports two different views of the disposition codes that you specify as Business Attributes, as a hierarchical folder tree with a search control or as a radio button list.



The folder tree hierarchy and the radio button list

Agents select an item from the tree or click a radio button to specify the disposition of an interaction. This disposition become part of the attached data of the interaction.

> **Important**
>
> The **Dispositions** tab and the **Note** do not become available until the call is established.

## Procedure

### Enabling an agent to use disposition codes

> **Tip**
>
> If you are creating disposition codes to report on a business result, for example to provide data for Genesys Info Mart (GIM) and Genesys Interactive Insights, configure the Disposition Code Business Attribute as a "Business Result". To use this feature, specify the name of the "Business Result" Business Attribute as the value of the interaction.disposition.key-name option.
> GIM supports reporting on Business Result out-of-box, provided that ICON has been configured to send the Business Result KVP. The GIM IP includes a customized ICON attached-data specification file that provides this configuration (refer to Sample ICON Attached Data Specification).
> For more information about how Genesys Info Mart handles user data (such as Business Result) that is attached to interactions, refer to the User Data Mapping topic in the *Genesys Info Mart Deployment Guide*. This topic has links to additional information in the GIM Deployment Guide and PDMs.
> The Mapping User Data Worksheet topic might also help you when setting up your business results. Search for "business result" on this page.

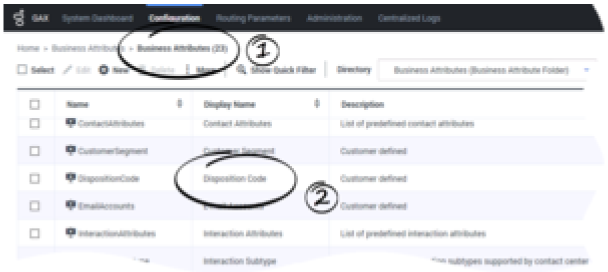
**Purpose:**

To enable an agent to specify the outcome (disposition) of an interaction.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- The Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group
- The Procedure: Provisioning Workspace for the Voice channel

**Start**

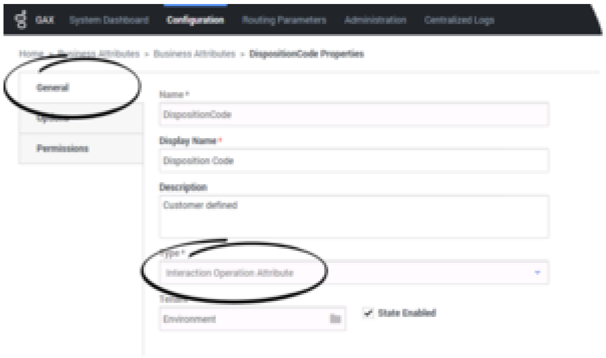
1. Start Genesys Administrator Extension
2. Select your tenant.
3. Open Routing/eServices in the Navigation area.
4. Select **Business Attributes**.
5. Create or update the **Disposition Code** Business Attribute. Alternately, you can create a different Business Attribute and specify it by using the interaction.disposition.value-business-attribute configuration option.



| Name | Display Name | Description |
|---|---|---|
| ContactAttributes | Contact Attributes | List of predefined contact attributes |
| CustomerSegment | Customer Segment | Customer defined |
| DispositionCode | Disposition Code | Customer defined |
| EmailAccounts | Email Accounts | Customer defined |
| InteractionAttributes | Interaction Attributes | List of predefined interaction attributes |
| | Interaction Subtype | subtypes supported by contact center |

Create or modify the Disposition Code object in the Business Attributes area

- The Type of the Business Attribute is `Interaction Operation Attributes`.
- The `Display Name` of the Business Attribute is used as the name of the section in the Agent interface.



Name *
DispositionCode

Display Name *
Disposition Code

Description
Customer defined

Type *
Interaction Operation Attribute

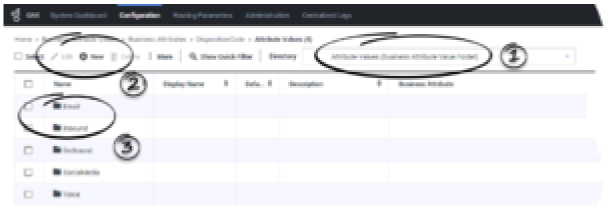
Tenant
Environment

☑ State Enabled

Create or modify the Disposition Code Business Attribute or other Business Attribute to be used for disposition codes

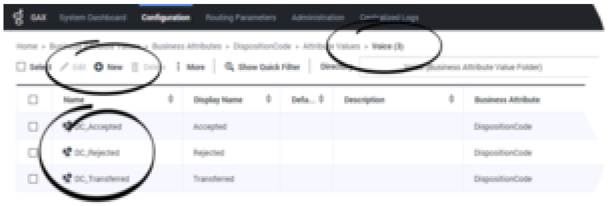
6. Click the **Attributes Values** tab to open it.

   If you want to create a hierarchical structure with different dispostions organized by folders into a tree in the agent interface, click **New Folder**. In the **Folder name** dialog box, enter a folder name and click **OK**. Create as many folders as you need. You can nest folders inside other folders to make a complex folder tree structure.



You can optionally create folders in the Dispostion Code Business Attribute to organize disposition codes

7. Create one or more Attribute Values.

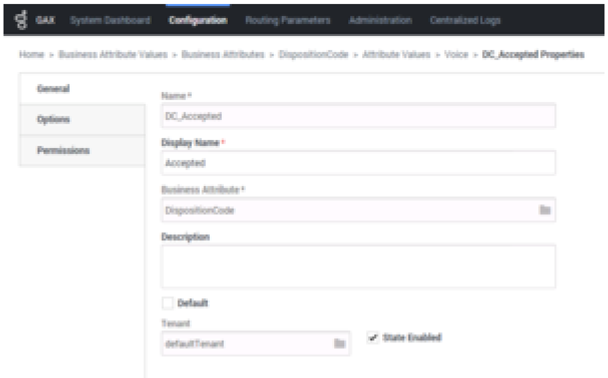

GAX
System Dashboard
Configuration
Routing Parameters
Administration
Centralized Logs
Home › Business Attribute Values › Business Attributes › DispositionCode › Attribute Values › Voice (3)
Select
Edit
New
Delete
More
Show Quick Filter
Directory
(Business Attribute Value Folder)

| Name | Display Name | Defa... | Description | Business Attribute |
|---|---|---|---|---|
| DC_Accepted | Accepted | | | DispositionCode |
| DC_Rejected | Rejected | | | DispositionCode |
| DC_Transferred | Transferred | | | DispositionCode |

You can create multiple Attribute Values in the **Attribute Values** tab

To create an Attribute Value, click **New** to open the Attribute Values Configuration view and specify the following for each disposition code:

- Name—Used in attached data
- `Display Name`—Used in the Agent interface
- `Enabled`—Used to make the attribute active


GAX
System Dashboard
Configuration
Routing Parameters
Administration
Centralized Logs
Home › Business Attribute Values › Business Attributes › DispositionCode › Attribute Values › Voice › DC_Accepted Properties
General
Options
Permissions

Name *: DC_Accepted

Display Name *: Accepted

Business Attribute *: DispositionCode

Description:

□ Default

Tenant: defaultTenant

☑ State Enabled

Specify a name and display name for each disposition code that you create

8. For the object to which the set of disposition codes apply, in the `interaction-workspace` section, set the value of the interaction.disposition.value-business-attribute option to the name of the business attribute that you configured.
9. Allow the `Can Set Interaction Disposition` privilege (see Role Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group):
    - Chat Privileges
    - Email Privileges
    - SMS Privileges
    - Voice Privileges
    - Web Callback Privileges
    - Workitem Privileges
10. For the object to which the set of disposition codes apply, configure the following Interaction options in the `interaction-workspace` section (refer to the Interaction configuration option reference for a list of Interaction options and a description of how to configure them):
    - interaction.disposition.is-mandatory

- interaction.disposition.email.mandatory-actions [**Added:** 8.5.103.10]
- interaction.disposition.<media-type>.mandatory-actions [**Added:** 8.5.150.06]
- interaction.disposition.is-read-only-on-idle
- interaction.disposition.key-name
- interaction.disposition.use-attached-data
- interaction.disposition.use-connection-id
- interaction.disposition.value-business-attribute

Optionally, if you want to display disposition codes in the legacy radio button interface, set the value of the interaction.disposition.display-mode option to `radio-buttons`.

11. To pre-load Business Attribute objects, such as Disposition Codes, when an agent logs in, configure the value of the general.configuration-business-attribute-cache-preload option with a list of Business Attributes to pre-load. Business Attributes and Transaction objects are otherwise loaded the first time that an interaction requiring them is received by an agent. They are then cached for future use. If there are a large number of possible attribute values, such as a large list of dispositions, there could be a delay in the display of the Interaction Notification while the dispositions load. Pre-loading Buiness Attributes related to disposition and case data when an agent logs in ensures that there is no delay in displaying Interaction Notifications.

    For dispositions that employ the folder/tree structure, you can choose to pre-load the folder structure when a agent logs in by using the general.configuration-business-attribute-folder-cache-preload option to specify the list of Business Attributes containing the folders that you want to pre-load.

    > ## Important
    >
    > You must specify the Business Attributes containing folders in both the general.configuration-business-attribute-folder-cache-preload and general.configuration-business-attribute-cache-preload options for the Business Attributes containing folders to be pre-loaded.

    [**Added:** 8.5.141.04]

**End**

# Contact History

[**Modified:** 8.5.104.15]

For information about Contact Management and search, refer to the Managing Contacts topic.

## Procedure

### Enabling agents to manage and search contact and interaction history

**Purpose:**

To enable an agent to view, search, and update the history of a contact.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to Universal Contact Server.
- The Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group.
- Enable one or more channels:
  - Provisioning Workspace for the Voice channel.
  - E-Mail, Chat, and/or SMS

**Start**

1. Allow the following Contact Actions privileges (see Contact Management Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group):
   - Can Use Contact Directory
   - Can Use Contact History
   - Can Use Interaction Search[**Added:** 8.5.104.15]
   - Can Use Contact History CaseData
   - Can Use Contact History Detail
   - Can Use Contact History Notepad
   - Can Use Contact Information
   - Can Use Contact my History
   - Can Use Save Contact

- Contact Module

2. Configure the Contact options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Contact configuration option reference for a list of Contact options and a description of how to configure them).
3. Enable UCS contact index to permit contact search in list views and Team Communicator, and enable UCS interaction index to permit searches on contact interactions in Contact History, My History, and Global Interaction Search views. For more information about enabling UCS index refer to the *eServices (Multimedia) 8.0 User's Guide*.
4. (Optional) Configure Global Interaction Search.

**End**

# Case Information editing

For a discussion of Case Information refer to the **Case** tab of the Handling Interactions topic. Case related configuration options are listed here. Case data privileges are discussed here.

## Procedure

### Configuring the Workspace application to enable an agent to edit case information

**Purpose:**

To enable an agent to edit the contents of case information.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- One or more custom Case Information Business Attributes in the Configuration Layer.

**Start**

1. In Genesys Administrator Extension, open a Case Information Business Attribute.
2. In the Attributes Values tab, open an attribute value.
3. Select the Options tab.
4. Add a new section named `interaction-workspace`.
5. Configure the option according to the values in the table **Editing Case Information** in the **Case** tab of the Handling Interactions topic.
6. Save your updates.

**End**

# Standard Responses

[**Modified:** 8.5.112.08, 8.5.118.10]

## Procedure

### Enabling agents to use the Standard Responses Library (SRL)

**Purpose:**

To enable an agent to access the Universal Contact Server database of prewritten standard responses for interactions.

Agents can insert these responses as replies into any email, instant messaging, or chat message, or they can read them to the contact during a voice interaction.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to Universal Contact Server.
- The Procedure: Creating a Role and allowing an Workspace privilege and assigning a Role to an agent or agent group.
- (Optional) The Procedure: Provisioning Workspace for the Voice channel.
- (Optional) The Procedure: Enabling an agent to use E-Mail to correspond with a contact.
- (Optional) The Procedure: Enabling an agent to use Chat to chat with a contact.

**Start**

1. For information about creating and managing Standard Responses and standard response field codes, refer to Knowledge Manager.
2. Allow the following SRL privileges (see Standard Response Privileges) for the role to which the agent is assigned (refer to the Creating a Role and allowing an Workspace privilege and assigning a Role to an agent or agent group):
   - Can Use SRL
3. Enable an index search on SRL in the Universal Contact Server configuration.
   - Set the `index\enabled` option to `true`.
   - Set the `index.srl\enabled` option to `true`.

   For more details about these settings, refer to the *eServices (Multimedia) 8.0 User's Guide*.

4. Configure the relevancy level for Suggested Responses:
   - Set the standard-response.suggested-responses-min-relevancy option to display responses in order according to their relevancy to the inbound interaction.
5. Configure the other Standard Response options to meet the requirements of your environment.
6. (Optional) Create custom field codes for agents, agent groups, tenants, or at the application level that can be used by Standard Response objects. Use the standard-response.field.<CustomFieldCode> option to specify a custom field code and value, such as an agent nickname, role, department, or other qualification, and then insert the field code into a Standard Response object.

   For example, you could create a set of field codes for a Standard Response for an agent signature such as the following:

   ```
   Name: "Signature"
    Text: "<$ Agent.Title $> <$ Agent.FullName $> (< $Agent.NickName$ >) - <$ Agent.Position
    $>
    <$ Department $>"
   ```

   In the Agent annex configure `standard-response.field.<[Agent.]CustomFieldCode>`:

   - `'interaction-workspace'/'standard-response.field.Agent.Title' = "Ms"`
   - `'interaction-workspace'/'standard-response.field.Agent.NickName' = "Beth"`
   - `'interaction-workspace'/'standard-response.field.Agent.Position' = "Technical Support Analyst"`

   In the Agent Group annex (in Configuration Server):

   - `'interaction-workspace'/'standard-response.field.Department' = "Customer Care"`
7. (Optional) Create shortcut keywords that agents can enter into the email, chat, SMS, and MMS composition areas to automatically add common Standard Responses. [**Added:** 8.5.118.10]
   a. Specify the prefix character that agents must type before entering the keyword by configuring the editor.shortcuts.prefix option. Workspace detects the prefix/keyword combination as a shortcut if the agent immediately types Ctrl+Space after typing the prefix character followed by the keyword. For example, if you have a standard response about a new sale and you create a keyword called `sale` and you specify # as the prefix, the agent would type `#sale` followed by Ctrl+Space to automatically populate the email interaction with the content of the sale Standard Response.
   b. For each shortcut that you want to create, add the standard-response.shortcuts.<keyword> option to the `interaction-workspace` of the configuration object for which you want to enable the shortcut. In the name of the configuration option, replace <keyword> with the name of the shortcut keyword. For example, if the keyword that you want your agent to type is `#sale`, add the following option:

      ```
      standard-response.shortcuts.sale
      ```

      Then, set the value of the option to the path to the response. For example: `Agent Responses\Latest Promotions`.

**End**

# Broadcast Messages

Workspace enables agents to receive messages that are sent simultaneously (broadcast) to multiple contact center parties. You must use an application that can publish messages, associated by topic, to a common communication DN. Workspace employs a simple protocol based on communication DN and provisioning to enable this functionality.

Agents can be provisioned to receive messages that are addressed, by topic, to a property of the agent or a property of an agent group (see the Procedure: Enabling agents to view Broadcast Messages).

Messages are displayed to agents by an Interactive Notification that is similar to the new interaction Interactive Notification. An audio alert can be configured to alert agents when a new broadcast message arrives. Messages are also displayed in the Workspace Main Window as a summary table in the `Messages` drop-down area. If the agent opens the message, a detailed view is displayed. If the agent uses the Gadget view, messages are displayed in a message gadget.

## Attributes

A broadcast protocol message is defined by the following attributes:

- `Message`: The content of the message.
- `Sender`: The identity of the sender.
- `Message Type`: The type of message, such as Error, Information, Notification, and so on.
- `Subject`: The subject of the message (optional).
- `Priority`: The relative importance of the broadcast message. The following subcategories are predefined; however, you can also configure your own values:
  - `Minimal`
  - `Low`
  - `Normal`
  - `High`
  - `Important`
- `Date`: The date sent, in local time of the agent.
- `Topic`: To which topic the message was sent.
- `Custom Data`: Any custom data included with the message.

## Protocol

Use the following protocol on your supervisor client configuration:

```
IWS_Message
IWS_Sender
IWS_MessageType
```

```
IWS_Subject
IWS_Priority
IWS_Date (RFC1123 pattern.)
IWS_Topic
IWS_CustomData
```

The following is an example of a `UserEvent` configuration:

```
Event:EventUserEvent
 Server:65200
 ReferenceID:7
 CustomerID:Resources
 ThisDN:BroadcastDN
 UserData:
 (Str) IWS_Subject Coffee Break
 (Int) IWS_Priority 3
 (Str) IWS_Message Please take your coffee break NOW !!!
 (Str) IWS_Date Thu, 11 Feb 2010 16:15:16 GMT
 (Str) IWS_Topic Agent4
 (Str) IWS_Sender Ministrator
 (Str) IWS_MessageType Error
 Seconds:1265904964
 USeconds:234000
 Server Time:11/02/2010@17:16:04.234
```

## Configuration options

You can use the following options in the `interaction-workspace` section to configure Broadcast Messaging:

- `broadcast.color.xxx-priority`: Specifies the Hexidecimal-color code of the border of the Message view frames for messages that have the xxx priority. The following priorities are supported:
  - broadcast.color.high-priority
  - broadcast.color.important-priority
  - broadcast.color.low-priority
  - broadcast.color.minimal-priority
  - broadcast.color.normal-priority
- `broadcast.displayed-columns`: Specifies the attribute columns that are displayed in the Broadcast Message window and the item tooltip in the My Messages tab/window.
- `broadcast.dn`: The name of the DN and switch that is used for broadcasting. Use the following value format: `DN@switch`
- `broadcast.mark-read-timeout`: Specifies the duration after which a message, as a tooltip, is considered to be read.
- `broadcast.message-content`: Specifies the attributes that are displayed in the Broadcast Message window and the item tooltip in the My Messages tab/window.
- `broadcast.preview-timeout`: Specifies the duration after which a message preview is closed.
- `broadcast.sound.xxx-priority`: Specifies the sound configuration string for messages that have priority xxx. The following priorities are supported:
  - broadcast.sound.high-priority

    - broadcast.sound.important-priority
    - broadcast.sound.low-priority
    - broadcast.sound.minimal-priority
    - broadcast.sound.normal-priority
- `broadcast.subscribed.topics`: Specifies the list of subscription topics.
- `broadcast.toast-summary`: Specifies the attributes that are displayed in the Interactive Notification.
- `broadcast.value-business-attribute`: Specifies the name of the Business Attribute that contains the Attribute Values that are used as an enumerated value for a custom attribute of message.

Message types can be customized by adding the following lines to the `Genesyslab.Desktop.Modules.Windows.en-US.xml` dictionary file:

```
<Value Id="Broadcast.MessageType.System" String="System"/>
<Value Id="Broadcast.MessageType.Error" String="Error"/>
<Value Id="Broadcast.MessageType.Information" String="Information"/>
<Value Id="Broadcast.MessageType.Internal Note" String="Internal Note"/>
```

The value that is set in the `String` property is displayed as the message type.

# Provisioning Broadcast Messages

## Procedure

### Enabling agents to view Broadcast Messages

**Purpose:**

To enable an agent to receive and view messages that are sent simultaneously (broadcast) to multiple contact center parties.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- The Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group.

**Start**

1. Allow the following Broadcast Message privilege (see Broadcast Privileges) for the role to which the agent is assigned (refer to the Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group):
    - Can Use Broadcast Message

2. Create a communication DN and configure it in `broadcast.dn`.
3. Configure the broadcast message topics to which an agent can be subscribed by using `broadcast.subscribed.topics`.
   Topics can be associated with different configuration objects such as agents (`$Agent$`) and agent groups (`$AgentGroup$`); or they can be the names of custom topics such as team (for example, `billing`) or site (for example `main_campus`).
4. Ensure that you have a Sender application that implements the protocol described in Protocol, above, that sends messages to topics that match what is configured in your system.

**End**

# Team Leads and Supervisors

[**Modified:** 8.5.126.07]

For details on the capabilities of Team Leads and Supervisors in Workspace, refer to these topics:

- Team Lead Help
- Team Lead Functionality

## Enabling agents to be Team Leads and Supervisors

### Procedure

Enabling agents to be Team Leads and Supervisors

**Purpose:**

To enable an agent who is configured to be a supervisor (Team Lead) to automatically monitor the SIP Voice and Chat interactions that are handled by other agents.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- The Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group.

**Start**

1. Allow the following Team Lead privilege (see Team Lead Privileges) for one of the roles to which the users who will be Team Leads are members:
   - Can Use Team Lead
2. Allow the following optional Team Lead privileges (see Team Lead Privileges) for the role to which the agents who will be Team Leads are members:
   - Can Auto-Monitor (Voice or Chat)
   - Can Switch to Barge-in (Voice or Chat)
   - Can Switch to Coaching (Voice or Chat)
   - Can Switch to Silent Monitoring (Voice or Chat)
   - Can End Monitoring (Voice or Chat)

3. Configure the Team Lead options.
4. Create or select an agent group to be used to specify the list of Agents that a Team Lead will monitor.
5. Add the agents to be monitored by that team lead to that agent group.
6. In Genesys Administrator Extension `Configuration` tab for the agent group, open the `Advanced` view.
7. In the `Supervisor` field, add the name of the user that will be acting as Team Lead for that agent group.
8. Save the changes to the Agent Group object.

**End**

## Enabling Team Leads and Supervisors to log off or change agent state

[**Added:** 8.5.126.07]

You can enable your supervisors/team leads to manually change an agent's state or log off an agent by using the Team Communicator. If a supervisor discovers that an agent is in the wrong state, he or she can use Team Communicator to select the agent, and then use the **Action** menu to set an agent to **Ready** or **Not Ready** (Not Ready Reasons options are not supported) on all channels or on specific channels. If a supervisor discovers that an agent has left their account logged on after their shift, he or she can use Team Communicator to select the agent, and then use the **Action** menu to log off the agent on all channels; this ability benefits the company in two ways: it ensures that seat licenses are not unnecessarily consumed, and interactions are prevented from being routed to an agent who is not present but is configured for auto-answer!

To enable the agent state control feature, grant the 'Team Lead - Agent Status Enabled Remote Actions' privilege, then configure the following Application option in the `interaction-workspace` section of a Tenant, Group, or User object:

- teamlead.agent-status.enabled-remote-actions

> ### Important
>
> When you are setting up supervisors/team leads with the remote actions, the following behaviors occur with this feature:
>
> - If an agent has set their status to **After Call Work**, **Not Ready <with the reason>**, or **Do Not Disturb**, these are displayed in Team Communicator as **Not Ready**.
> - Since Team Communicator does not support these statuses, you cannot set an agent status from **Ready** to **After Call Work**, **Not Ready <with the reason>**, or **Do Not Disturb**; you can only set the status to **Not Ready** from **Ready**.

## Warning

Team leads might experience unexpected behavior if they change the state of a particular eService channel from **Do Not Disturb**, to **Ready** for an agent who is assigned two or more eServices channels. Setting **Ready** on one eServices channel restores all other eServices channels to the status prior to **Do Not Disturb**.

# Call recording and screen recording

[**Modified:** 8.5.104.15, 8.5.106.19, 8.5.116.10, 8.5.118.10, 8.5.143.08]

Workspace supports call recording and screen capture. Conversations and screen image files are stored as a set of files in a centralized storage location. Agents can control and monitor this feature.

## Call recording

SIP Server supports call recording using two different methods: NETANN-based call recording, provided by Stream Manager or Genesys Media Server; and Media Server Markup Language (MSML)-based call recording, provided by Genesys Voice Platform (GVP) Genesys Media Server only.

### MSML-based call recording

Refer to the Genesys Quality Management 8.1 documentation.

MSML-based Call Recording enables agents to do the following:

- Control Active Call Recording (start, stop, pause, and resume)
- Display the status of Call Recording

MSML-based Call Recording functionality is enabled by the following privileges:

- Voice - Can Use
- Recording - MSML-based Recording - Can Use
- Recording - Can Control Voice Recording (optional)
- Recording - Can Monitor Voice Recording (optional)

Set the active-recording.voice.recording-type option in the `interaction-workspace` section to `MSML`.

### Legacy NETANN-based call recording

NETANN-based Call Recording enables agents to do the following:

- Control Call Recording (start and stop)

NETANN-based Call Recording functionality is enabled by the following privileges:

- Voice - Can Use
- Recording - Can Control Voice Recording (optional)

Set the active-recording.voice.recording-type option in the `interaction-workspace` section to

NETANN (the default value).

Display of Call Recording status is not possible with NETANN-based Call Recording.

## Screen recording

[**Added:** 8.5.106.19] [**Modified:** 8.5.116.10, 8.5.118.10, 8.5.143.08]

This functionality is supported for Genesys Interaction Recording (GIR) customers. You must have a login provided by Genesys to access the Genesys Interaction Recording documentation.

Screen Recording allows the recording of the full workstation screen of the agent during a voice call or an eServices login session. The video stream is recorded on a server by the GIR Screen Recording Service.

Screen Recording functionality is enabled by the following Privileges:

- Recording - Can Use MSML-based and Screen Recording
- Recording - Can Use Screen Recording

Use the following options to configure the behavior of Screen Recording:

- screen-recording.client.address: Specifies the IP address or host of the Screen Recording Service. If left blank, the connection to the Screen Recording Service is established on the localhost, according the IP version specified at the system level. [**Added:** 8.5.143.08]
- screen-recording.client.port: Specifies the port on which Screen Recording Service listens for credentials. The value of this option should be set to 443.
- screen-recording.client.ping-interval: Specifies the interval in milliseconds between two keep-alive requests to Screen Recording Service.
- screen-recording.client.max-attempts: Specifies the maximum number of attempts to establish communication with Screen Recording Service when Workspace is initialized before the Screen Recording Service is considered inactive.
- screen-recording.client.secure-connection: Specifies whether secure connection should be used for the communication between Workspace and Screen Recording Service. The value of this option should be set to `True`.
- screen-recording.htcc.uri: Specifies the URI representing the HTTP/HTTPS access to Genesys Interaction Recording Web Services (or Genesys Web Services for older versions of the Genesys Interaction Recording solutions). For example: http://server.domain:443.

> ### Tip
>
> When you are setting up GIR in a SIP Server environment, Genesys recommends that you set the value of the `enable-agentlogin-presence` option to `false`. For more information, see the **Deploying SIP Server for GIR** topic in the *Genesys Interaction Recording Solution Guide*.

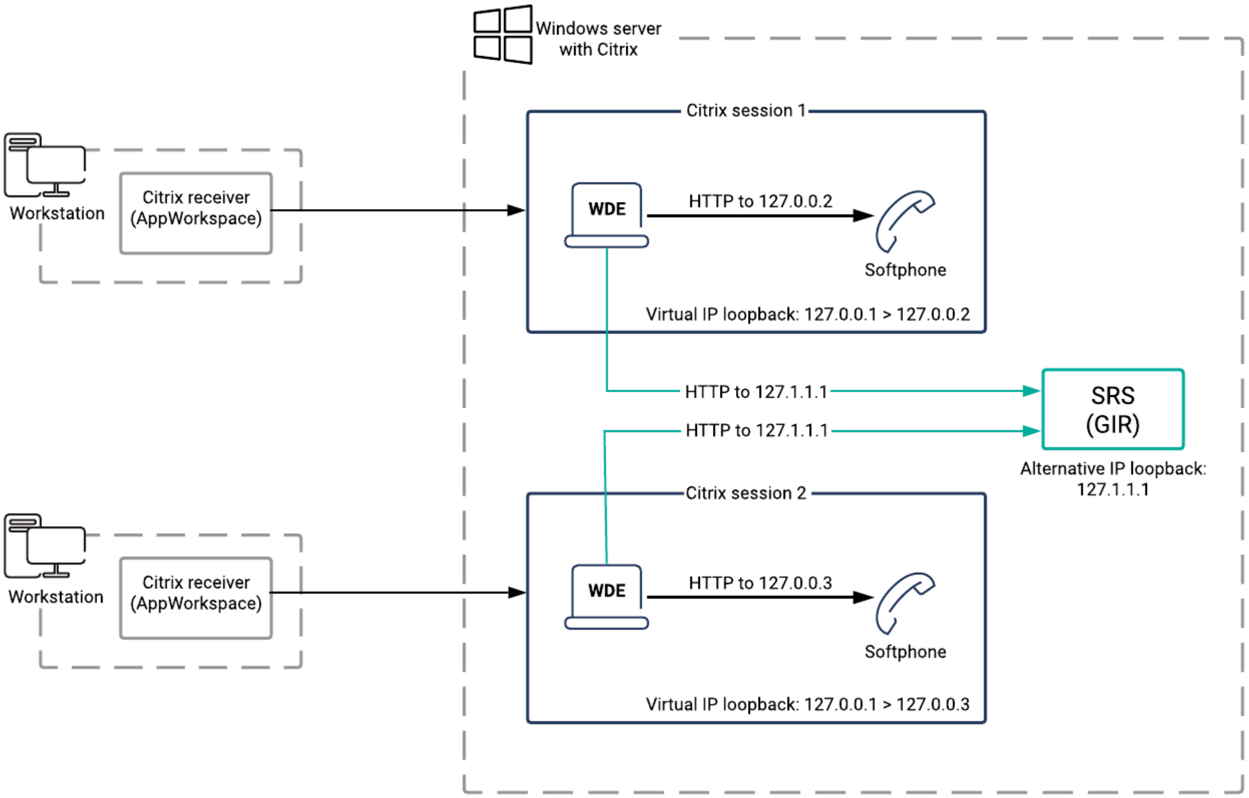
## Screen recording in a Genesys Softphone VDI environment

[**Added:** 8.5.143.08]

In environments where Workspace, Genesys Softphone, and Screen Recording Service (SRS) are deployed in a VDI environment, such as Citrix Xenapp or XenDesktop, Workspace and Genesys Softphone run in each Citrix user session of the Windows Server while SRS is installed as a unique service instance on the Windows Server. In this architecture, Workspace and Genesys Softphone communicate through the Citrix Virtual IP Loopback, while SRS accepts connections on an alternative Loopback IP address. To specify the address of the SRS, set the value of the screen-recording.client.address option to the alternative Loopback IP Address configured during SRS installation, such as `127.1.1.1`.

> ### Important
> The minimum SRS version to support this feature is 8.5.370.85

The following architectural diagram shows how Workspace running in multiple VDI sessions connects directly to the SRS while the Genesys Softphone connection remains on the regular loopback affected by Virtual IP Loopback. The SRS uses the explicitly configured alternative IP Loopback.



## Screen recording Disaster Recovery

[**Added:** 8.5.118.10]

Disaster Recovery is supported for Screen Recording. To enable this feature, you must have two clusters of Interaction Recording Web Services servers. You must configure both the screen-recording.htcc.uri and screen-recording.htcc.peer_uri options to point at those 2 clusters.

- screen-recording.htcc.uri: Specifies the URI representing the HTTP/HTTPS access to Genesys Interaction Recording Web Services (or Genesys Web Services for older versions of the Genesys Interaction Recording solutions). For example: http://server.domain:443.
- screen-recording.htcc.peer_uri: Specifies the URI representing the HTTP/HTTPS access to the Genesys Interaction Recording Web Services (or Genesys Web Services for older versions of the Genesys Interaction Recording solutions) of the peer site in a Disaster Recovery deployment. For example: http://server.domain:443.

This functionality is supported for Genesys Interaction Recording (GIR) customers. You must have a login provided by Genesys to access the Genesys Interaction Recording documentation.

## Screen recording in a Hot Seating environment

[**Added:** 8.5.116.10]

Workspace supports Genesys Interaction Recording (GIR) in hot seating (hot desking) environments in the following scenarios:

1. Agents log in to a Place.
2. Agents change Place during their session after logging in a Place.
3. Agents log in to a device in a Place where they have not previously logged in.

To support this feature, you must use the following versions of the GIR components:

- Screen Recording Service (SRS): 8.5.330.64 or higher
- Interaction Recording Web Services (RWS): 8.5.201.75 or higher

# Exposing Contacts to Agents

[**Modified:** 8.5.101.14, 8.5.104.15, 8.5.105.12, 8.5.117.18, 8.5.141.04]

> Important
>
> This topic includes the Contact Management portion of the former **Managing Contact** topic. The Contact History content has been moved to Exposing History to Agents and the Contact Lookup and Contact History Generation content has been moved to Triggering Contact Look-up and Populating History.

## Configuring contact management

[**Modified:** 8.5.104.15, 8.5.117.18]

Use the Procedure Enabling agents to manage and search contact and interaction history to enable the Contact History feature and Enabling Agents to Manage Contacts to set up agents, Workspace, and Universal Contact Server.

### privileges

Workspace enables agents to manage contacts. The privileges that can be enabled for an agent are the following:

- Can Use Contacts
- View Contact Record
- Edit Contact Record
- Delete Contact
- Create Contact
- Merge Contact
- Undo Merge Contact

Use the options in the `contact` section to configure the way in which agents can manage contacts.

### Configuring the Contact Profile

- contact.displayed-attributes: The list of Contact fields that are displayed when a Contact record is rendered.
- contact.multiple-value-attributes: A list of contact attributes that allow multiple values when the Contact record is displayed.

- contact.editable-attributes: The list of Contact fields that can be edited in the contact record.
- contact.mandatory-attributes: The list of contact fields that cannot be left blank when creating or editing a contact record.

## Configuring the Contact Directory

- contact.directory-displayed-columns: The list of contact fields displayed when the results of a contact search is rendered.
- contact.directory-permissions.<ContactAttributeName>: Specifies a custom contact attribute that is defined in Universal Contact Server that can be used to automatically filter the set of contact presented to the agent after a search. For UCS 8.5 environments, using this capability when using the grid view display mode might impact performance.
- contact.directory-default-mode: Specifies the type of display used by default to present the list of contacts. Applicable only in UCS 8.5 environments.
- contact.default-directory-page-size: The default value for the number of rows per page in the contact directory search result view. A value must be defined in the `contact.available-page-size` option.
- contact.available-directory-page-sizes: The number of rows per page in the contact directory search result view.
- contact.directory-advanced-default: The list of Contact fields that are displayed as default search parameters in advanced search.
- contact.directory-search-types: The list of search types that are available for the agent to use to search the contact database in advanced mode. Specifying the value `contains` might impact performance.
- contact.directory-search-attributes: The list of Contact fields that are used as search parameters in quick search and that can be selected in advanced search.

To mask contact information in the Workspace interface from agents, refer to Masking a contact phone number. [**Added:** 8.5.144.05]

## Enabling agents to manage contacts

Refer to *Genesys Administrator Extension Help* and *Genesys Administrator Extension Deployment Guide* for detailed information about how to use Genesys Administrator Extension and Management Framework to configure access permissions.

**Purpose:**

To enable an agent to view and manage contact information.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to Universal Contact Server.
- The Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group

- The Procedure: Provisioning Workspace for the Voice channel

**Start**

1. Allow the applicable Contact Actions privileges (see Contact Management Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group).
2. Configure the Contact options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Contact configuration option reference for a list of Contact options and a description of how to configure them).

**End**

## Configuring the Workspace application and Universal Contact Server to enable custom contact attributes

[**Modified:** 8.5.101.14]

Refer to *Genesys Administrator Extension Help* and *Genesys Administrator Extension Deployment Guide* for detailed information about how to use Genesys Administrator Extension and Management Framework to configure access permissions.

**Purpose:**

To enable an agent to search for and manage contacts based on custom Business Attributes. Business Attributes must be configured to be searchable and sortable.
In the Universal Contact Server (UCS), each contact is defined by a set of attributes that are known as Business Attributes. Business Attributes are metadata for the contact fields in the contact database. Each Business Attribute value contains a description of one of the contact fields in the contact database.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to UCS.
- The Procedure: Enabling agents to manage contacts

**Start**

1. In Genesys Administrator Extension, create a new Business Attribute by using the name and display name of the Custom Contact Attribute.
2. In UCS 8.5 environments, configure the new Business Attribute as follows (Business Attributes are automatically searchable and sortable in UCS 9.1 environments):
    - Set the `is-searchable` to `true` option to make the Business Attribute available for contact

searches.

- Set the `is-sortable` to `true` option to make the Business Attribute available in the directory view.

3. Add the Business Attribute to the list of searchable attributes in the Workspace `contact.directory-search-attributes` option.
4. Configure the Workspace contact.directory-displayed-columns option by using the display name of the Business Attribute to enable the Business Attribute to appear as a column heading in search results (refer to the Contact configuration option reference for a list of Contact options and a description of how to configure them).
5. To enable the Business Attribute to display in the record details for the contact, configure the Workspace contact.displayed-attributes option that is displayed (refer to the Contact configuration option reference for a list of Contact options and a description of how to configure them).
6. To specify/restrict the list of contact attributes that can be edited, use the contact.editable-attributes option. By default, the value `$ALl$` enables editing of all the displayed contact attributes.

**End**

# Restricting Contact Management access

You can configure Workspace to restrict the access of agents to the Contact Directory. Access to the contents of this view is restricted by using a custom filter based on the role of the Application, Tenant, Agent Group, or Agent. For example, you can create a contact search filter that is applied to the Team Communicator or the Contact Search for attributes such as department or customer.

## Restricting Contact Search by permissions

Workspace automatically restricts the results that are displayed on the contact list in the following interface view:

- Team Communicator
- Contact Directory
- Merge-Contact dialog
- Assign Contact
- Email address selection dialog

To provision restricted access to the Contact Directory, for each contact attribute that is used to grant permission to access contact records, use the following example as a guide:

In the `interaction-workspace` section of the Application, Tenant, Agent Group, or Agent for whom you want to configure permissions, create one or more options like the following option examples:

- contact.directory-permissions.<ContactAttributeName> where `ContactAttributeName1=AttributeValue1,AttributeValue2`
- contact.directory-permissions.<ContactAttributeName> where <ContactAttributeName2>= AttributeValue3,AttributeValue4

- contact.directory-enabled-modes: Specifies which view(s) of the Contact Directory can be selected by an agent in [[Documentation:ES:Admin:UCS:8.5.1|UCS 8.5 environments. **Warning:** Genesys recommends that the value is set to `ListView` in environments where contact segmentation is used, as `GridView` is known to cause performance issues with Universal Contact Server DB. [**Added:** 8.5.105.12]

The contact.directory-permissions.<ContactAttributeName> option modifies the search logic whenever the Agent makes a contact search request. For the example above, the following logical filtering criteria are added to the search criteria that are specified by the agent in the following way:

```
AND ((ContactAttributeName1=AttributeValue1) or
(ContactAttributeName1=AttributeValue2)) AND ((ContactAttributeName2=AttributeValue3)
or (ContactAttributeName2=AttributeValue4)) AND
```

The logic of the filtering might be slightly different than this depending on which search algorithm is being used.

The attributes used in contact permission configuration must be defined as Custom Contact Attributes in Universal Contact Server (UCS). For UCS 8.5 environments, in the Annex of the Business Attribute Value representing the custom contact attribute, the `is-searchable` option in the `settings` section must be set to `true`.

## Example

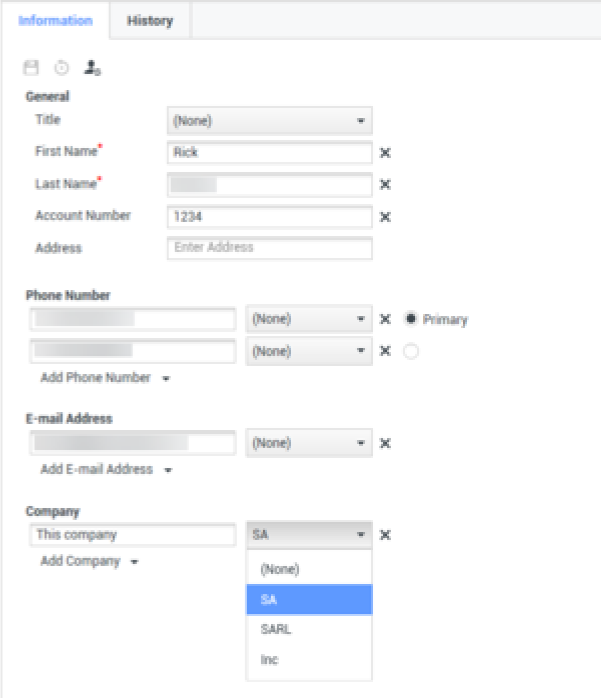
You have defined the following attributes in UCS: `IsVIP` and `DepartmentID` You want to restrict members of the Agent Group ABC so that they cannot access to the "VIP" contacts, and you want to restrict them to the following departments: `Sales` and `Pre-Sales`.

Configure the following `interaction-workspace` section options in the Annex of the `ABC` Agent Group:

- `contact.directory-permissions.IsVip=FALSE`
- `contact.directory-permissions.DepartmentID=Sales,PreSales`

# Add predefined descriptions for a custom contact attributes with multiple values

You can add a custom attribute to the Contact Information that can be populated with multiple values. It is possible to assign a description to those values, either by allowing the user to add plain text (the default mode) or through a selection of a pre-defined descriptions through a drop-down list (the mechanism described here). For example, you might want to create a new contact attribute called "Company" and, for each value assigned to this contact attribute, associate a **Company Type** from a predefined list.



General

Title: (None)

First Name*: Rick

Last Name*: [redacted]

Account Number: 1234

Address: Enter Address

Phone Number

[redacted] (None) ● Primary

[redacted] (None) ○

E-mail Address

[redacted] (None)

Company

This company SA

Use the following steps to create the attribute and add it to the Contact Information view:

1. Create a new Business Attribute where the Business Attribute Values represent the list of valid descriptions that are displayed in the drop-down control; for example, **CompanyTypes**.
2. Create a new Business Attribute Value in the Business Attribute **ContactAttributes**; for example, **Company**.
3. In the annex of the new Business Attribute Value of the Business Attribute **ContactAttributes**, create a section called **settings**.
4. In the **settings** section, create a Key-Value Pair (KVP) where the key is **MultipleValues-Descriptions** and the value is the name of the Business Attribute created in step 1 to store valid descriptions; for example, **MultipleValues-Descriptions** = **CompanyTypes**.
5. Make the new Contact Attribute part of the contact profile by adding the value, **Company** in this example, to the contact.displayed-attributes application option.
6. Make the new Contact Attribute of type **multiple** by adding its name to the contact.multiple-value-attributes application option. For example, `contact.multiple-value-attributes=` 'FirstName,LastName,Company'
7. For multiple contact attributes, specify whether the default Business Attribute value of a drop-down list is automatically populated in the associated contact attribute field of the Contact Information tab by using the contact.multiple-value-attributes-enable-default-description option. [**Added:** 8.5.141.04]
8. Restart Workspace.

# Exposing History to agents

[**Modified:** 8.5.117.18, 8.5.126.07, 8.5.136.07, 8.5.142.05, 8.5.143.08, 8.5.144.05]

> ### Important
>
> This topic includes the History Management portion of the former **Managing Contact** topic. The Contact Management content has been moved to Exposing Contacts to Agents and the Contact Lookup and Contact History Generation content has been moved to Triggering Contact Look-up and Populating History.

## Configuring History management

[**Modified:** 8.5.104.15, 8.5.117.18]

Use the Procedure Enabling agents to manage and search contact and interaction history to enable the Contact History feature and Enabling Agents to Manage Contacts to set up agents, Workspace, and Universal Contact Server.

### privileges

Workspace enables agents to manage contacts. The privileges that can be enabled for an agent are the following:

- Can Use Contact History
- Manually assign an interaction to a Contact
- Interaction Threads
- Interaction Ownership
- Populating the Contact History with eServices Interactions
- Resend email interactions from the Contact History

Use the options in the `contact` section to configure the way in which agents can manage interactions in the History.

### Accessing History

Workspace can search for and display a list of Historical Interactions in three different scopes:

- The Contact History search feature returns lists of interactions restricted by the `ContactID`. You can filter the result list by timeframe and by configured filters, and then search within this list in either quick search or advanced search mode.

- The My History Search feature returns lists of interactions restricted by the `ownerID`. You can filter the result by timeframe and configured filters, and then search within this list in either quick search or advanced search mode.
- The Interaction Search feature enables an agent to search the historical interactions without knowing the contact name or being restricted to interactions processed by that agent. This view does not return any interaction by default. It allows an agent to search for interactions by using quick search or advanced search mode. You can filter the result by timeframe and configured filters.

For UCS 8.5 environments, in any of these scopes, the search operation searches interactions that are stored in the UCS Lucene index and that correspond to the content of the "Main" UCS database. The interactions that have been pruned from the Main to the Archive UCS database are *not* available for searching.

## Configuring History display

[**Modified:** 8.5.126.07, 8.5.142.05, 8.5.143.08]

Use the following configuration options to specify how the contact history is displayed in Interaction Search, My History, and Contact History views:

- contact.history-displayed-columns: Specifies the list of Interaction Attributes that are used to display historical interactions in Contact History Flat View.
- contact.history-displayed-columns-treeview: Specifies the list of Interaction Attributes that are used to display historical interactions in Contact History Tree View.
- contact.myhistory-displayed-columns: Specifies the list of Interaction Attributes that are used to display historical interactions in My History Flat View.
- contact.myhistory-displayed-columns-treeview: Specifies the list of Interaction Attributes that are used to display historical interactions in My History Tree View.
- contact.all-interactions-displayed-columns: Specifies the list of Interaction Attributes that are used to display historical interactions in Interaction Search.
- contact.history.media-filters: Specifies the list of media types that can be used to filter the list of interactions.
- contact.history.filters-<attribute>: Specifies a custom interaction attribute that is defined in Universal Contact Server that can be used to automatically filter the set of interactions presented to the agent.
- contact.history-default-time-filter-main: Specifies the default position of the time filter slider in Contact History.
- contact.myhistory-default-time-filter-main: Specifies the default position of the time filter slider in My History.
- contact.all-interactions-default-time-filter-main: Specifies the default position of the time filter slider in interaction search list.
- <media-type>.contact-history.enable-combine-ixn-with-current: Specifies how an interaction is displayed when opened from the Interaction view **Contact History** tab. [**Added:** 8.5.143.08]

To mask contact information in the Workspace interface from agents, refer to Masking a contact phone number. [**Added:** 8.5.144.05]

### Formatting a custom history attribute as a date

When a custom attribute is designed to store dates, you can specify how it should be formatted in the History views.

First, create a Business Attribute Value in the Business Attribute **Interaction Attributes** to represent your custom attribute. Then, in the annex of this Business Attribute Value create an `interaction-workspace` section and add the following options:

- `display-type=date`
- `date.time-format=<date and time format>`
  Refer to date.time-format for supported formats.

## Configuring History Quick Search

- contact.history-quick-search-attributes: Specifies which interaction attributes are used to Quick Search interactions within the History of a Contact. Refer to list of interaction attributes available for search.
- contact.myhistory-quick-search-attributes: Specifies which interaction attributes are used to Quick Search interactions within My History. Refer to list of interaction attributes available for search.
- contact.all-interactions-quick-search-attributes: Specifies which interaction attributes are used to Quick Search interactions within the Interaction Search view. Refer to list of interaction attributes available for search.

## Configuring History Advanced Search

The Advanced Search enables agents to specify multiple search criteria by selecting predefined search attributes from drop-down buttons in Interaction Search, Contact History and My History views. The Advanced Search can by constrained by Match All and Match Any filter. Depending on the selected search criteria, various search types are allowed, such as Matches and Equals.

- contact.history-search-attributes: Specifies the list of interaction attributes that are available in advanced search (refer to list of interaction attributes available for search).
- contact.history-advanced-default: Specifies the list of interaction attributes that are presented as default search parameters in advanced search.
- contact.date-search-types: The list of search types that are available for the agent to search for historical interactions by date.
- Use the contact.history-custom-attribute-values.<attribute-name> options to specify the comma separated list of possible values for each custom search attribute that you want to enable. Optionally, in the dictionary, specify the display name of agent groups by adding the following parameter:

```
<Value Id="Contacts.ContactDirectoryView.CustomAttribute.<custom-attribute-name>.<attribute-value-name>" String=" Display Name"/>
```

- Configuring Groups: To group the search attributes that can be used in advanced search, specify a comma separated list of search attributes as the value for the contact.history-search-attribute-group.<group-name> option.

Optionally, in the dictionary, specify the display name of the attribute groups by adding the following key:

```
<Value Id="Contacts.InteractionSearchView.Group.<GroupName>" String=" Display Name"/>
```

## List of interaction system attributes available for search and column display

Quick, Advanced, Contact History, My History, and All Interactions search of Historical Interactions can be configured to operate with a list of search attributes. There are System and Custom attributes. This table defines the scope of configuration for each search type.

**Interaction History Search System Attributes**

| Attribute Name | Advanced Search | Quick Search | Contact/ My History (Grid) | Contact/ My History (Tree) | All Interactions Search (Grid) | All Interactions Search (Tree) | Description |
|---|---|---|---|---|---|---|---|
| CcAddresses | Yes | Yes | No | No | Yes | Yes | The email Cc address |
| ContactId | Yes | No | Yes | Yes | Yes | Yes | The Contact of the interaction (it can be searched by using Team Communicator) |
| EndDate | Yes | No | Yes | Yes | Yes | Yes | The date when the interaction was marked completed in the Genesys system |
| EstablishedDate | Yes | No | No | No | Yes | Yes | The date when the Chat session was established |
| FromAddress | Yes | Yes | No | Yes | Yes | Yes | The email From address |
| FromPersonal | Yes | Yes | No | No | Yes | Yes | The Personal Part of the email From address |

| Attribute Name | Advanced Search | Quick Search | Contact/ My History (Grid) | Contact/ My History (Tree) | All Interactions Search (Grid) | All Interactions Search (Tree) | Description |
|---|---|---|---|---|---|---|---|
| Id | Yes | Yes | No | Yes | No | Yes | The unique ID of the Interaction |
| Mailbox | Yes | Yes | No | No | Yes | Yes | The Mailbox from which the email was received |
| OwnerId | Yes | No | Yes | Yes | Yes | Yes | The person who processed the interaction (it can be searched by using Team Communicator) |
| PhoneNumber | Yes | Yes | No | No | No | Yes | The Phone Number from which the contact called or was used to call the contact |
| ReleasedDate | Yes | No | No | No | Yes | Yes | The date when the Chat session was ended |
| ReplyToAddress | Yes | Yes | No | No | Yes | Yes | The email Reply-To address |
| ReviewerId | Yes | No | No | No | Yes | Yes | The person who reviewed the interaction (typically an email — it can be searched by using |

| Attribute Name | Advanced Search | Quick Search | Contact/ My History (Grid) | Contact/ My History (Tree) | All Interactions Search (Grid) | All Interactions Search (Tree) | Description |
|---|---|---|---|---|---|---|---|
| | | | | | | | Team Communicator) |
| SentDate | Yes | No | No | No | Yes | Yes | The date when the outbound email was sent to the destination |
| StartDate | Yes | No | Yes | Yes | Yes | Yes | The date when the interaction was created in the Genesys system |
| Status | Yes | No | Yes | Yes | Yes | Yes | The Status of the interaction in UCS (In Progress, Done) |
| StructuredText | Yes | Yes | No | No | Yes | Yes | The Transcript of the Chat, SMS Session, or FacebookPrivateMessage session, or the E-Mail Rich Text Content |
| Subject | Yes | Yes | Yes | Yes | Yes | Yes | The Subject of the interaction |
| SubtypeId | Yes | No | No | Yes | No | Yes | The Sub-Type of the eServices interaction (for example: InboundNew, OutboundReply) |
| Text | Yes | Yes | No | No | Yes | Yes | The text received from or sent to the contact, |

| Attribute Name | Advanced Search | Quick Search | Contact/ My History (Grid) | Contact/ My History (Tree) | All Interactions Search (Grid) | All Interactions Search (Tree) | Description |
|---|---|---|---|---|---|---|---|
| | | | | | | | typically the email plain text content |
| TheComment | Yes | Yes | No | No | Yes | Yes | The Notes attached to the interaction by the person who handled it |
| ToAddresses | Yes | Yes | No | No | Yes | Yes | The email To address. |
| TypeId | Yes | No | No | Yes | No | Yes | The Type of the eServices interaction (for example: Inbound, Outbound) |

- System date attributes: "On", "OnOrAfter", "Before", and "Between" search types. This is configured by using the contact.date-search-types option.
- System text attributes: can be searched by using the Matches search type which, for each word typed into the query, returns at least one word that starts with this word. Text search does not support query containing double quotes. Interaction Search enables agents to search for the content of email and chat interactions. Content for these interactions is stored in "Text" and/or "StructuredText" attributes. Text includes the content of the plain-text email interactions. StructuredText includes the content of HTML-formatted email interactions and chat transcripts, as well as SMS interactions handled in "session mode" and Facebook Private Message sessions.

**Custom History Search Attributes:** A custom interaction search attribute is an interaction attribute that is not part of the default Genesys UCS data design. A custom interaction search attribute is typically defined during the Business Process design and is implemented by the addition of key-value pair to the attached data of the interactions that are then stored in UCS.

You can configure Workspace to use custom interaction search attributes as search criteria that are used in quick search or displayed in the advanced search mode of Interaction Search, Contact History, and My History views, by using the contact.history-quick-search-attributes, contact.myhistory-quick-search-attributes, contact.all-interactions-quick-search-attributes, contact.history-search-attributes configuration options.

**Limitation:** JOINT searches of the interaction list with the contact list are not possible unless you create a business process that copies attributes from the contact records into the corresponding interaction records.

### Custom interaction properties

[**Modified:** 8.5.136.07]

You can create custom attributes and make them searchable. In UCS 9.1 environments, the interaction properties are searchable when you add them to a custom attribute. In UCS 8.5 environments, you must configure the attribute first to make it searchable— for more information, refer to *Making an Attribute Searchable from the Desktop*' in the eServices documentation.

In UCS 9.1 environments, use the contact.history-custom-attributes-search-types option to specify whether the custom attribute is can be found as an exact match (`is`) or by a "starts-with" (`begins-with`) search. In UCS 8.5 environments, the only supported value is `is`; it is not necessary to configure this option in UCS 8.5 environments.

> **Warning**
>
> The following limitations **must** be taken into account before enabling an interaction custom attribute as an advanced search criteria:
>
> - For UCS 8.5 environments, custom interaction search attribute support **only** an *exact match* search; for UCS 9.1 environments, *begins-with* searches are also supported. Genesys *strongly* recommends that you use the contact.history-custom-attribute-values.<attribute-name> option to configure a list of predefined values that enable the agent to select the search value from a list. You can control the search behavior by using the contact.history-custom-attributes-search-types option. The custom attributes used in the interaction history search must be defined as a Business Attribute Value of the **Interaction Attributes** Business Attribute in the Configuration Layer. In the Annex of the Business Attribute Value, the `is-searchable` option in the settings section *must* be set to `true`.
> - For UCS 8.5 environments, when you assign custom interaction search attribute key names, you **must** avoid key names that are sub-strings of other key names that are also stored as business attached data of the same or other interactions. Failure to heed this warning will result in misleading search results.
>
>   For example, if the term `Priority` is defined as a custom interaction search attribute and the following attributes might also be part of the interactions that stored in UCS: `Priority`, `GEMX-Priority`, `_Priority`, and `GEMX-MSMail-Priority`. If these alternate `*Priority` attributes can be assigned with a value set that is partially shared with the `Priority` attribute, the wrong matching logic and extended result set might be returned.

## Contact Management: Summary of activity that is related to the current contact

In the interaction windows, Workspace displays visual indicators that inform the agent who is handling the interaction about the activities that are related to the current contact. To enable these features, allow the following privilege:

- Can Use Contacts

For Interaction Workspace 8.1.2 and later and Workspace Desktop Edition 8.5.0 and later, this feature displays the number of in-progress interactions for a contact in an icon. This indicator measures the number of eServices interactions that are currently in-progress somewhere in the workflow, excluding the current one. You can activate this feature by configuring the contact.metrics.enable-interactions-in-progress option in the `Contact` section. If the agent clicks the icon, the interactions are immediately displayed in the History view.

For Interaction Workspace 8.1.3 and later and Workspace Desktop Edition 8.5.0 and later, the Recent Interaction Notification is also displayed. This indicator provides the number of interactions that have been exchanged with this contact in the past specified number of days, excluding current interaction. This feature is useful for predicting the level of contact frustration. Configure the contact.metrics.time-frame-customer-notification option in the `Contact` section to specify the time interval.

If the following privilege is granted, Workspace displays the list of recent interactions with this contact as a tooltip for the icon:

- Can Use Contact History

## Restricting Contact History access

You can configure Workspace to restrict the access of agents to the Contact History. Access to the contents of these views is restricted by using a custom filter based on the role of the Application, Tenant, Agent Group, or Agent. For example, you can create a contact search filter that is applied to the Team Communicator or the Contact Search for attributes such as department or customer.

### Restricting Interaction History views and Search by permissions

Workspace automatically restricts the results that are displayed in the interaction list in the following interface views:

- Contact History
- My History
- Global Interaction Search

The contact.history.filters-<attribute> option modifies the search logic and presentation whenever the Agent accesses or searches an interaction list.

To provision restricted access to the interaction lists, in the `interaction-workspace` section of the Application, Tenant, Agent Group, or Agent for whom you want to configure permissions, create one or more options like the following option examples:

- contact.history.filters-<attribute> where `<InteractionAttributeName1>=AttributeValue1, AttributeValue2`

The custom attributes used in the interaction history search must be defined as a Business Attribute Value of the **Interaction Attributes** Business Attribute in the Configuration Layer. In the Annex of the Business Attribute Value, the `is-searchable` option in the settings section *must* be set to `true` and the value of the `is-sortable` option should also be set to `true` when you enable this feature.

### Example

The following interaction custom attribute is attached to interactions stored in UCS: `DepartmentID`

You want to restrict members of the Agent Group `ABC` so that they can see the Contact History only through filters that give them access to interactions related to the `Sales` or `Support` departments.

Configure the following `interaction-workspace` section options in the Annex of the `ABC` Agent Group:

- `contact.history.filters-DepartmentID=Sales,Support`

The `Sales` attribute is displayed as an option in the **Filter** menu and as an attribute in the ContactHistory view list or grid. Agents can alternatively access the Sales or the Support interactions, but cannot see any other interactions.

**Note:** If you define only one possible value, for example, `contact.history.filters-DepartmentID=Sales`, the related filter will not show up in the Contact History form, but this filter is applied automatically to all agent requests to access the history.

## Enabling History filtering

### Media filtering

The `Filter` menu of the Contact History view and My History view can be configured to display specific media types in a specific order by using the contact.history.media-filters option in the `interaction-workspace` section of the Interaction Workspace application object. You can use this option to add the media types of the workitems that are supported by 3rd party plug-ins.

### Custom filtering

You can create custom business attributes in Universal Contact Server for contacts. For example, you might want to create a set of service areas from your business and use these as custom contact attributes, or you might want to create a set of contact levels, such as silver, gold, and platinum, and use these as custom attributes. When you define your custom business attribute, you must define the valid values. Use the following configuration option to enable filtering on your custom business attribute values:

- contact.history.filters-<attribute>

## Managing interaction ownership

Workspace enables you to display the interaction owner that is defined in the UCS data base to the agents that can view the Contact History.

Display of interaction ownership is controlled by the following options:

- display-format.agent-name: Specifies the format of the agent name in the Contact History view. Workspace uses this information to convert the owner ID from UCS to a label that is displayed in the Contact History view. If there is no owner ID associated with an interaction, then this field is blank.
- contact.history-displayed-columns: Specifies which interaction attributes are displayed in the Contact History view. Add the value `OwnerId` to display the Interaction "Processed by" column.

# Triggering contact look-up and populating History

[**Modified:** 8.5.117.18]

> **Important**
>
> This topic includes the Contact Look-up portion of the former **Managing Contact** topic. The Contact Management content has been moved to Exposing Contacts to Agents and the Contact History content has been moved to Exposing History to Agents.

Interactions can be assigned to a contact in the contact database automatically or manually. Automatic assignment is handled by contact look-up when an inbound interaction is received.

Use the following configurations to specify how automatic contact assignment and creation is handled.

## Automatic contact look-up and interaction storage

[**Modified:** 8.5.117.18]

Workspace can be configured to automatically assign a new inbound interaction to an existing contact in the contact database, or to create a new contact if the contact is not found. This behavior can be specified for all channels or for individual channels. To enable this capability, you must configure the following options:

- contact.lookup.enable: Specifies that the Universal Contact Server (UCS) identify service is to be used for contact lookup.
- contact.lookup.enable-create-contact: Specifies that the Universal Contact Server (UCS) creates a contact service to be used if the identify service fails to find the contact.
- contact.lookup.auto-assign-mode: When there are multiple contact matches, specify whether the first found contact is assigned automatically (default behavior) or the agent is presented with a list of matches that he or she can manually choose the contact.
- contact.lookup.<media-type>.enable: Activates the Workspace features that rely on the Universal Contact Server (UCS) IdentifyService for contact lookup when an interaction is presented to the Agent.
- contact.lookup.<media-type>.auto-assign-mode: For the specified media type, when there are multiple contact matches, specify whether the first found contact is assigned automatically (default behavior) or the agent is presented with a list of matches that he or she can manually choose the contact.
- contact.lookup.<media-type>.enable-create-contact: Activates the Workspace features that rely on Universal Contact Server (UCS) for contact lookup when an interaction of the given media type is

presented to the agent.

- contact.ucs-interaction.<media-type>.enable-create: Activates the Workspace feature that generates the interaction history in Universal Contact Server (UCS) based on the inbound and outbound interactions of type <media-type> that are handled by Workspace. Enable agents to create interactions of type <media-type>.
- contact.ucs-interaction.<media-type>.enable-lookup: Activates the Workspace feature that looks up the history of existing interactions of the given <media-type> in Universal Contact Server (UCS) to update their content and status according to live interaction lifecycle.
- contact.ucs-interaction.<media-type>.use-server-date: For the specified <media-type>, it specifies whether Workspace sets the start and end dates of interactions by using the time of the local agent workstation, or uses the date and time specified by Universal Contact Server (UCS) when it creates or updates an interaction record in UCS. Use this option as a template and modify its name by replacing the <media-type> by an actual media type that is defined in Management Framework.
- contact.threading-ucs-interaction.enable: Activates the Workspace feature that associates interactions that are submitted during multi-channel contact communication, such as smssession, in threads in Universal Contact Server history.

### Directly dialed calls

If you want to record calls directly dialed by agents in your Contact Database so that it can be tracked in their history, ensure that the following two options are set to `true`:

- contact.lookup.<media-type>.enable-create-contact
- contact.ucs-interaction.<media-type>.enable-create

To enable agents to manually create a contact when they have an active interaction, set the value of the contact.lookup.enable-create-contact option to `true`

## Improving automatic contact assignment

[**Added:** 8.5.117.18]

If you implement the default contact look-up configuration, Workspace selects the first contact from the list of matching contacts returned by UCS based on interaction attributes. If more than one contact matches the information available for a new inbound interaction, subsequent matches are not considered. To improve automatic contact assignment when multiple matches are found, use the following configuration options to enable agents to choose a contact from the list of matches returned by UCS:

- contact.lookup.auto-assign-mode: When there are multiple contact matches, specify whether the first found contact is assigned automatically (default behavior) or the agent is presented with a list of matches that he or she can manually choose the contact.
- contact.lookup.<media-type>.auto-assign-mode: For the specified media type, when there are multiple contact matches, specify whether the first found contact is assigned automatically (default behavior) or the agent is presented with a list of matches that he or she can manually choose the contact.

### Example: Preventing automatic contact creation in case of no UCS match and automatic

contact assignment in case of multiple UCS matches

This example is for the voice channel, but it can be applied to all channels or to other specific channels. Normally, if there is a single contact in the Universal Contact Server (UCS) database, Workspace automatically assigns the contact. In these scenarios:

- If you want to enable your agents to assign a contact to an interaction based on a look-up in the UCS database in scenarios where no match is found for the inbound interaction, but you do not want a new contact to be created automatically without your agent searching the contact database first,
- If you want to enable an agent to review the possible contact matches and choose the appropriate one in scenarios where there are multiple contacts that match an incoming interaction,

### Use the following configuration:

- Contact - Can Assign is allowed
- `contact.lookup.voice.enable` = `true`
- `contact.lookup.voice.enable-create-contact` = `false`
- `contact.lookup.voice.auto-assign-mode` = `false`

## Contact Management: Last Routed Agent

The Last Routed Agent Feature enables you to save in the Contact Profile, information about the last agent who handled interactions from that contact. The agent handling information can then be used during the routing of subsequent interactions from this contact. When an agent actively handles an interaction of a given media type from a contact, the following keys are set in the Contact Profile:

- `LastCalledAgent_EmployeeID`
- `LastCalledAgent_TimeStamp`
- `LCA_EmplID_<MediaType>`
- `LCA_TimeStamp_<MediaType>`

Where `<MediaType>` corresponds to the media of the interaction.

Refer to the eServices and Routing documentation for more information about this feature.

You can activate this option globally by setting to true the contact.last-called-agent.enable option in the `Contact` section. Or you can activate it by media type by setting to `true` the contact.last-called-agent.<media-type>.enable option in the `Contact` section.

## Interaction threads

Workspace enables you to manage interaction threading in the Universal Contact Server (UCS) database. E-mail threading is set according to reply actions that are made by agents, automatic response, and contacts. Voice threading is set according to the transfer record of a call; each agent that handles the interaction generates an interaction in the UCS database. The contact.threading-ucs-interaction.enable option controls how multi-channel threading that results from the outbound interactions that are created during the handling of an original inbound or outbound contact interaction. For example, an inbound email might result in an outbound email, or or more outbound voice calls, and an SMS session. All of these related interactions can be associated as a single thread.

In the Workspace Contact Directory and My History views, agents can view the interaction history as threads. Threads are sorted in reverse chronological order, with the most recent first, but within threads, interactions are sorted chronologically, from first to most recent.

To use interaction threading, enable the following privilege:

- Can Use Contacts

Then, configure the following configuration option to `true`:

- contact.threading-ucs-interaction.enable: Enables the Workspace feature that associates interactions that are submitted during multi-channel contact communication, such as `smssession`, in threads in Universal Contact Server history.

## Populating the Contact History with eServices Interactions

eServices interactions differ by type in the way that they are submitted to the Contact History:

- `email`: E-mail interactions are automatically submitted to the Contact History by Email Server and Interaction Workspace. They are completed by Interaction Workspace or by a Business Workflow.
- `chat`: Chat interactions are automatically submitted to the Contact History by Chat Server. They are completed by Interaction Workspace or by a Business Workflow.
- `SMS Session`: SMS Session interactions are automatically submitted to the Contact History by Chat Server. They are completed by Interaction Workspace or by a Business Workflow.
- `SMS Page`: SMS Page interactions are submitted to the Contact History by a Business Workflow only. This is applicable to both inbound and outbound workflows.
- `workitem`: Custom workitem interactions are submitted to the Contact History by a Business Workflow only. This is applicable to both inbound and outbound workflows.

### Important

**Notes:**

- If the Contact History is created by a Business Workflow, the integrator is responsible for using the appropriate building blocks in the *ad-hoc* strategy.
- Interaction Workspace can submit interactions to the contact history if the contact.ucs-interaction.<media-type>.enable-create option is set to `true` for any media.
- Interaction Workspace can look for a matching contact for any media-type if the contact.ucs-interaction.<media-type>.enable-lookup option is set to `true`.

# KPIs and Contact Center Statistics

Refer to *Framework 8.5 Genesys Administrator Extension Help* and *Genesys Administrator Extension Deployment Guide* for detailed information on how to use Genesys Administrator Extension and Management Framework to configure access permissions.

## Viewing user and group metrics

Workspace enables agents to view real-time metrics of their performance and the performance of the contact center in a table view or in a dedicated gadget component. Statistical information is displayed in the form of industry standard- and contact center-defined Key Performance Indicators (KPIs). KPIs enable agents to focus on their efficiency and to compare their performance against that of their colleagues.

Workspace enables you to configure which KPIs are displayed to your agents, with what frequency, and with what alarm conditions.

Examples of statistics that can be displayed in Workspace:

### Login-time statistics:

- Login duration
- Ready duration
- Wrap duration
- Talk duration
- Hold duration
- Number of interaction transferred
- Number of internal calls
- Number of refused interactions
- Total number of interactions
- Average handling time
- Number of voice interactions
- Average handling time voice interactions
- Number of email interactions
- Average handling time email interactions
- Number of chat
- Average handling time chat

You can use the following options in the `interaction-workspace` section to configure the behavior of KPIs in Workspace:

- `kpi.displayed-kpis`: Defines the KPIs that are displayed to the agent. The KPI names refer to names of the sections that are defined by the Application KPI options.
- `kpi.show-agent-groups`: Defines whether KPIs are also calculated for the Agent Groups that contain the agent.
- `kpi.refresh-time`: Defines the frequency of notification (in seconds) for statistics.

You can use configuration options in each section that defines a KPI to configure the behavior of KPIs in Workspace (refer to Section KPI Name). Statistics are displayed in both the Main Window and the Statistics Gadget.

## Viewing Contact-Center Metrics

Workspace enables agents to view real-time metrics of the performance of the contact center. Statistical information is displayed in the form of industry standard- and contact center-defined metrics. Metrics enable agents to focus on their efficiency and to compare their performance against that of their colleagues. Statistics are displayed only for the Tenant to which the agent is logged.

Workspace enables you to configure which metrics are displayed to your agents, with what frequency, and with what alarm conditions.

### Queue statistics

- Number of interactions in queue (In the Login Queue)
- Average waiting time (In the Login Queue)
- Number of distributed calls (In the Login Queue)
- Number of abandoned calls (In the Login Queue)
- Number of agents logged in to the ACD Queue

The Workspace default statistics are controlled by the following privileges set in the `interaction-workspace` section, except where noted otherwise:

- `statistics.refresh-time`: Defines the frequency of notification (in seconds) for statistics.
- `statistics.queues`: Specifies the list of queues for which queue statistics are calculated. A comma-separated list of queues are defined as follows: `<QueueName>@<SwitchName>`. This option is part of the regular option hierarchy; therefore, you can define the list of applicable objects per Tenant, Group, or User; however, if the list is defined in the statistic section, the list is global.
- `statistics.routing-points`: Specifies the list of Routing Points for which routing point statistics are calculated. A comma-separated list of queues are defined as follows: `<RoutingPoint>@<SwitchName>`. This option is part of the regular option hierarchy; therefore, you can define the list of applicable objects per Tenant, Group, or User; however, if the list is defined in the statistic section, the list is global.

Statistics are calculated in the following way, the statistic is calculated for the list of objects specified by the statistics.queues option, which can be populated with the following tags; however, if the section contains an option named "object-id", the statistic is calculated only for that specific object:

- $Agent.LoginQueue$: Returns the list of queue identifiers on which the agent logs in. Set this value either in the object-id option in the contact center statistics section, or in the statistics.queues option.
- $AgentGroup.OriginationDns$: Returns the list of origination DNs for the list of agent groups to which the agent currently logged in. This value IS set by the object-id option in the contact center statistics section.

Contact Center Metrics are displayed in both the Main Window and the Statistics Gadget.

# Provisioning KPIs and Contact Center Statistics

## 1. Enabling an agent to view My Statistics (KPIs)

**Purpose:**

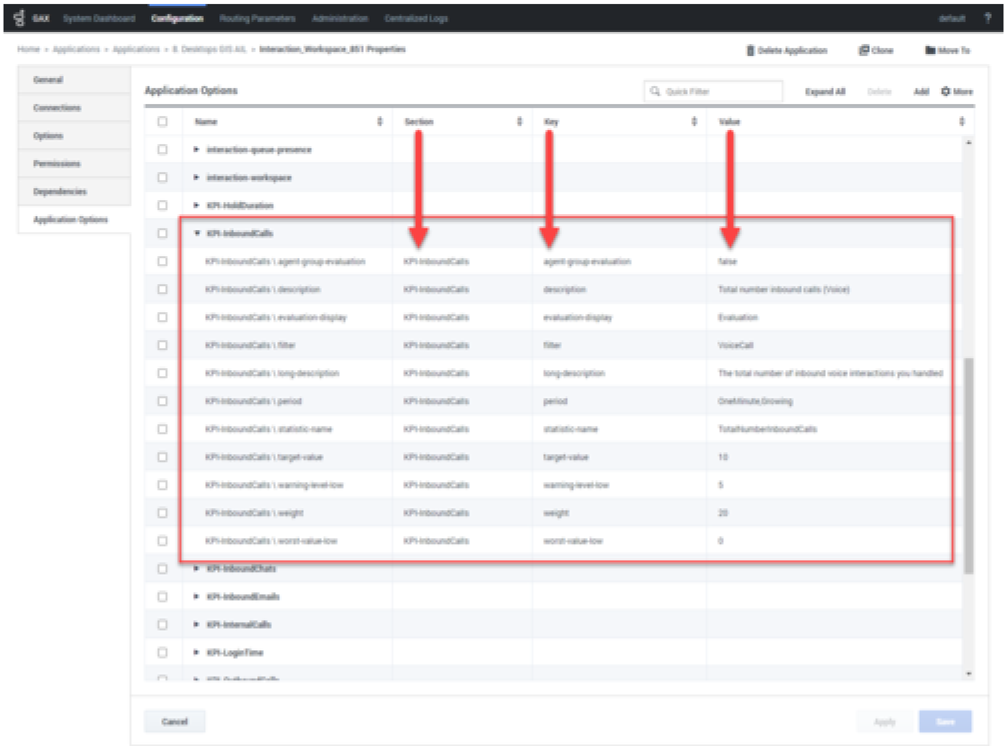
To enable an agent to view their Key Performance Indictors (KPIs).
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace Application object exists in the Configuration Database.
- Workspace has a connection to Stat Server.

**Start**

1. Configure Stat Server as described in *Framework Stat Server 8.1 Deployment Guide*. to produce the metrics that you want to employ to measure the KPIs in your contact center.
2. In the Workspace Application, configure the Workspace KPIs section following the option reference in Section KPI Name.
3. Allow the following Statistics Access privileges (see Statistics Access Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group):
    - KPI module
4. Configure the KPI options in the interaction-workspace section of the Workspace Application object (refer to the KPI configuration option reference for a list of KPI options and a description of how to configure them).

**Example**



Application Options

| | Name | Section | Key | Value |
|---|---|---|---|---|
| ☐ | ▸ interaction-queue-presence | | | |
| ☐ | ▸ interaction-workspace | | | |
| ☐ | ▸ KPI-HoldDuration | | | |
| ☐ | ▾ KPI-InboundCalls | | | |
| ☐ | KPI-InboundCalls \ agent-group-evaluation | KPI-InboundCalls | agent-group-evaluation | false |
| ☐ | KPI-InboundCalls \ description | KPI-InboundCalls | description | Total number inbound calls (Voice) |
| ☐ | KPI-InboundCalls \ evaluation-display | KPI-InboundCalls | evaluation-display | Evaluation |
| ☐ | KPI-InboundCalls \ filter | KPI-InboundCalls | filter | VoiceCall |
| ☐ | KPI-InboundCalls \ long-description | KPI-InboundCalls | long-description | The total number of inbound voice interactions you handled |
| ☐ | KPI-InboundCalls \ period | KPI-InboundCalls | period | OneMinute,Growing |
| ☐ | KPI-InboundCalls \ statistic-name | KPI-InboundCalls | statistic-name | TotalNumberInboundCalls |
| ☐ | KPI-InboundCalls \ target-value | KPI-InboundCalls | target-value | 10 |
| ☐ | KPI-InboundCalls \ warning-level-low | KPI-InboundCalls | warning-level-low | 5 |
| ☐ | KPI-InboundCalls \ weight | KPI-InboundCalls | weight | 20 |
| ☐ | KPI-InboundCalls \ worst-value-low | KPI-InboundCalls | worst-value-low | 0 |
| ☐ | ▸ KPI-InboundChats | | | |
| ☐ | ▸ KPI-InboundEmails | | | |
| ☐ | ▸ KPI-InternalCalls | | | |
| ☐ | ▸ KPI-LoginTime | | | |
| ☐ | ▸ KPI-OutboundCalls | | | |

**End**

## 2. Enabling an agent to view Contact Center Statistics (Object Metrics)

**Purpose:**

To enable an agent to view the overall performance of the contact center by viewing statistics regarding Queues, Routing Points, and so on.
An agent can log in to a queue or a routing point if the estimated wait times are particularly high or if the object is displaying a warning or error. Agents should log in to those queues that are experiencing high levels of abandoned calls.
For each Contact Center Statistic (Object Metric) that you want to define and use, you must define a section in the Workspace `Application` object in the Configuration Database.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to Statistics Server.

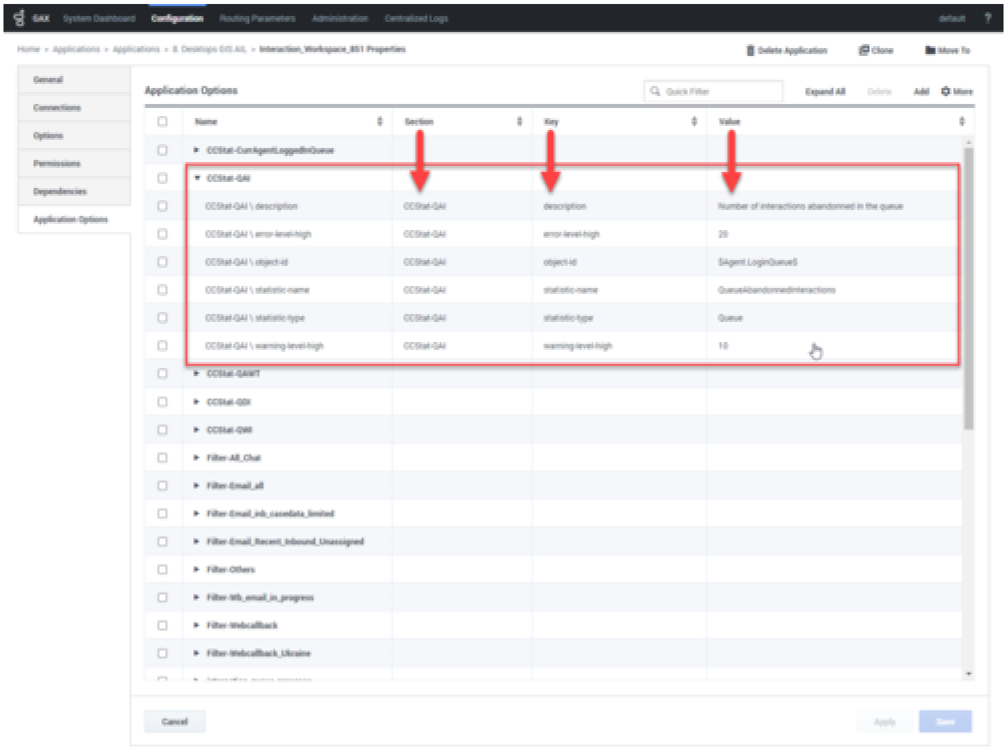
**Start**

1. In Genesys Administrator Extension, create a new section named after the Object Statistic that you

want to use.

2. Define the mandatory and optional options and values for the statistic (refer to Section Object Statistic Name).
3. Allow the following Statistics Access privileges (see Statistics Access Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group):
    - Object Statistics module
4. Configure the Statistics options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Statistics configuration option reference for a list of Statistics options and a description of how to configure them).

**Example**



Application Options

| Name | Section | Key | Value |
|---|---|---|---|
| ▸ CCStat-CurrAgentLoggedInQueue | | | |
| ▾ CCStat-QAI | | | |
| CCStat-QAI \ description | CCStat-QAI | description | Number of interactions abandonned in the queue |
| CCStat-QAI \ error-level-high | CCStat-QAI | error-level-high | 20 |
| CCStat-QAI \ object-id | CCStat-QAI | object-id | $Agent.LoginQueue$ |
| CCStat-QAI \ statistic-name | CCStat-QAI | statistic-name | QueueAbandonnedInteractions |
| CCStat-QAI \ statistic-type | CCStat-QAI | statistic-type | Queue |
| CCStat-QAI \ warning-level-high | CCStat-QAI | warning-level-high | 10 |
| ▸ CCStat-QAWT | | | |
| ▸ CCStat-QDI | | | |
| ▸ CCStat-QWI | | | |
| ▸ Filter-All_Chat | | | |
| ▸ Filter-Email_all | | | |
| ▸ Filter-Email_inb_casedata_limited | | | |
| ▸ Filter-Email_Recent_Inbound_Unassigned | | | |
| ▸ Filter-Others | | | |
| ▸ Filter-Wb_email_in_progress | | | |
| ▸ Filter-Webcallback | | | |
| ▸ Filter-Webcallback_Ukraine | | | |

**End**

## 3. Enabling an agent to view My Statistics and Contact Center Statistics in the Statistics Gadget

**Purpose:**

To enable an agent to view Statistics and Contact Center Metrics in the Statistics Gadget. The Statistics Gadget provides a small, convenient viewer for Statistics and Contact Center Metrics that does not require agents to keep opening the `My Statistics` tab and the `Contact Center Statistics` tab in the `Workspace`. The Statistics Gadget provides continuous updates and warnings.

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- Workspace has a connection to Statistics Server.
- Complete one or both of the following:
  - The Procedure: Enabling an agent to view My Statistics (KPIs) (Refer to Procedure 1 on this topic page)
  - The Procedure: Enabling an agent to view Contact Center Statistics (Object Metrics) (Refer to Procedure 2 on this topic page)

**Start**

1. Allow the following Statistics Access privilege (see Statistics Access Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group):
   - Gadget Statistics module
2. Configure the Statistics Gadget options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Gadget and Statistics Gadget configuration option reference for a list of Statistics options and a description of how to configure them).

**End**

# Reporting

[**Added:** 8.5.112.08] [**Modified:** 8.5.116.10]

This topic summarizes the Workspace features that contribute to statistics computation by the Genesys back-end.

## Focus duration

Workspace is an *omni-channel application* which means that agents might be handling multiple interactions on different channels for the same contact, or for multiple contacts. For example, an agent might be talking on the phone with a contact, sending the contact text information by the SMS channel, and composing an email to the contact while exchanging Instant Messages with someone in your back office; or, an agent might be handling multiple chats for multiple contacts while handling email interactions or workitems. In both of these example scenarios, the agent spends a little bit of time focused on each individual interaction; however, from a reporting perspective, the duration of handling is the total time from when each interaction was initiated until it was marked Done. This gives a false representation of the actual amount of time that an agent was actually handling each individual interaction.

When the value of the reporting.case.report-case-in-focus-duration option is set to `true`, Workspace reports to the Genesys back-end the time, in seconds, that an individual interaction had the focus, that is, the time that the agent actually spent working directly or indirectly on this interaction. The duration of each interaction is reported as the sum of the times that the interaction had the focus of the agent. The assignment of focus-time to an interaction is based on the following rules:

1. At any given time, only one Case can be considered as *in focus*.
   Therefore, the sum of the focus-times of the agent cannot exceed the total focus-time.
2. When a Case is considered to be *in focus*, the time in focus is assigned to the Main interaction of the case; that is, the interaction that initiated the case (for example an inbound chat or an outbound call).
3. The Case that contains the current Active Voice Call (`Established`) is considered as *in focus*, whether the voice call in the Case is the main interaction, a secondary interaction, or a consultation.
   There cannot be more that one Active Voice Call at a given time.
4. When there is no Active Voice Call, the Case that has the visual focus, corresponding to the selected view, is considered as *in focus*. This can be a Case that contains a non-Active Voice Call (for example, `Dialing`, `On Hold`, or `Released`).
5. If Workspace loses the application focus, the Case that had visual focus at the time Workspace lost the focus continues to be considered as *in focus*.

### Tip

Setting the values of the interaction.auto-focus and interaction.auto-focus.<media-type> options affects

> the focus time calculations for accepted interactions. [**Added:** 8.5.116.10]

# Hiding selected data in logs

Workspace enables you to specify and filter the contents of the application logs. You can choose to hide content by using asterisks or to skip specific key-value pairs.

Use the options in the `log` section to configure the way in which logs are filtered.

- log.default-filter-type: Specifies the default filter type for logging.
- log.filter-data.<keyName>: Specifies the treatment of log data. This option enables you to filter for specific attached data keys, by specifying the key name in the option name. This option overrides any values specified by the log.default-filter-type option.

# Client-side port security

Use the Procedure: Enabling client-side port definition to define the access ports for each application to which Workspace connects to ensure the security of the system. This feature is configured partially on Framework Configuration Server and partially on the Workspace application in Genesys Administrator Extension. The *Client-Side Port Definition* chapter of the *Genesys Security Deployment Guide*. provides detailed information on client-side port definition.

## Important

When you set the client-side port for the connection to Configuration Server, ensure that you use the `Interaction_Workspace_850.apd` template; do not use the `Interaction_Workspace_AgentDesktop_850.apd` template.

If a connection to at least one back-end server is configured with an explicit client-side port, after exiting, the agent must wait for a system timeout before they are able to initialize Workspace application again. The timeout is positioned at the Windows OS level through the following registry key: `TcpTimedWaitDelay`. This is a system level limitation.

# Business Continuity for SIP Server, Configuration Server, and Statistic Server

[**Modified:** 8.5.106.19, 8.5.108.11, 8.5.109.16, 8.5.111.21]

## Business Continuity Using High Availability Paired Servers (SIP Server, Statistic Server, Configuration Server Proxy)

Business Continuity relies on pairs of servers. A pair is composed of regular linked Primary and Backup Servers. Two Server pairs are considered peers when they support each other in a Business Continuity model.

You can specify the name of the preferred connection site and the Business Continuity connection site, and the time-out interval for switch-over to the Business Continuity site.

> Tip
>
> All Workspace Business Continuity-related (disaster recovery) options can be configured for any object in the configuration hierarchy (Application, Tenant, Agent Group, and Person).

Use the Procedure: *Configuring Workspace for Business Continuity* to enable Business Continuity for your agents. By using that procedure, you specify the site name in the options of the corresponding server application (SIP Servers, Stat Servers and Configuration Servers) in the `interaction-workspace` section.

### Procedure: Configuring Workspace for Business Continuity

**Purpose:**

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

**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- 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 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 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 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 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**

Then, use the following options in the interaction-workspace section of the Interaction Workspace Application object to configure Business Continuity:

- disaster-recovery.enabled: Specifies whether Business Continuity is enabled.
- disaster-recovery.preferred-site: Specifies the name of the preferred connection site for the application, tenant, agent Group, or agent. It must correspond to the value of the disaster-recovery.site option on the server object at the preferred site.
- disaster-recovery.peer-site: Specifies the name of the site that is to be the Business Continuity-peer. It must correspond to the value of the disaster-recovery.site option on the server object at the peer site.
- disaster-recovery.timeout: Specifies the timeout interval in seconds after loss of connection to the High Availability (HA) Pair of servers and before Business Continuity switchover is initiated.

## SIP Server specific options

For more information about SIP Server High-Availability, refer to Framework SIP Server High-Availability Deployment Guide.

To ensure that the switchover from the peer to the preferred site occurs correctly when the preferred site is restored, use the following options in the interaction-workspace section of the Interaction

Workspace Application object to configure SIP Server Business Continuity:

- `disaster-recovery.wait-for-sipphone-timeout`: Specifies the time interval in seconds to wait for SipPhone (SIPEndpoint) registration before initiating the Business Continuity switchover if the current SipPhone(SIPEndpoint) connection was lost or registration was expired.
- `disaster-recovery.auto-restore` (for T-Server only): Specifies whether or not switching back to the Preferred site should occur if it becomes available.

The default values for the following configuration options can cause the switchover to the preferred site to be delayed in some environments:

- sipendpoint.proxies.proxy0.reg_timeout=3600
- sipendpoint.proxies.proxy1.reg_timeout=3600

> ### Important
> These options are used by Workspace to configure Workspace SIP Endpoint or Genesys Softphone (since the end of 2018). It is not applicable to any other SIP Endpoint, hard or soft.

The default values of 3600 seconds means that the first SIP Endpoint re-registration attempt will occur after one hour. In scenarios where the preferred site is returned to service in a few minutes, there is a significant delay between the preferred site being available and the SIP Endpoint attempting to re-register with the preferred site.

You can choose much shorter re-registration attempt intervals by setting the values of these options to a value between 30 and 60 seconds.

If the agent is configured to restore the last seen state after switchover (the value of `disaster-recovery.restore-agent-state` is set to `true`), Workspace postpones automatic restoration of the last seen agent state until the agent closes all stacked interaction windows. In earlier releases of Workspace, the application restored the last seen state immediately after login on paired DR sites, but this made it possible to accept new calls while the last call was still in progress.[**Modified:** 8.5.105.12]

> ### Important
> - For SIP Server Business Continuity, the preferred Extension DN and the peer Extension DN must be assigned to the same Place. This equally applies to environments with Voice/IM only medias and to environments with "blended agents" (agents who have a SIP Business Continuity Voice/IM DN and at least one eServices media).
> - Stat Server 8.1.2 or above must be used to properly support SIP Business Continuity environment.

### Provision Workspace Client with Configuration Server HA settings

[**Added:** 8.5.111.21]

Genesys recommends that you edit the `InteractionWorkspace.exe.config` file that you deliver to agents to provide Configuration HA/Pair information to the client for the first time that Workspace is launched in a Configuration Server HA/Pair environment. This file is in the Workspace installation directory. Those settings are updated based on central configuration once Workspace is connected to a Configuration Server Proxy.

Edit or add the following keys:

```
<appSettings>
...
<add key="login.url" value="tcp://MyConfigEnvironment/ApplicationName" />
<add key="login.nodes.preferred-site.MyConfigEnvironment"
value="[CSP1Host:CSP1Port][CSP2Host:CSP2Port],Timeout=10" />
<add key="login.nodes.peer-site.MyConfigEnvironment"
value="[CSP3Host:CSP3Port][CSP4Host:CSP4Port],Timeout=10" />
...
</appSettings>
```

- **MyConfigEnvironment**: The name of the Configuration Environment that is displayed in the Login window.
- **ApplicationName**: The name of the Workspace Desktop application in Management framework
- **CSP1Host:CSP1Port,...,CSP4Host:CSP4Port**: CSP1 is the Primary Preferred, CSP2 the backup Preferred, CSP3 the Primary Peer, CSP4 the backup Peer of your configuration HA/Pair. The order indicates the preference (Primary first).
- **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.

## Business Continuity using clustered servers (Statistic Server and Configuration Server Proxy)

Instead of using Primary/backup pairs on each site, Workspace Desktop can be configured to connect to a cluster on each site to provide less down time and load balancing.

To properly set up clusters for Business Continuity, you must provision one cluster of Configuration Server Proxies and one cluster of Statistic Servers on the preferred site and similar clusters on the peer site. Use the procedures in the Load Balancing Using Clusters topic to create load balancing clusters.

Use the Procedure: *Configuring Workspace for Business Continuity based on Clusters* to enable Business Continuity for your agents.

### Procedure: Configuring Workspace for Business Continuity based on clusters

**Purpose:**

To manage server to enable Workspace to connect to an alternate (Peer) cluster in the event of a disaster has affected the Preferred cluster.

This Configuration applies to Statistic Servers and Configuration Server Proxies.
**Prerequisites**

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace Desktop Edition `Application` object exists in the Configuration Database.
- A cluster of Configuration Server Proxies or Statistic Servers has been defined for each Business Continuity site.

**Start**

1. On the object representing the cluster 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.
2. On the object representing the cluster 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.
3. For each agent or agent group, configure the `disaster-recovery.preferred-site` option in the `interaction-workspace` section by specifying the symbolic site name of the Server that you specified with the `disaster-recovery.site` option.
4. For each agent or agent group, configure the `disaster-recovery.peer-site` option in the `interaction-workspace` section with the symbolic site name of the Server that you specified with the `disaster-recovery.site` option.
5. The Preferred site for one agent or group of agents can also be the Peer site for another agent or group of agents.
6. Use option `disaster-recovery.enabled` to enable Business Continuity for each agent or agent group and use option `disaster-recovery.timeout` to specify the Business Continuity switch over behavior.

**End**

## Provision bootstrap configuration cluster settings in Workspace configuration file

Genesys recommends that you edit the `InteractionWorkspace.exe.config` file that you deliver to agents to provide Configuration cluster information to the client for the first time that Workspace is launched in a Configuration Server Cluster environment. This file is located in the Workspace installation directory. Those settings are updated based on central configuration once Workspace is connected to a Configuration Server Proxy.

Edit or add the following keys:

```
<appSettings>
 ...
 <add key="login.url" value="tcp://MyConfigEnvironment/ApplicationName" />
 <add key="login.cluster.nodes.preferred-site.MyConfigEnvironment"
value="[CSP1Host:CSP1Port][CSP2Host:CSP2Port][CSP3Host:CSP3Port],Timeout=10" />
 <add key="login.cluster.nodes.peer-site.MyConfigEnvironment"
```

```
value="[CSP4Host:CSP4Port][CSP5Host:CSP5Port][CSP6Host:CSP6Port],Timeout=10" />
 ...
</appSettings>
```

- **MyConfigEnvironment**: The name of the Configuration Environment that is displayed in the **Login** window.
- **ApplicationName**: The name of the Workspace Desktop application in Management framework
- **CS1PHost:CSP1Port...CS6PHost:CSP6Port**: The `host:port` pairs of your configuration cluster.
- **Timeout**: Sets the value in seconds of the `warm-standby.retry-delay` option.

# eServices Business Continuity with UCS 9.1

[**Added:** 8.5.126.07]

> **Important**
>
> This topic covers deployments that use UCS 9.1. For deployments that use UCS 8.5, refer to eServices Business Continuity with UCS 8.5.

Workspace enables you to configure and provision a Business Continuity model by defining Load Balancing rules in a single Workspace Application object in the Configuration Layer so that a single software package can be distributed to all agents, and to define a Disaster Recovery model that switches to a peer data center without requiring agents to re-start their application.

## Setting up your system

This section describes how to set up your environment to implement disaster recovery and load balancing for Interaction Server and UCS 9.1 in a high availability (HA) environment.

### Physical connections

You must create an eServices server environment that is divided between two data centers that are set up to support disaster recovery.

In a standard operational situation, the load is equally distributed between the two data centers, based on static distribution rules: Each agent is provisioned to connect preferably to one data center but can also connect to the other one if the preferred data center is no longer available. Therefore, each data center must be able to support the full agent load.

Set up your data centers following this model:

- **A Proxy Tier**
  - A pool of Interaction Server Proxies running in a N+1 failover schema (there is no primary-backup definition)
- **A Core Application Tier**
  - Contains a primary-backup Interaction Server pair
  - Contains UCS 9.1 Nodes
- **A Database Tier**
- Contains the database nodes which includes Interaction Server data running in *primary* or *replica* mode

- Contains the cassandra nodes for UCS 9.1 data running in a *Multiple-Data-Center* configuration

Interaction Server runs in an active/passive mode with respect to the eServices components:

- **Active**
  - The Interaction Server database is in Primary mode
  - The Interaction Server pair are running and connected to the primary database
  - The Interaction Server Proxies are running and connected to the core Interaction Server, and each is listening on its configured connection port
- **Passive**
  - The Interaction Server database is in Replica mode
  - The Interaction Server pair are stopped
  - The Interaction Server Proxies are running or not, connected or not, to the core Interaction Server, and each is not listening on its configured connection port. This means that it is not possible to open any network connection to them

> ### Important
>
> UCS 9.1 supports geo-replication by using the Datacenter Replication feature in Cassandra.

## Provisioning Interaction Server for Disaster Recovery

The Database Tier is critical for eServices components. The Disaster Recovery site model that is used for SIP Server, Stat Server, and Configuration Server Proxy (refer to eServices Business Continuity with UCS 8.5 or eServices Business Continuity with UCS 9.1) cannot be applied to eServices components. The advanced proxy architecture that enables the N+1 model of High Availability and load balancing also does not apply to the Primary/Backup model.

eServices and UCS 9.1 Disaster Recovery takes advantage of the Application Cluster (a pool of servers of different types; for example, UCS 9.1 Nodes and Interaction Server Proxies) in Genesys Management Framework. This model provisions server pools for the Interaction Server Proxy/UCS 9.1 Nodes connections types. The Application Cluster model also enables the support of various scale factors that depend on the application type (for example, three Interaction Server Proxy nodes for the eServices agents and six UCS 9.1 nodes for the eServices agents and the Voice agents).

> ### Important
>
> The cluster of Interaction Server Proxy objects discussed in this section should not be confused with the concept of the Interaction Server Cluster described in the eServices Documentation.

An Application Cluster can contain a set of optional Workspace specific key-value pairs which are defined in the `interaction-workspace` section. The `disaster-recovery.site` option defines the data center where the Cluster is located. The `disaster-recovery.site` option is a Key that you add in the options of another application to which Workspace connects (for example: SIP Server, Stat Server, and Config Server) to recognize it as a "peer" or a "preferred" site. See the examples below to see how this option is used.

The disaster-recovery.eservices-site Workspace option, which can be defined in the Application options or in the Tenant, Group, or User annex, is used to define the cluster assignment. This option defines the data center where a user must connect to enable eServices / UCS 9.1 links (it is optional and taken into account dynamically).

The list of connections is taken into account when the application is restarted.

- If the Workspace disaster-recovery.eservices-site option is not defined, or is left empty, Workspace selects the first cluster in the list that is available independent of the value specified for the `disaster-recovery.site` option, and uses the pool of servers that it contains.
- If Workspace option disaster-recovery.eservices-site is assigned a site name, Workspace selects the first cluster in the list that has an equivalent value specified in the `disaster-recovery.site`, and uses the pool of servers that it contains.

This approach enables you to define different kinds of deployment models that enable Load Balancing and Disaster Recovery.

## Provisioning examples

The following tables provide administrators with an example of how an eServices Business Continuity/ Disaster Recovery environment might be set up for each type of data center.

### Example 1: Load Balancing in one data center

**Cluster Applications**

| | Connections | Options |
|---|---|---|
| Cluster eService Site_A | IxnProxy_A_1, IxnProxy_A_2, IxnProxy_A_3<br>UCS_Node_A_1, UCS_Node_A_2, UCS_Node_A_3 | interaction-workspace/disaster-recovery.site=<not defined> |

**Notes:**

- UCS_Node_x_y stands for UCS Node number y on site x.
- IxnProxy_x_y stands for Interaction Server Proxy number y on site x.
- For example, IxnProxy_A_2 is the Interaction Server Proxy #2 on Site A

**Workspace Application**

| | Connections | Options |
|---|---|---|
| Workspace | Cluster eService Site_A | interaction-workspace/disaster-recovery.eservices-site=<not defined> |

### Example 2: Two data centers for Business Continuity, Load Balancing inside each data center

**Cluster Applications**

| | Connections | Options |
|---|---|---|
| Cluster eService Site_A | IxnProxy_A_1, IxnProxy_A_2, IxnProxy_A_3 UCS_Node_A_1, UCS_Node_A_2, UCS_Node_A_3 | interaction-workspace/disaster-recovery.site=Site_A |
| Cluster eService Site_B | IxnProxy_B_1, IxnProxy_B_2, IxnProxy_B_3 UCS_Node_B_1, UCS_ Node _B_2, UCS_ Node _B_3 | interaction-workspace/disaster-recovery.site=Site_B |

**Notes:**

- UCS_ Node _x_y stands for UCS Node number y on site x.
- IxnProxy_x_y stands for Interaction Server Proxy number y on site x.
- For example, IxnProxy_A_2 is the Interaction Server Proxy #2 on Site A

**Workspace Application**

| | Connections | Options before site switch-over | Options after site switch-over |
|---|---|---|---|
| Workspace | Cluster eService Site_A, Cluster eService Site_B | interaction-workspace/disaster-recovery.eservices-site=Site_A | interaction-workspace/disaster-recovery.eservices-site=Site_B |

### Runtime connection logic

At runtime, Workspace selects the initial Proxy node within the appropriate pool defined for the active data center. When Workspace needs to establish a connection to a node (UCS 9.1 Server Node or Interaction Server Proxy), Workspace has the following behavior:

1. Isolate the list of Server objects of the appropriate type from the Cluster Application that has the site name that corresponds to the current agent.
2. Create a random list of those servers to load balance connections
3. Select the first server from the list
4. Attempt to connect to the selected server
5. If there is a connection failure, take the next server from the list (go to step 4)

If Workspace fails over from one node to another node within the same data center because the connection to a node (UCS 9.1 or Interaction Server Proxy) is lost, Workspace tries to find another active node within the pool of nodes that were identified during initial node selection.

If Workspace fails over from the current active data center to the other other data center in a scenario that defines the failover by a manual update of the value of the disaster-recovery.eservices-site option, which is assigned to the agent through the configuration hierarchy (refer to Administrator operations in case of data center failover, below):

1. For each node type, Workspace refreshes the list of Server objects of the appropriate type from the Cluster Application that has the new site name
2. If Workspace is currently connected to UCS 9.1 and/or Interaction Server Proxy node, it forces the disconnection
3. For each proxy/Node type, Workspace applies the same random selection/round robin connection rules that it uses during initial connection.

> ### Important
>
> In a scenario where the Configuration Server is down during the modification of site, the following mechanism is applied when the connection of Configuration Server is back in service, Workspace:
>
> 1. retrieves the object of hierarchy defined by the disaster-recovery.eservices-site option
> 2. refreshes this object by using a request to Configuration Server
> 3. performs a *move site* if necessary

You can specify which eServices media Workspace should try to reconnect after reconnection to Interaction Server by using the following two options:

- eservices.session-restore-mediatype—Specifies which media types Workspace should attempt to reconnect.
- eservices.session-restore-timeout—Specifies the time, in seconds, after reconnection to Interaction Server to retrieve the ownership of interactions of media types that are specified by the value of the `eservices.session-restore-mediatype` option. The value of this option is dependent on the value that is specified for the Interaction Server agent-session-restore-timeout option.

When Workspace loses connection to Interaction Server or Interaction Server Proxy due to network disconnection, shutdown of Interaction Server Proxy instance, and so on, eServices interactions remain open in Workspace, but with a restricted set of controls until the connection to same or a new instance of Interaction Server or Interaction Server Proxy is restored. The following general restrictions apply:

- Case Information is read only
- It is not possible to assign a contact to the interaction
- Disposition code is read only
- Record Information is read only

For SMS interactions, the following restrictions apply:

- The Transfer, Done, and Delete controls are disabled
- Send message is active only for SMS in session mode

For email interactions, the following restrictions apply:

- All actions except for print preview are disabled

- Agent can edit To, From, Cc, Bcc, subject, and email body in outbound email only are active

For chat interactions, the following restrictions apply:

- The End, Transfer, Conference, and Done (if the chat session is already ended) controls are disabled
- The Send message control is active if the chat session is still active and the Chat Server connection is still up

### Administrator operations in case of data center failover

The key operation in a data center failover scenario is the transfer of mastership of the database from Site_A to Site_B.

> ## Important
>
> You should note that this is an intensive operation that can take a significant amount of time. It involves working with the **Database Administrator** who must initiate the procedure. Since a failover scenario can happen at any time, the Database Administrator might not be available immediately.

The following is a typical failover operation scenario:

1. A disaster is detected
2. The decision to switch over to data center 2 (Site_B) is taken
3. Stop all the *active* servers (core and proxies) that might still be running on Site_A
4. eServices agent activity is suspended
5. The database administrator must make the DB of Site_B the *primary*
6. Start the core Interaction Server pair of Site_B, UCS 9.1 nodes on Site_B should be already running
7. Start the Interaction Server Proxy instances of Site_B
8. Change the value of the disaster-recovery.eservices-site option of the agent at the appropriate hierarchy level (this can be at the Application level if everyone shares the same data center at the same time) so that it points to Site_B
9. Workspace instances automatically reconnect to UCS 9.1 nodes and Interaction Server Proxies of Site_B and agents can resume their eServices activity

> ## Important
>
> The transition from passive to active of the *peer* eServices data-center takes a significant amount of time, during which the eServices capabilities are not usable by agents.

### For blended agents (voice + at least one eServices channel)

The data center failover logic between data centers is not the same for SIP Voice/IM channels and eServices channels, nor is the login model the same. However, Workspace and Stat Server maintain a composite connection between these two solutions known as "blended agents". In particular, the Stat Server composite representation requires a single agent-place virtual runtime link.

In SIP Business Continuity:

- The configuration model is based on a pair of DNs (one for each data center)
- In typical deployment model, each DN belongs to its dedicated Place (preferred DN in Place 1, peer DN in Place 1_DR). To have the two DNs configured in one place, they must be of type `ACD Position`.
- Agents logon one DN at a time, according to the site currently defined as the *active preferred*, according to the agent configuration; this can change dynamically at runtime according to site failure detection.
- At runtime, Stat Server detects that an agent dynamically moves from the default Place to peer Place.

In Interaction Server:

- An agent logs in to a Place at the beginning of a session. This place remains the same during the session, even if Workspace has to connect to another Interaction Server Proxy, from the local data center or the remote data center.

Therefore, there are situations when an agent might be virtually logged in to two distinct Places, one for voice and one for eServices, which is a not a supported situation for Stat Server.

One possible approach to resolve this situation is to use the Single Place configuration model for the Voice DNs.

# Provisioning

You can configure eService Cluster and eServices Business Continuity together or independently, depending on the design of your eServices architecture. Use the following options to enable Workspace to connect correctly to your environment.

## Cluster provisioning

The following options enable you to specify how the connection to any node of your cluster should be set-up and how the transition between nodes should behave.

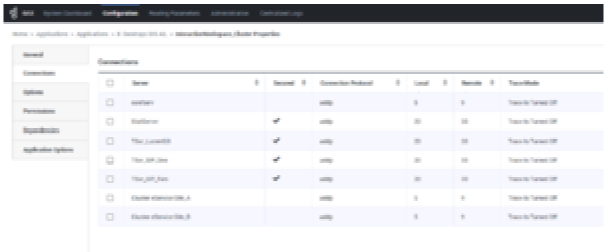
### Warm standby

These two options enable you to specify the time interval for reconnection. Refer to the configuration option reference for details about how to configure these options:

- warm-standby.reconnection-random-delay-range
- warm-standby.retry-delay

## Addp

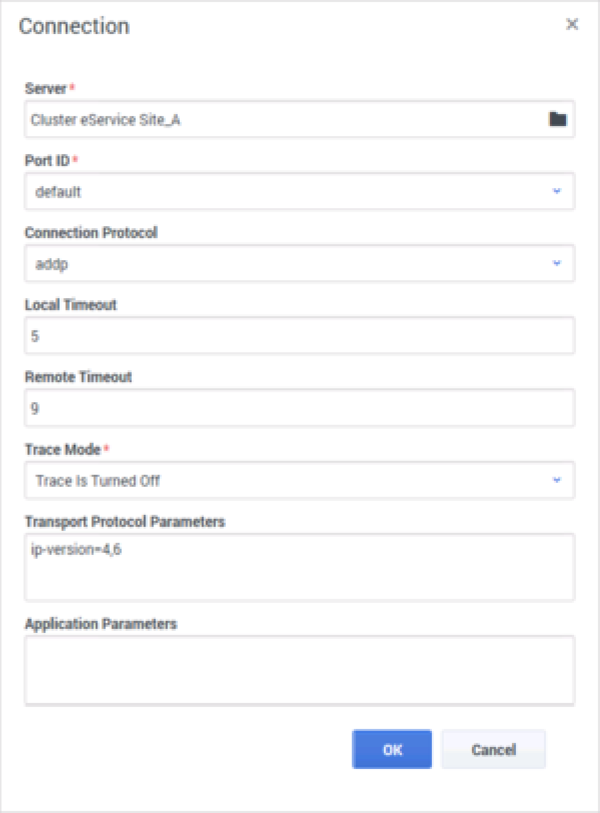
You can define the addp parameters for all applications of the cluster from the Workspace application connections table. These parameters can be overridden in each server application.



Example of Workspace in a cluster configuration for Disaster Recovery

## ip-version

You can define the `ip-version` option for all applications of the cluster from the Workspace application connections table. `ip-version` can be overridden in each server application options. In this example, the `ip-version` of all applications of the cluster is `4,6`:



Connection

Server *
Cluster eService Site_A

Port ID *
default

Connection Protocol
addp

Local Timeout
5

Remote Timeout
9

Trace Mode *
Trace Is Turned Off

Transport Protocol Parameters
ip-version=4,6

Application Parameters

Setting ip-version preferences for Workspace connections for Disaster Recovery

## eServices Disaster Recovery provisioning

These two options enable you to configure the data center infrastructure that is applicable to eServices components:

- disaster-recovery.eservices-site
- disaster-recovery.eservices-random-delay-range

# eServices Business Continuity with UCS 8.5

[**Added:** 8.5.106.19] [**Modified:** 8.5.109.16]

> ### Important
>
> This topic covers deployments that use UCS 8.5. For deployments that use UCS 9.1, refer to eServices Business Continuity with UCS 9.1.

Workspace enables you to configure and provision a Business Continuity model by defining Load Balancing rules in a single Workspace Application object in the Configuration Layer so that a single software package can be distributed to all agents, and to define a Disaster Recovery model that switches to a peer data center without requiring agents to re-start their application.

## Setting up your system

This section describes how to set up your environment to implement disaster recovery and load balancing for eServices in a high availability (HA) environment.

### Physical connections

You must create an eServices server environment that is divided between two data centers that are set up to support disaster recovery.

In a standard operational situation, the load is equally distributed between the two data centers, based on static distribution rules: Each agent is provisioned to connect preferably to one data center but can also connect to the other one if the preferred data center is no longer available. Therefore, each data center must be able to support the full agent load.

Set up your data centers following this model:

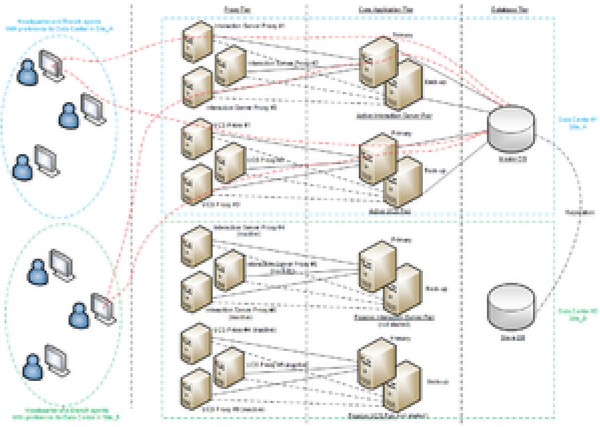
- **A Proxy Tier**
  - An Application Cluster containing a pool of Interaction Server Proxies and UCS Proxies running in a N+1 failover schema (there is no primary-backup definition)
- **A Core Application Tier**
  - Contains a primary-backup Interaction Server pair
  - Contains a primary-backup UCS pair
- **A Database Tier**
  - Contains the database node which includes UCS and Interaction Server data running in *primary* or

*replica* mode

Data centers run in an active/passive mode with respect to the eServices components:

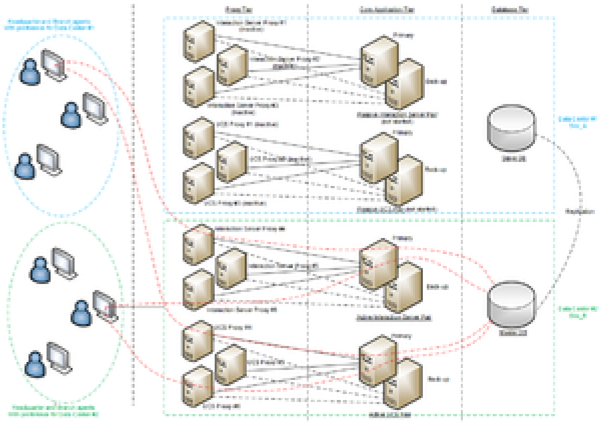
- **Active**
  - The database is in *Primary* mode
  - The Interaction Server pair and the UCS pair are running and connected to the primary database
  - The Interaction Server Proxies and UCS Proxies are running and connected to the core Interaction Server and core UCS, and each is listening on its configured connection port
- **Passive**
  - The database is in *Replica* mode
  - The Interaction Server pair and the UCS pair are stopped
  - The Interaction Server Proxies and UCS Proxies are running or not, connected or not, to the core Interaction Server and core UCS, and each is not listening on its configured connection port. This means that it is not possible to open any network connection to them

The following is an example of the physical network connections when the environment is running in regular operation, and data centers #1 and #2 are up and running:



Example of the physical network connections in regular operation when data centers #1 and #2 are up and running

The following is an example of the physical network connections when the environment is running in regular operation, and data center #1 is down:

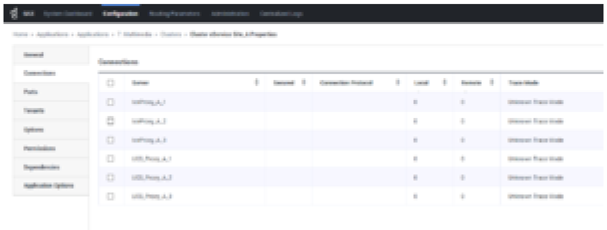


Example of the physical network connections in regular operation when data center #1 is down

## Provisioning eServices Disaster Recovery

The Database Tier is critical for eServices components. The disaster recovery site model that is used for SIP Server, Stat Server, and Configuration Server Proxy (refer to Configuration of Voice and Statistic Business Continuity) cannot be applied to eServices components. The advanced proxy architecture that enables the *N+1* model of High Availability and load balancing also does not apply to the Primary/Backup model.

eServices Disaster recovery takes advantage of the Application Cluster (a pool of Proxy servers of different types; for example, UCS Proxies and Interaction Server Proxies) in Genesys Management Framework. This model provisions *server pools* for the Interaction Server Proxy/UCS Proxy connections types. The Application Cluster model also enables the support of various scale factors that depend on the application type (for example, three Interaction Server Proxy nodes for the eServices agents and six UCS Proxy nodes for the eServices agents and the Voice agents). The following is an example of how an application cluster might be configured in Genesys Administrator Extension:



Connections

| □ | Server | Secured | Connection Protocol | Local | Remote | Trace Mode |
|---|---|---|---|---|---|---|
| □ | IxnProxy_A_1 | | | 0 | 0 | Unknown Trace Mode |
| □ | IxnProxy_A_2 | | | 0 | 0 | Unknown Trace Mode |
| □ | IxnProxy_A_3 | | | 0 | 0 | Unknown Trace Mode |
| □ | UCS_Proxy_A_1 | | | 0 | 0 | Unknown Trace Mode |
| □ | UCS_Proxy_A_2 | | | 0 | 0 | Unknown Trace Mode |
| □ | UCS_Proxy_A_3 | | | 0 | 0 | Unknown Trace Mode |

Application Cluster configuration in Genesys Administrator Extension

An Application Cluster can contain a set of optional Workspace specific key-value pairs which are defined in the `interaction-workspace` section. The `disaster-recovery.site` option defines the data center where the Cluster is located. The `disaster-recovery.site` option is a Key that you add in the options of another application to which Workspace connects (for example: SIP Server, Stat Server, and Config Server) to recognize it as a "peer" or a "preferred" site. See the examples below to see how this option is used.

The disaster-recovery.eservices-site Workspace option, which can be defined in the Application options or in the Tenant, Group, or User annex, is used to define the cluster assignment. This option defines the data center where a user must connect to enable eServices links (it is optional and taken into account dynamically).

In the example above, the `Workspace Application` has connections to one or several clusters. The list of connections is taken into account when the Application is restarted.

- If the Workspace disaster-recovery.eservices-site option is not defined, or is left empty, Workspace selects the first Cluster in the list that is available independent of the value specified for the `disaster-recovery.site` option, and uses the pool of proxies that it contains.
- If Workspace option disaster-recovery.eservices-site is assigned a site name, Workspace selects the first Cluster in the list that has an equivalent value specified in the `disaster-recovery.site`, and uses the pool of proxies that it contains.

This approach enables you to define different kinds of deployment models that enable Load Balancing and Disaster Recovery.

## Provisioning Examples

The following tables provide administrators with an example of how an eServices Business Continuity/ Disaster Recovery environment might be set up.

### Example 1: Load Balancing in one data center

**Cluster Applications**

| | Connections | Options |
|---|---|---|
| Cluster eService Site_A | IxnProxy_A_1, IxnProxy_A_2, IxnProxy_A_3<br>UCS_Proxy_A_1, UCS_Proxy_A_2, UCS_Proxy_A_3 | interaction-workspace/disaster-recovery.site=<not defined> |

**Notes:**

- UCS_Proxy_x_y stands for UCS Proxy number y on site x.
- IxnProxy_x_y stands for Interaction Server Proxy number y on site x.
- For example, IxnProxy_A_2 is the Interaction Server Proxy #2 on Site A

**Workspace Application**

| | Connections | Options |
|---|---|---|
| Workspace | Cluster eService Site_A | interaction-workspace/disaster-recovery.eservices-site=<not defined> |

### Example 2: Two data centers for Business Continuity, Load Balancing inside each data center

**Cluster Applications**

| | Connections | Options |
|---|---|---|
| Cluster eService Site_A | IxnProxy_A_1, IxnProxy_A_2, IxnProxy_A_3 UCS_Proxy_A_1, UCS_Proxy_A_2, UCS_Proxy_A_3 | interaction-workspace/disaster-recovery.site=Site_A |
| Cluster eService Site_B | IxnProxy_B_1, IxnProxy_B_2, IxnProxy_B_3 UCS_Proxy_B_1, UCS_Proxy_B_2, UCS_Proxy_B_3 | interaction-workspace/disaster-recovery.site=Site_B |

**Notes:**

- UCS_Proxy_x_y stands for UCS Proxy number y on site x.
- IxnProxy_x_y stands for Interaction Server Proxy number y on site x.
- For example, IxnProxy_A_2 is the Interaction Server Proxy #2 on Site A

**Workspace Application**

| | Connections | Options before site switch-over | Options after site switch-over |
|---|---|---|---|
| Workspace | Cluster eService Site_A, Cluster eService Site_B | interaction-workspace/disaster-recovery.eservices-site=Site_A | interaction-workspace/disaster-recovery.eservices-site=Site_B |

### Runtime connection logic

[**Modified:** 8.5.109.16]

At runtime, Workspace selects the initial Proxy node within the appropriate pool defined for the active data center.

When Workspace needs to establish a connection to a node (UCS Proxy or Interaction Server Proxy), Workspace has the following behavior:

1. Isolate the list of Server objects of the appropriate type from the Cluster Application that has the site name that corresponds to the current agent.
2. Create a random list of those servers to load balance connections
3. Select the first server from the list
4. Attempt to connect to the selected server
5. If there is a connection failure, take the next server from the list (go to step 4)

If Workspace fails over from one proxy node to another proxy node within the same data center because the connection to a node (UCS Proxy or Interaction Server Proxy) is lost, Workspace tries to find another active node within the pool of nodes that were identified during initial node selection.

If Workspace fails over from the current active data center to the other other data center in a scenario that defines the failover by a manual update of the value of the disaster-recovery.eservices-site option, which is assigned to the agent through the configuration hierarchy (refer to *Administrator operations in case of data center failover*, below):

1. For each proxy type, Workspace refreshes the list of Server objects of the appropriate type from the Cluster Application that has the new site name
2. If Workspace is currently connected to UCS Proxy and/or Interaction Server Proxy node, it forces the disconnection
3. For each proxy type, Workspace applies the same random selection/round robin connection rules that it uses during initial connection.

### Important

In a scenario where the Configuration Server is down during the modification of site, the following mechanism is applied when the connection of Configuration Server is back in service, Workspace:

1. retrieves the object of hierarchy defined by the disaster-recovery.eservices-site option
2. refreshes this object by using a request to Configuration Server
3. performs a *move site* if necessary

You can specify which eServices media Workspace should try to reconnect after reconnection to Interaction Server by using the following two options:

- eservices.session-restore-mediatype—Specifies which media types Workspace should attempt to reconnect.
- eservices.session-restore-timeout—Specifies the time, in seconds, after reconnection to Interaction Server to retrieve the ownership of interactions of media types that are specified by the value of the eservices.session-restore-mediatype option. The value of this option is dependent on the value that is specified for the Interaction Server `agent-session-restore-timeout` option.

When Workspace loses connection to Interaction Server or Interaction Server Proxy due to network disconnection, shutdown of Interaction Server Proxy instance, and so on, eServices interactions remain open in Workspace, but with a restricted set of controls until the connection to same or a new instance of Interaction Server or Interaction Server Proxy is restored.

The following general restrictions apply:

- Case Information is read only
- It is not possible to assign a contact to the interaction
- Disposition code is read only
- Record Information is read only

For SMS interactions, the following restrictions apply:

- The Transfer, Done, and Delete controls are disabled

- Send message is active only for SMS in session mode

For email interactions, the following restrictions apply:

- All actions except for print preview are disabled
- Agent can edit To, From, Cc, Bcc, subject, and email body in outbound email only are active

For chat interactions, the following restrictions apply:

- The End, Transfer, Conference, and Done (if the chat session is already ended) controls are disabled
- The Send message control is active if the chat session is still active and the Chat Server connection is still up

## Administrator operations in case of data center failover

The key operation in a data center failover scenario is the transfer of mastership of the database from Site_A to Site_B.

> ### Important
>
> You should note that this is an intensive operation that can take a significant amount of time. It involves working with the **Database Administrator** who must initiate the procedure. Since a failover scenario can happen at any time, the Database Administrator might not be available immediately.

The following is a typical failover operation scenario:

1. A disaster is detected
2. The decision to switch over to data center 2 (Site_B) is taken
3. Stop all the *active* servers (core and proxies) that might still be running on Site_A
4. eServices agent activity is suspended
5. The database administrator must make the DB of Site_B the *primary*
6. Start the core UCS pair and Interaction Server pair of Site_B
7. Start the Interaction Server Proxy and UCS Proxy instances of Site_B
8. Change the value of the disaster-recovery.eservices-site option of the agent at the appropriate hierarchy level (this can be at the Application level if everyone shares the same data center at the same time) so that it points to Site_B
9. Workspace instances automatically reconnect to UCS Proxies and Interaction Server Proxies of Site_B and agents can resume their eServices activity

> ### Important

> The transition from passive to active of the *peer* eServices data-center takes a significant amount of time, during which the eServices capabilities are not usable by agents.

### For blended agents (voice + at least one eServices channel)

The data center failover logic between data centers is not the same for SIP Voice/IM channels and eServices channels, nor is the login model the same. However, Workspace and Stat Server maintain a composite connection between these two solutions known as "blended agents". In particular, the Stat Server composite representation requires a single agent-place virtual runtime link.

In SIP Business Continuity:

- The configuration model is based on a pair of DNs (one for each data center)
- In typical deployment model, each DN belongs to its dedicated Place (preferred DN in Place 1, peer DN in Place 1_DR). To have the two DNs configured in one place, they must be of type `ACD Position`.
- Agents logon one DN at a time, according to the site currently defined as the *active preferred*, according to the agent configuration; this can change dynamically at runtime according to site failure detection.
- At runtime, Stat Server detects that an agent dynamically moves from the default Place to peer Place.

In Interaction Server:

- An agent logs in to a Place at the beginning of a session. This place remains the same during the session, even if Workspace has to connect to another Interaction Server Proxy, from the local data center or the remote data center.

Therefore, there are situations when an agent might be virtually logged in to two distinct Places, one for voice and one for eServices, which is a not a supported situation for Stat Server.

One possible approach to resolve this situation is to use the Single Place configuration model for the Voice DNs.

## Provisioning

You can configure eService Cluster and eServices Business Continuity together or independently, depending on the design of your eServices architecture. Use the following options to enable Workspace to connect correctly to your environment.

### Cluster provisioning

The following options enable you to specify how the connection to any node of your cluster should be set-up and how the transition between nodes should behave.

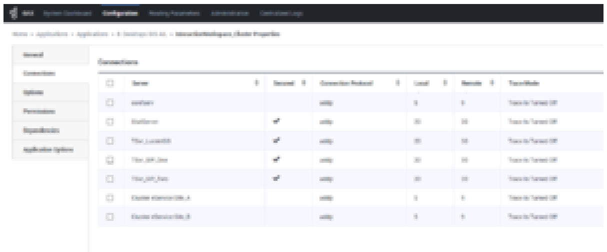
### Warm standby

These two options enable you to specify the time interval for reconnection. Refer to the configuration option reference for details about how to configure these options:

- warm-standby.reconnection-random-delay-range
- warm-standby.retry-delay

### Addp

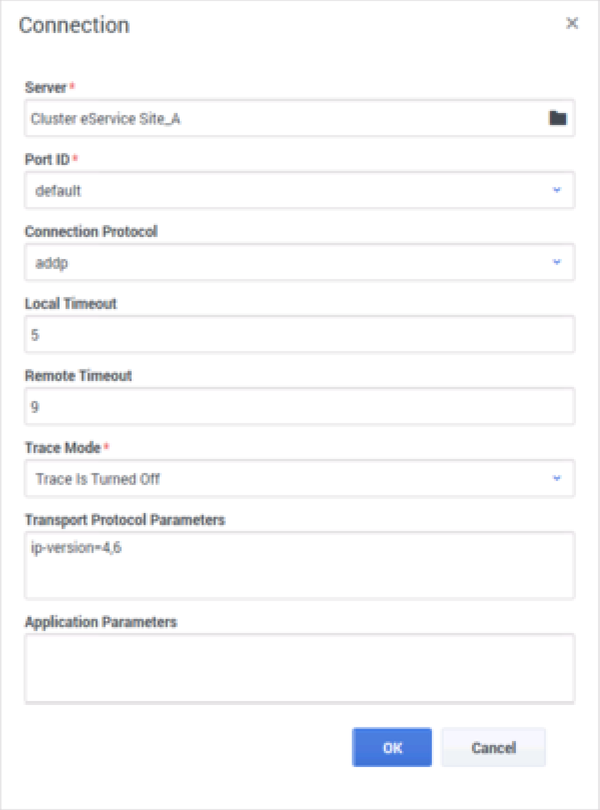
You can define the addp parameters for all applications of the cluster from the Workspace application connections table. These parameters can be overridden in each server application.



Example of Workspace in a cluster configuration for Disaster Recovery

### ip-version

You can define the `ip-version` option for all applications of the cluster from the Workspace application connections table. `ip-version` can be overridden in each server application options. In this example, the `ip-version` of all applications of the cluster is `4,6`:



Server *
Cluster eService Site_A

Port ID *
default

Connection Protocol
addp

Local Timeout
5

Remote Timeout
9

Trace Mode *
Trace Is Turned Off

Transport Protocol Parameters
ip-version=4,6

Application Parameters

Setting ip-version preferences for Workspace connections for Disaster Recovery

## eServices Disaster Recovery provisioning

These two options enable you to configure the data center infrastructure that is applicable to eServices components:

- disaster-recovery.eservices-site
- disaster-recovery.eservices-random-delay-range

# Load Balancing using clusters

[**Added:** 8.5.108.11] [**Modified:** 8.5.111.21, 8.5.126.07]

A Cluster is pool of Genesys Servers of the same type to which Workspace connects. Workspace connects to a single node of a cluster at a time. The node is selected by a client-side or server-side logic, depending on the clustering model. The Genesys servers that Workspace supports through the clustering model are: Statistic Server, Configuration Server Proxy, Universal Contact Server Proxy (8.5), Universal Contact Server Node (9.1), and Interaction Server Proxy.

There are two Configuration models to defined clusters for Workspace:

1. Stat Server, Interaction Server Proxy, and UCS Proxy (8.5) or UCS Node (9.1) clusters
2. Configuration Server Proxies

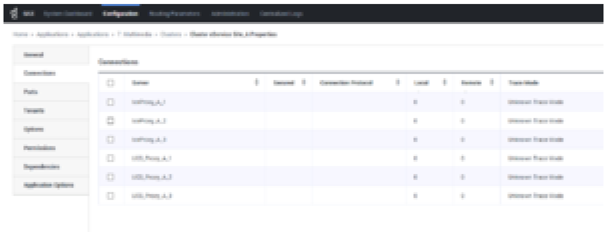
> **Important**
>
> For information about UCS 9.1 Nodes architecture, refer to the 9.1 Architecture topic in the *Universal Contact Server Deployment Guide*. [**Added:** 8.5.126.07]

Please refer to the Business Continuity page for details about how to provision as many clusters as business continuity sites.

## Provisioning clusters for Stat Servers, Interaction Server Proxies, and UCS proxies or nodes

Using clusters, Workspace can enable Load Balancing between each server of same type.

To enable Load Balancing through clusters, Workspace takes advantage of the Application Cluster in Genesys Management Framework (a pool of servers that can be of different types; for example, UCS Proxies (8.5) or UCS Nodes (9.1), Interaction Server Proxies and Statistic Servers). This model provisions server pools for the Interaction Server Proxy, UCS Proxy (8.5) or UCS Node (9.1), Stat Servers connections types. The Application Cluster model also enables the support of various scale factors that depend on the application type (for example, three Interaction Server Proxy nodes for eServices agents and six UCS Proxy (8.5) or UCS Node (9.1) clusters for eServices agents and Voice agents). The following figure shows an example of how an application cluster might be configured in Genesys Administrator Extension:



Connections

| □ | Server | Secured | Connection Protocol | Local | Remote | Trace Mode |
|---|---|---|---|---|---|---|
| □ | IxnProxy_A_1 | | | 0 | 0 | Unknown Trace Mode |
| □ | IxnProxy_A_2 | | | 0 | 0 | Unknown Trace Mode |
| □ | IxnProxy_A_3 | | | 0 | 0 | Unknown Trace Mode |
| □ | UCS_Proxy_A_1 | | | 0 | 0 | Unknown Trace Mode |
| □ | UCS_Proxy_A_2 | | | 0 | 0 | Unknown Trace Mode |
| □ | UCS_Proxy_A_3 | | | 0 | 0 | Unknown Trace Mode |

> ### Important
> Workspace employs a Cryptographically secure pseudo-random number generator (CSPRNG) to select the next node to ensure the best load balancing between all Workspace instances.

## Procedure

### Creating a cluster for Workspace

**Purpose:**

To enable Business Continuity for Statistic Server, Interaction Server Proxy, or Universal Contact Server Proxy (8.5), or Universal Contact Server Node (9.1) clusters in Workspace.

**Start**

1. Be sure to have ApplicationCluster template in Genesys Administrator Extension. if you don't have such application template, either import it from eService Interaction Management CD or create an empty template from scratch using "Application template" type.
2. Create a new application based on application cluster template
3. In connections, add all Stat Servers, Interaction Server Proxies, and UCS Proxies (or UCS Nodes) you want to load balance
4. In Server Info tab, select the tenant (ignored by Workspace) and a fake host and port (this information will not be used by Workspace), also working directory and command line can be filled with some fake chars
5. Save Application Cluster
6. Add this Application Cluster to the Connections of your Workspace Desktop Edition application.

**End**

### ADDP

In Genesys Administrator Extension, you can define the cluster addp parameter for all applications in the cluster application from the Workspace application connections table. These parameters can be overridden in each server application.

### IP Version

You can define the `ip-version` option for all applications of the cluster from the Workspace application connections table. The `ip-version` option can be overridden in each server application object. For example, you could set the value of the `ip-version` options for each application of the cluster to `4,6`.

### Time interval for reconnection

Use the following two options (in Workspace application to make it global to all clusters or in Application Cluster annex, in section 'interaction-workspace') to specify the time interval for reconnection:

- `warm-standby.reconnection-random-delay-range`
- `warm-standby.retry-delay`

## Provisioning cluster for Configuration Server proxies

There are two approaches to provisioning Cluster for Configuration server, Cluster based on Network Load Balancer F5 BIGIP and Cluster based on Client Side Load Balancing.

### Cluster based on Network Load Balancer F5 BIGIP

This approach involves a hardware network load balancer that achieves a server-side load balancing and fault detection to equally distribute the connection load between up and running Configuration Server Proxies configured in a pool. In this approach Workspace applications physically connect to the Network Load Balancer, which is connected to all the Configuration Server Proxies of the pool.

Refer to Load-Balanced Configuration Server Proxies for Agent-Facing Applications in the Genesys Management Framework documentation. In an F5 BIGIP environment, Workspace is configured to connect to one or several External Configuration Server Proxy applications; these External Configuration Server Proxies are not connected to an actual Configuration Server, but instead point to the hardware network load balancers.

> **Important**
>
> - This approach requires Config Server 8.5.1
> - The `CSProxy/proxy-cluster-name` option should be set with the name of the External CS Proxy in each of the CS Proxy application that simulate a real CS Proxy executable
> - In this approach, the selection of the node of the cluster is done by the Network Load Balancer.

## Cluster based on Client-Side Load Balancing

Unlike network load balancing, the client-side random balancing approach relies on the statistical Law of Large Numbers to achieve equal distribution of Workspace instances between the Configuration Server Proxies. In this approach, Workspace instances are directly connected to the Configuration Server Proxy instance selected by the random algorithm.

### Procedure

### Creating a CS Proxy Cluster for Workspace

**Purpose:**

To enable Business Continuity for CS Proxy in Workspace.

**Prerequisites**

- The Configuration Server Proxies are created as individual Application objects of type ConfigurationServer Provisioning Configuration Server proxies. They do not have any backup instance, to ensure that all instances are independent from each other.

**Start**

1. Create a Fake Host object and set its LCA port to 0 (zero). It will not be used at runtime.
2. Configure another Application object of type `ConfigurationServer`, to create a Virtual Configuration Server Proxy that represents the Configuration Server Proxy cluster. Set its host using the fake host and assign it a fake port. `Host` and `Port` are not used at run-time. The Virtual Configuration Server Proxy object, representing the Configuration Server Proxy cluster, is not monitored by SCS.
3. In the options of the virtual Configuration Server Proxy application, create in the Section `interaction-workspace`:
   - A key-value pair for each Configuration Server Proxy that composes the cluster where:
     - Key is `cluster.nodes.<CS Proxy name>`, where <CS Proxy name> refers to a static name, used internally for reference to that node.
     - Value is `host:port` that represents the Configuration Server Proxy host and port.
   - The `cluster.environment-name` option with a name that represent the configuration environment name.
4. Add a connection in the Workspace application to this Virtual Configuration Server Proxy.
5. If you are using Configuration Server Proxy version 8.5 or higher, in the [csproxy] section of each Configuration Server Proxy in the proxy cluster, set the value of `proxy-cluster-name` to the name of the Virtual Configuration Server Proxy object. For more information about this option, refer to the *Framework Configuration Options Reference Manual*.

### TLS

To enable TLS, if available, specify `autodetect` Configuration Server Proxy ports in the definition of the cluster nodes through options `cluster.nodes.*`.

### Kerberos

To enable authentication of Workspace users through Kerberos, all Configuration Server Proxies must be configured with the same SPN and the same `.keytab` file.

> **Important**
>
> To run multiple Configuration Server Proxies configured with the same SPN on the same host, refer to Management Framework External Authentication Guide for details about how to set up redundant/clustered applications. This is not a restriction specific to the cluster model, but is applicable to any Configuration Server connection model from Workspace.

### ADDP

In Workspace Application table connection, you can define the connection protocol ADDP by specifying the addp parameter for the Virtual Configuration Server Proxy application.

### Time interval for reconnection

Use the following two options in Workspace Desktop Application to specify the time interval for reconnection:

- `warm-standby.reconnection-random-delay-range`
- `warm-standby.retry-delay`

`warm-standby.retry-delay` can be overriden in the Virtual Configuration Server Proxy

### Provision Bootstrap Configuration Cluster Settings in Workspace Configuration File

Genesys recommends that you edit the `InteractionWorkspace.exe.config` file that you deliver to agents to provide Configuration cluster information to the client for the first time that Workspace is launched in a Configuration Server Cluster environment. This static provisioning is making the first connection of a user from a new workstation more safe. This file is in the Workspace installation directory.

Edit or add the following keys:

- For Stand-alone deployment:

```
<appSettings>
  ...
  <add key="login.url" value="tcp://MyConfigurationEnvironment/ApplicationName" />
  <add key="login.cluster.nodes.MyConfigurationEnvironment"
 value="[CSP1Host:CSP1Port][CSP2Host:CSP2Port][CSP3Host:CSP3Port],Timeout=10" />
  ...
 </appSettings>
```

- For Business Continuity deployment:

```
<appSettings>
```

```
 ...
 <add key="login.url" value="tcp://MyConfigurationEnvironment/ApplicationName" />
 <add key="login.cluster.preferred-site.nodes.MyConfigurationEnvironment"
value="[CSP1Host:CSP1Port][CSP2Host:CSP2Port][CSP3Host:CSP3Port],Timeout=10" />
 <add key="login.cluster.peer-site.nodes.MyConfigurationEnvironment"
value="[CSP4Host:CSP4Port][CSP5Host:CSP5Port][CSP6Host:CSP6Port],Timeout=10" />
 ...
</appSettings>
```

Where:

- **MyConfigurationEnvironment**: The name of the Configuration Environment that is displayed in the **Login** window. For example: 'Production' or 'Staging'. This must be consistent with the `cluster.environment-name` configured in the Virtual Configuration Server Proxy application(s).
- **ApplicationName**: The name of the Workspace Desktop application in Management framework
- **CSP1Host:CSP1Port...**: The `host:port` pairs of your configuration server proxies defining the cluster.
- **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.

### Summary of connection flow

A combination of three sources is used to define the connection logic to the Configuration Server Proxy nodes.

When an agent logs in to a workstation for the first time:

1. A pre-defined configuration is read from the `Interactionworkspace.exe.config` file.
2. Workspace tries to connect to one of the nodes of Configuration Server Proxy according to one of the following logic: Primary/Backup with Disaster Recovery, Cluster with Disaster Recovery, Primary/Backup without Disaster Recovery, Cluster without Disaster Recovery.
3. Once Workspace is connected, it reads the virtual Configuration Server Proxy connection(s) information.
4. Store the current configuration in the `localUserSettings.conf` file for the next login from this Workstation.

When an agent logs in to a workstation for the second and subsequent times:

1. Workspace reads the configuration information stored in the `localUserSettings.conf` file. Stored settings have a configuration environment name.
2. Workspace reads the predefined configuration stored in the `Interactionworkspace.exe.config` file, which has a configuration environment name.
3. Workspace compares the configuration environment name, if they match, then Workspace uses the stored settings from the `localUserSettings.conf` file. If they do not match, Workspace uses the `Interactionworkspace.exe.config` file as if this is a first login situation.

Important

- Workspace employs a Cryptographically secure pseudo-random number generator (CSPRNG) to select the next node to ensure the best load balancing between all Workspace instances.
- In all cases, Workspace does not try to close the current Configuration Server Proxy node connection if it does not match the configuration.

# Customizing display names

[**Modified:** 8.5.109.16, 8.5.120.05, 8.5.143.08, WSEP 8.5.114.05]

[**Added:** 8.5.101.14]

Workspace uses the `display-format.*` configuration options to enable you to customize how different interface elements are displayed to agents. They are also used to customize the display names of Framework objects, such as Routing Points and Queues, in the agent interface.

> **Tip**
>
> This article is a work in progress. Additional use cases and examples will be added in the future.

## Customizing display names for configuration objects

The `display-format.*` configuration options enable you to specify the data source for the display names of different objects. For example:

1. System attributes of configuration objects (for example, Routing Point Number or Agent Group Name)
2. Custom Display names defined in custom dictionary files
3. Custom Display names defined in the object Annex
4. If none of the defined sources contain an actual string to display, Workspace displays the mandatory attribute value that is identified as the default for a particular object (for example, 'Number' for a DN).

You can use the `display-format.*` options to define multiple sources, separated by the ‘|’ character, which specifies the precedence order of the sources. Precedence order if from left to right. If nothing is defined for the first source, the next one is checked, and so on.

### Configuring object display names using custom dictionary files

[**Added:** 8.5.101.14]

Starting with Workspace 8.5.100x.xx, the list of field codes for these options is extended to take local dictionary entries into account. For example, for the `display-format.routing-point.name` option, the following key is supported: `$RoutingPoint.DictionaryValue$`. This key selects the name for the routing point based on the value specified for it in the language dictionary file.

For the display-format.action-code.name option, if the `$ActionCode.DictionaryValue$` key is specified, then the value for the action code will be selected from the dictionary that corresponds to the language that the agent specified at login.

For example, in `custom.en-US.xml`, the action code might be specified as:

```
{code}
<Value Id="ActionCode.Break" Text="Break"/>
{code}
```

And, in `custom.fr-FR.xml`, the same action code might be specified as:

```
{code}
<Value Id="ActionCode.Break" Text="Pause"/>
{code}
```

The following is an example of a custom dictionary that specifies alternate text for configuration objects:

```
<?xml version="1.0" encoding="utf-8" ?>
<Dictionary EnglishName="English" CultureName="English" Culture="en-US">
 <!-- [<Tenant>].<object-type>.[<switch>].<object-identifier> (where [<Tenant>] and
[<switch>] are optional) -->

 <Value Id="defaultTenant.RoutingPoint.LucentG3.122" Text="Routing Point 122" />
 <Value Id="defaultTenant.ACDQueue.LucentG3.80001" Text="ACD Queue 80001" />
 <Value Id="defaultTenant.InteractionQueue.any-queue-to-agent-group-8002" Text="Interaction
Queue for Agent Group 8002" />
 <Value Id="defaultTenant.InteractionQueue.email-routing-queue-inbound" Text="Interaction
Queue for inbound emails" />
 <Value Id="defaultTenant.ActionCode.Break" Text="Coffee Break" />
 <Value Id="defaultTenant.Workbin.email-draft-wb" Text="Rough copy Emails" />
 <Value Id="defaultTenant.BusinessAttribute.DispositionCode" Text="Disposal Code" />
 <Value Id="defaultTenant.BusinessAttribute.DispositionCode.DC_Accepted" Text="Taken" />
 <Value Id="defaultTenant.Skill.Email-QualityConfidencePercentageSkill" Text="Email skill" />
 <Value Id="defaultTenant.AgentGroup.Agent Group 80001" Text="Lucent Agent Group 80001" />
</Dictionary>
```

## Configuring display names in the Object Annex

[**Added:** 8.5.109.16] [**Modified:** 8.5.120.05, WSEP 8.5.114.05]

You can add a display name for certain configuration layer objects. This feature enables you to name objects without relying on a local dictionary file. This feature makes localization and centralization more efficient.

This method provides a way to configure the display name centrally instead of locally in a dictionary file by enabling you to specify key-value pairs in object Annex. Key-value pairs can be defined for a default language and for localization in alternative languages.

### Important

To store a display name in an object Annex as a string value that does not use the character set that is used by Configuration Server, Configuration Server 8.1.3 or higher must be installed and its multi-language capability must be enabled. For example, using French accented characters in a U.S. English deployment or using Korean characters in a Japanese deployment. Refer to Deploying Genesys for Key Mixed Language Scenarios for information about supporting multi-language deployment.

For each object, the default display name is defined by using the `interaction-workspace/display-name` = <value> key-value pair.

For each object, additional language display names are defined by using the `interaction-workspace/display-name.<ISO_language_code>-<ISO_country_code>` = <value> key-value pair (for example, `display-name.fr-CA` for French Canadian.

The following precedence rules are followed for display names:

- If a particular object type is configured to be displayed through the configuration Annex, Workspace tries at runtime to find a key-value pair that matches the locale that selected by the agent at login time.
- If no match is found, Workspace uses the default `display-name=value` key-value pair.
- If no default key-value pair is found, Workspace the value that is defined by the `display-format.*` options.

The following is an example of a display name in two different languages, the default, and French (France), that could be defined in the object Annex of a Routing Point:

- `interaction-workspace/display-name = 'Technical Support Queue'`: Used if there is no matching language specific entry for the locale selected by the agent in the login window.
- `interaction-workspace/display-name.fr-FR = 'File d'Attente du Support Technique'`: Used if the locale selected by the agent in login window is French (France) (fr-FR)

Use the display-format.folder.name option to specify the display format of folders that are displayed in the Disposition Code and Case Data views. You can localize the folder name using the `$Folder.Name$` parameter. [**Added:** 8.5.120.05, WSEP 8.5.114.05]

## Summary of Display Format options

[**Modified:** 8.5.109.16]

The table **Summary of Display Format Options** contains descriptions of all of the new and updated display-format configuration options that use the Dictionary Value keys to support this feature.

**Summary of Display Format Options**

| Object Type | Option Name | Field codes to be used in display-format.* options | Dictionary Key Format to be spcified in the XML dictionary if the $DictionaryValue$ is specified in display-format.* options | Views affected by this option |
|---|---|---|---|---|
| DN - ACD Queue | display-format.acd-queue.name | $ACDQueue.DictionaryValue$,<br>$ACDQueue.AnnexValue$ | [<Tenant>].ACDQueue.<switch>.<dn-number> | Team Communicator<br>Login views |

| Object Type | Option Name | Field codes to be used in display-format.* options | Dictionary Key Format to be spcified in the XML dictionary if the $DictionaryValue$ is specified in display-format.* options | Views affected by this option |
|---|---|---|---|---|
| Action Code | display-format.action-code.name | $ActionCode.DictionaryValue$, $ActionCode.AnnexValue$ | [<Tenant>].ActionCode.<action-code-name> | Global Agent Status Control (tooltip + drop down menu)<br>My Channels view |
| Agent Group | display-format.agent-group.name | $AgentGroup.DictionaryValue$, $AgentGroup.AnnexValue$ | [<Tenant>].AgentGroup.<agent-group-name> | Team Communicator<br>My Statistics<br>Voice Mail (shared voice mail boxes) |
| Business Attribute | display-format.business-attribute.name | $BusinessAttribute.DictionaryValue$, $BusinessAttribute.AnnexValue$ | [<Tenant>].BusinessAttribute.<business-attribute-name> | Interaction View (Case Information, Disposition Code)<br>Contact Directory<br>Contact Profile<br>Contact History (detail - case data) |
| Business Attribute | display-format.business-attribute.name | $BusinessAttribute.DictionaryValue$, $BusinessAttribute.AnnexValue$ | [<Tenant>].BusinessAttribute.<business-attribute-name> | Interaction View (Case Information, Disposition Code)<br>Contact Directory<br>Contact Profile<br>Contact History (detail - case data)<br>Media type (login, my channels, agent status, and so on) |
| Business Attribute Value | | | [<Tenant>].BusinessAttribute.<business-attribute name>.<business-attribute-value-name> | |
| Folder | display-format.folder.name | $Folder.AnnexValue$, $Folder.DictionaryValue$, $Folder.Name$ | | Interaction View (Disposition Code, enum-tree KVP in Case Information and Outbound |

| Object Type | Option Name | Field codes to be used in display-format.* options | Dictionary Key Format to be spcified in the XML dictionary if the $DictionaryValue$ is specified in display-format.* options | Views affected by this option |
|---|---|---|---|---|
| | | | | Record) |
| Script - Interaction Queue | display-format.interaction-queue.name | $InteractionQueue.DictionaryValue$,<br>$InteractionQueue.AnnexValue$ | [<Tenant>].InteractionQueue.<script-name> | Team Communicator<br>Workbins view (My Interaction Queues) |
| DN - Routing Point | display-format.routing-point.name | $RoutingPoint.DictionaryValue$,<br>$RoutingPoint.AnnexValue$ | [<Tenant>].RoutingPoint.<switch>.<dn-number> | Team Communicator<br>Login views |
| Skill | display-format.skill.name | $Skill.DictionaryValue$,<br>$Skill.AnnexValue$ | [<Tenant>].Skill.<skill-name> | Team Communicator |
| DN - Virtual Queues | display-format.virtual-queue.name | $VirtualQueue.DictionaryValue$,<br>$VirtualQueue.AnnexValue$ | [<Tenant>].VirtualQueue.<switch>.<dn-number> | Login Views |
| Script - Interaction Workbin | display-format.workbin.name | $Workbin.DictionaryValue$,<br>$Workbin.AnnexValue$ | [<Tenant>].Workbin.<script-name> | Workbins view (My Workbin, My Team Workbins) |

## Masking a contact's phone number on inbound and outbound interaction views

[**Added:** 8.5.143.08]

Protecting the security and privacy of contacts is an important consideration, especially if you have agents who are working from home. You can use the configuration options in this section to hide the contact's phone number in the Interaction window. You can modify the default values of the configuration options that control the contact information that is displayed in inbound and outbound interactions. Workspace also supports plain text instead of field codes in the values of the following options:

- display-format.caller-name
- display-format.case-name-format
- display-format.customer-name-format
- display-format.interaction-callback-name
- display-format.interaction-outbound-pull-preview-name

- display-format.interaction-voice-name
- display-format.party-name-format
- interaction.window-title

For example, you can modify the default value of display-format.caller-name to replace `$Interaction.MainParty$` with plain text such as XXXXXXXXXXX or `Hidden Phone Number`.

For Outbound interactions, use the following configuration options and replace the `$OutboundRecord.PhoneNumber$` value with plain text to modify what your agents see in the Outbound interaction view:

- display-format.outbound-record-name: Specifies how an Outbound Record from a Record Chain is displayed when presented to an agent. The content is populated based on record attributes by a string that contains the following field codes: `$OutboundRecord.PhoneType$`, `$OutboundRecord.PhoneNumber$`,`$OutboundRecordField.X$`, where `X` is the name of the custom outbound field. [**Added:** 8.5.143.08]
- display-format.caller-name: Specifies the content of the 'Origin' field of the Case Information area. This option is enabled when the value of the interaction.case-data.content option contains the `History` key. This content is typically used when placing an outbound call where the origin contains a string such as "outbound call to xxx". The content is populated based on attached data keys or contact attributes (if there is a contact) or outbound record fields (if there is an outbound record) that are defined by a string that contains the following field codes: `$Interaction.CaseId$`,`$Interaction.MainParty$`, `$Contact.X$`,`$AttachedData.Y$`,`$OutboundRecord.PhoneType$`,`$OutboundRecord.PhoneNumber$`, `$OutboundRecordField.Z$`, where `X` is the name of contact attribute, `Y` is the attached data key name, and `Z` is the name of custom outbound field. If the values of the default field codes are empty, the following field code is used: `$Interaction.MainParty$`.

[**Modified:** 8.5.143.08]

# Supported systems and switches

[**Modified:** 8.5.116.10]

## Supported systems

Refer to the Workspace Desktop Edition topics and the Workspace SIP Endpoint topics in the Genesys Supported Operating Environment Reference Guide.

For information about Virtual Desktop Infrastucture (for example: RDP, VMWare, XenApp, XenDesktop), refer to the Genesys Virtualization Platform Support topics in the *Genesys Supported Operating Environment Reference Guide*.

## Supported switches

The following switches are supported:

- Avaya Communication Server
- Alcatel OmniPCX Enterprise (OXE)/A4400
- Cisco CallManager (CM) IP PBX
- EADS Telecom Intecom E Series
- EADS Telecom Intecom M6880 PointSpan
- Ericsson MD110
- Ericsson MX-ONE
- NEC Small TDM
- NEC Large TDM
- NEC Small Hybrid
- NEC Large Hybrid
- NEC SV7000
- Nortel Communication Server 1000
- Nortel Communication Server 2000/2100
- SIP Server
- Spectrum
- Siemens HiPath 4000 v (including family: 4000, 4300, 4500, 4900)

See *Supported Operating Environment Reference Guide* for a list of switches that are supported by the Workspace Voice Section. To achieve full support of the following switches, configure the place at which the agent logs in as described in the following tables, for the following DN configurations.

> **Important**
>
> For information about configuring Statistic Server to report properly the status of destination Agents in the case they are logged in a Place configured with two DNs, refer to statserver Section in the RTME Options Reference.

**Place Configuration for Agent Login: 2 DNs (1 Extension and 1 Position)** [**Modified:** 8.5.116.10]

**Place Configuration for Agent Login: 2 DNs (1 Extension and 1 Position)**

| Switches | DN in Configuration Manager | Agent login in Configuration Manager | DN ID reflected |
|---|---|---|---|
| • Cisco CallManager (CM) IP PBX [**Added:** 8.5.116.10]<br>• Nortel Communication Server 1000 with SCCS/MLS (formerly Nortel Symposium and Nortel Meridian 1)<br>• Nortel Communication Server 2000/2100 (formerly DMS 100)NEC APEX (American Version)NEC SV7000 | 2 DNs:<br>• 1 Extension<br>• 1 ACD Position | No constraint | 1 Voice DN (ACD Position number) |

**Place Configuration for Agent Login: 1 DN or More**

**Place Configuration for Agent Login: 1 DN or More**

| Switches | DN in Configuration Manager | Agent login in Configuration Manager | DN ID reflected |
|---|---|---|---|
| • Ericsson MD110<br>• Ericsson MX-ONE<br>• NEC SV7000 | 1 DN or more:<br>• 1 Extension (ODN)<br>• n= 0/1 ACD Positions (ADN) | No constraint | 1 Voice DN (Extension number) |

### Place Configuration for Agent Login: 1 DN (1 Extension or 1 Position)

**Place Configuration for Agent Login: 1 DN (1 Extension or 1 Position)**

| Switches | DN in Configuration Manager | Agent login in Configuration Manager | DN ID reflected |
|---|---|---|---|
| • Avaya Definity G3<br>• Cisco CallManager (CM) IP PBX<br>• EADS Telecom M6500EADS (Intecom)<br>• EEADS (Intecom) Point Span<br>• Rockwell Spectrum<br>• Siemens HiPath 4000 CSTA 3<br>• SIP Server | 1 DN:<br>• 1 Extension *or*<br>• 1 ACD Position | No constraint | 1 Voice DN (Extension number or ACD Position number) |

### Place Configuration for Agent Login: Alcatel OmniPCX Enterprise (OXE)/A4400-specific

**Place Configuration for Agent Login: Alcatel OmniPCX Enterprise (OXE)/A4400-specific**

| Switches | DN in Configuration Manager | Agent login in Configuration Manager | DN ID reflected |
|---|---|---|---|
| • Alcatel OmniPCX Enterprise (OXE)/A4400 Agent Substitute | In switch:<br>• 1 Extension<br>• 1 ACD Position<br>In place:<br>• Shortcut to Extension only | LoginID equal to ACD Position number | `(T-server option: agent-substitute=true)` Extension if logged outPosition if logged in |
| Alcatel OmniPCX Enterprise (OXE)/A4400 Agent emulated | In switch:<br>• 1 Extension<br>In place:<br>• Shortcut to Extension | Not define position for login ID | `agent-substitute=true/false` |

> Tip
>
> In some cases, for some of the switches that are listed in the Table - **Place Configuration for Agent Login: 2 DNs (1 Extension and 1 Position)**, an agent cannot see all of the DNs in the place configuration; sometimes only one DN is visible that includes the features of all of the other DNs.

For some switches you must set the `spl.switch-policy-label` option in either the switch annex or the DN annex to specify the operating mode of the switch if it is different from the default mode chosen by Workspace.

Workspace automatically assigns the best switch policy for the switch that you are using. If you want to override the default policy, you can force Workspace to use a different policy.

## Section: interaction-workspace

### spl.switch-policy-label

[**Modified:** 8.5.116.10, 8.5.117.18]

Possible values:

- Default Value: Depends on Switching office type. The default value is only available if Workspace detects an ACD Position\Extension pair.
- Valid Values:
  - Nortel CS 1000 switch: `NortelMeridianCallCenter::MLS` (default), `NortelMeridianCallCenter::SCCS`
  - Nortel Communication Server 2000 switch: Valid Values: `NortelDMS100` (default), `NortelDMS100::PDNMode`
  - Cisco CallManager switch for 2 DNs configuration [**Added:** 8.5.116.10]: Valid Values:
    - `CiscoCM::MultiDN::Position` (default): `Position` is used for `ThisDn` for the `MakeCall` request.
    - `CiscoCM::MultiDN::Extension`: `Extension` is used for `ThisDn` for the `MakeCall` request.
  - Microsoft Lync Switch: `SIPSwitch::Lync`: Prevents Workspace from starting Workspace SIP Endpoint for Lync DNs and also applies the specific Switch Policy for Lync. This option is required in hybrid environments where agents are configured to work with Places that contain at least one Voice DN from SIP Server and one Voice DN from Lync TServer [**Added:** 8.5.117.18].

# Configuration Options Reference

## Important

For the most up to date information about Workspace configuration options, refer to the Genesys Configuration Options Database.

- Search for options
- Browse options

This article is an appendix of Workspace configuration options, grouped by Configuration Section. This category contains the following sections:

- Introduction To Configuration Options
- Section: interaction-workspace
- Section: interaction-queue-presence
- Section: queue-presence
- Section: routing-point-presence
- Section: KPIName
- Section: ObjectStatisticName
- Not Ready Reason Codes
- Role Privileges

## Important

All options in the interaction-workspace section can be defined hierarchically at the following levels:

- Application
- Tenant
- Agent Group
- User (agent)

As you move down the hierarchy, the option setting overrides the previous level. That means that the value that you set for a User overrides what has been configured for the same option at a higher level, such as the value specified for the Agent Group of which the agent is a member.

The values specified for many options can also be overridden by Routing Strategies that reference Transaction objects.

For detailed information on this topic, refer to Configuration And Administration By Using Options And Annexes.

# Introduction to configuration options

As with all other Genesys 8 applications, the Workspace configuration options are loaded into the configuration layer by using an XML metadata file that is delivered with Genesys Administrator Extension. Use Genesys Administrator Extension to view, access, and configure Workspace configuration options.

KPI and statistics options are not part of the XML metadata file, because they are not composed of fixed key names. To use the KPIs section, create as many option blocks as the number of KPIs that you want to declare. For details, see Section: KPIName. To use the Statistics section, create as many option blocks as the number of statistics that you want to declare. For details, see Section: ObjectStatisticName.

Lists of privileges are currently implemented as Boolean options in the Annex of individual agents (see Role Privileges). For information on how to secure your deployment, see the Security options that are contained in the *Genesys 8 Security Deployment Guide*. For general information on configuring and extension, refer to Configuration And Administration By Using Options And Annexes.

For general procedures on how to configure specific agent functionality, refer to Provisioning Functionality.

Some options can be configured on the Application, the Tenant, an Agent Group, or an Access Group, while others must be configured on a Person object in the Agent Annex. The description of each configuration option specifies to what object the option is applicable. Options that are specific to the Person object (Agent Annex) are listed separately in this appendix.

The security.disable-rbac configuration option in the `interaction-workspace` section determines whether agents have all privileges allowed or whether the Role Based Access Control (RBAC) control system is used. Refer to Role Privileges for a list of all the privileges.

> **Warning**
>
> RBAC requires Configuration Server 8.0.2 or higher.

Refer to *Genesys Administrator Extension Help* and *Genesys 8 Security Deployment Guide* for detailed information on how to use Genesys Administrator Extension and Management Framework to configure access permissions

# Section interaction-workspace

> **Tip**
>
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

These options can be configured on the following Configuration Layer objects:

- Workspace Application object
- Tenant
- Agent Group
- Agent

The options are grouped into the following categories:

- **Accessibility**: Options that enhance the application for hearing and visually impaired agents
- **Active Recording**: Options that control how agents use Active Call Recording and Screen Capture functionality.
- **Agent status**: Options that control how agents set their Ready status
- **Alert**: Options that control the display of warning messages.
- **Application**: Options that control the default window display behavior.
- **Broadcast**: Options that control how broadcast messages appear and behave
- **Business Continuity**: Options that control the behavior of Workspace during a long term loss of connection to the primary host site.
- **Callback Options**: Options that control the various features of the Callback view.
- **Case Data**: Options that control the display of Case Data.
- **Channel Information**: Options that control the display of the media prompt window.
- **Chat**: Options that control the appearance and behavior of the Chat interface
- **Chatserver**: Options that control the connectivity parameters, like ADDP settings, between Workspace and Chat Server.
- **Contact**: Options that control contact management
- **Disaster Recovery**: Options that control the behavior of Workspace during a long term loss of connection to the primary host site. See Business Continuity options.
- **Display formats**: Options that control the appearance of various text elements in the various application windows
- **E-Mail**: Options that control the appearance and behavior of the E-Mail interface

- **Editor**: Options that control the display of fonts in text editor boxes in Workspace.
- **eServices**: Options that control the use of eServices licenses
- **Expression**: Options that control the parsing of phone numbers in contact interaction
- **Statistics Gadget**: Options that control the use and appearance of the Statistics Gadget
- **General**: Options that control the general behavior of Workspace.
- **GUI**: Options that control the availability of themes in the user interface.
- **IM**: Options that control the appearance and behavior of the Internal Instant Messaging interface
- **Interaction**: Options that control the behavior and appearance of various elements related to the Interaction window
- **Interaction Bar**: Options that control the display of the Interaction Bar.
- **Interaction Management**: Options that control the way that Team Leads view and manage interactions in Queues and Workbins for their team members.
- **Intercommunication**: Options that control the routing of internal IM and voice interactions
- **Keyboard**: Options that enable keyboard shortcuts
- **KPI**: Options that control the display of My Statistics (KPIs) on the agent Workspace
- **License**: Options that control how Workspace interacts with License Reporting Manager.
- **Log**: Options that control logging of the application
- **Login**: Options that control the appearance and behavior of the agent login window
- **Logout**: Options that control the behavior of agent log out from Workspace.
- **Main view**: Options that control the behavior of the Main Window
- **Open Media**: Options that enable open media features
- **Options**: Options that specify where the agent object configuration is stored.
- **Outbound**: Options that enable agents to participate in outbound campaigns
- **Presence**: Options that control how agent presence is evaluated and displayed.
- **Printing**: Options that control the display of the Print Preview feature.
- **Reporting**: Otpions that specify how agent activities are reported to the Genesys back-end.
- **Security**: Options that control the timing and behavior of the keyboard and mouse inactivity timeout feature and other security features
- **SIP Endpoint**: Options that control the functionality and display of Workspace SIP Endpoint enabled interactions
- **Screen Recording**: Options that control the automatic Screen Recording functionality.
- **SMS**: Options that control the appearance and behavior of the SMS interface
- **Sounds**: Options that specify the name and location in the application folder of audio files that are to be pre-loaded when an agent logs in.
- **Spellchecker**: Options that control the use of corporate dictionaries in the spelling check feature
- **Standard Responses**: Options that control the functionality and display of the Response view
- **Statistics**: Options that control the display of contact center statistics on the agent Workspace

- **System Tray**: Options that control the display of the tooltip that is displayed in the System Tray.
- **Team Communicator**: Options that control the appearance and behavior of the Team Communicator
- **Team Lead**: Options that specify the scope of monitoring that is to be used for voice interactions in environments that use SIP Server or Cisco UCM
- **Toast (Interactive Notification)**: Options that control the appearance and behavior of the interaction preview Interactive Notification
- **View**: Options that control the tab order and activation order of windows and menus
- **Voice**: Options that control various features of the Voice channel
- **Voicemail**: Options that control access to your system voicemail
- **Web Callback**: Options that control the various features of the Web Callback channel
- **Webproxy**: Options that control the use of a Webproxy for environments where Internet proxies require user authentication
- **Workbin**: Options that control various features of Workbins
- **Workitem**: Options that control various features of the Workitem channel
- **Miscellaneous**: Options that control the appearance of the Workspace application windows, the recording of options, the evaluation of presence, the enabling of RBAC, and many other miscellaneous features

# <media-type> options

[**Modified:** 8.5.143.08]

> ## Tip
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

The following options can be configured for any supported media type in Workspace. When setting these options, replace <media-type> with the name of the media type you want to configure. For example, `chat.auto-answer`.

- <media-type>.auto-answer
- <media-type>.auto-answer.enable-reject
- <media-type>.auto-answer.timer
- <media-type>.contact-history.enable-combine-ixn-with-current [**Added:** 8.5.143.08]
- <media-type>.prompt-for-done
- <media-type>.pull-from-history-isenabled
- <media-type>.ringing-bell
- <media-type>.toast-information-key

## Related Resources

The following topics discuss the implementation of these options:

# Accessibility options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- accessibility.agent-state-change-bell
- accessibility.disable-hyperlinks
- accessibility.focus-on-interaction-toast
- accessibility.interaction-state-change-bell
- accessibility.visual-impairment-profile
- accessibility.warning-message-bell
- accessibility.<media-type>.focus-on-interaction-toast

## Related Resources

The following topics discuss the implementation of these options:

- Accessibility and navigation
- 8. Enabling accessibility features
- Workspace And Genesys 8

# Active Recording options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- active-recording.voice.recording-type
- active-recording.voice.recorder-uri

## Related Resources

The following topic discusses the implementation of these options:

- Call recording and screen recording

# Agent Status options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- agent-status.enabled-actions-by-channel
- agent-status.enabled-actions-global
- agent-status.not-ready-reasons

## Related Resources

The following topics discuss the implementation of these options:

- 6. Declaring and using new Not-Ready Reason codes
- Managing agent inactivity

# Alert options

> **Tip**
>
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- alert.timeout

## Related Resources

The following topic discusses the implementation of this option:

- 8. Enabling accessibility features

# Application options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- application.available-layouts
- application.secondary-audio-out-device
- application.wiki-help-locale
- application.wiki-help-welcome-page

# Broadcast options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- broadcast.color.minimal-priority
- broadcast.color.low-priority
- broadcast.color.normal-priority
- broadcast.color.high-priority
- broadcast.color.important-priority
- broadcast.displayed-columns
- broadcast.dn
- broadcast.enable-removal
- broadcast.enable-removal-priority
- broadcast.mark-read-timeout
- broadcast.message-content
- broadcast.preview-timeout
- broadcast.sound.minimal-priority
- broadcast.sound.low-priority
- broadcast.sound.normal-priority
- broadcast.sound.high-priority
- broadcast.sound.important-priority
- broadcast.subscribed.topics
- broadcast.system-messages-auto-mark-read
- broadcast.toast-summary
- broadcast.value-business-attribute

## Related Resources

The following topics discuss the implementation of these options:

- Broadcast Messages

- Broadcast Message privileges
- 5. Enabling Workspace to play ring tones

# Business Continuity options

> **Tip**
>
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

Options that have the `disaster-recovery.*` prefix are used to configure the Business Continuity functionality.

- disaster-recovery.auto-restore
- disaster-recovery.disable-login-errors
- disaster-recovery.enabled
- disaster-recovery.eservices-random-delay-range
- disaster-recovery.eservices-site
- disaster-recovery.peer-site
- disaster-recovery.preferred-site
- disaster-recovery.restore-agent-state
- disaster-recovery.timeout
- disaster-recovery.wait-for-sipphone-timeout

## Related Resources

The following topics discuss the implementation of these options:

- Business Continuity for SIP Server, Configuration Server, and Statistic Server
- eServices Business Continuity with UCS 9.1
- eServices Business Continuity with UCS 8.5
- 4. Pre-Defining HA for Configuration Server
- Load Balancing using clusters

# Callback options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- callback.callback-information.content
- callback.callback-information.frame-color
- callback.callback-information.header-foreground-color
- callback.callback-types-business-attribute
- callback.gms-url
- callback.ringing-bell

## Related Resources

The following topics discuss the implementation of these options:

- Callback
- Callback privileges
- Web Callback
- Web Callback options
- Web Callback privileges
- Outbound campaigns
- Outbound options

# Case Data options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- case-data.float-separator

## Related Resources

The following topics discuss the implementation of these options:

- Case Data
- Case Information editing

# Channel Information options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- channel-information.window-title

# Chat options

## Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- chat.agent.prompt-color
- chat.agent.text-color
- chat.attachment-download-timeout
- chat.auto-answer
- chat.auto-answer.enable-reject
- chat.auto-answer.timer
- chat.auto-mark-done-non-owner-agent
- chat.auto-mark-done-non-owner-agent.timer
- chat.auto-mark-done-owner-agent
- chat.auto-mark-done-owner-agent.timer
- chat.client.prompt-color
- chat.client.text-color
- chat.emojis-business-attribute
- chat.enable-auto-disconnect
- chat.historical.maximum-age
- chat.max-attachments-files
- chat.max-attachments-size
- chat.max-file-size
- chat.new-message-bell
- chat.nickname
- chat.on-hold-queue
- chat.other-agent.prompt-color
- chat.other-agent.text-color
- chat.pending-response-to-customer
- chat.pending-response-to-customer-bell
- chat.prompt-for-end

- chat.reconnect-attempts
- chat.reconnect-timeout
- chat.restricted-attachment-file-types
- chat.ringing-bell
- chat.show-attachment-image-thumbnail
- chat.show-unread-notification
- chat.simple-transcript
- chat.system.text-color
- chat.time-stamp
- chat.toast-information-key
- chat.transcript-enable-history-filters
- chat.typing-isenabled
- chat.typing-timeout

## Related Resources

The following topics discuss the implementation of these options:

- Chat
- MonitoringChatInteractions
- Chat Server options
- Chat privileges

# Chat Server options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- chatserver.addp.local-timeout
- chatserver.addp.remote-timeout
- chatserver.addp.trace-mode

## Related Resources

The following topics discuss the implementation of these options:

- Configuring the Workspace application object
- Load Balancing using clusters
- eServices Business Continuity with UCS 9.1
- eServices Business Continuity with UCS 8.5
- Chat
- Chat options
- Chat privileges

# Contact options

[**Modified:** 8.5.144.05]

> ### Tip
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- contact.all-interactions-default-time-filter-main
- contact.all-interactions-displayed-columns
- contact.all-interactions-displayed-columns-treeview
- contact.all-interactions-quick-search-attributes
- contact.available-directory-page-sizes
- contact.cache-timeout-delay
- contact.date-search-types
- contact.default-directory-page-size
- contact.directory-advanced-default
- contact.directory-auto-append-star-to-search
- contact.directory-default-mode
- contact.directory-displayed-columns
- contact.directory-enabled-modes
- contact.directory-permissions.<ContactAttributeName>
- contact.directory-search-attributes
- contact.directory-search-types
- contact.displayed-attributes
- contact.editable-attributes
- contact.history-auto-append-star-to-search
- contact.history-custom-attributes-search-types
- contact.history.filters-<attribute>
- contact.history.highlight-current-interaction
- contact.history.media-filters
- contact.history-advanced-default
- contact.history-custom-attribute-values.<attribute-name>
- contact.history-default-time-filter-main
- contact.history-displayed-columns
- contact.history-displayed-columns-treeview
- contact.history-quick-search-attributes
- contact.history-search-attributes
- contact.history-search-attribute-group.<group-name>
- contact.history.voice-detail-attributes
- contact.last-called-agent.enable
- contact.last-called-agent.<media-type>.enable
- contact.lookup.auto-assign-mode
- contact.lookup.enable
- contact.lookup.enable-create-contact
- contact.lookup.<media-type>.auto-assign-mode
- contact.lookup.<media-type>.enable
- contact.lookup.<media-type>.enable-create-contact
- contact.lookup.voice.use-dialed-phone-number
- contact.mandatory-attributes
- contact.metrics.enable-interactions-in-progress
- contact.metrics.time-frame-customer-notification
- contact.multiple-value-attributes
- contact.myhistory-default-time-filter-main

- contact.myhistory-displayed-columns
- contact.myhistory-displayed-columns-treeview
- contact.myhistory-quick-search-attributes
- contact.threading-ucs-interaction.enable
- contact.timeout-delay
- contact.ucs-interaction.<media-type>.enable-create
- contact.ucs-interaction.<media-type>.enable-lookup
- contact.ucs-interaction.<media-type>.use-server-date

## Related Resources

The following topics discuss the implementation of these options:

- Exposing Contacts to Agents
- Exposing History to agents
- Triggering contact look-up and populating History
- Contact Management privileges

# Display Format options

[**Moadified:** 8.5.143.08, 8.5.144.05]

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- display-format.acd-queue.name
- display-format.action-code.name
- display-format.agent-group.name
- display-format.agent-name
- display-format.business-attribute.name
- display-format.caller-name
- display-format.case-name-format
- display-format.chat-agent-name
- display-format.contact-name
- contact.multi-value-attribute-display.<contact-attribute>
- display-format.current-agent-name
- display-format.customer-name-format
- display-format.field.name
- display-format.folder.name
- display-format.interaction-callback-name
- display-format.interaction-chat-name
- display-format.interaction-email-name
- display-format.interaction-im-name
- display-format.interaction-outbound-pull-preview-name
- display-format.interaction-outbound-push-preview-name
- display-format.interaction-queue.name
- display-format.interaction-sms-name
- display-format.interaction-voice-name
- display-format.interaction-workitem-name
- display-format.outbound-record-name
- display-format.party-name-format
- display-format.routing-point.name
- display-format.skill.name
- display-format.virtual-queue.name
- display-format.workbin.name

## Related Resources

The following topic discusses the implementation of these options:

- Customizing display names for configuration objects

# Email options

[**Modified:** 8.5.143.08]

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- email.attachment-download-timeout
- email.auto-answer
- email.auto-answer.enable-reject
- email.auto-answer.timer
- email.can-change-text-direction
- email.default-queue
- email.forward.enable-cc-addresses
- email.forward.enable-instructions
- email.forward.enable-multiple-to-addresses
- email.forward-queue
- email.from-addresses
- email.from-addresses.force-default-on-reply
- email.html-format
- email.include-original-text-in-reply
- email.include-standard-response-subject-on-insert
- email.inline-forward-prefix
- email.inline-forward-queue
- email.mandatory-subject
- email.max-attachments-size
- email.move-inbound-to-in-progress-workbin-on-reply
- email.outbound.copy-editable-case-data-in-inbound
- email.outbound-queue
- email.outbound.editable-bcc-addresses
- email.outbound.editable-cc-addresses
- email.outbound.editable-to-addresses
- email.prompt-for-done
- email.pull-from-history-isenabled
- email.qa-review-dispositions-business-attribute
- email.quote-char
- email.quote-header
- email.reply-copy-category-id
- email.reply-format
- email.reply-prefix
- email.restricted-attachment-file-types
- email.resend-prefix
- email.ringing-bell
- email.set-ownerid-on-send
- email.signature
- email.toast-information-key

## Related Resources

The following topics discuss the implementation of these options:

- Email
- E-Mail Privileges
- Email Quality Assurance

# Editor options

> **Tip**
>
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- editor.font-size-units
- editor.shortcuts.prefix
- editor.user-agent-http-header

# eServices Options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- eservices.disconnect-on-logoff
- eservices.session-restore-mediatype
- eservices.session-restore-timeout

## Related Resources

The following topics discuss the implementation of these options:

- eServices Business Continuity with UCS 9.1
- eServices Business Continuity with UCS 8.5

# Expression options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- expression.callable-phone-number
- expression.email-address
- expression.outbound-campaign-phone-number
- expression.phone-number
- expression.phone-number.supported-characters
- expression.team-communicator-phone-number
- expression.url

## Related Resources

The following topics discuss the implementation of these options:

- Email
- Setting up manual dialing of alternate numbers
- 4. Provisioning a hybrid voice agent

# Statistics Gadget options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- gadget-statistics.displayed-call-center-statistics
- gadget-statistics.displayed-kpis
- gadget-statistics.nb-tagged-stats-per-page
- gadget-statistics.show

## Related Resources

The following topics discuss the implementation of these options:

- 3. Enabling an agent to view My Statistics and Contact Center Statistics in the Statistics Gadget
- Statistics privileges

# General options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- general.configuration-agent-collection-loading-method
- general.configuration-business-attribute-cache-preload
- general.configuration-object-collection-cache-timeout
- general.configuration-transaction-cache-preload
- general.configuration-update-notification
- general.gad.attached-data
- general.non-unicode-connection-encoding
- general.restricted-attachment-file-content-types
- general.writable-downloaded-attachment-file-types
- general.configuration-object-path-folder-id.enabled

# GUI options

> ### Tip
>
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- gui.editor-zoom-range
- gui.emoji-font-name
- gui.magnification-factor
- gui.themes

## Related Resources

The following topics discuss the implementation of these options:

- Accessibility and navigation
- Setting up agents on the system
- Chat

# IM options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- im.agent.prompt-color
- im.agent.text-color
- im.auto-answer
- im.new-message-bell
- im.other-agent.prompt-color
- im.other-agent.text-color
- im.prompt-for-end
- im.ringing-bell
- im.simple-transcript
- im.system.text-color
- im.time-stamp
- im.toast-timeout

## Related Resources

The following topics discuss the implementation of these options:

- Instant Messaging
- Communicating inside your business
- IM privileges

# Interaction options

## Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- interaction.auto-focus
- interaction.auto-focus.<media-type>
- interaction.case-data.content
- interaction.case-data.enable-url-preview
- interaction.case-data.format-business-attribute
- interaction.case-data.frame-color
- interaction.case-data.header-foreground-color
- interaction.case-data.is-read-only-on-idle
- interaction.consult-user-data
- interaction.disposition.display-mode
- interaction.disposition.email.mandatory-actions
- interaction.disposition.is-mandatory
- interaction.disposition.is-read-only-on-idle
- interaction.disposition.key-name
- interaction.disposition.use-attached-data
- interaction.disposition.use-connection-id
- interaction.disposition.value-business-attribute
- interaction.evaluate-real-party-for-agent
- interaction.evaluate-real-party-for-agent.expression
- interaction.override-option-key
- interaction.reject-route
- interaction.unconditional-force-close
- interactions.window.allows-transparency-on-winos6
- interaction.window.popup-topmost-z-order
- interaction.window.show-case-interaction-panel-button
- interaction.window.show-in-taskbar

- interaction.window-title

## Related Resources

The following topics discuss the implementation of these options:

- Configuring the behavior of incoming interactions
- Reporting
- Case Data
- Workbin and Interaction Queue management
- Planning Your Deployment
- Disposition codes
- Overriding Workspace options
- Standard Responses Library
- Channels and interaction handling

# Interaction Bar options

## Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- interaction-bar.detail-tooltip.max-height
- interaction-bar.enable-quick-access
- interaction-bar.quick-access-auto-open
- interaction-bar.quick-access-auto-open.<media-type>
- interaction-bar.quick-access-modes
- interaction-bar.quick-access-modes.<media-type>

## Related Resources

The following topics discuss the implementation of these options:

- Interaction Bar
- Main Window privileges

# Interaction Management Options

### Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- interaction-management.available-interaction-page-sizes
- interaction-management.filters
- interaction-management.interactions-filter.displayed-columns
- interaction-management.snapshot-timeout-delay

## Related Resources

The following topics discuss the implementation of these options:

- Workbin and Interaction Queue management
- Interaction Management privileges

# Intercommunication options

> **Tip**
>
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- intercommunication.chat.conference.invite-timeout
- intercommunication.chat.queue
- intercommunication.chat.routing-based-actions
- intercommunication.chat.routing-based-targets
- intercommunication.email.queue
- intercommunication.email.routing-based-actions
- intercommunication.email.routing-based-targets
- intercommunication.im.routing-based-actions
- intercommunication.im.routing-based-targets
- intercommunication.im.routing-points
- intercommunication.sms.queue
- intercommunication.sms.routing-based-actions
- intercommunication.sms.routing-based-targets
- intercommunication.voice.routing-based-actions
- intercommunication.voice.routing-based-targets
- intercommunication.voice.routing-points
- intercommunication.voicemail.enabled-target-types
- intercommunication.voicemail.routing-points
- intercommunication.<media-type>.queue
- intercommunication.<media-type>.routing-based-actions
- intercommunication.<media-type>.routing-based-targets

## Related Resources

The following topics discuss the implementation of these options:

- Enabling Team Communicator calling features

- Instant Messaging
- Chat
- Email
- Voicemail

# Keyboard options

## Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

## Important

- Keyboard.**hotkey**.* options relate to keyboard shortcuts that have global workstation scope, meaning they can work while another application is in focus; therefore, they potentially conflict with hot keys subscribed by other applications in the system.
- Keyboard.**shortcut**.* options have Workspace Application scope. There is no conflict with shortcut keys of other applications, but Workspace must be in focus for these keyboard shortcuts to function.

- keyboard.hotkey.agent-not-ready
- keyboard.hotkey.agent-not-ready-with-reason.<action-code>
- keyboard.hotkey.agent-ready
- keyboard.hotkey.decrease-microphone-volume-active-sip-call
- keyboard.hotkey.decrease-speaker-volume-active-sip-call
- keyboard.hotkey.hold-active-call
- keyboard.hotkey.increase-microphone-volume-active-sip-call
- keyboard.hotkey.increase-speaker-volume-active-sip-call
- keyboard.hotkey.mute-microphone-active-sip-call
- keyboard.hotkey.mute-speaker-active-sip-call
- keyboard.hotkey.release-active-call
- keyboard.hotkey.toaster.accept
- keyboard.hotkey.toaster.decline
- keyboard.shortcut.action.help
- keyboard.shortcut.campaign.get-record
- keyboard.shortcut.contact.assigncontact
- keyboard.shortcut.contact.reset
- keyboard.shortcut.contact.save

- keyboard.shortcut.hamburger.open
- keyboard.shortcut.interaction.chat.conference
- keyboard.shortcut.interaction.chat.end
- keyboard.shortcut.interaction.chat.hold
- keyboard.shortcut.interaction.chat.transfer
- keyboard.shortcut.interaction.consult
- keyboard.shortcut.interaction.email.add-attachments
- keyboard.shortcut.interaction.email.delete
- keyboard.shortcut.interaction.email.forward
- keyboard.shortcut.interaction.email.inline-forward
- keyboard.shortcut.interaction.email.interim-send
- keyboard.shortcut.interaction.email.print
- keyboard.shortcut.interaction.email.put-back-to-origin-queue
- keyboard.shortcut.interaction.email.reply
- keyboard.shortcut.interaction.email.reply-all
- keyboard.shortcut.interaction.email.save
- keyboard.shortcut.interaction.email.save-in-workbin
- keyboard.shortcut.interaction.email.send
- keyboard.shortcut.interaction.email.transfer
- keyboard.shortcut.interaction.im.release
- keyboard.shortcut.interaction.mark-done
- keyboard.shortcut.interaction.preview.call-record
- keyboard.shortcut.interaction.preview.cancel-record
- keyboard.shortcut.interaction.preview.mark-done
- keyboard.shortcut.interaction.preview.mark-done-get-next
- keyboard.shortcut.interaction.preview.reject-record
- keyboard.shortcut.interaction.pull-preview.mark-done
- keyboard.shortcut.interaction.pull-preview.mark-done-get-next
- keyboard.shortcut.interaction.sms.delete
- keyboard.shortcut.interaction.sms.transfer
- keyboard.shortcut.interaction.voice.answer-call
- keyboard.shortcut.interaction.voice.hold-call
- keyboard.shortcut.interaction.voice.pause-recording-call
- keyboard.shortcut.interaction.voice.reconnect-call
- keyboard.shortcut.interaction.voice.release-call

- keyboard.shortcut.interaction.voice.resume-call
- keyboard.shortcut.interaction.voice.resume-recording-call
- keyboard.shortcut.interaction.voice.single-step-conference
- keyboard.shortcut.interaction.voice.single-step-transfer
- keyboard.shortcut.interaction.voice.start-recording-call
- keyboard.shortcut.interaction.voice.stop-recording-call
- keyboard.shortcut.interaction.webcallback.call-contact
- keyboard.shortcut.interaction.webcallback.mark-done
- keyboard.shortcut.interaction.workitem.move-to-workbin
- keyboard.shortcut.interaction.workitem.put-back-to-origin-queue
- keyboard.shortcut.interaction.workitem.transfer
- keyboard.shortcut.state.logout
- keyboard.shortcut.state.not-ready
- keyboard.shortcut.state.not-ready-after-call-work
- keyboard.shortcut.state.ready
- keyboard.shortcut.team-communicator.focus
- keyboard.shortcut.teamlead.chat.bargein
- keyboard.shortcut.teamlead.chat.stop-monitoring
- keyboard.shortcut.teamlead.stop-monitoring
- keyboard.shortcut.teamlead.voice.bargein
- keyboard.shortcut.teamlead.voice.stop-monitoring
- keyboard.shortcut.toaster.accept
- keyboard.shortcut.toaster.decline
- keyboard.shortcut.paste-text-only

## Related Resources

The following topics discuss the implementation of these options:

- Accessibility and navigation
- Configuring the appearance and content of the user interface
- Workspace And Genesys 8

# KPI options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- kpi.displayed-kpis
- kpi.refresh-time
- kpi.show-agent-groups

## Related Resources

The following topics discuss the implementation of these options:

- KPIs and Contact Center Statistics
- Section KPI Name
- Statistics Gadget options

# License options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- license.lrm-enabled

# Log options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- log.default-filter-type
- log.filter-data.<keyName>
- log.max-age
- log.PSDK
- log.PSDK.SwitchPolicy
- log.segment
- log.Trace
- log.verbose

## Related Resources

The following topics discuss the implementation of these options:

- Hiding selected data in logs

# Login options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- login.available-place-groups
- login.chat.auto-not-ready-reason
- login.chat.can-unactivate-channel
- login.chat.is-auto-ready
- login.default-place
- login.email.auto-not-ready-reason
- login.email.can-unactivate-channel
- login.email.is-auto-ready
- login.enable-login-without-channel
- login.enable-place-completion
- login.enable-same-agent-place
- login.im.auto-not-ready-reason
- login.im.available-queues
- login.im.can-unactivate-channel
- login.im.is-auto-ready
- login.im.prompt-agent-login-id
- login.im.prompt-dn-password
- login.im.prompt-queue
- login.place-location-source
- login.place-selection-type
- login.place-state-timeout
- login.prompt-place
- login.sms.auto-not-ready-reason
- login.sms.can-unactivate-channel
- login.sms.is-auto-ready
- login.store-recent-place

- login.store-username
- login.voice.auto-not-ready-reason
- login.voice.available-queues
- login.voice.can-unactivate-channel
- login.voice.force-relogin
- login.voice.is-auto-ready
- login.voice.prompt-agent-login-id
- login.voice.prompt-dn-less-phone-number
- login.voice.prompt-dn-password
- login.voice.prompt-queue
- login.voice.use-dn-less-login-extension
- login.webcallback.auto-not-ready-reason
- login.webcallback.can-unactivate-channel
- login.webcallback.is-auto-ready
- login.workmode
- login.<media-type>.auto-not-ready-reason
- login.<media-type>.can-unactivate-channel
- login.<media-type>.is-auto-ready

## Related Resources

The following topic discusses the implementation of these options:

- Agent login, authentication, and logout

# Logout options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- logout.enable-exit-on-logoff-error
- logout.voice.use-login-queue-on-logout

## Related Resources

The following topic discusses the implementation of these options:

- Agent login, authentication, and logout

# Main Window options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- main-window.auto-hide-display-delay
- main-window.bypass-auto-hide-conditions
- main-window.window-title

## Related Resources

The following topics discuss the implementation of these options:

- Configuring the appearance and content of the user interface
- Main Window privileges

# Open Media options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- openmedia.bundle.sms
- openmedia.workitem-channels

## Related Resources

The following topics discuss the implementation of these options:

- Workitems
- SMS and MMS

# Options options

## Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- options.clean-up-former-record-location
- options.record-location
- options.record-option-locally-only

## Related Resources

The following topics discuss the implementation of these options:

- Configuring the appearance and content of the user interface
- Setting up agents on the system
- Planning Your Deployment
- Chat

# Outbound options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- outbound-callback.ringing-bell
- outbound.callback-types
- outbound.call-result-is-mandatory
- outbound.call-result-values
- outbound.campaign-stale-timeout
- outbound.complete-record-before-transfer
- outbound.fields.float-separator-in-db
- outbound.load-at-startup
- outbound.push-preview.auto-answer
- outbound.push-preview.auto-answer.enable-reject
- outbound.push-preview.auto-answer.timer
- outbound.push-preview.media-types
- outbound.record-information.frame-color
- outbound.record-information.header-foreground-color
- outbound.reschedule-inherit-parent-availability-interval
- outbound.sound.campaign-updated
- outbound.timed-preview-auto-dial
- outbound.treatment-mode
- <media-type>.ringing-bell

## Related Resources

The following topic discusses the implementation of these options:

- Outbound campaigns

# Presence options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- presence.evaluate-presence

# Printing options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- printing.use-print-preview

## Related Resources

The following topics discuss the implementation of this options:

- Email
- E-Mail Privileges

# Reporting options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- reporting.case.report-case-in-focus-duration

## Related Resources

The following topic discusses the implementation of these options:

- Reporting

# Screen Recording options

[**Modified:** 8.5.143.08]

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- screen-recording.client.address [**Added:** 8.5.143.08]
- screen-recording.client.max-attempts
- screen-recording.client.ping-interval
- screen-recording.client.port
- screen-recording.client.secure-connection
- screen-recording.htcc.peer_uri
- screen-recording.htcc.uri

## Related Resources

The following topics discuss the implementation of these options:

- Call recording and screen recording
- Recording privileges

# Security options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- security.client-authentication-certificate-search-value
- security.disable-rbac
- security.enable-debug-information
- security.inactivity-force-not-ready-state
- security.inactivity-not-ready-reason
- security.inactivity-set-agent-not-ready
- security.inactivity-timeout
- security.session-lock-force-not-ready-state
- security.session-lock-not-ready-reason
- security.session-lock-set-agent-not-ready

## Related Resources

The following topics discuss the implementation of these options:

- Agent login, authentication, and logout
- Configuring system-access permissions
- Deployment overview
- Deployment prerequisites
- Managing agent inactivity
- Setting up agents on the system
- Client-side port security
- Security privileges

# Workspace SIP Endpoint options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

Important

Significant changes are made to the SIP Endpoint configuration options between SIP Endpoint 8.0.2 and SIP Endpoint 8.5.0. For a list of the changes, refer to the **SIP Endpoint 8.0.2 versus SIP Endpoint 8.5.0 options** table. If you want to continue to use Interaction Workspace SIP Endpoint 8.0.2, use the configuration options that are described in the *Interaction Workspace 8.1.4 Deployment Guide*.

- sipendpoint.authenticate-with-dn-password
- sipendpoint.codecs.g729/8000.fmtp
- sipendpoint.codecs.h264.fmtp
- sipendpoint.core-deadlock-detection-delay
- sipendpoint.exit-on-voice-logoff
- sipendpoint.headset-enforce-configured-usage
- sipendpoint.headset-unplugged-set-not-ready
- sipendpoint.headset-unplugged.not-ready-reason
- sipendpoint.headset-replugged-set-ready
- sipendpoint.init-attempt-nb
- sipendpoint.init-attempt-timer
- sipendpoint.log.verbose
- sipendpoint.policy.device.audio_in_device
- sipendpoint.policy.device.audio_out_device
- sipendpoint.policy.device.capture_device
- sipendpoint.policy.device.headset_name
- sipendpoint.policy.device.use_headset
- sipendpoint.policy.endpoint.defer_device_release
- sipendpoint.policy.endpoint.include_mac_address
- sipendpoint.policy.endpoint.public_address
- sipendpoint.policy.endpoint.rtp_inactivity_timeout
- sipendpoint.policy.endpoint.rtp_port_max
- sipendpoint.policy.endpoint.rtp_port_min
- sipendpoint.policy.endpoint.sip_port_max
- sipendpoint.policy.endpoint.sip_port_min
- sipendpoint.policy.endpoint.tcp_port_min
- sipendpoint.policy.endpoint.tcp_port_max
- sipendpoint.policy.endpoint.video_max_bitrate
- sipendpoint.policy.endpoint.webrtc_audio_layer
- sipendpoint.policy.session.agc_mode
- sipendpoint.policy.session.auto_accept_video
- sipendpoint.policy.session.auto_answer
- sipendpoint.policy.session.dtmf_method
- sipendpoint.policy.session.dtx_mode
- sipendpoint.policy.session.echo_control
- sipendpoint.policy.session.noise_suppression
- sipendpoint.policy.session.reject_session_when_headset_na
- sipendpoint.policy.session.ringback_enabled
- sipendpoint.policy.session.ringback_file

- sipendpoint.policy.session.rx_agc_mode
- sipendpoint.policy.session.sip_code_when_headset_na
- sipendpoint.policy.session.vad_level
- sipendpoint.proxies.proxy0.domain
- sipendpoint.proxies.proxy0.nat.ice_enabled
- sipendpoint.proxies.proxy0.nat.stun_server
- sipendpoint.proxies.proxy0.nat.stun_server_port
- sipendpoint.proxies.proxy0.nat.turn_password
- sipendpoint.proxies.proxy0.nat.turn_relay_type
- sipendpoint.proxies.proxy0.nat.turn_server
- sipendpoint.proxies.proxy0.nat.turn_server_port
- sipendpoint.proxies.proxy0.nat.turn_user_name
- sipendpoint.proxies.proxy0.reg_interval
- sipendpoint.proxies.proxy0.reg_timeout
- sipendpoint.proxies.proxy1.domain
- sipendpoint.proxies.proxy1.nat.ice_enabled
- sipendpoint.proxies.proxy1.nat.stun_server
- sipendpoint.proxies.proxy1.nat.stun_server_port
- sipendpoint.proxies.proxy1.nat.turn_password
- sipendpoint.proxies.proxy1.nat.turn_relay_type
- sipendpoint.proxies.proxy1.nat.turn_server
- sipendpoint.proxies.proxy1.nat.turn_server_port
- sipendpoint.proxies.proxy1.nat.turn_user_name
- sipendpoint.proxies.proxy1.reg_interval
- sipendpoint.proxies.proxy1.reg_timeout
- sipendpoint.retain-volume-settings-between-sessions
- sipendpoint.sbc-register-address
- sipendpoint.sbc-register-address.peer
- sipendpoint.sbc-register-port
- sipendpoint.sbc-register-port.peer
- sipendpoint.standalone.certificate-search-value
- sipendpoint.standalone.port
- sipendpoint.standalone.protocol
- sipendpoint.standalone.security-level
- sipendpoint.standalone.subject-criteria
- sipendpoint.standalone.subject-matching-properties
- sipendpoint.standalone.vdi-detection-model
- sipendpoint.system.diagnostics.enable_logging
- sipendpoint.system.diagnostics.log_filter
- sipendpoint.system.diagnostics.log_level
- sipendpoint.system.diagnostics.log_options_provider
- sipendpoint.system.security.cert_file
- sipendpoint.system.security.tls_enabled
- sipendpoint.system.security.use_srtp
- sipendpoint.transport-protocol
- sipendpoint.video.always-on-top
- sipendpoint.video.auto-activate
- sipendpoint.video.camera-frame-rate
- sipendpoint.video.camera-frame-size
- sipendpoint.video.camera-render-format
- sipendpoint.video.thumbnail-ratio

## Related Resources

The following topics discuss the implementation of these options:

- Workspace SIP Endpoint
- Video
- Configuring Workspace Desktop Edition to use Genesys Softphone

- Genesys Softphone

# SMS options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- sms.agent.prompt-color
- sms.agent.text-color
- sms.auto-answer
- sms.auto-answer.enable-reject
- sms.auto-answer.timer
- sms.client.prompt-color
- sms.client.text-color
- sms.default-queue
- sms.from-numbers-business-attribute
- sms.max-message-number
- sms.other-agent.prompt-color
- sms.other-agent.text-color
- sms.outbound-queue
- sms.prompt-for-done
- sms.reconnect-attempts [**Added:** 8.5.153.05]
- sms.reconnect-timeout [**Added:** 8.5.153.05]
- sms.ringing-bell
- sms.simple-transcript
- sms.subject-max-chars
- sms.system.text-color
- sms.time-stamp
- sms.transcript-enable-history-filters
- sms.transcript-time-frame

## Related Resources

The following topics discuss the implementation of these options:

- SMS and MMS
- SMS privileges

# Sounds options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- sounds.preloadfiles

## Related Resources

The following topic discusses the implementation of these options:

- 5. Enabling Workspace to play ring tones

# Spellchecker options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- spellchecker.corporate-dictionary
- spellchecker.corporate-dictionary-file
- spellchecker.<media-type>.prompt-on-send

## Related Resources

The following topic discusses the implementation of these options:

- Setting up Spelling Check

# Standard Responses options

[**Modified:** 8.5.144.05]

> ## Tip
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- standard-response.auto-append-star-to-search
- standard-response.categories
- standard-response.field.<CustomFieldCode>
- standard-response.categories
- standard-response.default-search-type
- standard-response.enable-usage-feedback
- standard-response.languages
- standard-response.shortcuts.<keyword>
- standard-response.suggested-responses-min-relevancy

## Related Resources

The following topics discuss the implementation of these options:

- Standard Responses
- Standard Response privileges
- Standard Responses Library
- Email
- Chat
- Chat privileges

# Statistics options

## Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- statistics.displayed-statistics
- statistics.queues
- statistics.refresh-time
- statistics.routing-points

## Related Resources

The following topics discuss the implementation of these options:

- KPIs and Contact Center Statistics
- Section Object Statistic Name
- Section KPI Name
- Section interaction-queue-presence
- Section routing-point-presence
- Statistics privileges
- Introduction to configuration options

# System Tray options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- system-tray.tooltip

## Related Resources

The following topics discuss the implementation of this option:

- Configuring the behavior of incoming interactions
- Managing agent inactivity

# Team Communicator options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- teamcommunicator.add-recent-filters.voice
- teamcommunicator.always-clear-textbox-on-new-interaction
- teamcommunicator.contact-favorite-fields
- teamcommunicator.corporate-favorites
- teamcommunicator.corporate-favorites-file
- teamcommunicator.custom-favorite-fields
- teamcommunicator.interaction-queue-presence-metrics
- teamcommunicator.internal-favorite-fields
- teamcommunicator.list-filter-showing
- teamcommunicator.list-status-reachable
- teamcommunicator.load-at-startup
- teamcommunicator.max-favorites-size
- teamcommunicator.max-suggestion-size
- teamcommunicator.queue-presence-metrics
- teamcommunicator.recent-max-records
- teamcommunicator.request-start-timer
- teamcommunicator.routing-point-presence-metrics

## Related Resources

The following topics discuss the implementation of these options:

- Enabling Team Communicator calling features
- 10. Creating Corporate Favorites
- Planning Your Deployment

# Team Lead options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- teamlead.agent-status.enabled-agent-group-security-mode
- teamlead.agent-status.enabled-remote-actions
- teamlead.monitoring-scope

## Related Resources

The following topic discusses the implementation of these options:

- Team Leads and Supervisors

# Toast options

### Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

These options control the Interactive Notification features.

- toast.case-data.content
- toast.case-data.format-business-attribute
- toast.window-title

## Related Resources

The following topic discusses the implementation of these options:

- Callback

# View options

## Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

These options control two different types of regions within the various views, sortable and selectable regions, and sortable regions.

## Sortable and Selectable Regions

- views.CaseContactRegion.activate-order
- views.CaseContactRegion.order
- views.ContactInfoHistoryMultiRegion.activate-order
- views.ContactInfoHistoryMultiRegion.order
- views.ContactTabBottomHistoryMultiRegion.activate-order
- views.ContactTabBottomHistoryMultiRegion.order
- views.InteractionDetailsRegion.activate-order
- views.InteractionDetailsRegion.order
- views.ToolbarWorkplaceRegion.activate-order
- views.ToolbarWorkplaceRegion.order
- views.WorkbinsTabBottomHistoryMultiRegion.activate-order
- views.WorkbinsTabBottomHistoryMultiRegion.order

## Sortable Regions

- views.ToolbarWorksheetButtonRegion.order

# Voice options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- voice.after-call-work-extension
- voice.auto-answer
- voice.auto-answer.enable-reject
- voice.auto-answer.timer
- voice.cancel-after-call-work-on-done
- voice.complete-conference-requires-connected-consultation-call
- voice.device-type
- voice.dtmf-inactivity-typing-timeout
- voice.enable-agent-reservation
- voice.enable-init-conference
- voice.end-consultation-method
- voice.hold-indicator-timer
- voice.hot-standby.backup-retry-delay
- voice.hybrid-switch-preference
- voice.mark-done-on-release
- voice.nb-max-independent-calls
- voice.one-step-trsf-mode
- voice.prompt-for-end
- voice.ringing-bell
- voice.show-hold-duration
- voice.show-post-call-duration
- voice.sip-preview-bell

## Related Resources

The following topics discuss the implementation of these options:

- 3. Provisioning Workspace for the Voice channel
- Voice
- Voice privileges

# Voicemail options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

Important

Refer to the following Genesys documentation for information about setting up voicemail boxes in your Genesys system:

- Genesys SIP Voicemail (Voicemail deployment, administration, and use)
- Feature Server Deployment Guide (mailbox configuration)

- voicemail.access-number
- voicemail.notification-types

## Related Resources

The following topics discuss the implementation of these options:

- Voicemail
- Voicemail privileges
- Intercommunication options
- Communicating inside your business

# Warm-Standby options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- warm-standby.reconnection-random-delay-range
- warm-standby.retry-delay

## Related Resources

The following topics discuss the implementation of these options:

- Load Balancing using clusters
- eServices Business Continuity with UCS 9.1
- eServices Business Continuity with UCS 8.5
- Business Continuity for SIP Server, Configuration Server, and Statistic Server

# Web Callback options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- webcallback.auto-answer
- webcallback.auto-answer.enable-reject
- webcallback.auto-answer.timer
- webcallback.auto-dial
- webcallback.complete-queue
- webcallback.park-queue
- webcallback.reschedule-queue
- webcallback.ringing-bell
- webcallback.callback-information.content
- webcallback.callback-information.frame-color
- webcallback.callback-information.header-foreground-color

## Related Resources

The following topics discuss the implementation of these options:

- Web Callback
- Web Callback privileges
- Callback
- Callback options
- Callback privileges
- Outbound campaigns
- Outbound options

# Webproxy options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- webproxy.address
- webproxy.password
- webproxy.username

## Related Resources

The following topic discusses the implementation of these options:

- Email

# Workbin options

> **Tip**
>
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- workbin.email.draft
- workbin.email.draft.displayed-columns
- workbin.email.in-progress
- workbin.email.in-progress.displayed-columns
- workbin.<media_type>.in-progress
- workbin.<media_type>.in-progress.displayed-columns
- workbin.<media-type>.<workbin-nickname>
- workbin.<media-type>.<workbin-nickname>.auto-update
- workbin.<media-type>.<workbin-nickname>.displayed-columns
- workbin.<media-type>.<workbin-nickname>.max-results
- workbin.<media-type>.<nick-name>.notify-property-changed
- workbin.<media-type>.<workbin-nickname>.quick-search-attributes

## Related Resources

The following topics discuss the implementation of these options:

- Setting up agents to use workbins
- Workbin and Interaction Queue management
- Workbins privileges
- Interaction Management privileges
- Email
- Workitems
- Email Quality Assurance

# Workitem options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

- <media-type>.auto-answer
- <media-type>.auto-answer.enable-reject
- <media-type>.auto-answer.timer
- <media-type>.prompt-for-done
- <media-type>.pull-from-history-isenabled
- <media-type>.ringing-bell
- <media-type>.toast-information-key

## Related Resources

The following topics discuss the implementation of these options:

- Workitems
- Workitem privileges
- Open Media options

# Miscellaneous options

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

Options that were formally listed on this page each now appear on a dedicated page for the option category.

- alert.timeout
- application.available-layouts
- case-data.float-separator
- channel-information.window-title
- editor.font-size-units
- interaction-bar.detail-tooltip.max-height
- license.lrm-enabled
- logout.enable-exit-on-logoff-error
- options.record-option-locally-only
- presence.evaluate-presence
- printing.use-print-preview
- sounds.preloadfiles
- system-tray.tooltip
- teamlead.monitoring-scope

# Section interaction-queue-presence

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

The interaction queue presence options enable agents to view interaction queue statistics information in Team Communicator. Refer to the Enabling Team Communicator Calling Features and Enabling the E-Mail Channel for information about how to use these options.

- associated-object-ids
- associated-statistic-type
- error-level
- object-ids
- statistic-name
- statistic-text
- warning-level

# Section queue-presence

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

The queue presence options enable agents to view queue statistics information in Team Communicator. Refer to the Enabling Team Communicator Calling Features and Enabling the E-Mail Channel for information about how to use these options.

- associated-object-ids
- associated-statistic-type
- error-level
- object-ids
- statistic-name
- statistic-text
- warning-level

# Section routing-point-presence

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

The routing point presence options enable agents to view routing point statistics information in Team Communicator. Refer to the Enabling Team Communicator Calling Features and Enabling the E-Mail Channel for information about how to use these options.

- associated-object-ids
- associated-statistic-type
- error-level
- object-ids
- statistic-name
- statistic-text
- warning-level

# Section KPI Name

Each KPI that you want to define and use must have its own section defined in the Workspace Application object in the Configuration Database.

> Tip
>
> KPIs are not part of the XML metadata file because they are not composed of fixed section names.

## Defining a KPI section

Use Genesys Administrator Extension to define a new section at the level at which you want the KPI to be displayed. Use the KPI name as the name of the section. Define the values that are to be displayed for the KPI as the Options and Values of the Section.

For example, for the `TotalTalkStatusTime` KPI, define a section that is named `TalkTime`, and then define a set of Options and specify values for those options. The Table - **Sample Options and Values for the KPI Section** provides a sample of Option names and values that you might define for this KPI.

**Sample Options and Values for the KPI Section**

| Option | Value | Mandatory |
|---|---|---|
| statistic-name | TotalTalkStatusTime | Yes |
| period | OneMinute | Yes |
| target-value | 40 | Yes |
| warning-level-low | | No |
| warning-level-high | | No |
| error-level-low | | No |
| error-level-high | | No |
| worst-value-low | 0 | No |
| worst-value-high | | No |
| description | Total talk time for the agent | Yes |
| filter | The value must be the filter for the statistic calculation. This should correspond to an option name that is defined by the Filters section of Statistics Server. | No |
| evaluation-display | Evaluation | Yes |

## Displaying KPIs

Workspace enables you to display the KPIs that you have defined on the Application object at one or more of the following levels:

- **Application level** -- Display KPI to all agents.
- **Tenant level** -- Display KPI to all the agents of the Tenant.
- **Agent Group level** -- Display KPI to all the agents of the Agent Group.
- **Agent level** -- Display KPI to the agent.

To display a KPI at a specific level, define and configure the kpi.displayed-kpis option in the `interaction-workspace` section of the level. The value of this option is a comma-separated list of KPI sections that are to be displayed.

## Setting the Warning, Error, and Worst Levels

Workspace provides eight non-mandatory options that you can use to define low and/or high levels of warning and error and low and/or high levels of worst values.

Some statistics are in an error state when they are below a certain value, while others are in an error state when they are above a certain value; for some statistics both a lower error threshold and a higher error threshold are required. The following non-mandatory options enable you to set a low and high threshold for a statistic:

- `error-level-low`--Values below this value are in an error state for the statistic.
- `error-level-high`--Values above this value are in an error state for the statistic.

Some statistics are in a warning state when they are below a certain value, while others are in a warning state when they are above a certain value; for some statistics both a lower warning threshold and a higher warning threshold are required. The following non-mandatory options enable you to set a low and high threshold for a statistic:

- `warning-level-low`--Values below this value are in a warning state for the statistic.
- `warning-level-high`--Values above this value are in a warning state for the statistic.

Use the error and warning options to specify ranges that are most suitable for the statistic.

Some statistics are performance based. The agent's result is compared to a target value to determine the agent's level of performance. Some statistics require a lower worst value and some require a higher worst value. For some statistics, both a lower and a higher worst value are required.

- `worst-value-low`--Values below this value result in a negative evaluation for the KPI.
- `worst-value-high`--Values above this value result in a negative evaluation for the KPI.
- `target-value`--The target value to be reached by the agent.
- `evaluation-display`--Specifies which value is displayed to the agent, a performance indicator or the raw statistic in the format of the statistic (for example, number, date, or percentage). If the option is set to `Result`, the actual statistic value is displayed. If the option is set to `Evaluation`, the performance of the agent is calculated by using the following formulae:

If the statistic value is lower than the target value, the following evaluation is applied: Agent Performance = (Agent Result - `worst-value-low`) / (Target Value -`worst-value-low`) x 100 or: If the statistic value is higher than the target value, the following evaluation is applied: Agent Performance = (`worst-value-high` - Agent Result) / (`worst-value-high` - Target Value) x 100

> ### Tip
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

# Section Object Statistic Name

Each Object Statistic (contact center statistic) that you want to define and use must have its own section defined in the Workspace Application object in the Configuration Database.

> Tip
>
> Object Statistics are not part of the XML metadata file because they are not composed of fixed section names.

## Defining a Object Statistic section

Use Genesys Administrator Extension to define a new section at the level at which you want the Object Statistic to be displayed. Use the Object Statistic name as the name of the section. Define the values that are to be displayed for the Object Statistic as the Options and Values of the section. Refer to the Table - **Mandatory and Optional Options for Object Statistics Section** for a list of the mandatory and optional options that you can define for each Object Statistic.

**Mandatory and Optional Options for Object Statistics Section**

| Option | Value description | Mandatory |
|---|---|---|
| description | The value must be the display name for the statistic. It is displayed in the Workspace statistics list. If this option is not defined (empty), the value of the statistic-name option is displayed instead. | No |
| error-level-high | Values above this value result in an error state for the statistic. | No |
| error-level-low | Values below this value result in an error state for the statistic. | No |
| filter | The value must be the filter for the statistic calculation. This should correspond to an option name that is defined by the `Filters` section of Statistics Server. | No |
| long-description | The value must be a complete description of the statistic. It is displayed as a tooltip in the Workspace interface. | No |
| object-id | The value must be the ID of the object that requests this statistic. The format of a queue `object-id` is: `<QueueName>@<SwitchName>` The format of a routing point | No |

| Option | Value description | Mandatory |
|---|---|---|
| | object-id is:<RPName>@<SwitchName> | |
| period | The value must be the period for the statistic calculation. This should correspond to an option name that is defined by the TimeProfiles section of Statistics Server. | No |
| refresh-time | The value must be the length of time, in seconds, between each update request from Statistics Server. | No |
| statistic-name | The value must be the name of the Statistic as defined in the Statistics Server options. | Yes |
| statistic-type | The value must be the type of the object—such as Queue, RoutePoint, or GroupQueues—as defined for the Object Statistic in Statistics Server. | Yes |
| time-range | The value must be the time range for the statistic calculation. This should correspond to an option name that is defined by the TimeRanges section of Statistics Server. Time ranges are used to calculate certain statistics such as those that specify a percentage. | No |
| time-range2 | The value must be the secondary time range for the statistic calculation. This should correspond to an option name that is defined by the TimeRanges section of Statistics Server. Time ranges are used to calculate certain statistics such as those specify a percentage. | No |
| warning-level-high | Values above this value result in an error state for the statistic. | No |
| warning-level-low | Values below this value result in an error state for the statistic. | No |

## Setting the Warning and Error levels

Workspace provides four non-mandatory options that you can use to define low and/or high levels of warning and error.

Some statistics are in an error state when they are below a certain value, while others are in an error state when they are above a certain value; for some statistics both a lower error threshold and a higher error threshold are required. The following non-mandatory options enable you to set a low and high threshold for a statistic:

- `error-level-low`--Values below this value result in an error state for the statistic.
- `error-level-high`--Values above this value result in an error state for the statistic.

Some statistics are in a warning state when they are below a certain value, while others are in a warning state when they are above a certain value; for some statistics both a lower warning threshold and a higher warning threshold are required. The following non-mandatory options enable you to set a low and high threshold for a statistic:

- `warning-level-low`--Values below this value result in an error state for the statistic.
- `warning-level-high`--Values above this value result in an error state for the statistic.

Use the error and warning options to specify ranges that are most suitable for the statistic.

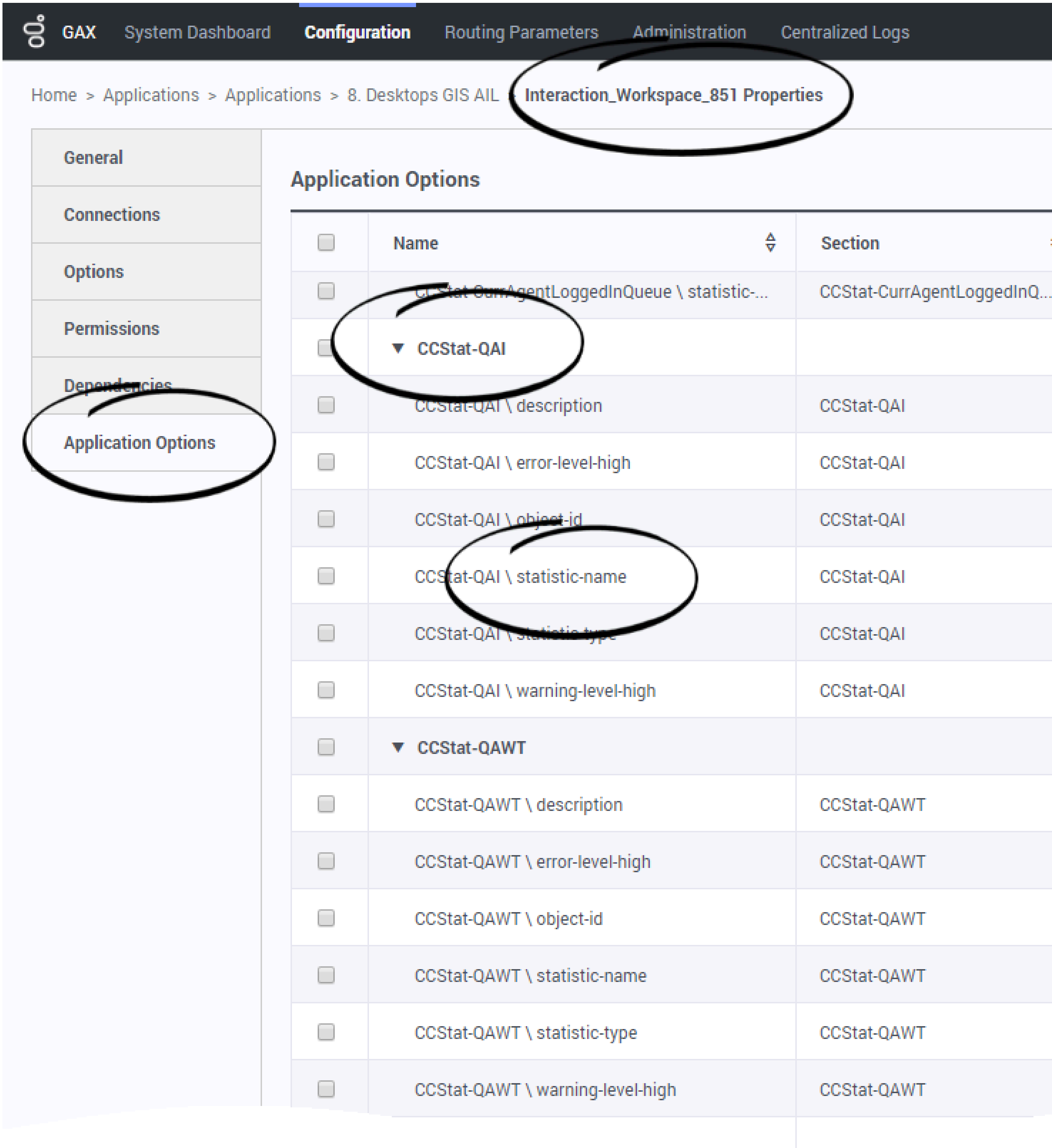
## Displaying Object Statistics

Workspace enables you to display the Object Statistics that you have defined on the Application object at one or more of the following levels:

- **Application level** -- Display Object Statistic to all agents
- **Tenant level** -- Display Object Statistic to all the agents of the Tenant
- **Agent Group level** -- Display Object Statistic to all the agents of the Agent Group
- **Agent level** -- Display Object Statistic to the agent

To display an Object Statistic at a specific level, define and configure the `statistics.displayed-statistics` option in the `interaction-workspace` section of the level. The value of this option is a comma-separated list of Object Statistic sections that are to be displayed.

The Figure **- Sample section defined in Genesys Administrator Extension for the Workspace Application object** provides an example of a statistic section that is defined on the Workspace Application object.



Home > Applications > Applications > 8. Desktops GIS AIL > Interaction_Workspace_851 Properties

Application Options

| □ | Name | Section |
|---|---|---|
| □ | CCStat-CurrAgentLoggedInQueue \ statistic-... | CCStat-CurrAgentLoggedInQ... |
| □ | ▼ CCStat-QAI | |
| □ | CCStat-QAI \ description | CCStat-QAI |
| □ | CCStat-QAI \ error-level-high | CCStat-QAI |
| □ | CCStat-QAI \ object-id | CCStat-QAI |
| □ | CCStat-QAI \ statistic-name | CCStat-QAI |
| □ | CCStat-QAI \ statistic-type | CCStat-QAI |
| □ | CCStat-QAI \ warning-level-high | CCStat-QAI |
| □ | ▼ CCStat-QAWT | |
| □ | CCStat-QAWT \ description | CCStat-QAWT |
| □ | CCStat-QAWT \ error-level-high | CCStat-QAWT |
| □ | CCStat-QAWT \ object-id | CCStat-QAWT |
| □ | CCStat-QAWT \ statistic-name | CCStat-QAWT |
| □ | CCStat-QAWT \ statistic-type | CCStat-QAWT |
| □ | CCStat-QAWT \ warning-level-high | CCStat-QAWT |

Sample section defined in Genesys Administrator Extension for the Workspace Application object

Tip

For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

# Not Ready Reason codes

Workspace provides "reasons" with which agents can specify details about their NotReady status; these are configured by creating as many Action Code objects of type Not Ready as you require.

Each Not Ready Reason can be customized by creating a section named interaction-workspace in the annexes of Action Code objects that are used to define Not Ready Reason codes, and then defining and configuring options in that section to customize the way that not-ready reasons are sent to your T-Server.

Define the following options in the interaction-workspace section that you create:

## workmode

- Default Value: ""
- Valid Values: "", aux-work
- Changes take effect: At next login.
- Description: Refines and extends the customized NotReady status monitoring, when it is supported by the switch.

## extensions

- Default Value: false
- Valid Values: true, false
- Changes take effect: At next login.
- Description: Available only if the workmode option is not defined or if it is set to none. If your switch does not support the aux-work value, this option creates and enters extensions as the option name, and either false (as the default value) or true (as a valid value).

## reason-extension-key

- Default Value: ReasonCode
- Valid Values: ReasonCode, <any string>
- Changes take effect: At next login.
- Description: The name that is set as the key of the key-value pair added to the Not Ready Reason or Extensions map. The corresponding value is set according to the Action Code that is defined in the Configuration Layer and the value of the reason-extension-value option.
  If the value of this option is empty, the key of the key-value pair is the Name attribute of the selected Action Code.

> ### Tip
> Genesys Workforce Management requires a specific configuration of the Workspace **reason-extension-key** and **extensions** options to ensure WFM Data Aggregator can read agent state reason codes. To read more about its dependency on these options, see Configuring Data Aggregator to process reason codes in the *Workforce Management Administrators Guide*.

## reason-extension-request-attribute

- Default Value: `""`
- Valid Values: `""`, `reasons`, `extensions`
- Changes take effect: At next login.
- Description: Specifies whether the reason code is published in the `reason` attribute or in the `extension` attribute. Empty means that the legacy behavior is preserved, where the reason code is published in the ‘reasons’ or ‘extensions’ attribute, depending on the selected workmode. **Note:** not all switches support the capability to pass Not Ready Reason through the `extensions` attribute. Refer to T-Server and switch vendor documentation.

## reason-extension-value

- Default Value: code
- Valid Values: name, code
- Changes take effect: At next login.
- Description: The type of content that is set as the value of the key-value pair added to the `Not Ready Reason` or `Extensions` map.
  - If the option is empty or not correct, the default value is: `code`.
  - The corresponding key is set according to the value of the option `reason-extension-key`.
  - When set to `code` the key is the `Code` attribute of the selected `Action Code`.
  - When set to `name` the key is the `Name` attribute of the selected `Action Code`.

> ### Tip
> For the most up to date Workspace Desktop Edition configuration options, see the Genesys Configuration Option Database.

# Role privileges

In the privilege-based model that is implemented by Workspace, an agent is assigned privileges based on the role of the agent. Privileges are enabled or disabled depending on the role that is assigned to the agent. Privileges are assigned as configuration options in the Role Privileges tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

Refer to *Genesys Administrator Extension Help* and *Genesys Security Guide* for detailed information on how to use Genesys Administrator Extension and Management Framework to configure access permissions. The following tables list and describe the privileges that you can set for Workspace agent roles:

- **Broadcast Message Privileges** lists the Broadcast Message privileges in the Workspace Broadcast Message Privileges section of the Role Privileges tab that can be enabled for a role.
- **Callback Privileges** lists the Callback Privileges in the Workspace Callback Privileges section of the Role Privileges section that can be enabled for a role.
- **Case Information Privileges** lists the Case Information privilege in the Workspace Case Information Tasks section of the Role Privileges tab that can be enabled for a role.
- **Chat Privileges** lists the Chat privileges in the Workspace Chat Access section of the Role Privileges tab that can be enabled for a role.
- **Contact Management Privileges** lists the Contact Management privileges in the Workspace Contact Privileges section of the Role Privileges tab that can be enabled for a role.
- **E-Mail Privileges** lists the E-Mail privileges in the Workspace E-Mail Privileges section of the Role Privileges tab that can be enabled for a role.
- **IM Privileges** lists the internal IM privileges in the Workspace Instant Messaging Privileges section of the Role Privileges tab that can be enabled for a role.
- **Interaction Management Privileges** lists the Interaction Management privileges in the Workspace Interaction Management Privileges section of the Role Privileges tab that can be enabled for a role.
- **Main Window Privileges** lists the Main Window privileges in the Workspace Workspace Privileges section of the Role Privileges tab that can be enabled for a role.
- **Outbound Campaign Privileges** lists the outbound campaign privileges in the Workspace Outbound Privileges section of the Role Privileges tab that can be enabled for a role.
- **Recording Privileges** lists the voice privileges in the Workspace Recording Privileges section of the Role Privileges tab that can be enabled for a role.
- **Security Privileges** lists the Security privileges in the Workspace Security Privileges section of the Role Privileges tab that can be enabled for a role.
- **SMS Privileges** lists the SMS privileges in the Workspace SMS Access section of the Role Privileges tab that can be enabled for a role.
- **Standard Response Privileges** lists the Standard Resource Library (SRL) privileges in the Workspace Standard Response Privileges section of the Role Privileges tab that can be enabled for a role.
- **Statistics Privileges** lists the Statistics privileges in the Workspace Statistics Privileges section of the Role Privileges tab that can be enabled for a role.

- **Team Communicator Privileges** lists the Team Communicator privileges in the `Workspace Team Communicator Privileges` section of the `Role Privileges` tab that can be enabled for a role.
- **Team Lead Privileges** lists the Team Lead privileges in the `Workspace Team Lead Privileges` section of the `Role Privileges` tab that can be enabled for a role.
- **Voice Privileges** lists the voice privileges in the `Workspace Voice Privileges` section of the `Role Privileges` tab that can be enabled for a role.
- **Voicemail Privileges** lists the voicemail privileges in the `Workspace Voice Privileges` section of the `Role Privileges` tab that can be enabled for a role.
- **Web Callback Privileges** lists the Web Callback privileges in the `Workspace Web Callback Access` section of the `Role Privileges` tab that can be enabled for a role.
- **Workbins Privileges** lists the Workbin privileges in the `Workspace Workbin Privileges` section of the `Role Privileges` tab that can be enabled for a role.
- **Workitem Privileges** lists the Workitem privileges in the `Workspace Workitem Privileges` section of the `Role Privileges` tab that can be enabled for a role.
- **Workspace SIP Endpoint Privileges** lists the Workspace SIP Endpoint privileges in the `Workspace SIP Tasks` section of the `Role Privileges` tab that can be enabled for a role.

# Broadcast Message privileges

The following table lists the Broadcast Message privileges in the `Interaction Workspace Broadcast Message Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role and allowing an Interaction Workspace privilege and assigning a Role to an agent or agent group).

**Broadcast Message Privileges**

| Role privilege | Description |
|---|---|
| Broadcast - Can Use | The agent is permitted to receive and view broadcast messages. |

# Callback privileges

[**Added:** 8.5.111.21]

The following table lists the Callback privileges in the `Workspace Callback` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Callback Privileges**

| Role privilege | Description |
|---|---|
| Callback - Can Use Callback | The agent is permitted to use the Callback media. |
| Callback - Can Reject Invitation | The agent is permitted to decline a Callback so that it can be processed by a different agent. Depends on 'Callback - Can Use Callback Channel'. |
| Callback - Can Reschedule Current Callback | The agent is permitted to reschedule the current Callback interaction. Depends on 'Callback - Can Use Callback Channel'. |
| Callback - Can Reschedule Or Submit On New Number | The agent is permitted to reschedule a Callback interaction or submit a new Callback by using a new phone number. Depends on 'Callback - Can Use Callback' and 'Callback - Can Reschedule Current Callback' or 'Callback - Can Submit New Callback'. |
| Callback - Can Submit New Callback | The agent is permitted to create a new Callback interaction from another interaction or by using the Team Communicator. Depends on 'Callback - Can Use Callback Channel'. |

# Case Information privileges

The following table lists the Case Information privilege in the `Workspace Case Information Tasks` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Case Information Privileges**

| Role privilege | Description |
|---|---|
| Case Information - Can Edit | Enables agents to edit case information that is configured to be editable. |
| Case Information - Can Add | Enable agents, agent groups, or roles to edit case information. |

# Chat privileges

[**Modified:** 8.5.108.11, 8.5.115.17, 8.5.128.07]

The following table lists the Chat privileges in the `Interaction Workspace Chat Access` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Chat Privileges**

| Role privilege | Description |
|---|---|
| Chat - Can Use Chat Channel | The agent is permitted to use the chat media channel. |
| Chat - Can Decline | The agent is permitted to reject chat interactions that are directed to the agent. |
| Chat - Can Use Emojis | The agent is permitted to add emojis to a chat interaction. [**Added:** 8.5.115.17] |
| Chat - Can Release | The agent is permitted to manually terminate a standard non-asynchronous chat conversation. [**Modified:** 8.5.128.07] |
| Chat - Can One Step Transfer | The agent is permitted to use the instant-transfer functionality. |
| Chat - Can Two Step Transfer | The agent is permitted to contact and chat (consultation) prior to transferring the chat interaction to the target. |
| Chat - Can One Step Conference | The agent is permitted to use the instant-conference functionality. |
| Chat - Can Two Step Conference | The agent is permitted to contact and chat (consultation) prior to starting a chat conference. |
| Chat - Can Transfer File From File System | The agent is permitted to select a file and transfer it to the other parties in the interaction. [**Added:** 8.5.115.17] |
| Chat - Can Transfer File From Standard Response | The agent is permitted to transfer a file from a selected standard response to the other parties in the interaction. [**Added:** 8.5.115.17] |
| Chat - Can Push Url | The agent is permitted to send URLs to contacts during chat interactions. |
| Chat - Can Save Attached files | The agent is permitted to save files from the chat transcript to their local workstation. [**Added:** 8.5.115.17] |
| Chat - Can Set Interaction Disposition | The agent is permitted to set the disposition code of a chat interaction. |
| Chat - Show Silent Monitoring | The agent is permitted to know when a supervisor is monitoring the agent during a chat interaction. |

| Role privilege | Description |
|---|---|
| Chat - Can Preview Customer Typing | The agent can see the text as it is typed by the contact on the your web site chat interface before the contact clicks **Send**. [**Added:** 8.5.108.11] |
| Chat - Can Place On Hold | The agent is permitted to leave and rejoin an asynchronous chat session. [**Added:** 8.5.128.07] |
| Chat - Can Release Async | The agent is permitted to manually terminate an asynchronous chat session.[**Added:** 8.5.128.07] |

## Warning

If the Chat - Can Preview Customer Typing privilege is also granted, and you have configured eServices to hide sensitive personal information that is entered by the contact during the chat, agents will be able to see the information as it is entered, but not after the contact sends it.
**Added:** 8.5.108.11

# Contact Management privileges

[**Modified:** 8.5.110.13, 8.5.126.07]

The following table lists the Contact Management privileges in the `Workspace Contact Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Contact Management Privileges**

| Role privilege | Description |
|---|---|
| Contact - Can Use | The agent is permitted to perform contact management privileges. The other contact management privileges cannot be configured if the value is `Not Assigned`. |
| Contact - Can Create Contact | The agent is permitted to create a new contact in the Universal Contact Server database. |
| Contact - Can Delete Contact | The agent is permitted to delete an existing contact from the Universal Contact Server database. |
| Contact - Can Edit Contact | The agent is permitted to edit contact information in the Universal Contact Server database. **Note:** Agents can save new contacts when the Contact - Can Create privilege is assigned even if the Contact - Can Edit Contact privilege is not assigned. Previously in this scenario, if the Contact - Can Create privilege was granted to agents and the Contact - Can Edit Contact privilege was not, agents could not save a new contact. |
| Contact - Can Mark Done Voice Interaction | The agent is permitted to mark an interaction as done. |
| Contact - Can Merge Contact | The agent is permitted to merge two contacts in the Universal Contact Server database. |
| Contact - Can Assign Contact | The agent is permitted to assign an interaction to an existing contact if the interaction has an unknown contact or is incorrectly assigned to a different contact. |
| Contact - Can Use Interaction Notepad | The agent is permitted to use the Notepad to view and edit notes that are included in the interaction. |
| Contact - Can Merge Interaction To Contact | The agent is permitted to merge interactions to an existing contact in the Universal Contact Server database. |
| Contact - Can Undo Merge Contact | The agent is permitted to unmerge a previously merged contact in the Universal Contact Server database. |
| Contact - Can Use Contact Directory | The agent is permitted to use the Contact Directory |

| Role privilege | Description |
|---|---|
| | to view and manage contact information in the Universal Contact Server database. |
| Contact - Can Use Contact History | The agent is permitted to view and manage contact history. |
| Contact - Can Use Contact History CaseData | The agent is permitted to view and manage contact history case data. |
| Contact - Can Use Contact History Detail | The agent is permitted to view and manage contact history details. |
| Contact - Can Use Contact History Notepad | The agent is permitted to view and manage contact history notepad information. |
| Contact - Can Use Contact Information | The agent is permitted to view and manage contact information. |
| Contact - Can Use My History | The agent is permitted to view and manage contact information for interactions that they have handled. |
| Contact - Can Use Interaction Search | The agent is permitted to search for any interaction available in Universal Contact Server index accross all contacts and all agents. [**Added:** 8.5.104.15] |
| Contact - Can Pull From Queue | From the Contact History view, the agent is permitted to pull interactions from a queue and perform any of the following actions: Reply, Reply All, Mark Done (beginning with 8.5.110.13), and Delete (beginning with 8.5.110.13) if the corresponding privileges are allowed. |
| Contact - Can Pull Interactions In Shared Workbins | From the Contact History view, the agent is permitted to pull interactions from shared workbins which are not explicitly accessible to the user and perform any of the following actions: Reply, Reply All, Mark Done (beginning with 8.5.110.13), and Delete (beginning with 8.5.110.13) if the corresponding privileges are allowed. |
| Contact - Can Pull Interactions In Workbins Not Owned By The User | From the Contact History view, the agent is permitted to pull interactions from personal workbins which are not owned by the user and perform any of the following actions: Reply, Reply All, Mark Done (beginning with 8.5.110.13), and Delete (beginning with 8.5.110.13) if the corresponding privileges are allowed. |
| Contact - Can Access Archive | The agent is permitted to access the interaction archive in the Contact History view. **Warning:** Do not allow this privilege if UCS 9.1 is used; if it is granted, an error will be displayed if the Agent selects the **Archive** option in the **Contact History** view. [**Modified:** 8.5.126.07] |

# E-Mail Privileges

[**Modified:** 8.5.113.11]

The following table lists the E-Mail privileges in the `Workspace E-Mail Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**E-Mail Privileges**

| Role privilege | Description |
|---|---|
| E-Mail - Can Add Attachments | The agent is permitted to include attached files in email interactions. |
| E-Mail - Can Add Embedded Image In Outbound E-Mail | The agent is permitted to add embedded images to outbound email interactions from the clipboard or file explorer. **Note:** If an agent uses drag and drop to insert an image into an email, it will be added as an attachment, not as an inserted image. **Added:** 8.1.5xx.xx |
| E-Mail - Can Change Format New Email | The agent is permitted to switch the format of a new outbound email interaction between HTML and plain text. **Added:** 8.1.40x.xx |
| E-Mail - Can Change Format Reply Email | The agent is permitted to switch the format of a reply outbound email interaction between HTML and plain text. **Added:** 8.1.40x.xx |
| E-Mail - Can Decline | The agent is permitted to reject email interactions that are directed to the agent. |
| E-Mail - Can Delete | The agent is permitted to delete email interactions from the contact database. |
| E-Mail - Can Forward As An Attachment | The agent is permitted to configure an external email address to which email interactions can be forwarded. |
| E-Mail - Can Forward | The agent is permitted to in-line forward email interactions to external resources.<br>**Added:** 8.1.5xx.xx |
| E-Mail - Can Interim Send | The agent is permitted to send interim email interactions to a target. |
| E-Mail - Can Mark Done | The agent is permitted to mark email interactions as Done. |
| E-Mail - Can Move to Workbin | The agent is permitted to move email interactions to a workbin for later handling or handling by another agent or agent group. |
| E-Mail - Can Print | The agent is permitted to print a hard copy of an email interaction. |

| Role privilege | Description |
|---|---|
| E-Mail - Can Reply | The agent is permitted to reply to the sender of an inbound email interaction. |
| E-Mail - Can Reply All | The agent is permitted to reply to the sender and all other addressees of inbound email interaction. |
| E-Mail - Can Save | The agent is permitted to save email interactions in the in-progress workbin. |
| E-Mail - Can Send | The agent is permitted to send email interactions to a target. |
| E-Mail - Can Set Interaction Disposition | The agent is permitted to set the disposition code of an email interaction. |
| E-Mail - Can Transfer | The agent is permitted to use the instant-transfer functionality. |
| E-Mail - Can Use E-Mail Channel | The agent is permitted to use the email media channel. |

# IM privileges

The following table lists the internal IM privileges in the `Workspace Instant Messaging Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**IM Privileges**

| Role privilege | Description |
|---|---|
| Instant Messaging - Can Release | The agent is permitted to end Instant Messaging sessions. |
| Instant Messaging - Can Make | The agent is permitted to initiate Instant Messaging sessions. |
| Instant Messaging - Can Use | The agent is permitted to use the Instant Messaging media. The other IM privileges cannot be configured if the value is `Not Assigned`. |

# Interaction Management privileges

[**Modified:** 8.5.110.13]

The following table lists the Interaction Management privileges in the `Workspace Interaction Management Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Interaction Management Privileges**

| Role privilege | Description |
|---|---|
| Interaction Management - Can Edit Case Data | The agent is permitted to edit the case information of an interaction in a queue or a workbin. Requires 'Workbins - Can Use My Workbins' or 'Workbins - Can Use My Team Workbins' or 'Interaction Queue Management - Can Use'. |
| Interaction Management - Can Search In Interaction Queues | The agent is permitted to use the search filter function in the My Interaction Queues view.<br>**Added:** 8.5.110.13 |
| Interaction Management - Can Move to Queue | The agent is permitted to move an interaction from a workbin or from a queue to a queue. Requires 'Workbins - Can Use My Workbins' or 'Workbins - Can Use My Team Workbins' or 'Interaction Queue Management - Can Use'. |
| Interaction Management - Can Move to Workbin | The agent is permitted to move an interaction from a workbin or from a queue to a workbin. Requires 'Workbins - Can Use My Workbins' or 'Workbins - Can Use My Team Workbins' or 'Interaction Queue Management - Can Use'. |
| Interaction Management - Can Use | The agent is permitted to access the interaction queue management functions. |

# Main Window privileges

The following table lists the interaction bar privileges, in the `Workspace Main Window Privileges` section of the `Role Privileges` tab, that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Main Window Privileges**

| Role privilege | Description |
|---|---|
| Main Window - Can Use Interaction Bar | Enables the use of the Interaction bar in the Main Window. |
| Main Window - Can Dock the Main Window | Enables the use of the docking of the Main Window to the top of the agent's display. |
| Main Window - Can Auto-hide the Main Window | Enables the automatic hiding of the Main Window when it is docked. |

# Outbound Campaign privileges

[**Modified:** 8.5.115.17]

The following table lists the outbound campaign privileges in the `Workspace Outbound Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Outbound Campaign Privileges**

| Role privilege | Description |
|---|---|
| Outbound - Can Use | The agent is permitted to use the Outbound Campaign functions. |
| Outbound - Can Reject Record | The agent is permitted to decline a preview record so that it can be processed by somebody else in the campaign. |
| Outbound - Can Cancel Record | The agent is permitted to decline a preview record so that it is not processed at all during the current campaign. |
| Outbound - Can Dial Alternative Chained Record | The agent is permitted to dial a number from the preview record chain that is different than the number selected by the system. |
| Outbound - Can Dial On New Number | The agent is permitted to dial an outbound contact using a new number. This results in a new record being added to the chain. Depends on Outbound - Can Use and Outbound - Can Dial Alternative Chained Record. [**Added:** 8.5.115.17] |
| Outbound - Can Get Next Preview Record | The agent is permitted to request a new preview record while the processing of the previous one terminates. |
| Outbound - Can Use Push Preview | The agent is permitted to actively take part in Outbound Push Preview campaigns. |
| Outbound - Push Preview Can Decline | The agent is permitted to decline Outbound Push Preview interactions. |
| Outbound - Can Mark Do Not Call | The agent is permitted to mark a contact as Do Not Call. |
| Outbound - Can Set Call Result | The agent is permitted to set a call result to the outbound record. |
| Outbound - Can Reschedule | The agent is permitted to reschedule an outbound record for an active call. Use the Outbound - Can Reschedule Before Call privilege to allow rescheduling before the call is dialed. Depends on Outbound - Can Use. |
| Outbound - Can Reschedule Before Call | The agent is permitted to reschedule an outbound record before calling the contact (in Pull and Push Preview Mode). Requires privilege Outbound - Can |

| Role privilege | Description |
|---|---|
| | Reschedule. |
| Outbound - Can Reschedule On New Number | The agent is permitted to reschedule an outbound record on a new number (which results in a new record added to the chain). |
| Outbound - Can Edit Record Data | The agent is permitted to edit the outbound record fields configured as editable. |

# Recording privileges

The following table lists the voice and screen recording privileges in the `Workspace Recording Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

## Important

A new privilege for Screen Recording was added in 8.5.106.19: `Recording - Can Use Screen Recording`. It allows a Workspace instance to activate a Screen Recorder Client when it is installed on the workstation. It applies to voice interactions and eServices.

**Active Recording Privileges**

| Role privilege | Description |
|---|---|
| Recording - Can Use MSML-based and Screen Recording | This privilege is a pre-requisite to permit an agent to use MSML-based and Screen Recording functionality. This privilege is required to:<br>• Control and monitor call recording in MSML mode. In this case it depends on 'Voice - Can Use Voice Channel'<br>• Enable screen recording |
| Recording - Can Monitor Call Recording | The agent is permitted display the status of a MSML-based recorded call. Depends on 'Voice - Can Use Voice Channel' and 'Recording - Can Use MSML-based and Screen Recording'. |
| Recording - Can Control Call Recording | The agent is permitted to control call recording (not available on all switches). Depends on 'Voice - Can Use Voice Channel'. The type of recording depends on the value specified for the active-recording.voice.recording-type option. For MSML-based recording, it depends on 'Recording - Can Use MSML-based Recording'. |
| Recording - Can Use Screen Recording<br>[**Added:** 8.5.106.19] | Enables a Workspace instance to activate a Screen Recorder Client if one is installed on the workstation. It applies to voice and eServices interactions. Depends on 'Recording - Can Use MSML-based and Screen Recording' |
| Recording - Can Control Screen Recording | The agent is permitted to control screen recording. Depends on 'Recording - Can Use MSML-based and |

| Role privilege | Description |
|---|---|
| | Screen Recording' |
| Recording - Can Monitor Screen Recording | The agent is permitted to monitor screen recording. Depends on 'Recording - Can Use MSML-based and Screen Recording' |

# Security privileges

The following table lists the Security privileges in the `Workspace Security Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Security Privileges**

| Role privilege | Description |
|---|---|
| Security - Can Manually Change Password | The agent is permitted to change their own password. This can be done by using a menu action, or it can be a requirement. |

# SMS privileges

[**Modified:** 8.5.110.13]

The following table lists the SMS privileges in the `Workspace SMS Access` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**SMS Privileges**

| Role privilege | Description |
|---|---|
| SMS - Can Use SMS Channel | The agent is permitted to use the SMS media channel. |
| SMS - Can Decline | The agent is permitted to reject SMS interactions that are directed to the agent. |
| SMS - Can One Step Transfer | The agent is permitted to use the instant-transfer functionality. |
| SMS - Can Set Interaction Disposition | The agent is permitted to set the disposition code of a SMS interaction. |
| SMS - Can Create | The agent is permitted to create SMS interactions from the Team Communicator and the Contact Directory. |
| SMS - Can Save Attached File | The agent is permitted to save MMS images.<br>[**Added:** 8.5.110.13] |

# Standard Response privileges

The following table lists the Standard Resource Library (SRL) privileges in the `Workspace Standard Response Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Standard Response Privileges**

| Role privilege | Description |
|---|---|
| Standard Response Library - Can Use | The agent is permitted to access the Standard Response Library. |

# Statistics privileges

The following table lists the Statistics privileges in the `Workspace Statistics Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Statistics Privileges**

| Role privilege | Description |
|---|---|
| Statistics - Can Use My Statistics | The agent is permitted to use the My Statistics tab to view Key Performance Indicators. |
| Statistics - Can Use Contact Center Statistics | The agent is permitted to use the Contact Center Statistics tab to view Object Metrics (Contact Center Statistics). |
| Statistics - Can Use Gadget Statistics | The agent is permitted to use the Statistics Gadget to view Key Performance Indicator and Contact Center Statistics. |

# Team Communicator privileges

The following table lists the Team Communicator privileges in the `Workspace Team Communicator Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Team Communicator Privileges**

| Role privilege | Description |
|---|---|
| Team Communicator - Can Use | The agent is permitted to use the Team Communicator. The other Team Communicator privileges cannot be configured if the value is `Not Assigned`. |
| Team Communicator - Can Manage Favorites | The agent is permitted to add, edit, and remove personal favorite internal targets and contacts in the Team Communicator. This privilege is dependent on Team Communicator - Can Use. |
| Team Communicator - Can View Favorites | The agent is permitted to see and use the favorite internal targets and contacts that they have saved in the Team Communicator. This privilege is dependent on Team Communicator - Can Use. |
| Team Communicator - Can View Recent Calls | The agent is permitted to see and use the recent call list of internal targets and contacts that they have saved in the Team Communicator. This privilege is dependent on Team Communicator - Can Use. |
| Team Communicator - Can Search All | The agent is permitted to search within all internal targets and contacts in the Team Communicator. This privilege is dependent on Team Communicator - Can Use. **Added:** 8.1.40x.xx |

# Team Lead privileges

[**Modified:** 8.5.126.07]

The following table lists the Team Lead privileges in the `Workspace Team Lead Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group). Also, refer to the Procedure: Enabling agents to be Team Leads.

**Team Lead Privileges**

| Role privilege | Description |
|---|---|
| Team Lead - Can Use | Allows the agent to use Team Lead functionality. |
| Team Lead - Can Auto Coach Voice Interactions | Permits a Team Lead to automatically coach all the voice interactions of a selected agent. |
| Team Lead - Can Auto Coach Chat Interactions | Permits a Team Lead to automatically coach all the chat interactions of a selected agent. |
| Team Lead - Can Auto Monitor Chat Interactions | Allows the automatic monitoring of all the chat interactions of a selected agent. |
| Team Lead - Can Auto Monitor Voice Interactions | Allows the automatic monitoring of all the voice interactions of a selected agent. |
| Team Lead - Can Barge-in Chat | Allows the team lead to Barge in to Chat interactions. |
| Team Lead - Can Barge-in Voice | Allows the team lead to barge in to voice interactions. |
| Team Lead - Can Change Agent State | Allows the team lead to change the status of a supervised agent. **Added:** 8.5.126.07 |
| Team Lead - Can Coach Chat Via Chat | Allows the team lead to coach an agent via the chat channel for a monitored chat interaction. |
| Team Lead - Can Coach Chat Via Voice | Allows the team lead to coach an agent via the voice channel during a monitored chat interaction. |
| Team Lead - Can Coach Chat and Voice Via IM | Allows the team lead to coach an agent via the instant messaging channel during a monitored chat or voice interaction. |
| Team Lead - Can Coach Current Voice Interactions | Permits a Team Lead to coach the current voice interactions of a selected agent. |
| Team Lead - Can Coach Current Chat interactions | Permits a Team Lead to coach the current chat interactions of a selected agent. |
| Team Lead - Can Monitor Current Monitor Chat Interactions | Allows the monitoring of a selected active chat interaction of a selected agent. |
| Team Lead - Can Monitor Current Voice Interactions | Allows the monitoring of the currently active voice interaction of a selected agent. |
| Team Lead - Can Stop Supervising Chat | Allows the team lead to stop supervising chat interactions for the selected agent. |

| Role privilege | Description |
|---|---|
| Team Lead - Can Stop Supervising Voice | Allows the team lead to stop supervising voice interactions for the selected agent. |

# Voice privileges

The following table lists the voice privileges in the `Workspace Voice Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Voice Privileges**

| Role privilege | Description |
|---|---|
| Voice - Can Answer Call | The agent can choose to answer a voice interaction that is routed to their desktop. Auto-answer is disabled. |
| Voice - Can Use Voice Channel | The agent is permitted to use the voice channel. The other voice privileges cannot be configured if the value is `Not Assigned`. |
| Voice - Can Answer Call | The agent can choose to answer a voice interaction that is routed to their desktop. Auto-answer is disabled. |
| Voice - Can Delete From Conference | The agent can remove a party from a voice conference. |
| Voice - Can Forward Call | The agent is permitted to configure a call forward to a different number for voice interactions. |
| Voice - Can Hold/Retrieve Call | The agent is permitted to put voice interactions on hold and retrieve voice interactions that are on hold. |
| Voice - Can Make Call | The agent is permitted to call both internal targets and contacts. |
| Voice - Can End Consultation Call | The agent is permitted to manually end a voice consultation call. The behavior of this privilege depends on the option voice.end-consultation-method. |
| Voice - Can One Step Conference | The agent is permitted to start conferences without speaking with the target first (Instant Conference). |
| Voice - Can One Step Transfer | The agent is permitted to transfer calls without speaking with the target first (Instant Transfer). |
| Voice - Can Suspend or Reinstate A Conference Party [**Modified:** 8.5.109.16] | Enables a conference member to suspend another member from the conference or reinstate a member to the conference. Enables agents in a conference to prevent a party in the conference from listening to the call (Suspend the party from the conference). Once listening is denied, any agent can then re-allow the party to listen to the conference (Reinstate the party to the conference). If you use SIP Server to control the voice channel, SIP Server version 8.1.101.81 or higher is required to support this feature. This privilege was formally Voice - Can Deny Or Authorize Listening For A |

| Role privilege | Description |
|---|---|
| | Conference Party. |
| Voice - Can Reject Call | The agent can choose to reject a voice interaction that is routed to their desktop. |
| Voice - Can Release Call | The agent is permitted to manually end calls. |
| Voice - Can Send DTMF | The agent is permitted to attach DTMF to the call data. |
| Voice - Can Set Interaction Disposition | The agent is permitted to specify the call outcome by setting the disposition code. |
| Voice - Can Two Step Conference | The agent is permitted to contact and speak (consultation) prior to starting a conference. |
| Voice - Can Two Step Transfer | The agent is permitted to contact and speak (consultation) prior to transferring the voice interaction to the target. |
| Voice - Show Silent Monitoring | The agent is permitted to know when they are being silently monitored by a supervisor. |
| Voice - Can Suspend or Reinstate Customer Party in a Coached Call<br>[**New:** 8.5.155.03] | Enables an agent or supervisor to suspend or reinstate the caller from a coached call. |

# Voicemail privileges

[**Added:** 8.5.100.05] [**Modified:** 8.5.118.10]

The following table lists the Voicemail privileges in the `Workspace Voicemail Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Voicemail Privilege**

| Role privilege | Description |
|---|---|
| Voice Mail - Can Use | The agent is permitted to use the voicemail feature to use, control, and monitor Voicemail boxes. |
| Voice Mail - Can Deposit Message | The agent is permitted to call the voicemail box of another agent or agent group. [**Added:** 8.5.118.10] |
| Voice Mail - Can Transfer Message | The agent is permitted to transfer a call to the voicemail box of another agent or agent group. [**Added:** 8.5.118.10] |

# Web Callback privileges

The following table lists the Web Callback privileges in the `Workspace Web Callback Access` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Web Callback Privileges**

| Role privilege | Description |
|---|---|
| Web Callback - Can Cancel | Permits an agent to decline a Web Callback so that it is not processed. Depends on 'Web Callback - Can Use Web Callback Channel'. **Added:** 8.1.40x.xx |
| Web Callback - Can Use Callback Channel | The agent is permitted to use the Web Callback media channel. |
| Web Callback - Can Decline | The agent is permitted to reject Web Callback interactions that are directed to the agent. |
| Web Callback - Can Reject | Permits an agent to decline a Web Callback so that it can be processed by a different agent. Depends on 'Web Callback - Can Use Web Callback Channel'. **Added:** 8.1.40x.xx |
| Web Callback - Can Reschedule | The agent is permitted to reschedule a Web Callback interaction. Use the Web Callback - Can Reschedule Before Call privilege to allow rescheduling before the call is dialed. Depends on Web Callback - Can Use Web Callback Channel. **Modified:** 8.1.40x.xx |
| Can Reschedule Before Call | The agent is permitted to reschedule a Web Callback Preview at a different date and/or time. The Can Reschedule privilege must be enabled for this privilege to be active. If Can Reschedule is enabled but Can Reschedule Before Call is disabled, agents can still reschedule the Web Callback Preview after they have connected and disconnected the call. Depends on 'Web Callback - Can Reschedule'. **Added:** 8.1.40x.xx |
| Web Callback - Can Reschedule On New Number | The agent is permitted to reschedule a Web Callback interaction by using a new phone number. |
| Web Callback - Can Set Interaction Disposition | The agent is permitted to set the disposition code of a Web Callback interaction. |
| Web Callback - Can Mark Done | The agent is permitted to mark inbound Web Callback interactions as Done without processing them further. |

# Workbins privileges

[**Modified:** 8.5.110.13]

The following table lists the Workbin privileges in the `Workspace Workbin Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Workbin Privileges**

| Role privilege | Description |
|---|---|
| Workbins - Can Search in Workbins | The agent is permitted to use the search filter function in the My Workbins and My Team Workbins views. **Added:** 8.5.110.13 |
| Workbins - Can Use My Workbins | The agent is permitted to access the My Workbins functions. **Modified:** 8.1.40x.xx |
| Workbins - Can Use My Team Workbins | The agent is permitted to access the My Team Workbin functions. **Added:** 8.1.40x.xx |

Workbin - Can search in Workbins

# Workitem privileges

The following table lists the Workitem privileges in the `Workspace Workitem Privileges` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Workitem Privileges**

| Role privilege | Description |
|---|---|
| Workitem - Can Use WorkItem Channel | The agent is permitted to use the workitem media channel. |
| Workitem - Can Decline | The agent is permitted to decline incoming workitem interactions. |
| Workitem - Can One Step Transfer | The agent is permitted to use the instant-transfer functionality. |
| Workitem - Can Set Interaction Disposition | The agent is permitted to set the disposition code of a workitem interaction. |
| Workitem - Can Mark Done | The agent is permitted to mark workitem interactions as `Done`. |
| Workitem - Can Move To Workbin | The agent is permitted to move workitem interactions to a workbin for later handling or handling by another agent or agent group. |

# Workspace SIP Endpoint privileges

The following table lists the Workspace SIP Endpoint privileges in the `Workspace SIP Tasks` section of the `Role Privileges` tab that can be enabled for a role. Privileges are assigned as configuration options in the `Role Privileges` tab of the Role object in Genesys Administrator Extension (refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group).

**Workspace SIP Endpoint Privileges**

| Role privilege | Description |
|---|---|
| SIP Endpoint - Can Use Embedded SIP Endpoint | Indicates if Workspace will start automatically an embedded SIP Endpoint for the SIP Agent. If set to false, you will require an external SIP Endpoint application. |