Genesys SR Service

8.5.230.23

12/21/2025

8.5.230.23

Genesys SR Service Release Notes

Release Date	Release Type	Restrictions	AIX	Linux	Solaris	Windows
02/01/16	General	Under Shipping Control				X

Contents

What's New

This release contains the following new features and enhancements:

- Citrix is now supported on Windows 2008 R2 for the SR Service.

- Support for SR Service on Windows 10 (32-bit + 64-bit).

- Support for SR Service Windows 8 / 8.1 32-bit.

- SR Service Auto-upgrade will only install digitally signed versions. Version Checksum verification is deprecated (`softwareChecksum` parameter).

- Auto-Downgrade is disabled and the `forceUpdate` parameter has been deprecated.

- The `allowedHosts` configuration parameter was added.

- SR Service now adds a unique ID as part of the voice recording file name.

- SR Service Authentication server now runs as a separate process.

- If the Agent credentials are invalid (403) or missing when trying to upload a screen recording to GWS, the SR Service will use another agent's credentials to upload the recordings and will log an appropriate log warning.

- SR Service log files have been moved under the Logs folder.

- The SR Service log now includes milliseconds.

- SR Service HTTPS certificate verification default behavior changed from False to True ("certificate" parameter default value).

- SR Service now supports:

    - Simultaneous screen recordings from multiple users.

    - Working with multiple different GWS instances simultaneously.

    - CSRF protection on local host communication with WWE.

    - Session cookies for the local host connection with WWE.

    - Using the network path for the recordings post processing and recordings shared folder. Please note the local system account must be given access permissions.

    - Separate configuration for the user Temp folder, Post Processing folder, and the Shared Recording folder using the following configuration parameters: `userSavePath, postProcessingSavePath, sharedSavePath`.

- SR Service Auto Updater will now only start after an agent logs in.

- Some SR Service client side parameters can now be dynamically configured in real time using the agent desktop.

- The SR Service version can now be queried using the browser.

Helpful Links

Releases Info

- List of 8.5.x Releases
- 8.5.x Known Issues

Product Documentation

Genesys Interaction Recording

Genesys Products

List of Release Notes

- The `diskFreeSpaceLimit` configuration parameter is now a client side parameter. Previously, it was a server side parameter.

Resolved Issues

This release contains the following resolved issues:

User Session detection fallback logic now supports Remote Desktop Protocol (RDP). (GIR-4259)

If the upgrade process fails during auto-upgrade, the SR Service will now rollback the upgrade changes and restart the service. (GIR-4235)

The `credentialsTimeout` configuration parameter now reflects minutes. Previously, this parameter reflected seconds. (GIR-4152)

SR Service no longer sends the "WWW-Authenticate" HTTP header on 401 responses. As a result, the credentials pop up on the web browser no longer appears. (GIR-3956)

The SR Service Recorder process name was changed from SRC.exe to SrsProcess.exe. (GIR-3848)

When the SR Service receives a 403 authentication error due to bad credentials, it will not retry to upload a screen recording using the same credentials. Previously, the SR Service continuously retried to upload the recording using the same incorrect credentials. (GIR-3778)

The SR Service default Temp folder (that is, the data save location), moved from the installation folder to the Windows LOCALAPPDATA. (GIR-3574)

The SR Service now uploads a recording using the credentials of the user that created the recording. Previously, the SR Service used any credentials to upload any recordings, regardless of which user created which recordings. (GIR-3540)

A separate log file is no longer created when you are logged in as an agent desktop and the SR Service is restarted. Previously, an exception was logged and a separate log file (SRC.EXE.LOG) was created. (GIR-3169)

Server TLS certificate validation is now enabled by default. Previously, the Server TLS certificate validation was disabled by default. (GIR-3019)

Upgrade Notes

No special procedure is required to upgrade to release 8.5.230.23.