Genesys Recording, Quality Management, and Speech Analytics Administrator's Guide

12/7/2025

Table of Contents

Search the table of all articles in this guide, listed in alphabetical order, to find the article you need.

Related documentation:

-
-

Get started

- 
- Administrator

Learn how to get started with the Recording, QM, and Speech Analytics solution.

Related documentation:

-

Contents

The Genesys Recording, QM and Speech Analytics solution leverages recorded customer interactions for review and analysis of critical business issues.

Designed to provide valuable voice interaction information in an intuitive and easy to use user interface, the solution allows you to uncover valuable insights about workforce performance and the customer experience that may be hidden within the agent-customer interactions your organization records. It provides insight into the cause and effect relationships that influence business issues and contact center performance.

In addition, with the optional Quality Management (QM) add-on product, specific agent training requirements, compliance breaches or customer satisfaction issues can be assessed on a regular basis to improve agent performance and customer service delivery.

With the Speech Analytics add-on, you can analyze 100% of recordings to uncover why customers are contacting your company, what are their topics of conversation, why multiple contacts are needed to resolve specific issues, what processes cause customer frustration and whether your agents are providing an appropriate level of service.

Important

SpeechMiner UI provides a single user interface (UI) across different products within the Genesys Workforce Optimization suite in Genesys Multicloud CX, including Interaction Recording, Quality Management and Speech Analytics, each product is sold separately. Interaction Recording is a pre-requisite, however, Quality Management and Speech Analytics can be added based on the specific needs of your business.

Screen recording is available only for voice interactions. Screen recording of chat and email interactions is not available.

The Genesys Recording, QM and Speech Analytics solution does not include:

- Text Analytics
- Access to SMART for Topics/Category creation
- Export of transcripts or Analytics data
- Distinct retention periods for Analytics and QM data; the retention period for all data is tied to the retention period of the underlying call recording

For additional information about the Genesys recording solution refer to:

How Recording, Quality Management and Speech Analytics works: The Recording, QM and Speech Analytics solution evaluates recorded customer interactions (from any recording system) for data about what is happening in your organization, and uncovers the cause and effect relationships that influence business issues and contact center performance.

Recording Certificate Management: The Genesys recording solution enables proper management of public and private keys used to encrypt voice and screen recordings.

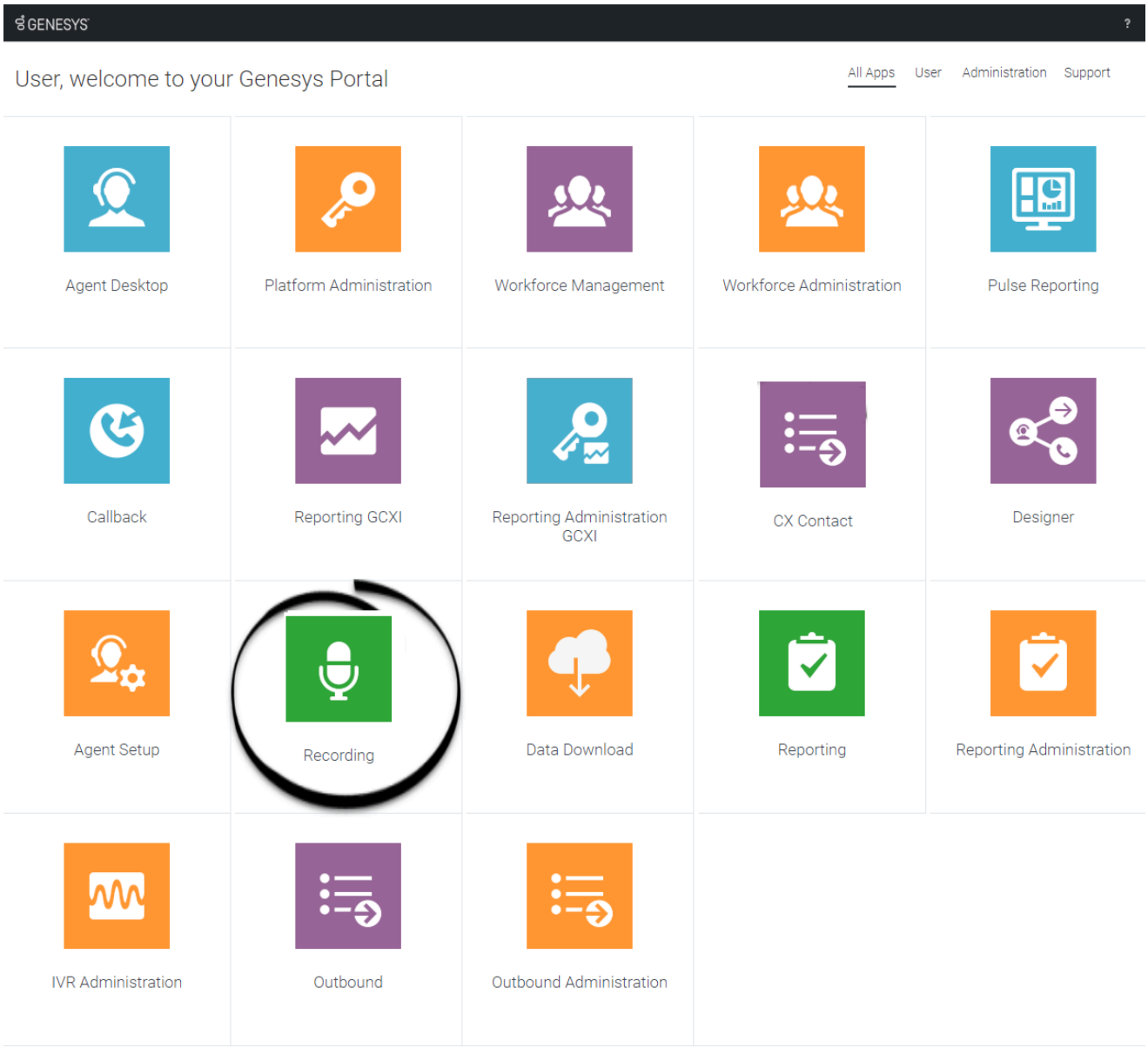
Access control for Recording users: The Genesys recording solution applies access control to recordings.

Deploying the Screen Recording Service: The Screen Recording Service (SR Service) enables the

Agent to capture what is happening on the screen at the time of an active voice interaction.

Recording Cloud Backup Service: The Recording Cloud Backup Service (RCBS) allows you to make a backup copy of your Genesys Interaction Recording voice files (some or all) prior to their automated deletion as per the Cloud retention policy.

Access the application



Once your Genesys Multicloud CX environment is up and running and you've checked that you meet the necessary requirements, log in to your Genesys Portal to access Recording. Click the Recording

icon and enter your username and password.

Multilingual support

SpeechMiner web application supports multiple languages. When you log into SpeechMiner, the web UI is displayed in a language that you selected in the browser. If you select an unsupported language in the browser, the SpeechMiner Web UI defaults to en-US.

SpeechMiner language support

SpeechMiner language recognition and user interface (UI) support is available for the following languages:

Language	Recognition Support	UI Support
Dutch - NL	X	Dutch - NL
English - USA	X	English - USA
English - UK	X	English - USA
English - Australia	X	English - USA
English - South African	X	English - USA
English - Indian	X	English - USA
French - Canadian	X	French - Canadian
Russian - Russia	X	Russian - Russia
Spanish - USA	X	Spanish - Mexican
Spanish - Columbian	X	Spanish - Mexican
Spanish - Mexican	X	Spanish - Mexican
Spanish - Spain	X	Spanish - Spain
German - Germany	X	German - Germany
Portuguese - Brazil	X	Portuguese - Brazil
Korean - Korea	X	Korean - Korea
French - France	X	French - France
Japanese - Japan	X	Japanese - Japan
Mandarin - China	X	Simplified Chinese (labeled as Mandarin)
Italian - Italy	X	Italian - Italy
Arabic - World Wide	X	Arabic - World Wide
Turkish - Turkey	X	Turkish - Turkey
Cantonese - Hong Kong	X	Traditional Chinese (labeled as Cantonese)

Recording certificate management

Contents

- 
- Administrator

The Genesys recording solution requires proper management of public and private keys used to encrypt voice and screen recordings. This page describes the process for generating and installing the public and private keys.

Related documentation:

-
-

The Genesys recording solution requires proper management of public and private keys used to encrypt voice and screen recordings. The public key is stored in a certificate file and is used to encrypt a unique session key that is then used to encrypt each media file. The public key must be provisioned for voice recordings and for screen recordings. The private key is stored securely on a protected server and is used to help decrypt each media file (voice or screen) for playback.

Protect your keys!

- **It is your responsibility to store your private keys and certificates, including the expired ones**. Genesys will not be able to re-apply any of your keys or certificates in the event of a catastrophic Genesys site failure. In this case, you will need to re-apply any previously created keys. Therefore, keep these keys somewhere safe and reliable for future use.
- Furthermore, if you are taking advantage of the Recording Cloud Backup Service utility, you will need to have these keys and certificates available in order to listen to the recordings once they have been moved to your own site.

Please contact your Genesys Professional if you have any questions.

Certificate requirements

Before you can encrypt certificates for voice and screen recordings, you must generate the following keys and certificates:

- Generate a recording private key in `.pem` format.
  2048-bit RSA (or higher). Align encryption strength requirements with your IT Security.
- Generate a self-signed recording certificate (also known as a public key) in `.pem X.509 RSA` format. The certificate validity period will determine when the next certificate should be generated for renewal.
  Note: It is the customer's responsibility to track this, install a new key and certificate prior to expiry and contact Genesys to help provision the new key and certificate before the expiration date.

Generating a self-signed certificate key pair using OpenSSL

> **Important**
>
> To generate a self-signed certificate key pair using OpenSSL you must have access to a Linux/Windows system with OpenSSL installed.

The following OpenSSL commands generate a private key and then use the private key to generate a self-signed certificate:

```
openssl genrsa -out tenant.key 2048

openssl req -new -x509 -key tenant.key -out tenant.pem -days validity_period -subj
"/CN=common_name/C=Country/ST=State/O=Organization"
```

Example:

```
openssl genrsa -out tenant.key 2048

openssl req -new -x509 -key tenant.key -out tenant.pem -days 3650 -subj "/CN=Genesys
Recording/C=US/ST=California/O=Genesys"
```

Refer to the following table for DN field descriptions and sample values:

DN Field	Description	Example
Common Name (CN)	The name of your recording solution.	Genesys Recording
Country (C)	A two-letter country code.	US
State or Province (ST)	The full state or province where your organization is legally located.	California
Organization (O)	The exact legal name of your organization. Do not abbreviate your organization name.	Genesys

As a result of this command, the following two files are created:

- tenant.key—the private key (PEM format) that is used to decrypt the recordings. It must be kept safe and should not be shared.
- tenant.pem—a self-signed recording certificate and the public key.

> **Important**
>
> **Azure hosted deployments** If your deployment is hosted on Azure, you must perform an extra step to convert the private key (see the next section).

Convert the private key (Azure only)

This step applies only to deployments hosted on **Azure**. Perform the following step to convert the private key (**tenant.key**) to a new format that can be used in Agent Setup:

```
openssl pkcs8 -topk8 -inform pem -in tenant.key -outform pem -nocrypt -out private.pem
```

This command converts the private key that you generated earlier (**tenant.key**) to a new file (**private.pem**) that can be uploaded and managed using Agent Setup. Thus, your private and public key files for Agent Setup are created as follows:

- **tenant.pem**—a self-signed recording certificate and the public key.
- **private.pem**—the private key (PEM format) that is used to decrypt the recordings. It must be kept safe and should not be shared.

When the keys are ready, follow the steps in Upload recording certificates (Azure).

Uploading/installing certificates to encrypt your voice recordings

Depending on your cloud hosting platform, follow the steps described in Upload recording certificates (AWS) or Upload recording certificates (Azure).

Upload recording certificates (AWS)

> **Important**
>
> The following steps describe how to configure encryption for voice recordings and should be performed by an administrator.

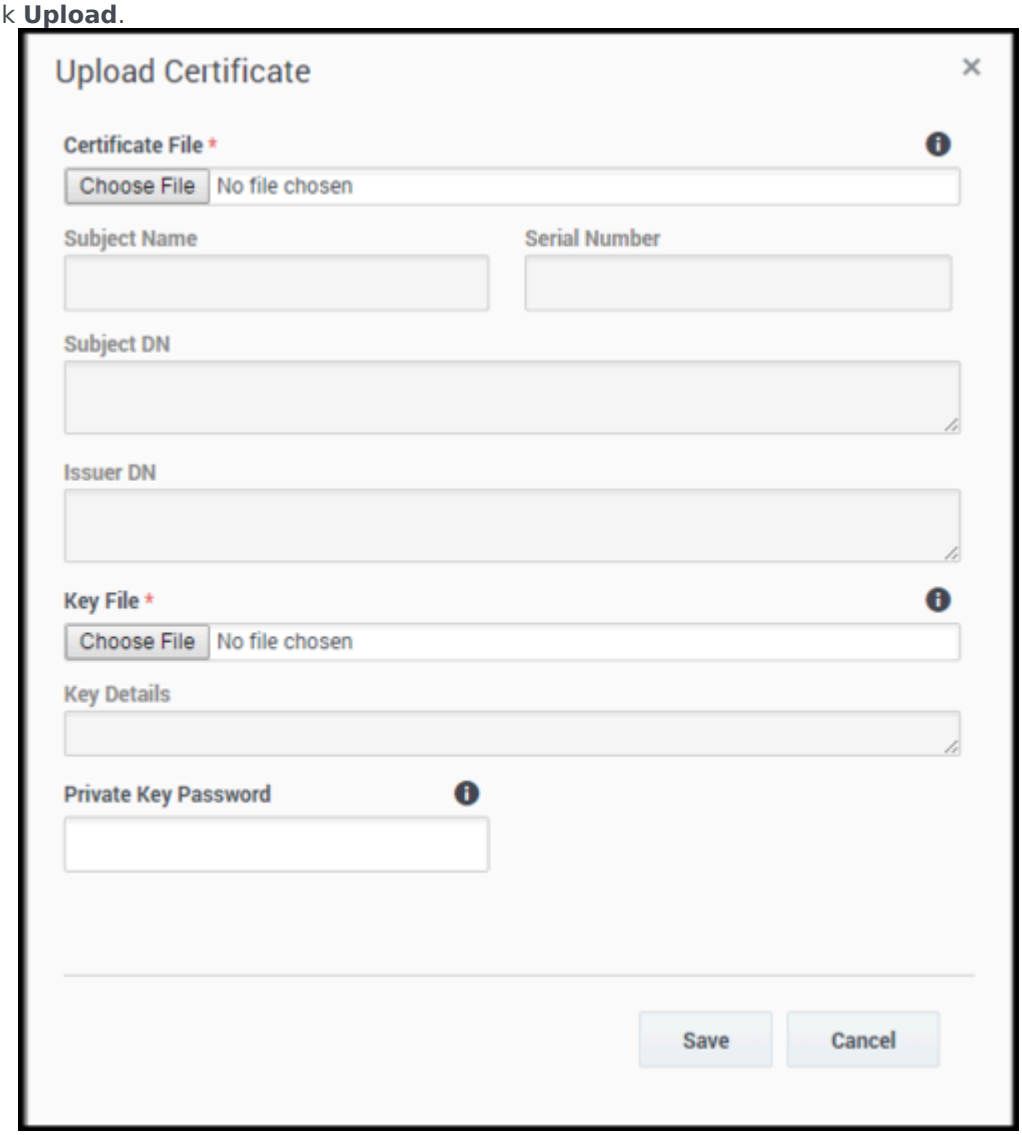
1. Verify that you have Administrator privileges.

   > **Important**
   >
   > The Platform Administration section of the Genesys Portal is the tool that should be used to manage recording certificates (public keys), and private keys.

2. Select **Administration > Certificates**.
   The **Recording Certificates** screen displays the list of defined Recording Certificates. To refresh the list at any time, click  .

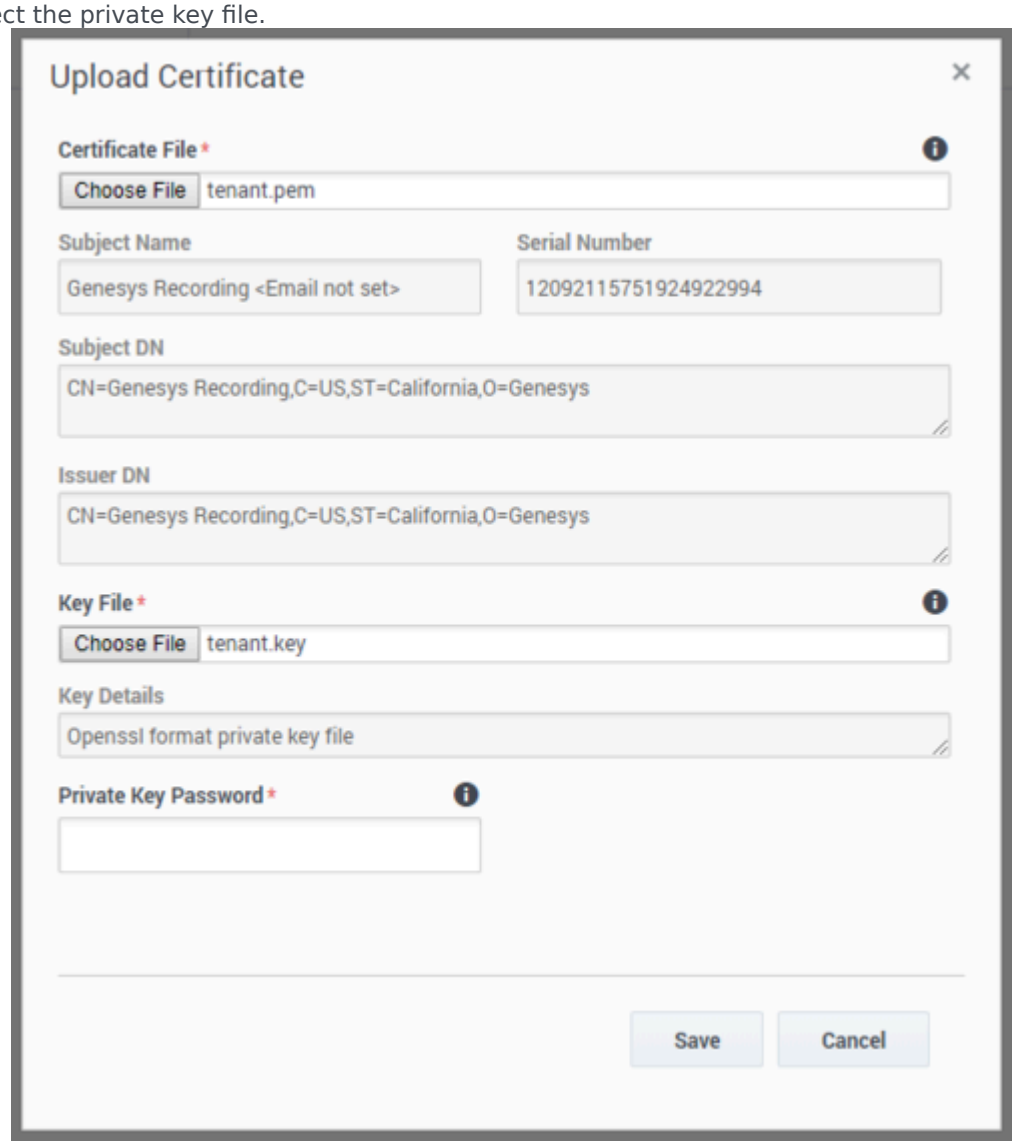
> **Tip**
> Click a recording certificate in the list to display its details.

3. Click **Upload**.



4. In the **Upload Certificate** panel, under **Certificate File**, click **Choose File**.

5. Select the recording certificate file (PEM file).
   The **Subject Name**, **Serial Number**, **Subject DN**, and **Issuer DN** fields automatically populate.
6. In the **Key File** section, click **Choose File**.
7. Select the private key file.



8. Leave the **Private Key Password** field empty.
9. Click **Save**. Both public and private keys are stored in a secure keystore file dedicated to your tenant.
10. After uploading the self-signed recording certificate you must contact your Genesys Professional and ask them to have the certificate assigned to your IVR profile. You will be asked for a copy of the Self-Signed Recording Certificate. You do not need to provide them your private key.

Important

- If you upload and/or delete recording certificates in one Platform Administration session, these changes are not reflected in another Platform Administration session. You must log out and log in again to the second Platform Administration session.
- In the Certificate Administration section, there is an option to Delete certificates. Do not delete any certificates without first discussing this with your Genesys Professional, since there may be adverse side-effects of doing this (for example, not being able to playback recordings). Even if a certificate is expired, it will need to remain in the system so that older recordings can be played back.

Upload recording certificates (Azure)

Important

The following steps should only be performed by an administrator or your Genesys representative.

The public and private keys are stored in a certificate file and are used to encrypt a unique session key that is then used to encrypt each media file. These keys must be provisioned for voice recordings. To learn how to generate the public and private keys, see Certificate requirements.

1. In Agent Setup, under the **Contact Center Settings** tab, go to **Keys Management** and select **Keys**.
2. Click **Upload Certificate**, and then click the browse icon () to locate and select the recording file on your local machine.

   ### Important

   Certificate files must be in Privacy Enhanced Mail (PEM) format.

3. Click **Save**. Agent Setup validates the format and stores the uploaded certificate file in the tenant "record" GVP IVR Profile (in the GVP Config Server) and then displays the **Key** and **Alias**.

Provisioning certificates for screen recording

Perform the following steps to configure encryption for screen recordings, only after completing the Uploading/installing certificates to encrypt your voice recordings procedure. If you have not purchased screen recording services, you may skip this step.

Screen Recording Certificates list

The Screen Recording Certificates page enables you to manage the certificates for screen recording encryption.

- Assign new certificates
- Remove certificates

Assigning Screen Recording Certificates

To assign a new certificate:

1. In the header, go to **Administration > Screen Recording Certificates**.
2. On the **Screen Recording Certificates** panel, click **Add**.
3. From the **Select Certificate** window, perform one of the following actions:
   - Select the check box next to the appropriate certificate, and click **Add**.
   - Click **Cancel** to discard any changes.
   - Perform one of the following actions:
   - Click the **Save** button to accept the changes.
   - Click the **Cancel** button to discard the changes.

Removing Screen Recording Certificates

To remove a Recording Certificate, perform the following actions:

1. In the header, go to **Administration > Screen Recording Certificates**.
2. On the **Screen Recording Certificates** panel, select the check box next to the certificate that you want to remove.
3. Click **Remove**.
4. Perform one of the following actions:
   - Click the **Save** button to accept the changes.
   - Click the **Cancel** button to discard the changes.

Important

- If you remove a certificate from the Screen Recording Certificates, you will turn off encryption, and screen recordings will no longer be encrypted. Do not remove any certificates without first discussing this with your Genesys Professional.
- The modifications to encryption settings described in this document only affect future recordings and do not change the encrypted status of old recordings.

Access control for Recording users

Contents

- 
- Administrator

Each recording file is considered an object that is subject to access control at the user level. This page describes how to control user access.

Related documentation:

-
-

When a recording file is generated, the access control for the recording file is set based on the following criteria:

1. Access control is set based on the agent that was recorded. Agents are organized as an agent hierarchy; for example, the hierarchy can be a reporting structure in an organization.
   Note: With IVR recording, there is no associated agent for the specific segment of the call, since IVR is not a user.
2. Access control is set based on partitions. Partitions are set as a specific attached data in a call, and the attached data is typically set by a routing strategy.

To search and playback a recording file that is subject to access control, the user accessing the Recording application must be assigned to the appropriate Access Groups to access the recordings. If the user accessing the application is an agent, they are granted implicit playback access to their own recordings.

Agent hierarchy

The agent hierarchy shows how the agents are organized in the hierarchy, and the hierarchy is represented as a field configured within Agent Setup. For more information, see the description of the Recording Hierarchy option in Manage agents and other users.

The following example shows the agent hierarchy with four agents:

- /
  - Anthony
    - John
      - Agent1
      - Agent2
    - Paul
      - Agent3

- Agent4

`Agent1` and `Agent2` are on John's team. John reports to Anthony.

To represent this structure, the following fields are configured in each agent:

Agent	agent_hierarchy
Agent1	/Anthony/John
Agent2	/Anthony/John
Agent3	/Anthony/Paul
Agent4	/Anthony/Paul

> **Important**
>
> When there are agents specified in the path, the path must contain the username for those agents. For example, for the hierarchy `/Anthony` and `/Anthony/John`, Anthony and John must match the usernames for Anthony and John.

If a user wants to listen to recordings handled by `Agent1`, the user needs to be granted access to either the `Anthony`, or the `John` Access Group. If a user is granted access to the `Anthony` Access Group, that user has access to recordings from all four agents, because all four agents are within Anthony's hierarchy.

Partitions

Partitions are arbitrary names that allows a contact center to partition recordings based on business rules. For example, partitions can be business groups such as sales, support, marketing, etc. To set one or more partitions to a recording, attach data to the call with the `GRECORD_PARTITIONS` key with a comma-separated list of partition names.

For example, if the `GRECORD_PARTITIONS` key is set to `/sales,/support`, the recording belongs to the `/sales` partition as well as the `/support` partition.

To access any recording belonging to a partition, the user must be assigned to an Access Group with the same name. For example, if `user1` is assigned to the `/sales` Access Group, `user1` can search and playback any recordings within the `/sales` partition.

Access groups

All access groups for recording purposes must be created within the **Recording** folder. The access group "/" grants access to all recordings. For more information on configuring access groups, see Access Groups.

Deploying the Screen Recording Service

Contents

- 
- Administrator

Genesys Interaction Recording (GIR) requires that a Screen Recording Service (SRS) be installed on each Agent's desktop. This page describes how to install the SRS.

Related documentation:

-
-

Genesys Interaction Recording (GIR) requires that a Screen Recording Service (SRS) be installed on each Agent's desktop to enable the Agent to capture what is happening on the screen at the time of an active interaction.

The procedures on this page show how to download, install, configure and test the Screen Recording Service.

> **Important**
> In a Genesys Multicloud CX deployment, screen recording is available only for voice interactions. Screen recording of chat and email interactions is not available in a Genesys Multicloud CX deployment.

Prerequisites

The following list provides you with the requirements you need to successfully deploy the Screen Recording Service (SRS):

- Before you can install and use the SR Service on your desktop, you must have the following information ready at hand. Your IT department or Genesys Professional can help you get this information.
  - Access to Agent Workspace
  - The software (minimum version 8.5.302.10)
- Verify that the client machine meets the following minimum specifications:
  - Pentium Dual Core CPU
  - 2 GB RAM (800 MB available for the SR Service)
  - A minimum of 5 GB of available space (in total) for the SR Service installation and working space.
- If you are running Bria 4 on Windows 7, you must enable Windows Aero. If you do not enable Windows

Aero, the Screen Recording Service may fail to capture the Bria 4 application.

- Verify the client machine is synchronized with an NTP server — for example, www.time.gov.

Installation considerations

After verifying that your system meets the basic prerequisites, you should consider the following:

- The recommended installation procedure will install the Screen Recording Service's self-signed PFX certificates to the root certificates store.
- When required use one of the following options to query the SR Service version:
  - Run the following command line `wmic datafile where name='C:\\\\GenesysServiceHandler.exe`.
  - Open the web browser and navigate to https://127.0.0.1/version if the SR Service is deployed with HTTPS enabled or http://127.0.0.1:8080/version if the SR Service is running as HTTP.
- Proxy support for outbound connections from SRS can be enabled either with or without authentication support.
  - The parameters used to configure the SRS Proxy are available in Advanced configuration for the Screen Recording Service.
- When a proxy is used it may interfere with the SR Service operation. The SR Service runs as an HTTP server and relies on an incoming socket connection to correctly identify the agent's windows session. If the HTTP requests are forwarded by a proxy, the SR Service may not be able to correctly identify the user session in a multi-user environment. With a single user, the SR Service will rollback to the currently active windows session.
  When a proxy is used it is recommended that localhost (127.0.0.1) connections be excluded from the proxy settings.

  When the proxy is an internal system service (like an Antivirus\Firewall), it is recommended that the SRS related processes (SrsProcess.exe and GenesysServiceHandler.exe) be added to the security software exception\white list.
- The Screen Recording Service can be used by a Citrix client. The following Citrix configurations are supported:
  - Citrix XenApp 6.x running under Windows Server 2008 R2 or Windows Server 2012 R2
  - Citrix XenApp 7.x or Citrix XenDesktop 7.x running under Windows Server 2008 R2 or Windows Server 2012 R2
- In a Citrix environment (for Genesys SR Service 8.5.230.23 and later), SRS only supports a single session per remote PC (Session Sharing is not supported).
- In a Citrix environment (for Genesys SR Service 8.5.370.85 and later), SRS can be configured to work with Citrix's Virtual Loopback feature.
  - Configure the `authenticationHost` parameter so that SRS uses a loopback IP address that is outside of the range being used by the Citrix Virtual Loopback Feature. See Advanced configuration for the Screen Recording Service for more details on how to configure the `authenticationHost` parameter.
- If SRS is deployed on a Citrix VDA, you need to disable Citrix API hooks for vlc.exe by creating the following registry values. For more information, see How to Disable Citrix API Hooks on a Per-application

Basis.

- **Keys:**
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook
  - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook
  - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook64
- **Value Name:** ExcludedImageNames
- **Type:** REG_SZ
- **Value:** vlc.exe

- If the IPv4 SRS `authenticationHost` parameter is configured to something other than 127.0.0.1, then use that IP address instead of 127.0.0.1 in the above URLs. See Advanced configuration for the Screen Recording Service for more details.
- If the IPv4 SRS `authenticationHost` parameter is configured to something other than 127.0.0.1, and SRS is configured to use HTTPS, then use that IP address when creating self-signed certificates. See Creating Self-Signed Certificates to support IP Loopback Addresses other than 127.0.0.1 for more details.
- The SR Service can be used in a VMware Horizon environment. The following VMware Horizon configuration is supported:
  - VMware Horizon 7 running under Windows Server 2012 R2
- If you are using Workspace Web Edition or Workspace Desktop Edition and the SR Service with Genesys Softphone in a VDI environment (such as Citrix Xenapp), you must configure the `screen-recording-client-address` option to point to the SRS Loopback address.

Screen Recording Service - operating systems

The Screen Recording Service is supported on the following operating systems in a non-Citrix mode:

- Windows 7 (32 and 64 bit)
- Windows 8, 8.1 (32 and 64 bit)
- Windows 10 (32 and 64 bit)

The Screen Recording Service is supported on the following operating systems for Citrix support:

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2019

The Screen Recording Service is supported on the following operating system for VMware Horizon support:

- Windows Server 2012 R2
- Windows Server 2019

Recommended screen resolutions

Genesys has tested the Screen Recording Service under the following recommended screen resolutions. If you use the Screen Recording Service on a computer with different screen resolution than listed above, you should do a field validation of the Screen Recording Service in your setup to ensure that it is working properly. If there you encounter unexpected results, Genesys recommends that you set your screen resolution to one of the recommended and tested resolutions listed below.

> ### Warning
> If a field validation has been completed against an earlier version using a non-supported resolution, there is no guarantee that resolution will continue to work on upgrades to new releases. Only supported resolutions are continually tested against each new version.

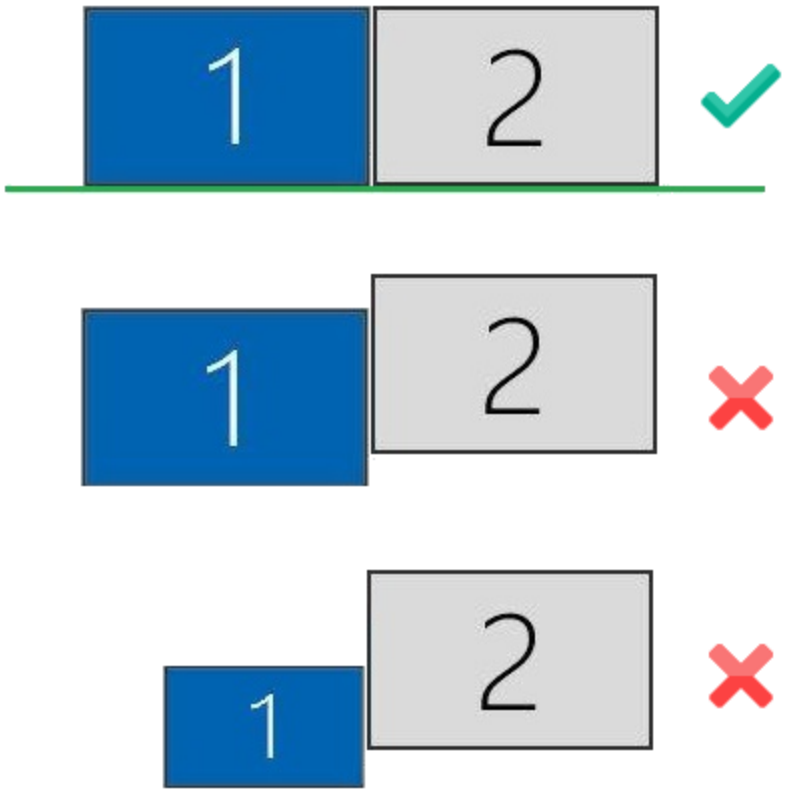
Single Monitor:

- 1024 x 768
- 1280 x 720
- 1600 x 1200
- 1920 x 1080

Dual Monitor:

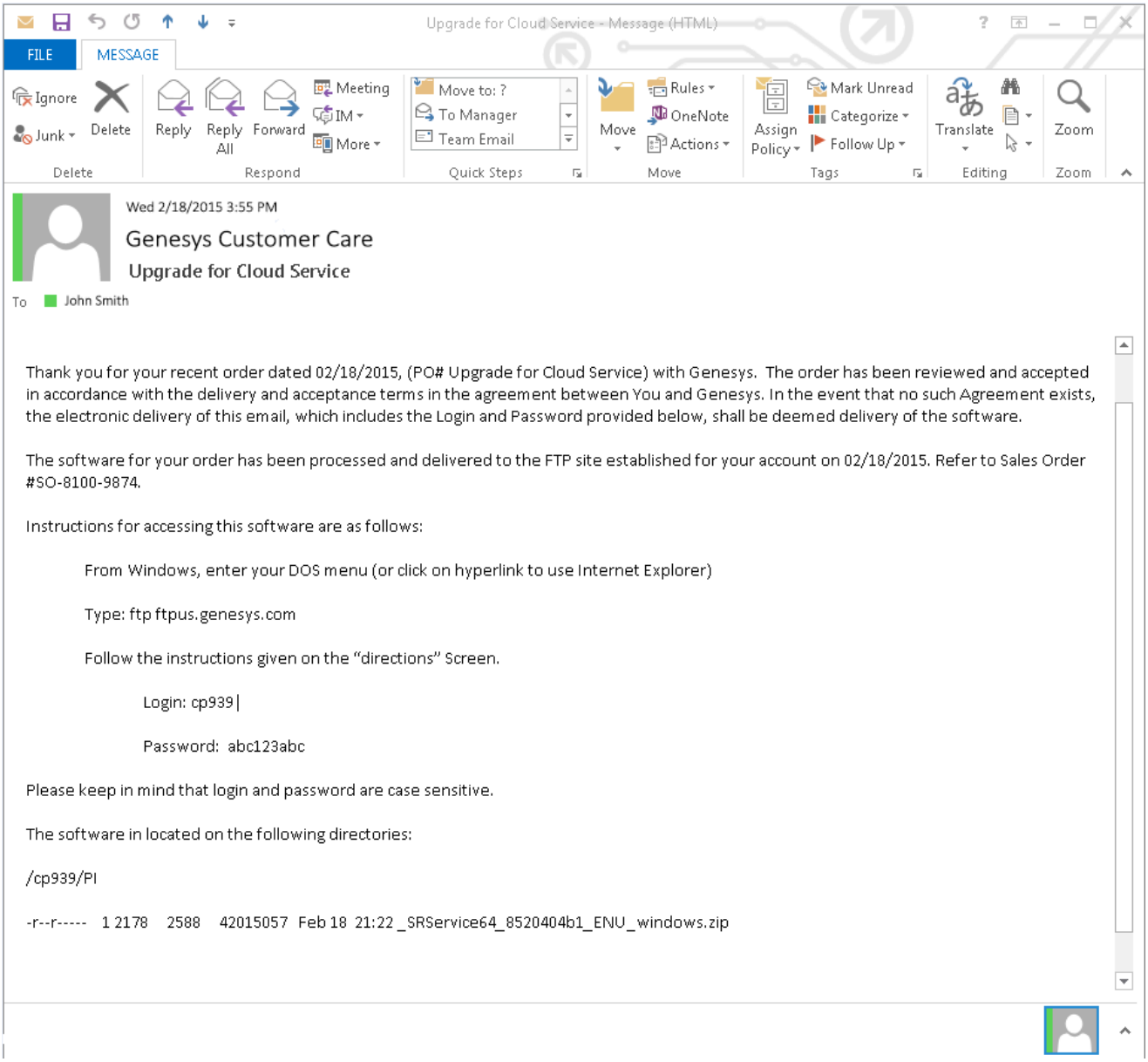
- Side-by-side 1024 x 768 + 1024 x 768
- Side-by-side 1280 x 720 + 1280 x 720
- Side-by-side 1600 x 1200 + 1600 x 1200
- Side-by-side 1920 x 1080 + 1920 x 1080

When using dual monitors, set both displays to the same resolution and arrange them side-by-side (not offset) in your display settings, as shown here:



Using dual monitors in a non-recommended configuration can result in errors.

Get your software



Find the email you received from Genesys with the details about your software (it will look similar to the example above), and using your favorite FTP client—for example, Filezilla, connect with the credentials listed in the email.

Download the zipped file to a temporary folder on your computer.

Installing your software for the first time

There are two ways to install Screen Recording Service:

- Installation Wizard - for version 8.5.3 and higher
- Command Prompt

> **Important**
>
> - To install Screen Recording Service, you must have Administrator privileges.
> - Firefox users must close the browser before installing Screen Recording Service. If Firefox is open while Screen Recording Service is being installed, restart the browser after the installation is completed.

Installing the SR Service for the first time with the installation wizard

This type of installation procedure is for version 8.5.3 and higher. Ensure you follow the specified steps so that the SR Service will work in a Genesys Multicloud CX deployment.

1. Locate the setup.exe and double-click its icon. The installation wizard is activated.
2. Select the Standard option and click **Next**.
3. Select **Use an existing configuration file** (optional) to copy the configuration of one machine, to all other installations of the SR Service on different machines in the same deployment. In the **Location** field, enter the location of the existing configuration file and click **Next**.
4. Verify that the location in the **Destination Folder**, is the correct location (that is, the location where the SR Service will be installed) for the SR Service. If it is not the correct location, enter the correct location and click **Next**.
5. Click **Install**, to complete the first-time installation.

Installing the SR Service for the first time with the command prompt

1. Open a command prompt, and type `cd` to change directories to the installation folder.
2. At the prompt, enter the following command and press **Enter**:

```
setup.exe /s /z"-s '' -sl '' -t ''"
```

> **Important**
>
> - Set the configured `genesys_silent.ini` file path in the command line. Use the absolute

path for the input file parameters.
For example, run `setup.exe /s /z"-s'c:\genesys_silent.ini' -sl 'c:\setup.log' -t'c:\setup_wizard.log'"`

- The `genesys_silent.ini` file must be configured when using command line silent installation and an unused parameter must be commented out in the `genesys_silent.ini` file. The standard **genesys_silent.ini** file is included with the installation package.
  - The **genesys_silent.ini** file provides all possible configuration parameters along with a description of each.
  - The file lists all the parameters with placeholders.
  - Verify that the unused configuration parameters are either deleted or commented.
  - Verify that the configuration file contains at least the following parameters:

    ```
    [SRServer]

    InstallationType=Standard

    [IPCommon]

    InstallPath=

    [MaintMode]

    Mode=FirstInstall
    ```

  - For additional security options, consult a Genesys Professional.
  - During the installation process, the antivirus program may block the installation when the installation process detects that the antivirus program is attempting to make system changes. In this scenario, the user will have to unblock the installation program to continue the installation.

Verify the installation

Use Windows Explorer to locate the directory where you installed the software. For example, `C:\Program Files (x86)\GCTI\Genesys SR Service\Logs\GSR`. Once you see the folder is there, restart your computer to confirm that the service starts automatically.

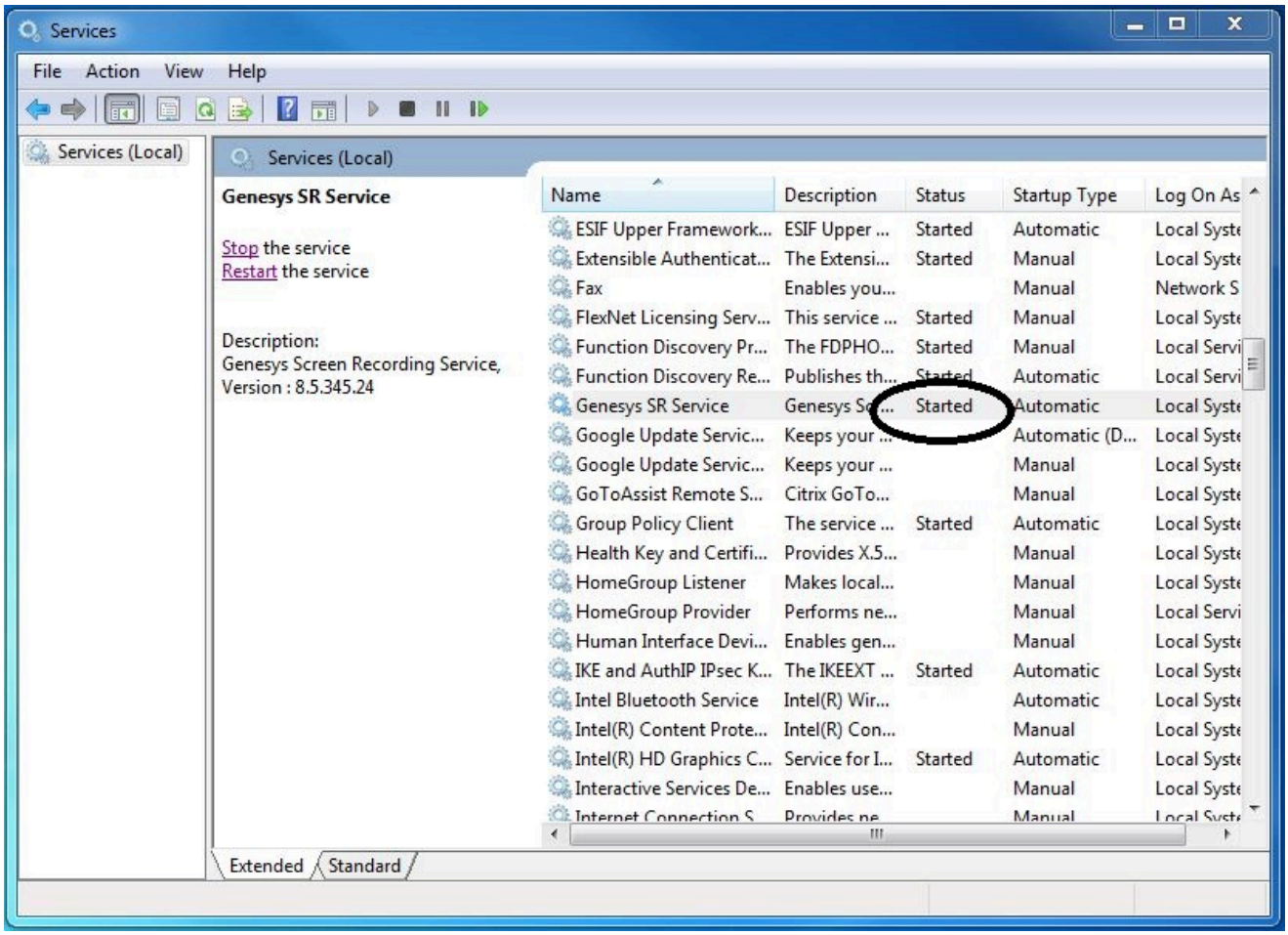
To verify the version installed, browse to https://127.0.0.1/version or http://127.0.0.1:8080/version.

Test the service and validate the installation

After installation, use Windows Services to confirm that the Genesys SR Service is ‘Started’. Check the startup log file as follows:

1. Open the `C:\Program Files (x86)\GCTI\Genesys SR Service\Logs\GSR.log` file, and make sure that something similar to the following lines are included (with the version reflecting the version you have just installed):
   ```
   ServiceHandler: Running Version:8.5.230.23, IP:135.39.66.17, OS:win32
   ```
2. Make sure that the C:\Program Files (x86)\GCTI\Genesys SR Service\Logs\GSR.log file contains no errors or exceptions.
3. Use the agent desktop to login as an agent that has been configured to have their voice interactions recorded. When the **`recordingWhen`** parameter is not set to `off`, the screens will also be recorded when the Screen Recording Service is running. Once logged-in as an agent, request an inbound call to that agent, or use the agent desktop to initiate an outbound call (For example, to a cell phone). Keep the interaction active for 10-20 seconds, and then disconnect the call. Proceed with step 4 to review the log file.
4. After the test, review the C:\Program Files (x86)\GCTI\Genesys SR Service\Logs\GSR.log for the following line: `Uploader: Upload of file was successful`.

> **Tip**
>
> If your installation is unsuccessful, contact your Genesys Professional.



Advanced Installation Procedures

Creating Self-Signed Certificates to support IP Loopback Addresses other than 127.0.0.1

SRS can be configured so that its Authentication Server uses Loopback IP Addresses other than 127.0.0.1. The HTTPS Certificates that are created by default only work if SRS is configured to use the Loopback IP Address 127.0.0.1. To use SRS with Loopback Addresses besides 127.0.0.1 and HTTPS, new HTTPS Certificates must be created specifically for the Loopback IP Address that SRS is using.

To create self-signed certificates with Loopback addresses other than 127.0.0.1, following installation, perform the following:

1. Open a command window as an Administrator.
2. Navigate to the **\Certificates\Self-Signed** directory.
3. Run **uninstall_certificates.bat** to remove the existing certificates.

4. Run **create_certificates.bat** and pass a value for the **IPV4_HOST** parameter. Below is an example to create certificates for 127.1.1.2:

   ```
   create_certificates.bat -IPV4_HOST 127.1.1.2
   ```

5. Run **install_certificates.bat** to install the new certificates. This installs the new self-signed certificates to the Windows trusted certificates store.
6. Configure SRS to use the newly created certificates. Please see the **authenticationCertificate** option in Advanced configuration for the Screen Recording Service for more details.
7. Restart the Genesys SR Service Windows service.

Upgrading the Screen Recording Service

Screen Recording Service can be upgraded manually or automatically. Both types of upgrades assume a functional existing deployment of Screen Recording Service. If the functionality of the existing deployment is in question, it is recommended to look for and stop the service, delete the previous installation folder and proceed as though this is the first time deploying the software. Contact your Genesys Professional if you are not sure if the software is working.

Manual upgrade from any version to 8.5.302.10

1. Create a backup copy of the `C:\Genesys\SRC` directory and name the backup directory `C:\Genesys\SRC.backup.`
2. Unzip your new software in a temporary directory (for example, C:\temp).
3. Update the **`.ini`** file. Access the temporary directory and type the following command in a command prompt window:

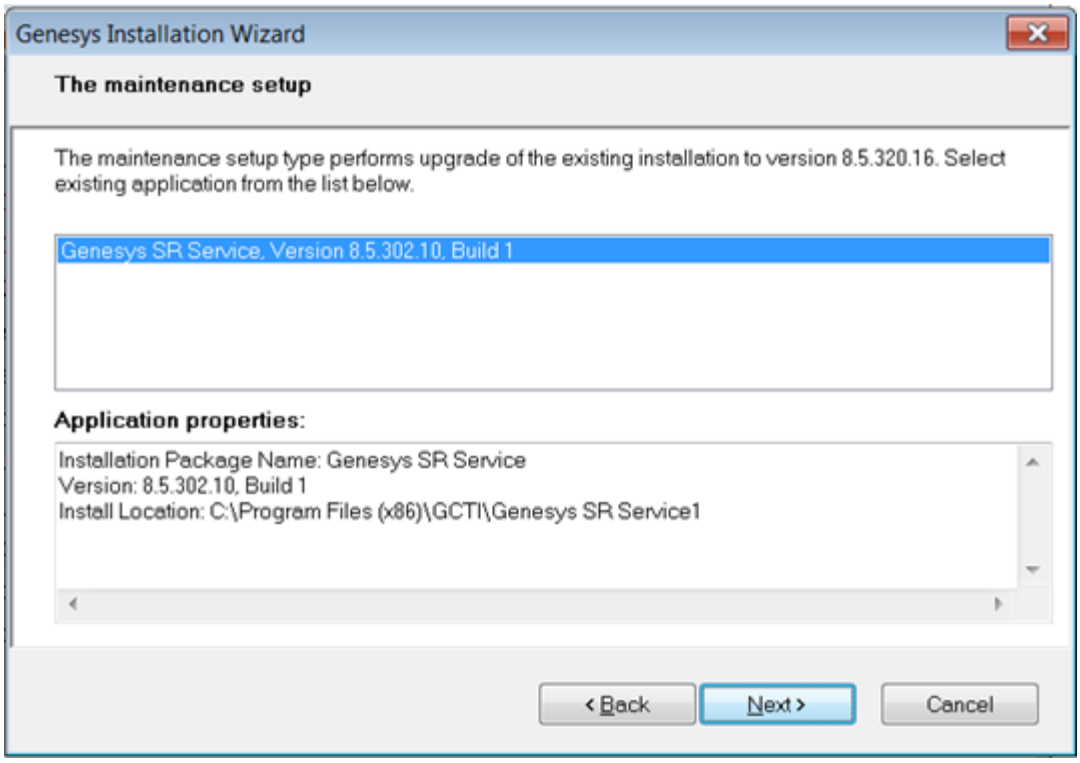
   ```
   setup.exe /s /z"-s '' -sl '' -t ''"
   ```

4. Validate the upgrade using the steps in the Test the Service and Validate the Installation section above.

Manual Upgrade

> ### Important
>
> - The following steps must be performed by a System Administrator.
> - Before you upgrade to a newer Screen Recording Service version, check with your Genesys Professional about compatibility with your system.

1. Copy the new SR Service software to a temporary directory.
2. Run the **`setup.exe`**. As shown in the following image, the setup process automatically detects the existing SR Service installation and selects it for upgradation.



3. Click **Next** and follow the instructions provided in the Installing the SR Service for the first time with the installation wizard section above.
4. Validate the upgrade using the steps in the Test the Service and Validate the Installation section.

Upgrading while using HTTPS with an IP address other than 127.0.0.1

When SR Service is upgraded, the self-signed HTTPS certificates are removed and new ones are generated and installed. The newly generated HTTPS certificates will be for the IP address 127.0.0.1. If the IPv4 SRS `authenticationHost` parameter (see Advanced configuration for the Screen Recording Service for more details about the `authenticationHost` parameter) is configured to something other than 127.0.0.1, then the HTTPS certificates will not work.

To continue using HTTPS with an IP address other than 127.0.0.1, new HTTPS certificates must be generated. Follow the instructions in Creating Self-Signed Certificates to support IP Loopback Addresses other than 127.0.0.1 to create and install new HTTPS certificates.

Advanced configuration for the Screen Recording Service

These parameters can be configured locally in the **config.json** file present in the SRS installation directory. All the configuration parameter values should be in JSON notation, for example: `{"name":"parameterName","value":"parameterValue"}`.

> **Important**
> Screen Recording Service does not support the use of System Proxies configured via PAC (Proxy Auto-Configuration) files.

Name	Mandatory	Description	Default value
authenticationHost	N	The IPv4 Address that the Authentication Server will bind to when SRS starts if SRS is configured to use IPv4. The parameter value must be an IPv4 address within 127.0.0.0/8. The IP addresses 127.0.0.0 and 127.255.255.255 are not allowed.	127.0.0.1
dummyRecordingDuration	N	When enabled, launches a VLC process for the specified duration during the start of the service. The parameter is disabled when a negative value is given. This parameter can be set to a value less than 60 (seconds). **Warning** Only configure this parameter if instructed by Genesys.	-1
preLoadVlc	N	Decides whether to load VLC process in advance after agent logs in. Valid values are `true` and `false`. **Warning** Only configure this parameter if instructed by Genesys.	false
proxyServerHost	N	The hostname of the proxy server.	Empty
proxyServerPort	N	The server port of the proxy server.	Empty
proxyServerUsername	N	The username to connect to the proxy server.	Empty
proxyServerPassword	N	The password to	Empty

Name	Mandatory	Description	Default value
		connect to the proxy server.	
useSystemProxy	N	If this value is `true`, the Screen Recording Service uses the Windows System Proxy settings.	false

> **Important**
>
> If specified, the proxy server parameters take precedence over the **useSystemProxy** parameter.

Rollback to a previous version

To rollback to a previous version of the Screen Recording Service:

> **Important**
>
> - The SR Service only supports a manual rollback.
> - Recordings captured but not uploaded will need to be manually moved to the upload folder of the active SRS directory after the rollback is complete.

1. In the Task Manager, verify that **Genesys SR Service** is stopped. If it has not been stopped, stop it now.
2. Copy the current `C:\Program Files (x86)\GCTI\Genesys SR Service` directory to a different folder. (For example: C:\Program Files (x86)\GCTI\Genesys SR Service.). This directory contains recordings that have not yet been uploaded; it may be needed for subsequent troubleshooting purposes.
3. Uninstall the existing SR Service installation.
4. Install the previous SR Service version.
5. Restart your computer or start the Genesys SR Service Windows service.
6. Validate the rollback using the steps in the Verify the Installation section above.

Uninstalling the Screen Recording Service

1. Open the **Start** menu and select **Control Panel**.

2. Click **Programs and Features**.
3. In the **Name** column, select the **Screen Recording Service** entry (for example, Genesys SR Service 8.5.xxx.yy), right click and select **Uninstall**.
   The Screen Recording Service is uninstalled.

Recording Cloud Backup Service

Contents

- 
- Administrator

The Recording Cloud Backup Service (RCBS) allows you to make a backup copy of your Genesys Interaction Recording voice and/or screen recording files prior to their automated deletion. This page describes how to set up the RCBS.

Related documentation:

-
-

The Recording Cloud Backup Service (RCBS) allows you to make a backup copy of your Genesys Interaction Recording voice and/or screen recording files prior to their automated deletion as per the Cloud retention policy. Once installed, you can securely download the encrypted voice and screen recording files and their respective metadata files from Genesys Multicloud CX and store them on your machines.

RCBS can be installed on local machines or on AWS EC2 instances. The recording file can then be decrypted and used as desired, for example, for compliance.

There are some things to know before you start:

- Unless backed up, all recordings will be deleted when the maximum retention date is reached.
- RCBS only works with encrypted recordings. Therefore, ensure encryption is enabled.
- RCBS does not support MPLS.

Prerequisites

Before you can install and use the Recording Cloud Backup Service on a machine, verify that you have the following prerequisites. Your IT department or your Genesys professional can help you get this information.

- Windows Server 2012/2019 64-bit or Red Hat Enterprise Linux 8 Operating System with admin privileges.
- 4 GB RAM, minimum 20 GB hard drive (the amount of space required depends on the number of recordings to be downloaded).
- The Recording Cloud Backup Service software (minimum version 8.5.2xx.xx).
- The target directory or shared folder in your environment to download the recording files to—for example, `C:/target_directory` (this is for the **targetDir** parameter).
- The private key you used to initially configure recording file encryption, so that the recording files can be decrypted (this is for decrypting the downloaded files).

- The name of your Platform Administration tenant administrator account – (this is for the `GWS_USERNAME` environment variable). Usernames should be in the format `username@customer_tenant.com`. For more information, refer to Creating a user.
- The password for your Platform Administration tenant administrator account – (this is for the `GWS_PASSWORD` environment variable). For more information, refer to Creating a user.
- Java 8 is the current supported version.

Security

The recording files are encrypted throughout the media lifecycle. After the recording files are created, they are encrypted and stored in Amazon S3. RCBS securely transfers the encrypted recordings from S3 to a machine by using the HTTPS internet protocol. The recordings can be decrypted only on that machine.

Getting Started

The following sections explain how to request RCBS functionality and install the software on Windows and Linux environments.

Requesting RCBS functionality

To request RCBS functionality, create a Salesforce case to request delivery of the software. Customer Care will provide an FTP download link to the software, and they will be in touch to request:

- The public IP ranges for the network where the RCBS client software will be installed and from where access to recordings will be established.
  - If a proxy is used, then the public IP range of the proxy will be requested instead.
- If RCBS is planned to be deployed on an AWS EC2 Instance, then additional information will be requested:
  - The AWS Region where RCBS is planned to be deployed.
  - Whether or not you wish to use a VPC Endpoint to connect to Genesys S3 Storage.
    - If you choose to use a VPC Endpoint, Customer Care will provide more information.
- A public PGP key so that the Genesys Operations team can securely transfer the S3 storage access credentials to you, which are needed by the RCBS to access the recording storage location.

Once the software has been delivered, Genesys will provide you with the following information:

- The Interaction Recording Web Services URL to access the recording metadata—for example, `https://example.com/api/v2` (this is for the **gwsUriPrefix** parameter).
- The access ID for the S3 storage, used to gain access to the recordings – (this is for the `AWS_ACCESS_KEY_ID` environment variable).
- The secret access key for the S3 storage, used to gain access to the recordings – (this is for the

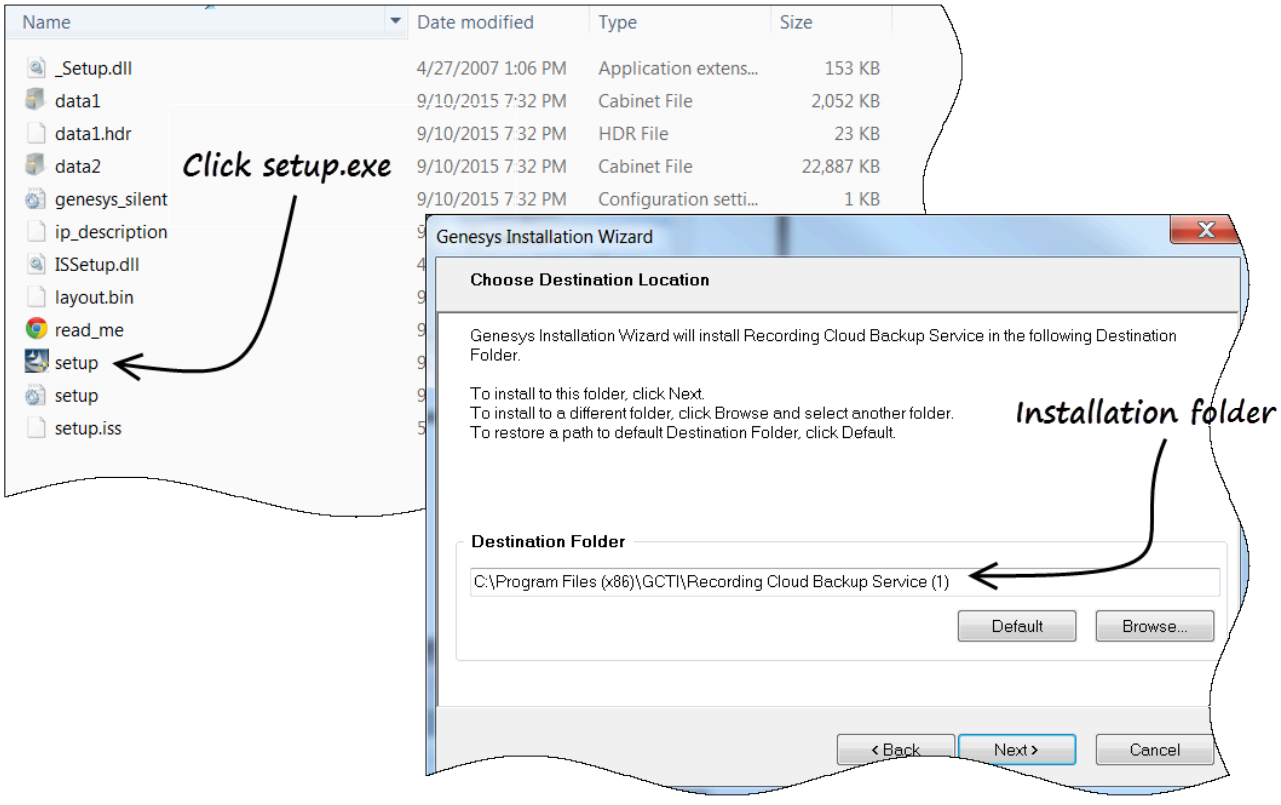
AWS_SECRET_ACCESS_KEY environment variable).

Creating a user

Refer to Add agents manually to create a non-agent user for RCBS. Complete all the required (*) fields and ensure that the user has administrator privileges. The user that is created is GWS_USERNAME environment variable and the password for this user is GWS_PASSWORD environment variable.

> **Important**
>
> If you plan to run RCBS in verification mode, an extra provisioning step is required for your user. Please contact Genesys to get the required provisioning.

Installing on Windows

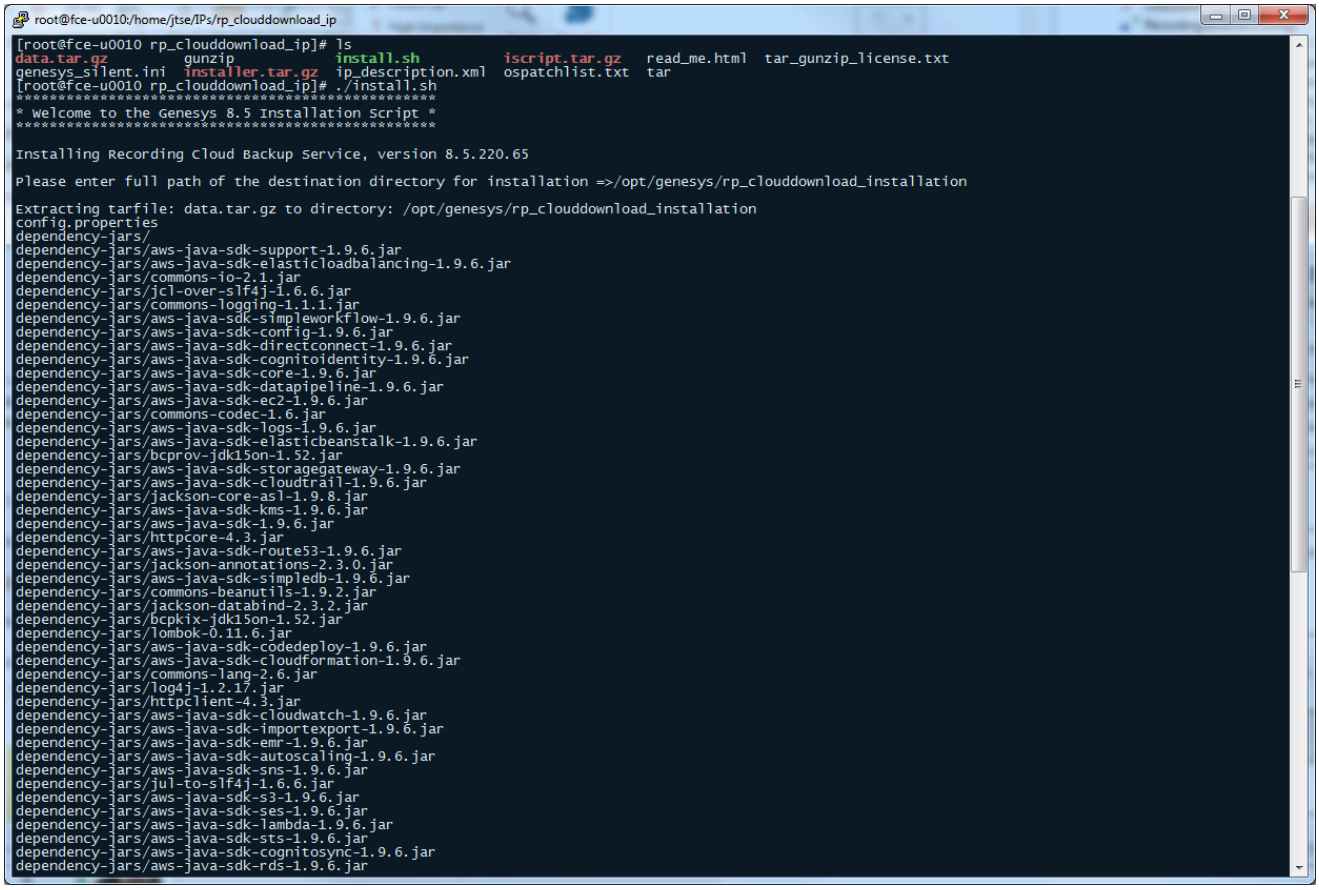


Locate your software in the installation directory, and click **setup.exe** to start the Genesys Installation Wizard.

Follow through the wizard until finished making sure that you make note of the installation directory.

Check the installation directory and verify that the **config.properties** file is available.

Installing on Linux



The **glibc.i686** package is required to install RCBS. To install **glibc.i686**, run the following command: `yum install glibc.i686`

In the installation directory, at the prompt, type `./install.sh`.

Let the script install your software.

Check the installation directory and verify that the **config.properties** file is available.

Configuration and setup

The following sections explain the configuration properties and environment variables to set for proper functioning of RCBS.

Configuration properties

The following properties must be modified to successfully retrieve recording files from Amazon S3. Locate your **config.properties** file, usually found in the installation directory, edit the file with a text editor, and set the following parameters:

Parameter Name	Description	Example Value
gwsUriPrefix	The URL prefix of Interaction Recording Web Services where the metadata for the recording files is retrieved from. This is a mandatory parameter and will be provided by Genesys.	`https://example.com/api/v2`
maxAge	All recordings newer than the specified **maxAge** value, in days, are downloaded. You can specify any integer greater than or equal to 0 (0 is any age). The default value is 2, which means that all recordings from the last 2 days will be retrieved. If recordings have already been downloaded, they will not be downloaded again. **Note:** If recordings are moved from their downloaded folder (**targetDir**), they will be downloaded again when RCBS is run. To ensure recordings are not downloaded more than once, only move recordings from this folder once **maxAge** days have passed since RCBS was last run.	2
targetDir	The directory where the recordings are downloaded to. This directory can be anywhere on the system as long as the account running the software has permission to write to the directory. Ensure that the required space is available to download the desired number of recordings. **Note:** • On both Windows and Linux, you must use the directory separator "/" (forward slash) instead of "\" (backslash). • RCBS supports the use of a UNC path for targetDir. For example, targetDir = //server_name/path.	`/target`

Specify the following parameters only if the machine running RCBS cannot connect directly to Amazon S3 or the Interaction Recording Web Services address.

Parameter Name	Description	Example Value
awsProxyHost	Indicates the proxy host address to be used for Amazon Web Services. Specify only the host name or IP address.	`10.0.1.31`
awsProxyPort	Indicates the proxy port to be used for the corresponding **awsProxyHost** parameter to connect to Amazon Web Services.	`8080`
gwsProxyHost	Indicates the proxy host address to be used for Interaction Recording Web Services. The format is `http://proxyaddress`.	`http://10.0.1.31`
gwsProxyPort	Indicates the proxy port to be used for the corresponding **gwsProxyHost** parameter to connect to Interaction Recording Web Services.	`8080`

Environment variables

Once configured, before running the Recording Cloud Backup Service from the command line, the following environment variables must be set based on those provided earlier:

- GWS_USERNAME
- GWS_PASSWORD
- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY

On Windows

To set environment variables, select **System** from the **Control Panel** (change category view (**View by**) to **Small icons**), click **Advanced system settings**, and then click **Environment Variables**. Under User variables for your_user> or System variables, add as the following:

Variable	Value
GWS_USERNAME	username@customer_tenant.com
GWS_PASSWORD	`your_password`
AWS_ACCESS_KEY_ID	`your_aws_access_key_id`
AWS_SECRET_ACCESS_KEY	`your_aws_secret_access_key`

On Linux

Create the **rcbs.sh** file under the `/etc/profile.d/` directory. The file should contain the following:

```
#!/bin/bash
export GWS_USERNAME=username@customer_tenant.com
export GWS_PASSWORD=your_password
export AWS_ACCESS_KEY_ID=your_aws_access_key_id
export AWS_SECRET_ACCESS_KEY=your_aws_secret_access_key
```

Provide execute permission and using the **source** command this file will be used for setting the environment variable as follows:

```
[root@rcbsmachine ~]# cd /etc/profile.d/
[root@rcbsmachine profile.d]# chmod +x rcbs.sh
[root@rcbsmachine profile.d]# source rcbs.sh
```

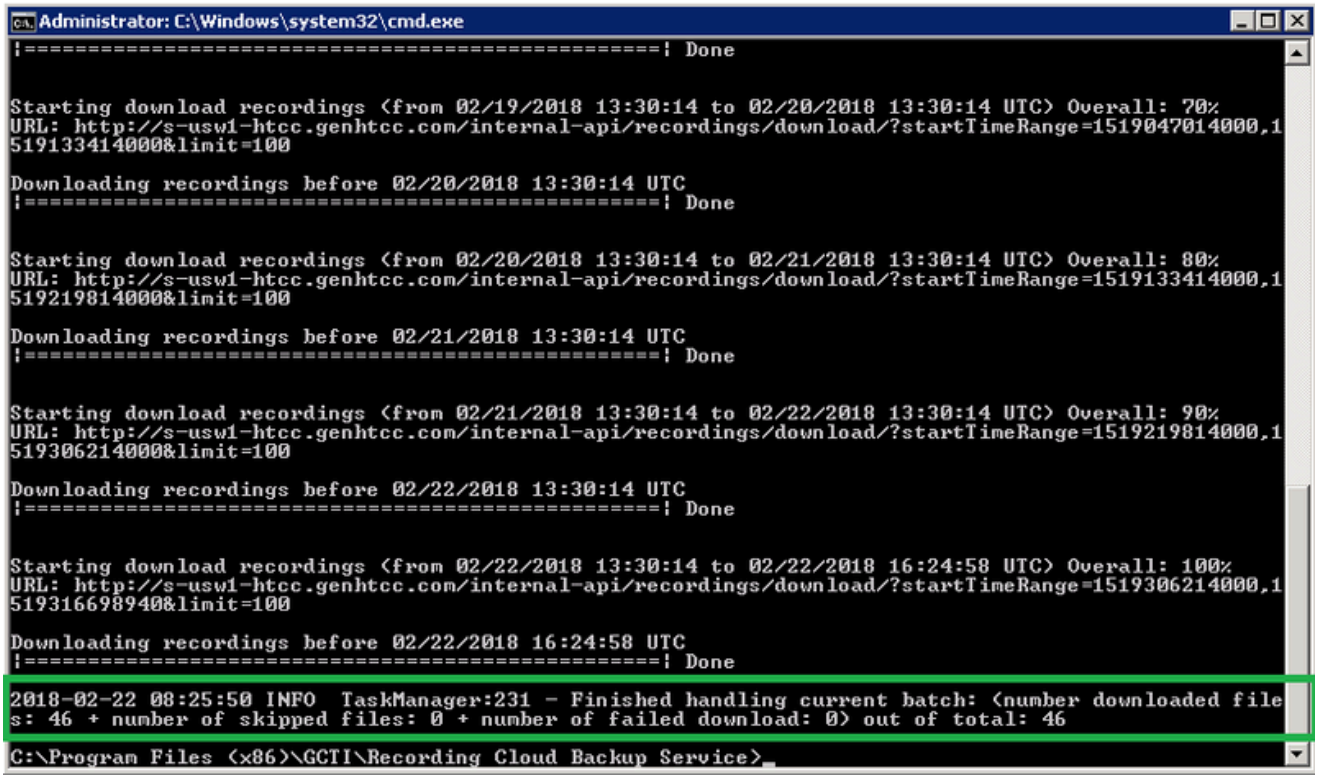
Launching the Recording Cloud Backup Service

After the config.properties file has been modified and the environment variables are set, access the RCBS installation directory and type the following command line to start RCBS:

```
java -jar rp_clouddownload.jar -config config.properties
```

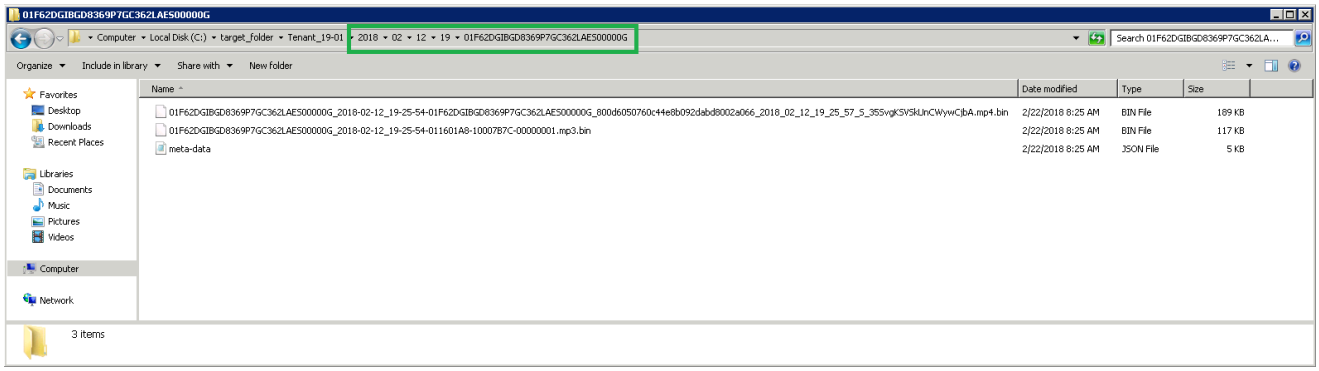
> **Important**
>
> **Do not copy and paste the command from this document.** Instead, manually type the command.

You can view the progress of the download process in percentage in console window. Download process will be completed once the progress reaches 100% with the message as shown in the following image.



The tool exits when the backup is complete. Check your **targetDir** to ensure that the expected recordings have been downloaded.

In the below example, 2018 is the year, 02 is the month, 12 is the date, 19 is the hour, and 01F62DGIBGD8369P7GC362LAES00000G is the recording folder. Recordings are grouped at the hour as the lowest level. Each recording folder has encrypted voice and screen recording files (if applicable) along with a metadata file in JSON format.



Running RCBS in verification mode

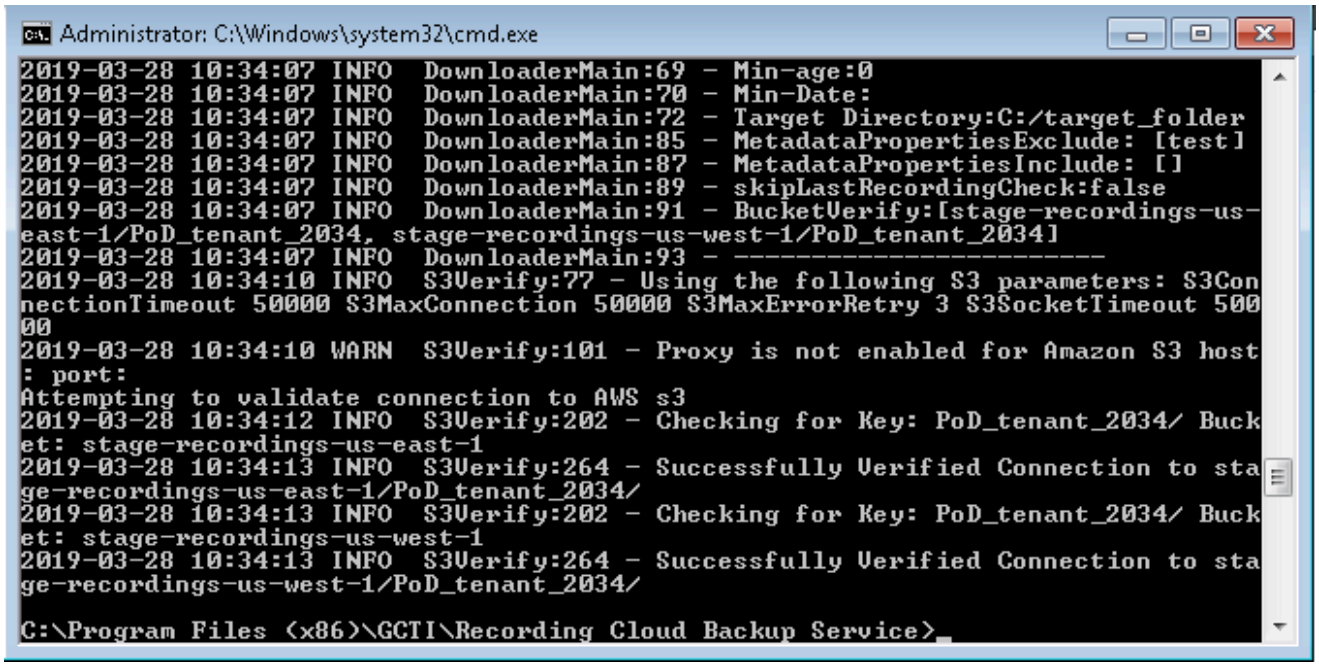
After the config.properties file has been modified and the environment variables are set, access the RCBS installation directory and type the following command line to start RCBS to verify your connection to download recordings from AWS S3:

```
java -jar rp_clouddownload.jar -config config.properties -verify s3
```

Important

- This function is only available in RCBS 8.5.298.58 and later versions.
- If you plan to run RCBS in verification mode, an extra provisioning step is required for your user. Please contact Genesys to get the required provisioning.

You can find out whether the connection is successful or not via the console window.



Scheduling backup

The following sections explain how to schedule a backup.

How to schedule a Windows task

For information on how to schedule or manage your tasks in Windows, see the Windows documentation. Do not forget to set your environment variables.

How to create a Linux cronjob

You can set up a recurring backup by using cronjob (crontab -e). The following example illustrates how to use "crontab -e" to configure an appropriate cronjob on Linux:

```
AWS_ACCESS_KEY_ID=
AWS_SECRET_ACCESS_KEY=
GWS_PASSWORD=
GWS_USERNAME=
30 4,10,16,22 * * * (cd ; java -jar rp_clouddownload.jar -config config.properties)
```

Replace the above , , , , with the actual values, and the job will be executed 4 times daily at 4:30, 10:30, 16:30 and 22:30.

> **Important**

- Genesys strongly recommends that you create backup copies several weeks prior to the expected deletion date.
- Ensure your local machine has enough space for the scheduled backup.

Decrypting the downloaded files

You will use OpenSSL to decrypt your recording files. You can download the software by following the instructions here.

When working with Windows, the OpenSSL binaries can be downloaded from: OpenSSL Binaries Distribution.

Each recording folder contains the encrypted recording files and the respective recording metadata files (in json format).

To decrypt the downloaded files that are in encrypted format, use the following OpenSSL commands:

- **Windows:**

```
openssl smime -decrypt -binary -inform DER -in  -inkey  -out
```

- **Linux:**

```
openssl cms –decrypt –inform DER -in  -binary -inkey  –out
```

where:

- is the file to be decrypted
- is the private key you used to initially configure recording file encryption, so that the recording files can be decrypted
- is the file that would be written after decryption

Storage

Ensure that the required space is available to download the desired number of recordings. Genesys recommends that you decrypt the recording files to a different destination than the encrypted files so that the original encrypted source file is not modified or overwritten by the decrypted file.

Advanced configuration

If you are an advanced user, you can change the behavior of the Recording Cloud Backup Service by

changing the values of the parameters in the **config.properties** file.

Configuring download period

Use the following parameters to set the download period.

Parameter Name	Description	Example Value
minAge	All recordings older than the specified **minAge** value, in days, are included in the download period. You can specify any integer greater than or equal to 0. The default is 0, which means that the download period includes recordings older than the current time. The **minAge** value must be less than the **maxAge** value. ISO 8601 format can also be used with respect to current time. Refer to ISO 8601 format for more information. If you specify a minimum age of PT30M, all recordings that are older than half an hour ago are included in processing. If you specify a minimum age of P30D, all recordings older than 30 days are included in processing.	`0`
maxAge	All recordings newer than the specified **maxAge** value, in days, are included in download period. You can specify any integer greater than or equal to 0 (0 is any age). The default value is 2, which means that the period includes recordings from the last 2 days. The **maxAge** value must be greater than the **minAge** value. ISO 8601 format can also be used with respect to current time. Refer to ISO 8601 format for more information. If you specify a maximum age of PT30M, all recordings that are newer than half an hour are included in processing. If you specify a maximum age of P30D, all recordings newer than 30 days are included in processing.	`2`

minDate	The absolute date, in the YYYY-MM-DD format (in GMT), to include recordings older than the specified date. When specified, this value would be used as the **minAge**. Note that **minDate** includes recordings up to 12 AM GMT on the specified date. Alternatively, the epoch time value can be specified instead of the YYYY-MM-DD format. Refer to UNIX Epoch time format for more information. This parameter is optional.	`2015-07-31`
		Or
		`1438300800000`

maxDate	The absolute date, in the YYYY-MM-DD format (in GMT), to include recordings newer than the specified date. When specified, this value would be used as the **maxAge**, and override the local storage's last recording endtime's value (last_recording_endtime.txt). Note that **maxDate** includes recordings from 12 AM GMT on the specified date. Alternatively, the epoch time value can be specified instead of the YYYY-MM-DD format. Refer to UNIX Epoch time format for more information. This parameter is optional.	`2015-07-31`
		Or
		`1438300800000`

Important

- RCBS stores the last time that it successfully downloaded recordings. If the stored last time is older than the specified **maxAge**, RCBS uses that value instead of **MaxAge** to determine which recordings to download. However, if the **maxAge** value is older than

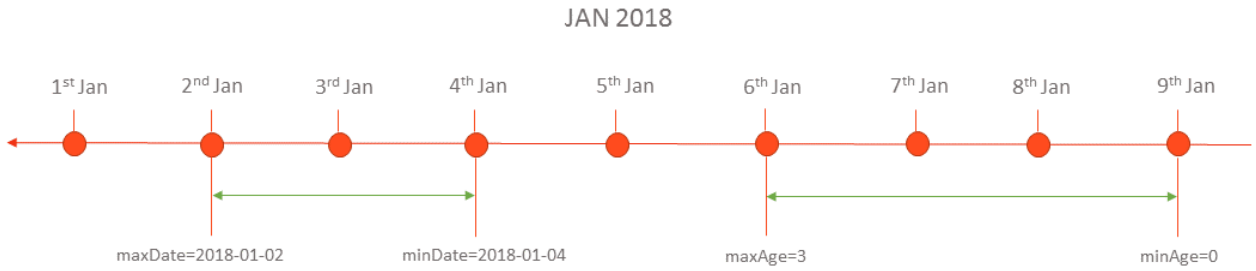
the last stored time, RCBS resumes from where it left off the last time it successfully ran.

- RCBS will not download duplicate recordings within the same instance. For example, if **maxAge** is set to 2 days but the machine where RCBS is installed is offline for 3 days, RCBS downloads only those recordings that were missed since the last time it successfully ran.

For repetitive scheduled download of recordings, use the **minAge** and **maxAge** parameters. RCBS will download recordings for the configured duration with respect to current time. For example, if the current date is January 09, 2018 and if you want to download recordings of three days with respect to current time, then set **minAge=0** and **maxAge=3** as shown in the following image. Recordings will be downloaded from 12 AM GMT on January 06 to 12 AM GMT of January 09.

For one-time download of recordings between two dates (GMT), use the **minDate** and **maxDate** parameters. RCBS will download recordings within the configured period. To perform a one-time download, Genesys recommends that you create a copy of the **config.properties** file, delete or rename the **last_recording_endtime.txt** file and make changes to the **minDate** and **maxDate** parameters.

When you execute RCBS, use the following command with the name of the copy of the configuration file (for example, new_config.properties): `java -jar rp_clouddownload.jar -config new_config.properties`. To download recordings between a date range, for example, between 02 January to 04 January, set the parameters such as the following: **minDate=2018-01-04** and **maxDate=2018-01-02**.



Download period always includes the recordings newer than the last download period as specified in the **last_recording_endtime.txt** file.

The **last_recording_endtime.txt** file is updated after download of recordings for configured period has completed successfully. The next time when the download tool starts, it checks to see if the **last_recording_endtime.txt** file is older than the specified **maxAge** parameter. If it is, the tool uses the value from the **last_recording_endtime.txt** instead of the configured **maxAge** value.

For example, the download tool is scheduled to run daily with **maxAge** set to 2 days. If the server was offline for three days, it is replaced with the **last_recording_endtime.txt** file check, and the tool downloads all the recordings that were missed.

UNIX Epoch time format

RCBS supports UNIX Epoch time format in milliseconds for certain parameters. It is a 13 digit integer value. You can convert the date and time to 13 digit integer value by using tools such as Epoch Converter.

ISO 8601 format

RCBS supports ISO 8601 format `P[n]Y[n]M[n]DT[n]H[n]M[n]S` for certain parameters. The description of the format is as follows:

- `P` - Mandatory prefix to identify that the configuration is in ISO format.
- `[n]` - Integer value which is specific for the suffix followed by it
- `[n]Y` - Number of Years. Example - 2Y means 2 years
- `[n]M` - Number of Months
- `[n]D` - Number of Days
- `T` - Mandatory prefix to identify the following content is time
- `[n]H` - Number of Hours
- `[n]M` - Number of Minutes
- `[n]S` - Number of Seconds

Examples of valid values:

- P1Y2DT4H30M - Indicates 1 Year + 2 Days + 4 Hours + 30 Minutes
- P6MT12H - Indicates 6 Months + 12 Hours

Configuring media

Use the following parameters to set the media configurations.

Parameter Name	Description	Example Value
mediaTypePattern	Indicates the file types that will be downloaded by RCBS in a regular expression. The default value is `audio\/mp3|video\/mp4`. This value will download both audio and video files. To download only MP3, set this value to audio\/mp3. To download only MP4, set this value to video\/mp4. This parameter is optional.	`audio\/mp3|video\/mp4`
recordingFolderFormat	The directory structure for storing the recordings. Default value is in the `yyyy/MM/dd/HH` format which means the top level folder is year, subfolder is month, then date, then hour. Note the directory separator "/" (forward slash) must be used instead of "\" (backslash) on both Windows and Linux.	`yyyy/MM/dd/HH`
encryptionFormat	The cipher to use if the encryption is performed by the download tool. The supported values are `AES-128` or `AES-256`. The default value is	`AES-128`

Parameter Name	Description	Example Value
	AES-128. **Note:** If AES-256 is used, the JCE unlimited Strength Jurisdiction Policy File must be installed.	
metadataOnly	Indicates whether to download the recording files along with the metadata. If set to `true`, the metadata is downloaded without the recordings. You do not need S3 credentials when using this option. Default value is `false`.	`false`
usePayloadSigning	Configures whether payload signing is used during the file transfer from Amazon S3. Disabling payload signing improves performance. Default value is `false`. To enable, set to `true`.	`false`

Configuring multiple instances

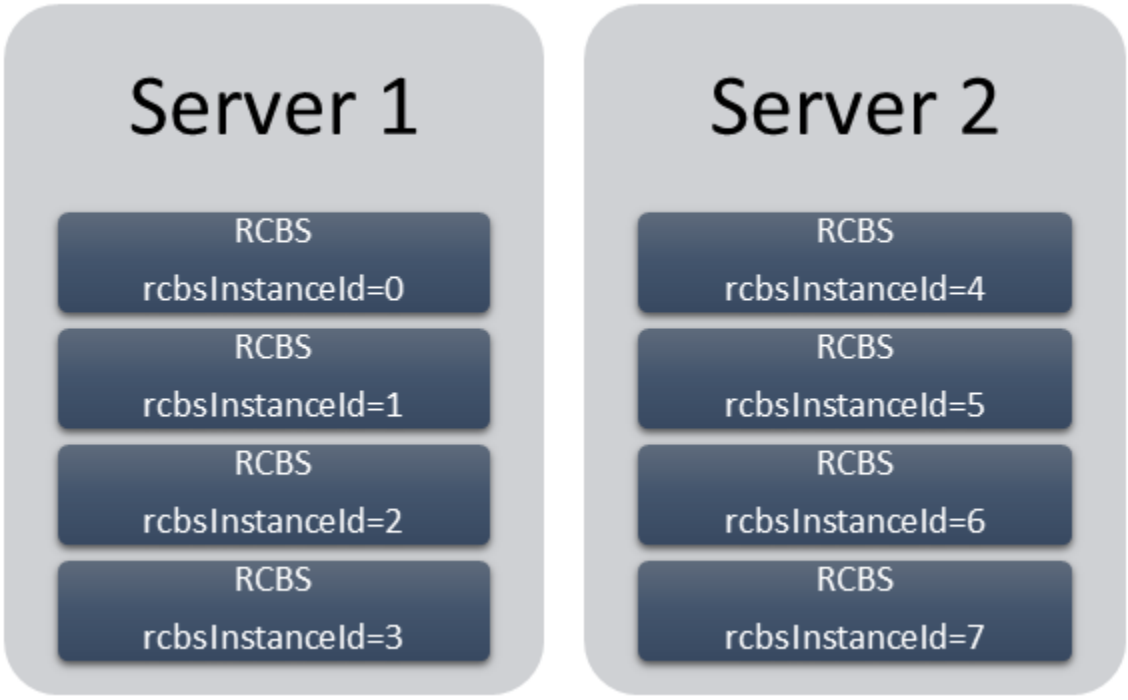
Multiple instances of RCBS can be used to increase the download rate of the recordings for the configured download period. Multiple instances can be used in the same machine or different machines based on network bandwidth. Each instance will process the same download period and split the download process based on hashing of the recording ID. A particular recording will be downloaded by only one instance and all other instances will skip that recording. All instances should be running properly to download all the recordings in the configured download period.

The **minAge** and **maxAge** of the separate instances must be the same. The point of multiple instances is that each instance is assigned a different subset of recordings to download to spread the load. Changing the **minAge** and **maxAge** means each instance will download a separate chunk of a different time period.

Note: If running multiple instances of RCBS on the same machine, each RCBS must be started from a different installation directory, and **targetDir** for each instance must point to a different output folder. RBCS has a built-in protection mechanism to prevent multiple instances from writing to the same directory; the second instance will terminate immediately if they share the same path.

Parameter Name	Description	Example Value
totalRcbsInstances	The total number of RCBS instances deployed.This parameter must be used with the **rcbsInstanceId** configuration parameter. This parameter is optional.	4
rcbsInstanceId	Indicates the current RCBS instance ID that shares the overall load. **rcbsInstanceId** starts at **0**, up to **totalRcbsInstances** minus **1**. For example, if the download load was distributed across four instances of a running RCBS process, then **totalRcbsInstances** should be set to 4. For each RCBS configuration, assign **rcbsInstanceId** to **0** for the first RCBS instance, **rcbsInstanceId** to **1** for the	`0`

Parameter Name	Description	Example Value
	second RCBS instance, **rcbsInstanceId** to **2** for the third RCBS instance, and **rcbsInstanceId** to **3** for the fourth RCBS instance. All RCBS instances should have the same **minAge** and **maxAge** configuration values.	



In the above image, eight instances of RCBS spread between two servers. Here, the value of **totalRcbsInstances** is 8 in all the instances.

Configuring URIs (optional)

The following parameters are optional. Do not set the URI path for these parameters unless instructed by Genesys.

Parameter Name	Description	Example Value
gwsRecordingsUri	The path to the recording API.	`/recordings`
gwsSettingsUri	The path to the settings API.	`/me/settings/rcbs`

Recording metadata

Metadata is organized by records and can be used for finding specific calls from a larger downloaded

group of recordings (for example, by searching for a particular string of text, perhaps the ‘callerPhoneNumber’). A record represents a single call interaction which may contain multiple calls and recording segments. A metadata record is uniquely identified (per switch) by a CallUUID (GUID).

The metadata record is stored in JSON format and contains three main sections within the top level object.

- The interaction level attributes (the top level object's attributes)
- The mediaFiles list—A list of media files connected to the call interaction
- The eventHistory list—A list of call events including attached data events and agent left and join events.

Metadata properties

Property	Description
Id	The CallUUID for the recording interaction.
callRecordingId	The call recording identifier. This attribute is in screen recording metadata only.
callerPhoneNumber	The caller's phone number.
dialedPhoneNumber	The dialed phone number.
startTime	The start time of the call.
stopTime	The end time of the call.
region	The region of the call.
mediaFiles	A list of media file records. See the mediaFile properties.
eventHistory	The events attached to the call. See the eventHistory properties.

mediaFile properties

The following table describes the mediaFile properties.

Property	Data Type	Description	Required
startTime	datetime	Specifies the start time of the media file.	Yes
stopTime	datetime	Specifies the stop time of the media file. If MCP fails, this value will be the same as the `startTime`.	Yes
mediaID	string	Specifies the media file name for the media file that is used by clients to refer to the same media file. MCP ensures that this value is globally unique.	Yes

Property	Data Type	Description	Required
type	string	Specifies the MIME type of the media file.	Yes
duration	time	Specifies the time duration of the media file.	No
size	number	Specifies the size, in bytes, of the media file.	No
tenant	string	Specifies the tenant that the recording belongs to.	Yes
ivrprofile	string	Specifies the IVR Profile name that serviced the recording.	Yes
parameters	object—The properties are parameters.	Specifies the list of additional metadata information provided by SIP Server and the client applications. The properties are: • username • sipsAppName • ani • dnis • dateTime • connid • agentId • id • record	Yes
masks	array of objects—Each object contains the time and type property.	Specifies the time stamps of the pause/ resume periods if the recording is masked by a client application.	No
certAlias	array of strings	Specifies a list of aliases to the encryption certificates if the media file is encrypted.	No
partitions	array of strings	Specifies a list of partition names for the media file.	Yes
accessgroups	array of strings	Specifies the access groups identified agent associated with the	Yes

Property	Data Type	Description	Required
		recording.	
channels	number	Specifies whether the recording audio is capture in mono (1) or stereo (2).	Yes

eventHistory properties

The following table describes the eventHistory properties.

Property	Data Type	Description	Required
occurredAt	datetime	Specifies the start time of the event.	Yes
calluuid	string	Specifies the call UUID that the event belongs to.	Yes
event	string	Specifies the event type: • `Joined` • `Left` • `data`	Yes
contact	object	Specifies the the contact information of the caller who joined or left the recording if the event is `Joined` or `Left`.	No
data	object	The attached data included in the recording if the event is `data`.	No

Metadata format

The following code snippet illustrates the metadata format:

```
{
  "id" : "021L6BI58K8FH7R5USI402LAES00000A",
  "callerPhoneNumber" : "+19059683343",
  "dialedPhoneNumber" : "+15126401290",
  "startTime" : "2021-07-21T16:49:00.000+0000",
  "stopTime" : "2021-07-21T16:49:37.000+0000",
  "eventHistory" : [ {
    "occurredAt" : "2021-07-21T16:49:42.131+0000",
    "eventId" : "021L6BI58K8FH7R5USI402LAES00000A_2021-07-21T16:49:42.131Z",
    "event" : "Data",
    "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
    "data" : {
```

```
    "updated" : {
      "DispositionCode" : "good"
    }
  }
}, {
  "occurredAt" : "2021-07-21T16:49:46.000+0000",
  "eventId" : "021L6BI58K8FH7R5USI402LAES00000A_2021-07-21T16:49:46.000Z",
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "contact" : {
    "type" : "User",
    "phoneNumber" : "+16478389098",
    "userName" : "agent_103001",
    "firstName" : "Hotseating",
    "lastName" : "Last103001"
  },
  "data" : {
    "ACW" : 9
  }
}, {
  "occurredAt" : "2021-07-21T16:48:48.787+0000",
  "eventId" : "2021-07-21T16:48:48.787Z_021L6BI58K8FH7R5USI402LAES00000A",
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "data" : {
    "added" : {
      "CallUUID" : "0194TKHEVS83786AE88362LAES0IG052"
    }
  }
}, {
  "occurredAt" : "2021-07-21T16:48:48.813+0000",
  "eventId" : "2021-07-21T16:48:48.813Z_021L6BI58K8FH7R5USI402LAES00000A",
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "data" : {
    "added" : {
      "RStrategyDBID" : "226",
      "RStrategyName" : "+15126401290:105"
    }
  }
}, {
  "occurredAt" : "2021-07-21T16:48:48.872+0000",
  "eventId" : "2021-07-21T16:48:48.872Z_021L6BI58K8FH7R5USI402LAES00000A",
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "data" : {
    "added" : {
      "322045d0-d10c-11ea-ad8d-736e48fb400b-flowentrycount" : "1",
      "orssessionid" : "01NSUD25908FHE4HK4I402LAES000007",
      "orsurl" : "http://usw1scl-2027-001.usw1.g1.genhtcc.com:9098"
    }
  }
}, {
  "occurredAt" : "2021-07-21T16:48:48.873+0000",
  "eventId" : "2021-07-21T16:48:48.873Z_021L6BI58K8FH7R5USI402LAES00000A",
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "data" : {
    "added" : {
      "GSYS_SystemApplicationDisposition" : "1"
    }
  }
}, {
```

```
    "occurredAt" : "2021-07-21T16:48:48.901+0000",
    "eventId" : "2021-07-21T16:48:48.901Z_021L6BI58K8FH7R5USI402LAES00000A",
    "event" : "Data",
    "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
    "data" : {
      "added" : {
        "GSYS_IVR" : "enter{1626886128888}",
        "IApplication" : "322045d0-d10c-11ea-ad8d-736e48fb400b",
        "IApplicationVersion" : "0.1",
        "gsw-ivr-profile-name" : "auto",
        "gvp-tenant-id" : "auto"
      }
    }
  }, {
    "occurredAt" : "2021-07-21T16:48:49.340+0000",
    "eventId" : "2021-07-21T16:48:49.340Z_021L6BI58K8FH7R5USI402LAES00000A",
    "event" : "Data",
    "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
    "data" : {
      "added" : {
        "IW_BundleUid" : "d52253c6-3c00-45d8-719c-7e4c8b27788e",
        "IW_CaseUid" : "d69691a5-745d-47b0-a871-a00b6ecccbb8"
      }
    }
  }, {
    "occurredAt" : "2021-07-21T16:48:55.121+0000",
    "eventId" : "2021-07-21T16:48:55.121Z_021L6BI58K8FH7R5USI402LAES00000A",
    "event" : "Data",
    "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
    "data" : {
      "added" : {
        "GVP-Session-Data" : "callsession=B6B1C806-8D4D-E81E-
B15B-1F7A1C7A11C0;2;1;sip:usw1spx-2027-002.usw1.g1.genhtcc.com:5060;;;Environment/
Tenant_2027;IVRAppDefault;;0;record",
        "GVP-Session-ID" : "B6B1C806-8D4D-E81E-B15B-1F7A1C7A11C0;gvp.rm.datanodes=2|
1;gvp.rm.tenant-id=1.432_IVRAppDefault",
        "__reason" : "exit"
      }
    }
  }, {
    "occurredAt" : "2021-07-21T16:48:55.137+0000",
    "eventId" : "2021-07-21T16:48:55.137Z_021L6BI58K8FH7R5USI402LAES00000A",
    "event" : "Data",
    "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
    "data" : {
      "updated" : {
        "GSYS_IVR" : "exit{1626886135124}"
      }
    }
  }, {
    "occurredAt" : "2021-07-21T16:48:55.187+0000",
    "eventId" : "2021-07-21T16:48:55.187Z_021L6BI58K8FH7R5USI402LAES00000A",
    "event" : "Data",
    "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
    "data" : {
      "added" : {
        "RPVQID" : "01GS2U2DAG8FHABOUSI402LAES000009",
        "RTargetAgentGroup" : "?:login(voice) & (GSYS_skill_1>3)"
      }
    }
  }, {
    "occurredAt" : "2021-07-21T16:48:55.188+0000",
    "eventId" : "2021-07-21T16:48:55.188Z_021L6BI58K8FH7R5USI402LAES00000A",
```

```
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "data" : {
    "added" : {
      "CBR-IT-path_DBIDs" : "",
      "CBR-Interaction_cost" : "",
      "CBR-actual_volume" : "",
      "CBR-contract_DBIDs" : "",
      "CustomerSegment" : "default",
      "RRequestedSkillCombination" : "",
      "RTargetAgSelDBID" : "7791",
      "RTargetAgentSelected" : "103001",
      "RTargetObjSelDBID" : "",
      "RTargetObjectSelected" : "?:login(voice) & (GSYS_skill_1>3)",
      "RTargetPlSelDBID" : "7205",
      "RTargetPlaceSelected" : "16478389098",
      "RTargetRequested" : "?:login(voice) & (GSYS_skill_1>3)",
      "RTargetRuleSelected" : "",
      "RTargetTypeSelected" : "2",
      "RTenant" : "Environment",
      "RTenantDBID" : "1",
      "RVQDBID" : "7296",
      "RVQID" : "01GS2U2DAG8FHABOUSI402LAES000009",
      "ServiceObjective" : "",
      "ServiceType" : "default"
    }
  }
}, {
  "occurredAt" : "2021-07-21T16:49:00.406+0000",
  "eventId" : "2021-07-21T16:49:00.406Z_021L6BI58K8FH7R5USI402LAES00000A",
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "data" : {
    "deleted" : {
      "RTargetAgentGroup" : "?:login(voice) & (GSYS_skill_1>3)"
    },
    "updated" : {
      "GSYS_SystemApplicationDisposition" : "301"
    }
  }
}, {
  "occurredAt" : "2021-07-21T16:49:00.537+0000",
  "eventId" : "2021-07-21T16:49:00.537Z_021L6BI58K8FH7R5USI402LAES00000A",
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "data" : {
    "added" : {
      "GSIP_RECORD" : "PENDING"
    }
  }
}, {
  "occurredAt" : "2021-07-21T16:49:00.941+0000",
  "eventId" : "2021-07-21T16:49:00.941Z_021L6BI58K8FH7R5USI402LAES00000A",
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "data" : {
    "added" : {
      "GSIP_REC_FN" : "021L6BI58K8FH7R5USI402LAES00000A_2021-07-21_16-49-00"
    },
    "updated" : {
      "GSIP_RECORD" : "ON"
    }
  }
```

```
}, {
  "occurredAt" : "2021-07-21T16:49:00.963+0000",
  "eventId" : "2021-07-21T16:49:00.963Z_021L6BI58K8FH7R5USI402LAES00000A",
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "data" : {
    "added" : {
      "GSRS_STATE" : "SRSScreenRecordingStateStarted"
    }
  }
}, {
  "occurredAt" : "2021-07-21T16:49:37.207+0000",
  "eventId" : "2021-07-21T16:49:37.207Z_021L6BI58K8FH7R5USI402LAES00000A",
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "data" : {
    "added" : {
      "IWAttachedDataInformation/CaseDataBusinessAttribute" : "",
      "IWAttachedDataInformation/DispositionCode.Key" : "DispositionCode",
      "IWAttachedDataInformation/DispositionCode.Label" : "Disposition Code",
      "IWAttachedDataInformation/Option.interaction.case-data.frame-co" : "#17849D",
      "IWAttachedDataInformation/SelectedDispositionCodeCompleteName" : "",
      "IWAttachedDataInformation/SelectedDispositionCodeDisplayName" : "",
      "IWAttachedDataInformation/SelectedDispositionCodeName" : ""
    }
  }
}, {
  "occurredAt" : "2021-07-21T16:49:37.480+0000",
  "eventId" : "2021-07-21T16:49:37.480Z_021L6BI58K8FH7R5USI402LAES00000A",
  "event" : "Data",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "data" : {
    "deleted" : {
      "GSIP_RECORD" : "ON"
    }
  }
}, {
  "occurredAt" : "2021-07-21T16:49:00.537+0000",
  "event" : "Joined",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "contact" : {
    "type" : "User",
    "phoneNumber" : "+16478389098",
    "userName" : "agent_103001",
    "firstName" : "Hotseating",
    "lastName" : "Last103001"
  }
}, {
  "occurredAt" : "2021-07-21T16:48:48.787+0000",
  "event" : "Joined",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "contact" : {
    "type" : "User",
    "phoneNumber" : "+19059683343",
    "userName" : "UNKNOWN",
    "firstName" : "UNKNOWN",
    "lastName" : "UNKNOWN"
  }
}, {
  "occurredAt" : "2021-07-21T16:49:37.479+0000",
  "event" : "Left",
  "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
  "contact" : {
```

```
      "type" : "User",
      "phoneNumber" : "+16478389098",
      "userName" : "agent_103001",
      "firstName" : "Hotseating",
      "lastName" : "Last103001"
    }
  }, {
    "occurredAt" : "2021-07-21T16:49:37.480+0000",
    "event" : "Left",
    "calluuid" : "021L6BI58K8FH7R5USI402LAES00000A",
    "contact" : {
      "type" : "User",
      "phoneNumber" : "+19059683343",
      "userName" : "UNKNOWN",
      "firstName" : "UNKNOWN",
      "lastName" : "UNKNOWN"
    }
  } ],
  "mediaFiles" : [ {
    "startTime" : "2021-07-21T16:49:00.000+0000",
    "stopTime" : "2021-07-21T16:49:37.000+0000",
    "callUUID" : "021L6BI58K8FH7R5USI402LAES00000A",
    "mediaId" :
"021L6BI58K8FH7R5USI402LAES00000A_2021-07-21_16-49-00-334B020F-10002D91-00000001.mp3.bin",
    "type" : "audio/mp3",
    "duration" : "36800",
    "tenant" : "Tenant_2027",
    "ivrprofile" : "record",
    "size" : "146304",
    "parameters" : {
      "dateTime" : "2021-07-21T16:49:00Z",
      "agentId" : "103001",
      "sipsAppName" : "SIPS_usw1_1_B",
      "recordDN" : "+16478389098",
      "connId" : "0195031f1ec49006",
      "dnis" : "+15126401290",
      "id" : "021L6BI58K8FH7R5USI402LAES00000A_2021-07-21_16-49-00",
      "ani" : "+19059683343",
      "callUuid" : "021L6BI58K8FH7R5USI402LAES00000A",
      "username" : "agent_103001"
    },
    "certAlias" : [ "rcs_Environment:1:CN=Basic Certification Authority:5" ],
    "partitions" : [ ],
    "accessgroups" : [ "/" ],
    "channels" : 2
  }, {
    "startTime" : "2021-07-21T16:49:00.000+0000",
    "stopTime" : "2021-07-21T16:49:46.000+0000",
    "mediaId" :
"W6x+Vq8fR2m3ngFfj9Um2g_021L6BI58K8FH7R5USI402LAES00000A_1d9439c7990141e3ad64a92eb43f4da4_2021_07_21_16_49_01",
    "type" : "video/mp4",
    "duration" : "0:00:46",
    "size" : "556410",
    "parameters" : {
      "muxed_mediaIds" : [
"021L6BI58K8FH7R5USI402LAES00000A_1d9439c7990141e3ad64a92eb43f4da4_2021_07_21_16_49_01",
"021L6BI58K8FH7R5USI402LAES00000A_2021-07-21_16-49-00-334B020F-10002D91-00000001.mp3.bin" ],
      "agentID" : "+16478389098",
      "virtualHeight" : "617",
      "contact" : {
        "userName" : "agent_103001",
        "lastName" : "Last103001",
        "firstName" : "Hotseating"
```

```
      },
      "virtualWidth" : "1920",
      "region" : "usw1",
      "originalVirtualHeight" : "1440",
      "originalVirtualWidth" : "4480",
      "callUuid" : "021L6BI58K8FH7R5USI402LAES00000A",
      "monitors" : [ {
        "name" : "monitor_0",
        "primary" : true,
        "originalPositions" : "[0, 0, 2560, 1440]",
        "actualPositions" : "[0, 0, 1096, 617]"
      }, {
        "name" : "monitor_1",
        "primary" : false,
        "originalPositions" : "[2560, 0, 4480, 1080]",
        "actualPositions" : "[1096, 0, 1919, 462]"
      } ]
    },
    "channels" : 2
  } ],
  "callType" : "Internal",
  "region" : "usw1"
}
```

Disk usage estimation

RCBS downloads the voice and screen recording files from the Genesys Interaction Recording system and stores the files on the local machine, thereby occupying the disk space. This section explains how to estimate the amount of disk space that will be used.

Estimating disk space required to store downloaded voice recordings

The disk space required to store voice recordings can be estimated as follows:

- **Estimated size of a metadata file**: The size of a metadata file for each voice recording has an upper bound of 1 MB. You can use that value to estimate how much space the metadata files will use.
- **Estimated size of a voice recording file**: The size of a voice recording file can be estimated by using the average call duration (in seconds) and the recording bitrate (in kbps, the default value is 32 kbps).

Total disk usage for a day

The estimated disk usage per day (in MB) can be calculated in one of the following ways:

- `* ( + )`
- `* [ * (( / 8 / 1024) + 1)]`

Estimating disk space required to store downloaded screen recordings

The disk space required to store screen recordings can be estimated as follows:

- **Estimated size of a metadata file**: The size of a metadata file for each screen recording has an

upper bound of 8 KB. You can use that value to estimate how much space the metadata files will use.

- **Estimated size of a screen recording file**: The size of a Screen Recording file can be estimated by using the average call duration (in seconds) and the screen recording bitrate (in kbps), which is the sum of the screen recording bitrate and voice recording bitrate because the RCBS downloads the muxed screen recording files. The default value for the total bitrate is 256 kbps.

Total disk usage for a day

The estimated disk usage per day (in MB) can be calculated in one of the following ways:

- `* ( + )`
- `* [ * (( / 8 / 1024) + 1)]`