



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.

Genesys Interaction Recording Solution Guide

Genesys Interaction Recording Solution Configuration

Genesys Interaction Recording Solution Configuration

This section describes how to configure the Genesys Interaction Recording Solution.

Prerequisites

- SIP Server is installed and configured. See the [SIP Server Deployment Guide](#) for the required steps.
- Genesys Voice Platform (GVP) Media Control Platform and Resource Manager are installed and configured. See the [Genesys Voice Platform](#) documentation for the required steps.
- The SpeechMiner components are installed and configured. See the [SpeechMiner Administration Guide](#) document for the required steps.

Important

You must request a recording-only license from the [Genesys Licensing Department](#) to use SpeechMiner for call recording.

- [Web Services](#) is installed and configured.
- [Interaction Concentrator \(ICON\)](#) is installed and configured.
- [Recording Processor](#), [Recording Crypto Server](#) and the [Recording Plug-in for Genesys Administrator Extension](#) are installed and configured.

Important

For information about upgrading the contributing solution components, see the specific upgrade procedures for each component, or see the latest [Genesys Migration Guide](#).

Enabling Call Recording

Configure the following components to enable call recording:

WebDAV Server

Configuring the WebDAV Server for Web Services

Important

Genesys has tested the interoperability with the Apache WebDAV server. If you wish to use a different WebDAV vendor, Genesys requires that RFC 2518 to be supported, as this is also supported by Apache WebDAV server.

1. Install WebDAV, run the following command:

```
yum install httpd
```

2. Edit the `/etc/httpd/conf/httpd.conf` file, and append the following to the end of the file:

```
Alias /recordings /mnt/recordings
<Directory /mnt/recordings>
    Options Indexes MultiViews FollowSymLinks
    EnableSendfile off
    AllowOverride None
    Order allow,deny
    allow from all
</Directory>
<Location "/recordings">
    DAV On
    AuthType Basic
    AuthName "user"
    AuthUserFile /var/www/htpasswd
    Require valid-user
</Location>
```

3. Open the firewall. Because WebDAV is an HTTP server, the incoming default HTTP and/or HTTPS ports (80 and/or 443) must be open to the server.

Important

It is possible to use custom ports by changing the permitted incoming ports in the firewall, the virtual host configuration file, and the URL used to reach the WebDAV server.

4. Create the directory to keep the recording files, and set the permission to apache, using the following command:

```
mkdir /mnt/recordings
chown apache:apache /mnt/recordings
```

5. Create a WebDAV user for httpd, and configure the password. The following example creates a user called "user":
`htpasswd -c /var/www/htpasswd user`

6. Configure the httpd to start on boot up (and start it now) using the following command:

```
chkconfig --levels 235 httpd on
service httpd start
```

7. Test the WebDAV installation"

- a. Upload a hello.world file to the WebDAV server using the following command:

```
curl -T hello.world -u user:password http://myserver/recordings/hello.world
```

- b. Using a browser, open the the `http://myserver/recordings/hello.world` URL. The browser will request for user credentials.

8. The WebDAV server is installed.

Web Services

Configuring Web Services

Configuring the Web Services Parameters

To configure Web Services for Genesys Interaction Recording: Set the following parameters in the **/genconfig/server-settings.yaml** file:

| Parameter Name | Mandatory | Description | Type | Default Value |
|--|-----------|---|------------------|---------------|
| enableBackgroundScheduledMediaOperations | | Specifies whether to allow Web Services to schedule purge and backup events. | Boolean | True |
| createCallRecordingCEN | | Specifies whether to create a call recording column family (CRCF) for a new contact center. | Boolean | False |
| crClusterName | Y | Specifies the name | Non-empty String | None |

| Parameter Name | Mandatory | Description | Type | Default Value |
|-------------------|-----------|--|------------------|---|
| | | of the elasticsearch cluster name. | | Note: This is a mandatory parameter, and the value must be the same for all Web Services nodes in the cluster. For example, if there are five nodes in the Web Services cluster, all five nodes must have the same crClusterName value. |
| crRegion | N | Specifies the name of the region where the Web Services node resides. | Non-empty String | None |
| cryptoSecurityKey | Y | Specifies the security key used for Web Services encryption of the recording settings in the database. | Non-empty String | None Note: This is a mandatory parameter, and the value must be the same for all Web Services nodes in the cluster. For example, if there are five nodes in the Web Services cluster, all |

| Parameter Name | Mandatory | Description | Type | Default Value |
|--|-----------|--|------------------|---|
| | | | | five nodes must have the same cryptoSecurityKey value. |
| defaultBackupExportURL | | Specifies the location to store backed up recordings. For example, file:///tmp/archLocDefault' . | Non-empty String | None |
| multiPartResolverMaxUploadSize | | Specifies the maximum size, in KB, of the recording file. | Integer | 536870912 |
| multiPartResolverMaxInMemorySize | | Specifies the maximum length of time allowed to upload a recording file. | Integer | 536870912 |
| recordCryptoServerDecryptMaxConnection | | Specifies the maximum TCP connections to each Recording Crypto Server instance defined in local-decrypt-uri-prefix settings. Note: This option applies to the Web Services version 8.5.200.85 and later only. | Integer | 50 |
| recordCryptoServerDecryptMaxTotalConnections | | Specifies the maximum TCP connections to all Recording Crypto Server instances defined in local-decrypt-uri- | Integer | 10 * recordCryptoServerDecryptMax |

| Parameter Name | Mandatory | Description | Type | Default Value |
|--|-----------|--|---------|--|
| | | <p>prefix settings.</p> <p>Note: This option applies to the Web Services version 8.5.200.85 and later only.</p> | | |
| recordCryptoServerDecryptSocketTimeout | | <p>Specifies the socket timeout, in milliseconds, for TCP connections to Recording Crypto Server instances defined in '<i>local-decrypt-uri-prefix</i>' settings.</p> <p>Note: This option applies to the Web Services version 8.5.200.85 and later only.</p> | Integer | 30000 |
| webDAVMaxConnections | | Specifies the maximum TCP connections for each WebDAV Storage. | Integer | 50 |
| webDAVMaxTotalConnections | | Specifies the maximum TCP connections the Web Services node allows to all WebDAV Storages. | Integer | 10 * webDAVMaxConnections |
| undocumentedExternalApiUrl | | <p>Specifies the reachable Web Services Server address for the SpeechMiner UI, and the Screen Recording Client.</p> <p>Note: This option applies to the Web</p> | String | http://<IP Address>:8090/internal-api |

| Parameter Name | Mandatory | Description | Type | Default Value |
|----------------|-----------|---|------|---------------|
| | | Services version 8.5.200.40 and later only. | | |

Configuring the Elasticsearch Engine

The Web Services Call Recording API uses the elastic search as the query engine. A configuration file is required if call recording is enabled (for example, **JETTY_HOME/resources/elasticsearch.yml**).

Configure the **JETTY_HOME/resources/elasticsearch.yml file as follows:**

```
index.analysis.analyzer.whitespace_lowercase.tokenizer: whitespace
index.analysis.analyzer.whitespace_lowercase.filter: lowercase

transport.tcp.port: 9200
http.port: 9300

discovery.zen.ping.multicast.enabled: false
discovery.zen.ping.unicast.hosts: <comma separated list of HTCC nodes which host the ES>
discovery.zen.minimum_master_nodes: 2

gateway.recover_after_nodes: 2
gateway.recover_after_time: 1m
gateway.expected_nodes: 3

threadpool.index.queue_size: -1
threadpool.bulk.queue_size: -1

path.conf: <Path to genconfig folder>/elasticsearch
path.data: <Path to the folder where ES stores its data>
```

For more configuration information, see <http://www.elasticsearch.org/guide/>.

The elastic search engine also requires a large PermGen space.

To increase the PermGen space:

- Add the following to your JAVA_OPTIONS:

```
JAVA_OPTIONS="-XX:MaxPermSize=512m -Djsse.enableSNIExtension=false"
```

- If you are using **/etc/default/jetty**, add:

```
JAVA_OPTIONS="-Xmx2048m -XX:MaxPermSize=512m -Xms2048m -Djsse.enableSNIExtension=false"
```

Important

The Elasticsearch index is saved in the **Jetty-Home/data** directory—for example, **/opt/jetty/data**.

Rebuilding the Elasticsearch Index

If you must upgrade your Jetty 8 version to Jetty 9 version, you might need to add the elasticsearch data file to the new Web Services cluster.

To move the elasticsearch data:

- Rebuild the elasticsearch index using the following command:

```
curl -XPOST "http://<FE VM host>/api/v2/ops/contact-centers/<ID contact center>/recordings"
-d '{ "operationName":"forceIndex", "from":<Time of previous 'green' state or backup
snapshot>}'
```

The command above executes the forceIndex operation and is used to rebuild the elasticsearch index when needed. The following information provides additional details for this API.

HTTP Request

POST
.../api/v2/ops/contact-centers/{id}/recordings

Request Body

```
{
  "operationName":"forceIndex",
  "from":1369272257713,
  "to":1369275857713,
  "purgeOld":true
}
```

The following table describes the request body attributes:

| Attributes | Type | Mandatory | Description |
|---------------|--------------|-----------|--|
| operationName | String | Y | The name of the operation. In this case it is forceIndex. |
| from | Long Integer | Y | The Java time stamp (in milliseconds) which equals the UNIX time * 1000. This is the time stamp from which the records are re-indexed. |
| to | Long Integer | N | The Java time stamp (in milliseconds) which equals the UNIX time * 1000. This is the time |

| Attributes | Type | Mandatory | Description |
|------------|---------|-----------|--|
| | | | stamp to which the records are re-indexed. If not specified, the current time of the request processing is used. |
| purgeOld | Boolean | N | Specifies whether the old index should be deleted prior to re-indexing. This attribute is necessary if the Web Services updated version uses indexes with a different structure. The default value is false. |

Restarting Web Services

For more information on starting and stopping Web Services, see the [Web Services Deployment Guide](#).

Configuring the Storage Credentials for Web Services

To enable voice recording:

1. Determine the contact center ID on Web Services using the following command with the ops username and password (ops:ops):

```
curl -u ops:ops http://<Web Services Server>:8080/api/v2/ops/contact-centers; echo
```

The following output is returned:

```
{"statusCode":0,"uris":["http://<Web Services Server>:8080/api/v2/ops/contact-centers/<contact center ID (in hex format)>"]}
```

Important

Use the <contact center ID (in hex format)> in all subsequent commands.

2. Using a text editor, created the create_table file using the following command:

```
{
  "operationName":"createCRCF"
}
curl -u ops:ops -X POST -d @create_table http://htcc:8080/api/v2/ops/contact-centers/<contact center ID (in hex format)>/recordings --header "Content-Type: application/json"; echo
```

To enable storage:

1. Using a text editor, create the `recording_settings` text file using the following command:

```
{
  "store": [{
    "webDAV": {
      "userName": "user1",
      "password": "password1",
      "uri": "http://apache1/webdav"
    }
  },
  {
    "webDAV": {
      "userName": "user2",
      "password": "password2",
      "uri": "http://apache2/webdav"
    }
  }
]
}
```

```
curl -u ops:ops -X PUT -d @recording_settings
http://<Web Services Server>:8080/api/v2/ops/
contact-centers/<contact center ID (in hex format)>/settings/recordings
--header "Content-Type: application/json"; echo
```

Configuring the Call Recording Audit Log

Web Services provides an audit log for the following call recording operations:

- Playback of the recording media file
- Deletion of the call recording file

To configure the audit log:

1. Stop the Web Service Jetty using the following command:
`sudo service jetty stop`
2. Update the Jetty LogBack Configuration:
 - Edit the `/opt/jetty/resources/logback.xml` file to include INFO level messaging similar to the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
  Example LOGBACK Configuration File
  http://logback.qos.ch/manual/configuration.html
-->
<configuration scan="true">
  <appender name="RECORDING" class="ch.qos.logback.core.rolling.RollingFileAppender">
    <filter class="ch.qos.logback.classic.filter.LevelFilter">
      <level>INFO</level>
      <onMatch>ACCEPT</onMatch>
      <onMismatch>DENY</onMismatch><!-- ACCEPT for printing log above INFO, DENY for
printing only INFO-->
    </filter>
    <file>${jetty.logs}/recording.log</file>
    <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
      <fileNamePattern>${jetty.logs}/recording-%d{yyyy-MM-dd-HH}.gz</fileNamePattern>
      <maxHistory>720</maxHistory><!-- 1 Month -->
    </rollingPolicy>
```

```

    <encoder>
      <pattern>%d{MM/dd/yyyy HH:mm:ss.SSS, UTC} [%X{principal.name}] [%X{req.userAgent}]
[%X{req.remoteHost}] %X{req.requestURI} %msg%n</pattern>
    </encoder>
  </appender>
  <appender name="FILE" class="ch.qos.logback.core.rolling.RollingFileAppender">
    <file>${jetty.logs}/cloud.log</file>
    <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
      <!-- hourly rollover -->
      <fileNamePattern>${jetty.logs}/cloud-%d{yyyy-MM-dd-HH}.gz</fileNamePattern>
      <!-- keep 5 days' worth of history -->
      <maxHistory>120</maxHistory>
    </rollingPolicy>
  </appender>
  <encoder>
    <pattern>%d{MM/dd/yyyy HH:mm:ss.SSS, UTC} %-5level [%X{principal.name}]
[%X{session}] [%X{contactCenter}]
[%thread] %X{req.requestURI} %X{req.queryString} %logger{36} %msg%n</pattern>
  </encoder>
</appender>
<logger name="com.<domain>.cloud.v2.api.controllers.callrecording">
  <appender-ref ref="RECORDING" />
</logger>
<logger name="com.<domain>.cloud.v2.api.tasks.callrecording">
  <appender-ref ref="RECORDING" />
</logger>
<logger name="com.<domain>" level="WARN" />
<logger name="com.<domain>.cloud" level="DEBUG" />
<logger name="com.<domain>.cloud.rtreporting" level="WARN" />
<logger name="com.<domain>.salesforce.security" level="INFO" />

<root level="WARN">
  <appender-ref ref="FILE" />
</root>

</configuration>

```

3. For MLM:

- Create a **RECORDING** appender if it does not exist. Use the following example:

```

<appender name="RECORDING" class="ch.qos.logback.core.rolling.RollingFileAppender">
  <filter class="ch.qos.logback.classic.filter.LevelFilter">
    <level>INFO</level>
    <onMatch>ACCEPT</onMatch>
    <onMismatch>DENY</onMismatch><!-- ACCEPT for printing log above INFO, DENY for
printing only INFO-->
  </filter>
  <file>${jetty.logs}/recording.log</file>
  <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
    <fileNamePattern>${jetty.logs}/recording-%d{yyyy-MM-dd}.gz</fileNamePattern>
    <maxHistory>720</maxHistory><!-- 1 Month -->
  </rollingPolicy>
  <encoder>
    <pattern>%d{MM/dd/yyyy HH:mm:ss.SSS, UTC} [%X{principal.name}] [%X{req.userAgent}]
[%X{req.remoteHost}] %X{req.requestURI} %msg%n</pattern>
  </encoder>
</appender>

```

- Add the following loggers:

```

<logger name="com.genesyslab.cloud.v2.api.controllers.callrecording">
  <appender-ref ref="RECORDING" />
</logger>

```

```
<logger name="com.genesyslab.cloud.v2.api.controllers.screenrecording">
  <appender-ref ref="RECORDING" />
</logger>
<logger name="com.genesyslab.cloud.v2.api.tasks.callrecording">
  <appender-ref ref="RECORDING" />
</logger>
<logger name="com.genesyslab.cloud.v2.api.tasks.screenrecording">
  <appender-ref ref="RECORDING" />
</logger>
<logger name="com.genesyslab.cloud.v2.api.tasks.settings">
  <appender-ref ref="RECORDING" />
</logger>
<logger name="com.genesyslab.cloud.v2.media.scheduler">
  <appender-ref ref="RECORDING" />
</logger>
<logger name="com.genesyslab.cloud.v2.media.task">
  <appender-ref ref="RECORDING" />
</logger>
```

For more information about Jetty Logback, see [Logback configuration](#).

4. Start Jetty using the following command:

```
sudo service jetty start
```

5. Review the audit log:

- Open the **/var/log/jetty/recording.log** file. The following example shows that two recordings are requested for playback and deletion:

```
10/28/2013 15:46:03.203 [ops] [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.71 Safari/537.36] [192.168.135.1] /api/v2/ops/contact-centers/46284f2f-d615-4329-957a-f5341edfd5d7/recordings/recid0/play/2cb4ea04-f81d-44e8-83b6-1f4a63a1a659.mp3 Play media [2cb4ea04-f81d-44e8-83b6-1f4a63a1a659] of recording [recid0] from contact center [46284f2f-d615-4329-957a-f5341edfd5d7] requested
```

```
10/28/2013 15:46:03.341 [ops] [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.71 Safari/537.36] [192.168.135.1] /api/v2/ops/contact-centers/46284f2f-d615-4329-957a-f5341edfd5d7/recordings/recid0/play/2cb4ea04-f81d-44e8-83b6-1f4a63a1a659.mp3 Play media [2cb4ea04-f81d-44e8-83b6-1f4a63a1a659] of recording [recid0] from contact center [46284f2f-d615-4329-957a-f5341edfd5d7] failed
```

```
10/28/2013 15:46:10.946 [ops] [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.71 Safari/537.36] [192.168.135.1] /api/v2/ops/contact-centers/46284f2f-d615-4329-957a-f5341edfd5d7/recordings/recid1/play/2cb4ea04-f81d-44e8-83b6-1f4a63a1a658.mp3 Play media [2cb4ea04-f81d-44e8-83b6-1f4a63a1a658] of recording [recid1] from contact center [46284f2f-d615-4329-957a-f5341edfd5d7] requested
```

```
10/28/2013 15:46:11.033 [ops] [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.71 Safari/537.36] [192.168.135.1] /api/v2/ops/contact-centers/46284f2f-d615-4329-957a-f5341edfd5d7/recordings/recid1/play/2cb4ea04-f81d-44e8-83b6-1f4a63a1a658.mp3 Play media [2cb4ea04-f81d-44e8-83b6-1f4a63a1a658] of recording [recid1] from contact center [46284f2f-d615-4329-957a-f5341edfd5d7] requested
```

f5341edfd5d7] succeed

10/28/2013 15:46:52.179 [admin@genesyslab.com] [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.71 Safari/537.36] [192.168.135.1] /api/v2/recordings/recid0 Delete recording [recid0] from contact center [46284f2f-d615-4329-957a-f5341edfd5d7] requested

10/28/2013 15:46:52.216 [admin@genesyslab.com] [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.71 Safari/537.36] [192.168.135.1] /api/v2/recordings/recid0 Delete recording [recid0] from contact center [46284f2f-d615-4329-957a-f5341edfd5d7] failed

10/28/2013 15:46:56.253 [admin@genesyslab.com] [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.71 Safari/537.36] [192.168.135.1] /api/v2/recordings/recid1 Delete recording [recid1] from contact center [46284f2f-d615-4329-957a-f5341edfd5d7] requested

10/28/2013 15:46:56.420 [admin@genesyslab.com] [Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.71 Safari/537.36] [192.168.135.1] /api/v2/recordings/recid1 Delete recording [recid1] from contact center [46284f2f-d615-4329-957a-f5341edfd5d7] succeeded

Setting the Advanced Options for Web Services

API Thread Pool

Web Services provides properties for the Call Recording API thread pool via archaius.

The following table describes the parameters required to set the API thread pool.

| Property/API Name | Thread Pool Name | Description |
|---|------------------|--|
| hystrix.command.[API Name]. execution.isolation.thread.timeoutInMilliseconds | N/A | The hystrix timeout. The default value is set to 6000. |
| hystrix.threadpool.[API Pool Name] .coreSize | N/A | The thread pool size. The default value is set to 10. |
| RecordingOperationApiTaskV2 | ApiOperationPool | The call or screen recording operation. |
| CreateCallRecordingApiTaskV2 | ApiCreatePool | Create call recording |
| DeleteCallRecordingApiTaskV2 | ApiDeletePool | Delete call recording |
| GetCallRecordingApiTaskV2 | ApiGetPool | Get call recording meta data |
| GetCallRecordingCFInfoApiTaskV2 | ApiGetPool | Get call recording CF Information |
| GetCallRecordingMediaApiTaskV2 | ApiGetPool | Streaming call recording media |
| QueryCallRecordingApiTaskV2 | ApiQueryPool | Query call recording Meta data |

For more information about the Web Services Call Recording API, see the [Web Services API Reference](#).

SIP Server

Configuring the SIP Server Application

| Section Name | Parameter Name | Description |
|--------------|------------------------------|--|
| TServer | msml-support | Set to true to enable support of the call recording solution. |
| | resource-management-by-rm | Set to true to enable support of the call recording solution. Resource monitoring and notification will be done by the Resource Manager. SIP Server will contact Media Server through Resource Manager. |
| | msml-record-support | Set to true to enable SIP Server to engage GVP as a Media Server through the msml protocol for call recording. |
| | msml-record-metadata-support | Set to true to send additional metadata in the INFO message of Genesys Media Server when starting call recording. |
| | record-consult-calls | Specifies whether to record consult calls: <ul style="list-style-type: none">• true—record consult calls.• false—do not record consult calls. |
| | recording-filename | Must be set to \$UUID\$_\$DATE\$_\$TIME\$. |

VoIP Service

Configuring a DN for VoIP Service

1. Create a new MSML DN object and add the following parameters to the General tab:
 - Number = The name of the MSML Server
 - Type = Voice over IP Service
2. Add the following parameters to the Annex tab of the new DN:

| Section Name | Parameter Name | Description |
|--------------|------------------------|--|
| TServer | Contact | Set this to the Resource Manager IP address and port. Use the following format: sip: <Resource Manager_IP_address:Resource Manager_SIP_port> Specifies the contact URI that SIP Server uses for communication with the treatment server. |
| | service-type | Set to msml |
| | Prefix | Set to msml= |
| | subscription-id | Set to the name of the tenant to which this SIP Server belongs, using the following syntax <TenantName> |
| | refer-enabled | Set to false |
| | make-call-rfc3725-flow | Set to 1. |
| | ring-tone-on-make-call | Set to false. |
| | sip-hold-rfc3264 | Set to true |
| | oos-check | Set to 5 |
| | oos-force | Set to 4 |

To enable separate voice recording storage for each SIP Server instance, add the following parameter to the VoIP Service DN (msml):

- `TServer.sip-uri-params = gvp-tenant-id=Recording00`, where `Recording00` is the IVR profile name assigned for this SIP Server instance.

Agent DN

Configuring the Agent's DN

On the Agent's DN, set the following parameter:

- `enable-agentlogin-presence` to `true`

GVP

Configuring Genesys Voice Platform

[+] Resource Manager

1. Set the the `rm` section of your Genesys Voice Platform (GVP) Resource Manager application, configure the following parameters:

| Section Name | Parameter Name | Value |
|--------------|---------------------------------|---------------|
| rm | conference-sip-error-respcode | Set to 503. |
| | resource-unavailable-respcode | Set to 603 |
| | ignore-ruri-tenant-dbid | Set to true. |
| monitor | sip.proxy.realeaseconfonfailure | Set to false. |

2. For each GVP shared tenant, a separate tenant is required by Resource Manager. Create a gateway resource for each tenant RM tenant using the SIP Server source address.

[+] IVR Profile

1. In Genesys Administrator Extension, navigate to **Configuration > System > Configuration Manager**. Under **Voice Platform**, select **Voice Platform Profiles**, and click **New**.
2. On the **General** tab, enter the following parameters:
 - **Name** (Genesys recommends naming it recording)

- **Display Name**
- **Description**

3. On the **Options** tab, configure for basic authorization:

- In the `gvp.service-paramters` section, set the `recordingclient.callrec_authorization` parameter to `fixed,rp_username:rp_password`.

Important

The `username:password` value must be the same username and password that is configured in the Recording Processor Script. For more information, see [Configuring Basic Authorization](#) for the Recording Processor Script.

4. On the **Recording** tab, add the Recording Certificates, and set the following parameters:

| Section | Parameter Name | Description |
|------------------------|-----------------------------------|--|
| Recording Destinations | Storage Destination | <p>The path to the first recording destination. For example, <code>http://testing.com</code>.</p> <p>Note: The Storage Destination must be unique for each IVR Profile.</p> |
| | Storage HTTP Authorization Header | <p>The authentication for the first destination of the recorder. The format is <code>username:password</code>, where <code>username</code> and <code>password</code> are the webserver credentials. This field is visible only if the Storage Destination is either HTTP or HTTPS.</p> |
| | Recording Processor URI | <p>The URI that MCP uses to post the metadata of the audio recording after the recording is complete. MCP uses HTTP POST to send the metadata to the Recording Processor. The format for this parameter is: <code>http:// <Recording Processor Host>/api/contact-centers/<Contact Center Domain Name>/recordings/</code>.</p> <p>Note: The value for the URI must always end with a forward</p> |

| Section | Parameter Name | Description |
|--|---|---|
| | | slash (/). |
| | SpeechMiner Interaction Receiver | Specifies the URL that points to the SpeechMiner service responsible for accepting metadata from the Recording Processor script for this profile. |
| | SpeechMiner Interaction Receiver Authorization Header | Specifies the authorization information required to connect to the SpeechMiner service used by the Recording Processor Script. The format is username:password, where the username and password are the webserver credentials. |
| Speech Analytics Parameters Note: Leave these parameters empty unless you have purchased and enabled speech analytics mode on SpeechMiner; otherwise, recording may not operate correctly. | SpeechMiner Destination | The path to the SpeechMiner server that is used for analytics. For example, http://speechminer/. This is an optional parameter and should be left empty if speech analytics is disabled. |
| | SpeechMiner HTTP Authorization Header | The authentication for the first destination of the recorder. The format is username:password, where username and password are the webserver credentials. This field is visible only if the SpeechMiner Destination is either HTTP or HTTPS. |
| Additional Recording Parameters | Recording Storage MIME Type | The audio file type used for the storage recording. Set to audio/mp3. |
| | Recording Alert Tone Source (Optional) | The URI of the audio tone. For example, http://example.com/tone.wav. |
| Recording File Name Template | File Name Template | <p>Specifies the name of the template used for generating the MSML recording. When left blank, the default value is \$id\$. Choose any, or all of the following parameters:</p> <ul style="list-style-type: none"> • ID—The unique identifier of the template. • Date Time—The date and time of the call in which the recording is started. The date and time is sent in ISO format with UTC time. The ISO format is YYYY-MM- |

| Section | Parameter Name | Description |
|---------|----------------|--|
| | | <p>DDTHH:MM:SSZ</p> <ul style="list-style-type: none">• MCP Date Time—The local date and time of the call in which the recording is started. The local time follows the MCP instance where the recording is taking place.• SIP Server Application Name—The SIP Server application name in which the recording is started.• Call UUID—The call UUID of the call in which the recording is started.• ANI—The ANI information of the call in which the recording is started.• Connection ID—The TLib Connection ID of the call in which the recording is started.• DNIS—The DNIS information of the call in which the recording is started.• Agent ID—The agent ID of the DN of the call in which the recording is started. If the recording has not started because the DN or Agent ID has not logged in, this parameter will not be present. <p>For example, if DNIS, ANI and Agent ID are selected, the File Name Template is set to \$dnis\$_\$ani\$_\$agentId\$.</p> <p>Note:Using too many parameters could exceed the 260 characters limit for a Windows file name.</p> |

[+] Logical Resource Group

A single Media Control Platform (MCP) pool can be used to provide all types of media services including call recording. A dedicated Logical Resource Group can also be used for call recording.

1. Modify a Logical Resource Group to include call recording:
 - Set the service-types option to `voicexml;conference;announcement;cpd;media;recordingclient`.
2. Create a new Logical Resource Group. In the **gvp.lrg** section, set the following parameters:

| Parameter Name | Value |
|----------------------|-----------------|
| service-types | recordingclient |
| load-balance-scheme | round-robin |
| monitor-method | option |
| port-usage-type | in-and-out |
| resource-confmaxsize | -1 |

Important

If using a dedicated Logical Resource Group, ensure that the `recordingclient` value is removed from the MCP pool's **service-types** parameter. For example, set the service type to `voicexml;conference;announcement;cpd;media`.

[+] Media Control Platform(s)

1. Ensure that the Media Control Platform (MCP) instances are included on the **Connections** tab of the Resource Manager Application object.
2. In mcp section, set the `default_audio_format` parameter to ULAW, or ALAW, depending on the G711 settings.
3. Configure the Root Certificate Authority (CA) for recording certificate validation by setting one of the following parameters in the **mpc** section:

| Parameter Name | Value |
|-----------------------|---|
| mediamgr.CA_File | Set to the location of the Root CA certificate. |
| mediamgr.CA_Directory | Set to the location of the Root CA directory. Note: When assigning the MCP(s) for handling call recording, the IP address and Port must match the |

| Parameter Name | Value |
|----------------|---|
| | details of the MCP. Set the max ports option to double the number of calls that you want to handle with the MCP. One port is used per stream in the call, one for the customer leg and one for the caller leg. If max_ports is set to 1000, the MCP can handle 500 calls. |

For more information about the GVP and Media Server options, see the [Genesys Voice Platform Media Server Configuration Options](#).

Geo-location

Configuring Geo-location

Geo-location is configured in two objects:

- DN objects in a switch
- Resource Groups for MCP and Recording Servers.

You can assign a geo-location tag for each DN (of type Trunk DN, Route Point DN, Extension DN, and Trunk Group DN). The geo-location option is configured in the TServer section of these places.

To assign a geo-location tag for a Resource Group (for MCP and Recording Server separately), use the Resource Group Wizard and set the geo-location as part of the Wizard process.

Usage

Geo-location is selected for each call depending on the usage model.

SIP Server selects the geo-location with the following order of preference for inbound calls:

1. Geo-location configured in the extensions of RequestRouteCall.
2. Geo-location configured in the Routing Point DN.
3. Geo-location configured in the inbound Trunk DN.
4. Geo-location configured in the DN where the recording is enabled.

For outbound calls, the following order of preference is used:

1. Geo-location configured in the extensions of RequestRouteCall.
2. Geo-location configured in the Routing Point DN.
3. Geo-location configured in the Agent DN.
4. Geo-location configured in the outbound Trunk DN if recording is enabled.

Full-time Recording

When a DN is configured to be recorded, the geo-location is set at the DN. When more than one DN involved in the call has the geo-location set (for example, both the inbound Trunk DN and the Routing Point DN have the geo-location parameter set), then SIP Server selects the geo-location based on the order of preference listed above.

Selective Recording from a Routing Strategy

If record=source is set in the RequestRouteCall extensions, the geo-location of the inbound Trunk DN of the call is selected (if it is configured). If record=destination is set in the RequestRouteCall extensions, the geo-location of the agent (Extension DN) is selected.

Dynamic Recording

When dynamic recording is initiated by the T-lib RequestPrivateService function, the geo-location is selected based on the recorded DN in the call. Specifically:

- If RequestPrivateService is requested with AttrExtensions as record = source, the geo-location configured for thisDN is selected. record=source is the default value if the extension is not defined.
- If RequestPrivateService is requested with AttrExtensions as record = destination, the geo-location configured for otherDN is selected.

Audio Tones

Configuring Audio Tones

The following section outlines the general configuration for audio tones.

Media Server

The following table describes the options required for audio tones when using Media Server:

| Section Name | Parameter Name | Description |
|--------------|--------------------------|--|
| Conference | record_recorddnhearstone | Specifies whether the RecordDN (Party A) hears the repeating tone. |

| Section Name | Parameter Name | Description |
|--------------|-------------------------|---|
| Conference | record_otherdnhearstone | Specifies whether the OtherDN (Party B) hears the repeating tone. |

Media Server allows you to configure whether the recording also gets the audio tone. When the audio tone is injected into the call, Media Server distinguishes between what the participant hears and what the participant says. The above two configuration parameters affect what the participant hears.

| Section Name | Parameter Name | Description |
|--------------|-------------------------|---|
| Conference | record_chan2source | <p>Specifies the recorded media that represents the first participant (Record DN) in the recording session.</p> <ul style="list-style-type: none">• recorddnsays• otherdnhears <p>If the Other DN is configured to receive consent and you want the consent to be recorded, set the value to otherdnhears.</p> |
| Conference | record_otherdnhearstone | <p>Specifies the recorded media that represents the second participant (Other DN) in the recording session.</p> <ul style="list-style-type: none">• otherdnsays• recorddnhears <p>If the Record DN is configured to receive consent and you want the consent to be recorded, set the value to recorddnhears.</p> |

Workspace Desktop Edition (formerly known as Interaction

Workspace)

Configuring Workspace

To configure MSML recording, set the following Workspace parameters:

| Parameter Name | Value |
|--|--|
| <code>active-recording.voice.recorder-uri</code> | Leave empty. The file recording destination is configured through the GVP IVR Profile. |
| <code>active-recording.voice.recording-type</code> | MSML |

Your Genesys Interaction Recording Solution is ready to start recording.

ICON

Configuring ICON

Configure your ICON application to filter the metadata to display specific keys in SpeechMiner.

In the `callconcentrator` section of the ICON application, set the following parameters:

- `adata-reasons-history` = none
- `adata-extensions-history` = none
- `adata-userdata-history` = all
- `role` = all

For more information about the ICON options, see the [Interaction Concentrator 8.1 Deployment Guide](#).

To improve ICON performance for Genesys Interaction Recording, Genesys recommends updating the Genesys Interaction Recording dedicated ICON database schema with the following new indexes:

- Index `G_PARTY`:
 - NONCLUSTERED/NONUNIQUE INDEX `G_PARTY.CALLID`

- Index G_USERDATA_HISTORY:
 - NONCLUSTERED/NONUNIQUE INDEX G_USERDATA_HISTORY.CALLID
- Index G_IS_LINK:
 - NONCLUSTERED/NONUNIQUE INDEX G_IS_LINK.CALLID

For optimal performance, it is recommended that the ICON's gsysPurge81 stored procedure (or similar) be used regularly to purge call data from the ICON database that is older than one or two days. See the [Interaction Concentrator 8.1 Deployment Guide](#) for more information.

Recording Processor Script

Configuring the Recording Processor Script

For information about configuring the Recording Processor components, see [Deploying the Recording Processor Script](#).

Recording Crypto Server

Configuring the Recording Crypto Server

For information about configuring the Recording Processor components, see [Deploying the Recording Crypto Server](#).

Recording Plug-in

Configuring the Recording Plug-in for Genesys Administrator Extension

For information about configuring the Recording Processor components, see [Deploying the Plug-in for Genesys Administrator Extension](#).

SpeechMiner

Configuring the SpeechMiner Components

Important

For information about upgrading the contributing solution components, see the specific upgrade procedures for each component, or see the latest [Genesys Migration Guide](#). Ensure that you have allotted sufficient time to upgrade the components, and that you have factored-in any downtime required for non-HA deployments. Plan accordingly.

[+] Change the Default Home

1. In the webserviceParams table in the SpeechMiner database, verify that the defaultHomePage parameter is set to /pages/calls/querySettings.aspx?.
2. Restart IIS.

Important

This step is required for Recording-only Licenses in order to prevent login permission errors.

[+] Configure the SpeechMiner Database

1. Set the HttcUrl field to the Web Services URL. For example, http://<Web Services host>:<port> or https://<Web Services host>:<port>.
2. Set the RcsUri field to the Recording Cytpo Server URL. For example, http://<Recording Crypto Server Host>:<port>/rcs or https://<Recording Crypto Server Host>:<port>/rcs/.

Important

Use https for the Web Services connection if the connection to the Speechminer web server is configured with https.

3. In the cmrsParms section, set the following parameters:

| Parameter Name | Value |
|-------------------|---|
| RP_Authorization | Set to the Recording Processor username and password. For example, <Recording Processor Username>:<Recording Processor Password>. |
| MCP_Authorization | Set to the Media Control Platform (MCP) username and password. For example, <MCP Username>:<MCP Password>. Note: The MCP_Authorization parameter applies to the Recording and Analytics mode only. |

4. Depending on the installation mode, perform one of the following:

- In **Recording and Analytics** mode, create and apply a program in SMART and set the DEF_PROGRAM_EX_ID in the cmrsparams section to that program's external ID.
- In **Recording Only** mode, set the name for the program you want to use.

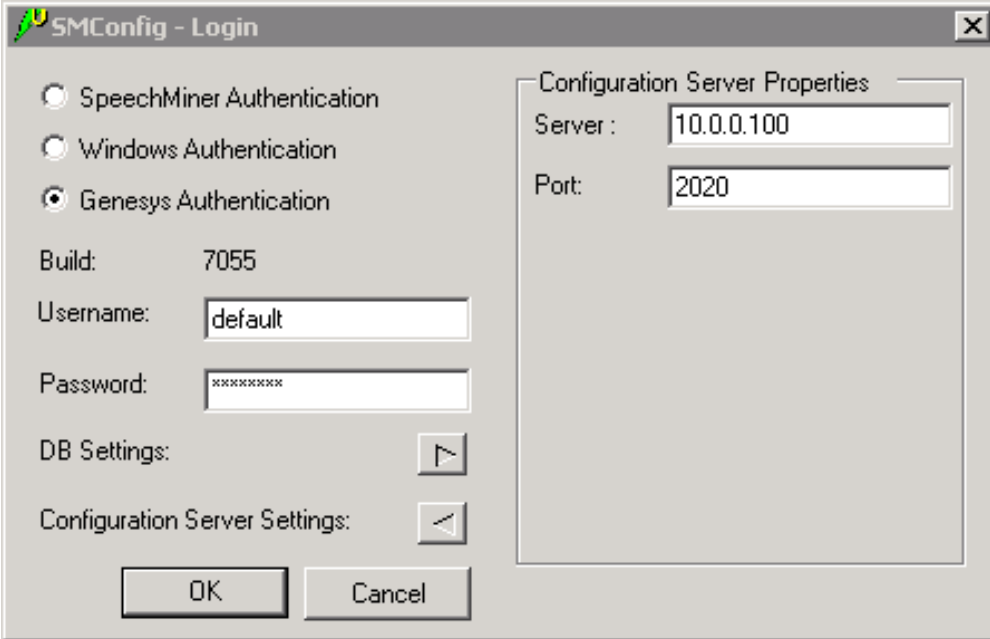
Important

Both of these actions can be skipped, if the default in the database is satisfactory, or if the Recording Processor includes the program ID in the metadata. On a per-call basis, the attached data key GRECORD_PROGRAM can be set to define the program external ID to be used for this call. For example, attached data can be set in a routing strategy.

[+] Configure SpeechMiner

1. Use Genesys Administrator, or Genesys Administrator Extension to create a new Application Template. Enter Speechminer in the **Name** field, Genesys Generic Server in the **Type** field, and 8.5.2 in the **Version** field.
2. Create a new Application object.
 - a. Enter SpeechMiner in the **Name** field.
 - b. Assign the Speechminer application template that you created in step 1.
 - c. Set the host to the <SpeechMiner host>.

- d. The **Start info** Working Directory, Command Line must not be empty. Set it to ". ".
3. In the **SMConfig-Login** screen (SpeechMiner Configuration), login with your Configuration Server credentials (for example, default/password) and set the Configuration Server host and port.

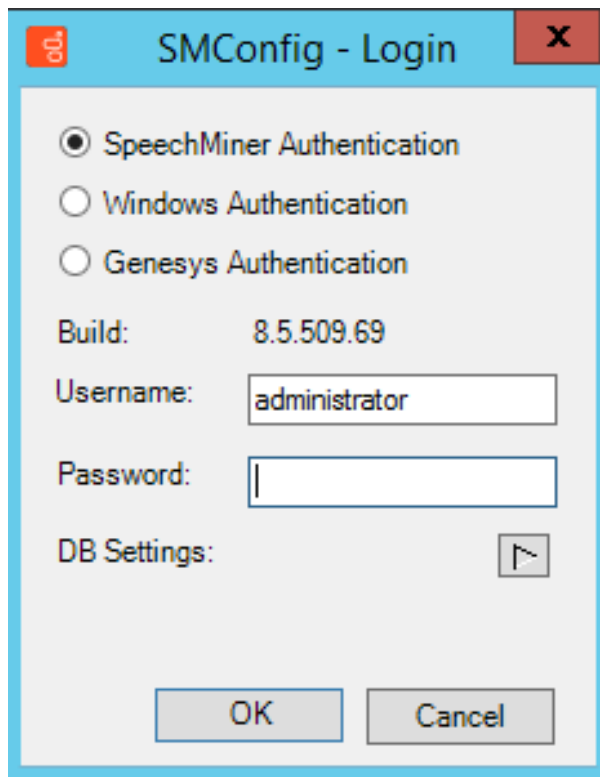


The image shows the 'SMConfig - Login' dialog box. It has a title bar with a green icon and a close button. The main area contains three radio buttons for authentication: 'SpeechMiner Authentication', 'Windows Authentication', and 'Genesys Authentication' (which is selected). Below these are fields for 'Build:' (7055), 'Username:' (default), and 'Password:' (masked with asterisks). There are also buttons for 'DB Settings:' and 'Configuration Server Settings:'. On the right, a 'Configuration Server Properties' panel shows 'Server:' (10.0.0.100) and 'Port:' (2020). At the bottom are 'OK' and 'Cancel' buttons.

Important

When you are logging in for the first time, you must go to the license tab, and add your recording-only license, and login to SM Config again. Step 2 will look different if you do not add the recording-only license.

4. In the **Sites and Machines/Machines and Tasks** screen:
 - Configure the Interaction Receiver tasks.



5. The following **tasks** must be enabled in your SpeechMiner configuration:

- Recording only mode:
 - web server
 - interaction receiver
 - indexer

6. In the **Audio** panel of SMConfig, set the following to avoid creating unnecessary audio files and storing them for too long:

| Parameter | Value |
|------------------------------|-----------------|
| Recognition Audio Format | WAV_PCM |
| Create compressed audio file | Do not Generate |
| WAV_PCM Retention Period | 0 |

Audio

Recognition Audio Format
Select the audio format for recognition:
WAV_PCM

Playback Audio Format
Create compressed audio file: Do not Generate
If compress format not available:
☒ Play recognition file
☐ Convert the recognition file on-the-fly to: WAV_MULAW

Retention Policies

| Site | Format | Retention Period (Hours) |
|---------|---------|--------------------------|
| default | WAV_PCM | 0 |

Playback Speeds

| Rate | |
|------|--|
| 1 | |

7. Configure the roles and permissions for the **SpeechMiner Users**.

Your Genesys Interaction Recording System is ready for voice recording.

TLS

Configuring TLS for the Genesys Interaction Components

For more information about configuring the transport layer security for the Genesys Interaction Recording components, see **Secure Transport Configuration**.

Access Control

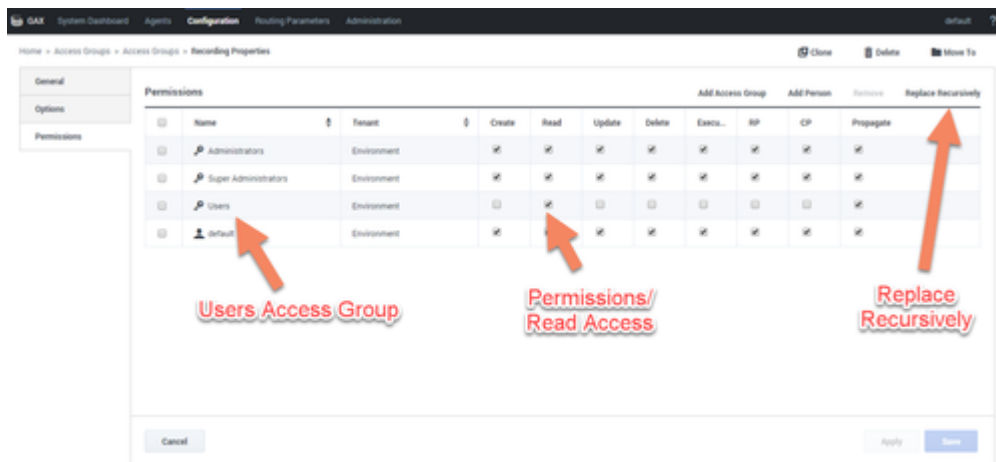
Configuring Access Control

Configuring Access Groups

By default, the Configuration Server has an Access Group called Users stored in the configuration database.

Install the Solution Deployment SPD file "Creation of base SpeechMiner access groups" option to perform the following steps:

1. Create an Access Group called SpeechMiner Users, and set the permission to grant Users Access Group with Read access.
2. Add a new folder within Access Groups, called Recording, and set the permission to add Users Access Group with Read access. Make sure the Replace Permissions Recursively flag is set as shown in the following diagram:



3. Create the / (forward slash) Access Group within the Recording folder.

Configuring SpeechMiner Users

All users for SpeechMiner must be assigned to two Access Groups—Users and SpeechMiner Users. If agent hierarchy and partition features are not used, assign all the SpeechMiner users to the / (slash) Access Group. If agent hierarchy or partition features are used, the users must be granted to the specific Access Groups in order to be able to access recordings for the various agent hierarchy and partitions.

Important

For your SpeechMiner users to have login access to the SpeechMiner UI, you must give SpeechMiner users Read and Execute rights on the default Application object.

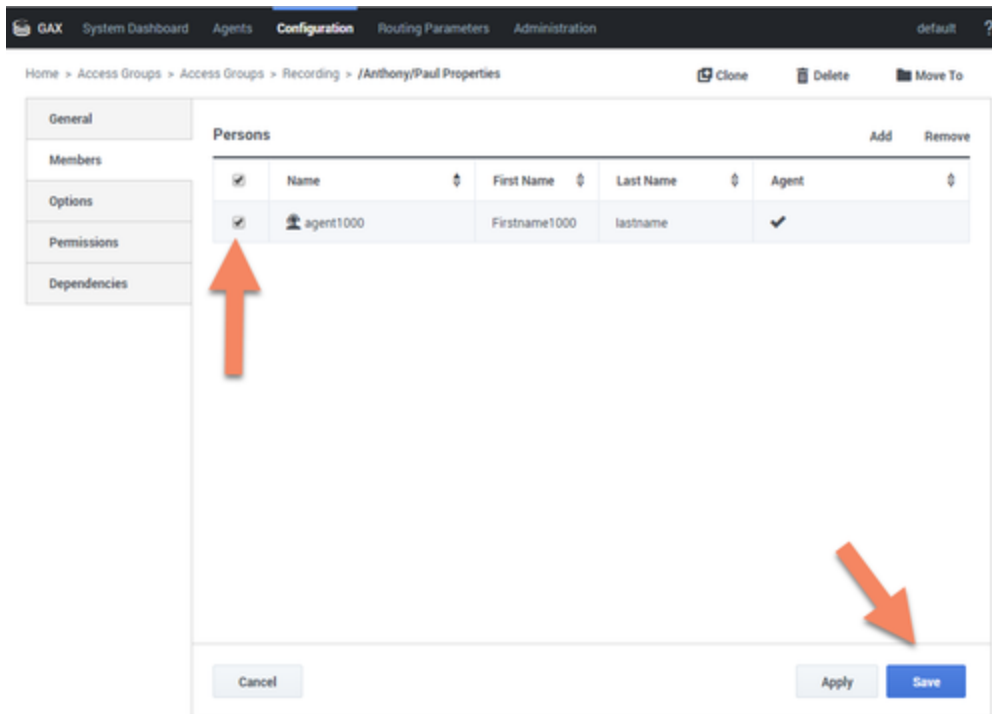
You must configure Genesys Interaction Recording to enable the SpeechMiner UI search option to display a list of agent names:

1. In the Agent's Person object, create a recording section in the Annex (if it doesn't already exist).
2. Add the `agent_hierarchy` option in the recording section, and set the value to slash: "/" or what is appropriate for access control.
3. Repeat these steps for any additional agents that might be searched for in the SpeechMiner UI.
4. The SpeechMiner cache might need to be updated for this configuration to take effect:
 - In the `configServer` table of the Configuration Server database, update the `updateAgentsEveryH` column to the number of hours between the SpeechMiner person object updates. SpeechMiner will check the Configuration Server according to this option at regular intervals to retrieve the list of person objects under the Recording folder access group. The names of these agents are then available when searching for call recordings or screen recordings. Restart the Interaction Receiver IIS application for this change to take effect.
 - If the list of agents does not update, update the `NextAgentsUpdate` column in the `configServer` table to a date in the near future to force a quicker update.

Important

- The Access Group / (forward slash) grants access to all recordings.
- Genesys Recommends using caution when using the Audio Protection: Comments role. You might not hear any part of the call if the call being played has no comments. You will only hear audio the corresponds to the areas where comments have been made.

The follow is a screen shot showing the assignment of Access Group members to /Anthony/Paul in Genesys Administrator Extension:



The Recording Plug-in for Genesys Administrator Extension includes a **Solution Definition (SPD)** file that can be used to configure roles and access groups.

Configuring Roles

For information about configuring roles for Genesys Interaction Recording users, see **Roles** in the Genesys Administrator Extension User's Guide.

Configuring Agent Hierarchy

Agent hierarchy and partitions are not required to record calls or access recordings; however, all agents must be assigned to the Users Access Group.

If agent hierarchy is required, assign the agent's hierarchy by configuring the `agent_hierarchy` option in the recording section of the Person object's Annex tab. For each hierarchy name, create a corresponding Access Group object within the Recording folder.

For the example above, create the following Access Groups:

- /
- /Anthony
- /Anthony/John

- /Anthony/Paul

The deployment can also grant access control for each specific agent, and in order to use this functionality, create an Access Group for each agent. For the same example, create the following Access Groups:

- /Anthony/John/Agent1
- /Anthony/John/Agent2
- /Anthony/Paul/Agent3
- /Anthony/Paul/Agent4

Important

Each branch in the hierarchy must have a unique name. You can not use branches with the same name. The following examples are will not work:

- /Anthony/Anthony (parent and child with the same name)
- /Anthony/John and /Steve/John (branches under Anthony and Steve have the same name)

Configuring Partitions

For each partition used in the contact, create an Access Group object with the name of the partition within the Recording folder. For example, if there are three partitions— /sales, /support, and /marketing, create three Access Group objects named /sales, /support, and /marketing, respectively.

Important

Access Group names for partitions and agent hierarchy must be unique for each tenant.

For more information about configuring Access Controls in Genesys Administrator Extension, see the [Genesys Administrator Extension User Guide](#).

Encryption

Configuring Encryption for Call Recording

Call Recording

A Recording Certificate binds a public encryption key to a particular recorded message identity.

The following steps describe how to configure encryption for voice recordings:

Prerequisites

- A certificate for the Certificate Authority (CA) in .pem format—for example, ca_cert.pem.
 - A recording certificate (also known as public key) in .pem format—for example, 02_gir_cert.pem.
 - A recording private key in .pem format—for example, 02_gir_priv_key.pem.
1. On the machine where the Recording Crypto Server is installed, place the Certificate Authority (ca_cert.pem) in the <Record Crypto Server Install Directory>\RCS directory.
 2. Edit the rcs.properties file:
 - a. Change the value of the cacertstorepath parameter to ca_cert.pem.
 - b. Set the value of the cacertstorepassword parameter to the valid password.
 3. Restart the Recording Crypto Server.
 4. Using Genesys Administrator, edit all your Media Control Platforms (MCP):
 - On the **Options** tab of each MCP application object, in the mpc section, set the mediamgr.CA_file parameter to the location of the Certificate Authority file (for example, c:\keystore\ca_cert.pem).
 5. Restart all the MCP instances.

You are now ready to upload and deploy your certificates to complete the encryption process.

A Recording Certificate binds a public encryption key to a particular recorded message identity.

Important

When configuring encryption, backup of the private key is your responsibility. If the private key becomes lost or corrupt, any

recording encrypted using that key will become unusable.

The following steps describe how to configure encryption for voice recordings:

Prerequisites

- A certificate for the Certificate Authority (CA) in .pem format—for example, `ca_cert.pem`.
 - A recording certificate (also known as public key) in .pem format—for example, `02_gir_cert.pem`.
 - A recording private key in .pem format—for example, `02_gir_priv_key.pem`.
1. On the machine where the Recording Crypto Server is installed, place the Certificate Authority (`ca_cert.pem`) in the <Recording Crypto Server Install Directory>\RCS directory.
 2. Edit the `rcs.properties` file:
 - a. Change the value of the `cacertstorepath` parameter to `ca_cert.pem`.
 - b. Set the value of the `cacertstorepassword` parameter to the valid password.
 3. Restart the Recording Crypto Server.
 4. Using Recording Plug-in for Genesys Administration Extension, edit all your Media Control Platforms (MCP):
 - On the **Options** tab of each MCP application object, in the `mcp/tt>` section, set the `mediamgr.CA_file` parameter to the location of the Certificate Authority file (for example, `c:\keystore\ca_cert.pem`).
 5. Restart all the MCP instances.

For an example of a certificate, see [Sample Certificate and Key File Generation](#). You are now ready to upload and deploy your certificates to complete the encryption process.

[+] Show how to upload a Certificate

To upload a new certificate:

1. Log in to Genesys Administrator Extension, and navigate to **Configuration > Recording Crypto Server > Certificates**.

The screenshot shows the Genesys Administrator Extension interface. The top navigation bar includes the Genesys logo, 'Administrator Extension', a user profile 'Welcome default', and links for 'Log Out', 'Help', and a settings icon. Below this is a secondary navigation bar with icons and labels for 'Home', 'Accounts', 'Configuration' (which is highlighted), and 'Operations'. The main content area is titled 'Recording Certificates' and features a 'Delete' button and an 'Upload' button. A 'Quick Filter' input field is also present. Below the filter is a table with the following data:

| Issued To | Issued By | Expires | Deployed Count |
|--|---------------------------|------------|----------------|
| ● Cert5user Lastname <cert5user@genesys.com> | Certificate Administrator | 2024-04-28 | 0 |
| ● Cert1 User <cert1.user@genesyslab.com> | Certificate Administrator | 2024-04-22 | 0 |
| ● User2 <user2@genesyslab.com> | Certificate Administrator | in 6 weeks | 0 |
| ● Cert1 User <cert1.user@genesyslab.com> | Certificate Administrator | Expired | 0 |
| ● User3 <user2@genesyslab.com> | Certificate Administrator | in 6 weeks | 1 |
| ● Cert6user Lastname <cert6user@genesys.com> | Certificate Administrator | 2024-04-28 | 0 |
| ● Cert7user Lastname <cert7user@genesys.com> | Certificate Administrator | 2024-04-28 | 0 |

2. On the **Recording Certificates** panel, click **Upload**.

Upload Certificate [X]

Certificate File * ⓘ

Choose File No file chosen

Subject Name

Serial Number

Subject DN

Issuer DN

Key File * ⓘ

Choose File No file chosen

Key Details

Private Key Password ⓘ

Save **Cancel**

3. On the **Upload Certificate** panel, in the **Certificate File** section, click **Choose File**.
4. Select the appropriate file. This file must contain an X.509 RSA certificate in PEM format. The **Subject Name**, **Serial Number**, **Subject DN**, and **Issuer DN** fields automatically populate.
5. In the **Key File** section, click **Choose File**.
6. Select the appropriate file. The file must contain an RSA private key in PEM format. The encoding can be in either Openssl RSA private key or PKCS8 format. The **Key Details** field automatically populates.

Upload Certificate [X]

Certificate File * [i]
[Choose File] cert1.pem

Subject Name [Cert1 User <cert1.user@genesyslab.com>] **Serial Number** [1]

Subject DN
C=CA,ST=Ontario,L=Markham,O=Genesys Telecommunications Laboratories,CN=Cert1 User,E=cert1.user@genesyslab.com

Issuer DN
C=CA,ST=Ontario,L=Markham,O=Genesys Telecommunications Laboratories,CN=Certificate Administrator,E=cert.admin@genesyslab.com

Key File * [i]
[Choose File] cert1.key

Key Details
Openssl format private key file

Private Key Password * [i]
[]

[Save] [Cancel]

7. If the private key file is encrypted, enter the **Private Key Password**.

8. Click **Save**.

Important

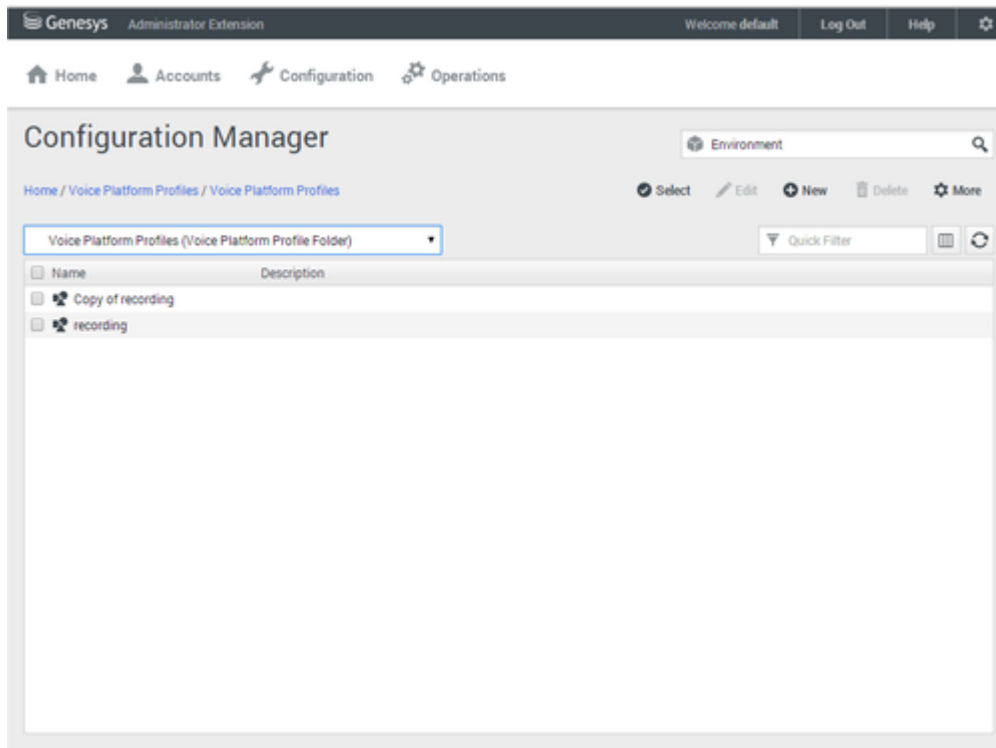
- If you Upload and/or delete recording certificates in one Genesys Administrator Extension session, these changes are not reflected in another Genesys Administrator Extension session. You must log out and login again to the second Genesys Administrator Extension session.
- If Recording Crypto Server (RCS) is restarted when a Genesys Administrator Extension user is logged in, the next Genesys Administrator Extension operation involving RCS

fails because the RCS session saved by the Recording Plug-in for Genesys Administrator Extension does not exist. RCS will return a 401 "RCS is not available" error. The agent must log out, and log in again when receiving the 401 "RCS is not available" error.

[+] Show how to deploy a Certificate

To deploy a new certificate:

1. Log in to Genesys Administrator Extension, and navigate to **Configuration > Configuration Manager > Voice Platform Profiles**.



2. From the **Voice Platform Profiles** screen, click on the recording that you want to add the certificate to.

The screenshot shows the Genesys Administrator Extension interface. The top navigation bar includes the Genesys logo, 'Administrator Extension', and links for 'Welcome default', 'Log Out', 'Help', and a settings icon. Below this is a secondary navigation bar with icons and labels for 'Home', 'Accounts', 'Configuration', and 'Operations'. The main content area is titled 'Configuration Manager' and shows a breadcrumb trail: 'Home / Voice Platform Profiles / Voice Platform Profiles / recording Properties'. To the right of the breadcrumb are icons for 'Clone', 'Delete', and 'Move To'. On the left, a sidebar menu has four items: 'General', 'Options', 'Permissions', and 'Recording'. The 'Recording' item is selected. The main form area contains the following fields: 'Name *' with the value 'recording', 'Display Name *' with the value 'Recording', a large empty 'Description' text area, a 'Tenant' dropdown menu currently showing 'Environment', and a checked checkbox labeled 'State Enabled'. At the bottom of the form are three buttons: 'Save', 'Apply', and 'Cancel'.

3. Select **Recording**.

The screenshot shows the Genesys Administrator Extension Configuration Manager. The left sidebar has a menu with 'General', 'Options', 'Permissions', and 'Recording'. The main content area is titled 'Configuration Manager' and shows the breadcrumb 'Home / Voice Platform Profiles / Voice Platform Profiles / recording Properties'. The 'Recording' tab is selected. The 'Recording Certificates' section has an 'Add' button and a table with columns 'Issued To', 'Issued By', and 'Expires'. Below this is the 'Recording Destinations' section with fields for 'Storage Destination', 'Recording Processor URI', 'SpeechMiner Destination', 'SpeechMiner Interaction Receiver', and 'SpeechMiner Interaction Receiver Authorization Header'. The 'Additional Recording Parameters' section has radio buttons for 'Recording Storage MIME Type' (audio/wav and audio/mp3) and a text field for 'Recording Alert Tone Source'. At the bottom are 'Save', 'Apply', and 'Cancel' buttons.

Genesys Administrator Extension

Home Accounts Configuration Operations

Configuration Manager

Home / Voice Platform Profiles / Voice Platform Profiles / recording Properties

General Options Permissions **Recording**

Recording Certificates

Add Remove

| Issued To | Issued By | Expires |
|-----------|-----------|---------|
| No items | | |

Recording Destinations

Storage Destination *?* SpeechMiner Destination *?*

Recording Processor URI *?* SpeechMiner Interaction Receiver *?*

SpeechMiner Interaction Receiver Authorization Header *?*

username password

Additional Recording Parameters

Recording Storage MIME Type

☐ audio/wav

☒ audio/mp3

Recording Alert Tone Source

Save Apply Cancel

- Click **Add**.
- From the **Select Certificate** screen, select the certificate you want to add to the IVR Profile, and click **Add**.

The screenshot shows the Genesys Configuration Manager interface. The top navigation bar includes Home, Accounts, Configuration, and Operations. The main title is 'Configuration Manager' with a breadcrumb trail: Home / Voice Platform Profiles / Voice Platform Profiles / recording Properties. On the left, a sidebar lists General, Options, Permissions, and Recording. The main content area is titled 'Recording Certificates' and includes an 'Add' button and a 'Remove' button. Below this is a table with columns: Issued To, Issued By, and Expires. The table contains one row: 'Cert1 User <cert1.user@genesyslab.com>', 'Certificate Administrator', and '2024-04-32'. Below the table is a 'Recording Destinations' section with three fields: 'Storage Destination', 'Recording Processor URI', and 'SpeechMiner Destination'. The 'SpeechMiner Destination' field is expanded, showing 'SpeechMiner Interaction Receiver' and 'SpeechMiner Interaction Receiver Authorization H...' with a 'username:password' placeholder. Below this is an 'Additional Recording Parameters' section with 'Recording Storage MIME Type' (radio buttons for audio/wav and audio/mp3, with audio/mp3 selected) and 'Recording Alert Tone Source'. Below that is a 'Recording File Name Template' section with a 'File Name Template' field and a list of checkboxes: ID, SIP Server Application Name, ANI, DNIS, Date Time, Call UUID, Connection ID, Agent ID, and MCP Date Time. At the bottom are 'Save', 'Apply', and 'Cancel' buttons.

6. Enter the appropriate values for the following parameters:

| Parameter Name | Description | Syntax and Examples |
|--------------------------------------|---|--|
| Recording Destination Section | | |
| Storage Destination | The path to the first recording destination. | http://testing.com |
| SpeechMiner Destination | The path to the SpeechMiner recording destination. | S3:bucket_test |
| Storage HTTP Authorization Header | The authentication for the first destination of the recorder. This field is visible only if the | The format is username:password, where username and password are |

| Parameter Name | Description | Syntax and Examples |
|---|--|--|
| | Storage Destination is either HTTP or HTTPS. | the web server credentials. |
| Storage AWS Access Key ID | Specifies the Amazon Web Services (AWS) Access Key ID used for building the authorization header to allow access to the Amazon S3 cloud. Note: This field is required if the Storage Destination field is set to S3 (Amazon Cloud). | |
| Storage AWS Secret Access Key | Specifies the AWS Secret Access Key ID used for building the authorization header to allow access to the Amazon S3 cloud. Note: This field is required if the Storage Destination field is set to S3 (Amazon Cloud). | |
| Recording Processor URI | The authentication for the first destination of the recorder. This field is visible only if the SpeechMiner Destination is either HTTP or HTTPS. | The format is username:password, where username and password are the web server credentials. |
| SpeechMiner HTTP Authorization Header | Specifies the Amazon Web Services (AWS) Access Key ID used for building the authorization header to allow access to the Amazon S3 cloud. Note: This field is required if the SpeechMiner Destination field is set to S3 (Amazon Cloud). | |
| SpeechMiner Interaction Receiver | Specifies the URL that points to the SpeechMiner service responsible for accepting metadata from the Recording Processor script for this profile. | |
| SpeechMiner Interaction Receiver Authorization Header | Specifies the authorization information required to connect | The format is username:password, where the |

| Parameter Name | Description | Syntax and Examples |
|--|--|---|
| | to the SpeechMiner serviced used by the Recording Processor Script. | username and password are the web server credentials. |
| Additional Recording Parameters Section | | |
| Recording Storage MIME Type | The audio file type used for the storage recording. | You can choose either audio/wav or audio/mp3. |
| Recording Alert Tone Source | The URI of the audio tone. | http://example.com/tone.wav |
| Recording File Name Template Section | | |
| File Name Template | <p>The template for generating MSML recording file name. When this field is left blank the default value is \$id\$.</p> <p>Note: Using too many parameters could exceed the 260 characters limit for a Windows file name. Select any combination from the following:</p> <ul style="list-style-type: none"> ID (\$id\$)—The unique identifier of the template. SIP Server Application Name (\$sipsAppName\$) —The SIP Server application name in which the recording is started. ANI (\$ani\$)—The ANI information of the call in which the recording is started. DNIS (\$dnis\$) —The DNIS information of the call in which the recording is started. Date Time (\$dateTime\$) —The date and time of the call in which the recording is started. The date and time is sent in ISO format with UTC time. The ISO format is YYYY-MM-DDTHH:MM:SSZ. Call UUID (\$callUuid\$) —The call UUID of the call in which the recording is started. | <p>\$id\$_\$sipsAppName\$_\$callUui d\$_\$ani\$_\$connId\$_\$dnis\$_</p> <p>\$agentId\$_\$dateTime\$_\$MCPDateT</p> |

| Parameter Name | Description | Syntax and Examples |
|----------------|---|---------------------|
| | <ul style="list-style-type: none">• Connection ID (\$connID\$) —The TLib Connection ID of the call in which the recording is started.• Agent ID (\$agentID\$) —The agent ID of the DN of the call in which the recording is started. If the recording has not started because the DN or Agent ID has not logged in, this parameter will not be present.• MCP Date Time (\$MCPDateTime\$) —The local date and time of the call in which the recording is started. The local time follows the MCP instance where the recording is taking place. | |

7. Click **Save**.

Enable Voice Recording

Enabling Voice Recording

Call recording can be enabled through three methods:

1. **Full-time recording or Total recording**—A specific DN is configured to enable recording for all calls for the specific DN.
2. **Selective Recording**—Record a party in the call is determined at a route point and the recording starts as soon as the call is established.
3. **Dynamic Recording**—Start/stop/pause/resume a recording call can be requested by an agent at any time after the call is established using Interaction Workspace.

Once a recording has started, there are two conditions where the recording stops:

1. When the party being recorded leaves the call, or when the customer drops the call. For example, when the recording applies to the agent in the call and the call is transferred to a second agent. The recording is stopped when the agent leaves the call. Note that the second agent can have recording

enabled and the same call gets recorded with a second call recording segment.

2. When dynamic recording control requests the recording to be stopped.

Important

If using Workspace Desktop Edition for the agent desktop, the agent can hide the status of the recording. This functionality can be enabled through Workspace role configuration. For more information, see the [Setting Up Agents on the System](#) in the Workspace Desktop Edition documentation.

Enabling Screen Recording

Configure the following components to enable screen recording:

Configure Web Services

Configuring Web Services for Screen Recording

[+] Configure the Parameters

Configuring the Parameters

1. On all Web Services instances, modify the JETTY_HOME/genconfig/server-settings.yaml file, and add the following parameters:

```
crossOriginSettings:
  corsFilterCacheTimeToLive: 120
  allowedOrigins: <Web Services servers>,<SpeechMiner Web Servers>
  allowedMethods: GET,POST,PUT,DELETE,OPTIONS
  allowedHeaders: "X-Requested-With,Content-Type,Accept,Origin,Cookie,authorization,ssid,surl,ContactCenterId,Range"
  allowCredentials: true
screenRecordingSettings:
  screenRecordingEServicesEnabled: true
  screenRecordingVoiceEnabled: true
syncNode: true
multiPartResolverMaxUploadSize: 536870912
multiPartResolverMaxInMemorySize: 536870912
```


Important

Change <Web Services Servers> and <SpeechMiner Web Servers> to the HTTP/HTTPS addresses of the HTCC instances and SpeechMiner Web Servers.

2. Add screen recording features to the Contact Center:

[+] Restart Web Services

Restarting Web Services

For more information on starting and stopping Web Services, see the [Web Services Deployment Guide](#).

[+] Configure Storage Credentials

Configuring the Storage Credentials for Web Services

1. Determine the contact center ID on Web Services using the following command with the ops username and password (ops:ops):

```
curl -u ops:ops http://<Web Services Server>:<Web Services port>/api/v2/ops/contact-centers; echo
```

The following output is returned:

```
{"statusCode":0,"uris":["http://<Web Services Server>:<Web Services port>/api/v2/ops/contact-centers/<contact center ID (in hex format)>"]}
```

Important

Use the <contact center ID (in hex format)> in all subsequent commands.

2. Using a text editor, create a new file called create_table, with the following content:

```
{  
  "operationName": "createCRCF"  
}
```

And then execute the following command:

```
curl -u ops:ops -X POST -d @create_table http:// <Web Services Server>:<Web Services Port>/api/v2/ops/contact-centers/<contact center ID (in hex format)>/screen-recordings --header "Content-Type: application/json"; echo
```

3. Enable storage for a single or multiple locations:

- For a **single** location:

- a. Using a text editor, created the create_single_location file using the following command:

```
{
  "name": "storage",
  "location": "/",
  "value": [
    {
      "storageType": "webDAV",
      "active": true,
      "credential": {
        "userName": "<webdav user>",
        "password": "<webdav password>",
        "storagePath": "<webdav uri>"
      }
    }
  ]
}
```

Important

Replace <webdav user>, <webdav password>, <webdav uri> with the appropriate values.

- b. Execute the following command:

```
curl -u ops:ops -X POST -d @create_single_location http:// <Web Services Server>:8080/api/v2/ops/contact-centers/<contact center ID (in hex format)>/settings/screen-recording --header "Content-Type: application/json"; echo
```

- For **multiple** locations:

- a. Using a text editor, create the create_first_location file using the following command:

```
{
  "name": "storage",
  "location": "<node_location>",
  "value": [
    {
      "storageType": "webDAV",
      "active": true,
      "credential": {
        "userName": "<webdav user>",
        "password": "<webdav password>",
        "storagePath": "<webdav uri>"
      }
    }
  ]
}
```

```
    }  
  ]  
}
```

- b. Execute the following command:

```
curl -u ops:ops -X POST -d @create_first_location http://<Web Services Server>:8080/  
api/v2/ops  
/contact-centers/<contact center ID (in hex format)>/settings/screen-recording  
--header "Content-Type: application/json"; echo
```

Important

Replace <node_location>, <webdav user>, <webdav password>, <webdav uri> with the appropriate values. The values for the <node_location> are similar to the nodePath settings in the server-settings.yaml file, but allow a hierarchical representation. For example, a Web Services node uses a storage setting with a location of "/US" in the nodePath set to "/US/AK" or "/US/HL".

- c. Repeat steps a and b for each location required.

[+] Advanced Configuration

Setting the Advanced Options for Web Services

API Thread Pool

Web Services provides properties for the Screen Recording API thread pool via archaius.

The following table describes the parameters required to set the API thread pool.

| Property/API Name | Thread Pool Name | Description |
|---|------------------|--|
| hystrix.command.[API Name]. execution.isolation.thread. timeoutInMilliseconds | N/A | The hystrix timeout. The default value is set to 6000. |
| hystrix.threadpool.[API Pool Name] | N/A | The thread pool size. The default value is set to 10. |

| Property/API Name | Thread Pool Name | Description |
|-------------------------------------|------------------|---|
| .coreSize | | |
| RecordingOperationApiTaskV2 | ApiOperationPool | The call or screen recording operation. |
| CreateScreenRecordingApiTaskV2 | ApiUploadPool | Create screen recording |
| DeleteScreenRecordingMediaApiTaskV2 | ApiDeletePool | Delete screen recording |
| GetScreenRecordingApiTaskV2 | ApiGetPool | Get screen recording meta data |
| GetScreenRecordingMediaApiTaskV2 | ApiStreamPool | Stream screen recording media |
| QueryScreenRecordingApiTaskV2 | ApiQueryPool | Query screen recording meta data |

For more information about the Web Services Call Recording API, see the [Genesys Interaction Recording API Reference](#).

Configure Encryption

Configuring Encryption for Screen Recording

Assigning Certificates

To assign a new certificate:

1. Using Genesys Administrator Extension, 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.
4. Perform one of the following actions:
 - Click the **Save** button to accept the changes.
 - Click the **Cancel** button to discard the changes.

Setting up the Decryption Proxy

1. Configure the Record Crypto Server (RCS) locations that Web Services uses for encrypted screen

recordings:

- For a **single** location:
 - a. Using a text editor, create the `create_single_location` file using the following command:

```
{
  "name": "decrypt-uri-prefix",
  "location": "/",
  "value": "<rsc uri>"
}
```

Important

Replace `<rsc uri>` with the appropriate value.

- b. Execute the following command:

```
curl -u ops:ops -X POST -d @create_single_location http://<Web Services
Server>:8080/api/v2/ops
/contact-centers/<contact center ID (in hex format)>/settings/screen-recording
--header "Content-Type: application/json"; echo
```

- For multiple locations:
 - a. Using a text editor, create the `create_first_location` file using the following command:

```
{
  "name": "storage",
  "location": "<node_location>",
  "value": "<rsc uri>"
}
```

- b. Execute the following command:

```
curl -u ops:ops -X POST -d @create_first_location http://<Web Services Server>:8080/
api/v2/ops
/contact-centers/<contact center ID (in hex format)>/settings/screen-recording
--header "Content-Type: application/json"; echo
```

Important

Replace `<node_location>` with the appropriate value. The values for the `<node_location>` are similar to the `nodePath` settings in the `server-settings.yaml` file, but allow a hierarchical representation. For example, a Web Services node uses a `decrypt-uri-prefix` setting with a location of `"/US"` if the `nodePath` set to `"/US/AK"` or `"/US/HI"`.

- c. Repeat steps a and b for each location required.

Enable Screen Recording

Enabling Screen Recording

1. To set up recording conditions, add the `recordingWhen` parameter to the `screen-recording-client` section of the `WWEWS_Cluster` object.

When this parameter is set at `WWEWS_Cluster` object, the recording condition applies to all agents in the environment. You can create the `recordingWhen` parameter in a `screen-recording-client` section of each agent object to override the settings at the environment level.

The parameter value is an expression of conditions to enable screen recording for each agent. The format is:

- For Non-voice agents: `recordingWhen=condition1,condition2,...` where `condition1`, `condition2`, etc. are a set of conditions that must all be true in order for the screen recording to be taking place.
- For Voice agents: Screen recording starts when `recordingWhen` is not set to off and the voice recording starts.

The following condition values are supported:

| Condition | Description |
|-------------------|---|
| off | A special case. Cannot appear with other conditions. When specified as such, screen recording never occurs for the agent. |
| loggedin | When the agent is logged in |
| DNDoff | When agent sets DND (do not disturb) to off |
| ready(any) | True when any media type is set to ready, or <code>list(ready media).count != 0</code> |
| ready(abc) | True when the abc media type is set to ready |
| ready(abc,...xyz) | A list of media types that are set to ready. Note that <code>ready(abc,...xyz) = ready(abc) ... ready(xyz)</code> . |
| random_voice(%) | Records the agent's screens based on a percentage (%) of the total voice call volume for that agent. |

2. For voice deployments, set up the maximum screen recording duration based on the quality preset in the screen recording client configuration. (see, [Configuring the Screen Recording Client](#) for more information about these parameters).

Depending on the `qualityPreset` value, set the screen recording duration as follows:

- If `qualityPreset` is Low— set `maxDurationMinutes` to 180.
- If `qualityPreset` is Standard—set `maxDurationMinutes` to 120.
- If `qualityPreset` is High—set `maxDurationMinutes` to 75.

Configure the Screen Recording Client

Configuring the Screen Recording Client

For information about configuring the Screen Recording Client, see [Deploying the Screen Recording Client](#).