Web Services and Applications Deployment Guide

Call Recording

4/6/2026

Call Recording

Contents

You can configure Workspace Web Edition & Web Services to store and retrieve call recordings from Genesys Interaction Recording—Voice Edition. These call recordings can also be accessed and played back through the Call Recording API.

To enable this functionality, complete the following steps:

1. Set up external storage.
2. Set up the external storage credentials.
3. The call recording feature in Workspace Web Edition & Web Services uses Elasticsearch as the query engine. To set up the query engine, see the Elasticsearch documentation.
4. Configure call recording.
5. Enable the following features on each Workspace Web Edition & Web Services node in your solution.
   - `api-voice-recording` — Controls whether an agent can initiate call recording through the API.
   - `api-supervisor-recording` — Controls whether you can access call recording through the API.

     See Feature Configuration for details.

Setting Up External Storage

Workspace Web Edition & Web Services uses Web Distributed Authoring and Versioning (WebDav) to store call recordings. WebDAV allows remote access to local folders through an HTTP-based web browser. The steps below provide a quick guide to setting up an HTTP-based file server using the Apache2 web server, which has a built-in WebDAV module.

Prerequisites

- You have installed JDK 1.7.

Start of Procedure

1. Install the Apache2 web server with the following command: sudo apt-get install apache2
2. Enable HTTPS by completing the following steps:
   a. Enable the `mod_ssl` module with the following command:

      ```
      sudo a2enmod ssl
      ```

   b. In order for Apache2 to provide HTTPS, a certificate and key file are also needed for your site. If you are using a site other than `default-ssl`, change the command accordingly:

      ```
      sudo a2ensite default-ssl
      ```

   c. Generate your own certificate file:

      ```
      sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/
      apache.key -out /etc/apache2/ssl/apache.crt
      ```

   d. Update `/etc/apache2/site-available/default-ssl`:

```
SSLEngine on
SSLCertificateFile /etc/apache2/ssl/apache.crt
SSLCertificateKeyFile /etc/apache2/ssl/apache.key
```

3. Restart the Apache2 service to enable the new settings:

   ```
   sudo /etc/init.d/apache2 restart
   ```

4. Open your firewall to the incoming default HTTP and HTTPS ports (80 and 443). It is also possible to use custom ports by changing the allowed incoming ports in the firewall, the virtual host configuration file, and the URL used to reach the WebDAV server.

5. Enable the Apache2 WebDAV modules:

   ```
   sudo a2enmod dav_fs
   ```

6. Restart the Apache2 service:

   ```
   sudo /etc/init.d/apache2 restart
   ```

7. Create a directory for WebDAV in the `/var/www` folder:

   ```
   sudo mkdir /var/webdav
   ```

8. Create a sub-directory for files:

   ```
   mkdir /var/webdav/files
   ```

9. Create WebDAV authentication users:

   a. For call recording, HTTP Basic Authentication is used on top of HTTPS. Enter the following command:

      ```
      sudo htpasswd -c /var/webdav/passwd.dav user1
      ```

   b. Type a password for the user `testuser`.

   c. Repeat for as many users as needed:

      ```
      sudo htpasswd /var/webdav/passwd.dav user2
      ```

10. Update the file and folder permission. The WebDAV folder should be accessible by Apache, so you need to change folder owner to `www-data` (or a user defined by your apache2 settings):

    ```
    sudo chown -R www-data:www-data /var/webdav
    ```

11. Edit the virtual host file:

    a. Edit the Apache default virtual host (`vhost`) file used for the URL through which WebDAV will be accessed:

       ```
       sudo vi /etc/apache2/sites-available/default
       ```

    b. If you are using HTTPS, change the site to `default-ssl` or your site name:

       ```
       sudo vi /etc/apache2/sites-available/default-ssl
       ```

    c. Add the following section:

       ```
       Alias /webdav /var/webdav/files
           <Directory /var/webdav/>
               Options Indexes MultiViews
               AllowOverride None
               Order allow,deny
       ```

```
        allow from all
    </Directory>
    <Location /webdav>
        DAV On
        AuthType Basic
        AuthName "user1"
        AuthUserFile /var/webdav/passwd.dav
        Require valid-user
    </Location>
```

d. Restart the Apache2 service to enable the new settings:

```
sudo /etc/init.d/apache2 restart
```

12. Test the WebDAV configuration:

a. Install cadaver, a command-line WebDAV client:

```
sudo apt-get install cadaver
```

b. Test WebDAV:

```
cadaver http://localhost/webdav/
```

c. You should be prompted for a user name. Type in `testuser` and then the password for `testuser`. If you are granted access, then WebDAV is working.

d. Exit the WebDAV shell:

```
quit
```

The sequence of commands to test WebDav should be as follows:

```
server1:~# cadaver http://localhost/webdav/
Authentication required for test on server `localhost':
Username: ''user1''
Password: *******
dav:/webdav /> quit
Connection to `localhost' closed.
server1:~#
```

13. If you are using HTTPS, add the server certificate to the Workspace Web Edition & Web Services keystore:

a. Copy `apache.crt` to the Workspace Web Edition & Web Services host:

```
scp /etc/apache2/ssl/apache.crt ubuntu@10.10.15.89:~/
```

b. Install the WebDAV server certificate to the Workspace Web Edition & Web Services JVM:

```
cd $JAVA_HOME/jre/lib/security
../../bin/keytool -import -alias webdav -file ~/apache.crt -keystore cacerts
```

c. Turn off `SNIExtension` by updating `/etc/default/jetty`:

```
JAVA_OPTIONS="... -Djsse.enableSNIExtension=false"
```

Note: In the command above, "..." represents other Java options that may be present in your Jetty config file.

d. Restart Jetty on the Workspace Web Edition & Web Services node:

```
sudo service jetty restart
```

End of Procedure

Configuring Call Recording

Start of Procedure

1. Open the `$JETTY_HOME/genconfig/server-settings.yaml` file.
2. Review the Call Recording configuration options. The following options are mandatory to enable call recording:

Option	Value
createCallRecordingCF	Set to `true` to enable Call Recording.
crClusterName	If you are using Elasticsearch, set this option to the value of the `cluster.name` property in the `elasticsearch.yml` file. For details, see the Elasticsearch documtation.
crRegion	Set to the name of the region where the Workspace Web Edition & Web Services resides. See Region Affinity for details.
cryptoSecurityKey	Set to the security key used for Workspace Web Edition & Web Services encryption.
webDAVMaxConnection	Set to the maximum number of TCP connections per route of WebDav storage.
webDAVMaxTotalConnection	Set to the maximum number of TCP connections from the Workspace Web Edition & Web Services node to all WebDav storage.

3. Save your changes and close the file.

End of Procedure