DOJ CAPSS Bulk Upload API

Overview

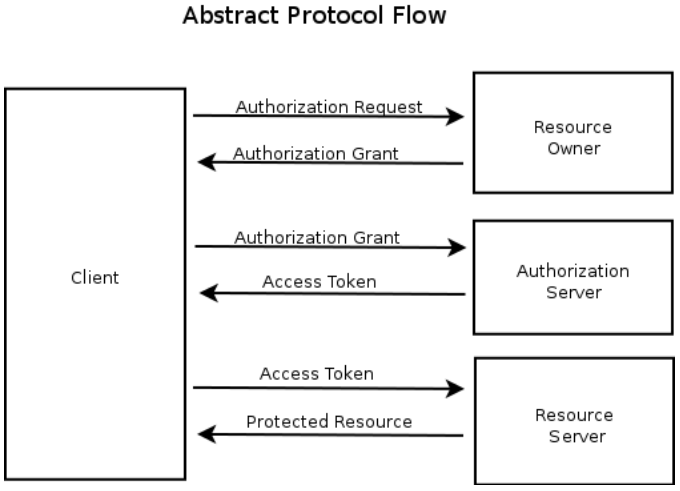
The CAPSS system has expanded the ability to upload an XML file containing multiple Property Transactions via a JSON web service. This is an optional service to help with automating the upload process for those interested and is not mandatory. The existing web based upload bulk import and online form will still be available.

Uploading Property Transactions requires an account for the user to be established. Uploading transactions require limited access to the CAPSS system, which can be controlled by the account admin. Third party clients are registered for an account by the CAPSS admin. An authorized client will request an access token prior to interacting with the system. The token is used as credentials to upload and check status of Property Transactions.

OAuth2 provides a mechanism for resource owners to delegate secure access to resources for third-party client applications. OAuth2 is an open standard and thoroughly documented. OAuth2 manages client registration, token generation, and resource authentication.

Steps to utilize CAPSS is as follows:

1. CAPSS User registers third-party client.
2. Client requests an access token.
3. Client interacts with CAPSS utilizing token.



OAuth2

The primary resource for OAuth2 documentation is the OAuth2 Specification: The OAuth 2.0 Authorization Framework. CAPSS only implemented a subset of the specification needed to provide basic CAPSS requirements. Additional features may be added as required.

Registration

Clients are registered in the CAPSS system by the CAPSS owner. Owners will grant clients access to the system in one of several methods. OAuth2 implements 4 methods to grant access to resources. Each method provides a different mechanism that is useful in different context. Currently CAPSS supports the following grants

1. Authorization Grants
2. Client Credentials

Authorization Grant provides a manual means to acquire grant access between the client web application and the CAPSS application. This model requires human interaction via the CAPSS authorized user. The Authorization Grant provides a seamless secured HTTPS method to grant clients access to specific resources. Third-Party clients requiring access to protected resources will negotiate a handshake with CAPSS via a web UI, which is driven by the CAPSS owner.

The process starts when the CAPSS owner registers the owner in CAPSS Application with a special client URL. The CAPSS owner will then visit the client web application to begin the grant process. The web application will redirect to CAPSS Application via a specific OAuth2 HTTP endpoint and the CAPSS user is presented a CAPSS login page to complete the grant authorization. The CAPSS Application will redirect back to the client application and return an Authorization Code embedded in the URL as a parameter. This completes the role of the CAPSS Owner in the registration process. The client application will capture the authorization code and use it to retrieve an access token. The authorization code expires after a short duration and can only be used once. This provides additional security.

Client Credentials grant is used for machine-to-machine interfaces and is expected to be the preferred method by most clients. The CAPSS owner registers the client in CAPSS. A client id and client secret (username and password) is given to the third party clients. The client sends an http request to CAPSS with credentials and a response is returned with the token. The token is used in subsequent requests to access CAPSS resources (upload and status endpoints).

Token

Access tokens are used to access resources shared by the resource owner (CAPSS authorized user). The tokens expire after a preset time, at which time a new token is granted.

The Clients will request tokens when they expire via specific endpoints. The end point will return the token in a JSON response that also contains additional information. The response contains the time to live for the token. If a token is requested before it has expired, the same token will be generated, which will include the remaining time to live information. Only one token is active at a time.

Resources

The resources are protected URI's within CAPSS. The CAPSS system allows registered clients limited access. Currently clients can Upload Property Transactions and Check the status of an Upload. The resources are available as web services and require credentials in the form of OAuth2 tokens.

Upload & Status

Property Transactions are uploaded via an XML document. URL Parameters are used to dictate how processing should be accomplished in the case of errors or duplicate transactions.

A limited check is performed during upload and the response will return the status of the upload. A successful upload will contain the submission id used to identify the upload along with the URL for checking the status. Errors will contain the errors encountered.

A status check URL is provided to identify if uploaded transaction were successfully processed into CAPSS. HTTP status codes will identify if the transactions are being processed or are complete. If the processing code is presented, the application will try again after a period of time until the complete status code is returned, or until a timeout is reached in the case of an application error. When successful, the response will contain the status code and the URL to resubmit. Uploads with errors will additionally provide a list of errors for transactions.

The upload status response contains a list of errors for each store if present. To facilitate automated submissions, error handling is provided via a duplicate and error parameter that defines the actions to take under those conditions. Please see documentation for details.

The nature of web services is that it allows the client to be implemented in any manner the client deems appropriate. Requests can be handcrafted with tools such as curl or with browser plug-ins (Postman and RESTClient), which can facilitate the testing process. However, a more automated process is expected to be implemented.

The requests and responses are implemented with JSON web services and utilize HATEOAS to provide additional URLs to the client to keep the API flexible. HATEOAS is a architectural style that presents the user with valid urls for subsequent requests. When the user submits a valid Bulk Upload, the response will provide the link to view the status of that file. When checking the status of a upload, the response will continue to contain the link of the status while it is being processed. Once completed, the save link will be presented.

Examples

Authorization Code Grant

Request grant by redirecting to url. Response will redirect back to the URL the CAPSS Admin registered the client with and will contain the authorization code. The code will be used to request a token.

Client HTTP Request

```
http://capss.doj.ca.gov/oauth/authorize.dispatch?response_type
=code&client_id=clientCapssId&client_secret=clientSecretPasswo
rd &scope=api
```

CAPSS response

```
http:// <REGISTERD-CAPSS-REDIRECRT-URL>/auth?code=iNCCnA
```

Token Request

```
curl -XPOST  -d "client_id=clientCapssId" -
d "client_secret=clientSecretPassword"   -
d "grant_type=authorization_code"  -
d "code=iNCCnA" http://capss.doj.ca.gov /oauth/token
```

Sample Response

```
{
    "access_token": "ffe735e4-ca79-4684-8d85-427474660b8d",
    "token_type": "bearer",
    "refresh_token": "09f94e8b-bb4c-4a02-9059-196769d6ceed",
    "expires_in": 43199,
    "scope": "read"
}
```

Client Credentials Grant

Request Grant by using credentials to retrieve a token. The CAPSS admin provides the user with credentials that are supplied for a token.

Client Request

```
curl -X POST -u clientCapssId:clientSecretPassword -
d "scope=api" -
d "grant_type=client_credentials" http://capss.doj.ca.gov/oaut
h/token
```

CAPSS Response

```
{
    "access_token":"68452eb6-f551-49d0-829c-1933a7435cd5",
    "token_type":"bearer",
    "expires_in":3599,
    "scope":"read"
}
```

Bulk Upload

The bulk upload process uploads a file containing Property Transaction files. The CAPSS application provides a “save” resource to submit bulk uploads to. The response contains the URL to check the status.

Client Request

```
curl -i -XPOST -H "Authorization: Bearer 68452eb6-f551-49d0-
829c-1933a7435cd5" -F "bulkUploadFile=@/Users/somplace-on-
client-file-
system/testuser/PropertyTransaction.xml" http://capss.doj.ca.g
ov/api/bulkupload/save
```

CAPSS Response

HTTP Status code 202

{"licenseNumber":"XXXXX000102","status":"new","submission":{"submissionId":"9dce766f-32f9-4243-b3a7-075e5bf59dd1"},"links":{"href":"http://capss.doj.ca.gov/api/bulkupload/show/4275","rel":"show"}}

Bulk Upload Status Check

The status of the Upload can be checked by requesting the show resource endpoint with the given id for the upload. The URL should not be stored and created by the client as it is possible for it to change over time. The responses provides the URLs to navigate to get the status and should be retrieved from the links property in the response.

Client Request

curl -i -XGET -H "Authorization: Bearer `68452eb6-f551-49d0-829c-1933a7435cd5`" http://capss.doj.ca.gov/api/bulkupload/show/4275

CAPSS Response

HTTP Status Code 200

{"licenseNumber":"XXXXX000102","status":"complete","stores":[{"errors":[],"licenseNumber":"xxxxx100","status":"complete","statusMessage":"Successfully uploaded file. File `PropertyTransaction`.xml uploaded 1 record(s) at Mon Nov 21 11:20:43 PST 2016"}],"links":{"href":"http:// capss.doj.ca.gov /api/bulkupload/save","rel":"new"}}

URL End Points

CAPSS URL	Description	Response	Method
`oauth/authorize.dispatch`	OAuth2 URL Authorization Code grant to request access	Redirect back to client application with a single use code.	POST
`oauth/token`	OAuth2 Token Request. Used to get a new token from Client Credentials.	A JSON object containing the Token.	POST
`api/bulkupload/save`	CAPSS endpoint for submitting Bulk Uploads	A JSON response representing the result of the upload. Can contain errors, and	POST

		the link to the status check url if successfully processing.	

Request Parameters

Parameters	Where Used	Values	Notes
`response_type`	OAuth2 Grant/Token requests	code	Only used for Authorization Grants during initial request.
`grant_type`	OAuth2 Grant/Token requests	`authorization_code` `client_credentials`	One or the other is used during code grants
client_id	OAuth2 Grant/Token requests	Client Username	The username supplied via CAPSS authorized user
client_secret	OAuth2 Grant/Token requests	Client password	The password supplied via CAPSS authorized user
scope	OAuth2 Grant/Token requests	api	Used to identify what resources the client can access.
code	OAuth2 Grant/Token requests	String response	Used during Authorization Code grants. A response code that is provided back to the client during a redirect. The client software will save this code to redeem for a token.
onDup	CAPSS BulkUpload Submission	cancel submitDups submitWithoutDup	The action to take when encountering dups in a transaction
onError	CAPSS BulkUpload Submission	cancel submit	The action to take when encountering errors in a transaction

Status Codes

Codes	Bulk Upload Save	Bulk Upload Status
200 OK	N/A	Request complete successfully. Processing is complete
202 Accepted	Bulk Import was accepted for processing	Bulk Import was accepted for processing. Processing is still in progress

400 Bad Request	A problem with the request. Check parameters and file being uploads	N/A
404 Not Found	N/A	Requested Bulk Import not in system
500 Internal Server Error	Error submitting file.	Error Processing file.

Glossary of Terms

Below are some terms used in this document and OAUTH2 spec as they apply to CAPSS. These definitions are summaries, more detailed and abstract explanations can be found in the OAuth2 spec.

Access Token A code representing user credentials used to access protected resources.

Authorization Code A code that is used ONLY during the Authorization Grant processes during the handshaking of web applications.

Authorization Server: The server that controls OAuth2 token management and client registration.

Bulk Upload An abstraction resource representing the uploaded file containing Property Transactions.

Client: The third-party granted access from the Resource Owner. The client may be a third-party organization submitting on behalf of the Resource Owner, or may be an application the Resource Owner uses to upload transactions to system.

Curl a tool/libarary for transferring data via HTTP and various other protocols.

Grant The OAuth2 mechanism for giving (granting) authorization to a third party client.

Grant Process The set of 4 methods defined by OAuth2 to grant authorization to a third party.

HATEOAS (Hypermedia as the Engine of Application State) A constraint of the REST application architecture. A hypermedia-driven site provides information to navigate the site's REST interfaces dynamically by including hypermedia links with the responses

OAUTH2 A protocol for providing specific authorization flows for web-applications. Used in CAPSS to delegate authorization to third party clients for uploading transactions

Resource A key abstraction of information that can be a document or image, a service, an object, or a collection of other resources. Resources are exposed as HTTP endpoints and comprise of the Bulk Upload in CAPSS

Resource Owner: The CAPSS User with permissions to grant third party applications access to system via OAuth2.

Resource Server: The CAPSS server containing the delegated resource. Includes the endpoints used to upload and check the status of an upload.

ReST (Representation State Transfer) A stateless communication protocol implemented over HTTPS for the CAPSS Application.

Status Codes Meta-information about the status of an HTTP request.