AccessControl Web Service Design

Version 1.0

# Description

AccessControl is Auxiliary Web Service to trace user sessions and resolve authorization queries within Blueprint services. AccessControl is the internal part of enterprise solution infrastructure and service endpoint is not visible to client web application.

# Scope

AccessControl is limited to persisting and providing files or any other large binary or textual data streams represented via file. AccessControl Web Service should replace FILESTREAM as persistence mechanism for file attachments. The following design principles are used to limit the scope of the AccessControl Web Service for the current version:

1. Service allows for upload / download single file per call.
2. URI of the file uniquely identifies the file within Blueprint Web Application.
3. IIS service supports DELETE HTTP method, alternatively X-HTTP-Method-Override header to be used in conjunction with POST method.
4. Service will not allow updates to enforce new GUID for each unique content. If update functionality will be implemented on the front end, it will use DELETE and then POST. It will prevent the issue with caching the older version of the file content.
5. Service will store files no larger than 16MB in size.

# Interface

## Endpoint

Service will be hosted in the path /svc/accesscontrol

All methods expect to receive header Token to identify user session. Token is used to authorize user for an action being requested.

## Methods

HEAD /files/{id}  
- where {id} is string containing 32 alphanumerical characters of unique identifier (GUID) of the file information to retrieve

Method for downloading file information (FileId, StoredDate, FileName, ContentType, file size).

Returns file details.

Returns status **200 OK** if no issue is detected.  
Returns status **401 Unauthorized** if session cannot be found or user is not permitted the action requested.  
Returns status **403 Bad Request** if GUID is unrecognized.  
Returns status **406 Not Acceptable** if Token is missing or malformed.  
Returns status **404 Not Found** if file is not found.  
Returns status **500 Internal Server Error** if error:  
- database connection failed;  
- database connection established but table Files not found.

Example: HEAD /svc/AccessControl/files/ee40d62d883d4eecb095f78883b69d63

GET /files/{id}  
- where {id} is string containing 32 alphanumerical characters of unique identifier (GUID) of the file to retrieve

Method for downloading file or file information.

Returns file stream.

Returns status **200 OK** if no issue is detected.  
Returns status **401 Unauthorized** if session cannot be found or user is not permitted the action requested.  
Returns status **403 Bad Request** if GUID is unrecognized  
Returns status **406 Not Acceptable** if Token is missing or malformed.  
Returns status **404 Not Found** if file is not found.  
Returns status **500 Internal Server Error** if error:  
- database connection failed;  
- database connection established but table Files not found.

Example: GET /svc/AccessControl/files/ee40d62d883d4eecb095f78883b69d63

### POST /files

Method for uploading file into the application.

Returns string containing 32 alphanumerical characters of unique identifier (GUID) of the posted file.

Returns status **200 OK** if no issue is detected.  
Returns status **401 Unauthorized** if session cannot be found or user is not permitted the action requested.  
Returns status **406 Not Acceptable** if Token is missing or malformed.  
Returns status **500 Internal Server Error** if error:  
- database connection failed;  
- database connection established but table Files not found.

DELETE /files/{id}  
- where {id} is string containing 32 alphanumerical characters of unique identifier (GUID) of the file to delete

Method for removal of previously uploaded file.

Returns string containing 32 alphanumerical characters of unique identifier (GUID) of the deleted file.

Returns status **200 OK** if no issue is detected.  
Returns status **401 Unauthorized** if session cannot be found or user is not permitted the action requested.  
Returns status **403 Bad Request** if GUID is unrecognized  
Returns status **406 Not Acceptable** if Token is missing or malformed.  
Returns status **404 Not Found** if file is not found.  
Returns status **500 Internal Server Error** if error:  
- database connection failed;  
- database connection established but table Files not found.

Example: DELETE /svc/AccessControl/files/ee40d62d883d4eecb095f78883b69d63

GET /status  
Method to return current status of AccessControl Web Service.

Returns status **200 OK** if no issue is detected.  
Returns status **401 Unauthorized** if session cannot be found or user is not permitted the action requested.  
Returns status **406 Not Acceptable** if Token is missing or malformed.  
Returns status **500 Internal Server Error** if error:  
- database connection failed;  
- database connection established but table Files not found.

# Technology

AccessControl Web Service will be implemented using ASP.NET Web API/C#. Database will be Microsoft SQL Server 2012.

# Behavior

## Methods

HEAD /files/{id}  
Method checks if database table contains the record identified by id provided as a parameter. If record is found then file record (Id, Stored, Name, ContentType) is returned as an object. If record is not found then attempt is made to retrieve FILESTREAM information from legacy file storage. Return value is cached.

GET /files/{id}  
Method checks if database table contains the record identified by id provided as a parameter. If record is found then file is returned as file stream. If record is not found then attempt is made to retrieve FILESTREAM from legacy file storage. Return value is cached.

### POST /files

Method creates new database table record using file stream provided as a parameter. File identifier is generated in the database using NEWSEQUENTIALID() and returned as a 32 alphanumerical character string. File name is passed as parameter / header and content type is taken from header.

DELETE /files/{id}  
Method checks if database table contains the record identified by id provided as a parameter. If record is found then the record is deleted asynchronously. Otherwise asynchronous attempt is made to delete the FILESTREAM from legacy file storage. Returns file identifier as it was supplied to allow for piping on the client side.

GET /status  
Method tries to execute SELECT COUNT(\*) FROM [FILES]; to test database connection.

# Storage

Records to be stored in AccessControl.Files (database AccessControl, table Files)

## Columns

FileId : uniqueidentifier, PK, default = NEWSEQUENTIALID()  
StoredTime : datetime  
FileName : varchar(256)  
FileType : varchar(64)  
FileContent : varbinary(max)