aws

API Reference

Digital Evidence Archive on AWS

Digital Evidence Archive on AWS: API Reference

Table of Contents

What Is Digital Evidence Archive on AWS?

Digital Evidence Archive on AWS (DEA) is a solution that enables investigative units to store and manage digital evidence through Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB. DEA provides a web user interface (UI) that investigators and other law enforcement personnel can use to create and update cases and associated digital evidence. DEA uses Amazon S3 Intelligent-Tiering to dynamically change the storage class used for digital evidence based on how often users access them, which reduces costs incurred when using DEA.

With DEA, law enforcement customers can optimize their total cost of ownership by reducing management of multiple storage repositories, reliance on physical devices such as USBs and hard drives, and operational costs associated with running a local data center.

DEA maintains file integrity, hashing, encryption, and audit logging to help customers meet requirements of the Criminal Justice Information Services (CJIS) Security Policy. There are no additional charges or upfront commitments required to use DEA. You only pay for AWS services used in your DEA deployment, such as Amazon Simple Storage Service pricing. DEA integrates with your external identity provider, allowing agencies to use their existing single sign-on (SSO) configuration. This solution can also support non-standard AWS partitions, including the AWS GovCloud (US) Regions.

Resources

The Digital Evidence Archive on AWS REST API includes the following resources.

Topics

- Auth – Login URL
- Auth – Logout URL
- Auth – Refresh token
- Auth – Revoke token
- Auth – Token
- Available endpoints
- Cases – Audit by caseId
- Cases – Available actions by caseId
- Cases – Case details by caseId
- Cases – Case file info
- Cases – Case owner
- Cases – Create case
- Cases – CSV audit entry for a case
- Cases – CSV audit entry for a case file
- Cases – File audit by caseId and fileId
- Cases – File contents
- Cases – Files by caseId
- Cases – List all cases
- Cases – Manage user memberships
- Cases – My cases
- Cases – Restore files
- Cases – Retrieve user memberships
- Cases – Scoped information
- Cases – Status
- Data vaults
- Data vaults – Audit

Auth – Login URL

When a user attempts to access DEA, the application redirects the user to the authorization login URL to authenticate. After successful authentication, the user receives an authorization token to access DEA's resources.

URI

`/auth/loginUrl`

HTTP methods

GET

Operation ID: `loginUrl`

Retrieves the login URL.

Query parameters

Name	Type	Required	Description
callbackUrl	String	True	callback URL for Hosted UI

Responses

Status code	Response model	Description
200	getLoginUrlResponse	Login URL for DEA

Schemas

Response bodies

getLoginUrlResponse schema

```
{
  "loginUrl": "string"
}
```

Properties

getLoginUrlResponse

Returns the login URL.

loginUrl

The URL to login to the DEA UI.

  Type: string
  Required: False

Auth – Logout URL

The authorization logout URL initiates the logout process for a user. Implementing an authorization logout URL ensures when a user is done accessing the system, their session is properly closed, reducing the risk of unauthorized access if someone gains access to their device.

URI

`/auth/logoutUrl`

HTTP methods

GET

Operation ID: `logoutUrl`

Get logout URL

Query parameters

Name	Type	Required	Description
`callbackUrl`	String	True	callback URL for Hosted UI

Responses

Status code	Response model	Description
200	[getLogoutUrlResponse](#)	Logout URL for DEA

Schemas

Response bodies

getLogoutUrlResponse schema

```
{
  "logoutUrl": "string"
```

```
    }
```

Properties

getLogoutUrlResponse

Returns the logout URL.

logoutUrl

The URL to logout.

> **Type**: string
> **Required**: False

Auth – Refresh token

Refresh tokens improve user experience by allowing the user to stay logged in for longer periods without having to frequently re-authenticate. It also enhances security by minimizing exposure of the user's credentials. When a user logs in, they receive both an access token and a refresh token. The refresh token obtains a new access token from the refresh endpoint when the current access token expires. If the refresh token is valid, the refresh endpoint returns a new access token.

URI

`/auth/refreshToken`

HTTP methods

POST

Operation ID: `refreshToken`

Responses

Status code	Response model	Description
200	[getTokenResult](#)	Id Token and Cognito information for fetching credentials

Schemas

Response bodies

getTokenResult schema

```
{
  "idToken": "string",
  "identityPoolId": "string",
  "userPoolId": "string",
  "expiresIn": number
}
```

Properties

getTokenResult

idToken

   Type: string

   Required: True

identityPoolId

   Type: string

   Required: True

userPoolId

   Type: string

   Required: True

expiresIn

   Type: number

   Required: True

Auth – Revoke token

Using a revocation token adds an extra layer of security and control for users. The revocation token, once validated, invalidates the corresponding access or refresh token to revoke access from DEA.

URI

`/auth/revokeToken`

HTTP methods

POST

Operation ID: `revokeToken`

Responses

Status code	Response model	Description
200	None	Successfully Revoked Token

Auth – Token

The authorization code token secures access to DEA by ensuring that only authorized users can access its resources. When a user or application wants to access DEA, they first authenticate themselves by providing their credentials. After successful authentication, the application requests an authorization code token from the API. This token acts as proof that the user has been authenticated and is authorized to access DEA. This token is a string of characters unique to the requester and has a limited lifespan. After the token expires, the user or application must authenticate again to obtain a new token.

URI

`/auth/`*`authCode`*`/token`

HTTP methods

POST

Operation ID: `getToken`

Path parameters

Name	Type	Required	Description
authCode	String	True	Auth code to trade for ID Token

Header parameters

Name	Type	Required	Description
`callback-override`	String	False	Callback url for oauth2/token. Override default callback url
`origin`	String	False	Override for origin URL

Responses

Status code	Response model	Description
200	[getTokenResult](#)	Id Token and Cognito information for fetching credentials

Schemas

Request bodies

POST schema

```
{
  "codeVerifier": "string"
}
```

Response bodies

getTokenResult schema

```
{
  "idToken": "string",
  "identityPoolId": "string",
  "userPoolId": "string",
  "expiresIn": number
}
```

Properties

codeVerifier

codeVerifier

  Type: string
  Required: False

getTokenResult

idToken

  Type: string
  Required: True

identityPoolId

  Type: string
  Required: True

userPoolId

    Type: string
    Required: True

expiresIn

    Type: number
    Required: True

Available endpoints

Available endpoints lists various endpoints used to interact with DEA.

URI

`/availableEndpoints`

HTTP methods

GET

Responses

Status code	Response model	Description
200	availableEndpoints Response	Success Response

Schemas

Response bodies

availableEndpointsResponse schema

```
{
  "endpoints": [
```

```
      "string"
   ]
}
```

Properties

availableEndpointsResponse

endpoints

> **Type**: Array of type string
> **Required**: False

Cases – Audit by caseId

This endpoint provides visibility into the history of actions performed on a specific case within DEA. The audit trail provided by this endpoint is crucial for security and compliance purposes, as it provides a record of who accessed the case and what actions were taken.

URI

/cases/*caseId*/audit

HTTP methods

POST

Path parameters

Name	Type	Required	Description
caseId	String	True	

Responses

Status code	Response model	Description
200	[Cases_response_200_6](#)	Audit Query ID

Schemas

Request bodies

POST schema

```
{
  "from": number,
  "to": number
}
```

Response bodies

Cases_response_200_6 schema

```
{
  "auditId": "string"
}
```

Properties

AuditPayload

from

   Type: number
   Required: False

to

   Type: number
   Required: False

Cases_response_200_6

auditId

   Type: string
   Required: False

Cases – Available actions by caseId

Requests to the /cases/{caseId}/actions endpoint returns a list of actions that can be performed on the specified case based on the permissions of the requesting user.

URI

/cases/*caseId*/actions

HTTP methods

GET

Get user for case and their available actions

Path parameters

Name	Type	Required	Description
caseId	String	True	

Responses

Status code	Response model	Description
200	CaseUser	Success

Schemas

Response bodies

CaseUser schema

```
{
  "userUlid": "string",
  "caseUlid": "string",
  "actions": [
    enum
```

```
    ],
    "caseName": "string",
    "userFirstName": "string",
    "userLastName": "string",
    "created": "string",
    "updated": "string"
}
```

Properties

CaseAction

```
VIEW_CASE_DETAILS
UPDATE_CASE_DETAILS
UPDATE_CASE_STATUS
UPLOAD
DOWNLOAD
VIEW_FILES
CASE_AUDIT
INVITE
RESTORE_FILES
```

CaseUser

userUlid

Type: string
Required: False

caseUlid

Type: string
Required: False

actions

Type: Array of type CaseAction
Required: False

caseName

    Type: string
    Required: False

userFirstName

    Type: string
    Required: False

userLastName

    Type: string
    Required: False

created

    Type: string
    Required: False

updated

    Type: string
    Required: False

Cases – Case details by caseId

This endpoint provides a way to retrieve detailed information about a specific case within Digital Evidence Archive, facilitating better management and understanding of the case. This information includes the case name, description, creation date, status, and any other relevant metadata. The API requires authentication and authorization to ensure that only authorized users can retrieve the details of the case.

URI

`/cases/`*`caseId`*`/details`

HTTP methods

GET

Get metadata for a specific case. return not found if user doesn't have access

Path parameters

Name	Type	Required	Description
caseId	String	True	

Responses

Status code	Response model	Description
200	Case	Success

PUT

Path parameters

Name	Type	Required	Description
caseId	String	True	

Responses

Status code	Response model	Description
200	Case	Success

DELETE

Path parameters

Name	Type	Required	Description
caseId	String	True	

Responses

Status code	Response model	Description
200	None	Success

Schemas

Request bodies

PUT schema

```
{
  "ulid": "string",
  "name": "string",
  "description": "string"
}
```

Response bodies

Case schema

```
{
  "ulid": "string",
  "name": "string",
  "status": enum,
  "description": "string",
  "objectCount": number,
  "totalSizeBytes": number,
  "fileStatus": enum,
  "s3BatchJobId": "string",
```

```
    "created": "string",
    "updated": "string"
}
```

Properties

Case

ulid

   Type: string

   Required: False

name

   Type: string

   Required: False

status

   Type: CaseStatus

   Required: False

description

   Type: string

   Required: False

objectCount

   Type: number

   Required: False

totalSizeBytes

   Type: number

   Required: False

fileStatus

   Type: CaseFileStatus

   Required: False

s3BatchJobId

   Type: string

   Required: False

created

   Type: string

   Required: False

updated

   Type: string

   Required: False

CaseFileStatus

```
ACTIVE
DELETING
DELETE_FAILED
DELETED
PENDING
```

CaseStatus

```
ACTIVE
INACTIVE
```

CaseUpdateRequest

ulid

> **Type**: string
> **Required**: True

name

> **Type**: string
> **Required**: True

description

> **Type**: string
> **Required**: False

Cases – Case file info

This endpoint provides a way to retrieve detailed information about a specific file within a case in DEA, facilitating better management and understanding of the file. The API requires authentication and authorization to ensure that only authorized users can retrieve the details of the file.

URI

/cases/*caseId*/files/*fileId*/info

HTTP methods

GET

Get details for a file within a case.

Path parameters

Name	Type	Required	Description
caseId	String	True	

Name	Type	Required	Description
fileId	String	True	

Responses

Status code	Response model	Description
200	CaseFile	Success Response

Schemas

Response bodies

CaseFile schema

```
{
  "fileName": "string",
  "filePath": "string",
  "caseUlid": "string",
  "contentType": "string",
  "createdBy": "string",
  "fileSizeBytes": number,
  "sha256Hash": "string",
  "ulid": "string",
  "status": enum,
  "uploadId": "string",
  "isFile": boolean,
  "created": "string",
  "updated": "string",
  "details": "string",
  "fileS3Key": "string",
  "dataVaultUlid": "string",
  "executionId": "string",
  "associationCreatedby": "string",
  "associationDate": "string",
  "dataVaultUploadDate": "string",
  "dataVaultName": "string",
  "reason": "string"
}
```

Properties

CaseFile

fileName

Type: string
Required: False

filePath

Type: string
Required: False

caseUlid

Type: string
Required: False

contentType

Type: string
Required: False

createdBy

Type: string
Required: False

fileSizeBytes

Type: number
Required: False

sha256Hash

Type: string

Required: False

ulid

Type: string

Required: False

status

Type: CaseFileStatus

Required: False

uploadId

Type: string

Required: False

isFile

Type: boolean

Required: False

created

Type: string

Required: False

updated

Type: string

Required: False

details

Type: string

Required: False

fileS3Key

Type: string
Required: False

dataVaultUlid

Type: string
Required: False

executionId

Type: string
Required: False

associationCreatedby

Type: string
Required: False

associationDate

Type: string
Required: False

dataVaultUploadDate

Type: string
Required: False

dataVaultName

Type: string
Required: False

reason

>   **Type**: string
>   **Required**: False

CaseFileStatus

>   ACTIVE
>   DELETING
>   DELETE_FAILED
>   DELETED
>   PENDING

Cases – Case owner

This elevated permissions endpoint provides a way to update the owner of a case in DEA, facilitating ownership management and access control.

URI

/cases/*caseId*/owner

HTTP methods

POST

Admin-only set new owner of a case

Path parameters

Name	Type	Required	Description
caseId	String	True	

Responses

Status code	Response model	Description
200	CaseUser	Case owner set successfully

Schemas

Request bodies

POST schema

```
{
  "userId": "string",
  "caseId": "string"
}
```

Response bodies

CaseUser schema

```
{
  "userUlid": "string",
  "caseUlid": "string",
  "actions": [
    enum
  ],
  "caseName": "string",
  "userFirstName": "string",
  "userLastName": "string",
  "created": "string",
  "updated": "string"
}
```

Properties

CaseAction

```
VIEW_CASE_DETAILS
UPDATE_CASE_DETAILS
UPDATE_CASE_STATUS
UPLOAD
DOWNLOAD
VIEW_FILES
CASE_AUDIT
INVITE
```

RESTORE_FILES

CaseUser

userUlid

Type: string
Required: False

caseUlid

Type: string
Required: False

actions

Type: Array of type [CaseAction](#)
Required: False

caseName

Type: string
Required: False

userFirstName

Type: string
Required: False

userLastName

Type: string
Required: False

created

Type: string

Required: False

updated

    Type: string
    Required: False

Caseownerdata

userId

    Type: string
    Required: True

caseId

    Type: string
    Required: True

Cases – Create case

The Cases endpoint provides a way to programmatically manage and interact with cases within DEA. It allows users to create a new case with its associated metadata, such as name, description, and status.

URI

`/cases`

HTTP methods

POST

Responses

Status code	Response model	Description
200	[Case](#)	Case successfully created

Schemas

Request bodies

POST schema

```
{
  "name": "string",
  "description": "string",
  "status": "string"
}
```

Response bodies

Case schema

```
{
  "ulid": "string",
  "name": "string",
  "status": enum,
  "description": "string",
  "objectCount": number,
  "totalSizeBytes": number,
  "fileStatus": enum,
  "s3BatchJobId": "string",
  "created": "string",
  "updated": "string"
}
```

Properties

Case

ulid

   Type: string
   Required: False

name

   Type: string

Required: False

status

Type: CaseStatus
Required: False

description

Type: string
Required: False

objectCount

Type: number
Required: False

totalSizeBytes

Type: number
Required: False

fileStatus

Type: CaseFileStatus
Required: False

s3BatchJobId

Type: string
Required: False

created

Type: string
Required: False

updated

> **Type**: string
> **Required**: False

CaseFileStatus

ACTIVE
DELETING
DELETE_FAILED
DELETED
PENDING

CaseStatus

ACTIVE
INACTIVE

CreateCaseObject

name

> **Type**: string
> **Required**: True

description

> **Type**: string
> **Required**: False

status

> **Type**: string
> **Required**: True

Cases – CSV audit entry for a case

This endpoint provides a way to export a specific audit trail entry for a case in CSV format, allowing users to further analyze or process the audit trail data. The API response would include the CSV file as the response body, which the client application can then process or download.

URI

/cases/*caseId*/audit/*auditId*/csv

HTTP methods

GET

Path parameters

Name	Type	Required	Description
caseId	String	True	
auditId	String	True	Audit log ID

Responses

Status code	Response model	Description
200	AuditResult	Audit log CSV result and status

Schemas

Response bodies

AuditResult schema

```
{
    "status": "string",
    "downloadUrl": "string"
}
```

Properties

AuditResult

status

    Type: string

    Required: False

downloadUrl

    Type: string

    Required: False

Cases – CSV audit entry for a case file

This endpoint provides a way to export a specific audit trail entry for a file within a case in CSV format, allowing users to further anaylyze or process the audit trail data. The API response would include the CSV file as the response body, which the client application can then process or download.

URI

/cases/*caseId*/files/*fileId*/audit/*auditId*/csv

HTTP methods

GET

Path parameters

Name	Type	Required	Description
caseId	String	True	
fileId	String	True	
auditId	String	True	Audit log ID

Responses

Status code	Response model	Description
200	AuditResult	Audit log CSV result and status

Schemas

Response bodies

AuditResult schema

```
{
  "status": "string",
  "downloadUrl": "string"
}
```

Properties

AuditResult

status

    Type: string
    Required: False

downloadUrl

    Type: string
    Required: False

Cases – File audit by caseId and fileId

This endpoint provides a way to retrieve the audit trail or history of actions performed on a specific file or piece of evidence identified by fileId within a case identified by caseId. The audit trail is crucial for security and compliance purposes, as it provides a record of who accessed the file and what actions were taken.

URI

/cases/*caseId*/files/*fileId*/audit

HTTP methods

POST

Path parameters

Name	Type	Required	Description
caseId	String	True	
fileId	String	True	

Responses

Status code	Response model	Description
200	Cases_response_200_6	Audit Query ID

Schemas

Request bodies

POST schema

```
{
  "from": number,
  "to": number
}
```

Response bodies

Cases_response_200_6 schema

```
{
  "auditId": "string"
```

```
}
```

Properties

AuditPayload

from

> **Type**: number
> **Required**: False

to

> **Type**: number
> **Required**: False

Cases_response_200_6

auditId

> **Type**: string
> **Required**: False

Cases – File contents

This endpoint provides a way to retrieve the contents of a file within a case in Digital Evidence Archive, allowing users to access and view the actual data stored in the file by providing a download URL. The API requires authentication and authorization to ensure that only authorized users can retrieve the contents of the file.

URI

/cases/*caseId*/files/*fileId*/contents

HTTP methods

POST

Download the contents of a file via s3 signed url

Path parameters

Name	Type	Required	Description
caseId	String	True	
fileId	String	True	

Responses

Status code	Response model	Description
200	[Cases_response_200_5](#)	Success Response

PUT

Path parameters

Name	Type	Required	Description
caseId	String	True	
fileId	String	True	

Responses

Status code	Response model	Description
200	[CompleteCaseFileUploadResponse](#)	Success Response

Schemas

Request bodies

POST schema

```
{
```

```
    "caseUlid": "string",
    "ulid": "string",
    "downloadReason": "string"
}
```

PUT schema

```
{
    "caseUlid": "string",
    "ulid": "string",
    "uploadId": "string"
}
```

Response bodies

Cases_response_200_5 schema

```
{
    "isArchived": boolean,
    "isRestoring": boolean,
    "downloadUrl": "string",
    "downloadReason": "string"
}
```

CompleteCaseFileUploadResponse schema

```
{
    "fileName": "string",
    "filePath": "string",
    "caseUlid": "string",
    "contentType": "string",
    "createdBy": "string",
    "fileSizeBytes": number,
    "sha256Hash": "string",
    "ulid": "string",
    "status": enum,
    "uploadId": "string",
    "isFile": boolean,
    "created": "string",
    "updated": "string",
```

```
      "details": "string",
      "fileS3Key": "string",
      "versionId": "string",
      "dataVaultUlid": "string",
      "executionId": "string",
      "associationCreatedBy": "string",
      "associationDate": "string",
      "dataVaultUploadDate": "string",
      "ttl": number,
      "dataVaultName": "string",
      "reason": "string"
 }
```

Properties

CaseFileCompleteUpload

caseUlid

Type: string
Required: True

ulid

Type: string
Required: True

uploadId

Type: string
Required: True

CaseFileStatus

ACTIVE
DELETING
DELETE_FAILED
DELETED
PENDING

Cases_response_200_5

isArchived

Type: boolean
Required: False

isRestoring

Type: boolean
Required: False

downloadUrl

Type: string
Required: False
Format: uri

downloadReason

Type: string
Required: False

CompleteCaseFileUploadResponse

fileName

Type: string
Required: False

filePath

Type: string
Required: False

caseUlid

Type: string

Required: False

contentType

Type: string

Required: False

createdBy

Type: string

Required: False

fileSizeBytes

Type: number

Required: False

sha256Hash

Type: string

Required: False

ulid

Type: string

Required: False

status

Type: CaseFileStatus

Required: False

uploadId

    Type: string

    Required: False

isFile

    Type: boolean

    Required: False

created

    Type: string

    Required: False

updated

    Type: string

    Required: False

details

    Type: string

    Required: False

fileS3Key

    Type: string

    Required: False

versionId

    Type: string

    Required: False

dataVaultUlid

Type: string

Required: False

executionId

Type: string

Required: False

associationCreatedBy

Type: string

Required: False

associationDate

Type: string

Required: False

dataVaultUploadDate

Type: string

Required: False

ttl

Type: number

Required: False

dataVaultName

Type: string

Required: False

reason

>   **Type**: string
>   **Required**: False

body

caseUlid

>   **Type**: string
>   **Required**: True

ulid

>   **Type**: string
>   **Required**: True

downloadReason

>   **Type**: string
>   **Required**: True

Cases – Files by caseId

This endpoint provides a way to manage files within a specific case in Digital Evidence Archive, allowing users to upload and retrieve files as needed. The API requires authentication and authorization to ensure that only authorized users can retrieve the details of the case.

URI

`/cases/`*`caseId`*`/files`

HTTP methods

GET

List files within a case in given file path or case root

Path parameters

Name	Type	Required	Description
caseId	String	True	

Query parameters

Name	Type	Required	Description
filePath	String	False	
limit	Integer	False	
next	String	False	

Responses

Status code	Response model	Description
200	[Cases_response_200_3](#)	Success

POST

Path parameters

Name	Type	Required	Description
caseId	String	True	

Responses

Status code	Response model	Description
200	[CaseUploadResponse](#)	Success Response

Schemas

Request bodies

POST schema

```
{
  "fileName": "string",
  "filePath": "string",
  "caseUlid": "string",
  "fileSizeBytes": number,
  "details": "string",
  "reason": "string",
  "uploadId": "string",
  "contentType": "string"
}
```

Response bodies

Cases_response_200_3 schema

```
{
  "caseFiles": [
    [
      {
        "fileName": "string",
        "filePath": "string",
        "caseUlid": "string",
        "contentType": "string",
        "createdBy": "string",
        "fileSizeBytes": number,
        "sha256Hash": "string",
        "ulid": "string",
        "status": enum,
        "uploadId": "string",
        "isFile": boolean,
        "created": "string",
        "updated": "string",
        "details": "string",
        "fileS3Key": "string",
        "dataVaultUlid": "string",
        "executionId": "string",
```

```
            "associationCreatedby": "string",
            "associationDate": "string",
            "dataVaultUploadDate": "string",
            "dataVaultName": "string",
            "reason": "string"
      }
    ]
  ],
  "total": number,
  "next": "string"
}
```

CaseUploadResponse schema

```
{
  "fileName": "string",
  "filePath": "string",
  "caseUlid": "string",
  "contentType": "string",
  "createdBy": "string",
  "fileSizeBytes": number,
  "sha256Hash": "string",
  "ulid": "string",
  "fileStatus": enum,
  "uploadId": "string",
  "isFile": boolean,
  "created": "string",
  "updated": "string",
  "details": "string",
  "fileS3Key": "string",
  "dataVaultUlid": "string",
  "executionId": "string",
  "associationCreatedby": "string",
  "associationDate": "string",
  "dataVaultUploadDate": "string",
  "dataVaultName": "string",
  "federationCredentials": "string",
  "bucket": "string",
  "region": "string",
  "reason": "string"
}
```

Properties

CaseFile

fileName

Type: string
Required: False

filePath

Type: string
Required: False

caseUlid

Type: string
Required: False

contentType

Type: string
Required: False

createdBy

Type: string
Required: False

fileSizeBytes

Type: number
Required: False

sha256Hash

Type: string

Required: False

ulid

Type: string

Required: False

status

Type: CaseFileStatus

Required: False

uploadId

Type: string

Required: False

isFile

Type: boolean

Required: False

created

Type: string

Required: False

updated

Type: string

Required: False

details

Type: string

Required: False

fileS3Key

Type: string
Required: False

dataVaultUlid

Type: string
Required: False

executionId

Type: string
Required: False

associationCreatedby

Type: string
Required: False

associationDate

Type: string
Required: False

dataVaultUploadDate

Type: string
Required: False

dataVaultName

Type: string
Required: False

reason

> **Type**: string
> **Required**: False

CaseFileInitiateUpload

fileName

> **Type**: string
> **Required**: True

filePath

> **Type**: string
> **Required**: True

caseUlid

> **Type**: string
> **Required**: True

fileSizeBytes

> **Type**: number
> **Required**: True

details

> **Type**: string
> **Required**: False

reason

> **Type**: string
> **Required**: False

uploadId

    Type: string

    Required: False

contentType

    Type: string

    Required: True

CaseFileStatus

```
ACTIVE
DELETING
DELETE_FAILED
DELETED
PENDING
```

CaseUploadResponse

fileName

    Type: string

    Required: False

filePath

    Type: string

    Required: False

caseUlid

    Type: string

    Required: False

contentType

Type: string

Required: False

createdBy

Type: string

Required: False

fileSizeBytes

Type: number

Required: False

sha256Hash

Type: string

Required: False

ulid

Type: string

Required: False

fileStatus

Type: CaseFileStatus

Required: False

uploadId

Type: string

Required: False

isFile

Type: boolean
Required: False

created

Type: string
Required: False

updated

Type: string
Required: False

details

Type: string
Required: False

fileS3Key

Type: string
Required: False

dataVaultUlid

Type: string
Required: False

executionId

Type: string
Required: False

associationCreatedby

Type: string
Required: False

associationDate

Type: string
Required: False

dataVaultUploadDate

Type: string
Required: False

dataVaultName

Type: string
Required: False

federationCredentials

Type: string
Required: False

bucket

Type: string
Required: False

region

Type: string
Required: False

reason

> **Type**: string
> **Required**: False

Cases_response_200_3

caseFiles

> **Type**: Array of type Array of type CaseFile
> **Required**: False

total

> **Type**: number
> **Required**: False

next

> **Type**: string
> **Required**: False

Cases – List all cases

This elevated permission endpoint provides a method for administrators to monitor the overall status of cases within DEA. When a request is made to this endpoint, the API responds with a list of all cases with specific metadata about each case.

URI

`/cases/all-cases`

HTTP methods

GET

admin-only returns list of cases

Query parameters

Name	Type	Required	Description
limit	Integer	False	
next	String	False	

Responses

Status code	Response model	Description
200	[Cases_response_200](#)	Success Response

Schemas

Response bodies

Cases_response_200 schema

```
{
  "total": number,
  "cases": {
  },
  "next": "string"
}
```

Properties

Case

ulid

Type: string
Required: False

name

Type: string

Required: False

status

Type: CaseStatus
Required: False

description

Type: string
Required: False

objectCount

Type: number
Required: False

totalSizeBytes

Type: number
Required: False

fileStatus

Type: CaseFileStatus
Required: False

s3BatchJobId

Type: string
Required: False

created

Type: string
Required: False

updated

    Type: string
    Required: False

CaseFileStatus

    ACTIVE
    DELETING
    DELETE_FAILED
    DELETED
    PENDING

CaseStatus

    ACTIVE
    INACTIVE

Cases_response_200

total

    Type: number
    Required: False

cases

    Type: object
    Required: False

next

    Type: string
    Required: False

Cases – Manage user memberships

This endpoint provides a way to manage user memberships for a specific case in DEA, facilitating user management and access control.

URI

/cases/*caseId*/users/*userId*/memberships

HTTP methods

PUT

Update the details on an existing case membership

Path parameters

Name	Type	Required	Description
caseId	String	True	
userId	String	True	

Responses

Status code	Response model	Description
200	CaseUser	Case user successfully updated

DELETE

Remove a collaborator from a case

Path parameters

Name	Type	Required	Description
caseId	String	True	

Name	Type	Required	Description
userId	String	True	

Responses

Status code	Response model	Description
204	None	204 response

Schemas

Request bodies

PUT schema

```
{
  "userUlid": "string",
  "caseUlid": "string",
  "actions": [
    enum
  ]
}
```

Response bodies

CaseUser schema

```
{
  "userUlid": "string",
  "caseUlid": "string",
  "actions": [
    enum
  ],
  "caseName": "string",
  "userFirstName": "string",
  "userLastName": "string",
  "created": "string",
  "updated": "string"
```

```
}
```

Properties

CaseAction

```
VIEW_CASE_DETAILS
UPDATE_CASE_DETAILS
UPDATE_CASE_STATUS
UPLOAD
DOWNLOAD
VIEW_FILES
CASE_AUDIT
INVITE
RESTORE_FILES
```

CaseUser

userUlid

Type: string
Required: False

caseUlid

Type: string
Required: False

actions

Type: Array of type CaseAction
Required: False

caseName

Type: string

Required: False

userFirstName

Type: string
Required: False

userLastName

Type: string
Required: False

created

Type: string
Required: False

updated

Type: string
Required: False

CaseUserRequest

userUlid

Type: string
Required: True

caseUlid

Type: string
Required: True

actions

Type: Array of type CaseAction

Required: True

Cases – My cases

This endpoint provides a way for users to retrieve a list of cases they are associated with in DEA, facilitating case managment and access. The API requires authentication and authorization to ensure that only authorized users can retrieve the list of cases they are associated with.

URI

`/cases/my-cases`

HTTP methods

GET

returns array of cases on which the user has membership

Query parameters

Name	Type	Required	Description
limit	Integer	False	
next	String	False	

Responses

Status code	Response model	Description
200	[My_cases_response](#)	Success

Schemas

Response bodies

My_cases_response schema

```
{
```

```
    "total": number,
    "cases": {
    },
    "next": "string"
}
```

Properties

CaseAction

VIEW_CASE_DETAILS

UPDATE_CASE_DETAILS

UPDATE_CASE_STATUS

UPLOAD

DOWNLOAD

VIEW_FILES

CASE_AUDIT

INVITE

RESTORE_FILES

CaseFileStatus

ACTIVE

DELETING

DELETE_FAILED

DELETED

PENDING

CaseStatus

ACTIVE

INACTIVE

MyCase

ulid

Type: string

Required: False

name

Type: string

Required: False

status

Type: CaseStatus

Required: False

description

Type: string

Required: False

objectCount

Type: number

Required: False

totalSizeBytes

Type: number

Required: False

fileStatus

Type: CaseFileStatus

Required: False

s3BatchJobId

Type: string
Required: False

actions

Type: Array of type CaseAction
Required: False

created

Type: string
Required: False

updated

Type: string
Required: False

My_cases_response

total

Type: number
Required: False

cases

Type: object
Required: False

next

Type: string
Required: False

Cases – Restore files

This endpoint provides a way to restore files or evidence within a case in DEA, allowing users to recover files that may have been archived. The API would require authentication and authorization to ensure that only authorized users can restore files.

URI

/cases/*caseId*/files/*fileId*/restore

HTTP methods

PUT

Restore archived file by moving it to frequent access tier (if archived in intelligent-tier) or creating a restored copy (if archived in glacier)

Path parameters

Name	Type	Required	Description
caseId	String	True	
fileId	String	True	

Responses

Status code	Response model	Description
204	None	204 response

Cases – Retrieve user memberships

This endpoint provides a way to retrieve information about user memberships associated with a specific case in DEA, facilitating user management and access control.

URI

/cases/*caseId*/userMemberships

HTTP methods

GET

get all users with membership on a case

Path parameters

Name	Type	Required	Description
caseId	String	True	

Query parameters

Name	Type	Required	Description
limit	Integer	False	
next	String	False	

Responses

Status code	Response model	Description
200	[Cases_response_200_2](#)	Success Response

POST

Path parameters

Name	Type	Required	Description
caseId	String	True	

Responses

Status code	Response model	Description
200	CaseUser	Case successfully created

Schemas

Request bodies

POST schema

```
{
  "userUlid": "string",
  "caseUlid": "string",
  "actions": [
    enum
  ]
}
```

Response bodies

Cases_response_200_2 schema

```
{
  "caseUsers": [
   [
     {
       "userUlid": "string",
       "caseUlid": "string",
       "actions": [
         enum
       ],
       "caseName": "string",
       "userFirstName": "string",
       "userLastName": "string",
       "created": "string",
       "updated": "string"
     }
   ]
  ],
```

```
  "total": number,
  "next": "string"
}
```

CaseUser schema

```
{
  "userUlid": "string",
  "caseUlid": "string",
  "actions": [
    enum
  ],
  "caseName": "string",
  "userFirstName": "string",
  "userLastName": "string",
  "created": "string",
  "updated": "string"
}
```

Properties

CaseAction

```
VIEW_CASE_DETAILS
UPDATE_CASE_DETAILS
UPDATE_CASE_STATUS
UPLOAD
DOWNLOAD
VIEW_FILES
CASE_AUDIT
INVITE
RESTORE_FILES
```

CaseUser

userUlid

Type: string

Required: False

caseUlid

Type: string
Required: False

actions

Type: Array of type [CaseAction](#)
Required: False

caseName

Type: string
Required: False

userFirstName

Type: string
Required: False

userLastName

Type: string
Required: False

created

Type: string
Required: False

updated

Type: string
Required: False

CaseUserRequest

userUlid

Type: string

Required: True

caseUlid

Type: string

Required: True

actions

Type: Array of type [CaseAction](#)

Required: True

Cases_response_200_2

caseUsers

Type: Array of type Array of type [CaseUser](#)

Required: False

total

Type: number

Required: False

next

Type: string

Required: False

Cases – Scoped information

This elevated permissions endpoint provides a way to retrieve scoped information related to a specific case in DEA, allowing for more detailed and customizable case management.

URI

/cases/*caseId*/scopedInformation

HTTP methods

GET

Get specific set case details. Intended for evidence managers and admins

Path parameters

Name	Type	Required	Description
caseId	String	True	

Responses

Status code	Response model	Description
200	ScopedCase	Success

Schemas

Response bodies

ScopedCase schema

```
{
  "ulid": "string",
  "name": "string"
}
```

Properties

ScopedCase

ulid

   Type: string
   Required: False

name

   Type: string
   Required: False

Cases – Status

This endpoint provides a way to update the status of a specific case in DEA, facilitating case management and tracking.

URI

/cases/*caseId*/status

HTTP methods

PUT

Path parameters

Name	Type	Required	Description
caseId	String	True	

Responses

Status code	Response model	Description
200	[Case](#)	Successfully updated case

Schemas

Request bodies

PUT schema

```
{
  "name": "string",
  "deleteFiles": boolean,
  "status": enum
}
```

Response bodies

Case schema

```
{
  "ulid": "string",
  "name": "string",
  "status": enum,
  "description": "string",
  "objectCount": number,
  "totalSizeBytes": number,
  "fileStatus": enum,
  "s3BatchJobId": "string",
  "created": "string",
  "updated": "string"
}
```

Properties

Case

ulid

Type: string
Required: False

name

Type: string

Required: False

status

Type: [CaseStatus](#)
Required: False

description

Type: string
Required: False

objectCount

Type: number
Required: False

totalSizeBytes

Type: number
Required: False

fileStatus

Type: [CaseFileStatus](#)
Required: False

s3BatchJobId

Type: string
Required: False

created

Type: string
Required: False

updated

> **Type**: string
>
> **Required**: False

CaseFileStatus

> ACTIVE
>
> DELETING
>
> DELETE_FAILED
>
> DELETED
>
> PENDING

CaseStatus

> ACTIVE
>
> INACTIVE

Casestatusupdatedata

name

> **Type**: string
>
> **Required**: False

deleteFiles

> **Type**: boolean
>
> **Required**: False

status

> **Type**: CaseStatus
>
> **Required**: False

Data vaults

This endpoint provides a way to manage data vaults in DEA, allowing users to create and retrieve information about data vaults as needed.

URI

/datavaults

HTTP methods

GET

returns list of data vaults

Query parameters

Name	Type	Required	Description
limit	Integer	False	
next	String	False	

Responses

Status code	Response model	Description
200	DataVaults_response_200	Success Response

POST

Responses

Status code	Response model	Description
200	DataVault	Data Vault successfully created

Schemas

Request bodies

POST schema

```
{
  "name": "string",
  "description": "string"
}
```

Response bodies

DataVaults_response_200 schema

```
{
  "datavaults": [
   [
     {
       "ulid": "string",
       "name": "string",
       "description": "string",
       "objectCount": number,
       "totalSizeBytes": number,
       "created": "string",
       "updated": "string"
     }
   ]
  ],
  "next": "string"
}
```

DataVault schema

```
{
  "ulid": "string",
  "name": "string",
  "description": "string",
  "objectCount": number,
  "totalSizeBytes": number,
  "created": "string",
```

```
    "updated": "string"
}
```

Properties

CreateDataVaultObject

name

    Type: string
    Required: True

description

    Type: string
    Required: True

DataVault

ulid

    Type: string
    Required: False

name

    Type: string
    Required: False

description

    Type: string
    Required: False

objectCount

    Type: number

Required: False

totalSizeBytes

Type: number
Required: False

created

Type: string
Required: False

updated

Type: string
Required: False

DataVaults_response_200

datavaults

Type: Array of type Array of type [DataVault](#)
Required: False

next

Type: string
Required: False

Data vaults – Audit

This endpoint provides visibility into the history of actions that have been performed on a specific data vault in DEA.

URI

/datavaults/*dataVaultId*/audit

HTTP methods

POST

Operation ID: `requestDataVaultAudit`

Path parameters

Name	Type	Required	Description
dataVaultId	String	True	Data vault ID to generate audit log for

Responses

Status code	Response model	Description
200	[DataVaults_response_200_4](#)	Audit Query ID

Schemas

Request bodies

POST schema

```
{
  "from": number,
  "to": number
}
```

Response bodies

DataVaults_response_200_4 schema

```
{
  "auditId": "string"
}
```

Properties

AuditPayload

from

> **Type**: number
> **Required**: False

to

> **Type**: number
> **Required**: False

DataVaults_response_200_4

auditId

> **Type**: string
> **Required**: False

Data vaults – Audit export as CSV

This endpoint provides a way to export a specific audit trail entry for a data vault in CSV format, allowing users to further analyze or process the audit trail data.

URI

/datavaults/*dataVaultId*/audit/*auditId*/csv

HTTP methods

GET

Operation ID: getDataVaultAudit

Path parameters

Name	Type	Required	Description
dataVaultId	String	True	Data vault ID to generate audit log for
auditId	String	True	Audit log ID

Responses

Status code	Response model	Description
200	<u>AuditResult</u>	Audit log CSV result and status

Schemas

Response bodies

AuditResult schema

```
{
  "status": "string",
  "downloadUrl": "string"
}
```

Properties

AuditResult

status

   Type: string
   Required: False

downloadUrl

   Type: string

Required: False

Data vaults – Case association and disassociation

This endpoint provides a way to manage associations between a data vault and cases in Digital Evidence Archive, allowing users to associate cases as needed.

URI

/datavaults/*dataVaultId*/caseAssociations

HTTP methods

POST

Creates a case file entry to associate data vault file to case

Path parameters

Name	Type	Required	Description
dataVaultId	String	True	Data vault ID to generate audit log for

Responses

Status code	Response model	Description
200	DataVaults_response_200_2	Success

Schemas

Request bodies

POST schema

```
{
```

```
    "caseUlids": [
      "string"
    ],
    "fileUlids": [
      "string"
    ]
}
```

Response bodies

DataVaults_response_200_2 schema

```
{
  "DataVaultFiles": [
    [
      {
        "fileName": "string",
        "filePath": "string",
        "dataVaultUlid": "string",
        "fileSizeBytes": number,
        "sha256Hash": "string",
        "ulid": "string",
        "versionId": "string",
        "fileS3Key": "string",
        "uploadId": "string",
        "isFile": boolean,
        "contentType": "string",
        "executionId": "string",
        "created": "string",
        "updated": "string",
        "caseCount": number,
        "cases": [
          {
            "ulid": "string",
            "name": "string"
          }
        ]
      }
    ]
  ]
}
```

Properties

DataVaultFile

fileName

Type: string
Required: False

filePath

Type: string
Required: False

dataVaultUlid

Type: string
Required: False

fileSizeBytes

Type: number
Required: False

sha256Hash

Type: string
Required: False

ulid

Type: string
Required: False

versionId

Type: string

Required: False

fileS3Key

Type: string
Required: False

uploadId

Type: string
Required: False

isFile

Type: boolean
Required: False

contentType

Type: string
Required: False

executionId

Type: string
Required: False

created

Type: string
Required: False

updated

Type: string
Required: False

caseCount

Type: number

Required: False

cases

Type: Array of type ScopedCase

Required: False

DataVaults_response_200_2

DataVaultFiles

Type: Array of type Array of type DataVaultFile

Required: False

ScopedCase

ulid

Type: string

Required: False

name

Type: string

Required: False

caseAssociationRequest

caseUlids

Type: Array of type string

Required: True

fileUlids

>   **Type**: Array of type string
>   **Required**: True

Data vaults – Case file disassociations

This endpoint provides a way to manage associations between a file within a data vault and cases in Digital Evidence Archive, allowing users to disassociate cases as needed.

URI

/datavaults/*dataVaultId*/files/*fileId*/caseAssociations

HTTP methods

DELETE

Path parameters

Name	Type	Required	Description
dataVaultId	String	True	Data vault ID to generate audit log for
fileId	String	True	

Responses

Status code	Response model	Description
200	None	Success

Schemas

Request bodies

DELETE schema

```
{
  "caseUlids": [
    "string"
  ]
}
```

Properties

caseAssociationRequest_1

caseUlids

    Type: Array of type string
    Required: True

Data vaults – Details

This endpoint provides a way to retrieve detailed information about a specific data vault in Digital Evidence Archive, facilitating better management and understanding of the data vault.

URI

/datavaults/*dataVaultId*/details

HTTP methods

GET

Get metadata for a specific data vault. return not found if user doesn't have access

Path parameters

Name	Type	Required	Description
dataVaultId	String	True	Data vault ID to generate audit log for

Responses

Status code	Response model	Description
200	DataVault	Success

PUT

Path parameters

Name	Type	Required	Description
dataVaultId	String	True	Data vault ID to generate audit log for

Responses

Status code	Response model	Description
200	DataVault	Success

Schemas

Request bodies

PUT schema

```
{
  "dataVaultId": "string",
  "dataVaultName": "string",
  "dataVaultDescription": "string"
}
```

Response bodies

DataVault schema

```
{
```

```
    "ulid": "string",
    "name": "string",
    "description": "string",
    "objectCount": number,
    "totalSizeBytes": number,
    "created": "string",
    "updated": "string"
}
```

Properties

DataVault

ulid

   Type: string
   Required: False

name

   Type: string
   Required: False

description

   Type: string
   Required: False

objectCount

   Type: number
   Required: False

totalSizeBytes

   Type: number
   Required: False

created

    Type: string

    Required: False

updated

    Type: string

    Required: False

DataVaultUpdateRequest

dataVaultId

    Type: string

    Required: True

dataVaultName

    Type: string

    Required: True

dataVaultDescription

    Type: string

    Required: False

Data vaults – File audit

This endpoint provides visibility into the history of actions that have been performed on a specific file within a data vault in Digital Evidence Archive.

URI

/datavaults/*dataVaultId*/files/*fileId*/audit

HTTP methods

POST

Operation ID: `requestDataVaultFileAudit`

Path parameters

Name	Type	Required	Description
dataVaultId	String	True	Data vault ID to generate audit log for
fileId	String	True	File ID to generate audit log for

Responses

Status code	Response model	Description
200	[DataVaults_response_200_4](#)	Audit Query ID

Schemas

Request bodies

POST schema

```
{
  "from": number,
  "to": number
}
```

Response bodies

DataVaults_response_200_4 schema

```
{
```

```
    "auditId": "string"
}
```

Properties

AuditPayload

from

    Type: number
    Required: False

to

    Type: number
    Required: False

DataVaults_response_200_4

auditId

    Type: string
    Required: False

Data vaults – File audit as CSV

This endpoint provides a way to export a specific audit trail entry for a file within a data vault in CSV format, allowing users to further analyze or process the audit trail data.

URI

/datavaults/*dataVaultId*/files/*fileId*/audit/*auditId*/csv

HTTP methods

GET

Operation ID: getDataVaultFileAudit

Path parameters

Name	Type	Required	Description
dataVaultId	String	True	Data vault ID to generate audit log for
fileId	String	True	File ID to return audit log entries for
auditId	String	True	Audit log ID

Responses

Status code	Response model	Description
200	AuditResult	Audit log CSV result and status

Schemas

Response bodies

AuditResult schema

```
{
  "status": "string",
  "downloadUrl": "string"
}
```

Properties

AuditResult

status

   Type: string
   Required: False

downloadUrl

> **Type**: string
> **Required**: False

Data vaults – File info

This endpoint provides a way to retrieve detailed information about a specific file within a data vault in Digital Evidence Archive, facilitating better management and understanding of the file.

URI

/datavaults/*dataVaultId*/files/*fileId*/info

HTTP methods

GET

Get details for a file within a data vault

Path parameters

Name	Type	Required	Description
dataVaultId	String	True	Data vault ID to generate audit log for
fileId	String	True	

Responses

Status code	Response model	Description
200	[DataVaults_response_200_3](#)	Success Response

Schemas

Response bodies

DataVaults_response_200_3 schema

```
{
  "file": {
    "fileName": "string",
    "filePath": "string",
    "dataVaultUlid": "string",
    "fileSizeBytes": number,
    "sha256Hash": "string",
    "ulid": "string",
    "versionId": "string",
    "fileS3Key": "string",
    "uploadId": "string",
    "isFile": boolean,
    "contentType": "string",
    "executionId": "string",
    "created": "string",
    "updated": "string",
    "caseCount": number,
    "cases": [
      {
        "ulid": "string",
        "name": "string"
      }
    ]
  }
}
```

Properties

DataVaultFile

fileName

Type: string
Required: False

filePath

Type: string
Required: False

dataVaultUlid

Type: string
Required: False

fileSizeBytes

Type: number
Required: False

sha256Hash

Type: string
Required: False

ulid

Type: string
Required: False

versionId

Type: string
Required: False

fileS3Key

Type: string
Required: False

uploadId

Type: string
Required: False

isFile

Type: boolean

Required: False

contentType

Type: string

Required: False

executionId

Type: string

Required: False

created

Type: string

Required: False

updated

Type: string

Required: False

caseCount

Type: number

Required: False

cases

Type: Array of type ScopedCase

Required: False

DataVaults_response_200_3

file

> **Type**: DataVaultFile
> **Required**: False

ScopedCase

ulid

> **Type**: string
> **Required**: False

name

> **Type**: string
> **Required**: False

Data vaults – Files

This endpoint provides a way to retrieve information about the files or evidence associated with a specific data vault in Digital Evidence Archive, allowing users to access and manage the evidence related to the data vault.

URI

/datavaults/*dataVaultId*/files

HTTP methods

GET

List files within a datavault in given file path or datavault root

Path parameters

Name	Type	Required	Description
dataVaultId	String	True	Data vault ID to generate audit log for

Query parameters

Name	Type	Required	Description
filePath	String	False	
limit	Integer	False	
next	String	False	

Responses

Status code	Response model	Description
200	DataVaults_response_200_1	Success

Schemas

Response bodies

DataVaults_response_200_1 schema

```
{
  "dataVaultFiles": [
    [
      {
        "fileName": "string",
        "filePath": "string",
        "dataVaultUlid": "string",
        "fileSizeBytes": number,
```

```
        "sha256Hash": "string",
        "ulid": "string",
        "versionId": "string",
        "fileS3Key": "string",
        "uploadId": "string",
        "isFile": boolean,
        "contentType": "string",
        "executionId": "string",
        "created": "string",
        "updated": "string",
        "caseCount": number,
        "cases": [
          {
            "ulid": "string",
            "name": "string"
          }
        ]
      }
    ]
  ],
  "next": "string"
}
```

Properties

DataVaultFile

fileName

> **Type**: string
> **Required**: False

filePath

> **Type**: string
> **Required**: False

dataVaultUlid

> **Type**: string
> **Required**: False

fileSizeBytes

Type: number

Required: False

sha256Hash

Type: string

Required: False

ulid

Type: string

Required: False

versionId

Type: string

Required: False

fileS3Key

Type: string

Required: False

uploadId

Type: string

Required: False

isFile

Type: boolean

Required: False

contentType

Type: string

Required: False

executionId

Type: string

Required: False

created

Type: string

Required: False

updated

Type: string

Required: False

caseCount

Type: number

Required: False

cases

Type: Array of type [ScopedCase](#)

Required: False

DataVaults_response_200_1

dataVaultFiles

Type: Array of type Array of type [DataVaultFile](#)

Required: False

next

    Type: string

    Required: False

ScopedCase

ulid

    Type: string

    Required: False

name

    Type: string

    Required: False

Data vaults – Task execution

This endpoint provides a way to manage executions of tasks associated data vaults in DEA, allowing users to view data vault details.

URI

/datavaults/tasks/*taskId*/executions

HTTP methods

POST

Path parameters

Name	Type	Required	Description
taskId	String	True	

Responses

Status code	Response model	Description
200	[DataVaultExecution](#)	Data Vault Execution successfully created

Schemas

Request bodies

POST schema

```
{
  "taskArn": "string"
}
```

Response bodies

DataVaultExecution schema

```
{
  "taskId": "string",
  "executionId": "string",
  "createdBy": "string",
  "created": "string"
}
```

Properties

DataVaultExecution

taskId

  Type: string
  Required: False

executionId

  Type: string

Required: False

createdBy

Type: string
Required: False

created

Type: string
Required: False

dataVaultExecutionObject

taskArn

Type: string
Required: True

Data vaults – Tasks

This endpoint provides a way to manage tasks associated with a specific data vault in Digital Evidence Archive, allowing users to create information about tasks as needed.

URI

/datavaults/*dataVaultId*/tasks

HTTP methods

POST

Path parameters

Name	Type	Required	Description
dataVaultId	String	True	Data vault ID to generate audit log for

Responses

Status code	Response model	Description
200	DataVaultTask	Data Vault Task successfully created

Schemas

Request bodies

POST schema

```
{
  "name": "string",
  "description": "string",
  "sourceLocationArn": "string",
  "destinationLocationArn": "string"
}
```

Response bodies

DataVaultTask schema

```
{
  "taskId": "string",
  "dataVaultUlid": "string",
  "name": "string",
  "description": "string",
  "sourceLocationArn": "string",
  "destinationLocationArn": "string",
  "taskArn": number,
  "created": "string",
  "updated": "string",
  "deleted": boolean
}
```

Properties

CreateDataVaultTaskObject

name

Type: string
Required: True

description

Type: string
Required: False

sourceLocationArn

Type: string
Required: True

destinationLocationArn

Type: string
Required: True

DataVaultTask

taskId

Type: string
Required: False

dataVaultUlid

Type: string
Required: False

name

    Type: string
    Required: False

description

    Type: string
    Required: False

sourceLocationArn

    Type: string
    Required: False

destinationLocationArn

    Type: string
    Required: False

taskArn

    Type: number
    Required: False

created

    Type: string
    Required: False

updated

    Type: string
    Required: False

deleted

> **Type**: boolean
> **Required**: False

DataSync tasks

This endpoint provides a way to return a list of all tasks in AWS DataSync with associated metadata.

URI

`/datasync/tasks`

HTTP methods

GET

returns list of datasync tasks

Responses

Status code	Response model	Description
200	[DataSync_response_200](#)	Success Response

Schemas

Response bodies

DataSync_response_200 schema

```
{
  "DataSyncTasks": [
    [
      {
        "taskArn": "string",
        "taskId": "string",
```

```
            "sourceLocationArn": "string",
            "destinationLocationArn": "string",
            "dataVaultUlid": "string",
            "status": "string",
            "created": "string",
            "lastExecutionCompleted": "string"
        }
    ]
  ],
  "next": "string"
}
```

Properties

DataSyncTask

taskArn

Type: string
Required: False

taskId

Type: string
Required: False

sourceLocationArn

Type: string
Required: False

destinationLocationArn

Type: string
Required: False

dataVaultUlid

Type: string

Required: False

status

Type: string
Required: False

created

Type: string
Required: False

lastExecutionCompleted

Type: string
Required: False

DataSync_response_200

DataSyncTasks

Type: Array of type Array of type DataSyncTask
Required: False

next

Type: string
Required: False

System audit

This endpoint provides visibility into the history of actions that have been performed within the Digital Evidence Archive system, helping to ensure the security and integrity of the system.

URI

```
/system/audit
```

HTTP methods

POST

Operation ID: `requestSystemAudit`

Responses

Status code	Response model	Description
200	[System_response_200](#)	Audit Query ID

Schemas

Request bodies

POST schema

```
{
  "from": number,
  "to": number
}
```

Response bodies

System_response_200 schema

```
{
  "auditId": "string"
}
```

Properties

AuditPayload

from

    Type: number
    Required: False

to

>   **Type**: number
>   **Required**: False

System_response_200

auditId

>   **Type**: string
>   **Required**: False

System audit – CSV export

This endpoint endpoint provides a way to export a specific audit trail entry within the Digital Evidence Archive system in CSV format, allowing users to further analyze or process the audit trail data.

URI

`/system/audit/`*`auditId`*`/csv`

HTTP methods

GET

Operation ID: `getSystemAudit`

Path parameters

Name	Type	Required	Description
auditId	String	True	Audit log ID

Responses

Status code	Response model	Description
200	AuditResult	Audit log CSV result and status

Schemas

Response bodies

AuditResult schema

```
{
  "status": "string",
  "downloadUrl": "string"
}
```

Properties

AuditResult

status

Type: string
Required: False

downloadUrl

Type: string
Required: False

Users

This endpoint provides a way to manage users within the Digital Evidence Archive system, allowing administrators to retrieve information about users as needed.

URI

`/users`

HTTP methods

GET

Query parameters

Name	Type	Required	Description
limit	Integer	False	
next	String	False	

Responses

Status code	Response model	Description
200	[Users_response_200](#)	Success Response

Schemas

Response bodies

Users_response_200 schema

```
{
  "users": [
    [
      {
        "ulid": "string",
        "firstName": "string",
        "lastName": "string",
        "lowerFirstName": "string",
        "lowerLastName": "string"
      }
    ]
  ],
```

```
    "next": "string"
}
```

Properties

User

ulid

Type: string
Required: True

firstName

Type: string
Required: True

lastName

Type: string
Required: True

lowerFirstName

Type: string
Required: True

lowerLastName

Type: string
Required: True

Users_response_200

users

Type: Array of type Array of type User
Required: False

next

> **Type**: string
> **Required**: False

Users – Audit by UserId

This endpoint provides visibility into the history of actions that have been performed by a specific user within the Digital Evidence Archive system, helping to ensure accountability and traceability.

URI

/users/*userId*/audit

HTTP methods

POST

Operation ID: requestUserAudit

Path parameters

Name	Type	Required	Description
userId	String	True	User ID to generate audit log for

Responses

Status code	Response model	Description
200	[Users_response_200_1](#)	Audit Query ID

Schemas

Request bodies

POST schema

```
{
  "from": number,
  "to": number
}
```

Response bodies

Users_response_200_1 schema

```
{
  "auditId": "string"
}
```

Properties

AuditPayload

from

> **Type**: number
> **Required**: False

to

> **Type**: number
> **Required**: False

Users_response_200_1

auditId

> **Type**: string
> **Required**: False

Users – Audit CSV export

This endpoint provides a way to export a specific audit trail entry for a user within the Digital Evidence Archive system in CSV format, allowing users to further analyze or process the audit trail data.

URI

/users/*userId*/audit/*auditId*/csv

HTTP methods

GET

Operation ID: getUserAudit

Path parameters

Name	Type	Required	Description
userId	String	True	User ID to return audit log entries for
auditId	String	True	Audit log ID

Responses

Status code	Response model	Description
200	AuditResult	Audit log CSV result and status

Schemas

Response bodies

AuditResult schema

```
{
```

```
    "status": "string",
    "downloadUrl": "string"
}
```

Properties

AuditResult

status

> **Type**: string
> **Required**: False

downloadUrl

> **Type**: string
> **Required**: False

Document History for API Reference

The following table describes important changes to the documentation for this release of Digital Evidence Archive on AWS.

- **API version:** 1.1.1
- **Latest documentation update:** April 2, 2024

Change	Description	Date
[Released API descriptions](#)	API guide released for DEA 1.1.1.	April 2, 2024

AWS Glossary

For the latest AWS terminology, see the [AWS glossary](#) in the *AWS Glossary Reference*.