

FTK CENTRAL - ENTERPRISE API GUIDE

JULY 2026

Table of Contents

About Exterro	5
API Introduction.....	5
Generating API Keys.....	6
Via Enterprise Interface	7
Via FTK Central Interface.....	9
Authentication	10
Using Enterprise API Key	10
Using Active Directory (AD) authentication	11
Identification.....	12
Pagination	12
Filtering	17
1 Cases.....	19
1.1 Create Case	19
1.2 Get Case Details.....	22
1.3 Delete Case	25
2 Custodians	26
2.1 List Custodian.....	26
2.2 List Custodian By ID	29
2.3 Delete Custodians.....	31
3 Targets	32
3.1 List Target	32
3.2 List Target By ID	35

3.3	Create Target	37
3.4	Delete Target	39
4	Jobs	40
4.1	List Jobs	40
4.2	List Job Types	42
4.3	List Jobs By Job Type	54
4.4	List Job State	57
4.5	List Jobs By Job State	59
4.6	List Jobs By Job ID	62
4.7	Cancel Job	64
4.8	Delete Job	65
5	Collections	67
5.1	List Collection Templates	67
5.2	Create Template	70
5.3	Create Collection (From Template)	73
5.4	List Collection Filter Templates	76
5.5	Start a collection	77
6	User Activity Log API	79
6.1	Filter Types	80
6.2	Category Information	83
7	Event Audit Log API	86
7.1	FTK Audit Log Report (CSV/JSON)	86
7.2	Case Audit Log Report (JSON)	88
7.3	Audit Actions API	90

8	Lookup APIs (Prerequisites).....	91
8.1	Get All Users	91
8.2	Get All Groups.....	91
8.3	Get All Cases	92
8.4	Get All Users, Roles, Permissions and Groups	93
8.5	Get AWS Region GUID	94
9	Manage Group Assignments	95
10	Create User	97
11	Create Case with Evidence and User Assignment	100
12	Add Evidence to an Existing Case	103
13	Export Case Grid to CSV	106
13.1	Supporting API — Get Exportable Columns	106
13.2	Supporting API — Get File Categories for a Case	107
14	Import Evidence via CSV	109
15	Export Evidence (Labels & Options)	112
	Appendix A: Quick Reference — Validation Behavior	114
	Known Issues	115
	Limitations	115
	Contact Exterro	116

About Exterro

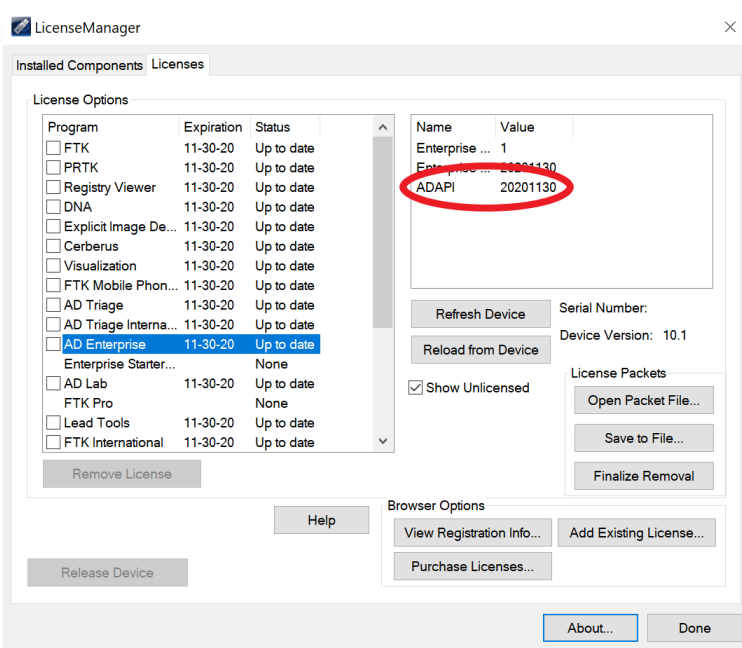
Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today. We deliver a fully integrated Data Risk Management platform that enables our clients to address their privacy, regulatory, compliance, digital forensics, and litigation risks more effectively and at lower costs. We provide software solutions that help some of the world's largest organizations, law enforcement and government agencies work smarter, more efficiently, and support the Rule of Law.

API Introduction

FTK Central - Enterprise APIs are RESTful APIs with the ability to access functional procedures and objects within the Exterro Forensic suite of products. Standard REST methodology is used throughout the API and a wide-range of parameters are used for modifying attributes. Modules exported as endpoints currently provide access to case management, evidence processing and browsing, label management, exporting files in multiple formats (from filters and IDs), and agent control. This allows for a quick and simple implementation of large and varied arrangement of production automations.

Generating API Keys

The REST interface acts similarly to many other interfaces, enforcing an API key to be valid on every request sent. To generate an API key that will be used to authenticate with the FTK Central service, a CodeMeter License dongle with the ADAPI license tag is required. The ADAPI tag will be displayed in the Enterprise section of the dongle licenses present in Exterro License Manager with 8.0. An example dongle and the tag are provided in the License Manager image below:



The following methods can be used to generate API keys:

- [Via Enterprise Interface](#)
- [Via FTK Central Interface](#) (only if the browser has valid cookies cached)

Note: You are advised to create an API key from the Administrator account to provide access to all endpoints for the following reasons:

- During this procedure, a **User ID** or **Name** should be provided. The corresponding API key generated will inherit any/all permissions from the account of the user ID/Name provided.
- The API keys inherit the permission of the provided user account over other users.

Via Enterprise Interface

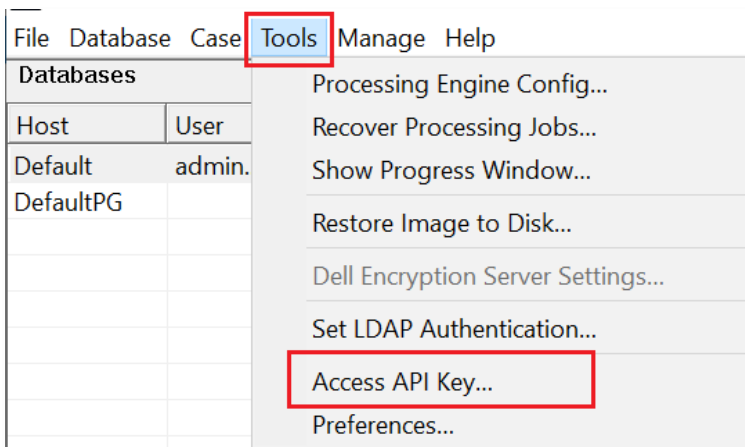
You can generate API keys through FTK Enterprise.

Note: Ensure a dongle is available to FTK and contains the ADAPI key.

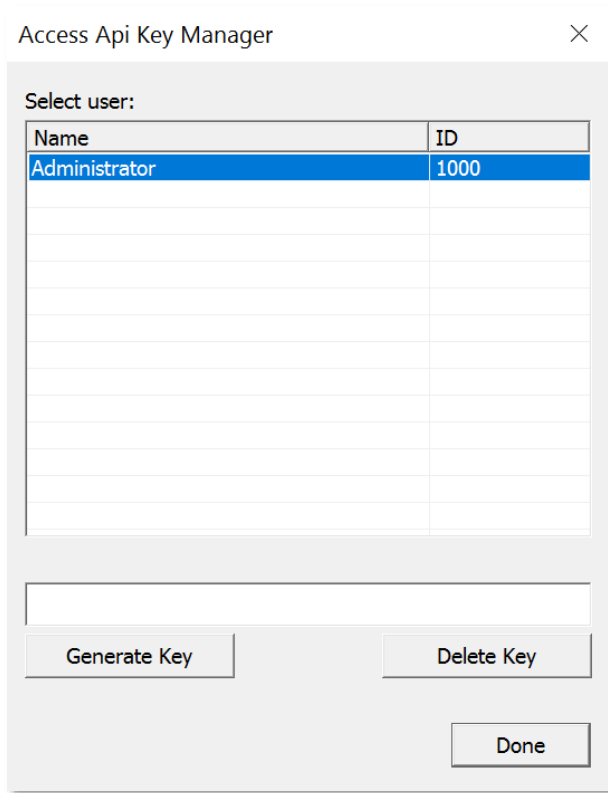
Follow the steps below to access the generated API key:

Steps:

1. Within the FTK Enterprise application, click on the **Tools** menu and select the **Access API Key** option.



- The **Access API Key Manager** pop-up is displayed.



The image shows a screenshot of the 'Access Api Key Manager' dialog box. It has a title bar with a close button (X). Below the title bar is a section labeled 'Select user:' containing a table with two columns: 'Name' and 'ID'. The first row of the table is highlighted in blue and contains the text 'Administrator' and '1000'. Below the table is a text input field. At the bottom of the dialog are three buttons: 'Generate Key', 'Delete Key', and 'Done'.

Name	ID
Administrator	1000

2. Select the required **User Name** with the application's administrator rights.
3. Click **Generate Key** and the API key will be generated.

Note: API Keys do not expire after a certain period, i.e., are valid indefinitely. In case of missing the API Keys, you are recommended to regenerate a new key using the above steps.

Via FTK Central Interface

When connecting the license dongle, CodeMeter will recognize the device and the FTK Central service will recognize the key. You can log into the FTK Central platform to push the validated cookies into the web browser, which is how the API key generation authenticates that it should release them.

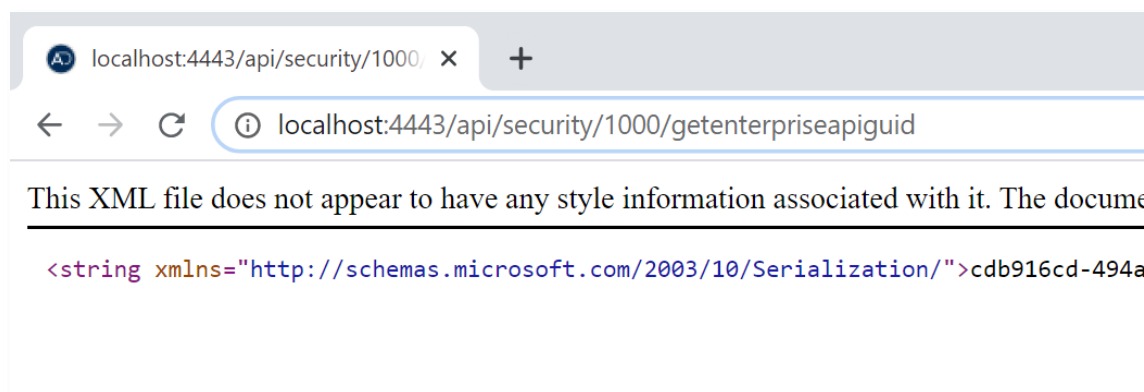
Follow the steps below to generate the API Key:

Steps:

1. Log into the FTK Central interface and navigate to the URL bar.
2. Replace 'ftklogin.html' with '**api/security/<user_id>/getenterpriseapiguid**' in the URL where the <user_id> is the user account's ID.

Note: It is required to provide the User having the application's admin rights.

Example: Consider the administrator user's ID is 1000. The URL should be updated as shown below:



Note: API Keys do not expire after a certain period, i.e., are valid indefinitely. If the keys are missing, you are recommended to regenerate a new key using the above steps.

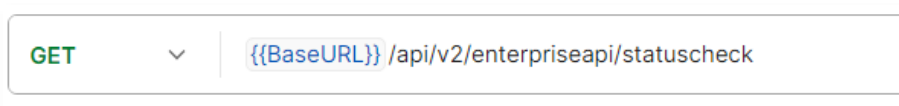
Authentication

Using Enterprise API Key

Each HTTP request must contain authentication to run the procedures by the service. The authentication trigger is provided to the service inside the HTTP request via request headers. And the request headers should include a key named "EnterpriseAPIKey" which defines the API key value.

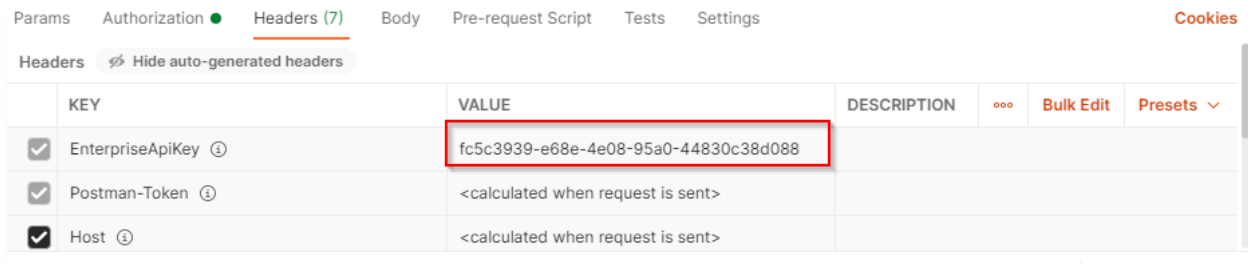
The HTTP headers will be displayed as below:

- **Request URL:**



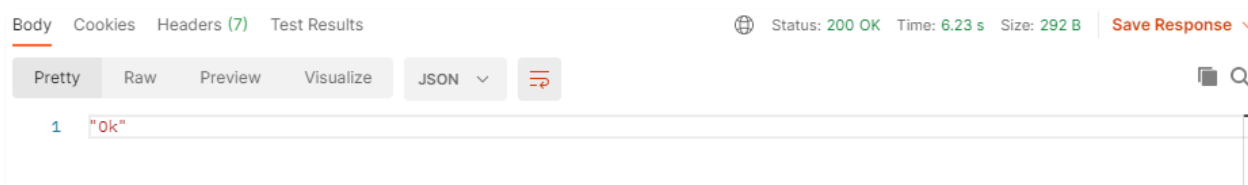
GET {{BaseURL}}/api/v2/enterpriseapi/statuscheck

- **Authentication Header:**



KEY	VALUE	DESCRIPTION	...	Bulk Edit	Presets
☒ EnterpriseApiKey ⓘ	fc5c3939-e68e-4e08-95a0-44830c38d088				
☒ Postman-Token ⓘ	<calculated when request is sent>				
☒ Host ⓘ	<calculated when request is sent>				

- **Response:**



Body	Cookies	Headers (7)	Test Results
Status: 200 OK Time: 6.23 s Size: 292 B Save Response			
Pretty Raw Preview Visualize JSON			
1 "Ok"			

Note: All API keys generated by Enterprise or FTK Central will be produced in the same format as displayed in the above images.

Using Active Directory (AD) authentication

To use the Active Directory (AD) authentication when making API calls, follow the general steps provided below.

Prerequisites: Before using AD authentication, ensure the following configurations are made in the config file:

Property Name	Value	Description
UseAD	1	This property must be set to 1 to enable Active Directory (AD) authentication.
EnabledADEnterpriseApi	true	This property must be set to true to allow the AD Enterprise API.

Steps:

Use the following endpoint to check the status of the API with AD authentication enabled:

- Request URL:**

GET ▼ `{{BaseURL}}/api/v2/enterpriseapi/statuscheck`

- Authorization:**

Params **Authorization** Headers (7) Body Scripts Settings

Auth Type
NTLM Authentication [Beta] ▼

The authorization header will be automatically generated when you send the request. Learn more about [NTLM Authentication \[Beta\]](#) authorization.

ⓘ Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about [variables](#).

Username
{{username}}

Password
{{password}} ⚠

- Response:**

Body Cookies Headers (10) Test Results 200 OK

{ } JSON ▼ ▶ Preview 🔗 Visualize ▼

1 "Ok"

© Exterro, Inc. All rights reserved.

www.exterro.com

11

Identification

Every object within the service contains an identifying integer that the API will use to target specific objects. These identifiers are supplied within the path and body of the HTTP request to denote which object will be targeted. Objects with identifiers include cases, evidence objects, custodians, labels, and jobs.

An example of the case and job identifiers in an URL is provided below:

```
https://localhost:4443/api/v2/enterpriseapi/core/{caseid}/getjobstatus/{jobid}
```

Pagination

The Enterprise API makes use of pagination in certain endpoints. Pagination is the method of producing a paging system and determining which page to pass back when a HTTP request is received. The number of objects per page (**pageSize**) and the target page are supplied to the API which then translates these values into the objects that will be returned.

Upon returning JSON from the API when using an API call with pagination, the return JSON will contain keys **totalCount** and entities to provide information on the total amount of objects that are available. Thus, the maximum page is the **totalCount/pageSize** floored (rounded down).

```
POST /api/v2/enterpriseapi/core/{caseid}/getobjectlist/{pageNumber}/{pageSize}
```

- **Input parameters:**

```
{
  "columns": [
    {
      "attribute": {
        "attributeUniqueName": "string",
        "isColumnSetMember": true,
        "description": "string",
        "displayName": "string",
        "dataType": 1,
        "productType": 0,
        "isSystemField": true,
        "isReadOnly": true,

```

```
"isGridEditable": true,
"isCustomField": true,
"isMappable": true,
"isFilterable": true,
"isBurnable": true,
"isAutoTextField": true,
"uiLayout": 0,
"isDefault": true,
"multiLine": true,
"maxLength": 0,
"isCategory": true,
"hasMetaDataValue": true,
"isVirtual": true,
"isLookup": true,
"isViewable": true,
"columnID": 0,
"isProducible": true,
"state": 0,
"id": 0,
"lastModifiedDate": "2021-05-25T08:46:52.262Z",
"lastModifiedBy": 0,
"hasSeqID": true,
"columnGUID": "00000000-0000-0000-0000-000000000000",
"columnClass": 0
},
"sort": 0,
"sortPriority": 0
}
],
"filter": {},
"objectId": 0
}
```

- **Enum - Product Type**

Product Type	Value
BrandNames	0
SummationMobile	1
SummationPro	2
EDiscovery	4
CIRT	8
SummationExpress	16
LAB	32
Insight	64
ResolutionOne	128
SummationReader	256
FtkSummation	512
ADRTK	1024
All	1847

- **Response:**

```
{
  "entities": [
    {
      "id": 10,
      "metaData": [
        {
          "clientProperties": {
            "$id": "1"
          },
          "displayValue": null,
          "hasIDs": false,
          "customColumn": null,
          "staticAttributeUniqueName": "ObjectFiles_FSFileClass",
          "value": null,
          "valueChanged": false
        },
        {
          "clientProperties": {
```

```
    "$ref": "1"
  },
  "displayValue": null,
  "hasIDs": false,
  "customColumn": null,
  "staticAttributeUniqueName": "ObjectID",
  "value": 10,
  "valueChanged": false
},
{
  "clientProperties": {
    "$ref": "1"
  },
  "displayValue": "2022-10-31T06:52:49.153",
  "hasIDs": false,
  "customColumn": null,
  "staticAttributeUniqueName": "LastModifiedDate",
  "value": "2022-10-31T06:52:49.153",
  "valueChanged": false
}
],
"appliedLabelIds": null,
"fileType": 0,
"listPosition": 0,
"hitCount": 0,
"lastModifiedDate": "2022-10-31T06:52:49.153",
"terms": null,
"childrenCount": 0,
"childEvidenceItems": null
}
],
"totalCount": 1
}
```

- **Response – File Types**

File Type - Details	Values
Graphic	0
PaperDoc	1
Email	2
EDoc	3
Volatile	4
Transcript	5
Note	6
Exhibit	7
Pleadings	8
RegularFile	9
Container	10
ThreatResult	11

Filtering

Filters are available in multiple API calls and are used to restrict a dataset for the procedure. Example usage of filters can be found in the agent, evidence browsing and export sections. Each filter is comprised of a column type, an attribute to compare against, a comparison type, and values to compare against the attribute. Moreover, multiple filters can be combined with AND/OR logical operators to create more complex filtering options.

The filter (JSON) will be used by the API to construct a filter in the service to be used while obtaining data.

A list of the possible filtering attributes can be obtained by making a **GET** request to get all attributes which returns all attributes and corresponding features.

Examples of file category and file name filters are provided below:

```
{
  "$type": "ADG.Service.Interfaces.DataContracts.Filtering.Grid.GridColumnFilter,
    ADG.Service.Interfaces",
  "staticAttributeName": "ObjectFiles_FileCategory",
  "mode": "Includes",
  "values": [0, ] ## All Categories
}
```

```
{
  "$type": "ADG.Service.Interfaces.DataContracts.Filtering.Grid.StringColumnFilter,
    ADG.Service.Interfaces",
  "staticAttributeName": "ObjectName",
  "operator": "StartsWith",
  "operand": "S",
}
```

```
{
  "$type": "ADG.Service.Interfaces.DataContracts.Filtering.BinaryOperatorFilter,
    ADG.Service.Interfaces",
  "operator": "AND",
  "left": {
    ## First filter.
  },
  "right": {
    ## Second filter.
  }
}
```

Each of the filter types allows for either string or integer input for the operator. The operators available for each filter are provided below:

- **GridColumnFilter Operators**

0 - Includes
1 - Excludes

- **GridColumnComparisonFilter Operators**

0 - GreaterThan
1 - GreaterThanEqualTo
2 - LessThan
3 - LessThanEqualTo
4 - EqualTo
5 - NotEqualTo

- **StringColumnFilter Operators**

0 - EqualTo
1 - NotEqualTo
2 - Contains
3 - StartsWith
4 - EndsWith

1 Cases

1.1 Create Case

This API is used to create a case.

POST `/api/v2/enterpriseapi/core/createcase`

Input Request:

- **Body Parameters** (*application/JSON format*)

The following parameters are **Mandatory**:

Name	Type	Description
Name	String	Provide the Name for the case.
ftkCaseFolderPath	String	Provide the FTK Case Folder Path for the Case
responsiveFilePath	String	Provide the Job Path for the case.

Example:

```
{
  "name": "Create Case Enterprise API",
  "description": "Case Created From Enterprise API",
  "ftkCaseFolderPath": "\\172.31.68.191\\ProjectData\\Cases",
  "responsiveFilePath": "\\172.31.68.191\\ProjectData\\Jobs",
  "CustodianIDs":
    ["f487d168-e38e-4681-a542-94956f54abbf","117b8f88-79e9-4030-8b57-e0cb4786753b"]
}
```

The following parameters are **Optional**:

Name	Type	Description
CustodianIds	List<string>	Provide the Custodian ID (Guid) for the case.
description	String	Provide the Description for the case.

Output Response:

- **Status Code – 200**

Response	Type	Description
("Created CaseId: <CASE_ID>")	String	The Case ID will be generated here.

Notes:

- The user must enter only the Custodian ID in the attribute **CustodianIds: ["VALUE"]** to map custodians to the case. You can add multiple custodians using commas as separators.
- Sending requests in the below-listed scenarios will result in the following error responses:

- **When the user tries to duplicate a case name, the below exception will be displayed:**

```
{"exceptionMessage":"Case Name - <CASE_NAME> already exists. Please provide an alternative name.", "exceptionType":"System.ApplicationException", "message":"An error has occurred."}
```

- **Without a case name:**

```
{"exceptionMessage":"Case name is required", "exceptionType":"System.ApplicationException", "message":"An error has occurred."}
```

- **With an invalid case name (consisting of special characters):**

```
{"exceptionMessage":"Error creating case: CaseId : 0, CaseName : CaseName-Test!@#%^&*()_+[]-=_2023-11-07_11.10.01: Illegal characters in path.; Error number: 36099fca-6c80-4a65-8a1d-47406227a4e9", "exceptionType":"System.ServiceModel.FaultException", "message":"An error has occurred."}
```

- **Without a case path:**

```
{"exceptionMessage":"Case folder path is required", "exceptionType":"System.ApplicationException", "message":"An error has occurred."}
```

- **With an invalid case path:**

```
{"exceptionMessage":"Please enter a valid Case Folder path", "exceptionType":"System.ApplicationException", "message":"An error has occurred."}
```

- **Without a responsiveFilePath:**

```
{"exceptionMessage":"Job data path is required,Please enter a valid Case Folder path","exceptionType":"System.ApplicationException","message":"An error has occurred."}
```

- **With an invalid responsiveFilePath:**

```
{"exceptionMessage":"Please enter a valid Job data path,Please enter a valid Case Folder path","exceptionType":"System.ApplicationException","message":"An error has occurred."}
```

1.2 Get Case Details

This API endpoint enables you to retrieve detailed information about a specific case by providing its unique identifier (Case ID) as a path parameter.

Get `{{Base_URL}}api/v2/enterpriseapi/cases?id=<VALUE>`

Input Request:

- **Path Parameter:**

The following parameter is **Mandatory**:

Name	Type	Description
id	long	Provide the unique identifier (Case ID) for which the details are to be retrieved. Only one Case ID can be provided in the path parameter.

Output Response:

- **Status Code – 200:** Indicates a successful retrieval of case details.

Response Parameters:

Response	Type	Description
caseName	string	Displays the name of the selected case.
caseID	long	Displays the unique identifier of the selected case.
casePath	string	Displays the folder path of the case.
jobPath	string	Displays the path to job data associated with the case.
createdByUsername	string	Displays the username of the user who created the case.
createdByID	long	Displays the user ID of the user who created the case.
totalSize	string	Displays the total size of the case.
totalObjects	long	Displays the total number of objects associated with the case.
creationDate	DateTime	Displays the date when the case was created.
accessedDate	DateTime	Displays the date when the case was last accessed.
modifiedDate	DateTime	Displays the date when the case was last modified.
displayTimezone	string	Displays the timezone selected during case creation.
databaseServer	string	Displays the database server used to save the case.
indexStatus	string	Indicates the indexing status of objects in the case.
description	string	Displays the description of the case.
assignedUsers	List<CasesAssignedUsers>	Lists users assigned to the case.
username	string	Displays the username of the user associated with the case.
firstName	string	Displays the first name of the user associated with the case.
lastName	string	Displays the last name of the user associated with the case.
email	string	Displays the email address of the user associated with the case.

Notes:

- **Retrieval Limitation:** The API allows retrieval of only one case detail per request.
- **Error Handling:**
 - **Invalid Case ID:** If an invalid case ID is provided, the API will return the following alert message:

```
{  
  "exceptionMessage": "Invalid Case ID.",  
  "exceptionType": "System.ApplicationException",  
  "message": "An error has occurred."  
}
```

- **Empty Value:** In case of an empty value, the API response will include the following message:

```
{  
  "exceptionMessage": null,  
  "exceptionType": null,  
  "message": "The request is invalid."  
}
```

1.3 Delete Case

This API endpoint enables the deletion of a case by providing either the Case ID or Case Name.

Delete `{{Base_URL}}api/v2/enterpriseapi/cases?id=<VALUE>`

Input Request:

- **Body Parameter** (*application/JSON format*):

The following parameter is Mandatory:

Name	Type	Description
id	long	Specify the unique identifier (Case ID) to delete the case. Only one case can be deleted at a time by specifying its unique identifier (Case ID).

Output Response:

- **Status Code – 200:** Indicates a successful deletion.

Upon successful deletion, the response will contain the following success message:

```
"Case has been deleted successfully."
```

Note:

- **Error Handling:**
 - **Invalid Case ID:** If an invalid case ID is provided, the API will return the following alert message:

```
{
  "exceptionMessage": "Invalid Case ID.",
  "exceptionType": "System.ApplicationException",
  "message": "An error has occurred."
}
```

2 Custodians

2.1 List Custodian

This API endpoint retrieves a list of custodian details.

Get `{{Base_URL}}api/v2/enterpriseapi/datasources/custodians`

Input Request:

- **Path Parameter** (*application/JSON format*):

The following parameter is **Optional**:

Name	Type	Description
Page	integer	Specify the page number from the total pages to retrieve custodian details. Example: <code>{{Base_URL}}api/v2/enterpriseapi/datasources/custodians?page=1</code>

Output Response:

- **Status Code – 200:** Indicates a successful response with the requested data.

Response Parameters:

Name	Type	Description
page	int	Displays the current page number of the results.
totalPages	int	Displays the total number of pages available.
totalRecords	long	Displays the total number of records across all pages.
currentPageRecords	int	Displays the number of records on the current page.
custodianId	Guid	Displays the GUID of the custodian.
firstName	string	Displays the first name of the custodian.
lastName	string	Displays the last name of the custodian.
middleInitial	string	Displays the middle initial of the custodian.
emailAddress	string	Displays the email address of the custodian.
createdDate	DateTime	Displays the date when the custodian was created.
createdByName	string	Displays the username of the user who created the custodian.
lastModifiedDate	DateTime	Displays the date when the custodian was last updated.
username	string	Displays the username associated with the custodian.
domain	string	Displays the domain associated with the custodian.
activeDirectoryId	Guid	Displays the Active Directory ID of the custodian.
profileImage	byte[]	Displays the profile image of the custodian.
employeeId	string	Displays the employee ID of the custodian.
custodianCases	IQueryable<string>	Displays a list of case names associated with the custodian, along with their IDs.
custodianHolds	IQueryable<string>	Displays a list of hold names associated with the custodian, along with their IDs.
isGroupMailBox	bool	Indicates whether the custodian is associated with a group mailbox (Teams).
oneDriveSiteUrl	string	Displays the OneDrive site URL associated with the custodian.
custodianCasesCount	long	Displays the total count of cases associated with the custodian.
custodianHoldsCount	long	Displays the total count of holds associated with the custodian.

Notes:

- **Pagination Details:**

- *Pagination details will be displayed in the response before the custodian details.*
- *By default, in the absence of pagination in the path parameter, the response will display the details of the last 10 custodians created.*
- *Users can check the total pages and records in the response and retrieve the details of custodians using page numbers.*

- **Error Handling:**

- **Invalid Page Number:** For an invalid page number, the API will return the following alert message:

```
{  
  "exceptionMessage": "Invalid page number : <Invalid Page Number>",  
  "exceptionType": "System.ApplicationException",  
  "message": "An error has occurred."  
}
```

2.2 List Custodian By ID

This API endpoint enables users to retrieve custodian details by specifying the custodian ID (GUID).

Get `{{Base_URL}}api/v2/enterpriseapi/datasources/custodians?id=<VALUE>`

Input Request:

- **Path Parameter:**

The following parameter is **Mandatory**:

Name	Type	Description
id	string	Provide the custodian ID (GUID) to get the details. Only one custodian detail can be retrieved by specifying the custodian ID (GUID).

Output Response:

- **Status Code – 200:** Indicates a successful retrieval of custodian details by either custodian ID or Username.

Response Parameters:

Name	Type	Description
custodianId	Guid	Displays the GUID of the custodian.
firstName	string	Displays the first name of the custodian.
lastName	string	Displays the last name of the custodian.
middleInitial	string	Displays the middle initial of the custodian.
emailAddress	string	Displays the email address of the custodian.
createdDate	DateTime	Displays the date when the custodian was created.
createdByName	string	Displays the username of the user who created the custodian.
lastModifiedDate	DateTime	Displays the date when the custodian was last updated.
username	string	Displays the username associated with the custodian.
domain	string	Displays the domain associated with the custodian.
activeDirectoryId	Guid	Displays the Active Directory ID of the custodian.
profileImage	byte[]	Displays the profile image of the custodian.
employeeId	string	Displays the employee ID of the custodian.
custodianCases	IQueryable<string>	Displays a list of case names associated with the custodian, along with their IDs.
custodianHolds	IQueryable<string>	Displays a list of hold names associated with the custodian, along with their IDs.
isGroupMailBox	bool	Indicates whether the custodian is associated with a group mailbox (Teams).
oneDriveSiteUrl	string	Displays the OneDrive site URL associated with the custodian.
custodianCasesCount	long	Displays the total count of cases associated with the custodian.
custodianHoldsCount	long	Displays the total count of holds associated with the custodian.

2.3 Delete Custodians

This API Endpoint is used to delete the Custodians.

Delete `{{Base_URL}}api/v2/enterpriseapi/datasources/custodians?id=<VALUE>`

Input Request:

- **Path Parameter**

The following parameter is **Mandatory**:

Name	Type	Description
id	string	Provide the Custodian ID (GUID) . Only one custodian can be deleted at a time by specifying its ID (GUID).

Output Response:

- **Status Code – 200:** Indicates a successful deletion of custodians.

Upon successful deletion, the response will contain the following success message:

```
"Custodians have been deleted successfully."
```

Notes:

- **Deleting Custodian details:**
 - Deleting a custodian associated with Litigation Holds, Collections, and Groups will result in the deletion of any associated jobs. Moreover, for groups, the custodian will be removed from the group as well.
- **Error Handling:**
 - **Invalid Custodian ID:** For an invalid custodian ID, the API will return the following alert message:
 - **Deleting an already deleted custodian:** For an attempt to delete a custodian that has already been deleted, the API will return the following exception message:

```
{
  "exceptionMessage": "Invalid Custodian ID.",
  "exceptionType": "System.ApplicationException",
  "message": "An error has occurred."
}
```

3 Targets

3.1 List Target

This API Endpoint lists the target details.

Get `{{Base_URL}}api/v2/enterpriseapi/datasources/targets`

Input Request:

- **Path Parameter:**

The following parameter is **Optional**:

Name	Type	Description
Page	integer	Provide the Page number from the total pages to get the target details. Example: <code>{{Base_URL}}api/v2/enterpriseapi/datasources/targets?Page=1</code>

Output Response:

- **Status Code – 200:** Indicates a successful retrieval of target details.

Response Parameters:

Name	Type	Description
page	int	Displays the current page number of the results.
totalPages	int	Displays the total number of pages available.
totalRecords	long	Displays the total number of records across all pages.
currentPageRecords	int	Displays the number of records on the current page.
computerId	Guid	Displays the unique identifier of the computer target.
computerName	string	Displays the name of the computer target.
computerDescription	string	Displays the description of the computer target.
createdDate	DateTime	Displays the date when the computer target was created.
createdBy	long	Displays the user ID of the creator of the computer target.
isDeleted	bool	Displays a flag indicating whether the computer target has been deleted.
deletionDate	DateTime	Displays the date when the computer target was deleted.
deletedBy	long	Displays the username of the user who deleted the computer target.
canPhoneHome	bool	Displays the phone home status of the computer target.
agentId	Guid	Displays the ID of the agent installed on the computer target, if applicable.
agentVersion	string	Displays the version of the agent installed on the computer target, if applicable.
agentLastContacted	DateTime	Displays the last contact date of the agent installed on the computer target, if applicable.
agentIsTemporary	bool	Displays a flag indicating if the agent installed on the computer target is temporary.
agentOperatingSystem	string	Displays the operating system of the computer target's agent, if applicable.
processorName	string	Displays the name of the processor of the computer target.
createdByType	int	Displays the type of creator of the computer target.
isAlive	bool	Displays a flag indicating whether the computer target is currently active or alive.

Name	Type	Description
groups	string	Displays any groups to which the computer target is mapped.
hasPersonAssociation	bool	Displays a flag indicating if the computer target is associated with any custodians.
activeDirectoryStatus	string	Displays the status of the computer target in the Active Directory.
createdByUsername	string	Displays the username of the user who created the computer target.

Notes:

- **Pagination Details:**

- The Pagination details will be displayed in the response before the target details.
- By default, in the absence of pagination in the path parameter, the response will display the details of the last 10 custodians created.
- You can check the total pages and records in response and get the details of targets using page numbers.

- **Error Handling:**

- **Invalid Page Number:** For an invalid page number, the API will return the following alert message:

```
{  
  "exceptionMessage": "Invalid page number : <Invalid Page Number>99891",  
  "exceptionType": "System.ApplicationException",  
  "message": "An error has occurred."  
}
```

3.2 List Target By ID

This API Endpoint lists the target details by Target ID.

Get `{{Base_URL}}api/v2/enterpriseapi/datasources/targets?id=<VALUE>`

Input Request:

- **Path Parameter**

The following parameter is **Mandatory**:

Name	Type	Description
id	string	Provide the Target ID to get the details. Only one target detail can be retrieved by specifying the target ID.

Output Response:

- **Status Code – 200:** Indicates successful retrieval of target details by Target ID.

Response Parameters:

Name	Type	Description
computerId	Guid	Displays the unique identifier of the computer target.
computerName	string	Displays the name of the computer target.
computerDescription	string	Displays the description of the computer target.
createdDate	DateTime	Displays the date when the computer target was created.
createdBy	long	Displays the user ID of the creator of the computer target.
isDeleted	bool	Displays a flag indicating whether the computer target has been deleted.
deletionDate	DateTime	Displays the date when the computer target was deleted.
deletedBy	long	Displays the username of the user who deleted the computer target.
canPhoneHome	bool	Displays the phone home status of the computer target.
agentId	Guid	Displays the ID of the agent installed on the computer target, if applicable.

Name	Type	Description
agentVersion	string	Displays the version of the agent installed on the computer target, if applicable.
agentLastContacted	DateTime	Displays the last contact date of the agent installed on the computer target, if applicable.
agentIsTemporary	bool	Displays a flag indicating if the agent installed on the computer target is temporary.
agentOperatingSystem	string	Displays the operating system of the computer target's agent, if applicable.
processorName	string	Displays the name of the processor of the computer target.
createdByType	int	Displays the type of creator of the computer target.
isAlive	bool	Displays a flag indicating whether the computer target is currently active or alive.
username	string	Displays the username of the user who created the computer target.
groups	string	Displays any groups to which the computer target is mapped.
hasPersonAssociation	bool	Displays a flag indicating if the computer target is associated with any custodians.
activeDirectoryStatus	string	Displays the status of the computer target in the Active Directory.
createdByUsername	string	Displays the username of the user who created the computer target.

3.3 Create Target

This API Endpoint is to create a Target by Target HostName/Target IP.

Post `{{BASE_URL}}/api/v2/enterpriseapi/datasources/targets`

Input Request:

- **Body Parameters** (*application/JSON format*):

The following parameters are **Mandatory**:

Name	Type	Description
ComputerName	string	Provide the target hostname and target IP to create a new target. Only one target can be created at a time.
AgentOS	string	Specify the operating system (OS) you want to create a target against by providing one of the following values: • Windows • Linux Note: MAC agent cannot be created through the API Endpoint.

The following parameter is **Optional**:

Name	Type	Description
ComputerDescription	String	Provide a description of the target.

Request Example:

```
{
  "ComputerName": "<Target IP/Target Hostname>",
  "AgentOS": "<windows/linux>",
  "ComputerDescription": "<Value>"
}
```

Output Response:

- **Status Code – 200:** Indicates successful creation of the target.

Response Parameters:

Name	Type	Description
computerName	string	Displays the name of the computer associated with `<Value used in ComputerName paramater>`.
computerDescription	string	Displays the description of the computer.
canPhoneHome	bool	Displays the phone home status of the computer.
createdDate	DateTime	Displays the date when the computer was created.
agentLastContacted	DateTime	Displays the last contact date of the agent installed on the computer, if applicable.
agentVersion	string	Displays the version of the agent installed on the computer, if applicable.
agentIsTemporary	bool	Displays a flag indicating whether the installed agent is temporary.
createdByUsername	string	Displays the username of the user who created the computer.
createMethod	string	Displays the method used to create the computer.
agentOS	string	Displays the operating system of the agent installed on the computer.
hasPersonAssociation	bool	Displays a flag indicating if the computer is associated with any custodians.
isDeleted	bool	Displays a flag indicating whether the computer has been deleted.
groups	string	Displays any groups to which the computer is mapped.
activeDirectoryStatus	bool	Displays the status of the computer in the active directory.
ipAddressLastContacted	string	Displays the flag indicating the last contact status of the computer.

3.4 Delete Target

This API Endpoint is used to delete the Target by target ID.

Delete `{{Base_URL}}api/v2/enterpriseapi/datasources/targets?id=<VALUE>`

Input Request:

- **Path Parameter:**

The following parameter is **Mandatory**:

Name	Type	Description
id	string	Provide the Target ID to delete. Only one target can be deleted at a time by specifying its ID (GUID). Note: Deleting a target associated with collection jobs would not retain them when resubmitting the existing jobs.

Output Response:

- **Status Code – 200:** Indicates successful deletion of the target.

Upon successful deletion, the response will contain the following success message:

```
"Target has been deleted successfully."
```

Notes:

- **Error Handling:**
 - **Invalid Target ID:** For an invalid target ID, the API will return the following alert message:
 - **Deleting an already deleted target:** For an attempt to delete a target that has already been deleted, the API will return the following exception message:

```
{
  "exceptionMessage": "Invalid Target ID.",
  "exceptionType": "System.ApplicationException",
  "message": "An error has occurred."
}
```

4 Jobs

4.1 List Jobs

This API Endpoint lists all the available Jobs from the Job Queue.

Get `{{BASE_URL}}api/v2/enterpriseapi/jobs`

Input Request:

- **Path Parameter:**

The following parameter is optional

Name	Type	Description
Page	integer	Provide the Page number from the total pages to get the job details. Example: <code>{{BASE_URL}}api/v2/enterpriseapi/jobs?Page=1</code>

Output Response:

- **Status Code – 200:** Indicates successful retrieval of all available Jobs from the Job Queue.

Response Parameters:

Name	Type	Description
page	int	Displays the current page number of the results.
totalPages	int	Displays the total number of pages in the job queue.
totalRecords	long	Displays the total number of job records present in the job queue.
currentPageRecords	int	Displays the number of jobs present in the current page.
jobType	string	Displays the type of the job.
jobState	string	Displays the state of the job.
caseId	long	Displays the ID of the case associated with the job.
userId	long	Displays the ID of the user who triggered the job.
userName	String	Displays the username of the user who triggered the job.
dateStarted	DateTime	Displays the start date and time of the job.
timeElapsed	String	Displays the duration taken to complete the job.

Name	Type	Description
dateResultsUpdated	DateTime	Displays the date and time when the job result was last updated in the job queue.
otherJobData	String	Displays additional data related to the job type.
jobName	String	Displays the name of the job.
state	String	Displays the status of the job.
jobId	long	Displays the ID of the job.
lastModifiedDate	DateTime	Displays the date and time when the job was last modified.
lastModifiedBy	long	Displays the ID of the user who last modified the job.
processingMachine	string	Displays the processing machine used to process the job.
casePath	string	Displays the path of the case on which the job is processed.
submittedDate	DateTime	Displays the date and time when the job was submitted.
errors	long	Displays the number of errors encountered during the job processing.
totalDocumentCount	long	Displays the total count of documents (objects) the job is triggered for.
completedDocumentCount	long	Displays the count of documents (objects) successfully completed by the job.

Note:

- **Pagination Details:**

- Pagination details will be displayed in the response before the job details.
- By default, in the absence of pagination in the path parameter, the response will display the details of the last 10 custodians created.
- You can check the total pages and records in the response and retrieve the details of jobs using page numbers.

4.2 List Job Types

This API Endpoint lists all the available Job Types.

Get `{{BASE_URL}}api/v2/enterpriseapi/jobs/types`

Input Request:

- **Path Parameters:** *Not applicable*

Output Response:

- **Status Code - 200:** Indicates successful retrieval of all available Job Types.

Response Parameters:

Name	Type	Description
Unknown	enum JobType - string	Indicates that the job status is initially unknown upon creation.
Import	enum JobType - string	Triggered when a user performs an import job.
Production	enum JobType - string	Triggered when a user performs an export job (production export).
ReviewSet	enum JobType - string	Triggered when batches are created for a case from Batch Administration.
FolderAssignment	enum JobType - string	Triggered when a user performs bulk labeling.
DeleteProduction	enum JobType - string	Triggered when a user deletes an export job.
BulkCoding	enum JobType - string	Triggered when a user performs bulk coding from the context menu.
DeleteSummaries	enum JobType - string	Triggered when a user deletes objects from the context menu; set Product Type in config file to eDiscovery.

Name	Type	Description
Search	enum JobType - string	Represents a generic search job.
TBR	enum JobType - string	Represents a TBR (To Be Released) job.
Export	enum JobType - string	Triggered when a user performs an export job.
DeleteExport	enum JobType - string	Triggered when a user deletes an export.
AdvancedSearchReport	enum JobType - string	Triggered when a user performs an advanced search report.
SallyProcessing	enum JobType - string	Represents a Sally processing job.
DtSearchIndexing	enum JobType - string	Triggered when a user performs case-level DTSearch indexing.
PredictiveCoding	enum JobType - string	Represents a predictive coding job.
GlobalReplace	enum JobType - string	Represents a global replace job.
SearchReport	enum JobType - string	Triggered when a user performs a search term report.
ConfidenceScoreCalculation	enum JobType - string	Represents a confidence score calculation job.
ExportToCSV	enum JobType - string	Triggered when exporting all objects to a CSV file.
KFFProcessing	enum JobType - string	Triggered when processing KFF (Known File Filter).
AddHashToKFF	enum JobType - string	Triggered when importing hashes from System Management to KFF.

Name	Type	Description
OCR	enum JobType - string	Represents an OCR (Optical Character Recognition) job.
AddEvidenceToBookmark	enum JobType - string	Triggered when adding evidence to a bookmark.
RemoveEvidenceFromBookmark	enum JobType - string	Triggered when removing evidence from a bookmark.
CreateBookmarkReport	enum JobType - string	Triggered when generating a bookmark report.
MassAction	enum JobType - string	Represents a mass action job.
Unitization	enum JobType - string	Triggered when performing unitization to an object from Viewer pane.
CopyEvents	enum JobType - string	Triggered when copying events.
LiveSearch	enum JobType - string	Triggered when creating a Live search in the review.
SearchAndAssignFolder	enum JobType - string	Represents a search and assign folder job.
BelkaSoftWrapper_deprecated	enum JobType - string	Represents a deprecated BelkaSoft wrapper job.
BulkEvidenceUpdate	enum JobType - string	Triggered when updating bulk evidence.
CompulsionWrapperJob	enum JobType - string	Represents a compulsion wrapper job.
SearchAndAlertJob	enum JobType - string	Represents a search and alert job.
ImageRecognition	enum JobType - string	Represents an image recognition job.

Name	Type	Description
AddEvidenceJob	enum JobType - string	Indicates the status of evidence added and progressing state in detail.
VideoThumbNailProcessorJob	enum JobType - string	Represents a video thumbnail processor job.
SqlLiteProcessorJob	enum JobType - string	Represents a SQLite processor job.
BulkAddUpdateEvidenceJob	enum JobType - string	Triggered when bulk adding or updating evidence.
ReIndexProcessorJob	enum JobType - string	Triggered when reindexing a specific case.
GenericBusinessJob	enum JobType - string	Represents a generic business job.
SearchCountReport	enum JobType - string	Triggered when generating a search term report.
ExportSet	enum JobType - string	Triggered when exporting a set of objects.
TBRCreation	enum JobType - string	Triggered when assigning DOCID from the context menu.
SearchExcerptReport	enum JobType - string	Represents a search excerpt report job.
TimeLineExportToExcel	enum JobType - string	Triggered when exporting Timeline events to Excel from Timeline view.
FTKDetailReport	enum JobType - string	Triggered when generating an FTK detail report.
ListIndexWordsJob	enum JobType - string	Represents a list index words job.
RegistryFilesJob	enum JobType - string	Represents a registry files job.

Name	Type	Description
EmailThreadingAggregator	enum JobType - string	Represents an email threading aggregator job.
BreadViewerImaging	enum JobType - string	Represents a Bread Viewer imaging job.
FolderMonitorJob	enum JobType - string	Represents a folder monitor job.
FtkReportsGenerator	enum JobType - string	Represents an FTK reports generator job.
EmailSender	enum JobType - string	Represents an email sender job.
ConnectorJob	enum JobType - string	Represents a connector job.
BulkBookMarkJob	enum JobType - string	Represents a bulk bookmark job.
CreateCaseJob	enum JobType - string	Represents a create case job.
LitHoldEmailHandlerJob	enum JobType - string	Represents a LitHold email handler job.
ListnerInformation	enum JobType - string	Represents a listener information job.
AppleFsParserWrapperJob	enum JobType - string	Represents an Apple FS parser wrapper job.
ExecuteSqlJob	enum JobType - string	Represents an execute SQL job.
BackupRestoreJob	enum JobType - string	Represents a backup restore job.
ConvertXmlToReport	enum JobType - string	Represents a convert XML to report job.

Name	Type	Description
ZipUnZip	enum JobType - string	Represents a zip unzip job.
TensorImageRecognition	enum JobType - string	Represents a TensorFlow text classification job.
ImageExtractionJob	enum JobType - string	Represents an image extraction job.
DatabaseParserJob	enum JobType - string	Represents a database parser job.
ListIndexWordsJob Managed	enum JobType - string	Represents a managed list index words job.
MultiSearchStatsJob	enum JobType - string	Represents a multi-search stats job.
ObjectFileImporterJob	enum JobType - string	Represents an object file importer job.
TensorImageTraining	enum JobType - string	Represents a tensor image training job.
DumpObjectFileJob	enum JobType - string	Represents a dump object file job.
FaceRecognitionJob	enum JobType - string	Represents a face recognition job.
EntityExtractionJob	enum JobType - string	Represents an entity extraction job.
AttachmentsMergeJob	enum JobType - string	Represents an attachments merge job.
AutoRedactionJob	enum JobType - string	Represents an auto redaction job.
ObjectColumnParser Processor	enum JobType - string	Represents an object column parser processor job.

Name	Type	Description
SentimentAnalysisJob	enum JobType - string	Represents a sentiment analysis job.
DeleteQuincPreviewCasesjob	enum JobType - string	Represents a delete Quinc preview cases job.
ReplacePDF	enum JobType - string	Represents a replace PDF job.
RestorePDF	enum JobType - string	Represents a restore PDF job.
RedactPDF	enum JobType - string	Represents a redact PDF job.
BrandPDF	enum JobType - string	Represents a brand PDF job.
CreateTabbedProduction	enum JobType - string	Represents a create tabbed production job.
CustomMergeProcessor	enum JobType - string	Represents a custom merge processor job.
ObjectAttributeCopyProcessor	enum JobType - string	Represents an object attribute copy processor job.
AbbyOcrProcessor	enum JobType - string	Represents an Abby OCR processor job.
HistoricalCaseSizeJob	enum JobType - string	Represents a historical case size job.
DeleteCasesJob	enum JobType - string	Represents a delete cases job.
ADDataSourceSyncJob	enum JobType - string	Represents an Active Directory data source sync job.
LegacyVolatileInsertJob	enum JobType - string	Represents a legacy volatile insert job.

Name	Type	Description
TensorFlowTextClassification	enum JobType - string	Represent the TensorFlow Text Classification.
TensorFlowTextClassificationTraining	enum JobType - string	Represents a TensorFlow text classification training job.
SyncOfflineDatabase	enum JobType - string	Represents a sync portable case job.
BulkDocumentConversion	enum JobType - string	Represents a bulk document conversion job.
IndexMetricJob	enum JobType - string	Represents an index metric job.
BulkPrint	enum JobType - string	Represents a bulk print job.
SqliteInsertProcessor	enum JobType - string	Represents a SQLite insert processor job.
RunFTKReport	enum JobType - string	Represents a run FTK report job.
BavariaImportJob	enum JobType - string	Represents a Bavaria import job.
DataVolumeReport	enum JobType - string	Represents a data volume report job.
DeduplicationEmailsReport	enum JobType - string	Represents a deduplication emails report job.
DeduplicationFilesReport	enum JobType - string	Represents a deduplication files report job.
AuditLogReport	enum JobType - string	Represents an audit log report job.
DumpWordListJob	enum JobType - string	Represents a dump word list job.

Name	Type	Description
ExecuteDNAPRTKJob	enum JobType - string	Represents an execute DNA PRTK job.
MessagePDFGenerator	enum JobType - string	Represents a message PDF generator job.
MessagingParserJob	enum JobType - string	Represents a messaging parser job.
MessageNativeGeneratorJob	enum JobType - string	Represents a message native generator job.
FolderMonitorClientJob	enum JobType - string	Represents a folder monitor client job.
SingleDocPrintJob	enum JobType - string	Represents a single document print job.
PasswordResetJob	enum JobType - string	Represents a password reset job.
MacSystemSummaryJob	enum JobType - string	Represents a Mac system summary job.
LabelImageAllocationJob	enum JobType - string	Represents a label image allocation job.
LegacyAgentJob	enum JobType - string	Represents a legacy agent job.
AutoMessageLabelJob	enum JobType - string	Represents an auto message label job.
ContainerExtraction	enum JobType - string	Represents a container extraction job.
CollectCaseStatistics	enum JobType - string	Represents a collect case statistics job.
FBFSFamilyProcessorJob	enum JobType - string	Represents an FBFS family processor job.

Name	Type	Description
ContactEntityMergeProcessor	enum JobType - string	Represents a contact entity merge processor job.
QviewCloudProcessorJob	enum JobType - string	Represents a Qview Cloud processor job
RunFTKHtmlReport	enum JobType - string	Represents a run FTK HTML report job.
UploadToAwsProcessor	enum JobType - string	Represents an upload to AWS processor job.
EDiscoveryFileScanJob	enum JobType - string	Represents an eDiscovery file scan job.
EnhancedInternetArtifactAnalysisJob	enum JobType - string	Represents an enhanced internet artifact analysis job.
GenericHierarchyJob	enum JobType - string	Represents a generic hierarchy job.
CreateProjectCaseJob	enum JobType - string	Represents a create project case job.
ProcessingErrorsReport	enum JobType - string	Represents a processing errors report job.
TensorVideoRecognition	enum JobType - string	Initiated when video recognition and tagging frames are performed.
EDiscoverySystemJob	enum JobType - string	Initiated for jobs related to eDiscovery system tasks.
CollectionReportJob	enum JobType - string	Automatically created when an agent scan job is triggered to generate a collection report.
EDiscoveryAgentScanJob	enum JobType - string	Triggered when an agent scan collection job is created for eDiscovery tasks.
QViewAuditLogReport	enum JobType - string	Initiated for generating audit log reports across multiple cases in QView.

Name	Type	Description
CrossCaseLiveFaceDetectionJob	enum JobType - string	Initiated when using image recognition to find similar faces across multiple cases.
CrossCaseSimilarObjectsJob	enum JobType - string	Initiated when using image recognition to find similar images across multiple cases.
ComputerReport	enum JobType - string	Triggered when exporting a list from a computer data source.
DeleteExternalEvidence	enum JobType - string	Initiated when deleting associated external evidence.
ProductionSetSizeProcessor	enum JobType - string	Initiated when calculating export sizes for productions.
BulkBookMarkObjectsJob	enum JobType - string	Job for bulk bookmarking objects based on specified criteria.
CreateEntityJob	enum JobType - string	Initiated when entities are created based on case objects.
SyncSharePointSubsites	enum JobType - string	Represents a sync SharePoint subsites job.
IndexMergeJob	enum JobType - string	Represents a case index merge job.
KFF Export	enum JobType - string	Represents a KFF export job.
KFF Object Assign To Bookmark	enum JobType - string	Represents a KFF object assign to bookmark job.
LoadSearch Report	enum JobType - string	Represents a load search report job.
Mac Agent Collection	enum JobType - string	Represents a Mac agent collection job.
Offline Agent Collection	enum JobType - string	Represents an offline agent collection job.

Name	Type	Description
Portable case export job	enum JobType - string	Represents a portable case export job.
Semantics21 Export	enum JobType - string	Represents a Semantics21 export job.
Similar Face Detection	enum JobType - string	Represents a similar face detection job.
Similar Image Detection	enum JobType - string	Represents a similar image detection job.
System Wide Collection Report	enum JobType - string	Represents a system-wide collection report job.
Timeline Data Processor	enum JobType - string	Represents a timeline data processor job
Timeline Reports	enum JobType - string	Represents a timeline reports job.
FTK Connect - Automation Status	enum JobType - string	Represents an FTK Connect automation status job

4.3 List Jobs By Job Type

This API Endpoint lists the Job details by Job Type.

Get `{{BASE_URL}}api/v2/enterpriseapi/jobs?jobtype=<VALUE>`

Input Request:

- **Path Parameters** (*application/JSON format*):

The following parameter is **Mandatory**:

Name	Type	Description
jobtype	string	List the details of the job by the 'Job Type'. Example: <pre>{{Base_URL}}api/v2/enterpriseapi/jobs?jobtype=AddEvidenceJob&page=6</pre> <pre>{{Base_URL}}api/v2/enterpriseapi/jobs?jobtype=Import&page=3</pre> Note: Users can get the job details for only one job type.

Output Response:

- **Status Code - 200:** Indicates successful retrieval of Job details by Job Type.

Response Parameters:

Name	Type	Description
page	int	Displays the current page number of the results.
totalPages	int	Displays the total number of pages in the job queue.
totalRecords	long	Displays the total number of job records present in the job queue.
currentPageRecords	int	Displays the number of jobs present in the current page.
jobType	string	Displays the type of the job.
jobState	string	Displays the state of the job.
caseId	long	Displays the ID of the case associated with the job.
userId	long	Displays the ID of the user who triggered the job.
userName	string	Displays the username of the user who triggered the job.
dateStarted	DateTime	Displays the start date and time of the job.
timeElapsed	string	Displays the duration taken to complete the job.
dateResultsUpdated	DateTime	Displays the date and time when the job result was last updated in the job queue.
otherJobData	string	Displays additional data related to the job type.
jobName	string	Displays the name of the job.
state	string	Displays the status of the job.
jobId	long	Displays the ID of the job.
lastModifiedDate	DateTime	Displays the date and time when the job was last modified.
lastModifiedBy	long	Displays the ID of the user who last modified the job.
processingMachine	string	Displays the processing machine used to process the job.
casePath	string	Displays the path of the case on which the job is processed.
submittedDate	DateTime	Displays the date and time when the job was submitted.
errors	long	Displays the number of errors encountered during the job processing.
totalDocumentCount	long	Displays the total count of documents (objects) the job is triggered for.
completedDocumentCount	long	Displays the count of documents (objects) successfully completed by the job.

Notes:

- **Pagination Details:**

- Pagination details will be displayed in the response before the job details.
- By default, in the absence of pagination in the path parameter, the response will display the details of the last 10 custodians created.
- You can check the total pages and records in the response and retrieve the details of jobs using page numbers.
- You can specify the required page number to filter the job details in the response.

4.4 List Job State

This API Endpoint lists all the available Job States.

Get `{{BASE_URL}}api/v2/enterpriseapi/jobs/states`

Input Request:

- **Body Parameters** (*application/JSON format*): **Not applicable**

Output Response:

- **Status Code – 200:** Indicates successful retrieval of all available Job States.

Response Parameters:

Name	Type	Description
"Unknown"	enum JobState - string	The initial state of a job when its status is unknown.
"Submitted"	enum JobState - string	The job has been submitted and is awaiting processing.
"InProgress"	enum JobState - string	The job is currently in progress.
"Completed"	enum JobState - string	The job has successfully completed.
"Canceled"	enum JobState - string	The job has been canceled by a user or system.
"Failed"	enum JobState - string	The job execution has failed.
"Cancelling"	enum JobState - string	The job is currently in the process of being canceled.
"CancelRequested"	enum JobState - string	A request to cancel the job has been submitted.

Name	Type	Description
"PauseRequested"	enum JobState - string	A request to pause the job has been submitted.
"Paused"	enum JobState - string	The job is currently paused.
"ResumeRequested"	enum JobState - string	A request to resume the paused job has been submitted.
"CompletedWithErrors"	enum JobState - string	The job completed with some errors.
"Deleted"	enum JobState - string	The job has been deleted and removed from the system.
"Interrupted"	enum JobState - string	The job execution was interrupted unexpectedly.

4.5 List Jobs By Job State

This API Endpoint lists the Job details by Job State.

Get `{{BASE_URL}}api/v2/enterpriseapi/jobs?jobstate=<VALUE>`

4.5.1 Input Request:

- **Path Parameters** (*application/JSON format*):

The following parameter is **Mandatory**:

Name	Type	Description
jobstate	string	List the details of the job by the 'Job Type'. Example: For Job Status - <pre>{{BASE_URL}}api/v2/enterpriseapi/jobs?jobstate=Completed</pre> For Job Status with Page numbering - <pre>{{Base_URL}}api/v2/enterpriseapi/jobs?jobstate=Inprogress&page=2</pre> Note: Users can retrieve the details of the job for a specific job type based on its status.

Output Response:

- **Status Code – 200:** Indicates successful retrieval of Job details by Job State.

Response Parameters:

Name	Type	Description
page	int	Specifies the current page number in the paginated results.
totalPages	int	Total number of pages available in the job queue.
totalRecords	long	Total number of job records present in the job queue.
currentPageRecords	int	Number of jobs present in the current page of results.
jobType	string	Type of the job being processed.
jobState	string	Current state of the job.
caseId	long	ID of the case associated with the job.
userId	long	ID of the user who triggered the job.
userName	string	Username of the user who triggered the job.
dateStarted	DateTime	Date and time when the job started processing.
timeElapsed	String	Duration taken to complete the job.
dateResultsUpdated	DateTime	Date when the job result was last updated in the queue.
otherJobData	String	Additional data related to the job type.
jobName	String	Name of the job.
state	String	Current status of the job.
jobId	long	Unique identifier of the job.
lastModifiedDate	DateTime	Date and time of the last modification made to the job.
lastModifiedBy	long	ID of the user who last modified the job.
processingMachine	String	Name of the processing manager used for the job.
casePath	String	Path of the case where the job is being processed.
submittedDate	DateTime	Date and time when the job was submitted for processing.
errors	long	Number of errors encountered during job processing.
totalDocumentCount	long	Total number of documents or objects associated with the job.
completedDocumentCount	long	Number of documents or objects successfully processed by the job.

Notes:

- **Pagination Details:**

- Pagination details will be displayed in the response before the job details.
- By default, in the absence of pagination in the path parameter, the response will display the details of the last 10 custodians created.
- You can check the total pages and records in the response and retrieve the details of jobs using page numbers.
- You can specify the required page number to filter the job details in the response.

4.6 List Jobs By Job ID

This API Endpoint lists the Job details by Job ID.

Get `{{BASE_URL}}api/v2/enterpriseapi/jobs?id=<VALUE>`

Input Request:

- **Path Parameters** (*application/JSON format*):

The following parameter is **Mandatory**:

Name	Type	Description
id	long	List the details of a specific job by its unique identifier. Example: <code>{{Base_URL}}api/v2/enterpriseapi/jobs?id=1</code>

Output Response:

- **Status Code – 200:** Indicates successful retrieval of Job details by Job ID.

Response Parameters:

Name	Type	Description
jobType	string	Displays the type of job.
jobState	string	Displays the current state of the job.
caseId	long	The ID of the case associated with the job.
userId	long	The ID of the user who triggered the job.
userName	string	The name of the user who triggered the job.
dateStarted	DateTime	The date and time when the job started processing.
timeElapsed	string	The duration taken to complete the job.
dateResultsUpdated	DateTime	The date and time when the job results were last updated or displayed in the job queue.
otherJobData	string	Additional data related to the job type.
jobName	string	The name of the job.
state	string	The current status of the job.
jobId	long	The unique identifier of the job.
lastModifiedDate	DateTime	The date and time of the last modification made to the job.
lastModifiedBy	long	The ID of the user who last modified the job.
processingMachine	string	The name or identifier of the processing manager used for the job.
casePath	string	The path of the case on which the job is being processed.
submittedDate	DateTime	The date and time when the job was submitted for processing.
errors	long	Indicates if any errors were encountered during the job processing.
totalDocumentCount	long	The total number of documents or objects processed or triggered by the job.
completedDocumentCount	long	The number of documents or objects successfully completed by the job

4.7 Cancel Job

This API Endpoint is used to Cancel the jobs that are in progress.

Post `{{Base_URL}}api/v2/enterpriseapi/jobs?id=<VALUE>`

Input Request:

- **Path Parameter:**

The following parameter is **Mandatory**:

Name	Type	Description
id	long	Allows users to cancel jobs by providing the unique identifier in the path parameter. Example: <code>{{Base_URL}}api/v2/enterpriseapi/jobs?id=1</code>

Note: Users are allowed to cancel collection/FTKC case-related jobs only if the status of the job is 'Pending' or 'In-Progress' status.

Output Response:

- **Status Code – 200:** Indicates successful cancellation of the job in progress.

Upon successful cancelation of jobs, the response will contain the following success message:

```
"Job cancelled successfully"
```

Notes:

- **Error Handling:**
 - **Invalid Jobs:** For an invalid job, the API will return the following alert message:
 - **Canceling an already canceled Job:** For an attempt to cancel a job that has already been canceled, the API will return the following exception message:

```
{  
  "exceptionMessage": "Invalid Target ID.",  
  "exceptionType": "System.ApplicationException",  
  "message": "An error has occurred."  
}
```

4.8 Delete Job

This API Endpoint is used to delete the Jobs by the Job ID.

Delete `{{Base_URL}}api/v2/enterpriseapi/jobs?id=<VALUE>`

Input Request:

- **Path Parameter:**

The following parameter is **Mandatory**:

Name	Type	Description
id	long	Provide the unique identifier in the path parameter to delete the jobs. Example: <code>{{Base_URL}}api/v2/enterpriseapi/jobs?id=1</code>

Note: Users can delete the collection/FTKC case-related jobs when in the following status:

- Cancelled
- Completed
- CompletedWithErrors
- Failed
- NotStarted
- Pending
- Not Started But Approved

Output Response:

- **Status Code – 200:** Indicates successful deletion of the job by Job ID.

Upon successful deletion of jobs, the response will contain the following success message:

```
"Job deleted successfully"
```

Notes:

- **Error Handling:**
 - **Invalid Jobs:** For an invalid job, the API will return the following alert message:
 - **Deleting an already deleted jobs:** For an attempt to delete a job that has already been deleted, the API will return the following exception message:

```
{  
  "exceptionMessage": "Invalid Target ID.",  
  "exceptionType": "System.ApplicationException",  
  "message": "An error has occurred."  
}
```

5 Collections

5.1 List Collection Templates

This API Endpoint lists all the Collection templates.

Get `{{Base_URL}}api/v2/enterpriseapi/agent/collection/templates`

Input Request:

- **Path Parameter:**

The following parameters are **optional**:

Name	Type	Description
page	int	The page number from the total pages to retrieve job details. Example: <code>{{BASE_URL}}api/v2/enterpriseapi/agent/collection/templates?Page=1</code>
totalPages	int	Total number of pages available in the job queue.
totalRecords	long	Total number of job records present in the job queue.
currentPageRecords	int	Number of jobs present in the current page.
filterTemplateId	Guid	GUID of the template displayed here.
PathURLContainsSS	bool	Indicates if the filter type includes 'PathURLContainsSS'.
Values	bool	Indicates if the filter type includes 'Values'.
Path	bool	Indicates if the filter type includes 'Path'.
IsFolder	bool	Indicates if the filter type includes 'IsFolder'.
IsRecursive	bool	Indicates if the filter type includes 'IsRecursive'.
IsRelative	bool	Indicates if the filter type includes 'IsRelative'.
Folder	string[]	Array of filter types that include 'Folder' and their values.
Value	bool	Indicates if the filter type includes 'Value'.
Relative	string[]	Array of filter types that include 'Relative' and their values.
Recursive	string[]	Array of filter types that include 'Recursive' and their values.
dataSourceType	enum	Displays the job data source type ID.

Name	Type	Description
createdDate	DateTime	The date when the template was created.
createdBy	long	The username of the template creator.
isInclusion	bool	Indicates if the template has an inclusion filter (true/false).
filterType	string	Displays the ID value of the filter type.
name	string	The name of the filter displayed here.

Output Response:

- **Status Code – 200:** Indicates successful retrieval of all Collection templates.

This API will return the response for the following job types:

- **File Scan:**
 - Filtered Collection
 - Full Disk Acquisition
- **Agent Scan:**
 - Software Inventory
 - Memory Analysis
 - Memory Acquisition
- **Reports Only:**
 - Filtered Collection
 - Full Disk Acquisition

Notes:

- **Pagination Details:**
 - Pagination details will be displayed in the response before the template details.
 - By default, in the absence of pagination in the path parameter, the response will display the details of the last 10 custodians created.
 - You can check the total pages and records in the response and retrieve the details of templates using page numbers.

Response Parameters:

Name	Type	Description
page	int	Displays the current page number.
totalPages	int	Displays the total number of pages.
totalRecords	long	Displays the total number of records.
currentPageRecords	int	Displays the number of records on the current page.
templateId	Guid	Displays the GUID of the template.
name	string	Displays the name of the template.
xmlOptions	string	Displays the XML options (Case and Job Details).
createdByName	string	Displays the name of the template creator.
createdDate	DateTime	Displays the date when the template was created.
description	string	Displays the description of the template.

5.2 Create Template

This API Endpoint is to create a collection template.

Post `{{BASE_URL}}api/v2/enterpriseapi/agent/collection/templates`

Input Request:

- **Body Parameters** (*application/JSON format*):

The following parameters are **Mandatory**:

Name	Type	Description
templateName	String	Provide the name of the Template.
JobType	string	Provide the Job Type ID for the Template.
JobExecutionMode	string	Provide the Execution Mode ID for the Template.
ProcessingOption	string	Provide the Processing Option ID for the Template.

Example:

```
{
  "templateName": "Template API 8.2 SP2",
  "caseId": "55",
  "CustodianIds": ["c2da9d7d-d7ad-4a87-8c99-9924f0550f44"],
  "TargetIds": [],
  "collectionfiltertemplateIds": ["1c037f8a-48f3-4ff9-9124-8b3def8f33e0"],
  "JobType": "0",
  "JobExecutionMode": "0",
  "ProcessingOption": "4"
}
```

The following parameters are **Optional**:

Name	Type	Description
collectionfiltertemplateId	string	Provide the Filter Template ID for a collection template to be created based on the given filters. Note: <i>If the value is not provided, the template will be created as a 'Full Disk Acquisition'.</i>
CustodianIds (or) TargetIds	Array<String>	Provide the custodian ID as the target for a collection or you can provide the Target GUID, Computer Name, or IP as the target for a collection. Note: <i>The Custodian value will be considered when you provide values for both the custodians and the targets.</i>
Caseld	string	The case ID to be mapped for the collection template.

Note: Template can be created only for the following job types:

- **File Scan:**
 - Filtered Collection
 - Full Disk Acquisition
- **Agent Scan:**
 - Software Inventory
 - Memory Analysis
 - Memory Acquisition
- **Reports Only:**
 - Filtered Collection
 - Full Disk Acquisition

Output Response:

- **Status Code – 200:** Indicates successful creation of the collection template.

Response Parameters:

Name	Type	Description
templateId	Guid	Displays the GUID of the template.
name	string	Displays the name of the template.
xmlOptions	string	Displays the XML options for Case and Job details.

Notes:

- The default value for the Case ID will be '-1' when you create a template without specifying a case value.
- The user can either use custodians or targets to create the template.
- Below are the Processing Options, Job Types and Job Execution Modes:

Processing Options	Job Types	Execution Modes
○ Forensic Processing = 1 ○ Field Mode = 2 ○ Summation Processing = 3 ○ eDiscovery Processing = 4 ○ Basic Assessment = 5 ○ Image Processing = 6 ○ Video Processing = 7 ○ All Communication = 8 ○ Mobile Processing = 9	○ Basic = 0, ○ MemoryAnalysis = 8, ○ SoftwareInventory = 9, ○ MemoryAcquisition = 10, ○ ReportOnly = 41,	○ Auto = 1 ○ Manual = 0

5.3 Create Collection (From Template)

This API Endpoint is to create a Collection by using a collection template.

Post `{{BASE_URL}}api/v2/enterpriseapi/agent/collection?template=<VALUE>`

Input Request:

- **Path Parameters** (*application/JSON format*):

The following parameter is **Mandatory**:

Name	Type	Description
template	string	Provide the Template ID for which the collection needs to be created.

- **Body Parameters** (*application/JSON format*):

The following parameters are **Optional**:

Name	Type	Description
jobName	String	Provide a name for the Collection.
Caseld	String	The case ID is provided for a collection to be created against the required case.
CustodianIds (or) TargetIds	Array<String>	Provide the custodian ID or as the target for a collection. (Or) Provide the Target GUID, Computer Name, or IP as the target for a collection. Note: The Custodian value will be considered when you provide values for both the custodians and the targets.

Example:

```
{
  "JobName": "File Scan Job Using Template_NC",
  "Caseld": "55",
  "CustodianIds": ["c2da9d7d-d7ad-4a87-8c99-9924f0550f44", "63fe2d06-dbe0-4ee4-b86d-57e5ce582f8b"],
  "TargetIds": []
}
```

Note: Collection can be created only for the following job types:

- **File Scan:**
 - Filtered Collection
 - Full Disk Acquisition
- **Agent Scan:**
 - Software Inventory
 - Memory Analysis
 - Memory Acquisition
- **Reports Only:**
 - Filtered Collection
 - Full Disk Acquisition

Output Response:

- **Status Code – 200:** Indicates successful creation of the Collection from the template.
Upon successful collection creation, the Job ID will be displayed in the response.

Notes:

- **Error Handling:**

- **Invalid Template ID:** If an attempt to create a collection with an invalid Template ID is made, an exception will be displayed in the response:

```
{  
  "exceptionMessage": "Invalid Job TemplateId.",  
  "exceptionType": "System.ApplicationException",  
  "message": "An error has occurred."  
}
```

- **Creating Collection from Template details:**

- The name field is not mandatory; failing to enter the value will create the collection with the name <CollectionJob_Date_Time>.
- If the user fails to pass the case name value during template creation, they can add the case parameter here and select any existing case to create a collection.
- Upon creating a collection using the template, parameters (Custodians and Target) are to be included as optional, and the user should provide a value when failing to do it in the created template. The user can provide multiple values for CustodianIds/TargetIds.
- If custodians/targets are provided in both the collection templates as well as the collection, then the values provided in the collection will take precedence.

5.4 List Collection Filter Templates

This API Endpoint lists all the Collection Filter templates.

Get `{{BASE_URL}}api/v2/enterpriseapi/agent/collection/filtertemplates`

Note: Only the Include/Exclude filters from the Computer Filtered collection job type would be displayed in this API Endpoint.

Input Request:

- **Path Parameter**

The following parameters are **optional**:

Name	Type	Description
Page	integer	Provide the Page number from the total pages to get the job details. Example: <code>{{BASE_URL}}api/v2/enterpriseapi/agent/collection/filtertemplates?Page=1</code>

Output Response:

- **Status Code – 200:** Indicates successful retrieval of all Collection Filter templates.

5.5 Start a collection

This API Endpoint is to start a collection job waiting for Execution.

Post `{{BASE_URL}}api/v2/enterpriseapi/agent/collection?id=<VALUE>`

Input Request:

- **Path Parameter** (*application/JSON format*):

The following parameter is **Mandatory**:

Name	Type	Description
id	Array[string]	Provide the Job ID to execute the collection job. only one ID can be provided in the path parameter to start the collection job. Example: <code>{{Base_URL}}api/v2/enterpriseapi/agent/collection?id=1</code> Note: Only the jobs that are set to Manual Execution can be started using this API.

Output Response:

- **Status Code – 200:** Indicates successful start of the collection job waiting for execution.

Upon successful execution of a valid job ID, the following message will be displayed in the response:

`"Job executed successfully."`

Notes:

- **Error Handling:**

- **Executing Invalid Job:** Executing an invalid job ID will display an exception in the response:

```
{  
  "exceptionMessage": "Job execution failed - Invalid Job ID.",  
  "exceptionType": "System.ApplicationException",  
  "message": "An error has occurred."  
}
```

- **Executing already executed job:** Executing an already executed job will throw the following exception in the response:

```
{  
  "exceptionMessage": "Can't execute Job ID.",  
  "exceptionType": "System.ApplicationException",  
  "message": "An error has occurred."  
}
```

6 User Activity Log API

The **User Activity Log API** provides the activity logs of users within the system. The API supports filtering, sorting, and pagination for more efficient querying of user activities. Use the following endpoint for the user activity log:

Post `{{Base_URL}} api/v2/enterpriseapi/activitylogs`

- **Payload Example:**

The following payload is mandatory for fetching activity logs with sorting and pagination:

```
{
  "sort": [{"field": "DateVal", "dir": "desc"}],
  "filter": {"filters": [], "logic": "and"},
  "skip": 0,
  "take": 10
}
```

- **Parameters:**

Name	Type	Description
filter	object	Defines the filtering criteria for the logs. You can chain multiple filters with a logical operator (and , or). Each filter inside filters is an object with keys like field , operator , and value .
sort	array of objects	Defines the sorting criteria. Each object includes field (e.g., "DateVal") and dir ("asc" or "desc").
skip	integer	The number of records to skip (used for pagination).
take	Integer	The number of records to return (used for pagination).
group	array of strings (optional)	A grouping key to group the results. Optional. If provided, it groups the logs by the specified field(s).

6.1 Filter Types

You can apply different types of filters to the activity logs, such as filters based on activity date, username, activity type, or category.

6.1.1 Activity Date Filter

Filters logs based on a specific date range.

```
{
  "filter": {
    "filters": [
      {
        "field": "ActivityDate",
        "operator": "gte",
        "value": "2025-02-10T00:00:00.000Z",
        "ignoreCase": true
      },
      {
        "field": "ActivityDate",
        "operator": "lte",
        "value": "2025-02-11T23:59:59.000Z",
        "ignoreCase": true
      }
    ],
    "logic": "and",
    "group": [],
    "skip": 0,
    "sort": [
      {
        "field": "DateVal",
        "dir": "desc"
      }
    ],
    "take": 10
  }
}
```

6.1.2 User Name Filter

Filters logs based on a specific username.

```
{
  "filter": {
    "filters": [
      {
        "field": "Username",
        "operator": "contains",
        "value": "admin"
      }
    ],
    "logic": "and",
    "group": [],
    "skip": 0,
    "sort": [
      {
        "field": "DateVal",
        "dir": "desc"
      }
    ],
    "take": 10
  }
}
```

6.1.3 Activity Filter

Filters logs based on a specific activity type (e.g., "login").

```
{
  "filter": {
    "filters": [
      {
        "field": "Activity",
        "operator": "contains",
        "value": "login",
        "logic": "and"
      }
    ],
    "group": [],
    "skip": 0,
    "sort": {
      "field": "DateVal",
      "dir": "desc"
    },
    "take": 10
  }
}
```

6.1.4 Category Filter

Filters logs based on a specific category value.

```
{
  "filter": {
    "filters": [
      {
        "field": "Category",
        "operator": "eq",
        "value": "10003",
        "logic": "or"
      }
    ],
    "group": [],
    "skip": 0,
    "sort": {
      "field": "DateVal",
      "dir": "desc"
    },
    "take": 10
  }
}
```

▪ Response

The API returns a JSON object containing the requested activity logs based on the applied filters and pagination.

Example response:

```
{
  "Data": [
    {
      "Activity": "Pradeep created case Confluence validation 21_04.",
      "ActivityDate": "2025-04-21T11:36:53.023",
      "Category": "CreateCase",
      "Username": "Pradeep",
      "MachineIP": null
    },
    {
      "Activity": "Administrator created case BAT_21.",
      "ActivityDate": "2025-04-21T11:35:32.647",
      "Category": "CreateCase",
      "Username": "Administrator",
      "MachineIP": null
    }
  ],
  "Total": 56,
  "FilteredTotal": 0
}
```

Notes:

- The *DateVal* field represents the timestamp when the activity log entry was created.
- You can adjust the filters and pagination to fit your requirements, allowing for more granular results.

6.2 Category Information

This API provides category information for system management and allows filtering based on various operators like equality, substring matching, and more. Use the following endpoint for category information:

Get`{{Base_URL}} api/quinc2/systemmanagement/getallcategoryinfo`

▪ Response

The response is an array of categories with two properties:

- **value:** A numeric identifier for the category.
- **label:** The name or description of the category.

Example response:

```
[
  {
    "value": 0,
    "label": "None"
  },
  {
    "value": 1,
    "label": "Error"
  },
  {
    "value": 999,
    "label": "GlobalMgtBegin"
  },
  {
    "value": 1000,
    "label": "GlobalNoldsBegin"
  },
  {
    "value": 1001,
    "label": "UserLoggedIn"
  }
]
```

▪ Operators :

You can filter or query the categories using the following operators:

- **eq**: is equal to.
- **neq**: is not equal to.
- **contains**: checks if a value contains a certain substring.
- **startswith**: checks if a value starts with a certain substring.
- **endswith**: checks if a value ends with a certain substring.

These operators can be used to filter or compare category labels or values when interacting with the API.

Example response for an activity log:

```
{
  "Data": [
    {
      "Activity": "Login",
      "ActivityDate": "2025-01-27T06:49:31.55",
      "Category": "LogIn",
      "Username": "Administrator",
      "MachineIP": "devvdi037"
    },
    {
      "Activity": "LogOut",
      "ActivityDate": "2025-01-24T17:03:28.673",
      "Category": "UserLoggedOut",
      "Username": "Administrator",
      "MachineIP": null
    },
    {
      "Activity": "LogOut",
      "ActivityDate": "2025-01-24T17:03:28.643",
      "Category": "UserLoggedOut",
      "Username": "Administrator",
      "MachineIP": null
    },
    {
      "Activity": "LogOut",
      "ActivityDate": "2025-01-24T17:03:28.623",
      "Category": "UserLoggedOut",
      "Username": "Administrator",
      "MachineIP": null
    }
  ]
}
```

(Example) This log entry captures an activity where:

- **Activity:** "Login"
- **ActivityDate:** The date and time of the activity.
- **Category:** "LogIn" (which might match one of the categories from the first response list)
- **Username:** The user associated with the activity (in this case, "Administrator")
- **MachineIP:** The machine IP where the activity took place ("devvdi037")

7 Event Audit Log API

7.1 FTK Audit Log Report (CSV/JSON)

Post `{{Base_URL}} api/v2/enterpriseapi/cases/{caseId=}/runftkcauditlogreport`

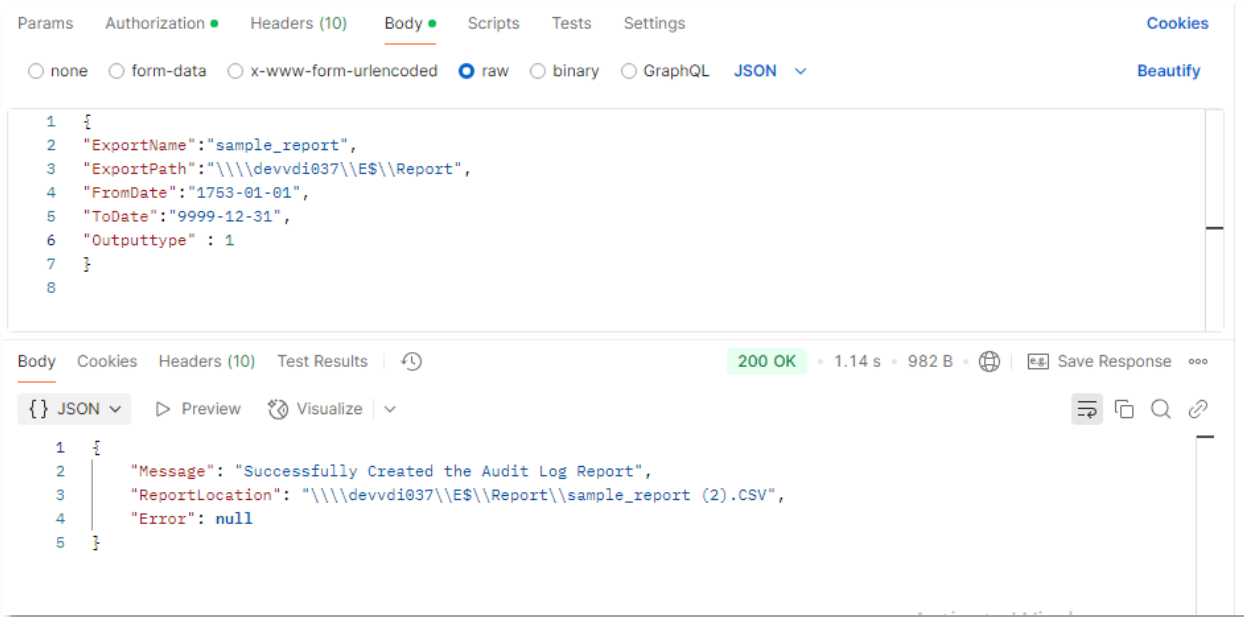
Generates a CSV file containing the activity log for the user ID specified in the payload and returns the path to the saved file.

- **Report Payload (CSV Example):**

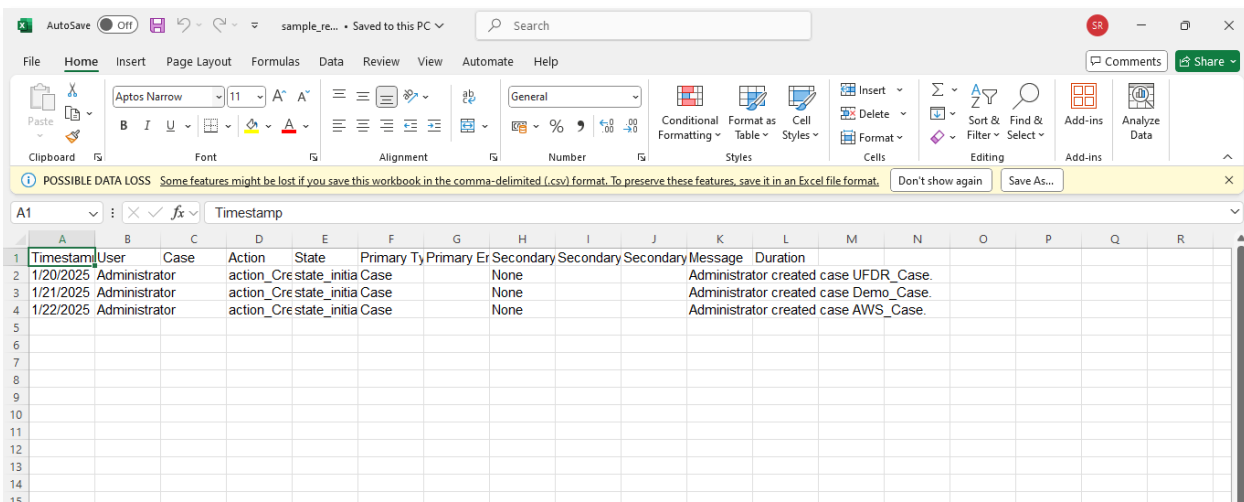
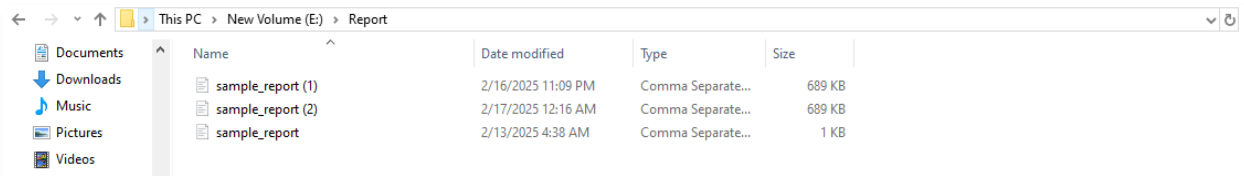
```
{
  "UserIds": [1000],
  "ExportName": "sample_report",
  "ExportPath": "\\devvdi037\\E$\\Report",
  "AuditActions": [{"ActionType": 9001}, {"ActionType": 1801}],
  "FromDate": "1753-01-01",
  "ToDate": "9999-12-31",
  "OutputType": 1
}
```

- **Report Response (CSV Example):**

```
{
  "Message": "Successfully Created the Audit Log Report",
  "ReportLocation": "\\devvdi037\\E$\\Report\\sample_report (2).CSV",
  "Error": null
}
```



○ **Reference Report Location :**



7.2 Case Audit Log Report (JSON)

Post `{{Base_URL}} api/v2/enterpriseapi/cases/{caseId=}/getcaseauditlogs`

Returns only the activity logs for a specific case in JSON format, including pagination details.

- **JSON Payload:**

```
{
  "UserIds": [1000],
  "ExportName": "sample_report",
  "ExportPath": "\\devvdi037\\E$\\Report",
  "AuditActions": [{"ActionType": 9001}, {"ActionType": 1801}],
  "FromDate": "1753-01-01",
  "ToDate": "9999-12-31",
  "PageNumber": 1
}
```

- **JSON Response:**

```
{
  "PaginationDetails": {
    "Page": 1,
    "TotalPages": 240,
    "TotalRecords": 2407,
    "CurrentPageRecords": 100
  },
  "ActivityLogs": [
    {
      "SecondaryEntityIDs": null,
      "UserID": 1000,
      "UserName": "Administrator",
      "CaseName": "",
      "PrimaryEntityName": "Administrator",
      "SecondaryEntityName": "",
      "Duration": null,
      "SecondaryEntityID": -1,
      "ActivityLogID": 0,
      "ActionType": 25065,
      "ActionState": 1,
      "DateVal": "2025-02-13T10:58:44.547",
      "PrimaryEntityType": 3,
      "PrimaryEntityID": 1000,
    }
  ]
}
```

```
"SecondaryEntityType": 4,  
"Message": "Login",  
"SHA1_1": null,  
"SHA1_2": null,  
"MachineIP": null  
}  
}
```

Notes:

- The **AuditActions** filter is used to specify the action types (e.g., 9001, 1801).
- **Pagination** details help in retrieving logs across multiple pages if the dataset is large.

7.3 Audit Actions API

This API provides a list of audit actions for a given scope, where each action has an ID, a name, and a description. This API helps in retrieving the available audit actions, which can be used for filtering logs, reports, or auditing purposes. Use the following endpoint for audit actions:

Get`{{Base_URL}} api/cases/getauditactions/{scopeItems=scopeItems}`

- **Parameters:**

- **scopeItems:** This defines the scope of the audit actions. For example, scopeItems=0.

- **Response :**

The response is an array of audit actions, each containing:

- **id:** The **id** field provides a unique identifier for each audit action.
- **name:** The **name** field corresponds to the action type.
- **description:** The **description** field gives more context about what the action represents.

```
[
  {
    "id": 0,
    "name": "action_None",
    "description": "AuditAction_action_None"
  },
  {
    "id": 1,
    "name": "action_Error",
    "description": "AuditAction_action_Error"
  },
  {
    "id": 999,
    "name": "action_GlobalMgtBegin",
    "description": "AuditAction_action_GlobalMgtBegin"
  }
]
```

8 Lookup APIs (Prerequisites)

The write APIs in this document reference users, groups, cases, and roles by numeric ID. Use the following lookup endpoints to retrieve valid IDs before invoking any assignment, creation, or export operation.

8.1 Get All Users

Returns all enterprise users. Use the id field as the **UserIds** value in assignment APIs.

GET `/api/v2/enterpriseapi/core/getusers`

Example Response:

```
[
{
  "id": 1011,
  "userName": "jdoe",
  "emailAddress": "jdoe@example.com", "firstName": "John",
  "lastName": "Doe", "department": null, "isActive": true, "isSuperAdmin": false,
  "creationDate": "2026-05-29T12:10:23.61",
  "createdByld": 1000,
  "lastModifiedByld": 1000
}
```

8.2 Get All Groups

Returns all groups. Use **groupId** in assignment APIs.

GET `/api/v2/enterpriseapi/core/getgroups`

Example Response:

```
[
{
  "groupId": 1003, "groupName": "Users", "description": "Users"
}
```

8.3 Get All Cases

Returns all cases with full case metadata. Use the id field as the **caseId** value in other APIs. Key fields are shown below; the full response contains additional case configuration properties.

GET `/api/v2/enterpriseapi/core/getcaselist`

Example Response:

```
[
{
  "id": 1,
  "name": "ct_1",
  "description": "",
  "casePath": "\\<file-server>\\Projects\\ct_1", "active": true,
  "isDeleted": false,
  "createdDate": "2026-05-27T13:07:17.5",
  "caseUUID": "7b5cfc14-6f5a-4b88-b6f9-e88d79744fef", "creatorId": 1000,
  "dbServerID": 2,
  "processingStatus": 1,
  "size": 486214027,
  "createdByUserName": "Administrator", "lastModifiedDate": "2026-05-27T13:07:16.203"
}
```

8.4 Get All Users, Roles, Permissions and Groups

Returns the complete security configuration in a single call. The response contains the following top-level collections:

GET `/api/v2/enterpriseapi/core/getallsecurityinfo`

Request Parameters:

Parameter	Type	Required	Description
caseList	array	<i>Not applicable</i>	Cases: caseID, caseName, description, path, active flag.
userList	array	<i>Not applicable</i>	Users: userId, userName, name fields, account status flags.
groupList	array	<i>Not applicable</i>	Groups: groupId, groupName, description.
userGroupInfoList	array	<i>Not applicable</i>	Existing user-to-group mappings (userId / groupId pairs).
roleInfoList	array	<i>Not applicable</i>	Roles: roleId, roleName, description, and the list of permission IDs granted by the role.
entityUserInfoList	array	<i>Not applicable</i>	Effective user/group/case/role associations (userId, groupId, caseId, roleId).

Example Response (abridged)

```
{
  "caseList": [
    { "caseID": 1, "caseName": "ct_1", "isActive": true, ... }
  ],
  "userList": [
    { "userId": 100, "userName": "<AccessData admin>", "isSuperAdmin": true, ... }
  ],
  "groupList": [
    { "groupId": 600, "groupName": "FTK Users Group", "description": "Group of users created in FTK" }
  ],
  "userGroupInfoList": [
    { "groupId": 1002, "userId": 1006 }
  ],
  "roleInfoList": [
    { "roleId": 800, "roleName": "Project/Case Administrator", "description": "This role has all case privileges.",
      "permissions": [7122, 2500000, 7105, ...] }
  ],
  "entityUserInfoList": [
    { "userId": 100, "groupId": null, "caseId": null, "roleId": 100, "entityTypeId": 0 }
  ]
}
```

8.5 Get AWS Region GUID

Returns AWS region GUIDs and region names configured in the system. The returned **RegionGuid** is required when ingesting evidence from AWS S3.

Refer to the [Create Case with Evidence and User Assignment](#) and [Add Evidence to an Existing Case](#) sections for more information.

GET`api/getregionguid/{userid}`

9 Manage Group Assignments

Assigns one or more existing enterprise users to a specified group, with optional case and role mappings. The API supports:

- Adding a single user or multiple users in one request
- Group assignment validation
- Case association validation
- Role validation
- Duplicate prevention for users already in the target group

Endpoint:

POST `/api/v2/enterpriseapi/ManageGroupAssignments`

Request Parameters:

Parameter	Type	Required	Description
UserIds	int[]	Yes	IDs of existing users to assign. Obtain from Get All Users .
groupId	int[]	Yes	Target group ID(s). Obtain from Get All Groups .
caseIds	int[]	No	Case IDs to associate with the assignment. Obtain from Get All Cases .
roleIds	int[]	No	Role IDs to apply. Obtain from Get All Security Info .

Example Request:

```
{
  "UserIds": [1470],
  "groupId": [1476],
  "caseIds": [2],
  "roleIds": [1001]
}
```

Success Response:

- When all provided IDs are valid, the user is added to the group and the API returns:

```
true
```

Validation and Error Responses:

Scenario	Response
User already a member of the group (duplicate prevention)	<code>{"exceptionMessage":"Failed to ManageGroupAssignments - User(Id:1011) is already part of Group(s): 1003", "exceptionType":"System.Exception", "message":"An error has occurred."}</code>
Invalid group ID	<code>{"exceptionMessage":"Failed to ManageGroupAssignments - Invalid user group IDs 3000", ...}</code>
Invalid case ID	<code>{"exceptionMessage":"Failed to ManageGroupAssignments - Invalid CaseIds: 1000", ...}</code>
Invalid role ID	<code>{"exceptionMessage":"Failed to ManageGroupAssignments - Invalid RoleIds: 8000", ...}</code>
UserIds or groupId empty (both are mandatory)	<code>{"exceptionMessage":"Failed to ManageGroupAssignments - User group cannot be empty\r\nInvalid user group IDs", ...}</code>

Note: *UserIds* and *groupId* are mandatory; *caseIds* and *roleIds* are optional.

10 Create User

Creates a new enterprise user and assigns roles, groups, and cases in a single operation. The API supports:

- Creating new enterprise users
- Assigning roles, groups, and case mappings during creation
- Username uniqueness validation
- Password policy validation
- Email format validation
- Group and role validation
- Audit logging of user creation and assignments

Endpoint:

POST `api/v2/enterpriseapi/core/CreateUser`

Request Parameters:

Parameter	Type	Required	Description
userName	string	Yes	Unique username. Duplicate usernames are rejected.
emailAddress	string	Yes	Email address in valid format (<i>user@example.com</i>).
firstName	string	Yes	User's first name. Must not be empty.
lastName	string	Yes	User's last name. Must not be empty.
password	string	Yes	Initial password. Must satisfy the password policy .
groups	int[]	Yes	Group IDs to assign. Invalid group IDs are rejected.
roles	int[]	No	Role IDs to assign.
caseIds	int[]	No	Case IDs to associate with the user.

Example Request:

```
{
  "userName": "DemoUser34",
  "emailAddress": "demo.user@example.com",
  "firstName": "Demo",
  "lastName": "User",
  "password": "<StrongPassword>",
  "groups": [1476],
  "roles": [1002],
  "caselds": [2]
}
```

Password Policy:

The password must satisfy all of the following conditions:

- Minimum length of 8 characters
- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character
- Must not be empty

Success Response:

```
true
```

Validation and Error Responses:

Scenario	Response
Username already exists	<code>{"exceptionMessage":"UserName - jdoe already exists. Please provide an alternative name.", ...}</code>
Username empty	<code>{"exceptionMessage":"UserName is empty. Please provide the UserName.", ...}</code>
First name / last name empty, or invalid group ID (errors are combined)	<code>{"exceptionMessage":"Invalid Groups: 2000.Please provide valid Groups.\r\nFirstName is empty. Please provide the FirstName.\r\nLastName is empty. Please provide the LastName.", ...}</code>
Password policy violation (all failed rules listed)	<code>{"exceptionMessage":"Password is required.\r\nPassword must be at least 8 characters long.\r\nPassword must contain at least one uppercase letter.\r\nPassword must contain at least one lowercase letter.\r\nPassword must contain at least one number.\r\nPassword must contain at least one special character.", ...}</code>
Invalid email format	<code>{"exceptionMessage":"Validation Error: The email address 'invalid.example' is not in a valid format. Expected format: user@example.com.", "exceptionType":"System.ApplicationException", ...}</code>

11 Create Case with Evidence and User Assignment

Creates a case, ingests evidence, and assigns users and groups in a single operation. The API supports:

- Adding evidence while creating a case (single or multiple evidence items)
- Configuring evidence-specific processing options
- Assigning users and groups during case creation
- Automatically triggering evidence processing
- Evidence ingestion from network shares and from AWS S3
- Audit logging of user/group assignment activities

Endpoint:

POST `api/v2/enterpriseapi/core/createcase`

Request Parameters:

Parameter	Type	Required	Description
name	string	Yes	Case name. Validated for uniqueness/format.
description	string	No	Case description.
ftkCaseFolderPath	string	Yes	UNC path of the case folder. Must exist and be accessible.
responsiveFilePath	string	Yes	UNC path for responsive files. Must exist and be accessible.
EvidencePath	string[]	Yes	One or more evidence paths (UNC folder/file paths, or object keys when using AWS S3). Each path is validated.
EnhancedInternetArtifactAnalysis	bool	No	Enables enhanced internet artifact analysis.
GenerateTimelineData	bool	No	Enables timeline data generation.
GenerateEntities	bool	No	Enables entity extraction.
ProcessingOption	string	Yes*	Processing profile, e.g. "Forensic Processing". Required when processing is triggered.

Parameter	Type	Required	Description
ProcessingManager	string	Yes*	Hostname or IP of the Distributed Processing Manager (DPM). Required when processing is triggered.
TriggerTheProcessing	bool	No	If true, processing jobs start automatically after ingestion.
UserIds	int[]	No	User IDs to assign to the case.
GroupIds	int[]	No	Group IDs to assign to the case.
EnterpriseAWSS3	object	No	AWS S3 source configuration (Refer Example Request - AWS S3 Evidence).

Example Request — Network Share Evidence:

```
{
  "name": "DemoCase01",
  "description": "Case created from Enterprise API",
  "ftkCaseFolderPath": "\\<file-server>\\Cases",
  "responsiveFilePath": "\\<file-server>\\Responsive",
  "EvidencePath": ["\\<file-server>\\Evidence\\Set01"],
  "EnhancedInternetArtifactsAnalysis": false,
  "GenerateTimelineData": false,
  "GenerateEntities": false,
  "ProcessingOption": "Forensic Processing",
  "ProcessingManager": "<dpm-host>",
  "TriggerTheProcessing": true,
  "UserIds": [1470],
  "GroupIds": [1476]
}
```

Example Request — AWS S3 Evidence

To ingest evidence from AWS S3, first obtain the **region GUID** using **GET/api/getregionguid/{user Id}**

Refer to the [Get AWS Region GUID](#) section, then include the EnterpriseAWSS3 object. **EvidencePath** contains the S3 object key(s).

```
{
  "name": "DemoCaseS3",
  "description": "Case created from Enterprise API",
  "ftkCaseFolderPath": "\\<file-server>\\Cases",
  "responsiveFilePath": "\\<file-server>\\Responsive",
  "EvidencePath": [ "evidence/demo.ad1" ],
  "EnhancedInternetArtifactsAnalysis": false,
  "GenerateTimelineData": false,
  "GenerateEntities": false,
}
```

```
"ProcessingOption": "Forensic Processing",
"ProcessingManager": "<dpm-host>",
"TriggerTheProcessing": true,
"UserIds": [],
"GroupIds": [],
"EnterpriseAWSS3": {
  "BucketName": "<your-s3-bucket>",
  "RegionGuid": "<region-guid-from-lookup>"
}
```

Validation Rules:

- Case name validation — the case name must be valid and acceptable to the system.
- Folder path validation — the case folder path must exist and be accessible.
- File path validation — the responsive file path must exist and be accessible.
- Evidence path validation — every evidence path (network share or S3 object) must exist and be accessible.

12 Add Evidence to an Existing Case

Adds evidence to an existing case. The API supports:

- Adding single or multiple evidence items
- Network share evidence ingestion
- AWS S3 evidence ingestion
- Evidence-specific processing options
- Optional processing trigger
- Case-level permission validation
- Audit logging

Endpoint:

POST `/api/v2/enterpriseapi/core/addevidence`

Request Parameters:

Parameter	Type	Required	Description
caseId	int	Yes	ID of an existing case. Invalid IDs are rejected before processing.
EvidencePath	string[]	Yes	One or more evidence paths (UNC paths, or S3 object keys when using AWS S3).
EnhancedInternetArtifactsAnalysis	bool	No	Enables enhanced internet artifact analysis.
GenerateTimelineData	bool	No	Enables timeline data generation.
GenerateEntities	bool	No	Enables entity extraction.
ProcessingOption	string	Yes*	Processing profile, e.g. "Forensic Processing". Required when processing is triggered.
ProcessingManager	string	Yes*	Hostname or IP of the DPM. Required when processing is triggered.
TriggerTheProcessing	bool	No	If true, processing jobs are initiated after the evidence is attached.

Parameter	Type	Required	Description
AddEvidenceRequestForAWSS3	object	No	Wrapper containing the EnterpriseAWSS3 source configuration (Refer to the Example Request - AWS S3 Evidence).

Example Request — Network Share Evidence:

```
{
  "caseId": 6,
  "EvidencePath": ["\\\\<file-server>\\Evidence\\TestEvidence"],
  "EnhancedInternetArtifactsAnalysis": false,
  "GenerateTimelineData": false,
  "GenerateEntities": false,
  "ProcessingOption": "Forensic Processing",
  "ProcessingManager": "<dpm-host>",
  "TriggerTheProcessing": true
}
```

Example Request — AWS S3 Evidence:

```
{
  "caseId": 4,
  "EvidencePath": [ "evidence/demo.ad1" ],
  "EnhancedInternetArtifactsAnalysis": false,
  "GenerateTimelineData": false,
  "GenerateEntities": false,
  "ProcessingOption": "Forensic Processing",
  "ProcessingManager": "<dpm-host>",
  "TriggerTheProcessing": true,
  "AddEvidenceRequestForAWSS3": {
    "EnterpriseAWSS3": {
      "BucketName": "<your-s3-bucket>",
      "RegionGuid": "<region-guid-from-lookup>"
    }
  }
}
```

Success Response:

- When all validations pass, the evidence is attached to the case. If **TriggerTheProcessing** is true, processing jobs are also initiated.

```
"Evidence added to the caseId: 63"
```

Validation and Error Responses:

Scenario	Response
Invalid case ID	<pre>{"exceptionMessage": "Invalid CaseIds: 20000", "exceptionType": "ADG.BusinessServices.EvidenceServices.Validations.ValidationException", ...}</pre>
Invalid evidence path (network share or AWS S3)	<pre>{"exceptionMessage": "Evidence file/folder does not exist: '\\\\<file-server>\\Evidence\\demo.ad1"', ...}</pre>
Invalid processing option	<pre>{"exceptionMessage": "Please enter a valid Processing option", ...}</pre>
Invalid processing manager	<pre>{"exceptionMessage": "Please enter a valid Processing manager", ...}</pre>
User not assigned to the case (access denied)	<pre>{"exceptionMessage": "User does not have required permissions.", "exceptionType": "System.Exception", ...}</pre>

Note: The calling user must be assigned to the case and hold the Manage Evidence permission; otherwise the request is rejected with an access-denied error.

13 Export Case Grid to CSV

Exports case grid data to CSV with optional filtering and column selection. The API supports:

- Column-based export selection
- File category filtering
- Label and bookmark filtering
- Background job processing with job tracking via Job ID
- CSV generation with headers
- Permission-based access control

13.1 Supporting API — Get Exportable Columns

Returns the available column display names for use in the **exportColumns** payload field.

GET `/api/v2/enterpriseapi/getcolumns`

Example Response (abridged):

```
[  
  "Abbreviation", "AboutMe", "AboutUrl", "AccessedFileName", "AccessedFilePath", "AccessedTime",  
  ...  
]
```

13.2 Supporting API — Get File Categories for a Case

Returns the file categories present in the case, with each category's ID and object count. Use **fileCategoryId** values in the **fileCategory** field of the export request.

GET `/api/v2/enterpriseapi/getfilecategoriesforcase/{caseId}`

Example Response:

```
[
  { "fileName": "Message", "fileCategoryId": 745, "objectCount": 1169 },
  { "fileName": "JPEG", "fileCategoryId": 572, "objectCount": 111 }
]
```

Export Endpoint:

POST `/api/v2/enterpriseapi/executecsvgridexport`

Request Parameters:

Parameter	Type	Required	Description
caseId	int	Yes	Case to export. An invalid value returns a validation error.
exportColumns	string[]	No	Column display names to export (Refer to Supporting API - Get Exportable Columns). If omitted, a default column set is used (Refer to Supporting API - Get File Categories for a Case GET).
fileCategory	int[]	No	File category IDs to filter by (Refer to Supporting API - Get File Categories for a Case GET).
labels	string[]	No	Label names to filter by (case-insensitive).
bookmarks	string[]	No	Bookmark names to filter by (case-insensitive).

Example Request:

```
{
  "caseId": 1,
  "exportColumns": [ "ObjectId", "Author" ],
  "fileCategory": [ 101, 102 ],
  "labels": [ "Confidential", "Reviewed" ],
  "bookmarks": [ "Page10", "Section4" ]
}
```

Export Behavior:

- No filters provided — all objects are exported using the General column set.
- Single file category — the Default column set for that category is used.
- Multiple file categories — the General column set is used.
- Labels / bookmarks (tags) provided — only matching objects are exported, using the General column set.
- Explicit exportColumns provided — only the selected columns are exported; no default column set is applied.
- Mixed filters — file categories, labels, and bookmarks are combined with OR logic: objects matching any valid filter are included.

Note: Filters are combined with an OR condition. If all provided filter values are invalid, no export is created. If at least one value is valid, the export is created and the response lists the invalid values that were ignored.

Responses:

Scenario	Response
At least one valid filter; invalid values ignored (export job created)	<code>{"message": "FileCategories [1] are invalid. Invalid Values has been Ignored. Export to CSV Job has been created successfully.", "jobId": 452}</code>
All provided filter values invalid (export not created)	<code>{"exceptionMessage": "FileCategories [1] are invalid.. Export cannot be created", "exceptionType": "System.ApplicationException", ...}</code>
User lacks permission for the case	<code>{"exceptionMessage": "User does not have case permissions. CaseId 1", "exceptionType": "System.ApplicationException", ...}</code>

Successful requests return a **jobId**; the export runs as a background job that can be tracked by this ID.

14 Import Evidence via CSV

Bulk-imports evidence into an existing case from a CSV file, automating evidence ingestion with optional processing.

The API supports:

- Bulk evidence import via CSV with row-wise evidence processing
- Validation of case existence and CSV content
- Optional evidence processing trigger and processing profile selection
- Timeline and entity generation
- Background job execution with tracking

Endpoint:

POST `api/v2/enterpriseapi/processevidencecsv`

Request Parameters:

Parameter	Type	Required	Description
caseId	int	Yes	Existing case to import evidence into.
csvFilePath	string	Yes	Path to the evidence import CSV. Must exist and be accessible to the server.
firstRowContainsHeader	bool	Yes	Whether the first CSV row is a header row.
customColumnExists	bool	Yes	Whether the CSV contains custom columns.
processingOption	string	Yes*	Processing profile, e.g. "Forensic Processing". Required when triggerTheProcessing is true .
generateTimelineData	bool	No	Enables timeline data generation.
generateEntities	bool	No	Enables entity extraction.
enableEnhanceInternetArtifactAnalysis	bool	No	Enables enhanced internet artifact analysis.
processingManager	string	Yes*	Hostname or IP of the DPM. Required when processing is triggered.

Parameter	Type	Required	Description
triggerTheProcessing	bool	No	If true, an evidence import job is created and processing starts; if false, evidence details are saved without processing.

Example Request:

```
{
  "caseId": 3,
  "csvFilePath": "E:\\EvidenceImportTemplate.csv",
  "firstRowContainsHeader": true,
  "customColumnExists": false,
  "processingOption": "Forensic Processing",
  "generateTimelineData": true,
  "generateEntities": true,
  "enableEnhanceInternetArtifactAnalysis": true,
  "processingManager": "<dpm-host>",
  "triggerTheProcessing": true
}
```

Success Responses:

Scenario	Response
Processing triggered (triggerTheProcessing = true)	"Add Evidence Job have Created Successfully with Processing option as Forensic Processing and Processing Manager as <dpm-host> and JobId is 117"
Processing not triggered (triggerTheProcessing = false)	"Evidence details are Saved Successfully"

Validation and Error Responses:

Scenario	Response
Invalid case ID	<i>{"exceptionMessage":null,"exceptionType":null,"message":"Case Id : -1 is not Valid"}</i>
CSV file path empty	<i>{"exceptionMessage":null,"exceptionType":null,"message":"CSV Filepath Should not be Empty"}</i>
CSV file path does not exist	<i>{"exceptionMessage":null,"exceptionType":null,"message":"CSV FilePath does not exists"}</i>
Processing triggered but processing option missing	<i>{"exceptionMessage":null,"exceptionType":null,"message":"Proc essing option Should not be Empty, Since TriggerProcessing is true"}</i>
Invalid processing option	<i>{"exceptionMessage":null,"exceptionType":null,"message":"Proc essing option : fore is not Valid"}</i>
Processing triggered but processing manager missing	<i>{"exceptionMessage":null,"exceptionType":null,"message":"proc essing manager Should not be Empty, Since TriggerProcessing is true"}</i>

15 Export Evidence (Labels & Options)

The Export Evidence API programmatically exports evidence from an FTK Central case using labels, export options, or previously saved export templates. It follows the same validation rules, processing workflow, and default export behavior as the Export Wizard UI. Export operations run asynchronously as background jobs and return a Job ID for tracking progress.

Endpoint:

POST `/api/v2/enterpriseapi/ADexport?CaseId={caseId}`

The target case is identified by the **caseId** query-string parameter.

Request Parameters (general object):

Parameter	Type	Required	Description								
name	string	Yes	Name of the export.								
path	string	Yes	UNC destination path for the export output.								
exportLabelList	object[]	No	Labels selecting the objects to export, <i>e.g.</i> <code>[{"name": "test"}]</code> .								
exportType	int	Yes	Export type identifier (matches Export Wizard export types). Export Type Reference Mapping: <table><tr><th>Format</th><th>Value</th></tr><tr><td>AD1</td><td>0</td></tr><tr><td>Native</td><td>1</td></tr><tr><td>Load File</td><td>2</td></tr></table>	Format	Value	AD1	0	Native	1	Load File	2
Format	Value										
AD1	0										
Native	1										
Load File	2										
exportNativeFiles	bool	No	Include native files in the export.								
generateLoadFile	bool	No	Generate a load file.								
exportImageFiles	bool	No	Include image files.								
exportTextFiles	bool	No	Include text files.								
exportRSMF	bool	No	Include RSMF output.								

Parameter	Type	Required	Description
excludeEDiscoveryIgnorables	bool	No	Exclude eDiscovery-ignorable files.
generateExclusionReport	bool	No	Generate an exclusion report.
saveAsTemplate	bool	No	Save this configuration as a reusable template.
templateName	string	No	Template name when saveAsTemplate is true .

Example Request:

```
{
  "general": {
    "name": "test",
    "path": "\\|\\|\\|<file-server>\\|\\ProjectData\\|Cases",
    "exportLabel": [{"name": "test"}],
    "exportType": 1,
    "exportNativeFiles": false,
    "generateLoadFile": false,
    "exportImageFiles": true,
    "exportTextFiles": true,
    "exportRSMF": true,
    "excludeEDiscoveryIgnorables": false,
    "generateExclusionReport": false,
    "saveAsTemplate": false,
    "templateName": ""
  }
}
```

Appendix A: Quick Reference — Validation Behavior

The following validation behaviors are shared across the APIs documented in this reference:

Validation Type	Applies To (Sections)	Behavior / Requirement
Entity ID Validation	Manage Group Assignments Create User Create Case with Evidence and User Assignment Add Evidence to an Existing Case Export Case Grid to CSV Import Evidence via CSV	Requests referencing non-existent IDs (user, group, case, role) are rejected before any changes are applied.
Duplicate Prevention	Manage Group Assignments	A user who is already a member of the target group cannot be assigned to it again.
Path Validation	Create Case with Evidence and User Assignment Add Evidence to an Existing Case Import Evidence via CSV	All UNC paths, evidence paths, and CSV file paths must exist and be accessible by the server.
Processing Prerequisites	Create Case with Evidence and User Assignment Add Evidence to an Existing Case Import Evidence via CSV	When processing is triggered, a valid Processing Option and Processing Manager are mandatory.
Case Permission Checks	Add Evidence to an Existing Case Export Case Grid to CSV	The calling user must be assigned to the case and hold the relevant permission (e.g., <i>Manage Evidence</i>), or the request is rejected.
Background Jobs	Export Case Grid to CSV Import Evidence via CSV	Long-running operations execute asynchronously and will immediately return a Job ID.

Note: In parameter tables, "Yes*" indicates the field is required only when processing is triggered: (*TriggerTheProcessing* / *triggerTheProcessing* = true).

Known Issues

The following known issues will be resolved in a future release:

1. The generateExclusionReport parameter in the Export Enterprise API depends on the Exclude Export Labels and Exclude Export Categories options. Because these dependent options are currently available only in the UI and not supported in the API payload, setting generateExclusionReport to 'true' will not function as expected. **(FTKC-72034)**
2. During both Manual Export and Enterprise API exports, eDiscovery Ignorable objects are automatically excluded regardless of whether the Exclude eDiscovery Ignorables option is enabled or disabled. **(FTKC-72248)**

Limitations

1. The filecategory parameter in the executecsvgridexport API expects integer values. If a non-numeric string value is provided (for example, "abc" or "752g"), the API treats the value as null instead of returning an invalid input error. As a result, the API follows the default behavior for a null filecategory value rather than explicitly validating the input. Numeric string values (for example, "101") are successfully converted to integers and processed. **(FTKC-68984)**

Contact Exterro

If you have any questions, please refer to this document, or any other related materials provided to you by Exterro. For usage questions, please check with your organization's internal application administrator. Alternatively, you may contact your Exterro Training Manager or other Exterro account contact directly.

For technical difficulties, support is available through support@exterro.com.

Contact:

Exterro, Inc.

2175 NW Raleigh St., Suite 110

Portland, OR 97210.

Telephone: 503-501-5100

Toll Free: 1-877-EXTERRO (1-877-398-3776)

Fax: 1-866-408-7310

General E-mail: info@exterro.com

Website: www.exterro.com

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Exterro, Inc. The trademarks, service marks, logos or other intellectual property rights of Exterro, Inc and others used in this documentation ("Trademarks") are the property of Exterro, Inc and their respective owners. The furnishing of this document does not give you license to these patents, trademarks, copyrights or other intellectual property except as expressly provided in any written agreement from Exterro, Inc.

The United States export control laws and regulations, including the Export Administration Regulations of the U.S. Department of Commerce, and other applicable laws and regulations apply to this documentation which prohibits the export or re-export of content, products, services, and technology to certain countries and persons. You agree to comply with all export laws, regulations and restrictions of the United States and any foreign agency or authority and assume sole responsibility for any such unauthorized exportation.

You may not use this documentation if you are a competitor of Exterro, Inc, except with Exterro Inc's prior written consent. In addition, you may not use the documentation for purposes of evaluating its functionality, or for any other competitive purposes.

If you have any questions, please contact Customer Support by email at support@exterro.com.