exterro
Data Risk Management

FTK CENTRAL 8.2 SP3

USER GUIDE

Table of Contents

ABOUT FTK CENTRAL **14**

ABOUT THIS MANUAL 14

LOGGING INTO FTK CENTRAL 15

FTK Central Home Screen *16*

FTK Central UI Guide *25*

BEFORE YOU BEGIN 30

FTK Central Requirements *30*

About User Accounts *31*

Opening FTK Central *31*

CASES **33**

CREATING CASES 33

Primary Details *34*

Custodian Mapping *38*

Load Files *39*

Process Evidence *46*

Evidence Decryption *60*

Copy from a previous case *64*

User Assignment *65*

Case Index Status *67*

PROCESSING OPTIONS **68**

EVIDENCE PROCESSING 71

Commonly Used Processing Options *71*

COMPOUND FILES 76

Filtering the Compound File Expansion Options List *76*

Supported Compound File Types *77*

SEARCH TEXT INDEX 79

Search Text Indexing Space Requirements *79*

© Exterro, Inc. All rights reserved

Configuring Case Indexing Options *80*
DATA CARVING 84
Supported Carving Options *84*
Importing Data Carvers *85*
CREATING THUMBNAILS FOR VIDEOS 86
CREATING COMMON VIDEO FILES 89
OPTICAL CHARACTER RECOGNITION 92
Running Optical Character Recognition *93*
ABBYY FineReader Integration *96*
Optical Character Recognition: Confidence Score *97*
EXPLICIT IMAGE DETECTION 98
Adding EID evidence to cases *98*
CERBERUS ANALYSIS 101
About Cerberus Stage 1 Threat Analysis *102*
About Cerberus Score Weighting *102*
About Cerberus Override Scores *103*
Running Cerberus Analysis *104*
Filtering Scanned Files and Viewing Threat Scores *107*
Cerberus Stage 1 Threat Scores *108*
Cerberus Stage 1 File Information *111*
About Cerberus Stage 2 Static Analysis *112*
Cerberus Stage 2 Function Call Data *112*
File Access Call Categories *113*
Networking Functionality Call Categories *116*
Process Manipulation Call Categories *119*
Security Access Call Categories *121*
Windows Registry Call Categories *122*
Surveillance Call Categories *124*
Uses Cryptography Call Categories *124*
Low-level Access Call Categories *125*
Loads a drive Call Categories *126*

© Exterro, Inc. All rights reserved

Subverts API Call Categories *126*
DOCUMENT CONTENT ANALYSIS 127
Considerations of Cluster Topic *128*
Running Document Content Analysis *129*
Filtering Documents by Document Content Analysis *132*
LANGUAGE IDENTIFICATION 133
Performing Language Identification *133*
Viewing Language Identified Documents *136*
Basic Languages *136*
Extended Languages *137*
LANGUAGE TRANSLATION 138
ENTITY EXTRACTION 140
LAB/E-DISCOVERY OPTIONS 142
EVIDENCE REFINEMENT 145
INDEX REFINEMENT 148
Refining an Index by File Status/Type *149*
Refining an Index by File Date/Size *150*
AI JOBS 151
Image Recognition *152*
Similar Face Detection *156*
AI Summarization *159*
Multimedia Intelligence *164*
CREATING CUSTOM PROCESSING PROFILES 167
Creating a Custom Processing Profile *167*

KNOWN FILE FILTER (KFF) 168

INTRODUCTION TO THE KFF ARCHITECTURE 169
COMPONENTS OF KFF DATA 170
ABOUT THE ORGANIZATION OF HASHES, HASH SETS AND KFF GROUPS 171
ABOUT PRE-DEFINED KFF HASH LIBRARIES 171
NIST NSRL 172

© Exterro, Inc. All rights reserved

NDIC HashKeeper 173
Bloom Filter 174
Installing KFF 176
Downloading the Latest KFF Installation Files *176*
Determining Where to Install the KFF Server *176*
Installing Cassandra *177*
Cassandra and Firewalls *178*
Manually Configuring Remote Setting for Cassandra *178*
Configuring a Remote KFF Server *179*
Installing KFF Import Utility *180*
Importing a CSV using the KFF Import Utility 180
Verifying a File Using the KFF Import Utility 181
Removing Pre-defined KFF Libraries Using the KFF Import Utility 181
Using the KFF Utility in FTK Central 182
Creating a Hash Set *182*
Importing a Hash Set *184*
Importing a Hash Set from Review Mode *186*
Creating a KFF Group *188*
Associating Hash Sets to KFF Group *189*
Running KFF Against a Case 190
Reviewing KFF Results in a Case 191
KFF Facet Filters *191*
KFF Columns *192*

PROCESSING IWORK FILES FOR REVIEW 193

MANAGING CASES 194

Viewing Details about a Case 197
Opening a Case 198
Opening a Case via Case Dashboard *198*
Opening a Case via Case List *199*
Opening a Case via Review Mode *200*

© Exterro, Inc. All rights reserved

Case List Options *201*
Case Dashboard *203*
CASE SUMMARY 212
General Statistics *213*
Managing Custodians *213*
Managing Evidence *214*
Managing Process Data *215*
Managing Default Filters *215*
Managing Case Auditing *216*
CODING PANELS 218
Creating Coding Panel *219*
Reorganizing a Coding Panel *222*
Deleting Coding Panels *224*
BATCHES 225
BATCH ADMINISTRATION PANEL 225
Viewing Review Set Details *226*
Dashboard: Viewing Case Coding Summary *227*
CREATING REVIEW SETS 228
EDITING REVIEW SETS 231
DELETING REVIEW SETS 231
BATCH REVIEW PANEL 232
Checking In/Out a Review Set *232*
Reviewing a Review Set *233*
BACKUP AND RESTORING CASES 234
BACKUP AND RESTORING CASES 234
Backing up the Cases *234*
Restoring Cases *238*
VIEWING DATA 242
VIEWING DOCUMENTS IN THE GRID 244
Dark and Light Modes *245*

© Exterro, Inc. All rights reserved

File Icons *246*
File Status *246*
Viewed/Unviewed Files *247*
Grid Details *247*
Review Page Time Zone *248*
Selecting Files *249*
About the Amount of Data Displayed in Fields *250*
Performing Actions in the Grid *251*
COLUMNS 264
Using Quick Columns *264*
Provided Quick Columns *265*
Using Custom Columns *265*
Moving Columns in the Grid *266*
USING VIEWS 267
Using the List View *268*
Using the Thumbnail View *269*
Using the Smart Grid View *274*
Using the Timeline View *276*
VIEWING THE PANELS 287
Viewer *288*
Info *290*
Tags Panel *295*
Mini Timeline *296*
Maps *297*
Entity Management Dashboard *299*
USING DOCUMENT VIEWING PANELS 312
Using the Native Panel *312*
Using the Image Panel *317*
Using the Text Panel *334*
Using the Viewer Panel on Another Monitor *334*
Using the Desktop Viewer *335*

© Exterro, Inc. All rights reserved

EXPORTING **336**

EXPORTING GRID TO CSV 336

EXPORT WIZARD 337

AD1 – Optional Configuration *340*

Native – Optional Configuration *342*

Load Files – Optional Configuration *345*

Imaging – Optional Configuration *348*

Text – Optional Configuration *350*

Numbering – Optional Configuration *351*

Summary *354*

REVIEWING CASES **355**

FILTERING 357

Types of Filters *357*

Exclusion Filter *359*

Quick Filter *360*

Common Filter *362*

Artifacts Filter *364*

Evidence Explorer *366*

Column Filters *367*

SEARCHING 371

Simple Searching *372*

Relationships *372*

Live Search *373*

Advanced Searching *375*

Search Hits Column *387*

Search Term Excerpt Report *388*

WORKING WITH LABELS 401

Creating Labels *401*

Editing Labels *402*

Deleting Labels *402*

© Exterro, Inc. All rights reserved

Applying Labels *403*
Creating Label Groups *404*
Editing Label Groups *404*
Filtering for Labels *405*
WORKING WITH BOOKMARKS 405
Creating Bookmarks *406*
Editing Bookmarks *407*
Deleting Bookmarks *407*
Applying Bookmarks *408*
Bulk Bookmarking *408*
Filtering for Bookmarks *408*
SHARING TAGS 409
CREATING REPORTS 410
Report Types *411*
Creating a Detail Report *412*
Creating a Search Term Report *427*
Exporting Reports *430*
Portable Case *431*
Viewing and Downloading Completed Reports *439*
CODING PANELS WITHIN REVIEW 442
Creating Coding Panel *442*
Reorganizing a Coding Panel *448*
Deleting Coding Panels *449*

DATA SOURCES 450

MANAGING DATA SOURCES 451
Network Share *453*
Computer *459*
Gmail *466*
Google Drive *471*
OneDrive *476*

© Exterro, Inc. All rights reserved

Microsoft Teams *482*
Slack *487*
AWS S3 ..... *495*
SharePoint *499*
Exchange *505*
Box *522*
Confluence *526*

CUSTODIANS 530

MANAGING CUSTODIANS 531
Adding Custodians *531*
Editing Custodians *538*
Deleting Custodians *539*
MAPPING DATA TO CUSTODIANS 540
MANAGING ACTIVE DIRECTORY GROUP 542
Adding Active Directory Group *542*
Associating Active Directories *544*

LITHOLDS 550

CONFIGURING LITHOLDS 552
LitHold Configuration *552*
Managing IT Staff *555*
Managing Approver *560*
Email Templates *563*
Documents Templates *566*
Interview Templates *569*
CREATING LITHOLDS 572
APPROVING LITHOLDS 581
DEACTIVATING LITHOLDS 582
ACTIVATING LITHOLDS 583
RESUBMITTING LITHOLDS 584
VIEWING LITHOLDS 586

© Exterro, Inc. All rights reserved

Viewing Custodian Responses of a LitHold 588
Generating Reports for LitHolds 590
Hold Summary report *590*
Custodian Details report *592*
Hold Details report *594*
Hold Custodians report *595*
Editing LitHolds 596
Deleting LitHolds 597

COLLECTIONS 598

Windows, Linux, and Other Data Sources 600
Creating Collections *600*
Managing Collections *642*
Data Source Configuration for Collection *656*
Mac 699
Creating Mac Collection *699*
Viewing Mac Collection Details *706*
Remote Mobile Discovery 708
Creating Remote Mobile Collection *709*
Viewing Mobile Collection *730*

LIVE PREVIEW 736

Windows, Linux, and Other Data Sources 737
UI Breakdown *737*
Live Previewing an Agent *740*
Acquiring a Logical Drive from an Agent *747*
Mac 748
Live Previewing a Mac Agent *748*
Acquiring a Logical Drive from a Mac Agent *751*

FTK CONNECT 753

Managing FTK Connect 754

© Exterro, Inc. All rights reserved

AUTOMATIONS 755
UI Breakdown *755*
Automation Workflows *759*
Creating an automation *769*
JOB MONITORS 774
LIMITATIONS/KNOWN BUGS 776
API Trigger Workflow *777*
ADMINISTRATING FTK CENTRAL 781
ADMINISTRATION PORTAL 781
User Management *782*
System Management *809*
MONITORING DPM AND DPE 887
DPM DPE ASSOCIATED JOBS 888
MONITORING PROCESSING JOBS 890
VIEWING JOBS 890
Active Jobs *891*
Completed Jobs *892*
PAUSING/RESUMING JOBS 893
DELETING JOBS 894
EDITING AN AI JOB'S PRIORITY 896
CONFIGURING PROJECT VIC/CAID 898
INITIALIZING PROJECT VIC/CAID 898
INITIALIZING PROJECT VIC/CAID ON A CASE LEVEL 899
CATEGORIZING DOCUMENTS IN REVIEW MODE 901
Using the Coding Panel to Categorize Images *902*
Pixelating Categorized Images *903*
EXPORTING MEDIA CATEGORIES 904
FILTERING CATEGORIZED DATA 906

© Exterro, Inc. All rights reserved

MANAGING SECURITY DEVICES AND LICENSES 907

INSTALLING AND MANAGING SECURITY DEVICES 907

Installing the Security Device 907

INSTALLING LICENSE MANAGER 909

Starting License Manager 911

Using License Manager 913

Sending a Dongle Packet File to Support 924

VIRTUAL CODEMETER ACTIVATION GUIDE 925

Introduction 925

Preparation 925

Setup for Online Systems 926

Setting up VCM for Offline Systems 927

Virtual CodeMeter FAQs 929

ABOUT API KEY GENERATION 931

AGENT INSTALLATIONS 934

MANUALLY INSTALLING THE WINDOWS AGENT 934

Agent Certificate Requirements 934

Manual Installations 934

Important Information 940

INSTALLING THE LINUX AGENT 941

Installing The Enterprise Agent on Linux 941

INSTALLING THE MAC AGENT 945

Comparing the Mac OS X Agent to the macOS Agent 945

Installing the macOS Managed Agent 946

Installing the Legacy Mac Agent 977

REFERENCES 982

FTK CENTRAL WORKFLOW 982

ADMINISTRATORS WORKFLOW 983

CASE MANAGERS WORKFLOW 983

© Exterro, Inc. All rights reserved

DATA SOURCES WORKFLOW 983
SUPPORTED FILE SYSTEMS AND DRIVE IMAGE FORMATS 984
File Systems *984*
Hard Disk Image Formats *986*

© Exterro, Inc. All rights reserved

About FTK Central

FTK Central is a one-stop, web-based solution assisting you with eDiscovery and Digital Forensic challenges. Right from identifying and collecting data from various data sources to reviewing and evaluating the evidentiary value of data. FTK Central provides an integrated approach to aid law enforcement officials, corporate security, and IT professionals.

About this manual

The FTK Central User Guide helps the users of FTK Central to do the following:

- Create and Manage Case
- Evidence Processing Options
- Create and Manage Custodians
- Reviewing Cases
- Create and Manage Users
- Configure System Settings, Site Servers and Agents
- Configure data sources and Active Directories
- Create and Manage Custodians
- Create and Manage LitHolds
- Create and Manage Collections
- Automate Jobs using FTK Connect

For information about new features, fixed issues, and known issues, see the *Exterro FTK Central Release Notes*.

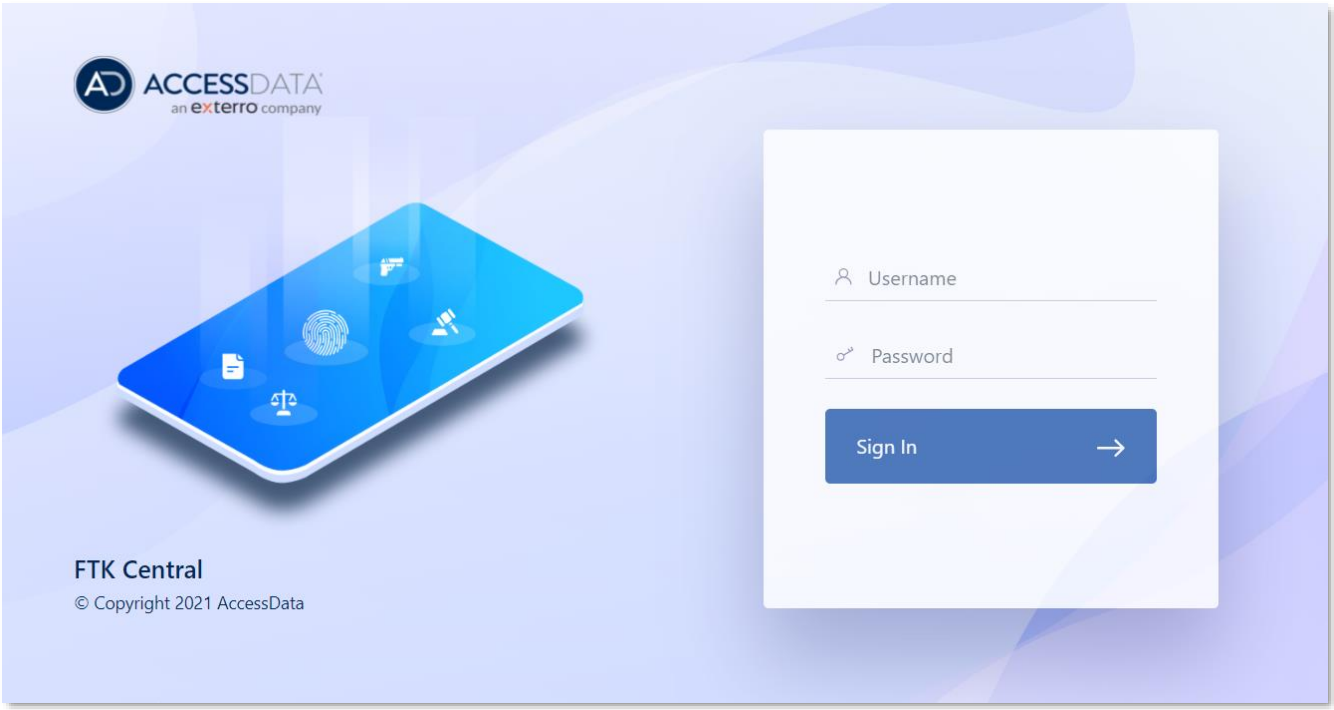
For information about software and hardware requirements, refer to the *Exterro FTK Central System Specification Guide*.

© Exterro, Inc. All rights reserved

Logging into FTK Central

To log into FTK Central:

1. Enter the FTK Central URL on the address bar and press Enter**.**
    - The FTK Central sign in screen is displayed.

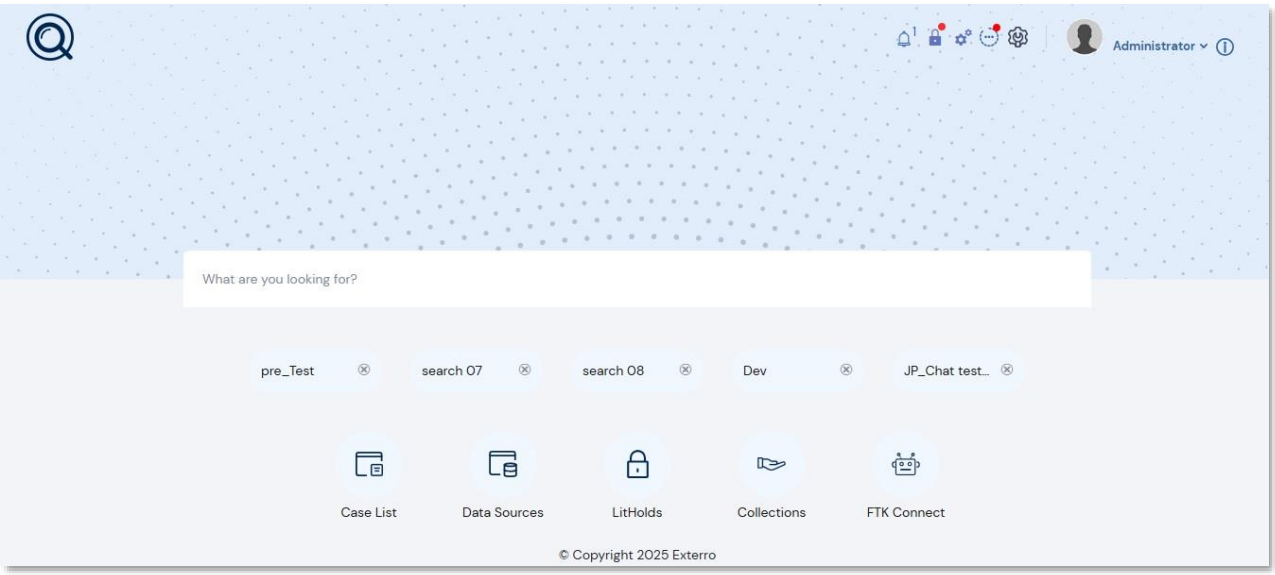


2. Enter the Username and Password.
3. Click **Sign In**.
    - The FTK Central Home Screen is displayed.

© Exterro, Inc. All rights reserved

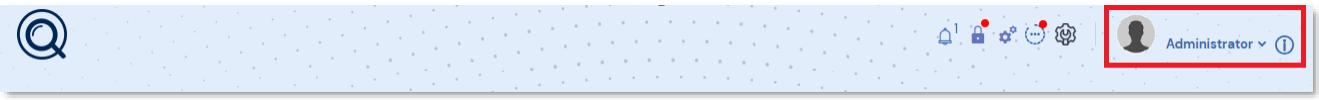
FTK Central Home Screen

Your home screen may look different from the image seen here. The contents of the home screen is dependent on the FTK Central modules/add-ons that are licensed for your company.



User Information

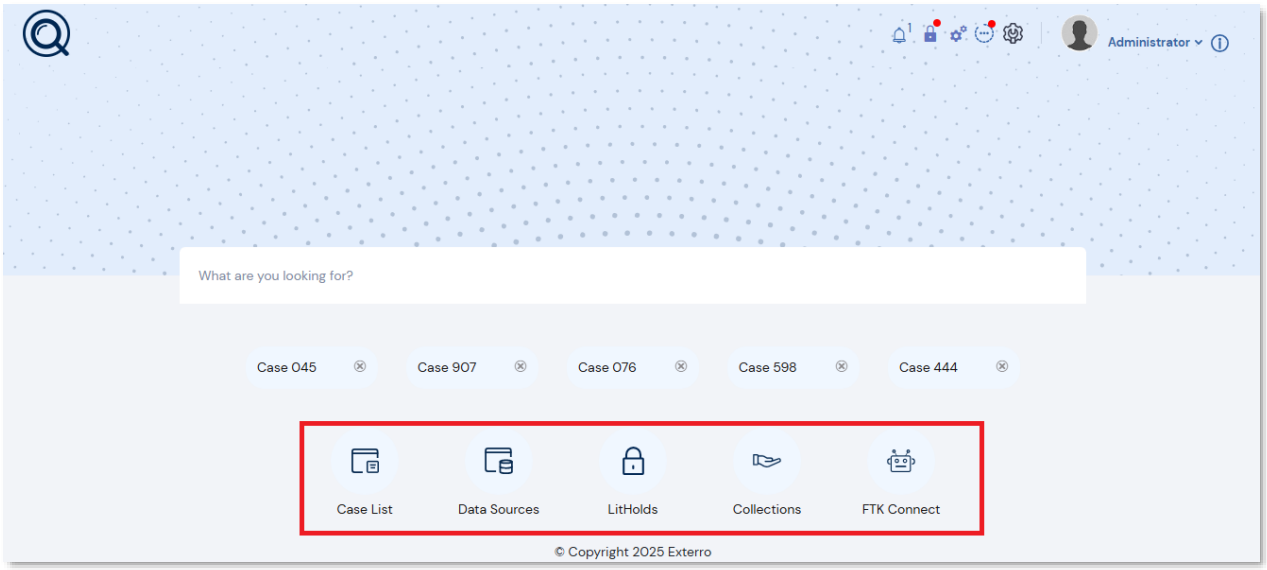
The logged in username with their title will be displayed on the top-right corner of the home screen.



© Exterro, Inc. All rights reserved

Quick Links

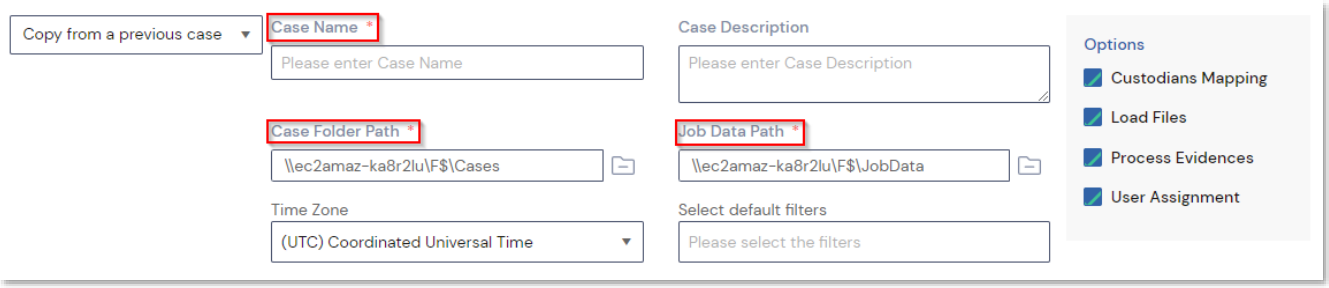
The recently viewed entities will be listed in the home page as displayed below.



You can click on it to navigate to that particular file or click **Remove** against the file to be removed from the quick link.

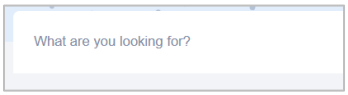
Mandatory Fields

Some of the fields in the application are mandatory and you cannot skip providing a value to it. Such mandatory fields are marked with an asterisk * against it.

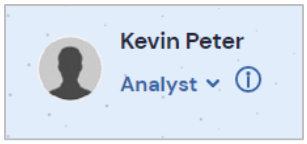


© Exterro, Inc. All rights reserved

User Interface Icon Dictionary

Component	Description
	The Home button lets you navigate to FTK Centrals home page at any stage of the application.
	The Cases tab lets you manage cases. The cases that are displayed will depend on the permissions that you have been assigned by the administrator.
	The Data Sources tab lets you manage custodians, computers, active directory groups network shares, evidence, Gmail, Google Drive, OneDrive, Microsoft Teams, Slack, SharePoint and Exchange. This tab allows you to manage these sources throughout the application, not just by case.
	The LitHolds tab lets you create and manage litigation holds.
	The Collections tab allows you to manage all collections.
	The FTK Connect tab allows you to create automated jobs.
	The Search Bar lets you search for cases efficiently without having to look through the Grid view.
	The Job Queue page lets users track both active and completed jobs and can be accessed from all pages.
	The Management page lets administrators perform global management tasks and can be accessed from all pages.
	The Live Preview status allows users to see the last 5 connected agents. If an agent has been offline and the user has chosen to get notified

© Exterro, Inc. All rights reserved

Component	Description
	about the agent regaining connection to the site server, the IP/Hostname will be listed here.
	Actions specific to the logged-in user that affects the user's account. Allows you to logout of the application. The user's first, last name and the username of the user will appear.
	The Information tab will open a prompt with version information of the application.

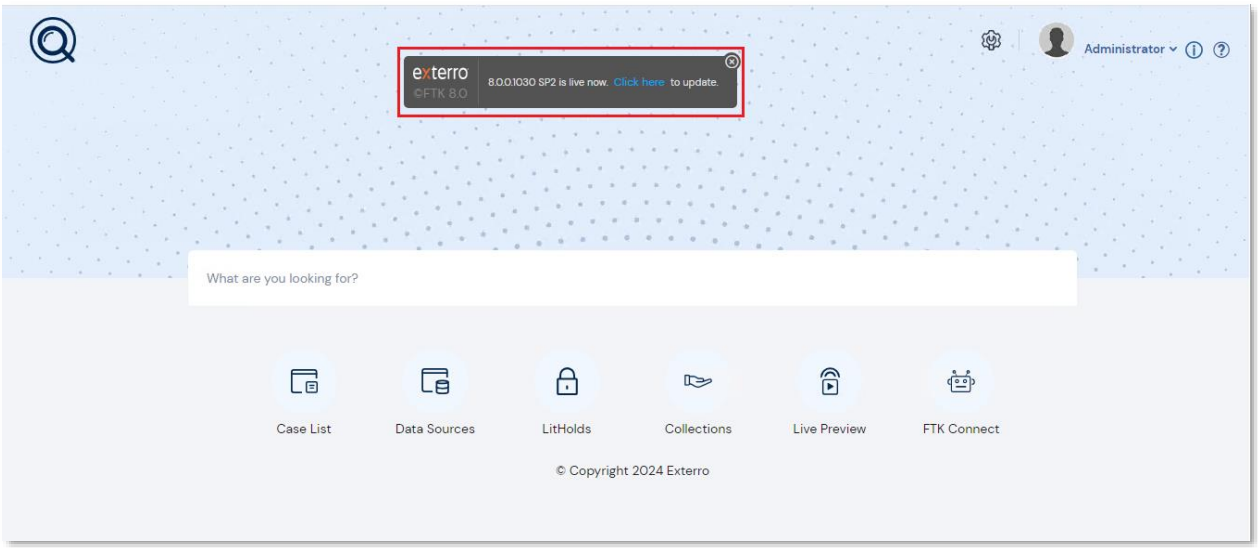
© Exterro, Inc. All rights reserved

FTK Upgrade Packages

For the FTK Standalone users who navigate to the FTK Central application via the Smart View feature, a package upgrade notification banner will be displayed whenever a new version of the application is published.

You can click on the link from the banner to automatically download the package and upgrade the FTK Standalone application to the latest version.

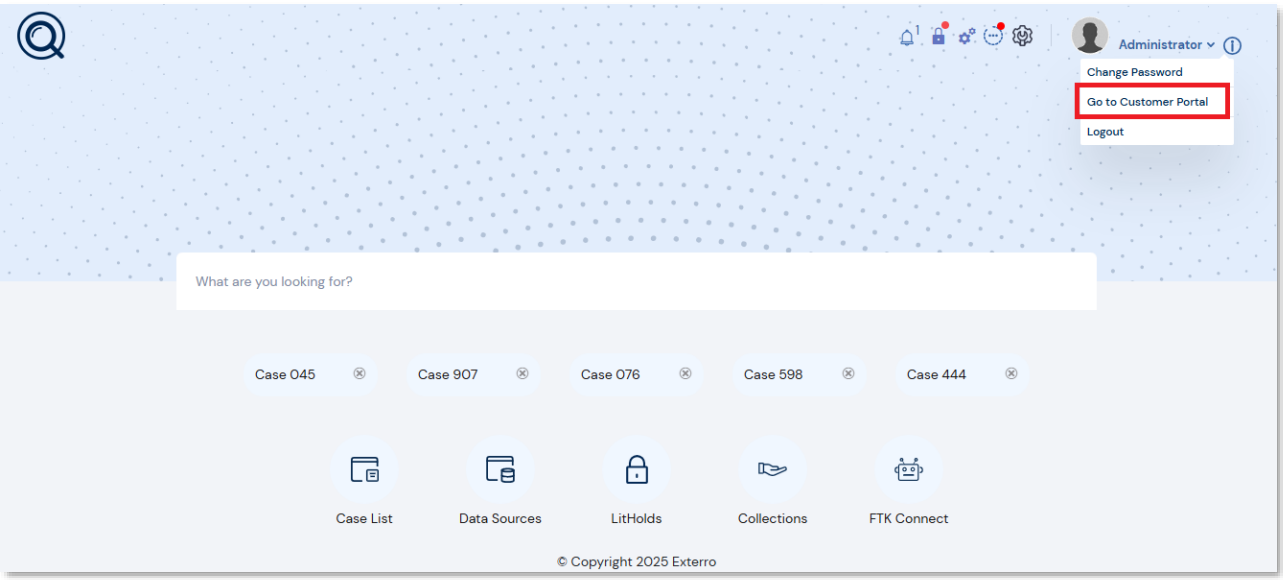
Note: Ensure the 7-Zip file archiver is installed in the system where the FTK Standalone application is installed.



© Exterro, Inc. All rights reserved

FTK Customer Portal

FTK Customer Portal is a centralized user interface (UI) that provides you with all the information, clarifications, and support related to the FTK Central. You can access this portal by clicking on the **Go to Customer Portal** option from the user information menu.



Customer Portal:

© Exterro, Inc. All rights reserved

This portal consists of the following information:

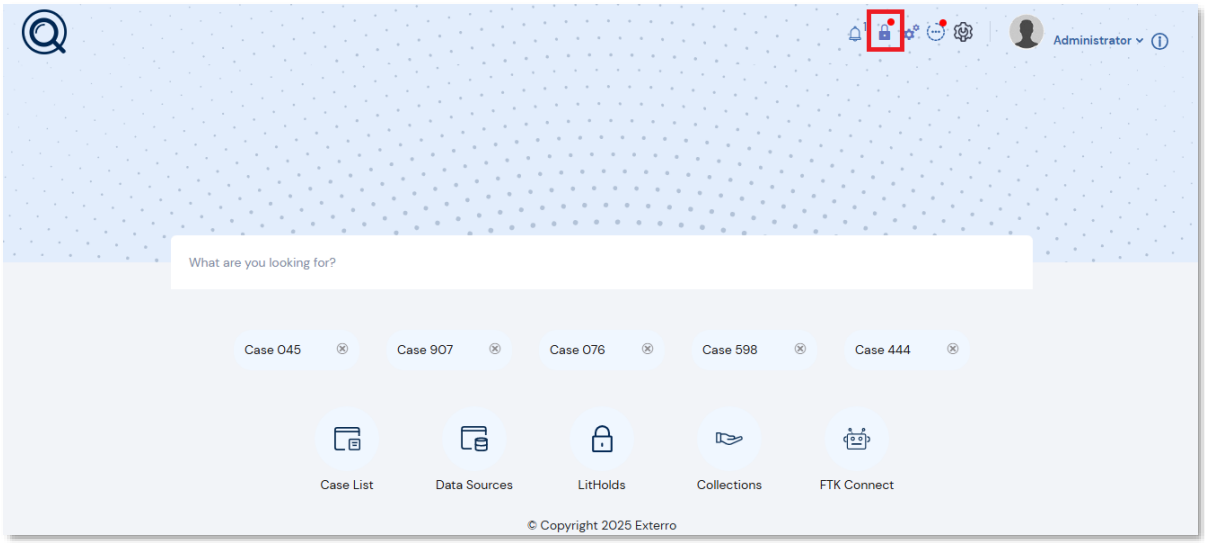
- **My Products** – Lists the products you have purchased.
- **Knowledge Base** – Exterro knowledge base consisting of articles, solutions, and FAQs related to the application.
- **Get Support** – To raise support tickets and resolve issues related to the product.
- **Exterro Academy** – Training and certifications related to the Exterro products.
- **Submit Ideas** – A portal to submit your ideas and suggestions for the product.
- **Webcasts, Workshops, and Customer Newsletter** – Archives of all the webcasts, workshops, and newsletters that the Exterro organization has published.
- **Events and Webinars** – Details of all the past and upcoming events and webinars that Exterro organized.
- **What's New** – The Exterro product download page from where you can access the latest version of release notes.
- **User Guide** - The Exterro product download page from where you can access the latest version of user guide.

© Exterro, Inc. All rights reserved

Encrypt Evidence List

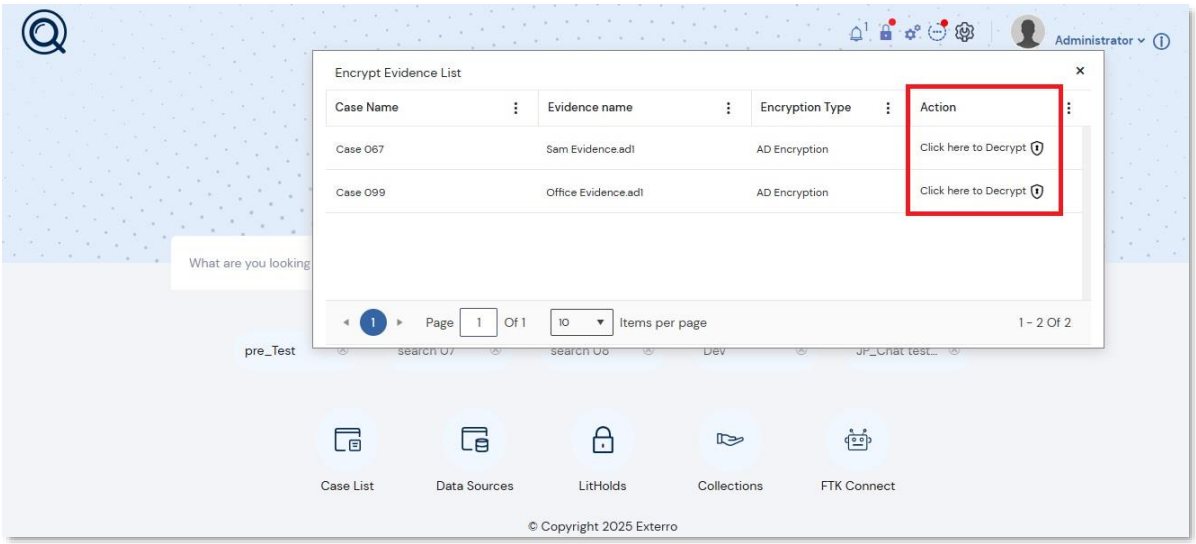
You can click on the icon to view all the encrypted evidence added to the cases via AWS S3. This list displays only the encrypted evidence using the following methods:

- Uploaded from the local directory to the AWS S3 and added to a new or existing case.
- Adding evidence to a case via AWS S3



You can decrypt the required evidence by clicking on the icon displayed against it. Refer to the Evidence Decryption section for more details.

© Exterro, Inc. All rights reserved

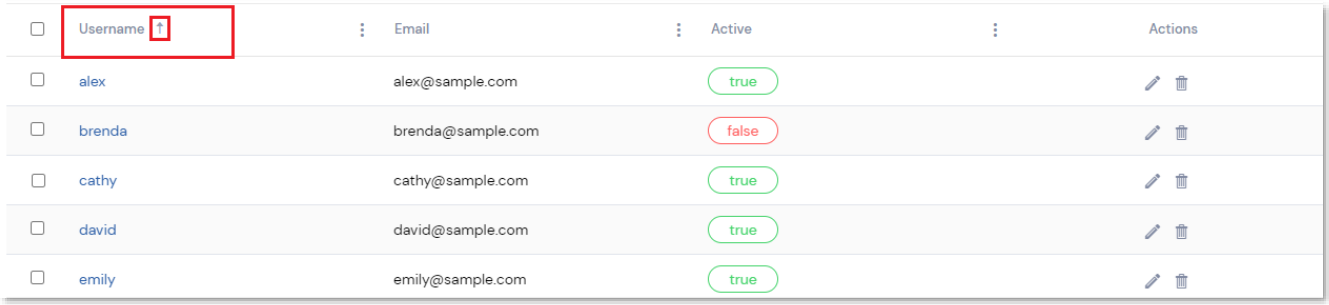


© Exterro, Inc. All rights reserved

FTK Central UI Guide

Sorting Columns

All the lists in FTK Central can be sorted as required. You can click on the column header by which you want to sort and an arrow mark will be displayed. You can toggle the arrow to ↑ or ↓ to sort in Ascending or Descending order.



Applying Filters

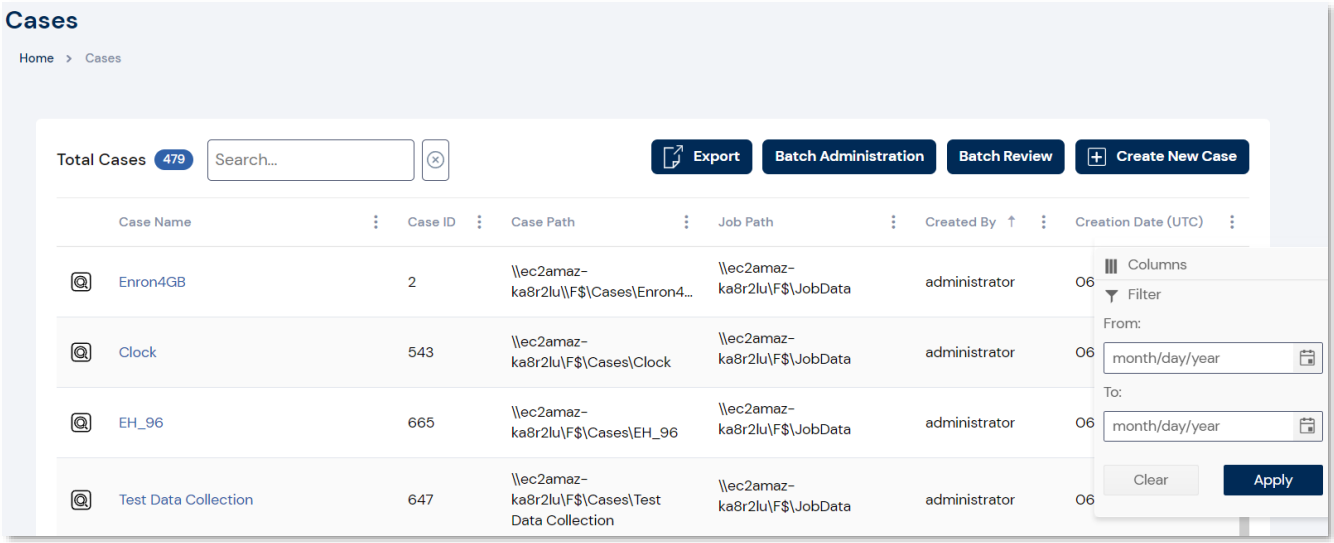
When there are multiple records, you can always use a filter to display the required records. The filter criteria may depend upon the type of records you intend to filter, however, you follow the steps below to filter any records.

For example, when looking at the Cases list, there could be hundreds of items. You may want to view only the items that pertain (not limited to) to a certain creation date or case name. To view only the items that include specific creation date ranges, you can filter the records by using **Creation Date** filter.

© Exterro, Inc. All rights reserved

To apply filters:

1. Click the More options against the column header.
2. Click **Filter**.
    - The available filter criteria for the column is displayed.



3. Configure the required filter.
4. Click **Filter**.

Note: You can click **Clear** to reset the filters.

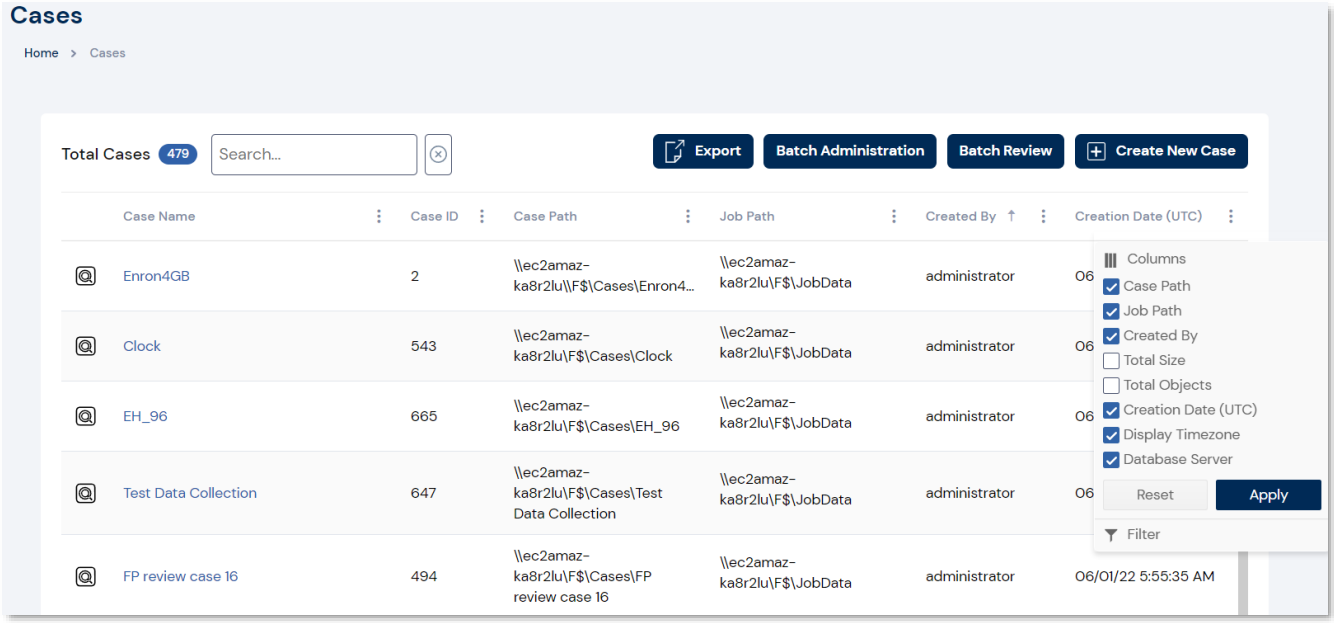
© Exterro, Inc. All rights reserved

Show/hide Columns

Based on the need, you can choose to either show or hide a column while viewing a list of entities. However, some columns are mandatory for identification and hence cannot be hidden. You can show/hide the remaining columns.

To show/hide columns:

1. Click More options against any column header in the list.
2. Click **Columns**.
    - The optional (non-mandatory) columns will be displayed.

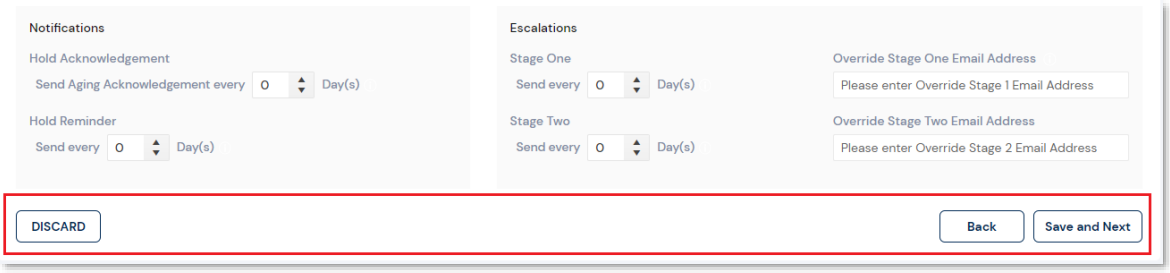


3. Select the columns to be displayed.
4. Click **Apply**.

© Exterro, Inc. All rights reserved

Navigating between pages during a process

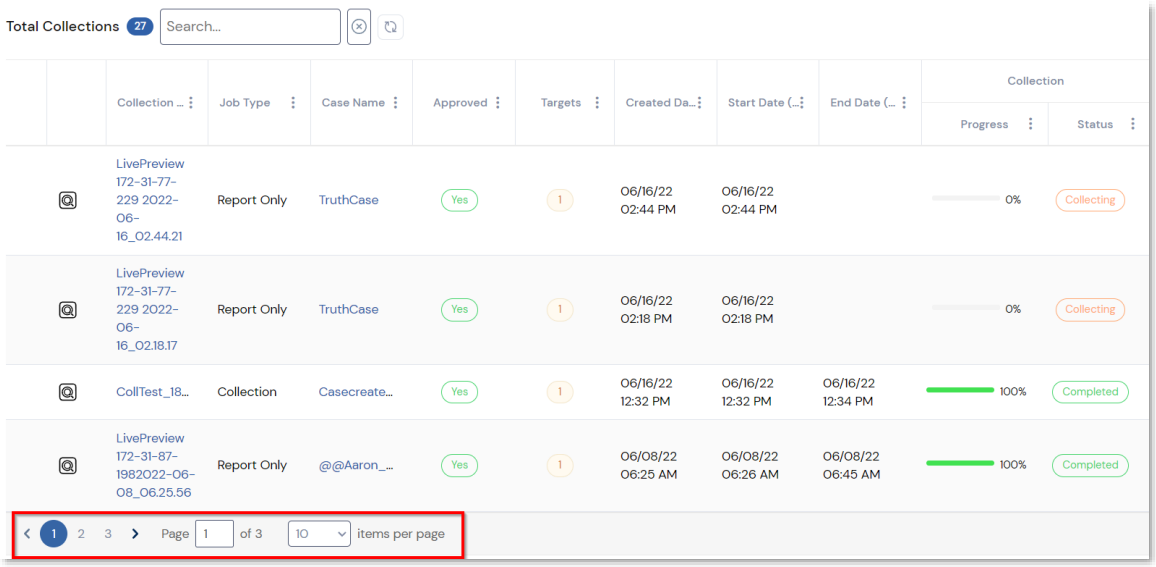
While performing a task involving multiple pages, you are provided with navigation buttons to go back to the previous page, to the next page, or to discard the whole process.



- You can click **Back** to navigate to the previous page.
- You can click **Save and Next** to save the provided information and move to the next page.
- You can click **Discard** to cancel the creation/update.

Pagination

FTK Central allows you to choose the number of records to be displayed in a page as per your convenience. You can select 10, 25, 50, 75, or 100 items per page.

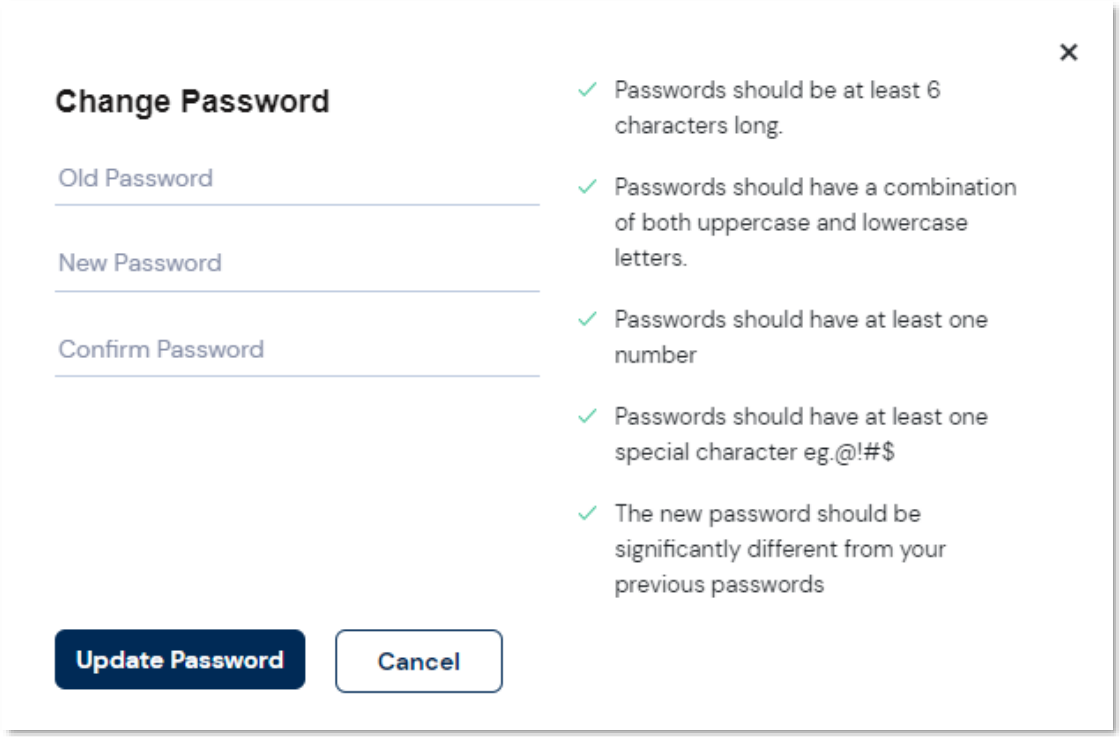


Also, you can navigate between the pages by either clicking **Previous** ‹ or **Next** › to navigate to previous or next page respectively.

© Exterro, Inc. All rights reserved

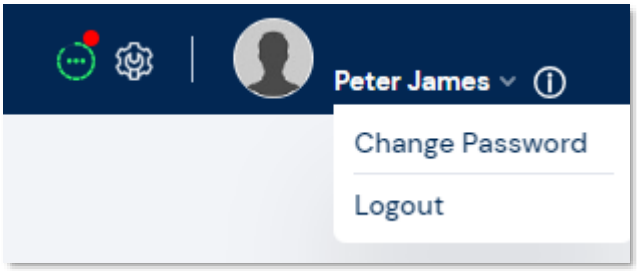
Changing the login password of FTK Central

You can change you application password by clicking on drop-down icon against your user name from any page and select **Change Password**.



Logging Out of FTK Central

You can log-out or terminate your session by clicking on drop-down icon against your user name from any page and select **Logout**.



© Exterro, Inc. All rights reserved

Before You Begin

- Your ability to perform actions in the FTK Central software is controlled by permission(s). If you are unable to perform the actions as described in this documentation, please contact Support team.
- Some of the features discussed in the document are add-on features. If you are unable to view or use it fully, please contact the Administrator to verify the features licensed for your organization.

FTK Central Requirements

The application displays the Exterro web-based console that you can open from any computer connected to the network.

All users are required to enter a username and password to open FTK Central.

What you can see and do in the application depends on your product license and the rights and permissions granted to you by the administrator. You may have limited privileges based on the work you do.

See About User Accounts section.

Software Requirements

The following are required for using the features available in FTK Central:

- HTML-5 Supported browser such as (but not limited to):
  - Google Chrome
  - Mozilla Firefox
  - Microsoft Edge

Hardware Requirements

- Use a display resolution of 1280 x 1024 or higher.

  Press **F11** to display the application in full-screen mode and maximize the viewing area.

© Exterro, Inc. All rights reserved

About User Accounts

Each user that uses FTK Central must log in with a user account. Each account has a username and password. Administrators configure the user accounts.

User accounts are granted permissions based on the tasks those users perform. For example, one account may have permissions to create and manage cases while another account has permissions only to review files in a case.

Your permissions determine which items you see and the actions you can perform in FTK Central.

There is a Application administrator account.

Opening FTK Central

You can use FTK Central to perform many application tasks.

You can launch the application from an approved web browser on any computer that is connected to the application server on the network.

There are multiple methods to open FTK Central:

- If you know the IP address/Host Name of the application server, the address will look like: <Hostname>:<Port – 4443 is the default>.
- Alternatively, you can open FTK Central by using the application icon located on the desktop if the application has been installed locally on the machine you are accessing.

Whenever you access FTK Central you will be prompted to log in. Your administrator will provide you with your username and password.

© Exterro, Inc. All rights reserved

To open FTK Central in a browser

To open FTK Central in a browser:

1. Open a supported browser.
    a. Google Chrome
    b. Microsoft Edge
    c. Mozilla Firefox
2. Enter the following URL in the browser's address field:

    <Hostname>:<Port – 4443 is the default>

    Where <HostName>is the host name or the IP address of the application server.

    This opens the login page.

    You can save this webpage as a bookmark.
3. The login page will display the product name as well as the form fields required for your username and password.
4. On the login page, enter the username and password for your account.
5. Click **Sign In**.
    a. If you have entered account details which are not yet active or incorrect you will be notified with an incorrect username or password prompt.
6. Successful logins will open FTK Central in its entirety.

© Exterro, Inc. All rights reserved

Cases

Case information is stored in a database and allows case administration as each new case is created. During case creation information must be provided for primary details, custodian mapping, load file imports.

Elements of Cases

Creating Cases	• Primary Details
	• Custodian Mapping
	• Load Files
	  ○ Importing Generic load files
	  ○ Importing QuinC/Summation DII load file
	  ○ Importing Concordance/Relativity load file
	• Process Evidence
	• Copy from a previous case
	• User Assignment
	• Case Index Status

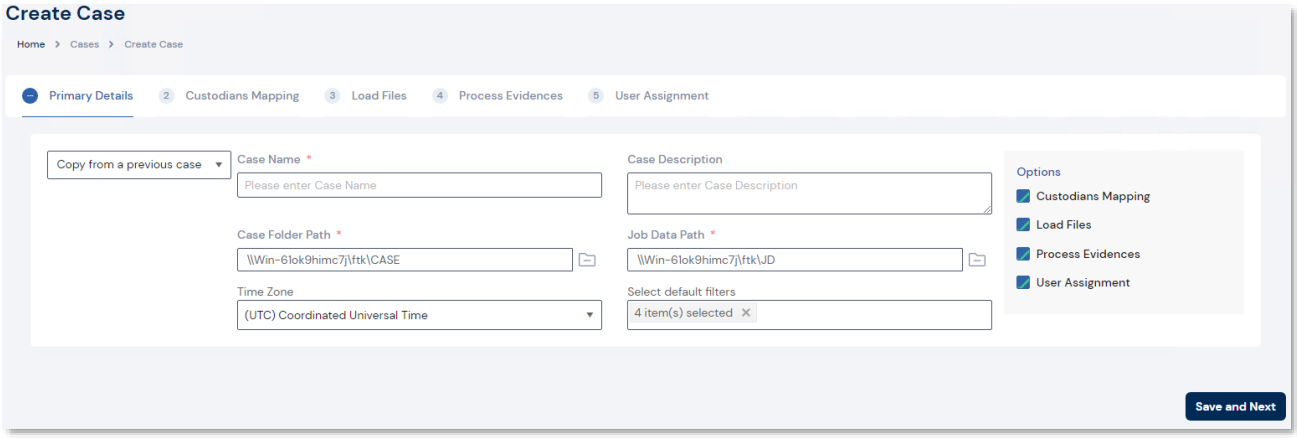
Creating Cases

To create a case:

1. From the home page, click **Case List**.
2. Click **Create New Case**.

© Exterro, Inc. All rights reserved

Primary Details



To add the primary details:

1. Configure the primary details of a case as explained below.

Options	Description
Copy from a previous case	Allows you to use previously created case's details. Options available to copy range from, but are not limited to, copying custodians, custom fields, coding panels and labels.
Case Name	Provide a name for the case. The case names must be only alphanumeric characters. Special characters will cause the case creation to fail.
Case Description	Provide a description for the case.
Case Folder Path	Allows you to specify a local path or a UNC network path to the case folder. This path is the location where all case data is stored. ***Note:*** *Only unique file storage paths should be configured i.e., the same location path cannot be used for two or more cases simultaneously*

© Exterro, Inc. All rights reserved

Options	Description
Job Data Path	This sets the responsive folder path for data from jobs. Under this path, a folder is created for each job. The job sub-folders contain job reports and ad1 files for collected files.
Time Zone	This sets the time zone displayed within the case.
Default Filters	This sets default quick filters to a case. Filters available range from, Hide Duplicates, Ediscovery Refinement, Hide Containers and Hide Bookmarks. **This option is dependent on the product type value set in the ADG.weblabselfhost.exe.config file**. If set as ediscovery, these default filters will be selected by default during case creation. If set as forensics, these default filters will not be selected by default during case creation.
Custom Case Properties	This option will allow users to select custom properties that have been defined by an administrator. Refer to the Creating Custom Case Properties section.
Options	Allows you to pick which optional processes to add to the case creation. The processes are: • **Custodian Mapping** – To configure the custodians of the evidence in this case. You can associate existing custodians or add new custodians. Custodians for the case can be configured later, but should be done before processing evidence. • **Load Files** – To configure any load files that you would like to import into a case. • **Process Evidence** – To add evidence items and set the options for how the evidence is processed when added to the case.

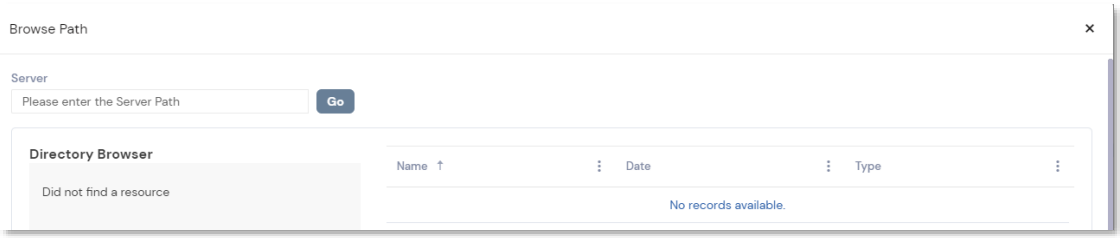
© Exterro, Inc. All rights reserved

Options	Description
	• **User Assignment** – To add specific users/user groups to a created case. ***Note**: Click Submit if none of the (optional) options are required.*

Note: The location for **Case Folder Path** and **Job Data Path** will be automatically populated based on the case defaults configured. However, you can change the path if required. To do so,

i. Click **Folder** against the Results Path field.

- The below page appears.

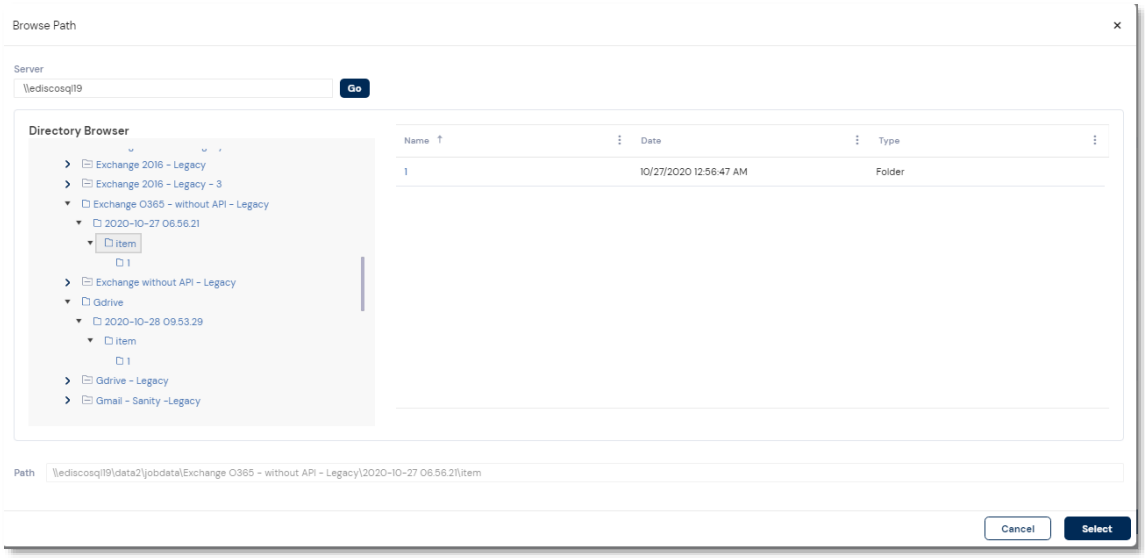


ii. Enter the **Server Path**.

iii. Click **Go** to view the directories available on the server.

iv. Select the folder to be where the results are to be saved.

© Exterro, Inc. All rights reserved



v. Click **Select**.

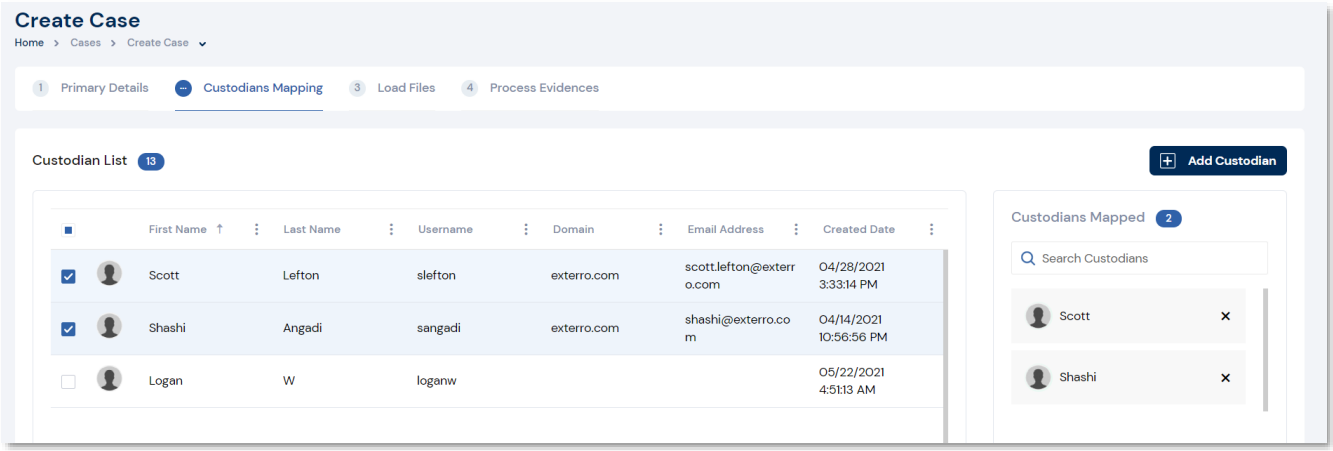
2. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Custodian Mapping

To map a custodian:

1. Select the custodians to be added to the case.
    - The selected custodians are displayed on the Custodians Mapped pane.



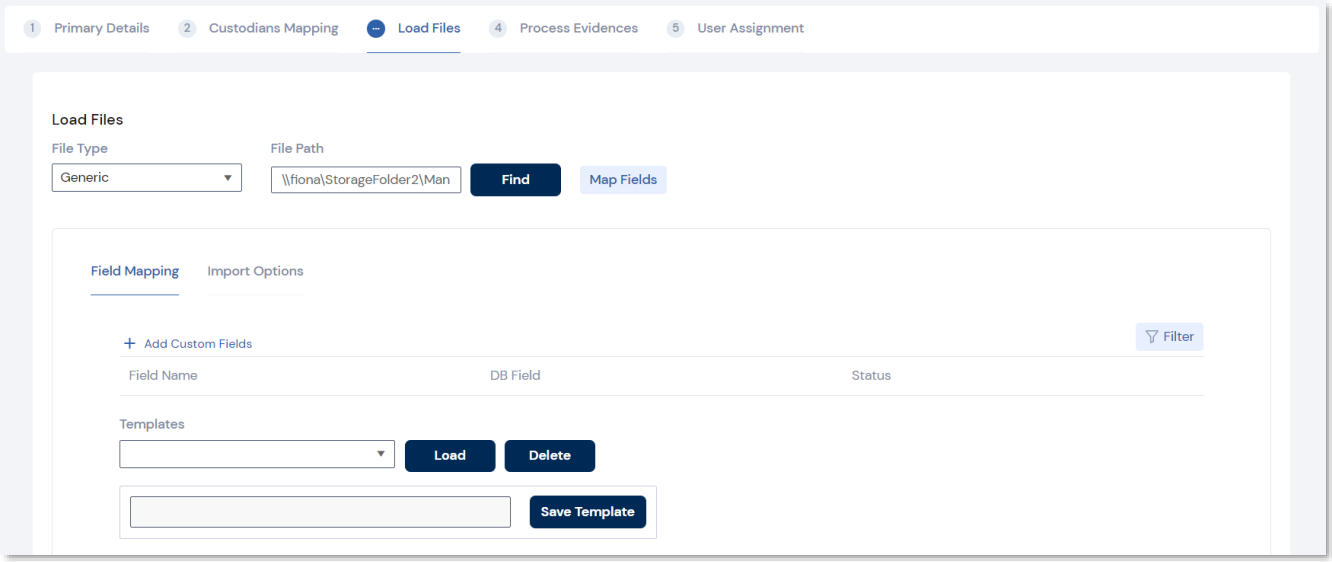
Note: You can also click **Add Custodian** to create a new custodian from this page and add to the case.

2. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Load Files

You import evidence by using a load file, which allows you to import metadata and physical files, such as native, image, and/or text files that were obtained from another source, such as a scanning program or another processing program.



You can import the following types of load files:

- **Summation DII** - A proprietary file type from Summation.
- **Generic** - A delimited file type, such as a CSV file.
- **Concordance/Relativity** - A delimited DAT file type that has established guidelines as to what delimiter should be used in the fields. This file should have a corresponding LFP or OPT image file to import.

When importing, you must specify which import file fields should be mapped to database fields. Mapping the fields will put the correct information about the document in the correct columns in the case.

After clicking **Map Fields**, a process runs that checks the imported load file against existing case fields. Most of the import file fields will automatically be mapped for you. Any fields that could not be automatically mapped are flagged as needing to be mapped. Users can create Custom Fields if required.

© Exterro, Inc. All rights reserved

Optionally, users can utilize the **Run Validation** option. This will verify:

- The path information within the load file is correct.
- The records contain the correct fields. For example, the system verifies that the delimiters and fields in a Generic or Concordance/Relativity file are correct.
- All physical files are present (Native, Image and Text) which are listed in the load file.

Importing Generic load files

To import generic load file:

1. Select **Generic** as the **File Type**.
2. Enter the **File Path** or click **Find** to select the path.
3. Click **Map Fields** to configure the required values for Field Mapping.
    i. Choose a similar field (e.g. mapping a text field to a text field, a date field to a date field, etc.) to use for mapping.
    ii. Choose **SKIP THIS FIELD** to ignore the field.
    iii. If neither of the previous options works, talk to the case manager or application administrator about creating a custom field to be used for mapping.
    iv. Select **Skip Unmapped** to mark all unmapped fields with **SKIP THIS FIELD**.

Note: Alternatively, you can use an existing Field Mapping Template.

© Exterro, Inc. All rights reserved

4. Select the correct delimiters by clicking **Filter** as explained below.

Fields	Description
First Row Contains Field Names	Enable this to consider the first row as Column headers.
Field Separator	Select a character that is used as a delimiter. i.e., the character to be placed between the columns.
Quote Separator	Select a character that is placed on either side of the value within each of the columns.
Multi-Entry Separator	Select a character that is used to separate multi-entries in the column.
Return Placeholder	Select a character to mark the end of a line in a load file.

5. Click **Import Options** to set specific options.
6. Select **Enable Fast Imports** to exclude database indexes while importing.
7. Select the **Record Handling Options** as explained below.

Fields	Options	Description
New Record	Add	To add the new records present in the load file to the case.
	Skip	To skip adding the new records present in the load file to the case
Existing Record	Update	To update duplicate records with the record being imported.
	Overwrite	To overwrite any duplicate records with the record being imported.
	Skip	To skip adding the existing records in load file to the case

8. Select the **Date Format** as needed. This format appears in the load file system, allowing the system to properly parse the date to store in the database.

Note: All dates are stored in the database in a yyyy-mm-dd hh:mm:ss format.

9. Select the **Load File Timezone** to choose the time zone that the load file was created. The values can be converted to a normalized UTC value in the database.
10. Click **Run Validation** to verify the import and then click **Finish**.

© Exterro, Inc. All rights reserved

Importing QuinC/Summation DII load file

To import QuinC/Summation DII load file:

1. Select **QuinC EDII** as the **File Type**.
2. Enter the **File Path** or click **Find** to select the path.
3. Click **Map Fields** to configure the required values for Field Mapping.
    i. Choose a similar field (e.g. mapping a text field to a text field, a date field to a date field, etc.) to use for mapping.
    ii. Choose **SKIP THIS FIELD** to ignore the field.
    iii. If neither of the previous options works, talk to the case manager or application administrator about creating a custom field to be used for mapping.
    iv. Select **Skip Unmapped** to mark all unmapped fields with **SKIP THIS FIELD**.

Note: Alternatively, you can use an existing Field Mapping Template.

4. Click **Import Options** to set specific options as explained below.

Fields	Description
Enable Fast Imports	This will exclude database indexes while importing.
Page count follows DocID	Enable this if your DII file has an @T value that contains both a Doc ID and a page count.
Import OCR/Fulltext	Select to import OCR or Full Text documents for each record.
Import Native Documents	Enable this option to import native files for each record.
Process files to extract metadata	Enable this to import only the metadata that exists on the load file and not process native files as you import them with a load file.
Import Images	Enable this to load images.

© Exterro, Inc. All rights reserved

5. Select the **Record Handling Options** as explained below.

Fields	Options	Description
New Record	Add	To add the new records present in the load file to the case.
	Skip	To skip adding the new records present in the load file to the case
Existing Record	Update	To update duplicate records with the record being imported.
	Overwrite	To overwrite any duplicate records with the record being imported.
	Skip	To skip adding the existing records in load file to the case

6. Select the **Date Format** as needed. This format appears in the load file system, allowing the system to properly parse the date to store in the database.

Note: All dates are stored in the database in a yy-mm-dd hh:mm:ss format.

7. Select the **Load File Timezone** to choose the time zone that the load file was created. The values can be converted to a normalized UTC value in the database.
8. Click **Run Validation** to verify the import and then click **Finish**.

© Exterro, Inc. All rights reserved

Importing Concordance/Relativity load file

To import concordance/relativity load file:

1. Select **Concordance/Relativity** as the **File Type**.
2. Enter the **File Path** or click **Find** to select the path.
3. Enter the **Image Path** or click **Find** to select the path. This may be an LFP or OPT file type.
   - **OPT** - Concordance file type that contains preferences and option settings associated with the files.
   - **LFP** – IPRO file type that contains load images and related information.
4. Click **Map Fields** to configure the required values for Field Mapping.
   i. Choose a similar field (e.g. mapping a text field to a text field, a date field to a date field, etc.) to use for mapping.
   ii. Choose **SKIP THIS FIELD** to ignore the field.
   iii. If neither of the previous options works, talk to the case manager or application administrator about creating a custom field to be used for mapping.
   iv. Select **Skip Unmapped** to mark all unmapped fields with **SKIP THIS FIELD**.

Note: Alternatively, you can use an existing Field Mapping Template.

5. Select the correct delimiters by clicking **Filter** as explained below.

Fields	Description
First Row Contains Field Names	Enable this to consider the first row as Column headers.
Field Separator	Select a character that is used as a delimiter. i.e., the character to be placed between the columns.
Quote Separator	Select a character that is placed on either side of the value within each of the columns.
Multi-Entry Separator	Select a character that is used to separate multi-entries in the column.
Return Placeholder	Select a character to mark the end of a line in a load file.

© Exterro, Inc. All rights reserved

6. Click **Import Options** to set specific options as explained below.

Fields	Description
Enable Fast Imports	This will exclude database indexes while importing.
Import OCR/Fulltext	Select to import OCR or Full Text documents for each record.
Import Native Documents	Enable this option to import native files for each record.
Process files to extract metadata	Enable this to import only the metadata that exists on the load file and not process native files as you import them with a load file.
Import Images	Enable this to load images.

7. Select the **Record Handling Options** as explained below.

Fields	Options	Description
New Record	Add	To add the new records present in the load file to the case.
	Skip	To skip adding the new records present in the load file to the case
Existing Record	Update	To update duplicate records with the record being imported.
	Overwrite	To overwrite any duplicate records with the record being imported.
	Skip	To skip adding the existing records in load file to the case

8. Select the **Date Format** as needed. This format appears in the load file system, allowing the system to properly parse the date to store in the database.

Note: All dates are stored in the database in a yyyy-mm-dd hh:mm:ss format.

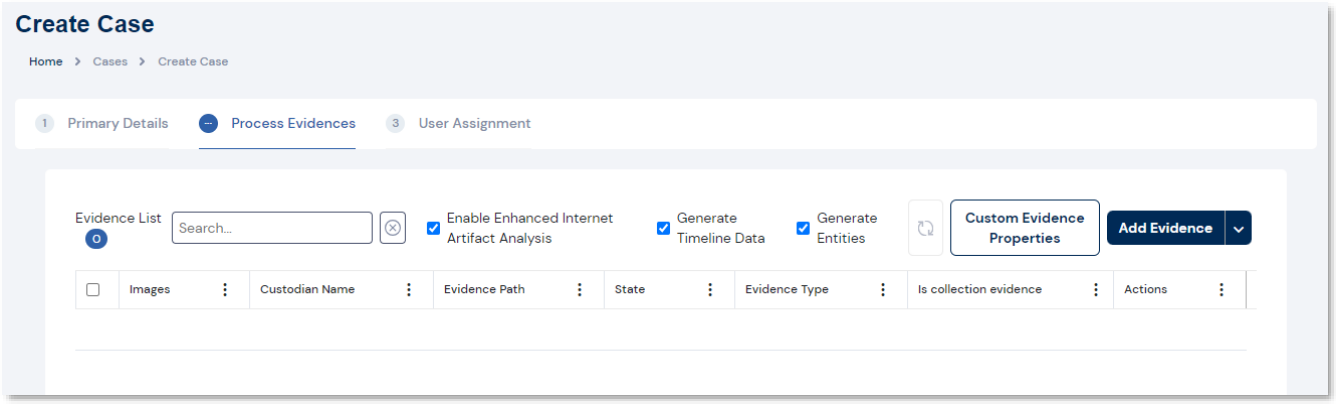
9. Select the **Load File Timezone** to choose the time zone that the load file was created. The values can be converted to a normalized UTC value in the database.
10. Click **Run Validation** to verify the import and then click **Finish**.

© Exterro, Inc. All rights reserved

To save a Field Mapping template:

1. When you have selected the relevant field mapping options for a specific load file type, enter a template name in the templates section.
2. Click **Save Template**.
   a. Saved templates can be loaded by selecting it within the Templates drop-down list.

Process Evidence



During case creation you can use the Process Evidence section to specify the data that you want to add. You specify to add either parent folders or individual files.

© Exterro, Inc. All rights reserved

For example, you could have a parent folder with a set of subfolders.

- \\10.10.3.39\EvidenceSource\
  - \\10.10.3.39\EvidenceSource\John Smith
  - \\10.10.3.39\EvidenceSource\Bobby Jones
  - \\10.10.3.39\EvidenceSource\Samuel Johnson
  - \\10.10.3.39\EvidenceSource\Edward Peterson
  - \\10.10.3.39\EvidenceSource\Jeremy Lane

You could import the parent \\10.10.3.39\EvidenceSource\ as one evidence item. If you associated a custodian to it, all files under the parent would have the same custodian.

Additionally, you could have each subfolder to be its own evidence item, and then you could associate a unique custodian to each item. An evidence item can either be a folder or a single file. If the item is a folder, it can have other subfolders, but they would be included in the item. This can be done by selecting **Import subfolder as unique evidence items** and **Subfolder names are custodians**.

The following table lists the default Evidence Properties available during ingestion.

Options	Description
Evidence Name	Name of the evidence. This can be a custom name.
Evidence Path	The full pathname of the evidence file. Use universal naming convention (UNC) syntax in your evidence path for best results.
Evidence Number	Any numbering associated to evidence. This is optional.
Evidence Date	Any dates associated to the evidence. This is optional.
Custodian	Custodians (People) can be added and associated to specific evidence if required. This is optional.
Time Zone	Local machines must be set to the same time and date settings as the case evidence to correctly display all dates and times.

© Exterro, Inc. All rights reserved

Options	Description
Media Type	The media type will be automatically identified by FTK Central, however in rare occurrences you may need to select an option yourself.
Evidence Source	Source of the evidence being ingested. Computer, Mobile, CCTV or Body Cam. This is optional.
Suspect Name	Names of suspects relating to the evidence being ingested. This is optional.
Make and Model	Any specific make and model relating to the evidence being ingested. This is optional.
Place of Acquisition	Any specific location relating to the evidence being ingested. This is optional.
Notes	Any other notes relating to the evidence being ingested. This is optional.
Images	Any images/graphics relating to the evidence being ingested.

You can enable the following checkbox options to perform the corresponding operations for the case:

- **Generate Timeline Data** - To automatically generate the timeline data in the **Timeline View** of Review page.
- **Enable Enhanced Internet Artifact Analysis** – To categorize and display the information collected from browsers. The categorization will be displayed under the **Web Page Category** section of **Internet and Browser** filter.
- **Generate Entities** – To automatically identify and categorize entities from the case files including details such as phone numbers, email addresses, and social media profiles. This information can be viewed from the **Entity Management Dashboard** in the Review page.

Note: The above fields are enabled by default. You can disable the fields if required.

© Exterro, Inc. All rights reserved

To add an evidence item to a case:

1. Upon checking the Process Evidence option, you will be navigated to a new section.
2. Click **Add Evidence**.
3. Enter **Evidence Path**. Ensure this is a UNC path.

Note: Upon adding encrypted evidence, a pop-up will be displayed to perform the decryption process. Refer to the Evidence Decryption section for more details.

4. Click the **Explore** button to browse to the specified path and select the evidence. If it is a single file or folder, ensure it is selected in the item grid.
5. Click **Select**.
6. Select the **Time Zone**. Click **Apply To All** if required.
7. Click **Save**.

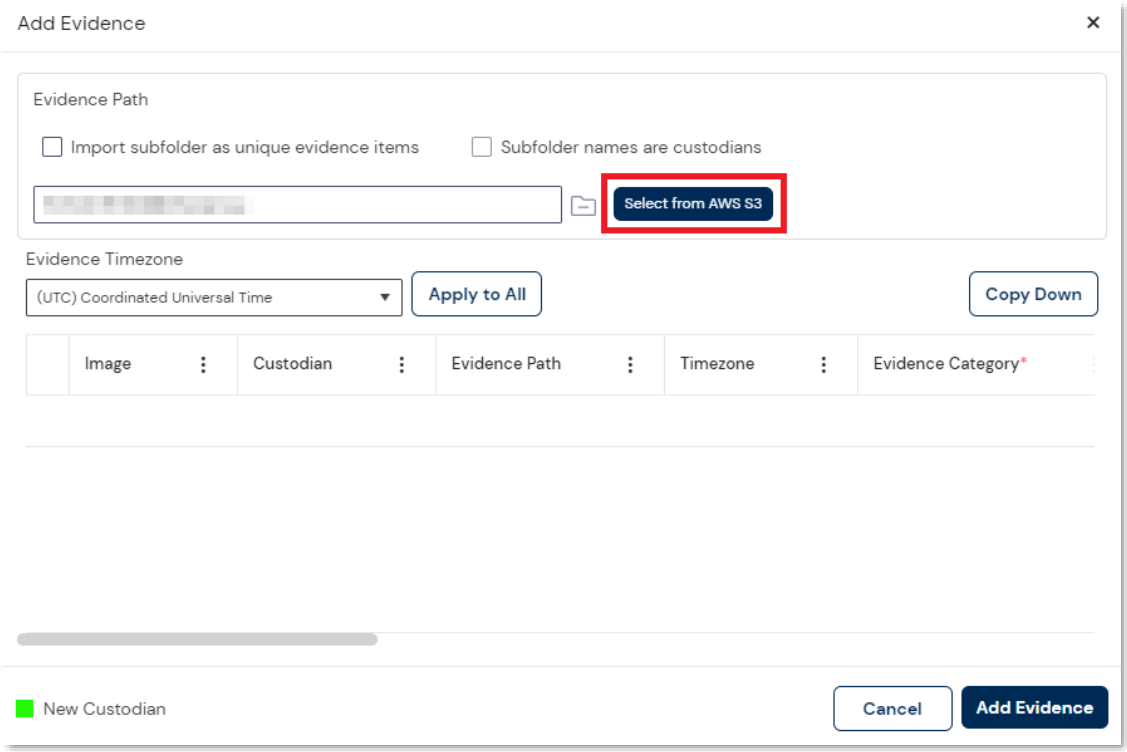
Note: Additionally, by clicking on **Copy Down**, the fields in the first row of the evidence grid will be copied to all other rows. Do not click this if the evidence being ingested do not share the same field data.

© Exterro, Inc. All rights reserved

To add evidence a case from AWS S3:

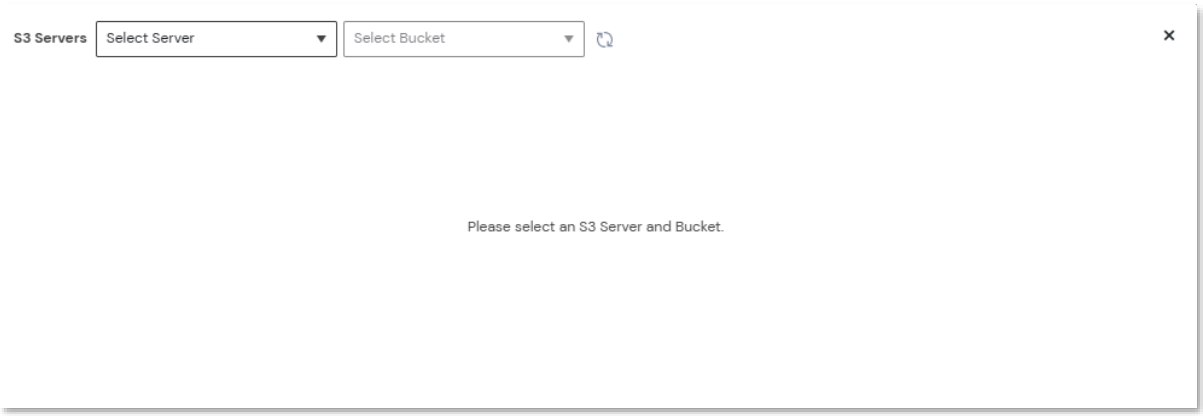
Note: This option displays only the S3 buckets configured within the AWS S3 Management section of **System Settings** in the FTK Central application.

1. From the Add Evidence pop-up, click on the Select from AWS S3 button.

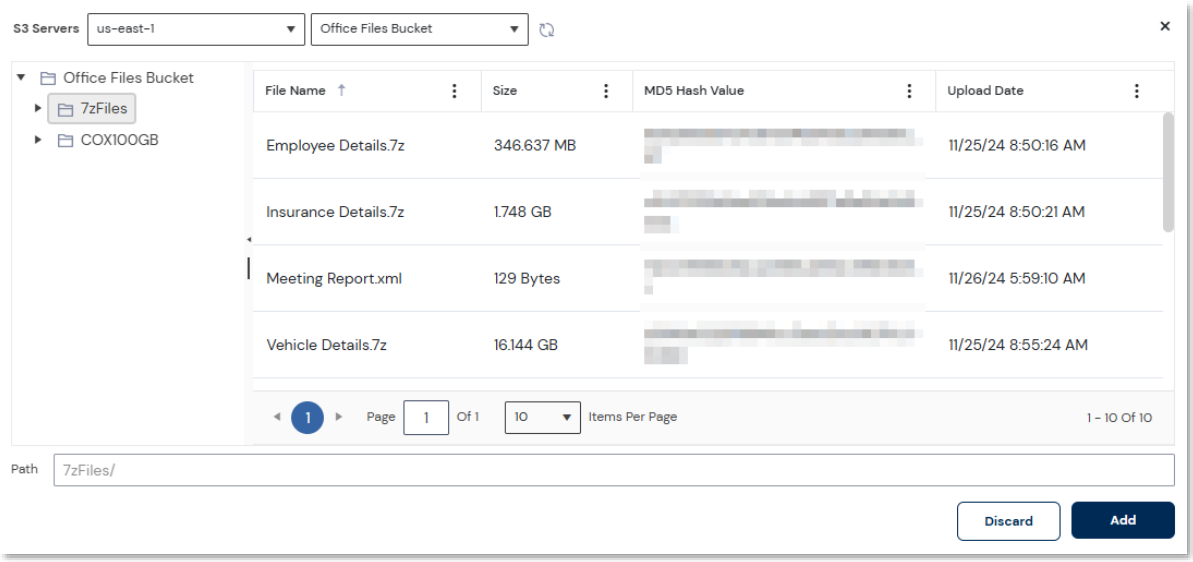


© Exterro, Inc. All rights reserved

2. Select the required **Server** and **Bucket** from the **S3 Servers** field.

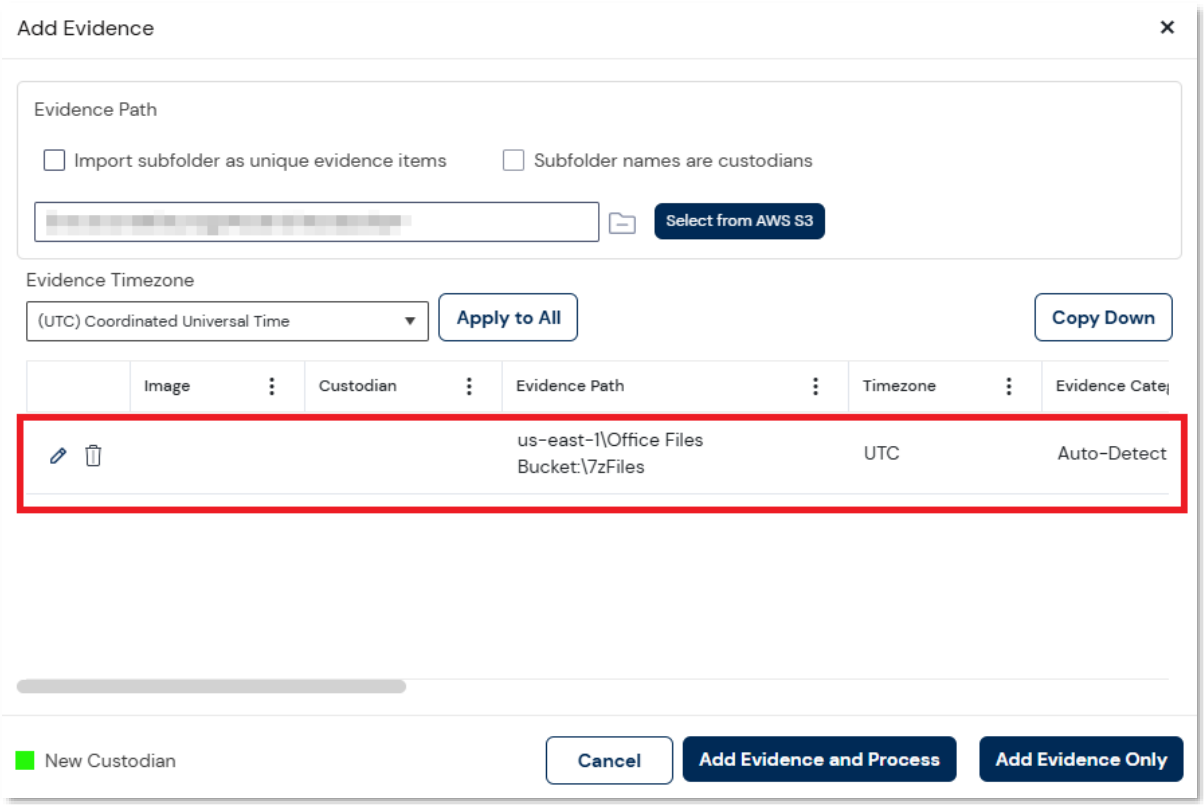


3. Select the required file or folder and click on **Add**.



© Exterro, Inc. All rights reserved

- The selected files and folders will be displayed in the **Add Evidence** pop-up.



4. Click on any one of the below buttons to perform the corresponding action:
   - **Add Evidence and Process** – To add the selected files to the case and process it.
   - **Add Evidence Only** – To only add the selected files to the case.

The **Add Evidence from AWS S3** job will be initiated to add the files/folders selected from the AWS S3 into the case.

Note: Regardless of how many files were selected from the S3 bucket, only one **Add Evidence from AWS S3** job will be initiated upon clicking on the **Add Evidence and Process** or **Add Evidence Only** button in the **Add Evidence** pop-up.

© Exterro, Inc. All rights reserved

To add an evidence item to a case using the CSV Template:

1. Upon checking the Process Evidence option, you will be navigated to a new section.
2. Click **Add Evidence > Import from CSV file**.
3. Click **Select files** to import.
4. If required, check **First row contains headers/1 or more custom columns**.
5. Click **Add Evidence**.

Note: CSV imports can use the following columns: Custodian, Evidence Path, Timezone, Evidence Source, Suspect Name, Evidence Number, Evidence Name, Evidence Date, Make and Model, Place of Acquisition, Notes, Images. However, only the evidence path is required. Other columns can be left empty.

Tip: Evidence files can be deleted and edited from the Evidence List by clicking on the **Context** button.

If the case had evidence added and processed previously, it will be listed here. By accessing the context menu, previous procession options can be displayed.

To select specific Processing Managers and Processing Profiles:

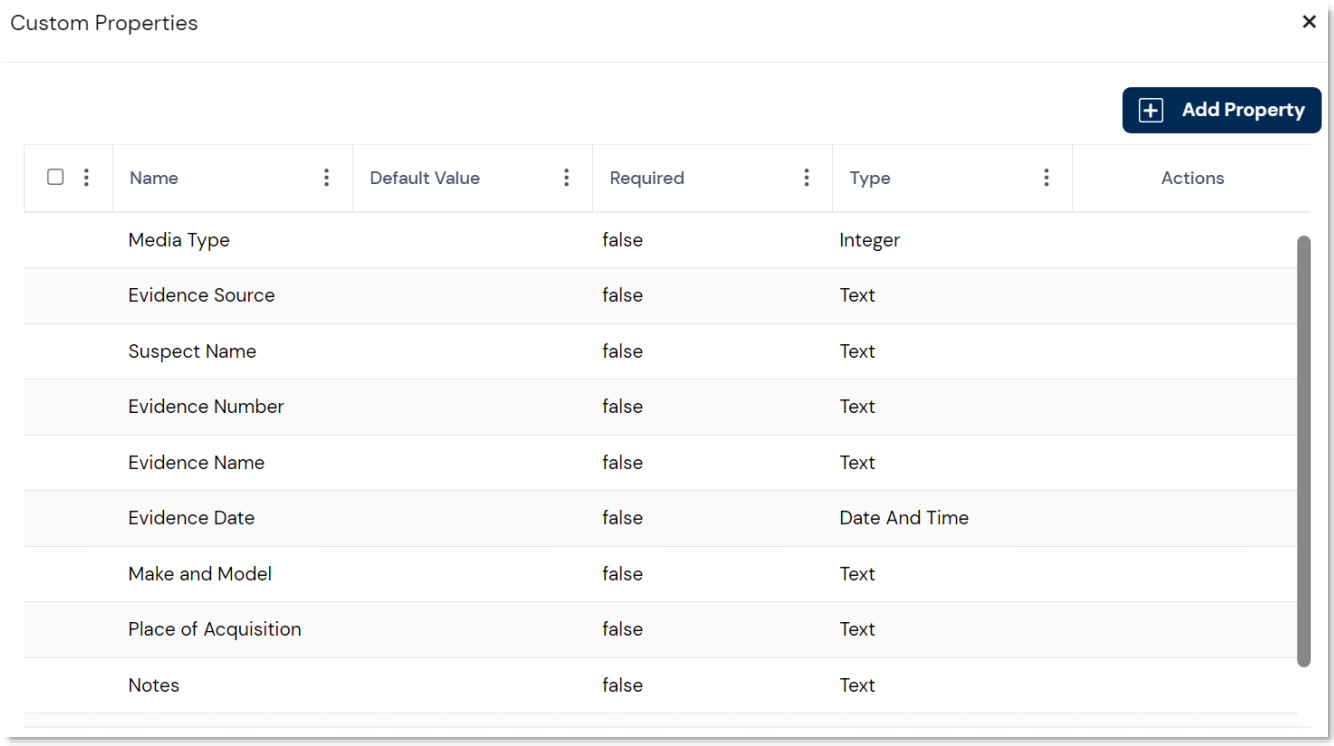
1. Upon checking the Process Evidence option, you will be navigated to a new section.
2. The bottom of the page will display the currently selected processing manager and processing profile being used.
3. If available, click the drop-down list on either to toggle these options.

Tip: By clicking on the **Customize Options** button, the currently selected processing profile can be edited efficiently.

© Exterro, Inc. All rights reserved

To Manage Custom Evidence Properties:

Evidence properties relate to the fields that appear for each evidence item being ingested. These fields can be customized for specific requirements.



1. Upon checking the Process Evidence option, you will be navigated to a new section.
2. Click **Custom Evidence Properties**.
3. Click **Add Property**.
4. Enter a **Name** and **Description**.
5. Check the **Required** box to ensure this field is filled in during ingesting of evidence. If a value is not selected for a pick list, a choice will be selected automatically.
6. Select the **Type**.
    - **Date**
    - **Pick List** – Items should be listed one per line.
    - **Text**

© Exterro, Inc. All rights reserved

To Manage Custom Evidence Properties:

1. Upon checking the Process Evidence option, and ingesting evidence; the evidence will be listed in the Evidence List.
2. Click the **Context menu** .
   - The **Evidence Options** pop-up is displayed.
3. Click **Edit Evidence**.
4. Make any necessary changes to the evidence properties.
5. Click **Update**.

To set predefined Processing Options:

Once evidence has been added to a case, you have the ability to set predefined processing options.

1. Click the drop-down list located in the **Profile Setting** pane.
2. Select a Processing Option from the available (table below).
3. Click **Process Evidence**.

Options	Description
Forensic Processing	▪ MD5 Hash ▪ SHA-1 Hash ▪ SHA-256 Hash ▪ Expand common compound files ▪ File Signature Analysis ▪ Flag Bad Extensions ▪ Search Test Index ▪ Create Thumbnails for Graphics ▪ Include Deleted Files ▪ Include File Slack

© Exterro, Inc. All rights reserved

Options	Description
	▪ Include Free Space ▪ Create Email Threads
Field Mode	▪ Include Deleted Files ▪ Include Free Space ▪ Only add items that match both File Status AND file Types criteria
Summation Processing	▪ MD5 Hash ▪ Flag Duplicate Files ▪ Expand Compound Files ▪ Flag Bad Extensions ▪ File Signature Analysis ▪ Search Text Index ▪ Create Thumbnails for Graphics ▪ Create Thumbnails for Videos ▪ Generate Common Video File ▪ Document Content Analysis ▪ Enable Advanced De-duplication Analysis ▪ Propagate email attributes ▪ Create Email Threads ▪ Cluster Analysis ▪ Include extended information in the index ▪ Don't Expand Embedded Graphics ▪ eDiscovery Refinement
eDiscovery Processing	▪ MD5 Hash ▪ Flag Duplicate Files ▪ Expand Compound Files ▪ Flag Bad Extensions

© Exterro, Inc. All rights reserved

Options	Description
	▪ File Signature Analysis ▪ Search Text Index ▪ Create Thumbnails for Graphics ▪ Document Content Analysis ▪ Enable Advanced De-duplication Analysis ▪ Propagate email attributes ▪ Create Email Threads ▪ Cluster Analysis ▪ Include extended information in the index ▪ Don't Expand Embedded Graphics ▪ eDiscovery Refinement
Basic Assessment	▪ Expand Compound Files ▪ Include Deleted Files ▪ Include File Slack ▪ Include Free Space ▪ Only add items that match both File Status AND file Types criteria
Image Processing	▪ MD5 Hash ▪ SHA-1 Hash ▪ Expand Compound Files ▪ File Signature Analysis ▪ Search Text Index ▪ Create Thumbnails for Graphics ▪ Create Thumbnails for Videos ▪ Generate Common Video File ▪ Explicit Image Detection ▪ Include Deleted Files

© Exterro, Inc. All rights reserved

Options	Description
	▪ Create Email Threads ▪ Include extended information in the index ▪ Include File Slack ▪ Include Free Space ▪ Only add items that match both File Status AND file Types criteria
Video Processing	▪ MD5 Hash ▪ SHA-1 Hash ▪ Expand Compound Files ▪ File Signature Analysis ▪ Flag Bad Extensions ▪ Search Text Index ▪ Create Thumbnails for Videos ▪ Generate Common Video File ▪ Explicit Image Detection ▪ Include Deleted Files ▪ Create Email Threads ▪ Include File Slack ▪ Include Free Space ▪ Only add items that match both File Status AND file Types criteria
All Communication	▪ MD5 Hash ▪ SHA-1 Hash ▪ Expand Compound Files – All Communication ▪ File Signature Analysis ▪ Flag Bad Extensions ▪ Search Text Index

© Exterro, Inc. All rights reserved

Options	Description
	▪ Include Deleted Files ▪ Create Email Threads ▪ Include extended information in the index ▪ Include File Slack ▪ Include Free Space ▪ Only add items that match both File Status AND file Types criteria

To select additional Processing Options & saving a new profile:

While you are able to select predefined processing profiles, you can select additional options and add them to an existing profile while saving it as a new profile.

1. Click **Customize Options**.
2. Select the additional processing options.
3. Click **Save User Profile**.
4. Enter a **Name**.
5. Enter a **Description**.
6. Click **Save**.

© Exterro, Inc. All rights reserved

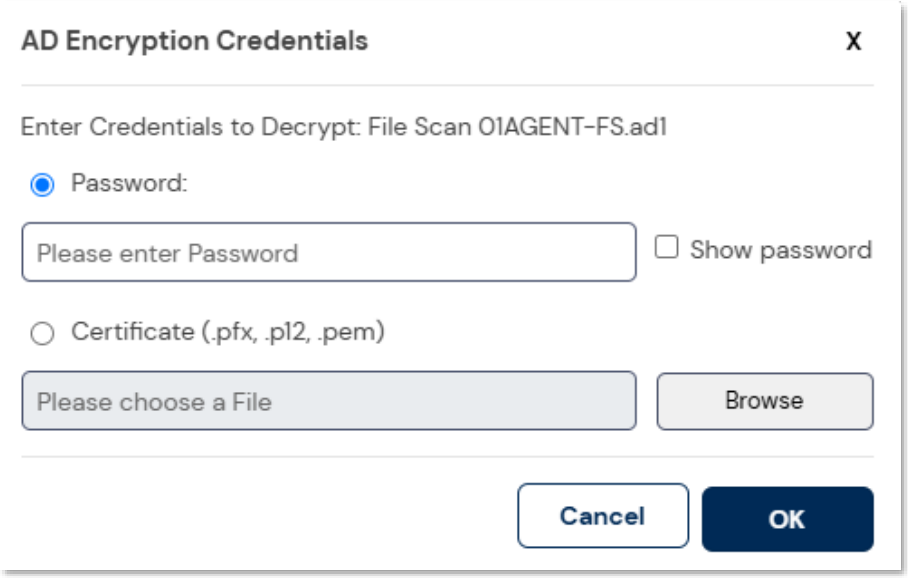
Evidence Decryption

FTK Central automatically detects the evidence encrypted using the following methods and provides you with the corresponding options to decrypt while adding it to a case:

- AD1 Encryption
- BitLocker Encryption
- Advanced Forensic Format 4 (AFF4) Encryption

AD1 Encryption

The **AD Encryption Credentials** pop-up will be displayed upon adding the evidence encrypted using AD1 encryption.

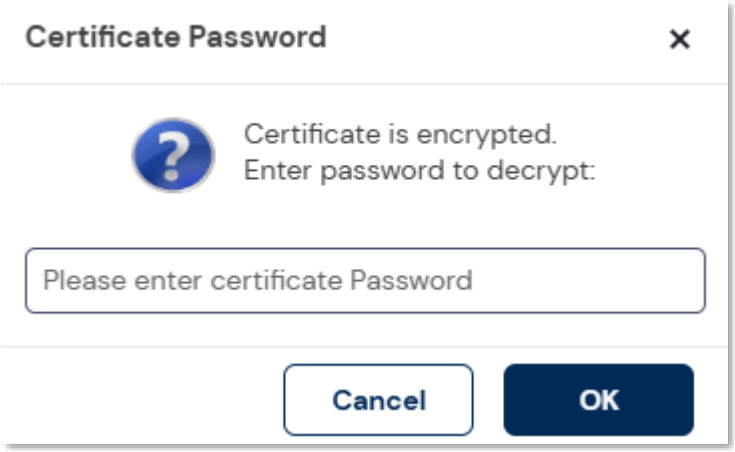


To decrypt the files:

1. From the pop-up, select any one of the following decryption methods:
   - **Password** – Decrypting the evidence using the password.
   - **Certificate** – Decrypting the evidence using the PFX, P12, or PEM certificate.

© Exterro, Inc. All rights reserved

Note: While using the **Certificate** option, the below provided pop-up will be displayed upon uploading an encrypted certificate:



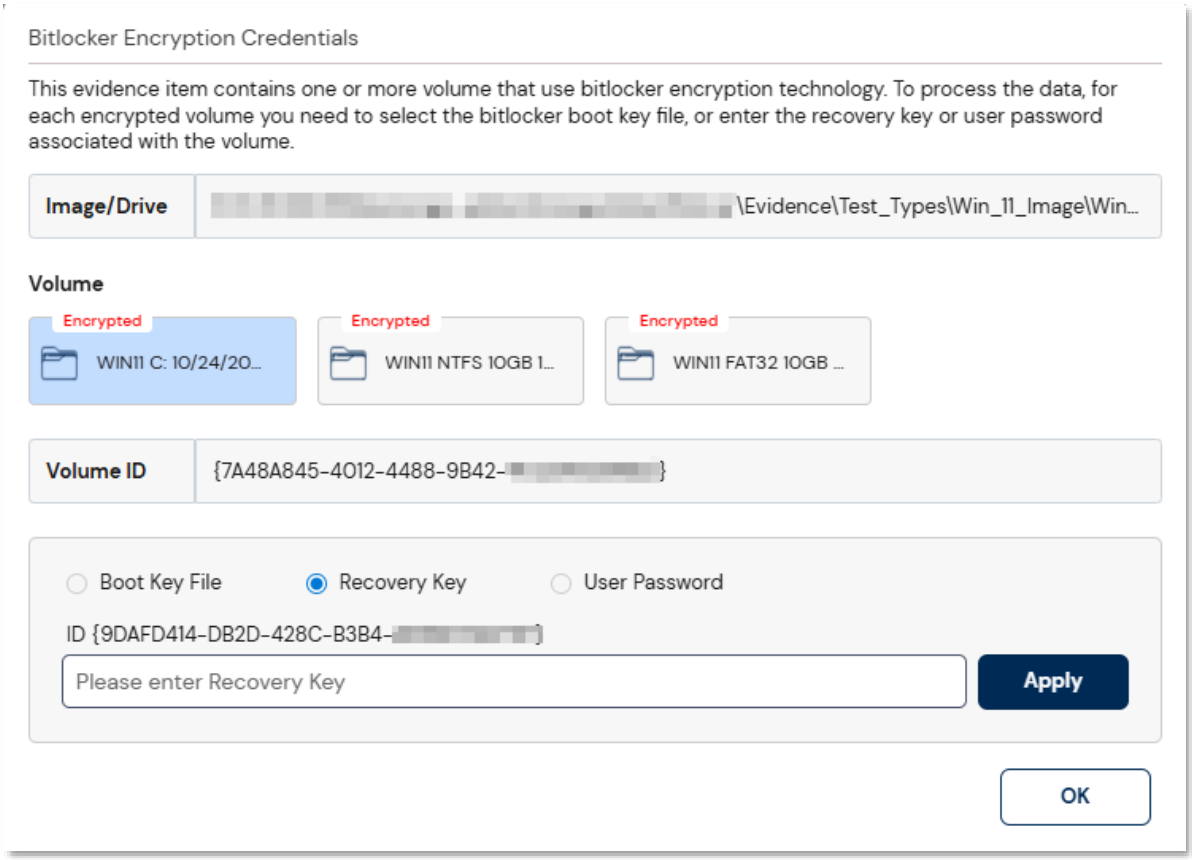
You should provide the correct password and click on **OK** to proceed.

2. Click **OK**.

© Exterro, Inc. All rights reserved

BitLocker Encryption

The **Bitlocker Encryption Credentials** pop-up will be displayed upon adding the evidence encrypted using BitLocker encryption:



To decrypt the files:

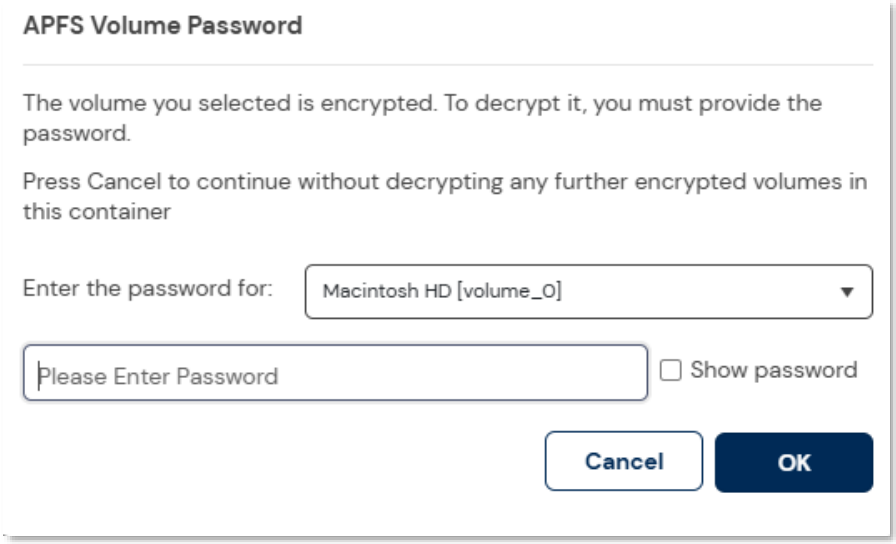
1. From the pop-up, select the required **Volume.**
2. Select any one of the following decryption options and provide the corresponding key/password.
   - Boot Key File
   - Recovery Key
   - User Password

3. Click **OK**.

© Exterro, Inc. All rights reserved

AFF4 Encryption

The **APFS Volume Password** pop-up is displayed upon adding the evidence encrypted using Advanced Forensic Format 4 (AFF4) Encryption.



To decrypt the files:

1. From the pop-up, select the volume from the drop-down which should be decrypted.
2. Provide the password of the volume to decrypt it.

© Exterro, Inc. All rights reserved

Copy from a previous case

To copy from a previous case:

1. From the home page, click **Case List**.
2. Click **Create New Case**.

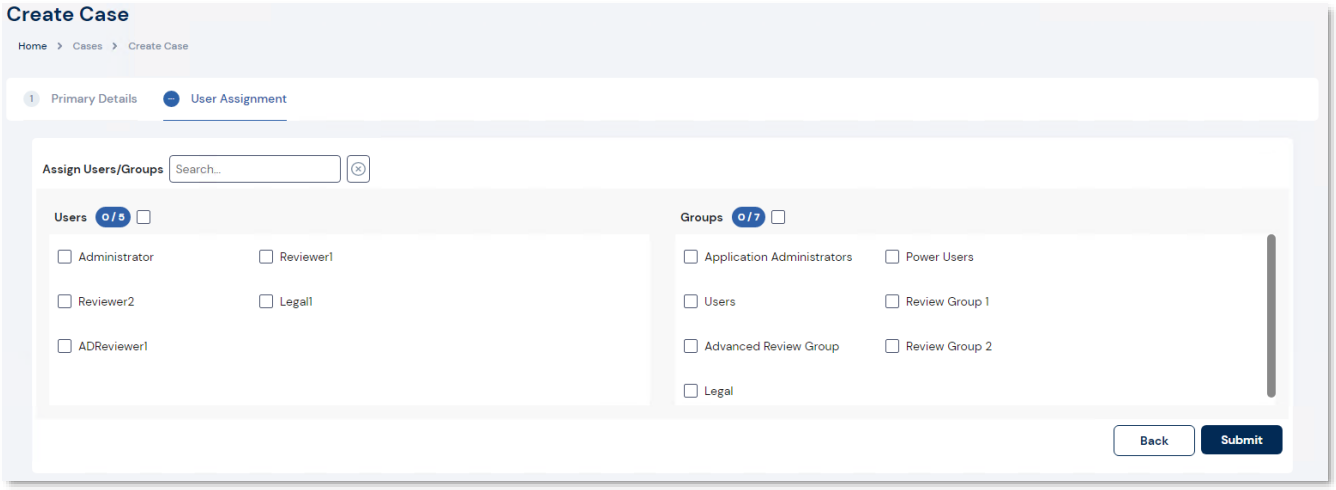
Note: There must be a case created prior to attempting this function.

3. Click the **Copy from a previous case** drop-down list and select the required case.
4. Select the required field values that needs to be copied over to the new case.
   - All
   - Custom Fields
   - Labels
   - Issues
   - Users
   - Custodians
   - Coding Panels
   - Bookmarks
   - User Groups
5. Enter a **Case Name**.
6. Configure the primary details for the **Case Description**, **Case Folder Path** and **Job Data Path**.
7. Select additional options such as **Custodians Mapping**, **Load Files** and **Process Evidences**.
8. Click **Save and Next**.
9. Add any additional **Custodians**. *(Refer to the Custodian Mapping section for more details)*
10. Click **Save and Next**.
11. Add any additional **Load Files**. *(Refer to the Load Files section for more details)*
12. Click **Next**.
13. Add **Evidence** and select a **Processing Option**. *(Refer to the Process Evidence section for more details)*
14. Click **Process Data**.

© Exterro, Inc. All rights reserved

User Assignment

During case creation, users/user groups can be assigned to a case. If a user is not assigned to a case, they will not be able to see it within the case list.



To assign users:

1. Upon checking the User Assignment option, you will be navigated to a new section.
2. Check any uses/user groups.
3. Click **Submit**.

Note: To remove users/user groups from a case, you must use the **User Management** option in the administration panel. *(Refer to the User Management section for more details)*

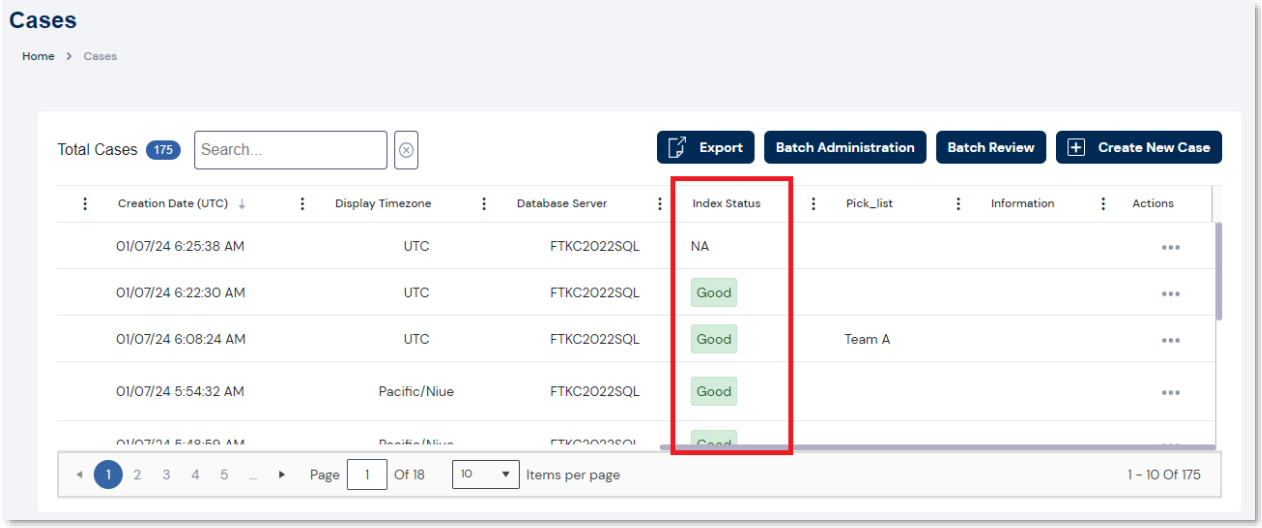
© Exterro, Inc. All rights reserved

© Exterro, Inc. All rights reserved

Case Index Status

You can view a case's index status from the **Index Status** column in the **Case List.** This column displays the following values to indicate a case's index status:

- **Unknown** – This indicates that the indexing status is not yet known for the case.
- **Good** – This indicates that the indexing has been completed for the case.
- **Bad** – This indicates that the indexing has not been completed for the case.
- **N/A** – This indicates that the indexing is not done for the case



© Exterro, Inc. All rights reserved

Processing Options

Processing in simple terms is a treatment of data provided to evidence created and stored in the database to facilitate an efficient data review.

Generally, the processing is done right away while loading the evidence in to a case or just prior to performing an analysis of the data. Typically, the data processing involves any or all of the following:

- Generating hash values for the files in the evidence.
- Categorizing the data by file types such as graphics, Office documents, encrypted files, etc.
- Extracting the contents of container and compound files, such as ZIP and TAR files.
- Creating an index of the frequently encountered words in the evidence files for quick searches and retrieval.
- Creating thumbnails for the graphics and videos in the evidence for easier identification.
- Decrypting encrypted files, if any.
- Identifying files that may need attention before reviewing. Files such as (Windows) system files, Archive files, etc.

© Exterro, Inc. All rights reserved

Elements of Processing Options

Evidence Processing	• Commonly Used Processing Options
Compound Files	• Filtering the Compound File Expansion Options List • Supported Compound File Types
Search Text Index	• Search Text Indexing Space Requirements • Configuring Case Indexing Options
Data Carving	• Supported Carving
Creating Thumbnails for Videos	• Creating Thumbnails for Videos
Creating Common Video Files	• Creating Common Video Files
Optical Character Recognition	• Running Optical Character Recognition • ABBYY FineReader Integration • Optical Character Recognition: Confidence Score
Explicit Image Detection	• Adding EID evidence to cases
Cerberus Analysis	• About Cerberus Stage 1 Threat Analysis • About Cerberus Score Weighting • About Cerberus Override Scores • Running Cerberus Analysis • Filtering Scanned Files and Viewing Threat Scores • Cerberus Stage 1 Threat Scores • Cerberus Stage 1 File Information • About Cerberus Stage 2 Static Analysis • Cerberus Stage 2 Function Call Data • File Access Call Categories • Networking Functionality Call Categories • Process Manipulation Call Categories • Security Access Call Categories • Windows Registry Call Categories

© Exterro, Inc. All rights reserved

	• Surveillance Call Categories • Uses Cryptography Call Categories • Low-level Access Call Categories • Loads a drive Call Categories • Subverts API Call Categories
Document Content Analysis	• Considerations of Cluster Topic • Running Document Content Analysis • Filtering Documents by Document Content Analysis
Language Identification	• Performing Language Identification • Viewing Language Identified Documents • Basic Languages • Extended Languages
Entity Extraction	• Entity Extraction
Lab/E-discovery Options	• Lab/E-discovery Options
Evidence Refinement	• Evidence Refinement
Index Refinement	• Index Refinement
AI Jobs	• AI Jobs
Processing Profiles	• Processing Profiles

© Exterro, Inc. All rights reserved

Evidence Processing

When a case is created, you can define the default processing options that are to be used whenever evidence is added to that case. By specifying default processing options for a case, you do not have to manually configure the processing options each time you add new evidence. The case-level defaults can be overridden and customized when you add new evidence or when you perform an additional analysis.

Commonly Used Processing Options

Processing Option	Description
MD5 Hash	Creates a digital fingerprint using the Message Digest 5 algorithm, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.
SHA-1 Hash	Creates a digital fingerprint using the Secure Hash Algorithm-1, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.
SHA-256 Hash	Creates a digital fingerprint using the Secure Hash Algorithm-256, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. SHA-256 is a hash function computed with 32-bit words, giving it a longer digest than SHA-1.
Max Hash File Size (MB)	The maximum size limit (in MB) for the hash files to be created. The default is 512 MB.
Flag Duplicate Files	Identifies files that are found more than once in the evidence. This is done by comparing file hashes.
KFF	Enables the Known File Filter (KFF) that lets you identify either known insignificant files that you can ignore or known illicit or dangerous files that you want to be alerted to. See Known File Filter section.

© Exterro, Inc. All rights reserved

Processing Option	Description
Expand Compound Files	Automatically extracts and processes the contents of compound files such as ZIP, email, and OLE files.
Expand Compound Image Files	For any given evidence image file, expand any other evidence image files it contains and add their contents to the evidence.
Enhanced File Identification	Enables additional processing to determine the contents of multimedia files. ***Note:*** *You are advised to perform this processing since some multimedia files may be misidentified without this processing.*
File Signature Analysis	File Signature Analysis is an optional processing option. This lets you initially see the contents of compound files without necessarily having to process them. Processing can be done later, if it is deemed necessary or beneficial to the case by selecting File Signature Analysis.
Flag Bad Extensions	Identifies files whose types do not match their extensions, based on the file header information. Enabling this automatically forces File Signature Analysis to be selected.
Entropy Test	Performs an entropy test. This is useful when used in conjunction with indexing to not index binary data, etc.
Include Deleted Files	Scan enumerated objects (e.g. file systems, ZIP, email archives) for deleted items. ***Note:*** *If this is not selected it cannot be done later.*
Search Text Index	Stores the words from evidence in an index for quick retrieval. Using this processing option adds up to the memory consumption, approximately 25% of the memory required for the total evidence in the case.

© Exterro, Inc. All rights reserved

Processing Option	Description
	When FTK Central creates a full text index of evidence or places all text characters in an index file with a case, it does not capture spaces or the following symbols:

.	,	:	;	#	"
'	~	!	*	+	=
$	%	^	&		

Create Thumbnails for Graphics	Creates thumbnails for all graphics in the case. The thumbnails are always created in JPG format, regardless of the original graphic file type.
Create Thumbnails for Videos	Creates thumbnails for all videos in the case. The thumbnails are always created in JPG format, regardless of the original video file type. ***Note:*** *You can set the frequency for picking a thumbnail from the video. You can do it by either providing the percent (1 thumbnail per n% of the video) or the time interval (1 thumbnail per n seconds of the video).*
Generate Common Video File	When you process the evidence in your case, you can choose to create a common video type for all the videos in your case. These common video types are not the actual video files from the evidence, but a copied conversion of the media that is generated and saved as an MP4 file that can be previewed on the video tab.
EXIF for Videos	Parses XMP metadata (similar to EXIF data) from processed MP4 and most of the other modern video file formats. When parsed from a video file, the metadata values are displayed on the Properties tab of the file viewer pane.

© Exterro, Inc. All rights reserved

Processing Option	Description
HTML File Listing	Creates a HTML version of the File Listing in the case folder.
CSV File Listing	Creates a File Listing Database in CSV format instead of an MDB file.
Data Carve	Carves data immediately after pre-processing. This uses file signatures to identify deleted files contained in the evidence.
Meta Carve	Carves deleted directory entries and other metadata. The deleted directory entries often lead to data and file fragments that can prove useful to the case, that could not be found otherwise.
Optical Character Recognition (OCR)	Scans graphic files for text and converts graphics-text into actual text. That text can then be indexed, searched and treated as any other text in the case.
Explicit Image Detection	Generates explicit image scores (range 0-100) for graphic files.
Cerberus Analysis	Calculates the Cerberus Stage 1 Score for the evidence. See Cerberus Analysis section.
Process Internet Browser History for Visualization	Processes internet browser history files so that you can see them in the detailed visualization timeline.
Language Identification	Analyses the first two pages of every document to identify the languages contained within.
Document Content Analysis	Analyzes the content and groups it according to topic in the Overview tab.
Entity Extraction	Identifies and extracts specific types of data in your evidence. See Entity Extraction section.
Enable File Encryption Detection	Identifies files which may be encrypted.
Perform Automatic Decryption	Attempts to decrypt files using a list of passwords that you provide.

© Exterro, Inc. All rights reserved

Processing Option	Description
Populate Family for FTK Central	Makes the SMS and MMS messages (and their associated family objects / attachments) available for review in FTK Central.

© Exterro, Inc. All rights reserved

Compound Files

You can expand individual compound file types. This lets you see child files that are contained within a container such as ZIP files. You can access this feature during case creation and additional analysis.

Be aware of the following before you expand compound files:

- If you have labeled or hashed a family of files, then later choose to expand a compound file type that is contained within that label or family, the newly expanded files do not inherit the labeling from the parent, and the family hashes are not automatically regenerated.
- Compound file types such as AOL, Blackberry IPD Backup, EMFSpool, EXIF, MSG, PST, RAR, and ZIP can be selected individually for expansion.
- Only the file types selected are expanded. For example, if you select ZIP, and a RAR file is found within the ZIP file, the RAR is not expanded.

Note: If you expand data, you will have files that are generated when the data was processed and were not part of the original data.

Filtering the Compound File Expansion Options List

It is possible to filter the Compound File Expansion Options list by category. Use the Categories dropdown at the top of the list to select a category. Use the **Select All** and **Deselect All** buttons to select or clear all options within the selected category.

© Exterro, Inc. All rights reserved

Supported Compound File Types

- 7-Zip
- Active Directory
- AFF4
- Android Backup
- AOL Files
- BZIP2
- Cellebrite UFDR
- Chrome Bookmarks
- Chrome Cache
- Chrome Json
- Chrome LevelDB
- Chrome SNSS
- Chrome SQLite
- DBX
- Edge Bookmarks
- Edge Cache
- Exterro Mobile Parsers
- Edge SQLite
- EMFSPOOL
- ESE DB
- EVT
- EVTX
- FireFox Cache
- FireFox JSON
- FireFox SQLite
- GZIP
- IE Cookie Text (IE 10 and newer)
- IE Recovery (IE 10 and newer)
- IE WebCache (IE 10 and newer)
- IIS Log
- iMessage SQLite
- Internet Explorer Files (IE 9)
- iOS Backup
- Log2t CSV
- Lotus Notes (NSF)
- Mail.ru Chat
- MBOX
- McAFee Log
- Microsoft Exchange
- MS Office, OLE and OPC documents
- MSG
- OneNote
- OpenSSH known_hosts File
- Outlook for Mac OLM
- PDF
- Pidgin Chat Log
- PKCS7 and S/MIME Files
- PST
- RAR
- Registry (full)
- Registry (timeline)
- RFC822 Internet Email
- Safari Plist
- Safari SQLite
- Skype SQLite
- SQLite Databases
- TAR
- Unistore Database (Windows 10 Mail)
- Windows Firewall Log
- Windows Registry.pol
- Windows Thumbnails
- XRY (Extended XML only)
- XWAY
- ZIP
- $Log file

© Exterro, Inc. All rights reserved

Compound File Expansion Options Category List

Category	Description
All	This is the full list of supported Compound File Expansion Options.
All Communication	This option includes all supported file types that are used for communication.
All Mobile	This option includes all supported file types found on any mobile device.
Archives	This option includes all supported archive file types.
Browsers	This option includes all supported file types used within a browser.
Email	This option includes all supported email file types.
Logs	This option includes all supported log file types.
Other Forensic Tools	This option includes all support third-party forensic tool image types.
Windows	This option includes all supported file types used within a Windows system.

© Exterro, Inc. All rights reserved

Search Text Index

All evidence should be indexed to aid in searches. Index evidence when it is added to the case by checking the **Search Text Index** option in the process evidence dialog, or index after the fact by clicking and specifying indexing options.

Scheduling is another factor in determining which process to select. Time restraints may not allow for all tasks to be performed initially. For example, if you disable indexing, it shortens the time needed to process a case. You can return at a later time and index the case if needed.

Warning: While performing this processing option, users must note that the File Slack and Free Space is not indexed by default. These areas can be indexed by selecting the **Index Refinement options**.

Search Text Indexing Space Requirements

To estimate the space required for a Search Text Index, plan on approximately 25% of the space needed for each case's evidence.

© Exterro, Inc. All rights reserved

Configuring Case Indexing Options

Case Indexing gives you almost complete control over what goes into your case index. These options can be applied globally during case creation.

Option	Description
Letters	Specifies the letters and numbers to index. Specifies Original, Lowercase, Uppercase, and Unaccented. Choose **Add** or **Remove** to customize the list. You may need to add characters to this list for specific index searches to functionproperly. For example, you may want to do an index search for 'Password#123'. By default, the # symbol is treated as a space and is not indexed. To have the # symbol included in the index, you would need to do two things: • Remove the # from the Spaces list. • Add # to the Letters list.
Noise Words	A list of words to be considered "noise" and ignored during indexing. Choose **Add** or **Remove** to customize the list.
Hyphens	Specifies which characters are to be treated as hyphens. You can add standardkeyboard characters, or control characters. You can remove items as well.
Hyphen Treatment	Specifies how hyphens are to be treated in the index. Options are: • Ignore Hyphens will be treated as if they never existed. For example, the term "coun-ter-culture" would be indexed as "counterculture." • Hyphen Hyphens will be treated literally. For example, the term "counter-culture"would be indexed as "counter-culture."

© Exterro, Inc. All rights reserved

Option	Description
	• Space Hyphens will be replaced by a non-breaking space. For example, the term "counter-culture" would be indexed as two separate entries in the index being"counter" and "culture." • All Terms with hyphens will be indexed using all three hyphen treatments. For example, the term "counter-culture" will be indexed as "counterculture", "coun-ter-culture", and as two separate entries in the index being "counter" and "cul-ture."
Spaces	Specifies which special characters should be treated as spaces. Remove characters from this list to have them indexed as any other text. Choose **Add** or **Remove** to customize the list. You may need to remove characters from this list for specific index searches to function properly. For example, you may want to do an index search for 'Password'123'. By default, the # symbol is treated as a space and is notindexed. To have the # symbol included in the index, you would need to do two things: • Remove the # from the *Spaces* list. • Add the # to the *Letters* list. ***Note:*** *If special characters (e.g. @, ., etc. used in emails or other strings) are configured as spaces within the indexing options, users must search for single words beginning/ending with an asterisk *. dtSearch will not allow partial words to be searched for without a wildcard asterisk.*
Ignore	Specifies which control characters or other characters to ignore. Choose **Add** or **Remove** to customize the list.

© Exterro, Inc. All rights reserved

Option	Description
Max Word Length	Allows you to set a maximum word length to be indexed.
Index Binary Files	Specify how binary files will be indexed. Options are: • Index all • Skip • Index all (Unicode)
Enable Date Recognition	Choose to enable or disable this option.
Presumed Date Format for Ambiguous Dates	If date recognition is enabled, specify how ambiguous dates should be formattedwhen encountered during indexing. Options are: • MM/DD/YY • DD/MM/YY • YY/MM/DD
Set Max Memory	Allows you to set a maximum size for the index.
Auto-Commit Interval(MB)	Allows you to specify an Auto-Commit Interval while indexing the case. When theindex reaches the specified size, the indexed data is saved to the index. The sizeresets, and indexing continues until it reaches the maximum size, and saves again, and so forth.
Cache Filtered Text in Index	Filtered Text is being cached in the dtSearch index by default, however it can be toggled on or off. The advantage to caching filtered text is that it produces more reliable search hit highlighting and it reduces the time to return index search results. However, NOT caching filtered text will result in a smaller index and shorter time to complete the indexing process.
Modify for TR1 Expressions	Configures the indexing engine to index TR1 regular expressions. *On selecting this option, a set of special characters (example: /, @ , :) will be automatically added under 'Letters' section and these characters will be included*

© Exterro, Inc. All rights reserved

Option	Description
	in the search index and search results will be generated including these characters. The special characters added should be removed from spaces box.
Create Optional Accent Sensitive Index	Generates the index in such a way that, when the "Accents are Significant" option is enabled for index searching, the investigator can optionally control whether characters with accent marks are distinguished from those without. *For example: "abc" versus "äbc".* FTK has always and still does default to an Accent Sensitive Index. This means that, *"abc" will only find "abc"* *"äbc" will only find "äbc"*

© Exterro, Inc. All rights reserved

Data Carving

Data carving is the process of looking for data on media that was deleted or lost from the file system. Often this is done by identifying file headers and/or footers, and then "carving out" the blocks between these two boundaries.

Exterro provides several specific pre-defined carvers that you can select when adding evidence to a case. Data carving can be selected in the Case Creation dialog or from Additional Analysis.

Supported Carving Options

- AOL bag Files
- EMF Files
- FUJI Raw Files
- JPEG Files
- MP4 Files
- OLE Files (MS Office)
- PSD Files
- WMV Audio Video Files
- Blu-ray MPEG-2 Files
- EML Files
- GIF Files
- LNK Files
- MPG Files
- PDF Files
- TIFF Files
- ZIP Files
- BMP Files
- Flash Video Files
- HTML Files
- MKV Files
- Ogg video
- PNG Files
- WEBM Files

© Exterro, Inc. All rights reserved

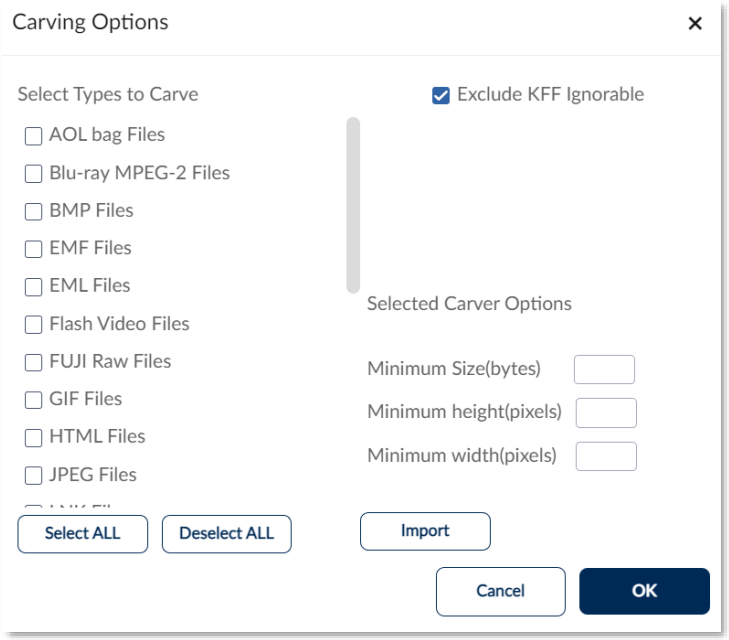
Importing Data Carvers

To import data carvers:

1. From the Process Evidence page of case creation, click **Customize Options**.

Note: Alternatively, during review, select the desired items, right-click **> Additional Analysis > Customize Options**.

2. Select **Data Carve**.
3. Click the **Context menu** to open the configuration.
   - The **Carving Options** pop-up is displayed.



4. Click **Import**.
5. Select any carvers requiring import within the windows explorer. They must be .XML.
6. Click **Open**.
7. The carver(s) selected will be imported and available for use globally.

Note: Users can delete any carvers imported by clicking on the **delete** button.

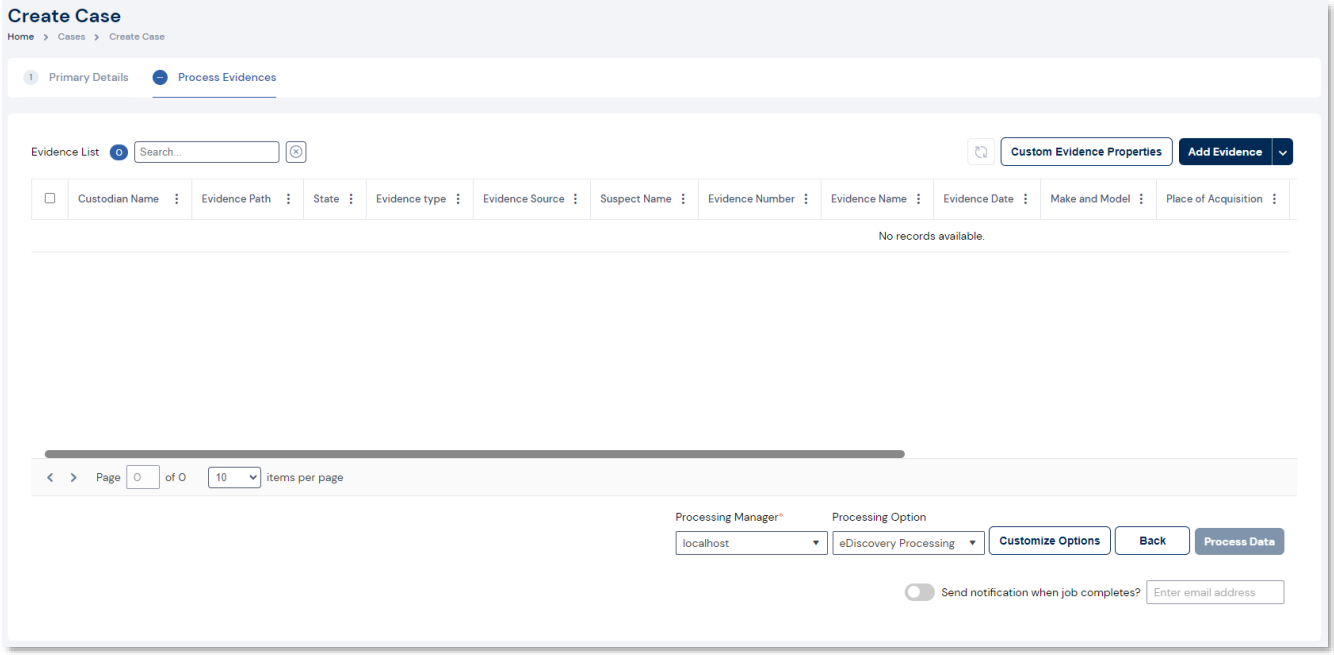
© Exterro, Inc. All rights reserved

Creating Thumbnails for Videos

You can generate thumbnail graphics based on the content that exists within video files in your case. Video thumbnail generation is accomplished during processing. You can either set up video thumbnail generation during Case Creation, or you can run the processing against an existing case by using Additional Analysis.

To generate thumbnails for videos:

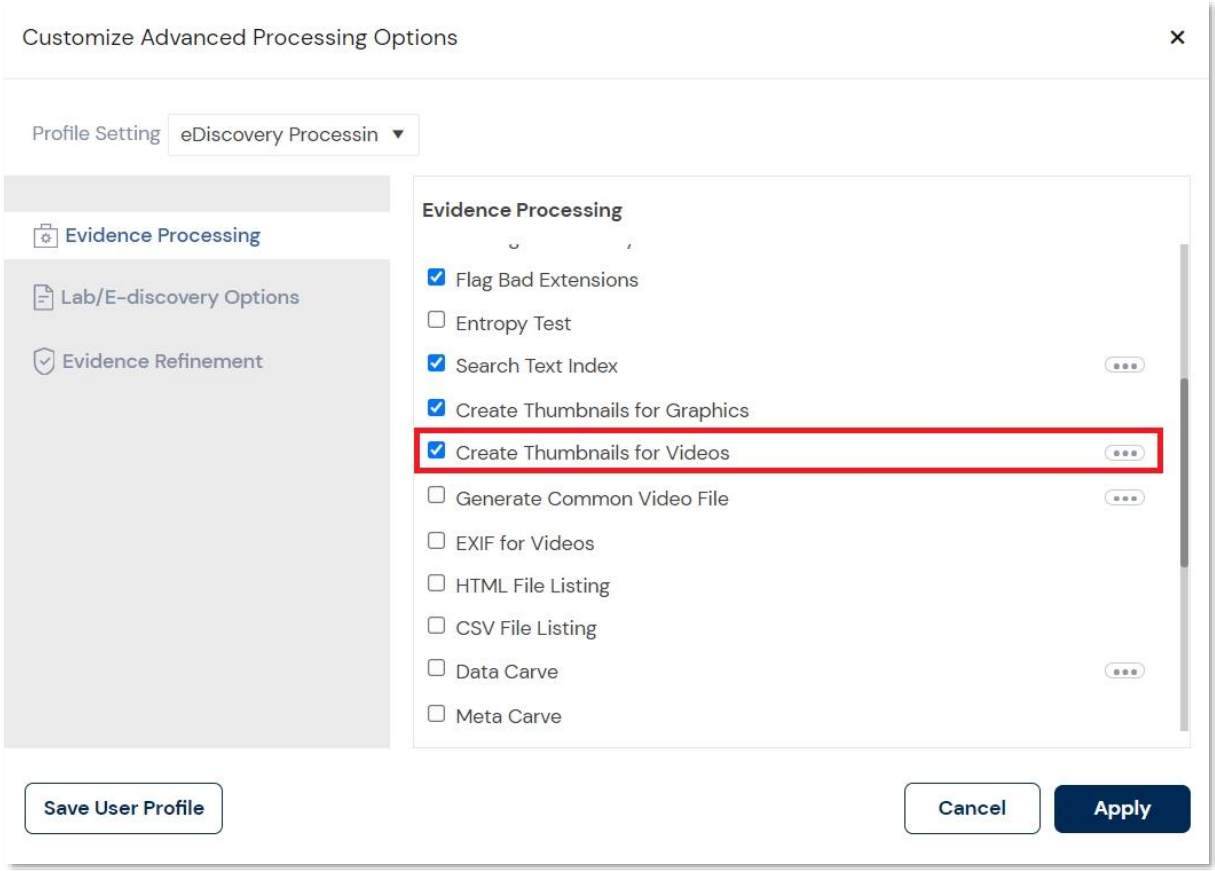
1. From the Process Evidence page of case creation, click **Customize Options**.



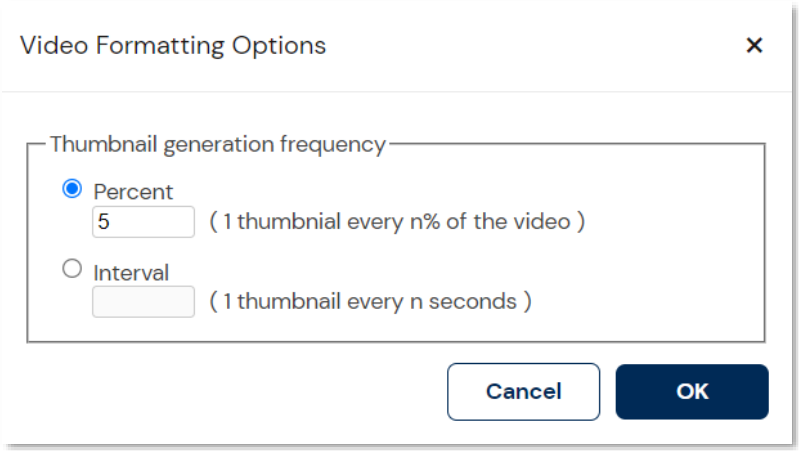
Note: Alternatively, during review, select the desired items, right-click **> Additional Analysis > Customize Options**.

© Exterro, Inc. All rights reserved

2. Select **Create Thumbnails for Videos**.



3. Click the **Context menu** ••• to open the configuration.
    - The **Video Formatting Options** pop-up is displayed.



© Exterro, Inc. All rights reserved

4. Set the following values:
   - **Percent** – This option generates thumbnails against videos based on the percentage of a videos total content. For example, if you set this value to 5, then at every 5% of the video a thumbnail is generated.
   - **Interval** – This option generates thumbnails against videos based on seconds. For example, if you set this value to 5, then at every 5 seconds within a video, a thumbnail is generated.
5. Click **Apply**.
6. Click **Process Data** or **Run Analysis**.

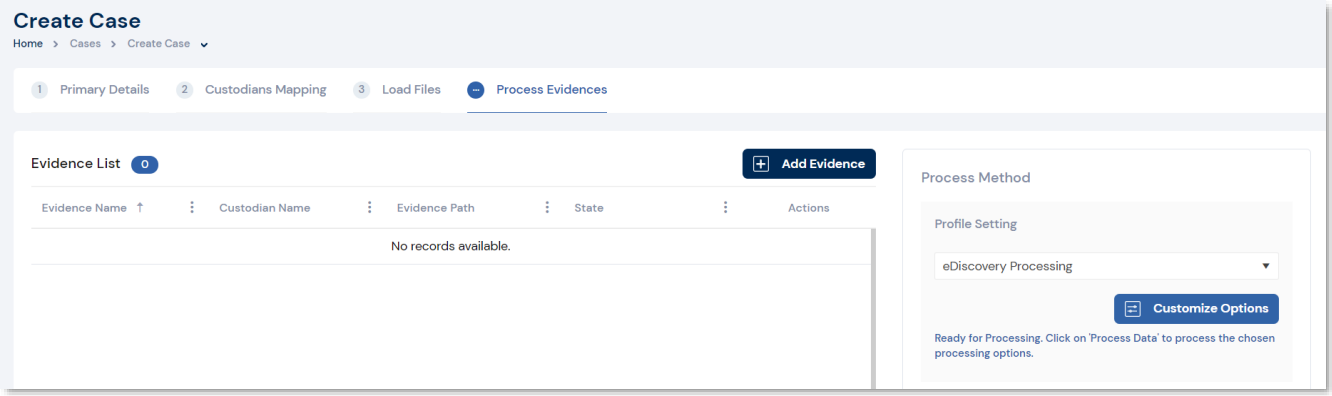
© Exterro, Inc. All rights reserved

Creating Common Video Files

When you process the evidence during Case Creation or during Additional Analysis, you can choose to create a common video type for videos in your case. These common video types are not the actual video files from the evidence, but a copied conversion of the media that is generated and saved as an MP4 file that can be previewed in the viewer.

To create a common video file:

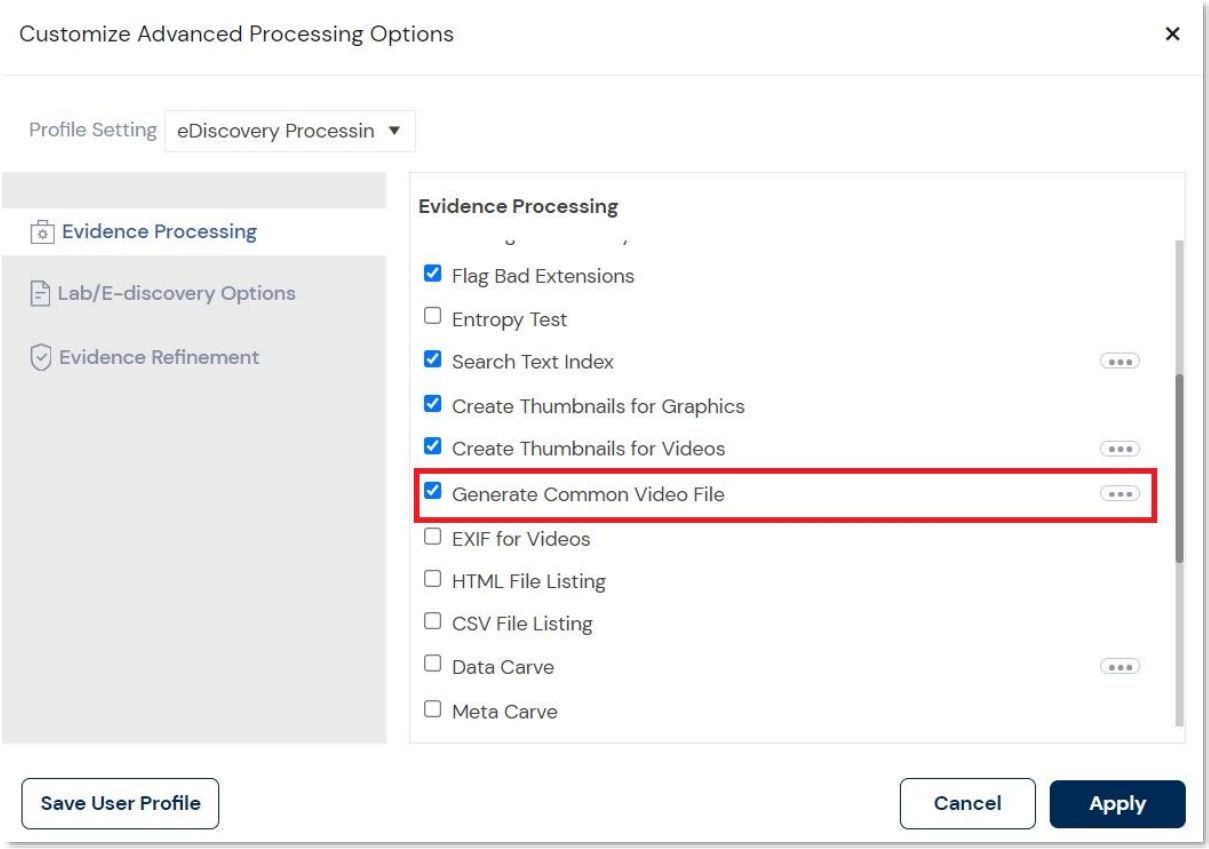
1. From the Process Evidence page of case creation, click **Customize Options**.



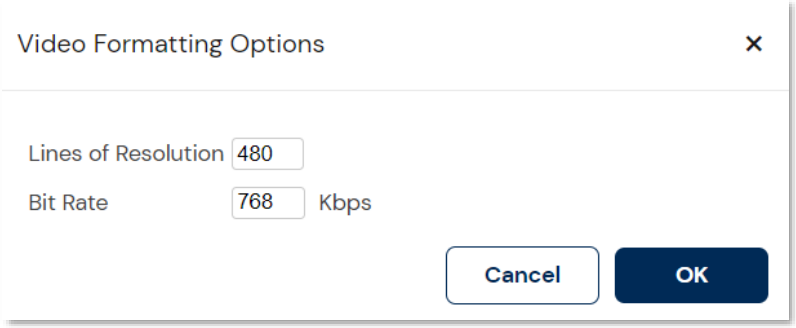
Note: Alternatively, during review, select the desired items, right-click > **Additional Analysis** > **Customize Options**.

© Exterro, Inc. All rights reserved

2. Select **Create Common Video Files**.



3. Click the **Context menu** ••• to open the configuration.
   - The **Video Formatting Options** pop-up is displayed.



© Exterro, Inc. All rights reserved

4. Set the following values:
   - **Lines of Resolution** – Sets the number of vertical lines in the video. The higher it is, the better the resolution.
   - **Bit Rate** – Sets the rate of bits in Kbps measurements. The higher it is, the better the resolution.

5. Click **Apply**.
6. Click **Process Data** or **Run Analysis**.

© Exterro, Inc. All rights reserved

Optical Character Recognition

The Optical Character Recognition (OCR) process lets you extract text that is contained in graphics files. The text is then indexed so that it can be, searched, and bookmarked.

Running OCR against a file type creates a new child file item. The graphic files are processed normally, and another file with the parsed text from the graphic is created. The new OCR file is named the same as the parent graphic, [graphicname.ext], but with the extension OCR, for example, graphicname.ext.ocr.

You can view the graphic files in the Viewer when it is selected in the Grid View. The Native tab shows the graphic in its original form. The Text tab shows the OCR text that was added to the index.

The LeadTools OCR engine can be selected in the Case Processing and Additional Analysis areas LeadTools of the application interface. The ABBYY FineReader OCR engine integration is available as a separate add-on tool (with separate license from ABBYY).

Before running OCR, be aware of the following:

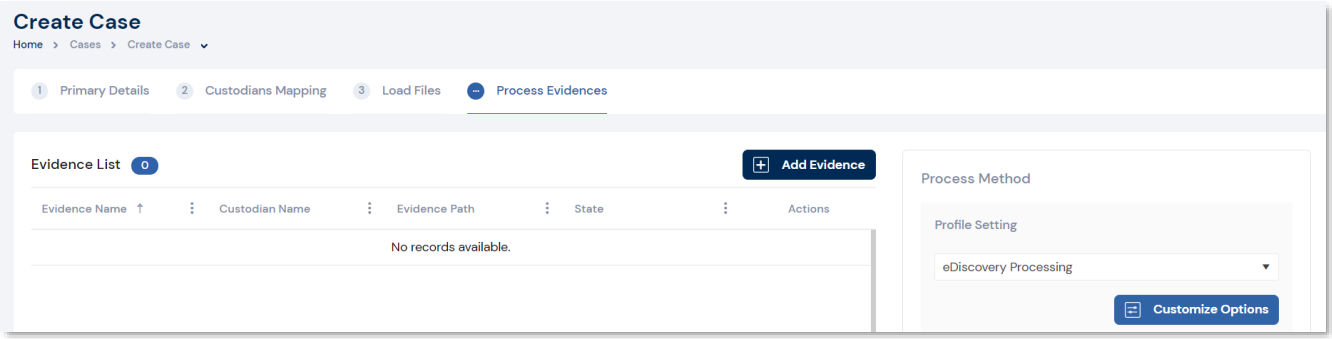
- OCR is only a helpful tool for the investigator to locate images from index searches. OCR results should not be considered evidence without further review.
- OCR can have inconsistent results. OCR engines by nature have error rates. This means that it is possible to have results that differ between processing jobs on the same machine with the same piece of evidence.
- Some large images can cause OCR to take a very long time to complete. Under some circumstances, they may not generate any output.
- Graphical images that have no text or pictures with unaligned text can generate bad output.
- OCR is best on typewritten text that is cleanly scanned or similarly generated. All other picture files can generate unreliable output that can vary from run to run.

© Exterro, Inc. All rights reserved

Running Optical Character Recognition

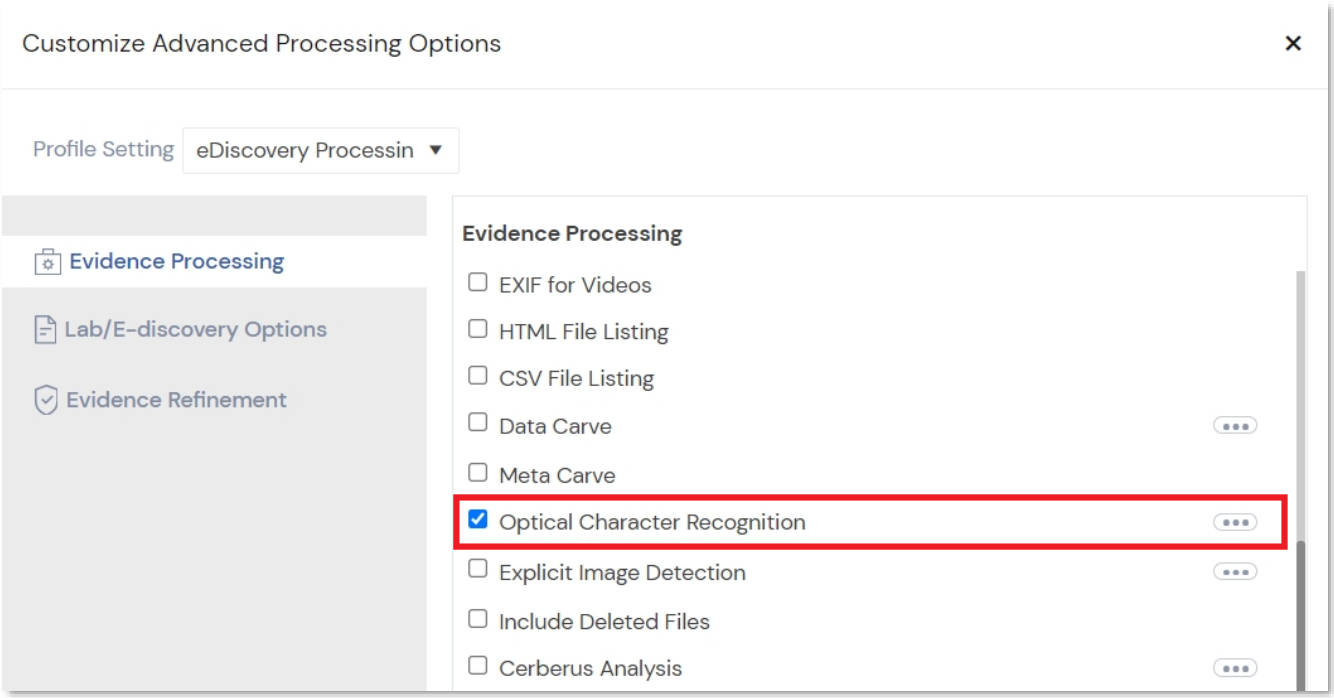
To run OCR:

1. From the Process Evidence page of case creation, click **Customize Options**.



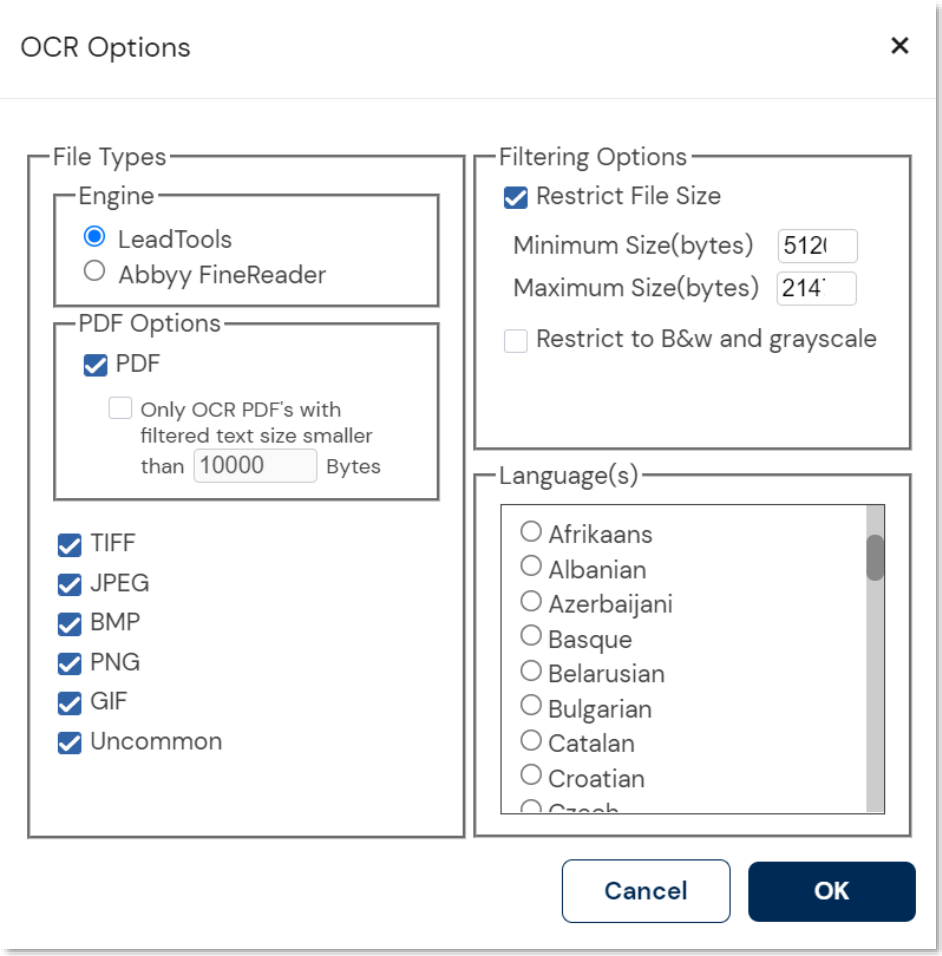
Note: Alternatively, during review, select the desired items, right-click > **Additional Analysis** > **Customize Options**.

2. Select **Optical Character Recognition**.



© Exterro, Inc. All rights reserved

3. Click the **Context menu** ••• to open the configuration.
    - The **OCR Options** pop-up is displayed.



© Exterro, Inc. All rights reserved

4. Configure the following:

Options	Description
File Types	Specify which file types to include in the OCR process during case processing. For PDF files, you can also control the maximum filtered text size for which to run OCR against.
Filtering Options	Specify a range in file size to include in the OCR process. You can also specify whether or not to only run OCR against black and white, and grayscale. The Restrict File Size option is selected by default. By default, OCR file generation is restricted to files larger than 5K. If you do not want to limit the size of OCR files, you must disable this option.
Language	Specify the output language for the OCR text.
Engine	Specify the processing engine to use for the OCR process.

5. Click **OK**.
6. Click **Apply**.
7. Click **Process Data** or **Run Analysis**.

© Exterro, Inc. All rights reserved

ABBYY FineReader Integration

FTK can leverage the Exterro API to access the ABBYY FineReader OCR engine integration which provides a robust alternative OCR engine for indexing graphic image files. In addition to an Exterro FTK Central installation, the ABBYY product integration requires an add-on component installation and a license sold separately from ABBYY (not included with Exterro licensing – Please contact sales@exterro.com). The option to select an ABBYY OCR engine in the processing options interface will be grayed out until properly installed and configured.

Note: To use ABBYY, you must have followed the KB article ABBYY/Zeta OCR: Installation.

© Exterro, Inc. All rights reserved

Optical Character Recognition: Confidence Score

There is an option to show the confidence score for each file that has been processed with OCR. It is recommended to use this feature to sort documents processed using OCR to determine which files may need to be manually reviewed for the desired keywords.

The OCR Confidence Score value may be one of the following:

Options	Description
1-100%	The OCR confidence % score for a document that had a successful OCRprocess; the higher the score, the higher the confidence.
No Score Available (2)	The OCR results are from a previous version.
Minimal Confidence (1)	The OCR extraction is not in a supported language or is not clear.
No Text Found (0)	The OCR process did not identify any text to extract.
OCR Skipped (-1)	The OCR process was skipped due to some condition.
OCR Extraction Error (-2)	The OCR process failed for that file.
Blank	The file does not need the OCR process; for example, a .DOC file or email.

To use the OCR Confidence Score:

1. Process your data using the Optical Character Recognition option.
2. Add a custom column named **OcrScore**.

   Refer to the Custom Columns section for more information.

© Exterro, Inc. All rights reserved

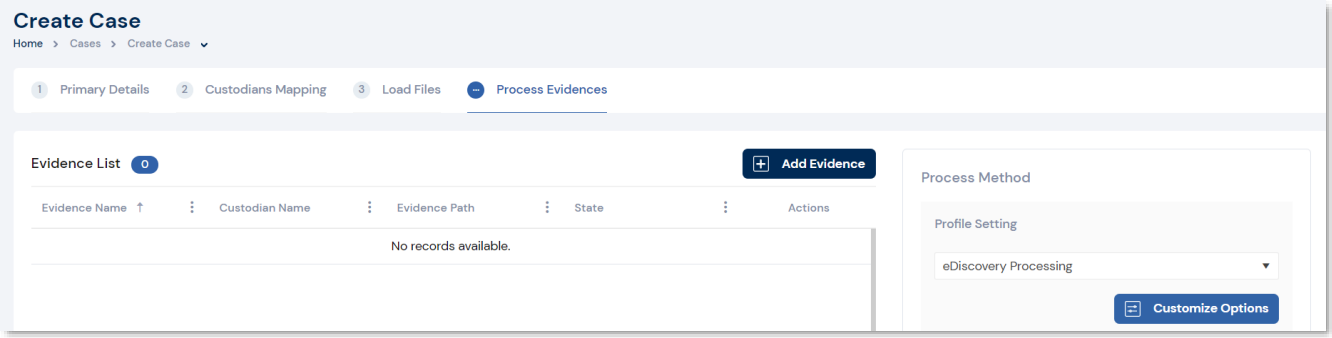
Explicit Image Detection

EID reads all graphics in a case and assigns both the files and the folders they are contained within a score according to what it interprets as being possibly illicit content.

Adding EID evidence to cases

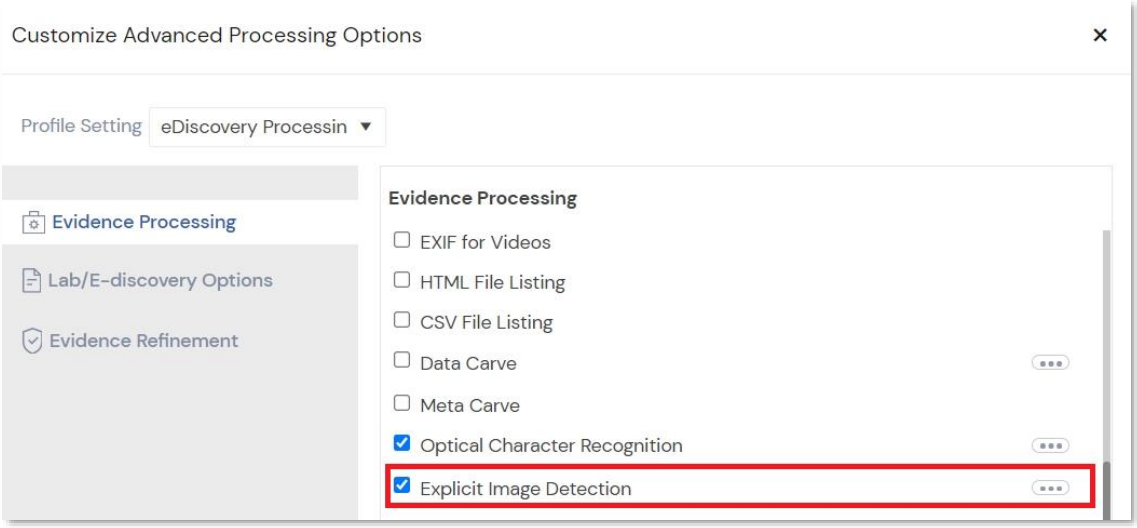
To add EID evidence to a case:

1. From the Process Evidence page of case creation, click **Customize Options**.



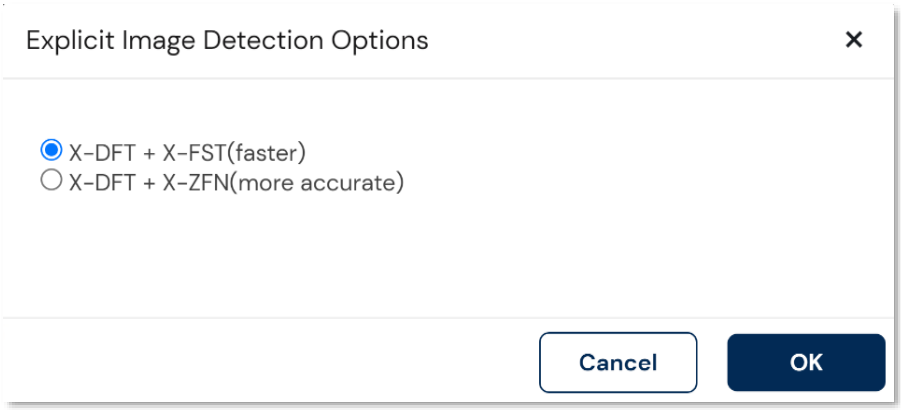
Note: Alternatively, during review, select the desired items, right-click > **Additional Analysis** > **Customize Options**.

2. Select **Explicit Image Detection**.



© Exterro, Inc. All rights reserved

3. Click the **Context menu** ••• to open the configuration.
    - The **Explicit Image Detection Options** pop-up is displayed.



4. Select one based on the required option. The components of the option are provided below:

Profile Name	Level	Description
X-DFT	Default (XS1)	This is the most generally accurate. It is always selected.
X-FST	Fast (XTB)	This is the fastest. It scores a folder by the number of files it contains that meet the criteria for a high likelihood of explicit material. It is built on a different technology than X-DFT and does not use "regular" DNAs. It is designed for very high volumes, or real-time page scoring. Its purpose is to quickly reduce, or filter, the volume of data to a meaningful set.
X-ZFN	Less False Negatives (XT2)	This is a profile similar to X-FST but with more features and with fewer false negatives than X-DFT. You can apply this filter after initial processing to all evidence, or to only the folders that score highly using the X-FST option. Check-mark or highlight those folders to isolate them for Additional Analysis. In Additional Analysis, File Signature Analysis must be selected for EID options to work correctly.

© Exterro, Inc. All rights reserved

5. Click **OK**.
6. Click **Apply**.
7. Click **Process Data** or **Run Analysis**.

Tip: Exterro recommends that you run Fast (X-FST) for folder scoring, and then follow with Less False Negatives (X-ZFN) on high-scoring folders to achieve the fastest, most accurate results.

After you select EID in Evidence Processing or Additional Analysis, and the processing is complete, you must select or modify a filter to include the EID related columns in the Grid View.

© Exterro, Inc. All rights reserved

Cerberus Analysis

Cerberus lets you do a malware analysis on executable binaries. You can use Cerberus to analyze executable binaries that are on a disk, on a network share, or that are unpacked in system memory.

Cerberus consists of the following stages of analysis.

- Stage 1: Threat Analysis

  Cerberus stage 1 is a general file and metadata analysis that quickly examines an executable binary file for common attributes it may possess. It identifies potentially malicious code and generates and assigns a threat score to the executable binary.
- Stage 2: Static Analysis

  Cerberus stage 2 is a disassembly analysis that takes more time to examine the details of the code within the file. It learns the capabilities of the binary without running the actual executable.

Cerberus first runs the Stage 1 threat analysis. After it completes Stage 1 analysis, it will then automatically run a static analysis against binaries that have a threat score that is higher than the designated threshold. Cerberus analysis may slow down the speed of your overall processing.

Warning: Cerberus writes binaries to the AD Temp folder momentarily in order to perform the malware analysis. Upon completion it will quickly delete the binary. It is important to ensure that your antivirus is not scanning the AD Temp folder. If antivirus deletes/Quarantines the binary from the temp Cerberus analysis will not be performed.

Cerberus analyzes the following types of files:

• acm	• ime	• tmp	• dll	• com	• new	• so	• exe
• ax	• lex	• tsp	• dll~	• cpl	• ocx	• sys	• iec
• cnv	• mui	• wpc	• drv	• dat	• pyd	• tlb	• rfll
• scr							

© Exterro, Inc. All rights reserved

About Cerberus Stage 1 Threat Analysis

Cerberus stage 1 analysis is a general analysis for executable binaries. The Stage 1 analysis engine scans through the binary looking for malicious artifacts. It examines several attributes from the file's metadata and file information to determine its potential to contain malicious code within it. For each attribute, if the condition exists, Cerberus assigns a score to the file. The sum of all of the file's scores is the file's total threat score.

More serious attributes have higher positive scores, such as +20 or +30. Safer attributes have smaller or even negative numbers such as +5, -10 or -20.

The existence of any particular attribute does not necessarily indicate a threat. However, if a file contains several attributes, then the file will have a higher sum score which may indicate that the executable binary may warrant

further investigation. The higher the threat score, the more likely a file may be to contain malicious code.

For example, you may have a file that had four attributes discovered. Those attributes may have scores of +10, +20, +20, and +30 for a sum of +80. You may have another file with four attributes of scores of +5, +10, -10, -20 for a sum of -15. The first file has a much higher risk than the second file.

Cerberus stage 1 analysis also examines each file's properties and provides information such as its size, version information, signature etc.

About Cerberus Score Weighting

There are default scores for each attribute of Cerberus Stage 1 threat scoring. However, you can modify the scoring so that you can weigh the threat score attributes with your own values.

For example, the Bad Signed attribute as a default value of +20. You can give it a different weight of +30.

You must configure these scores before the files are analyzed.

© Exterro, Inc. All rights reserved

About Cerberus Override Scores

Some threat attributes have override scores. If a file has one of these attributes, instead of the score being the sum of the other attributes, the score is overridden with a set value of 100 or -100. This is useful in quickly identifying files that are automatically considered either as a threat or safe. If a bad artifact is found that requires immediate attention, the file is given the maximum score. If an artifact is found that is considered safe, the file is automatically given the minimum score.

Score ranges have maximum and minimum values of -100 to 100.

- High threat signatures will result in a final score of 100.
- Low threat signatures will result in a final score of -100.

Cerberus attributes that have maximum override scores include:

- Bad signatures
- Revoked signatures
- Expired signatures
- Packed with known signature

Note: If any of these attributes are found, the score is overridden with a score of +100.

Cerberus Minimum override score includes:

- Valid digital signature

If this attribute is found, thew score is overridden with a score of -100.

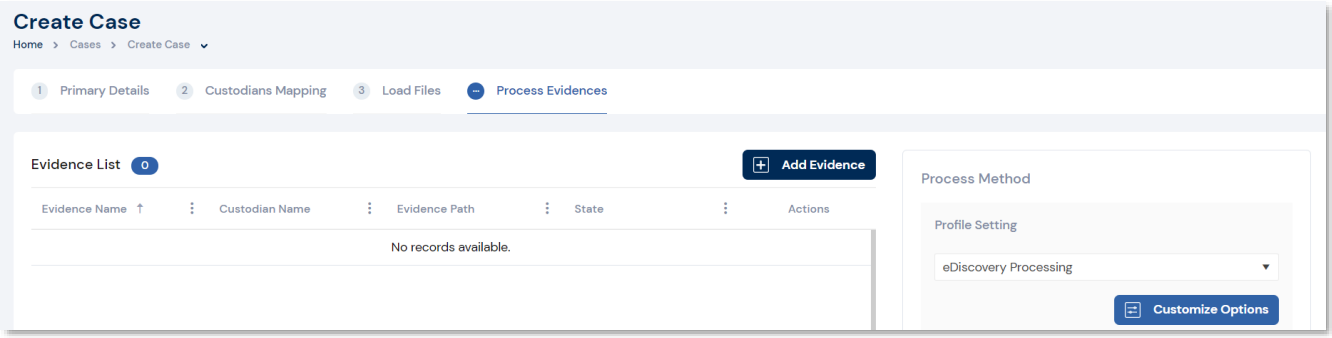
Note: If a file that is malware has a valid digital signature, the override will score the file as -100 (low threat), even though the file is really malware.

© Exterro, Inc. All rights reserved

Running Cerberus Analysis

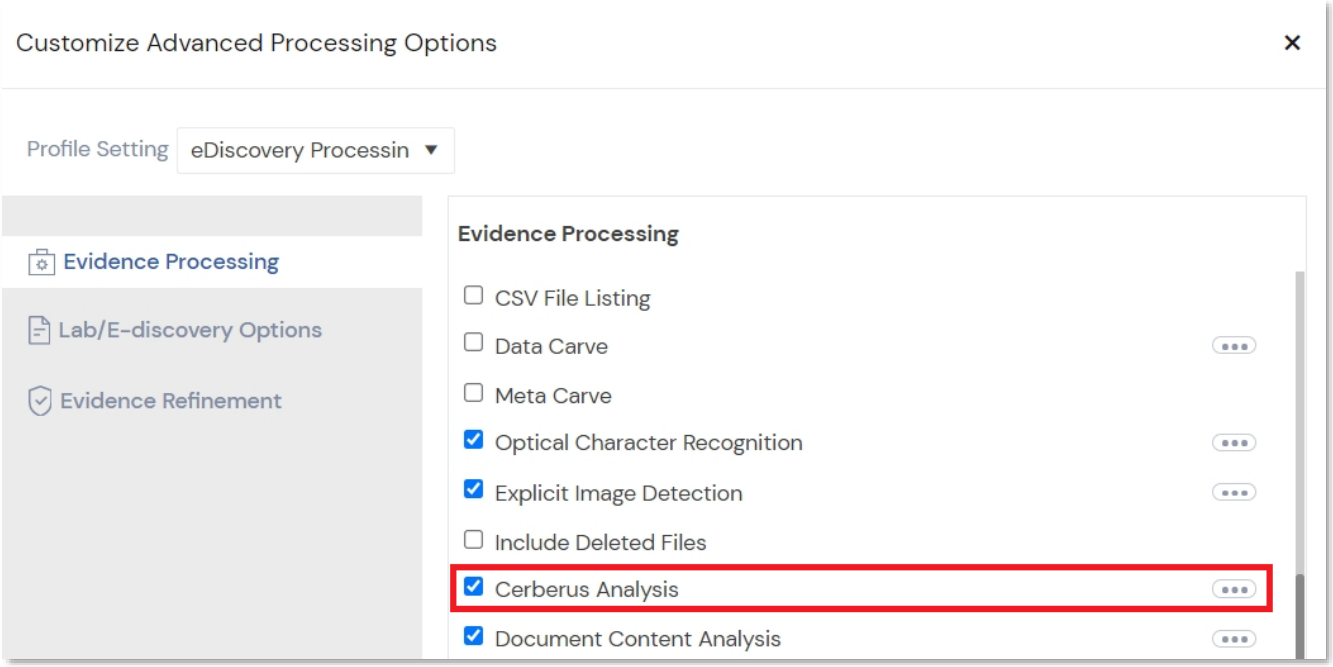
To run Cerberus Analysis:

1. From the Process Evidence page of case creation, click **Customize Options**.



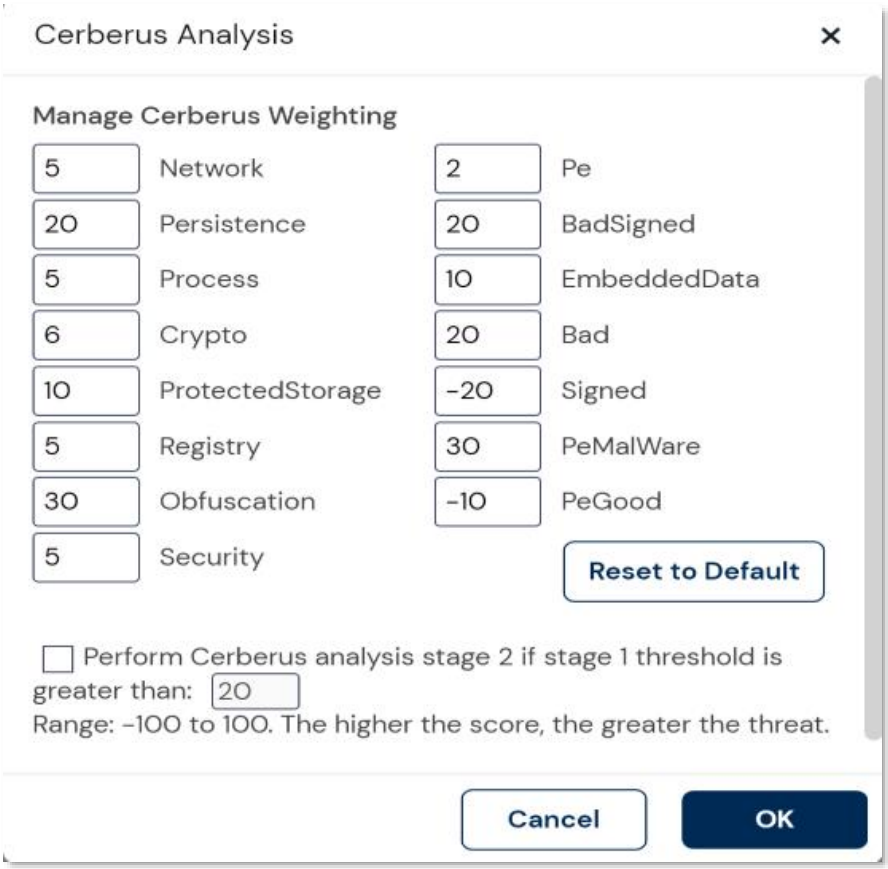
Note: Alternatively, during review, select the desired items, right-click > **Additional Analysis** > **Customize Options**.

2. Select **Cerberus Analysis.**



© Exterro, Inc. All rights reserved

3. Click the **Context menu** ••• to open the configuration.
    - The **Cerberus Analysis** pop-up is displayed.



4. Select one from the options.
    i. In the Cerberus Analysis dialog, you can define the weight assigned to each Cerberus stage 1 score. These Stage 1 scores are designed to identify and score specific malware properties and traits.

© Exterro, Inc. All rights reserved

ii. In the Cerberus Analysis dialog, you can choose the option Perform Cerberus Analysis stage 2 if stage 1 threshold is greater than the value provided. This option lets you choose to automatically run stage 2 analysis after stage 1 analysis completes. Do one of the following:

Options	Description
To run stage 1 analysis only	Deselect the option to Perform Cerberus Analysis stage 2 if stage 1 threshold is greater than, then only Cerberus Analysis stage 1 is run.
To run both stage 1 and 2 analysis	Select the option to Perform Cerberus Analysis stage 2 if stage 1 threshold is greater than n. Specify a threshold for a minimum threat score against which you want to run the stage 2 analysis. If a file's threat score is higher than the threshold value that you set, then stage 2 is run. If a file's threat score is lower than the threshold value, then stage 2 analysis is not run. By default, the threshold automatically runs stage 2 analysis against files with a threat score greater than +20.

5. Click **OK**.
6. Click **Apply**.
7. Click **Process Data** or **Run Analysis**.

© Exterro, Inc. All rights reserved

Filtering Scanned Files and Viewing Threat Scores

After you have processed evidence with Cerberus enabled, you can view a threat score for each executable file by filtering for scanned files. Using the **CerberusScore** column shows the Cerberus scores that were calculated during processing.

To filter scanned files and view threat scores:

1. See Facet Filters section.
2. Click **Cerberus**.
3. Click **Cerberus Stage 1 Analysis** or **Cerberus Stage 2 Analysis.**
4. Click your selected **attribute type**.
5. See Using Custom Columns section.
6. Use the **Cerberus Score** column.

© Exterro, Inc. All rights reserved

Cerberus Stage 1 Threat Scores

The following table lists the threat scores that are provided in a Stage 1 analysis:

Attribute	Default Score	Description
Network	+5	The Network category is triggered when a program contains the functionality to access a network. This could involve any kind of protocol from high-level HTTP to a custom protocol written using low-level raw sockets.
Persistence	+20	Persistence indicates that the application may try to persist permanently on the host. For example, the application would resume operation automatically even if the machine were rebooted.
Process	+5	Process indicates the application may start a new a process or attempt to gain access to inspect or modify other processes. Malicious applications attempt to gain access to other processes to obfuscate their functionality or attack vector or for many other reasons. For example, reading or writing into a process's memory, or injecting code into another process.
Crypto	+6	Crypto is triggered when an application appears to use cryptographic functionality. Malicious software uses cryptography to hide data or activity from network monitors, anti-virus products, and investigators.
Protected Storage	+10	ProtectedStorage indicates that the application may make use of the Windows "pstore" functionality. This is used on some versions of Windows to store encrypted data on the system. For example, Internet Explorer stores a database for form-filling in protected storage.
Registry	+5	Registry is triggered when a target application attempts to use the registry to store data. The registry is commonly used to store

© Exterro, Inc. All rights reserved

Attribute	Default Score	Description
		application settings, auto-run keys, and other data that the application wants to store permanently but not in its own file.
Security	+5	Imports functions used to modify user tokens. For example, attempting to clone a security token to impersonate another logged on user.
Obfuscation	+30	Stage 1 searches for signs that the application is 'packed', or obfuscated in a way that hinders quick inspection. The Obfuscation category is triggered when the application appears to be packed, encrypted, or otherwise obfuscated. This represents a deliberate decision on behalf of the developer to hinder analysis.
Process Execution Space	+2	Unusual activity in the Process Execution Space header. For example, a zero length raw section, unrealistic linker time, or the file size doesn't match the Process Execution Space header.
Bad Signed	+20	This category is triggered when a binary is cryptographically signed, but the signature is invalid. A signature is generally used to demonstrate that some entity you trust (like a government or legitimate company, called a 'signing authority') has verified the authorship and good intentions of the signed application. However, signatures can be revoked and they can expire, meaning that the signature no longer represents that the signing authority has trust in the application.
Embedded Data	+10	This category is triggered when an application contains embedded executable code. While all programs contain some program code, this category indicates that the application has an embedded 'resource', which contains code separate from the code which runs normally as part of the application.

© Exterro, Inc. All rights reserved

Attribute	Default Score	Description
Bad / Bit-Bad	+20	This category is triggered when the application contains signatures indicating it uses the IRC protocol or shellcode signature. Many malware networks use IRC to communicate between the infected hosts and the command-and-control servers.
Signed / Bit-Bad	-20	This category is triggered when a program is signed. A program that is signed is verified as 'trusted' by a third party, usually a legitimate entity like a government or trusted company. The signature may be expired or invalid though; check the 'BadSigned' category for this information.
PE Good	-10	Scores for good artifacts in PE headers.
PE Malware	+30	Scores for known malware artifacts in PE headers.

© Exterro, Inc. All rights reserved

Cerberus Stage 1 File Information

The following table lists the threat scores that are provided in a Stage 1 analysis:

Item	Description
File Size	Displays the size of the file in bytes.
Import Count	Displays the number of functions that Cerberus examined.
Entropy Score	Displays a score of the binaries entropy used for suspected packing or encrypting.
Entropy may be packed	Displays if the files are possibly packed.
Interesting Functions	Displays the name of functions from the process execution space that contributed to the file's threat score.
Suspected Packer List	Attempts to display a list of suspected packers whose signature matches known malware packers.
Modules	Displays the DLL files included in the binary.
Has Version	Displays whether or not the file has a version number.
Version Info	Displays information about the file that is gathered from the Windows API including the following: ▪ CompanyName ▪ FileDescription ▪ FileVersion ▪ InternalName ▪ LegalCopyright ▪ LegalTrademarks ▪ OriginalFilename ▪ ProductName ▪ ProductVersion
Is Signed	Displays whether or not the file is signed. If the file is signed the following information is also provided:

© Exterro, Inc. All rights reserved

Item	Description
	▪ IsValid ▪ SignerName ▪ ProductName ▪ SignatureTime ▪ SignatureResult
Unpacker results	Attempts to show if and which packers were used in the binary.

About Cerberus Stage 2 Static Analysis

When you run a stage 1 analysis, you configure a score that will launch a Cerberus stage 2 analysis. If an executable receives a score that is equal or higher than the configured score, Cerberus stage 2 is performed. Cerberus stage 2 disassembles the code of an executable binary without running the actual executable.

Cerberus Stage 2 Function Call Data

Stage 2 analysis data is generated for the following function call categories:

- File Access
- Networking functionality
- Process Manipulation
- Security Access
- Windows Registry
- Surveillance
- Uses Cryptography
- Low-level Access
- Loads a driver
- Subverts API
- Misc

© Exterro, Inc. All rights reserved

File Access Call Categories

Cerberus Stage 2 File Access Function Call Categories

Category	Description
File Access Functions that manipulate (read, write, delete, modify) files on the local file system.	
Filesystem.File.Read.ExecutableExtension	This is triggered by functionality which reads executable files from disk. The executable code can then be executed, obfuscated, stored elsewhere, transmitted, or otherwise manipulated.
FileSystem.Physical.Read	This application may attempt to read data directly from disk, bypassing the filesystem layer. This is very uncommon in normal applications, and may indicate subversive activity.
FileSystem.Physical.Write	This application may attempt to write data directly to disk, bypassing the filesystem layer in the operating system. This is very uncommon in normal applications, and may indicate subversive activity. It is also easy to do incorrectly, so this may help explain any system instability seen on the host.
FileSystem.Directory.Create:	This indicates the application may attempt to create directory. Modifications to the file system are useful for diagnosing how an application persists, where its code and data are stored, and other useful information.
FileSystem.Directory.Create.Windows:	This indicates an application may try to create a directory in the \Windows directory. This directory contains important operating system files, and legitimate applications rarely need to access it.
FileSystem.Directory.Recursion:	This indicates the application may attempt to recurse through the file system, perhaps as part of a search functionality.

© Exterro, Inc. All rights reserved

Category	Description
FileSystem.Delete:	This indicates the application may delete files. With sufficient permissions, the application may be able to delete files which it did not write or even system files which could affect system stability.
FileSystem.File.DeleteWindows:	This indicates the application may try to delete files in the \Windows directory, where important system files are stored. This is rarely necessary for legitimate applications, so this is a strong indicator of suspicious activity.
FileSystem.File.DeleteSystem32:	This indicates the application may try to delete files in the \Windows\System32 directory, where important system files are stored. This is rarely necessary for legitimate applications, so this is a strong indicator of suspicious activity.
FileSystem.File.Read.Windows	This indicates the application may attempt to read from the \Windows directory, which is very uncommon for legitimate applications. \Windows is where many important system files are stored.
FileSystem.File.Write.Windows:	This indicates the application may attempt to write to the \Windows directory, which is very uncommon for legitimate applications. \Windows is where many important system files are stored.
FileSystem.File.Read.System32:	This indicates the application may attempt to read from the \Windows\System32 directory, which is very uncommon for legitimate applications. \Windows\System32 is where many important system files are stored.
FileSystem.File.Write. System32:	This indicates the application may attempt to write to the \Windows\System32 directory, which is very uncommon for

© Exterro, Inc. All rights reserved

Category	Description
	legitimate applications. \Windows\System32 is where many important system files are stored.
FileSystem.File.Write.ExecutableExtension:	This indicates the application may attempt to write an executable file to disk. This could indicate malicious software that has multiple 'stages', or it could indicate a persistence mechanism used by malware (i.e. write an executable file into the startup folder so it is run when the system starts up).
FileSystem.File.Filename.Compression:	This indicates the program may write compressed files to disk. Compression can be useful to obfuscate strings or other data from quick, automated searches of every file on a filesystem.
FileSystem.File.Filename.Autorun:	This indicates the application may write a program to a directory so that it will run every time the system starts up. This is a useful persistence mechanism.

© Exterro, Inc. All rights reserved

Networking Functionality Call Categories

Cerberus Stage 2 Networking Functionality Function Call Categories

Category	Description
Networking Functionality - Functions that enable sending and receiving data over a network.	
Network.FTP.Get:	Describes the use of FTP to retrieve files. This could indicate the vector a malware application uses to retrieve data from a C&C server.
Network.Raw:	Functions in this category indicate use of the basic networking commands used to establish TCP, UDP, or other types of connections to other machines. Programmers who use these build their own communication protocol over TCP (or UDP or other protocol below the application layer) rather than using an application-layer protocol such as HTTP or FTP.
Network.Raw.Listen:	Functionality in this category indicates the application accepts incoming connections over TCP, UDP, or other lower-level protocol.
Network.Raw.Receive:	Functionality in this bucket indicates that the application receives data using a socket communicating over a lower-level protocol such as TCP, UDP, or a custom protocol.
Network.DNS.Lookup.Country.XX:	This indicates the application may attempt to resolve the address of machines in one of several countries. “XX” will be replaced by the ‘top level domain’, or TLD associated with the lookup,

© Exterro, Inc. All rights reserved

Category	Description
	indicating the application may attempt to establish contact with a host in one of these countries.
Network.HTTP.Read:	The application may attempt to read data over the network using the HTTP protocol. This protocol is commonly used by malware so that its malicious traffic appears to 'blend in' with legitimate web traffic.
Network.HTTP.Connect.Nonstandard.Request:	This indicates the application may make an HTTP request which is not a head, get, or post request. The vast majority of web applications use one or more of these 3 kinds of requests, so this category indicates anomalous behavior.
Network.HTTP.Connect.Nonstandard.Port:	Most HTTP connections occur over either port 80 or 443. This indicates the application is communicating with the server over a non-standard port, which may be a sign that the server is not a normal, legitimate web server.
Network.HTTP.Connect.Nonstandard.Header:	HTTP messages are partially composed of key-value pairs of strings which the receiver will need to properly handle the message. This indicates the application includes non-standard or very unusual header key-value pairs.
Network.HTTP.Post:	This indicates the application makes a 'post' http request. 'post' messages are normally used to push data to a server, but malware may not honor this convention.

© Exterro, Inc. All rights reserved

Category	Description
Network.HTTP.Head:	This indicates the application makes a 'head http request. 'head' messages are normally used to determine information about a server's state before sending a huge amount of data across the network, but malware may not honor this convention.
Network.Connect.Country.XX:	This indicates the application may attempt to connect to a machine in one of several countries. "XX" will be replaced by the 'top level domain', or TLD associated with the lookup.
FTP.Put:	The application may attempt to send files over the network using FTP. This may indicate an exfiltration mechanism used by malware.

© Exterro, Inc. All rights reserved

Process Manipulation Call Categories

Cerberus Stage 2 Process Manipulation Function Call Categories

Category	Description
Process Manipulation – May contain functions to manipulate processes.	
ProcessManagement.Enumeration:	This functionality indicates the application enumerates all processes. This could be part of a system survey or other attempt to contain information about the host.
ProcessManagement.Thread.Create:	This indicates the target application may create multiple threads of execution. This can give insight into how the application operates, operating multiple pieces of functionality in parallel.
ProcessManagement.Thread.Create.Suspended:	This indicates the application may create threads in a suspended state. Similar to suspended processes, this may indicate that the threads are only executed sometime after they're created or that some properties are modified after they are created.
ProcessManagement.Thread.Create:	This indicates the application may attempt to create a thread in another process. This is a common malware mechanism for 'hijacking' other legitimate processes, disguising the fact that malware is on the machine.
ProcessManagement.Thread.Create.Remote:	This indicates that the application may create threads in other processes such that they start in a suspended state. Thus, their functionality or

© Exterro, Inc. All rights reserved

Category	Description
	other properties can be modified before they begin executing.
ProcessManagement.Thread.Open:	The application may try to gain access to observe or modify a thread. This behavior can give insight into how threads interact to affect the host.
ProcessManagement.Process.Open:	This application may attempt to gain access to observe or modify other processes. This can give strong insight into how the application interacts with system and what other processes it may try to subvert.
ProcessManagement.Process.Create:	This application may attempt to create one or more other processes. Similar to threads, multiple processes can be used to parallelize an application's functionality. Understanding that processes are used rather than threads can shed insight on how an application accomplishes its goals.
ProcessManagement.Process.Create.Suspended:	Describes functionality to create new processes in a suspended state. Processes can be created in a 'suspended' state so that none of the threads execute until it is resumed. While a process is suspended, the creating process may be able to substantially modify its behavior or other properties.

© Exterro, Inc. All rights reserved

Security Access Call Categories

Cerberus Stage 2 Security Access Function Call Categories.

Category	Description
Security Access - Functions that allow the program to change its security settings or impersonate other logged on users.	
Security:	This category indicates use of any of a large number of security related functions, including those manipulating security tokens, Access Control Entries, and other items. Even without using an exploit, modification of security settings can enable a malicious application to gain more privileges on a system than it would otherwise have.

© Exterro, Inc. All rights reserved

Windows Registry Call Categories

Cerberus Stage 2 Windows Registry Function Call Categories.

Category	Description
Windows Registry – Functions that manipulate (read, write, delete, modify) the local Windows registry. This also includes the ability to modify autoruns to persist a binary across boots.	
Registry.Key.Create:	The application may attempt to create a new key in the registry. Keys are commonly used to persist settings and other configuration information, but other data can be stored as well.
Registry.Key.Delete:	This application may attempt to delete a key from the registry. While it is common to delete only keys that the application itself created, with sufficient permissions, Windows may not prevent an application from deleting other applications' keys as well.
Registry.Key.Autorun:	This indicates the application may use the registry to try to ensure it or another application is run automatically on system startup. This is a common way to ensure that a program continues to run even after a machine is restarted.
Registry.Value.Delete:	This indicates the application may attempt to delete the value associated with a particular key. As with the deletion of a key, this may not represent malicious activity so long as the application only deletes its own keys' values.
Registry.Value.Set:	The application may attempt to set a value in the registry. This may represent malicious behavior if the value is set in a system key or the key of another application.
Registry.Value.Set.Binary:	This indicates the application may store binary data in the registry. This data could be encrypted, compressed, or otherwise is not plain text.

© Exterro, Inc. All rights reserved

Category	Description
Registry.Value.Set.Text:	This indicates the application may write plain text to the registry. While the 'text' flag may be set, this does not mandate that the application write human-readable text to the registry.
Registry.Value.Set.Autorun:	The application may set a value indicating it will use the registry to persist on the machine even after it restarts.

© Exterro, Inc. All rights reserved

Surveillance Call Categories

Cerberus Stage 2 Surveillance Function Call Categories.

Category	Description
Surveillance – Usage of functions that provide audio/video monitoring, keylogging, etc.	
Driver.Setup:	Functionality in this category involves manipulation of INF files, logging, and other driver-related tasks. Drivers are used to gain complete control over a system, potentially even gaining control of other security products.
Driver.DirectLoad:	Functionality in this category involves loading drivers. As noted in 'driver.setup', drivers represent ultimate control over a host system and should be extremely trustworthy.

Uses Cryptography Call Categories

Cerberus Stage 2 Uses Cryptography Function Call Categories.

Category	Description
Uses Cryptography – Usage of the Microsoft CryptoAPI functions.	
Crypto.Hash.Compute:	This indicates a hash function may be used by the target application. Hash functions are used to verify the integrity of communications or files to ensure they were not tampered with.
Crypto.Algorithm.XX:	The "XX" could be any of several values, including 'md5', 'sha-1', or 'sha-256'. These represent particular kinds of hashes which the target application may use.
Crypto.MagicValue:	This indicates that the target contains strings associated with cryptographic functionality. Even if the application does not use Windows OS functionality to use cryptography, the 'magic values' will exist so long as the target uses standard cryptographic algorithms.

© Exterro, Inc. All rights reserved

Low-level Access Call Categories

Cerberus Stage 2 Low-level Access Function Call Categories

Category	Description
Low-level Access – Functions that access low-level operating system resources, for example reading sectors directly from disk.	
Driver.Setup:	Functionality in this category involves manipulation of INF files, logging, and other driver-related tasks. Drivers are used to gain complete control over a system, potentially even gaining control of other security products.
Driver.DirectLoad:	Functionality in this category involves loading drivers. As noted in 'driver.setup', drivers represent ultimate control over a host system and should be extremely trustworthy.
Debugging.dbghelp:	This indicates use of functionality included in the dbghelp.dll module from the "Debugging Tools for Windows" package from Microsoft. With the proper permissions, the functionality in this library represents a power mechanism for disguising activity from investigators or for gaining control of other processes.
Misc.SystemRestore:	Describes functionality involved in the System Restore feature, including removing and adding restore points. Restore points are often used as part of a malware-removal strategy, so removal of arbitrary restore points, especially without user interaction, may represent malicious activity.
Debugging.ChecksForDebugger:	This is triggered if the application tries to determine whether it is being debugged. Malicious applications commonly try to determine whether they're being analyzed so that they can modify the behavior seen by analysts, making it difficult to discover their true functionality.

© Exterro, Inc. All rights reserved

Loads a drive Call Categories

Cerberus Stage 2 Loads a drive Function Call Categories.

Category	Description
Loads a driver	Function that loads drivers into a running system.

Subverts API Call Categories

Cerberus Stage 2 Subverts API Function Call Categories.

Category	Description
Subverts API	Undocumented API functions, or unsanctioned usage of Windows APIs (for example, using native API calls).

© Exterro, Inc. All rights reserved

Document Content Analysis

You can use Document Content Analysis to group document data together for quicker review.

The application uses an algorithm to cluster the data. The algorithm accomplishes this by creating an initial set of cluster centers called pivots. The pivots are created by sampling documents that are dissimilar in content. For example, a pivot may be created by sampling one document that may contain information about children's books and sampling another document that may contain information about an oil drilling operation in the Arctic. Once this initial set of pivots is created, the algorithm examines the entire data set to locate documents that contain content that might match the pivot's perimeters. The algorithm continues to create pivots and clusters documents around the pivots. As more data is added to the case and processed, the algorithm uses the additional data to create more clusters.

Word frequency or occurrence count is used by the algorithm to determine the importance of content within the data set. Noise words that are excluded from Document Content Analysis are also not included in the Cluster Topic pivots or clusters.

Note: If you activated Document Content Analysis as an Evidence Processing option when you created the case, Document Content Analysis will automatically run after processing data and will not need to be run manually.

© Exterro, Inc. All rights reserved

Considerations of Cluster Topic

You need to aware the following considerations when examining the Cluster Topic categories:

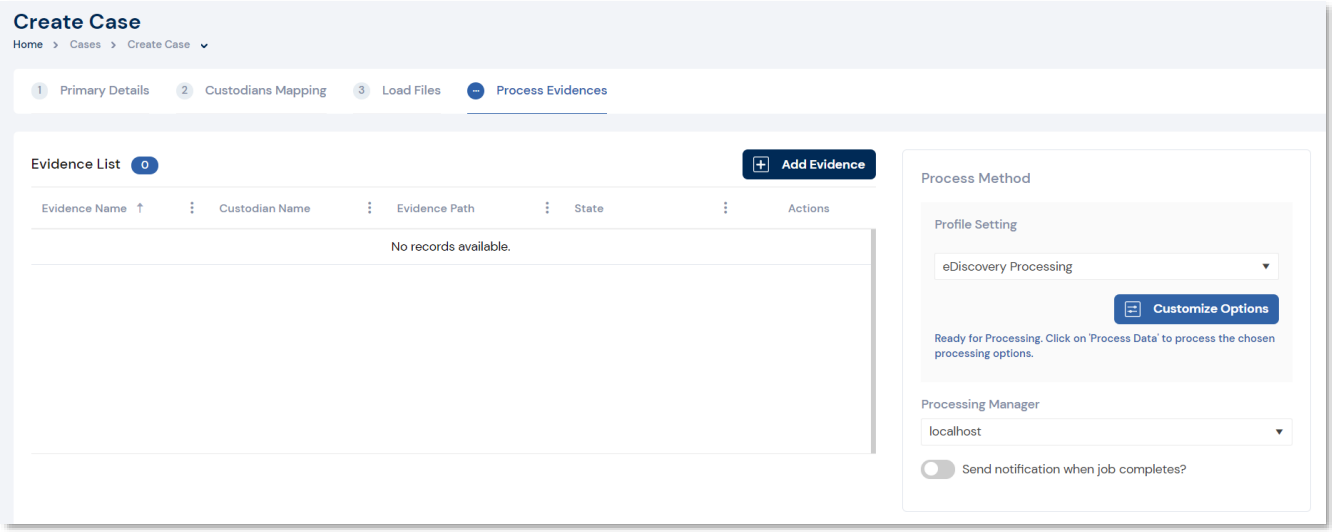
- Not all data will be grouped into categories at once. The application creates categories in an incremental fashion in order to return results as quickly as possible. Since the application is continually creating categories, the Cluster Topic container is continually updated.
- Duplicate documents are grouped together as they match a specific category. However, if a category is particularly large, duplicate documents may not be included as part of any category. This is to avoid performance issues. You can examine any duplicate documents or any documents not included in a category by highlighting the UNCLUSTERED category of the Cluster Topic container/filter.
- Cluster Topic results can vary when performed on different databases and/or different computers. This is due to the analytic behavior of the Document Content Analysis process. Since limits have been set on the algorithm to allow for efficient collection of data, large amounts of content can thus produce varying results.

© Exterro, Inc. All rights reserved

Running Document Content Analysis

To run document content analysis:

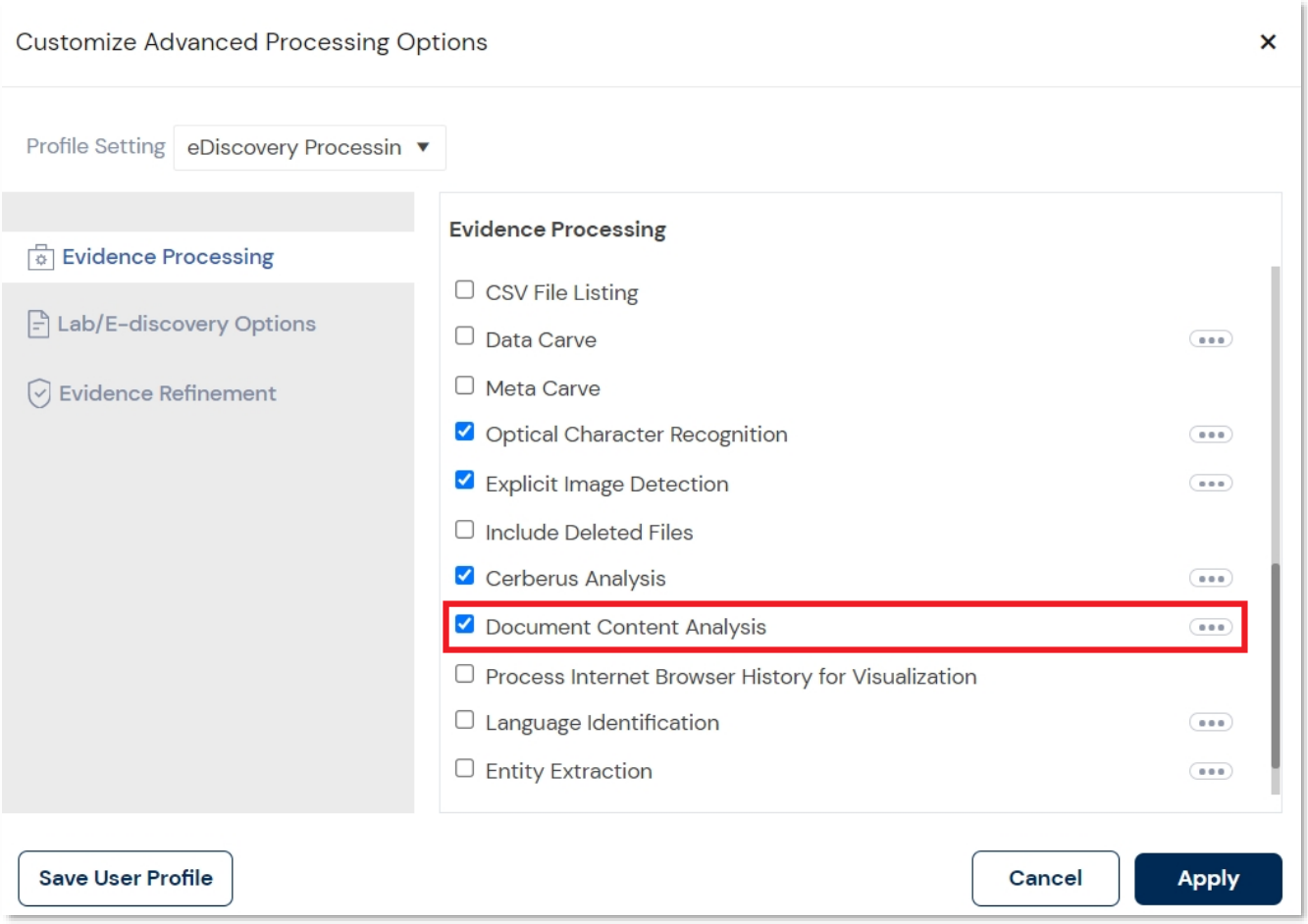
1. From the Process Evidence page of case creation, click **Customize Options**.



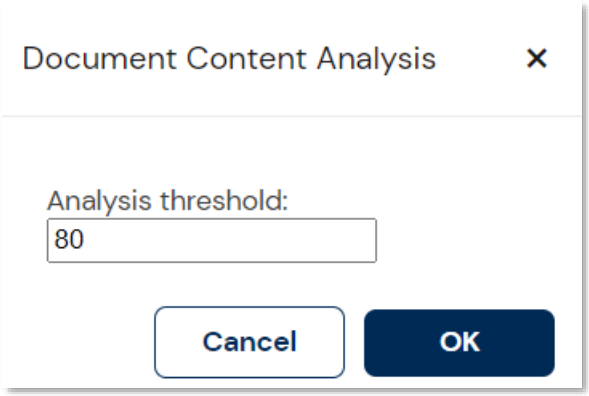
Note: Alternatively, during review, select the desired items, right-click > **Additional Analysis** > **Customize Options**.

© Exterro, Inc. All rights reserved

2. Select **Document Content Analysis**.



3. Click the **Context menu** ••• to open the configuration.
   - The **Document Content Analysis** pop-up is displayed.



© Exterro, Inc. All rights reserved

4. Configure the **Analysis Threshold** to sets the level of similarity (in a percentage) that is required for documents to be considered related or near duplicates. The higher the percentage, the more similar the documents need to be in order to be considered similar.
5. Click **OK**.
6. Click **Apply**.
7. Click **Process Data** or **Run Analysis**.

© Exterro, Inc. All rights reserved

Filtering Documents by Document Content Analysis

Documents processed with Document Content Analysis can be filtered by the content of the documents in the evidence. The Cluster Topic container is created from data processed with Document Content Analysis. Data included in the Cluster Topic container is taken from documents, including Word documents, text documents, and PDF documents.

To filter document by document content analysis:

1. See Facet Filters section.
2. Click **General**.
3. Click **Document Content**.
4. Click **Cluster Topic**.
5. Check a topic from the list to see related items in the Grid.

© Exterro, Inc. All rights reserved

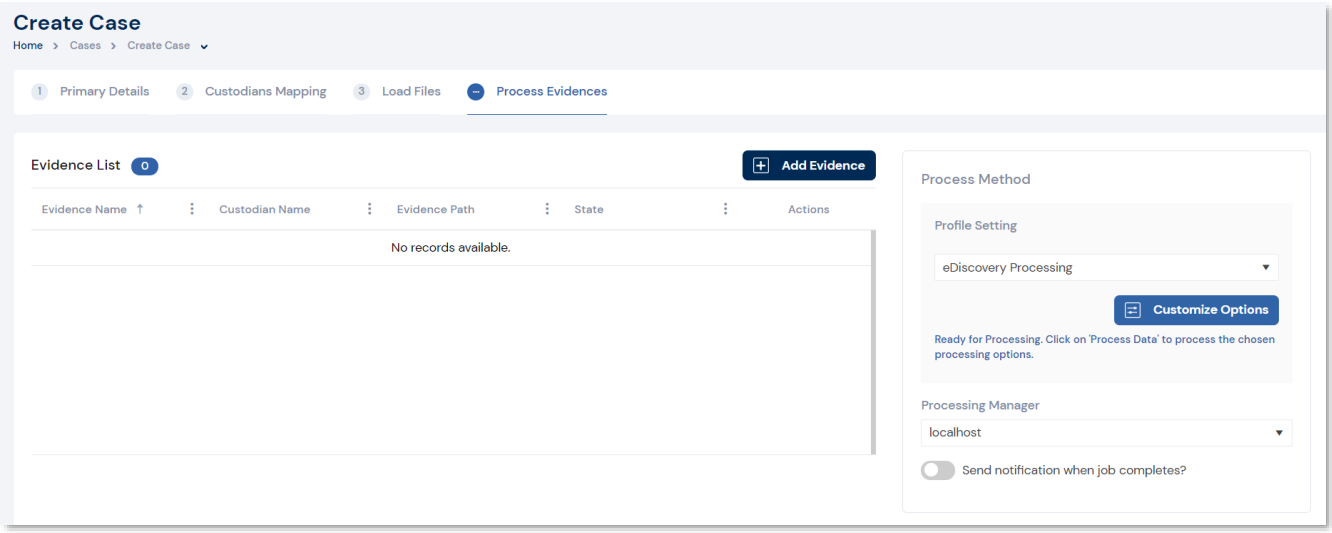
Language Identification

When processing evidence, you can perform automatic language identification. This will analyze the first two pages of every document to identify the language. To identify languages, you have to enable the Language Identification processing option.

Performing Language Identification

To perform language identification:

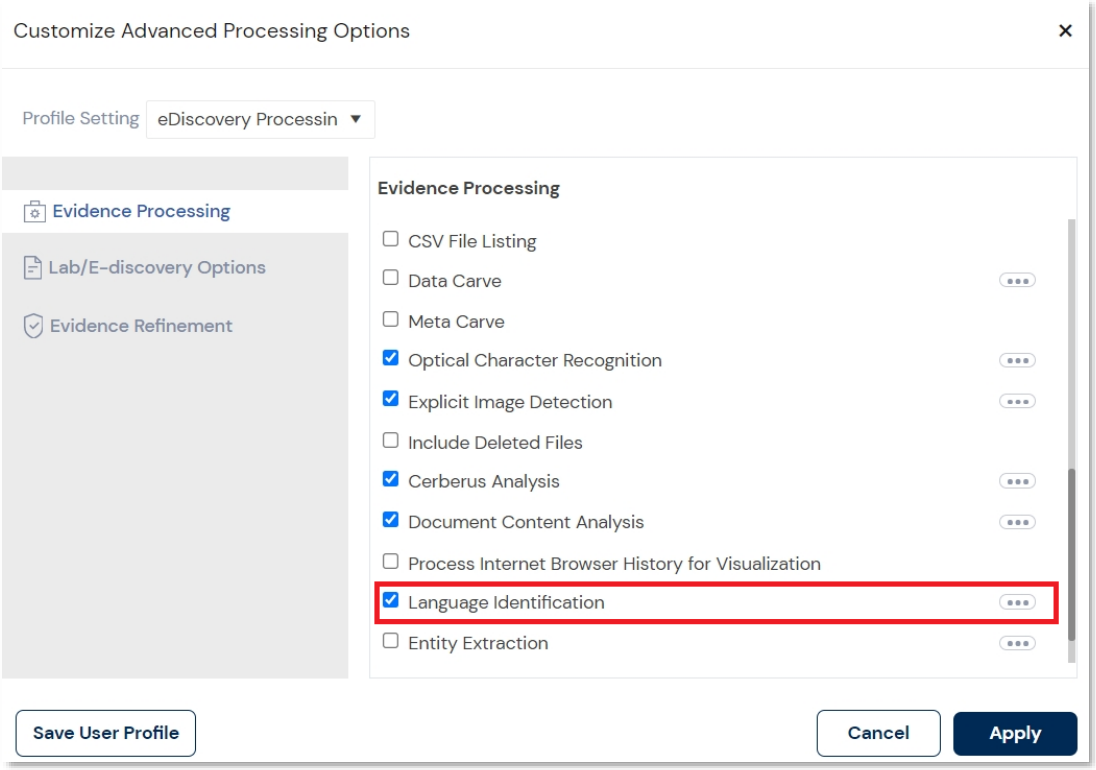
1. From the Process Evidence page of case creation, click **Customize Options**.



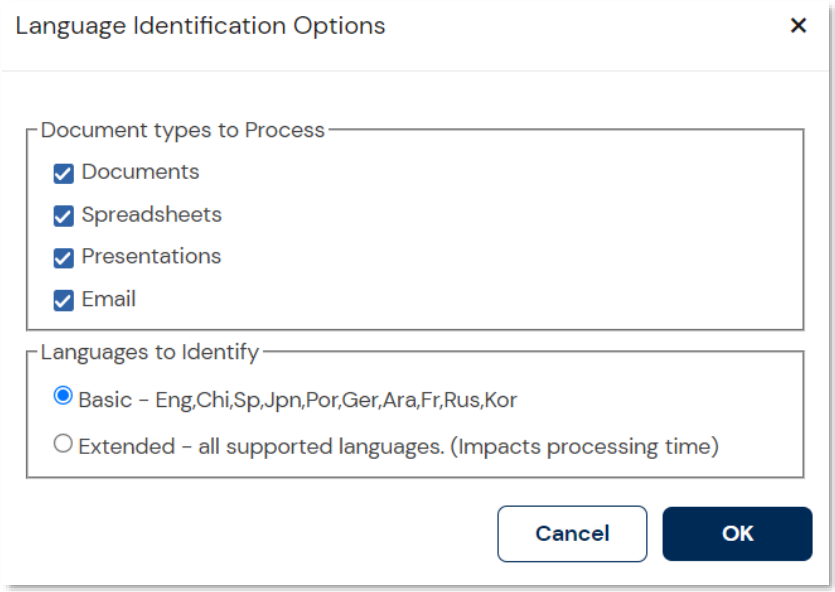
Note: Alternatively, during review, select the desired items, right-click > **Additional Analysis** > **Customize Options**.

© Exterro, Inc. All rights reserved

2. Select **Language Identification**.



3. Click the **Context menu** ••• to open the configuration.
   - The **Language Identification Options** pop-up is displayed.



© Exterro, Inc. All rights reserved

4. Set the **Language Identification Options** as explained below.

Options	Description
Document Types to Process	You can select to process the following file types: • Documents • Presentation • Spreadsheets • Email
Languages to Identify	You can select to identify the following: • Basic languages that include English, Chinese, Spanish, Japanese, Portuguese, Arabic, French, Russian, and Korean. • Extended languages. Performs language identification for 67 different languages. This is the slowest processing option.

5. Click **OK**.
6. Click **Apply**.
7. Click **Process Data** or **Run Analysis**.

Note: The Language Identification processing option is disabled by default. If you enable it, the basic language setting and all four document types are enabled by default.

© Exterro, Inc. All rights reserved

Viewing Language Identified Documents

After processing is complete, you can add the **Language** column in the File List in the Grid.

See Using Custom Columns section.

You can filter by the Language field within review and determine who needs to review which documents based on the language contained within the document. If there are multiple languages in a document, the first language will be identified.

Basic Languages

The system will perform language identification for the following languages:

- Arabic
- Chinese
- English
- French
- German
- Japanese
- Korean
- Portuguese
- Russian
- Spanish

If the language to identify is one of the ten basic languages (except for English), select Basic when choosing Language Identification. The Extended option also identifies the basic ten languages, but the processing time is significantly greater.

© Exterro, Inc. All rights reserved

Extended Languages

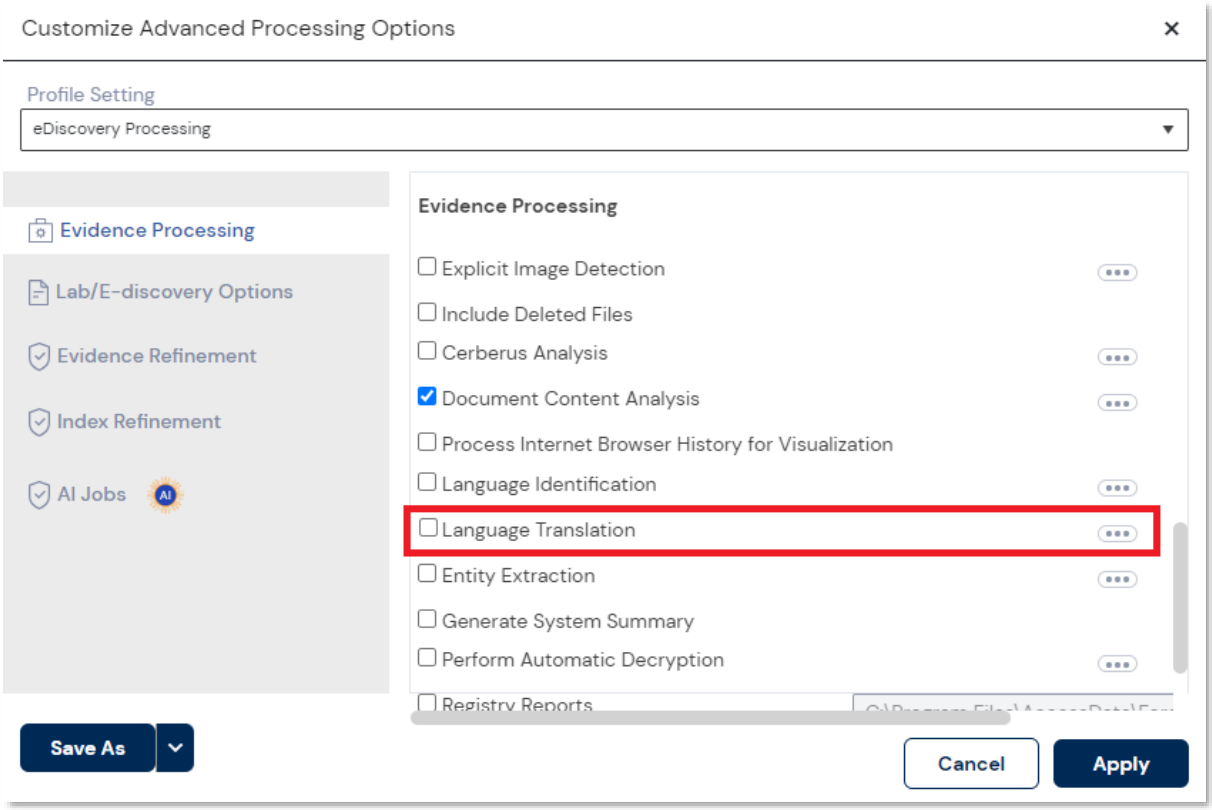
The system will perform language identification for 67 different languages. This is the slowest processing option. The following languages can be identified:

- Afrikaans
- Arabic
- Belarusian
- Bulgarian
- Croatian
- Dutch
- Estonian
- Georgian
- Hawaiian
- Hungarian
- Irish
- Korean
- Lithuanian
- Marathi
- Persian
- Quechua
- Russian
- Scottish Gaelic
- Slovenian
- Swedish
- Thai
- Vietnamese
- West Frisian
- Albanian
- Armenian
- Bosnian
- Catalan
- Czech
- English
- Finnish
- German
- Hebrew
- Icelandic
- Italian
- Latin
- Malay
- Nepali
- Polish
- Romanian
- Sanskrit
- Serbian
- Spanish
- Tagalong
- Turkish
- Welsh
- Amharic
- Basque
- Breton
- Chinese
- Danish
- Esperanto
- French
- Greek
- Hindi
- Indonesian
- Japanese
- Latvian
- Manx
- Norwegian
- Portuguese
- Rumantsch
- Scots
- Slovak
- Swahili
- Tamil
- Ukrainian
- Yiddish

© Exterro, Inc. All rights reserved

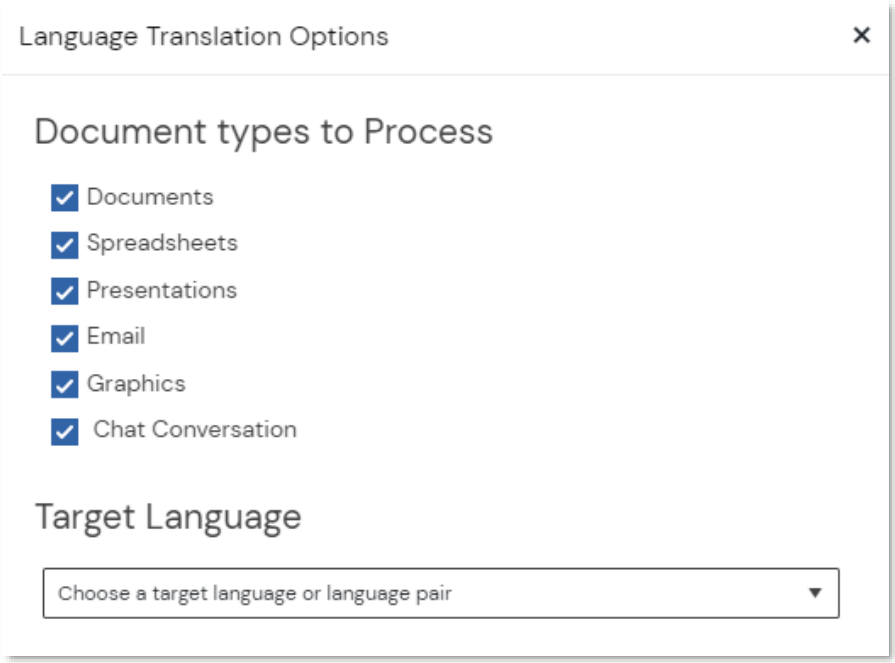
Language Translation

FTK Central allows you to automatically translate the files of other languages to English for an effective review process. This action can be performed by enabling the **Language Translation** processing option while creating or editing a case.

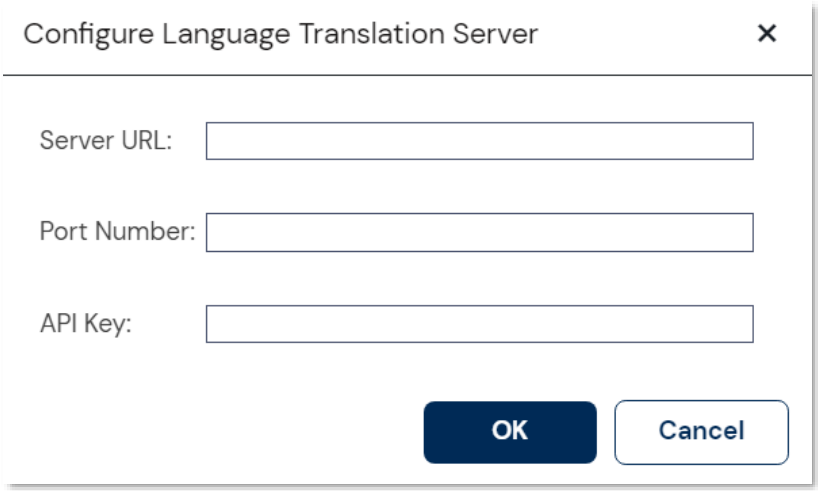


© Exterro, Inc. All rights reserved

Upon enabling this option, click on the button to open the Language Translation Options pop-up and configure the following details:



- To select the file types from the **Document Types to Process** section for which the language translation should be performed.
- To click on **Configure** and configure the server details using which the language translation should be performed.



© Exterro, Inc. All rights reserved

Entity Extraction

The Entity Extraction process extracts data from the content of files in your evidence. Unlike other processing option, this option extracts the data from the body of data rather than the metadata. Users can extract the following types of data:

- Credit Card Numbers
- Phone Numbers
- Social Security Numbers
- E-Mail Addresses

Information Type	Syntax	Successful extraction example	Fail case extraction example
Credit Card Numbers	16-digit numbers used by VISA, MasterCard, and Discover	• 1234-5678-9012-3456 • 1234 5678 9012 3456	• 1234567890123456 • 12345678-90123456
Credit Card Numbers	15-digit numbers used by American Express	• 1234-5678-9012-345 • 1234 5678 9012 345	• 1234567890123456 • 12345678-90123456
Phone Numbers	Standard 7-digit numbers	• 123 4567 • 123.3567 • 123-4567	• 1234567
Phone Numbers	Standard 10-digit numbers (A leading 1, for long-distance or 001 for international, is not included in the	• 123 456 7890 • (123)456-7890 • (123)456 7890 • (123) 456-7890 • (123) 456.7890 • +1 (123) 456.7890	• 1234567890

© Exterro, Inc. All rights reserved

Information Type	Syntax	Successful extraction example	Fail case extraction example
	extraction, however, a +1 is.)		
International Phone Numbers		• +12-34-567-8901 • +12 34 567 8901 • +12-34-5678-9012 • +12 34 5678 9012	• 12345678901 • (10) 69445464 • 07700 954 321 • (0295) 416,72,16
Social Security Numbers	Standard 9-digit number	• 123-45-6789 • 123 45 6789	• 123456789 • 12345-6789
Email Address	A prefix to the left of the @ symbol and a domain to the right of the @ symbol.	• username@company.com	• @companyname.com • username.com • username@.net • username.net@company

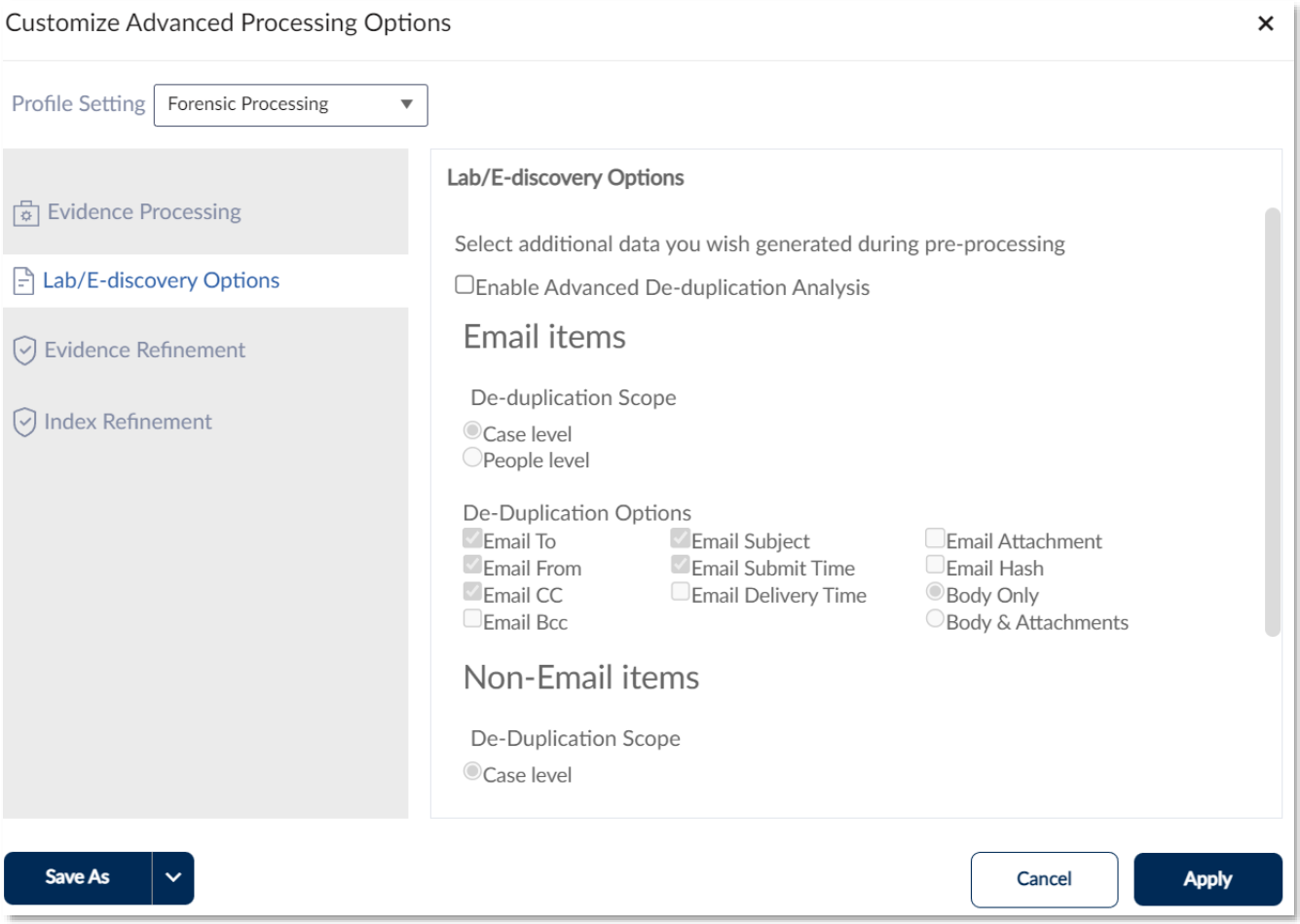
Warnings:

- Entities matching syntaxes with each other may be wrongly identified. For instance, a 15-digit Credit Card Number, 5105-1051-051-5100 may also be extracted as the phone number 510-5100.
- Apart from the 16-digit and 15-digit credit card number, other formats, such as 14-digit Diners Club numbers will not be extracted as credit card numbers

© Exterro, Inc. All rights reserved

Lab/E-discovery Options

De-duplication is separated by email items and non-email items. Within each group, the available options can be applied by Case or by Custodian (People).



© Exterro, Inc. All rights reserved

The following table provides more information regarding each option and its description.

Option	Description
Enable Advanced De-duplication Analysis.	Enable this option to perform de-duplication on the email items and non-email items. This acts as the parent function for all the child function options listed in the page.
Email Items - De-duplication Scope	Choose whether you want this de-duplication process to be applied at the Case level, or at the Custodian (People) level.

Email Items - De-duplication Options	Select the duplicates to be eliminated from the case as it processes through the collected evidence.
	Options available:
	• Email To
	• Email From
	• Email CC
	• Email BCC
	• Email Subject
	• Email Submit Time
	• Email Delivery Time
	• Email Attachment Time
	• Email Attachment Count
	• Email Hash
	  ○ Body Only
	  ○ Body and Attachments

Non-email items - De-duplication Scope	Choose whether you want this de-duplication process to be applied at the Case level, or at the Custodian (People) level. There is only one option available for non-email items; either you are going to deduplicate just the actual files, or if unmarked, you

© Exterro, Inc. All rights reserved

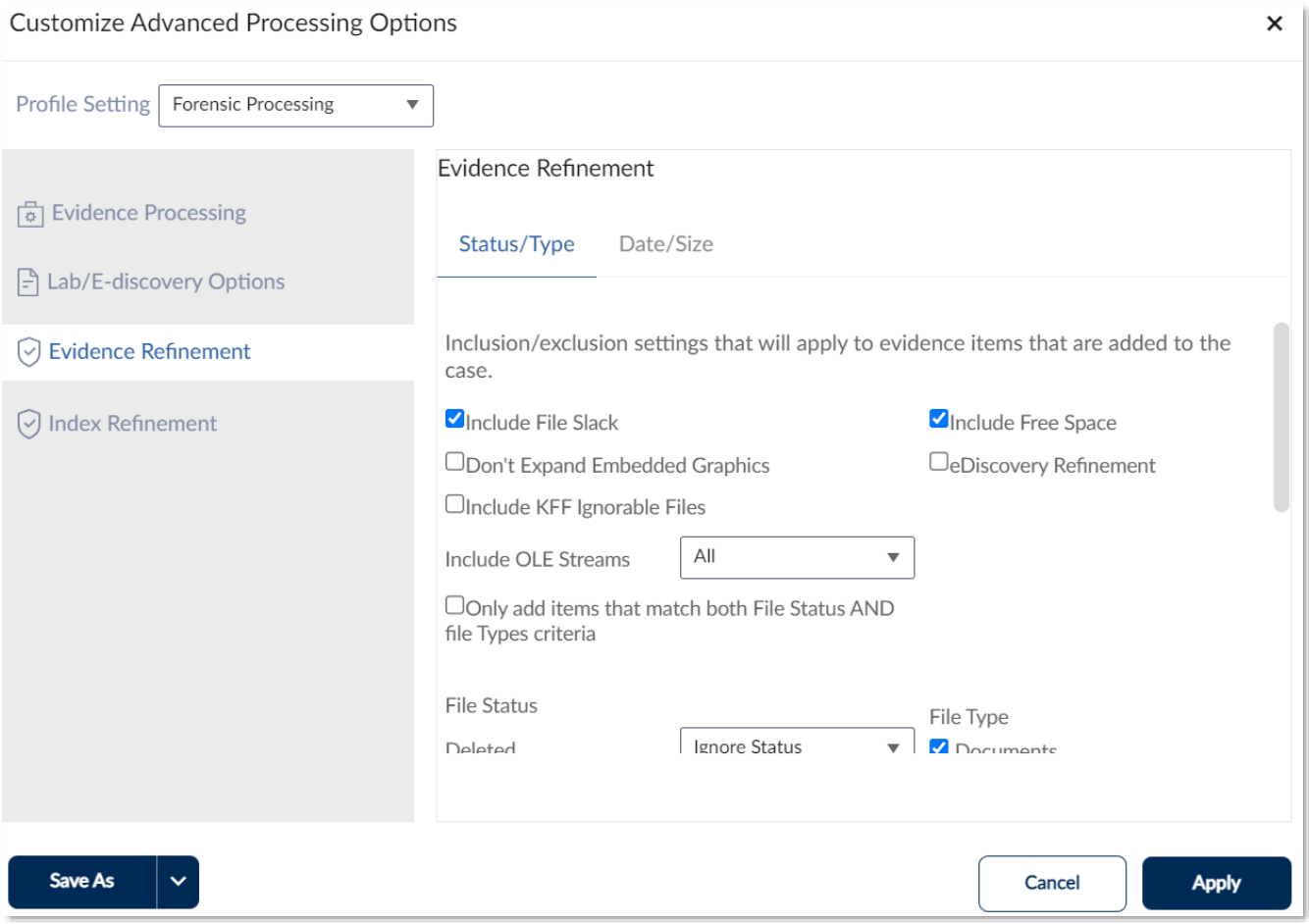
Option	Description
	will de-duplicate actual files only, or all files, including children, zipped, OLE, and carved files.
Propagate Email Attribute	When an email has attachments or OLE items, marking this option causes the email's attributes to be copied and applied to all "child" files of the email "parent."
Cluster Analysis	Invokes the extended analysis of documents to determine related, near duplicates, and email threads. This lets you specify the options for Cluster Analysis. You can specify which document types to process: • Documents • Presentations • Spreadsheets • Email You can also specify the similarity threshold, which determines the level of similarity required for documents to be considered related or near duplicates. Click **Cluster Analysis Options** to select the document types for performing Cluster Analysis.
Include Extended Information in the Index	Enable this to make the index data fully compatible with Summation/eDiscovery. This is generally enabled if you created a case in Exterro FTK and need to review it in Summation or eDiscovery.
Create Email Threads	Enable this to sort and group emails by conversation threads.

© Exterro, Inc. All rights reserved

Evidence Refinement

The Evidence Refinement Options allow you to specify how the evidence is to be sorted and displayed. Also, this allows you to exclude specific data from the case evidence.

Many factors can affect which processing options are required. For example, if you have text-based data, you may perform a full text index to aid in the review process. Also, you may have identified the dataset has no use of encryption. In this case an entropy test may not be needed.



© Exterro, Inc. All rights reserved

Refining Evidence by File Status/Type

Processing Option	Description
Include File Slack	To include file slack space in which evidence may be found.
Include Free Space	To include unallocated space which evidence may be found.
Include KFF Ignorable Files	To include files flagged as 'Ignorable' in the KFF for analysis.
Include OLE Streams	To include Object Linked and Embedded (OLE) data streams that are layered, linked, or embedded.
eDiscovery Refinement	To exclude files and folders that are not useful for most eDiscovery cases.
Don't Expand Embedded Graphics	This option lets you skip processing the graphics embedded in the email files.
Deleted	To decide how to treat the deleted files. You can choose to: • Ignore Status • Include Only • Exclude
Encrypted	To decide how to treat encrypted files. You can choose to: • Ignore Status • Include Only • Exclude
From Email	To decide how to treat email files. You can choose to: • Ignore Status • Include Only • Exclude
File Types	To select the required file types. You can exclude the files by proceeding to the next step without selecting it.

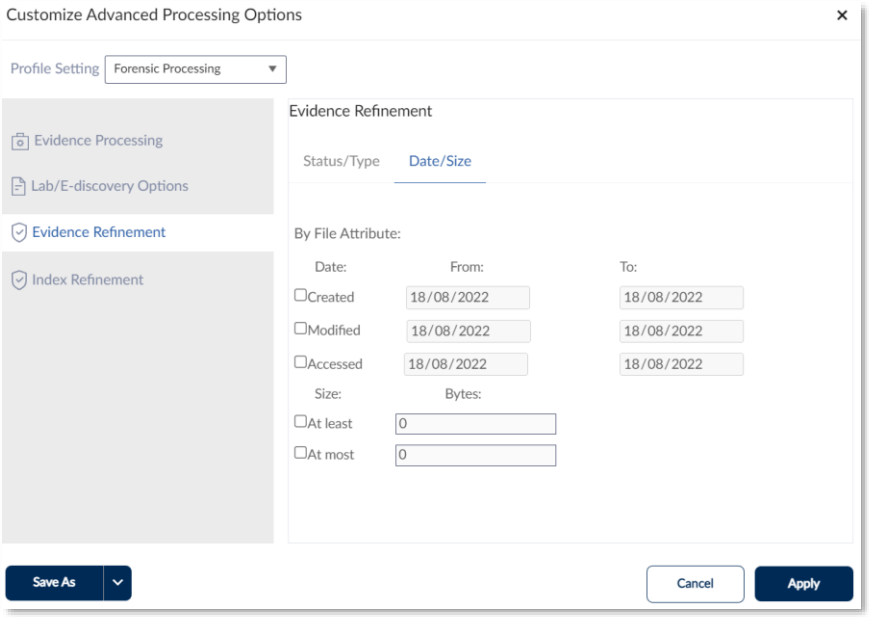
© Exterro, Inc. All rights reserved

Processing Option	Description
Only add items to the case that match both File Status and File Type criteria	To add files matching all the criteria selected in both.
Exclude by Category	To exclude any categories from indexing.

Refining Evidence by File Status/Type

You can filter files by the date range defined for Created, Last Modified, or Last Accessed date of the files. Files matching any of the three date filters will be considered here.

Similarly, you can filter the files based on the minimum and maximum file size using the **At least** and **At most** fields. Files matching any of the two size filters will be considered here.



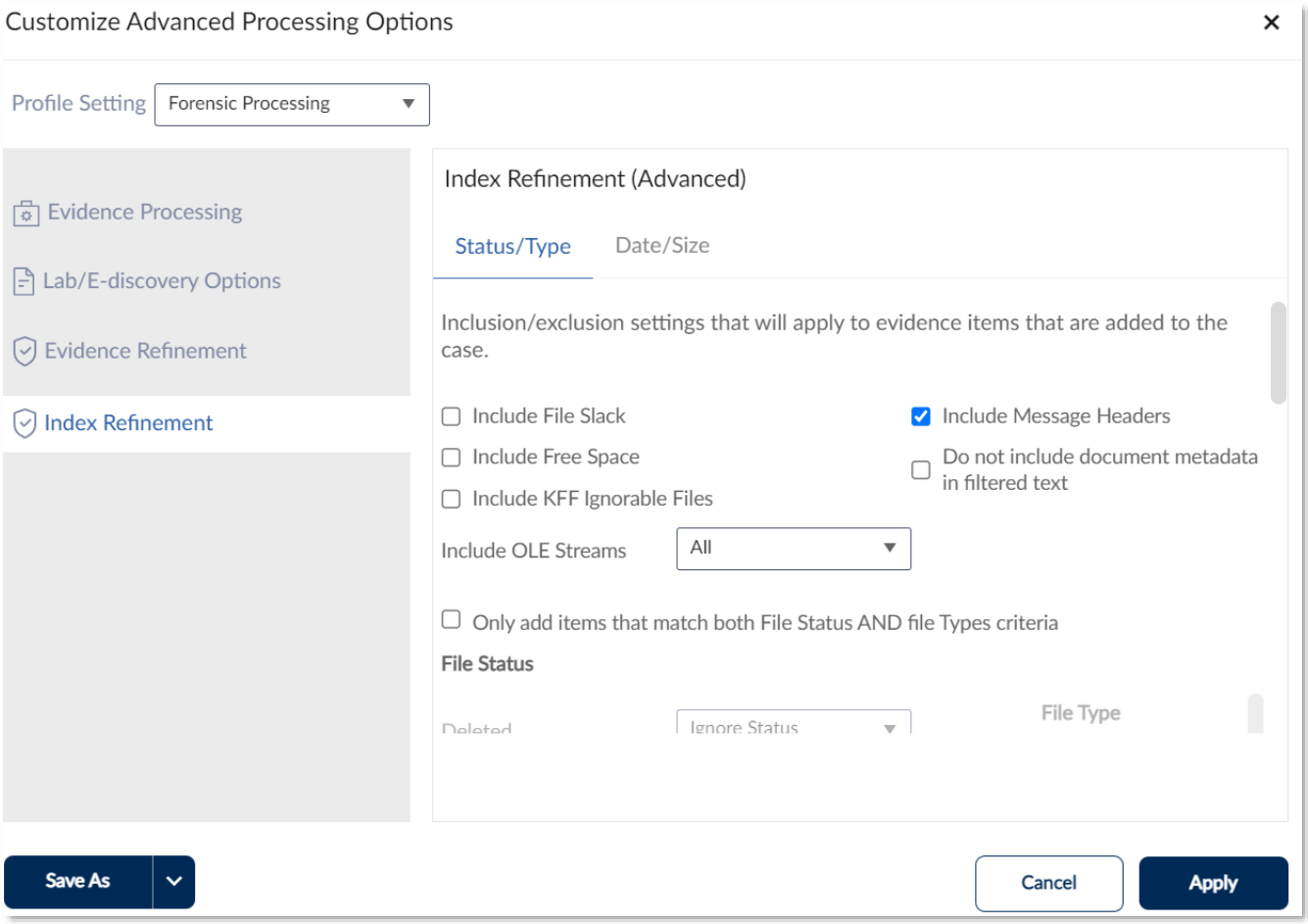
Warning: When both date and size filters are used, only the files matching both the conditions are included.

© Exterro, Inc. All rights reserved

Index Refinement

The Index Refinement option allows you to specify types of data that you do not want to index. You may choose to exclude data to save time and resources, or to increase searching efficiency.

Warning: Exterro strongly recommends that you use the default index settings.



© Exterro, Inc. All rights reserved

Refining an Index by File Status/Type

Refining an index by file status and type allows the investigator to focus attention on specific files needed for a case through a refined index defined in a dialog. At the bottom of the Status/Type Index Refinement tab you can choose to mark the box for Only index items that match both File Status AND File Types criteria, if that suits your needs.

Processing Option	Description
Include File Slack	Mark to include free space between the end of the file footer, and the end of a sector, in which evidence may be found.
Include Free Space	Mark to include both allocated (partitioned) and unallocated (unpartitioned) space in which evidence may be found.
Include KFF Ignorable Files	Mark to include files flagged as ignorable in the KFF for analysis.
Include Message Headers	Marked by default. Includes the headers of messages in filtered text. Unmark this option to exclude message headers from filtered text.
Do not include document metadata in filtered text	Not marked by default. This option lets you turn off the collection of internal metadata properties for the indexed filtered text. The fields for these metadata properties are still populated to allow for field level review, but the you will no longer see information such as Author, Title, Keywords, Comments, etc in the Filtered text panel of the review screen. If you use an export utility such as ECA or eDiscovery and include the filtered text file with the export, you will also not see this metadata in the exported file.
Include OLE Streams	Includes Object Linked or Embedded (OLE) data streams that are part of files that meet the other criteria.
Deleted	Specifies the way to treat deleted files. Options are: • Ignore status • Include only • Exclude

© Exterro, Inc. All rights reserved

Processing Option	Description
Encrypted	Specifies the way to treat encrypted files. Options are: • Ignore status • Include only • Exclude
Email	Specifies the way to treat email files. Options are: • Ignore status • Include only • Exclude
File Types	Specifies types of files to include and exclude.
Only add items to the index that match both File Status and File Type criteria	Applies selected criteria from both File Status and File Types tabs to the refinement. Will not add items that do not meet all criteria from both pages.

Refining an Index by File Date/Size

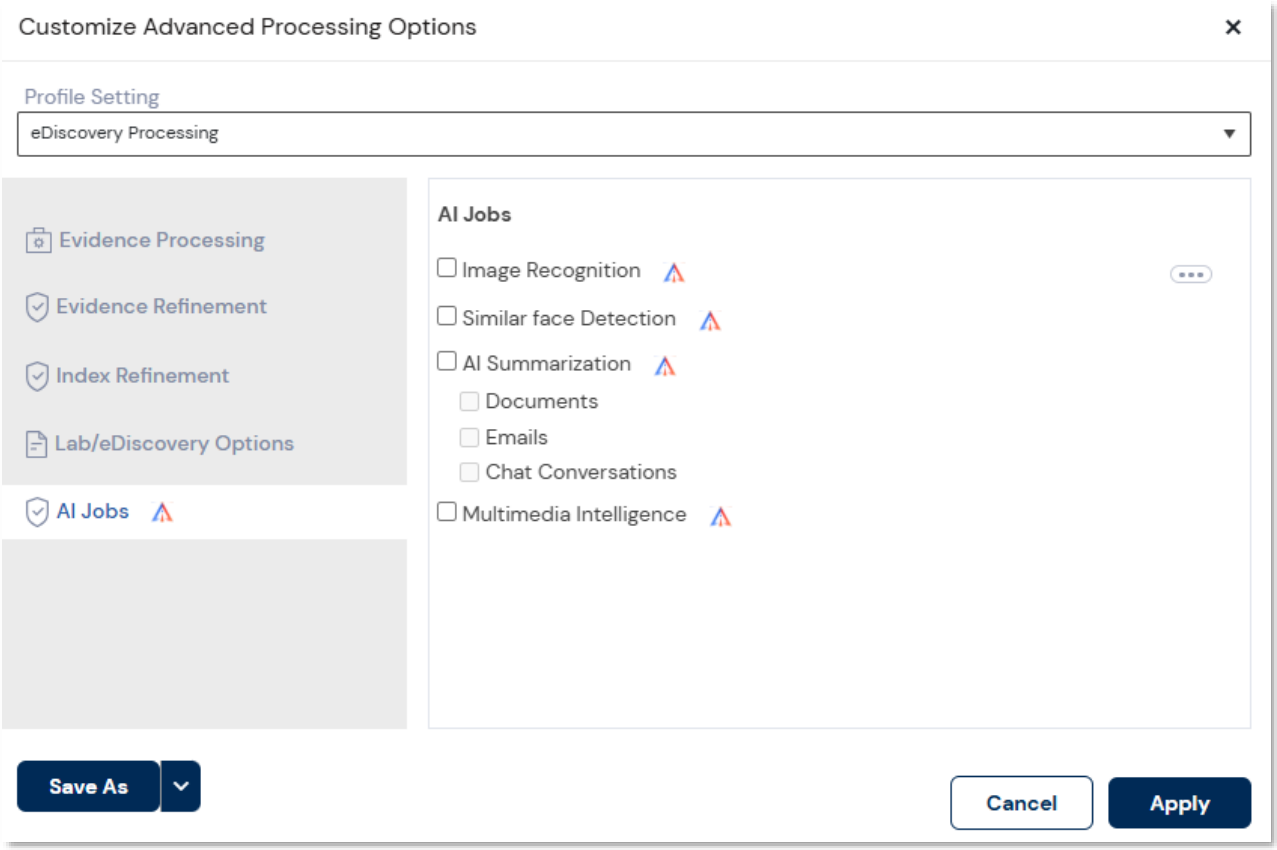
Refine index items dependent on a date range or file size you specify.

Processing Option	Description
Refine Index by File Date	To refine index content by file date: 1. Select Created, Last Modified, or Last Accessed. 2. In the date fields, enter beginning and ending dates within which to include files.
Refine Index by File Size	To refine index content by file size: 1. Click in either or both of the size selection boxes. 2. In the two size fields for each selection, enter minimum and maximum file sizes (bytes) to include.

© Exterro, Inc. All rights reserved

AI Jobs

FTK Central provides you with the following features that employs the power of Artificial Intelligence (AI) to search and extract crucial information from images:

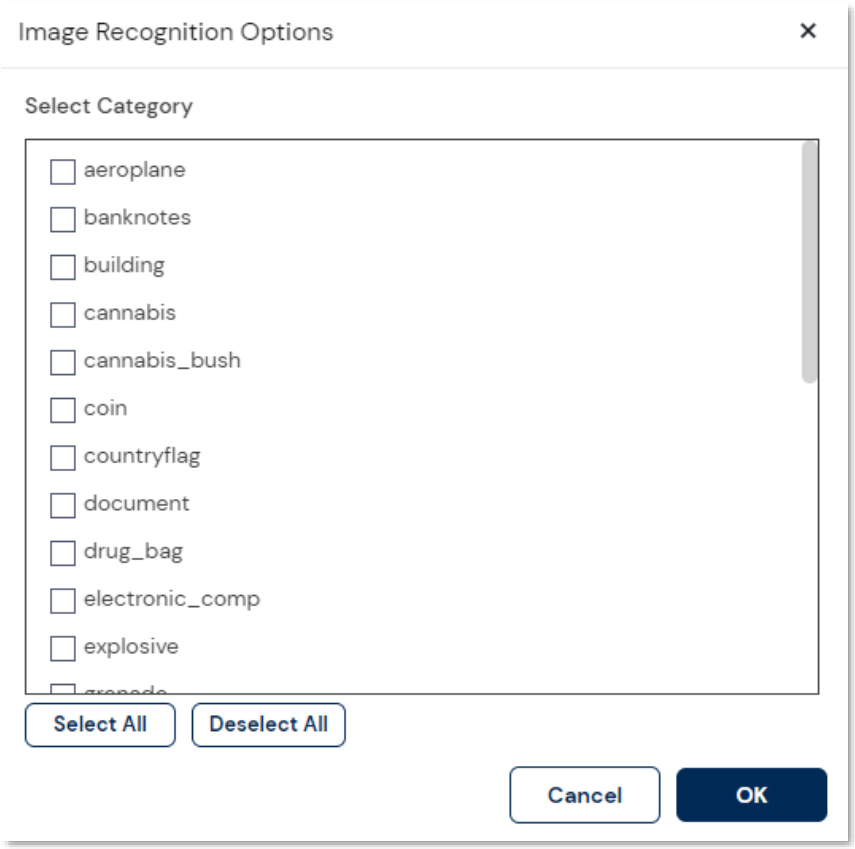


© Exterro, Inc. All rights reserved

Image Recognition

This option allows you to automatically process and categorize the image and video files consisting of certain objects that are potentially relevant to the case.

Upon enabling this option, you can click on ... and select the required image models from the **Image Recognition Options** pop-up.



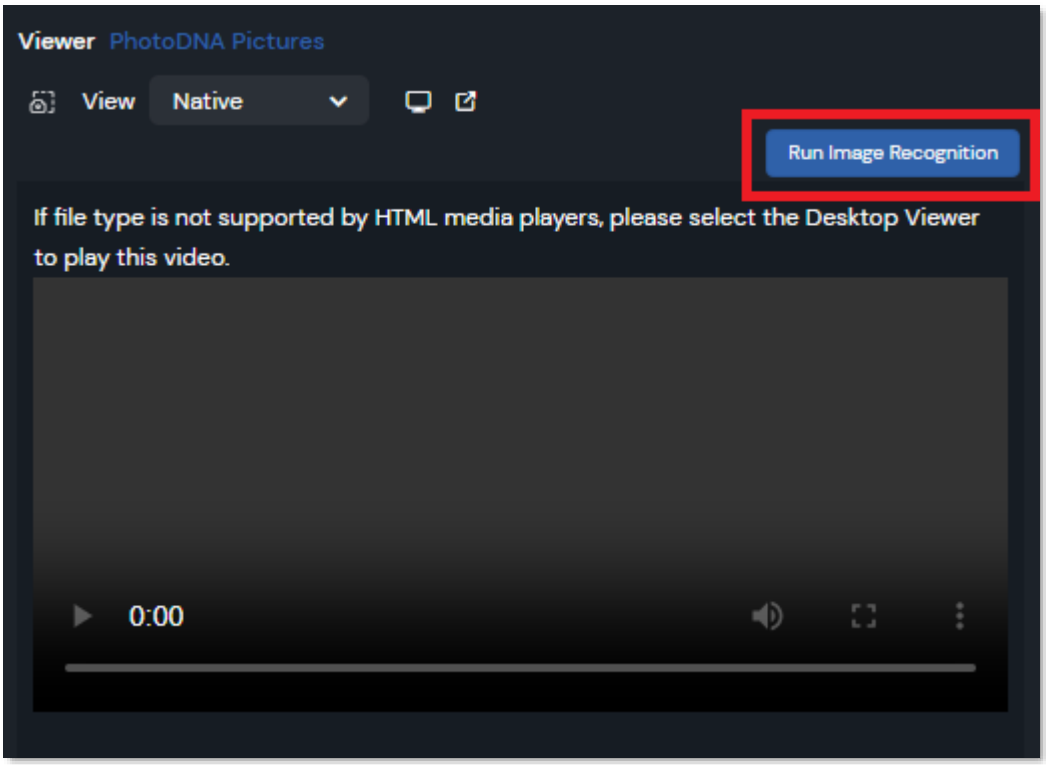
© Exterro, Inc. All rights reserved

Based on the models selected, the application automatically identifies relevant files and labels them based on the below provided image models.

- Aeroplane
- Bank notes
- Building
- Cannabis
- Cannabis Bush
- coin
- Country Flag
- Document
- Drug Bag
- Electronic Component
- Explosive
- Grenade
- ID Cards
- Knife
- Number Plate
- People
- Pill
- Pistol
- Rifle
- Road Sign
- Signature
- Syringe
- Unusual Bong
- Usual Bong
- Vehicle

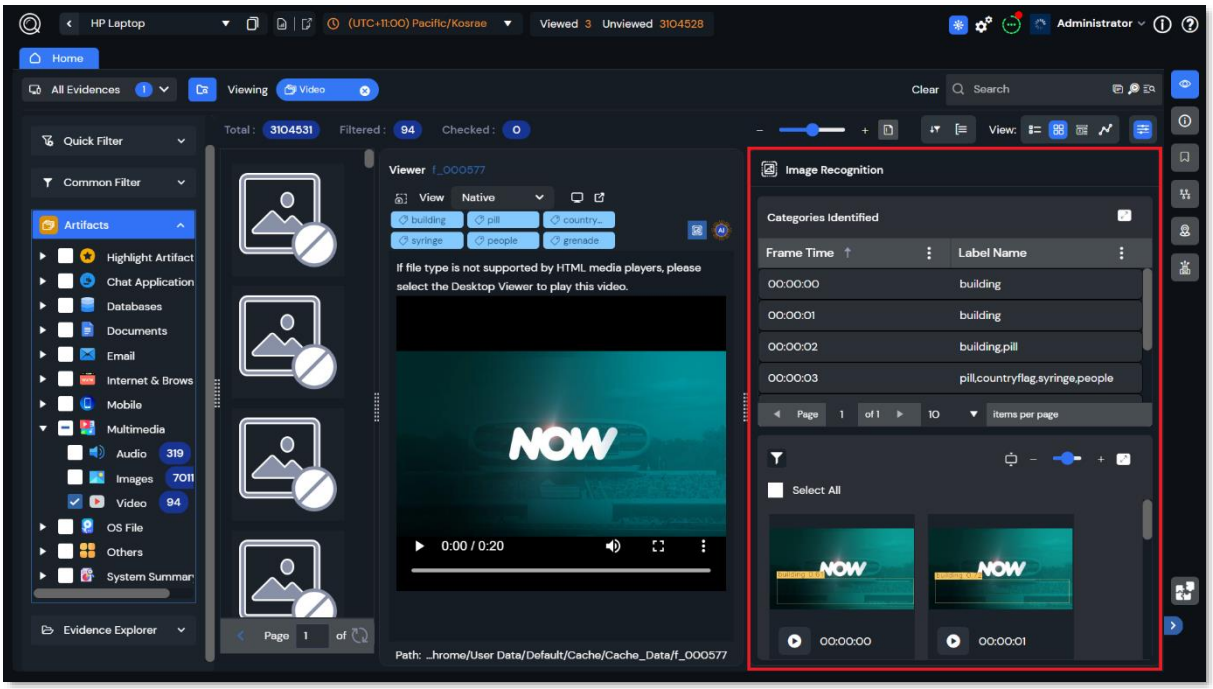
© Exterro, Inc. All rights reserved

For video file types, the **Run Image Recognition** button will be displayed in the viewer. You can click on it to identify and label the images models present in the video.



© Exterro, Inc. All rights reserved

Upon performing the operation, the label will be applied to each frame of the video consisting of the image models. You can view the frame-wise images from the **Image Recognition** pane.



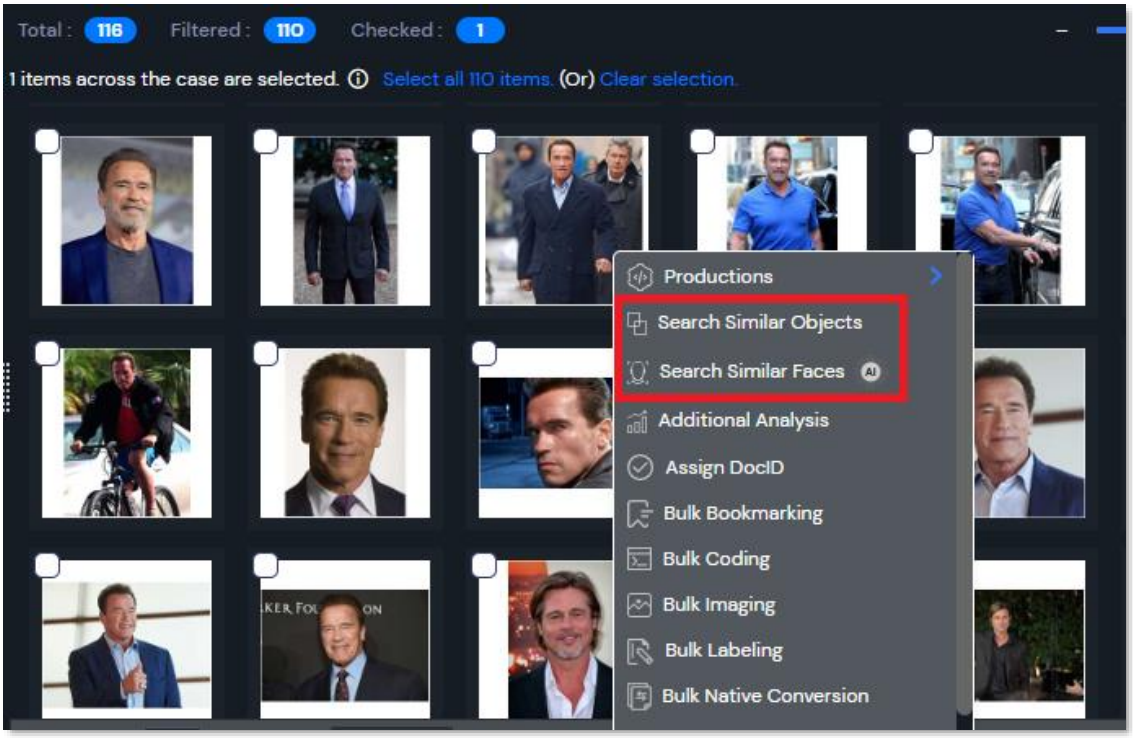
© Exterro, Inc. All rights reserved

Similar Face Detection

Enabling this option will allow the application to search for and identify similar faces/objects that are present in all the image files in the case.

For the cases enabled with this processing option, the following options will be displayed in the right-click menu in the Thumbnail View of Review page:

- Search Similar Objects
- Search Similar Faces

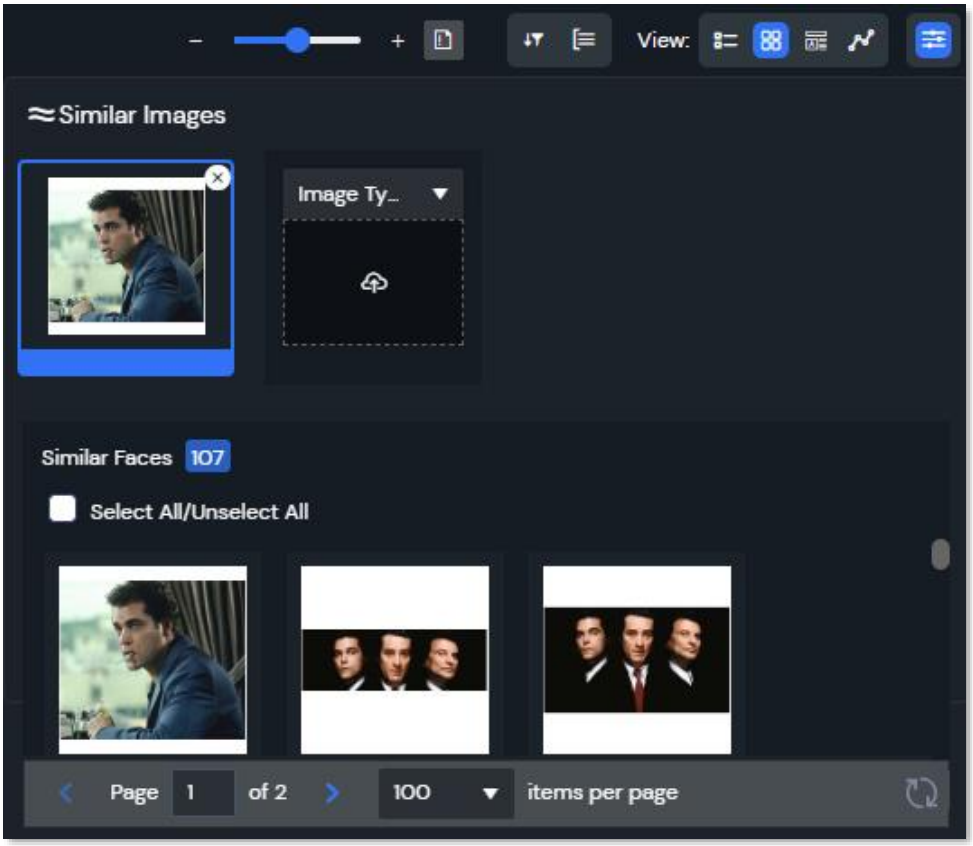


Note: To make use of the 'Search Similar Objects' option, the following conditions should be met:

- You should possess the Law Enforcement license
- The PhotoDNA processing option should be enabled for the case.

© Exterro, Inc. All rights reserved

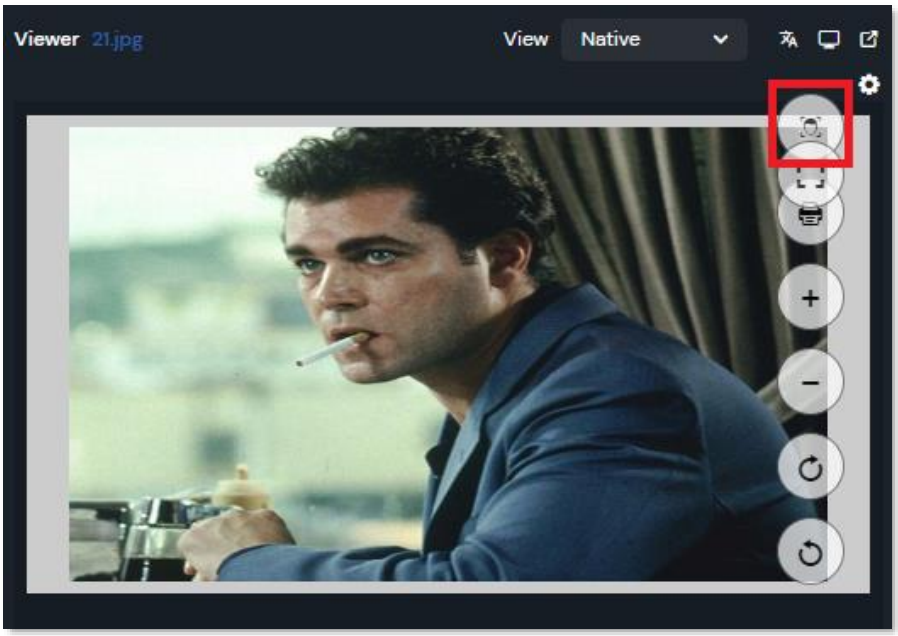
You can select the required option to open the **Similar Images** pane to search and display all the files consisting of similar faces or objects.



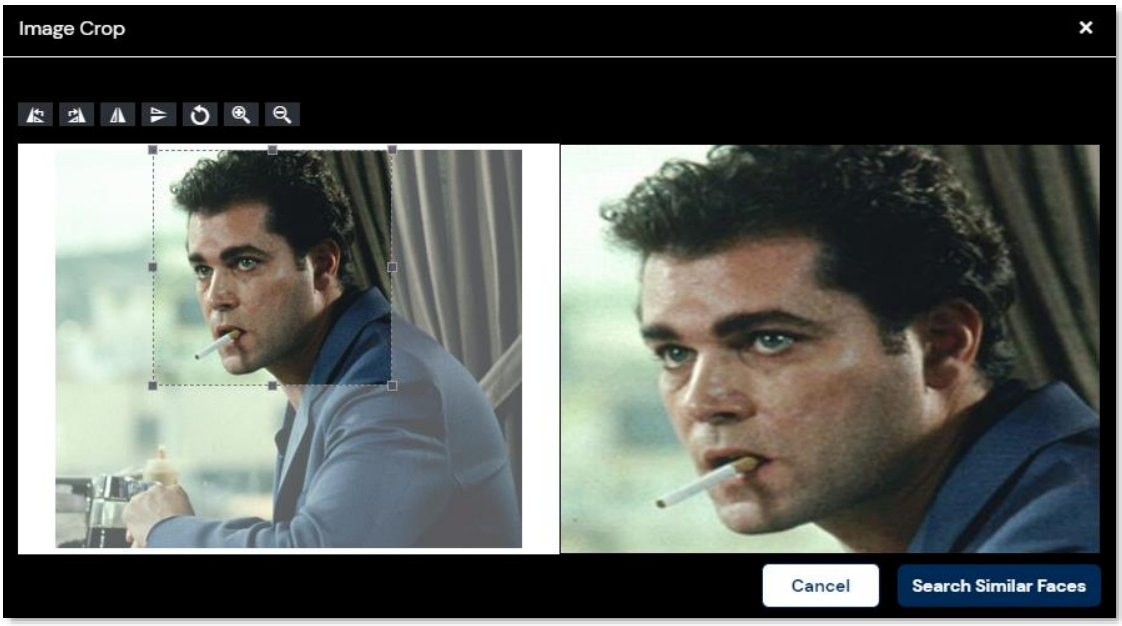
Note: You can click on the button to upload image files from your local system and search for similar faces/objects within the evidence.

© Exterro, Inc. All rights reserved

Moreover, the **Image Crop** icon will be displayed in the viewer of image files in the Review page.



You can click on it and access the **Image Crop** pop-up to crop specific faces and search for similar faces/objects across the evidence.

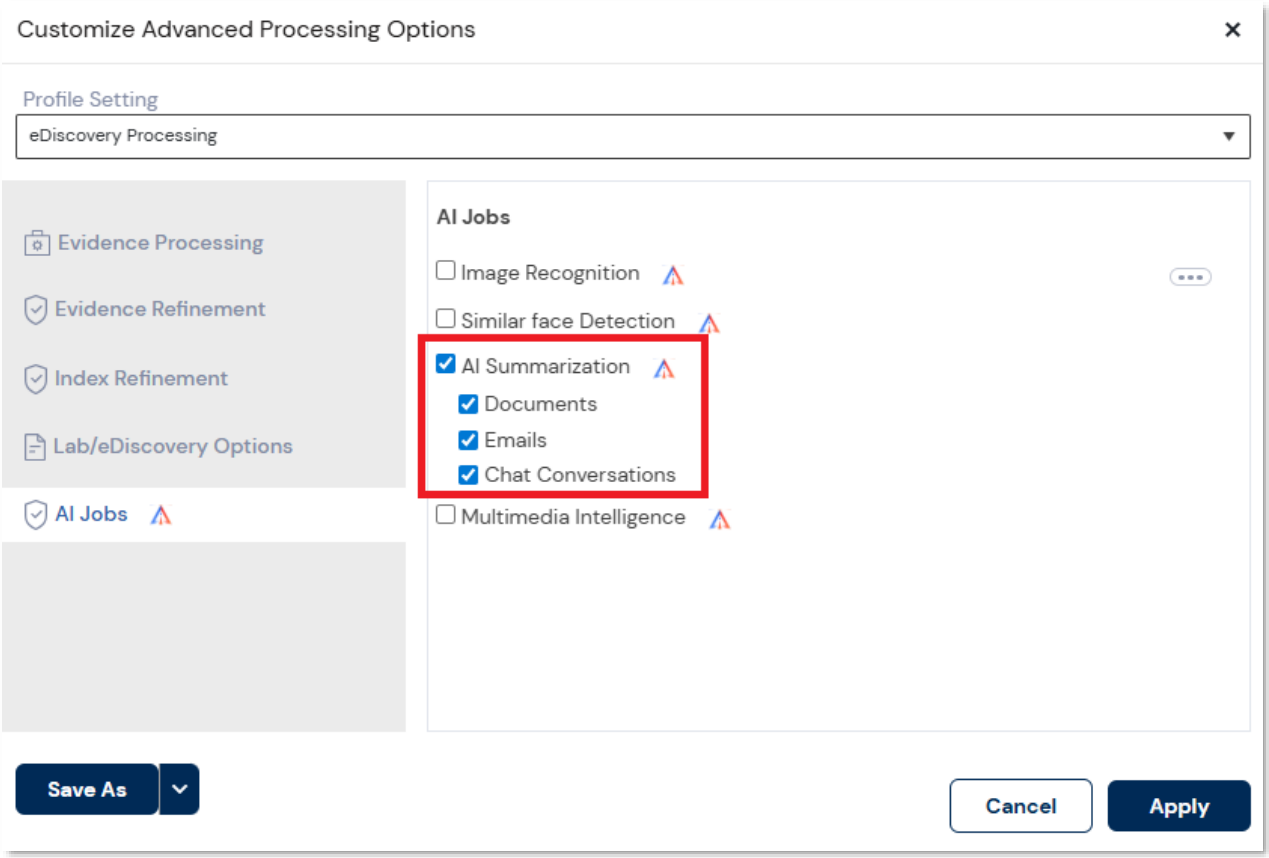


© Exterro, Inc. All rights reserved

AI Summarization

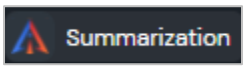
AI Summarization allows you to effectively summarize information from the evidence files and quickly obtain vital details and insights related to your investigation. Enabling this option will automatically generate summaries for all applicable files (Chats, Emails, and Documents) during evidence processing.

Note: You can make the necessary configurations for the summary process from the **Summarization** section of **Exterro Intelligence (AI)** in **System Management**.

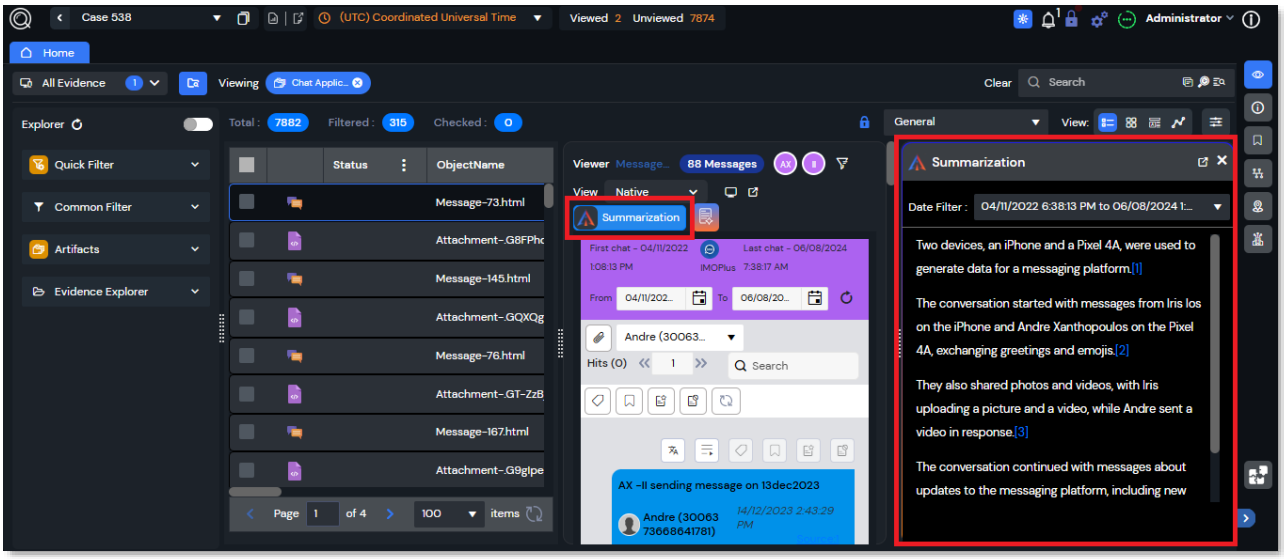


© Exterro, Inc. All rights reserved

Note: At least one of the file types (Documents, Chats, and Emails) should be selected when enabling the **AI Summarization** option to automatically generate summaries. For the other file types, the **Summarization** button will still be displayed, allowing you to click and generate a summary for each file individually.

After completing the evidence processing, you can click on the **Summarization** 

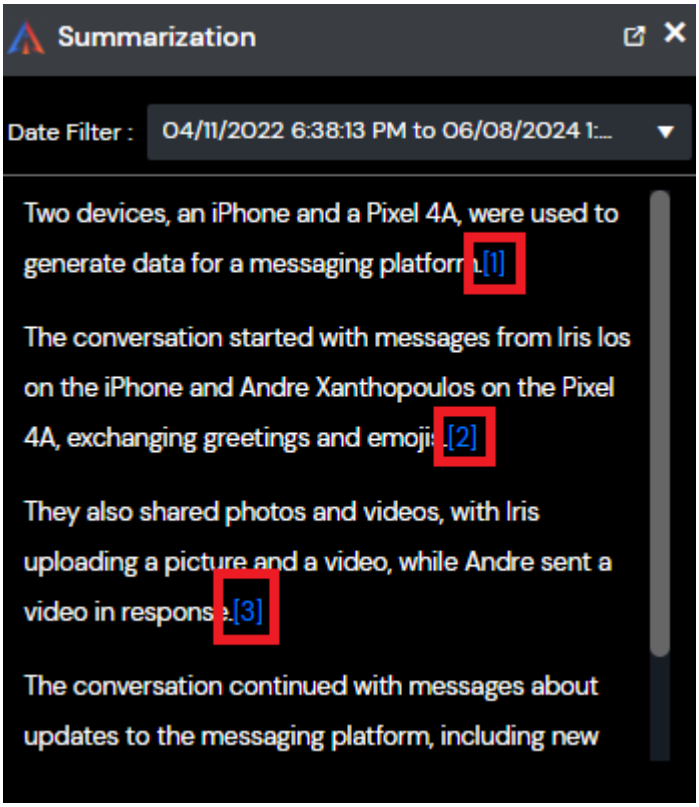
button in the Viewer of the required file to view the summarized information.



Warning: AI Summarization cannot be performed if the information in the files is contextually sparse or contain high levels of noise (Example: HTML tags, repeated line breaks, or irrelevant characters).

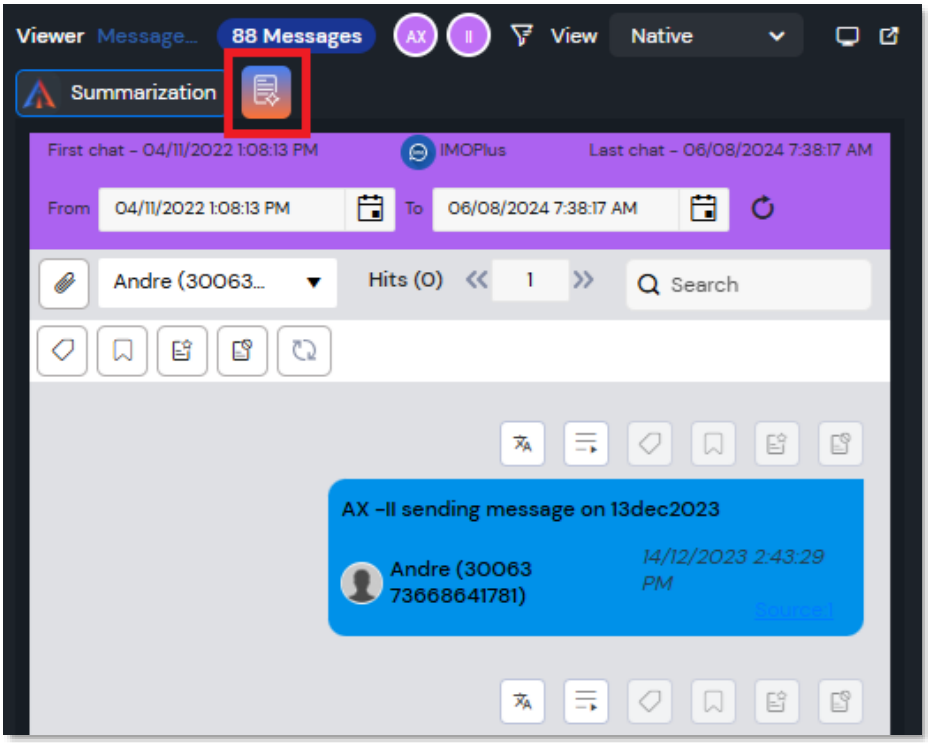
© Exterro, Inc. All rights reserved

Moreover, the summarized content will consist of citations linking to corresponding information in the file. You can hover over it to view the information brief or clicking on it to search and find it in the file (Only for Native Viewer).

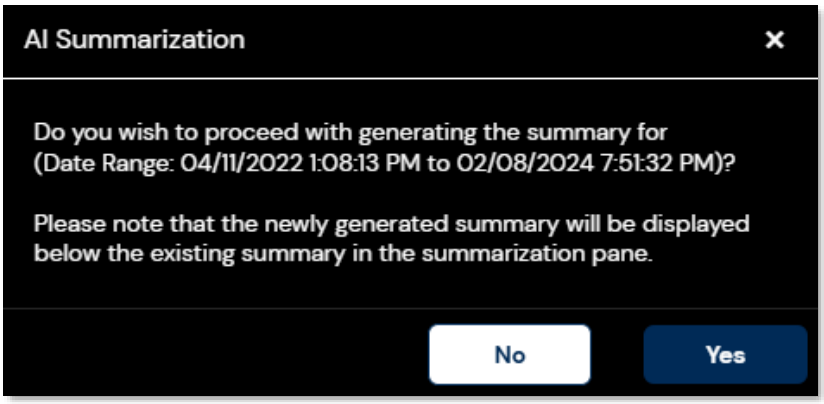


© Exterro, Inc. All rights reserved

For chat conversations, an additional date filter button is displayed to generate summaries for different date ranges.

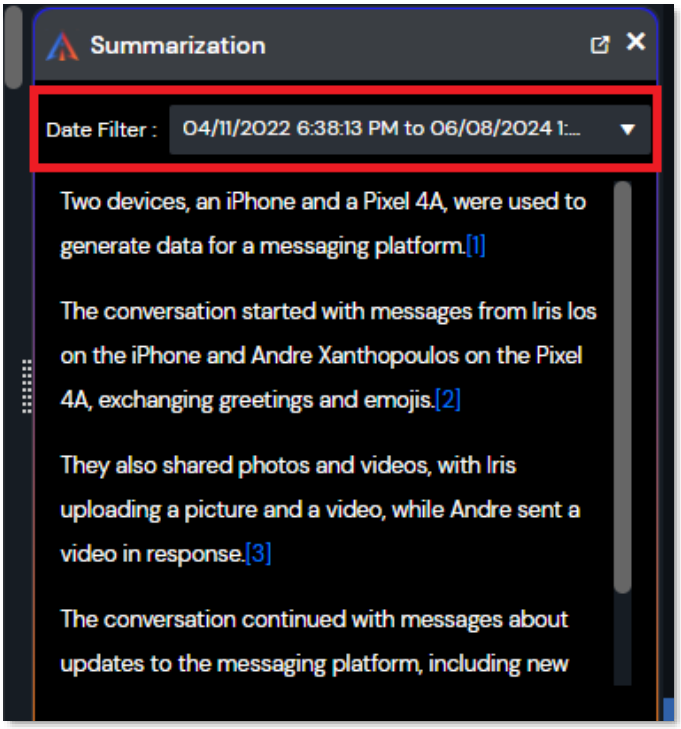


You can configure different date filters in the chat viewer and click on to generate summary containing only the chats within that specific date range.



© Exterro, Inc. All rights reserved

All versions (date ranges) of the summaries will be displayed in the **Summarization** pane, and you can select the required version from the drop-down to view the corresponding details.

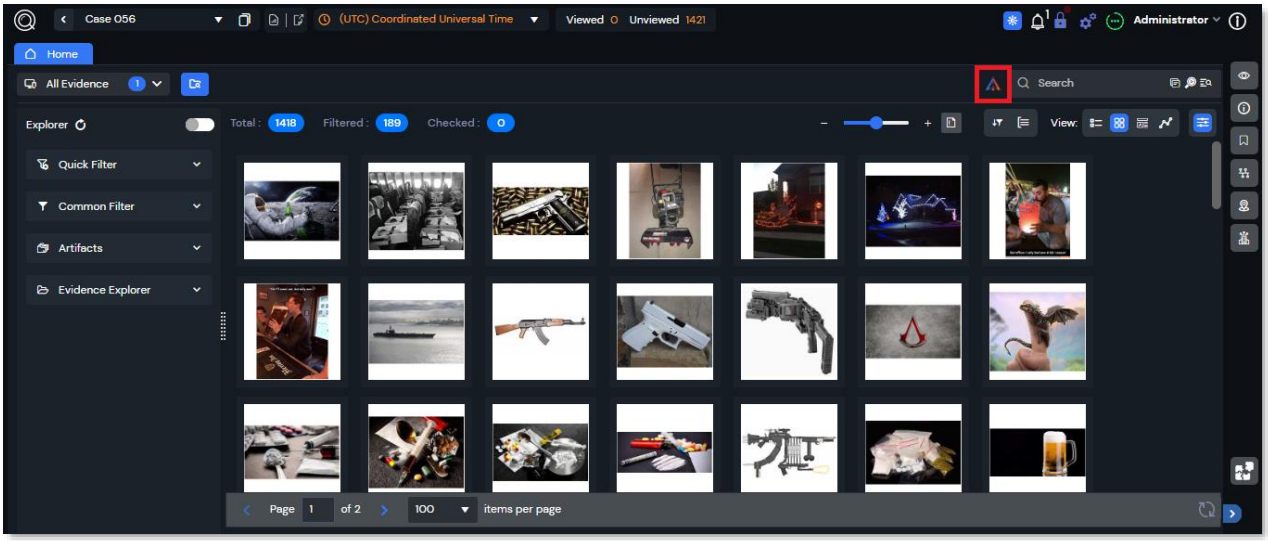


© Exterro, Inc. All rights reserved

Multimedia Intelligence

FTK Central is empowered to recognize and identify objects within static images. This feature allows you to effectively search for specific objects in images, streamlining your review process.

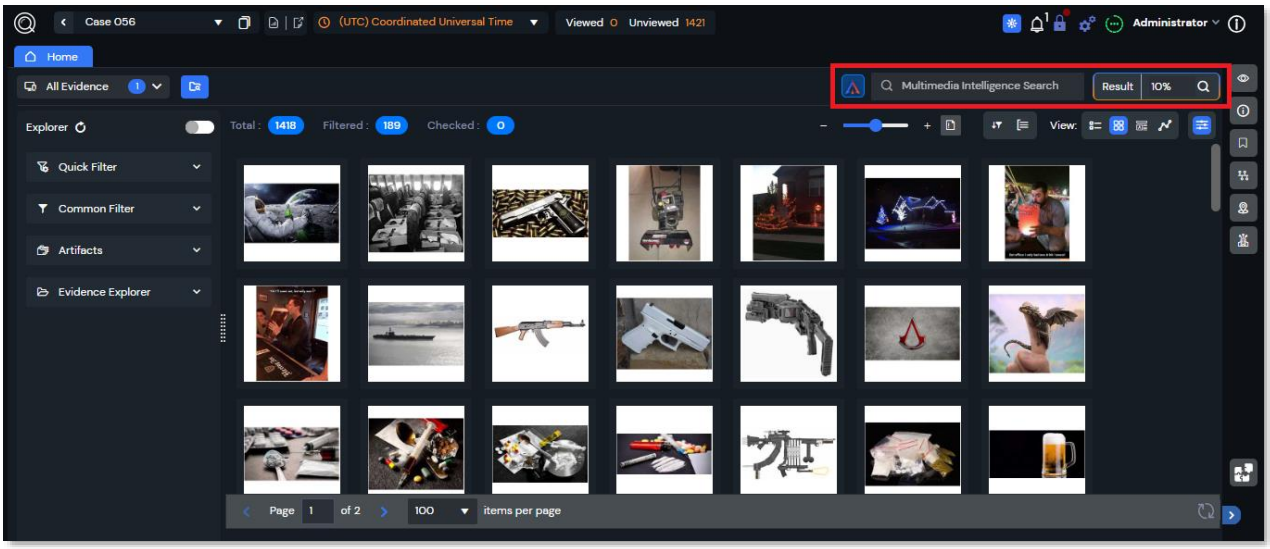
You can enable or disable the multimedia search by clicking on the **Multimedia Intelligence Search** button in the **Thumbnail View.**



Note: The images processed using the Multimedia Intelligence option can be filtered using the **AI Processed Images** (**Common Filters)** of Review page.

© Exterro, Inc. All rights reserved

Enter the keyword related to the desired object in the **Multimedia Intelligence Search** bar and search to find all images containing the object.



© Exterro, Inc. All rights reserved

The percentage configured in the **Results** field will determine whether to display the entire search results or just a fraction of the most relevant results.

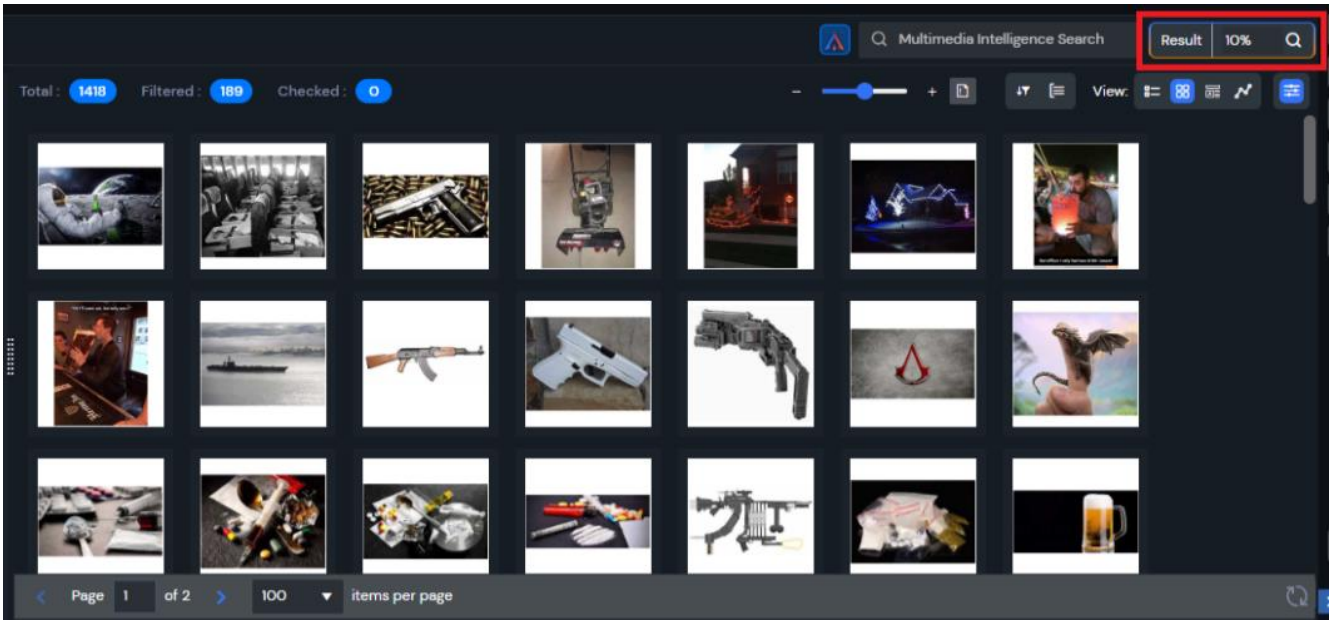
Example:

Results *- 20%*

Search keyword *- Knife*

The total number of images containing knife *– 100*

Results displayed in Thumbnail View *– 20 (with the highest relevancy score)*

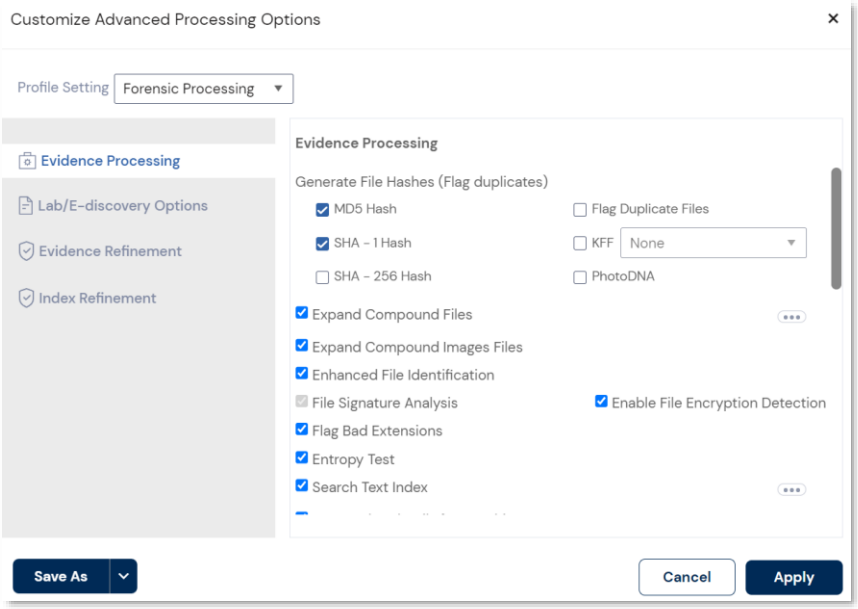


Note: The default value for the **Results** field can be configured in the **Multimedia Search** section of **Exterro Intelligence (AI)** in **System Management**.

© Exterro, Inc. All rights reserved

Creating Custom Processing Profiles

You can create a processing profile by selecting a set of processing options and then saving them as a profile. Processing profiles can only be created during case creation or within the case summary page.



Creating a Custom Processing Profile

To create a custom processing profile:

1. Navigate to a **Case Summary** page.
2. Click **Customize Options**.
3. Select any processing options applicable.
4. Click **Save As**.
5. Enter a **Name** and **Description** (optional) for the custom processing profile.
6. Click **Save**.

Note: Only users assigned with the **Application Administrator** role can edit or delete the custom processing profiles.

© Exterro, Inc. All rights reserved

Known File Filter (KFF)

KFF (Known File Filter) is a utility that compares the file hash values of known files against the files in your case. The known files that you compare against may be the following:

- Files that you want to ignore, such as operating system or application files
- Files that you want to be alerted about, such as malware or other contraband files

The hash values of files, such as MD5, are based on the file's content, not on the file name or extension. This helps you identify files even if they are renamed.

Using KFF during your analysis can provide the following benefits:

- Immediately identify and ignore 40-70% of files irrelevant to the case.
- Immediately identify known contraband files.

Elements of Known File Filter

Introduction to the KFF Architecture	• Introduction to the KFF Architecture
Components of KFF Data	• Components of KFF Data
About the Organization of Hashes, Hash Sets and KFF Groups	• About the Organization of Hashes, Hash Sets and KFF Groups
About Pre-defined KFF Hash Libraries	• About Pre-defined KFF Hash Libraries
NIST NSRL	• NIST NSRL
NDIC HashKeeper	• NDIC HashKeeper
Installing KFF	• Downloading the Latest KFF Installation Files • Determining Where to Install the KFF Server • Installing Cassandra • Cassandra and Firewalls

© Exterro, Inc. All rights reserved

	• Manually Configuring Remote Setting for Cassandra • Configuring a Remote KFF Server • Installing KFF Import Utility
Importing a CSV using the KFF Import Utility	• Importing a CSV using the KFF Import Utility
Verifying a File Using the KFF Import Utility	• Verifying a File Using the KFF Import Utility
Removing Pre-defined KFF Libraries	• Removing Pre-defined KFF Libraries Using the KFF Import Utility
Running KFF Against a Case	• Running KFF Against a Case
Reviewing KFF Results in a Case	• KFF Facet Filters • KFF Columns

Introduction to the KFF Architecture

There are two distinct components of the KFF architecture:

- **KFF Server** - The KFF Server is the component that is used to store and process the KFF data against your evidence. After you install the KFF Server, you import your KFF data into it.
  See KFF Server section.

- **KFF Data** - The KFF data are the hashes of the known files that are compared against the files in your case. The KFF data is organized in KFF Hash Sets and KFF Groups. The KFF data can be comprised of hashes obtained from pre-configured libraries (such as NSRL) or custom hashes that you configure yourself.
  See KFF Data section.

© Exterro, Inc. All rights reserved

Components of KFF Data

Item	Description
Hash	The unique MD5 or SHA-1 hash value of a file. This is the value that is compared between known files and the files in your case.
Hash Set	A collection of hashes that are related somehow. The hash set has an ID, status, name, vendor, package, and version. In most cases, a set corresponds to a collection of hashes from a single source that have the same status.
Group	KFF Groups are containers that are used for managing the Hash Sets that are used in a case. KFF Groups can contains Hash Sets as well as other groups. Cases can only use a single KFF Group. However, when configuring your case, you can select a single KFF Group which can contain nested groups.
Status	The specified status of a hash set of the known files which can be either Ignore or Alert. When a file in a case matches a known file, this is the reported status of the file in the case.
Library	A pre-defined collection of hashes that you can import into the KFF Server. You can use the following pre-defined libraries: • NSRL • NDIC HashKeeper • DHS For law enforcement users, you can also use Project Vic/CAID libraries. See About Pre-defined KFF Hash Libraries section.

© Exterro, Inc. All rights reserved

About the Organization of Hashes, Hash Sets and KFF Groups

Hashes, such as MD5, SHA-1, etc., are based on the file's content, not on the file name or extension.

You can also import hashes into the KFF Server in .csv format.

For FTK-based products, you can also import hashes into the KFF Server that are contained in .tsv, .hke, .hke.txt, .hdi, .hdb, .hash, .nsrl, or .kff file formats.

Hashes are organized into Hash Sets. Hash Sets usually include hashes that have a common status, such as Alert or Ignore.

About Pre-defined KFF Hash Libraries

There are pre-configured hash sets currently available for KFF that come from federal government agencies and are available in KFF libraries.

The following pre-defined libraries are currently available for KFF and come from federal government agencies:

- NIST NSRL (The default library included in the KFF installer package)
- NDIC HashKeeper (An optional library)
- DHS (An optional library)

For law enforcement users, you can also use Project Vic libraries.

Use the following information to help identify the origin of any hash set within the KFF.

- The NSRL hash sets do not begin with "ZZN" or "ZN". In addition, in the AD Lab KFF, all the NSRL hash set names are appended (post-fixed) with multi-digit numeric identifier. For example: "Password Manager & Form Filler 9722."

- All HashKeeper Alert sets begin with "ZZ", and all HashKeeper Ignore sets begin with "Z". (There are a few exceptions. See below.) These prefixes are often followed by numeric characters ("ZZN" or

© Exterro, Inc. All rights reserved

"ZN" where N is any single digit, or group of digits, 0-9), and then the rest of the hash set name. Two examples of HashKeeper Alert sets are:

- "ZZ00001 Suspected child porn"
- "ZZ14W"

  An example of a HashKeeper Ignore set is:

  "Z00048 Corel Draw 6"
- The DHS collection is broken down as follows:
- In 1.81.4 and later there are two sets named "DHS-ICE Child Exploitation JAN-1-08 CSV" and "DHS-ICE Child Exploitation JAN-1-08 HASH".
- In AD Lab there is just one such set, and it is named "DHS-ICE Child Exploitation JAN-1-08".

Once an investigator has identified the vendor from which a hash set has come, he/she may need to consider the vendor's philosophy on collecting and categorizing hash sets, and the methods used by the vendor to gather hash values into sets, in order to determine the relevance of Alert (and Ignore) hits to his/her case. The following descriptions may be useful in assessing hits.

NIST NSRL

The NIST NSRL collection is described at: http://www.nsrl.nist.gov/index.html. This collection is much larger than HashKeeper in terms of the number of sets and the total number of hashes. It is composed entirely of hash sets being generated from application software. So, all of its hash sets are given Ignore status by Exterro staff except for those whose names make them sound as though they could be used for illicit purposes.

The NSRL collection divides itself into many sub-collections of hash sets with similar names. In addition, many of these hash sets are "empty", that is, they are not accompanied by any hash values. The size of the NSRL collection, combined with the similarity in set naming and the problem of empty sets, allows Exterro to modify (or selectively alter) NSRL's own set names to remove ambiguity and redundancy.

© Exterro, Inc. All rights reserved

NDIC HashKeeper

NDIC's HashKeeper collection uses the Alert/Ignore designation. The Alert sets are hash values contributed by law enforcement agents working in various jurisdictions within the US - and a few that apparently come from Luxemburg. All of the Alert sets were contributed because they were believed by the contributor to be connected to child pornography. The Ignore sets within HashKeeper are computed from files belonging to application software.

During the creation of KFF, Exterro staff retains the Alert and Ignore designations given by the NDIC, with the following exceptions. Exterro labels the following sets Alert even though HashKeeper had assigned them as Ignore: "Z00045 PGP files", "Z00046 Steganos", "Z00065 Cyber Lock", "Z00136 PGP Shareware", "Z00186 Misc Steganography Programs", "Z00188 Wiping Programs". The names of these sets may suggest the intent to conceal data on the part of the suspect, and Exterro marks them Alert with the assumption that investigators would want to be "alerted" to the presence of data obfuscation or elimination software that had been installed by the suspect.

Note: The basic rule is to always consider the source when using KFF in your investigations. You should consider the origin of the hash set to which the hit belongs. In addition, you should consider the underlying nature of hash values in order to evaluate a hit's authenticity.

© Exterro, Inc. All rights reserved

Bloom Filter

The Bloom filter efficiently identifies known system files, reducing processing overhead and boosting performance, especially in large datasets.

Bloom filter is configured based on the Computer Incident Response Center Luxembourg (CIRCL) hash sets for Identifying the Known System Files from the evidence more quickly and efficiently.

Bloom filter comprises 298M hash values (700 MB) referenced from the following software repositories:

- Common System files of Windows 10 and Windows 11 versions (in French, Dutch, German, English (United States, United Kingdom) languages)
- National Institute of Standards and Technology (NIST) National Software Reference Library (NSRL) (Hash Library) - All RDS hash sets including current, modern, Android, iOS and legacy + SHA256 mapping
- Ubuntu packages distribution
- CentOS core OS distribution
- Fedora project Extra Packages for Enterprise Linux (EPEL) repository
- Kali Linux packages distribution
- OpenSUSE distribution packages
- OpenBSD binary tar.gz distribution
- CDNJS
- Snap public repository

© Exterro, Inc. All rights reserved

Warning: While Bloom filters can tell you with certainty that an element is not in the set, it can only tell you with a certain probability that an element is in the set. So, Exterro advises you to verify the files suggested by the Bloom filter to ensure accuracy.

Notes:

- The KFF Server setup is not necessary to use this feature since it is built-in as part of the FTK Processing engine.
- It is mandatory to calculate the SHA1 Hash before proceeding with configuring the Bloom Filter.

© Exterro, Inc. All rights reserved

Installing KFF

Downloading the Latest KFF Installation Files

You can download the latest KFF installation files and guides from https://Exterro.com/product-download.

Determining Where to Install the KFF Server

Where you install the KFF Server depends on the application and environment you are running.

- For AD Lab, Enterprise and FTK Central applications, the KFF Server is generally installed on a different computer than that runs the main application.
- For large environments, it is recommended that the KFF Server be installed on a dedicated computer.

© Exterro, Inc. All rights reserved

Installing Cassandra

To install Cassandra:

1. If required, install 64-bit Java 8.
2. Navigate to **AccessData_Casandra_Installer.exe**.
3. Run **AccessData_Cassandra_Installer.exe as an administrator**.
4. If required, install Python 2.7.
5. On the Welcome page, click **Next**.
6. Review and accept the license terms and click **Next**.
7. Verify or change the **Destination Folder** and click **Next**.
8. If needed, configure **Remote Access**.
   i. Select **Enable Remote Access**.
   ii. In the **RPC_Address** field, enter the IP address of the computer you are installing on. For example, 10.10.10.10.
   iii. In the Native Transport Port Number field, leave the default 9042.
   iv. Click **Next**.
9. If you enabled Remote Access, set the User Credentials for the service and click **Next**.
10. Click **Install**.
11. Click **Finish**.

© Exterro, Inc. All rights reserved

Cassandra and Firewalls

During the installation, if you check the box to Enable Remote Access, the installer creates an inbound exception rule for the port entered in the Cassandra installer (if the rule has not already been created).

The rule has the following attributes:

- name = AccessData Cassandra Remote Access Port
- direction = in
- program = "<install directory>\Cassandra\bin\daemon\prunsrv.exe"
- local port = 9042 (or whatever the user entered)
- protocol = tcp

If you uninstall Cassandra, the installer checks to see if Enable Remote Access was checked during install, and if it was, the installer looks for the above firewall rule using the 5 listed attributes, and if it finds the rule, it removes it from the firewall.

Manually Configuring Remote Setting for Cassandra

In some situations, Cassandra needs to be configured to enable Remote Access.

During the installation of Cassandra there is the option to Enable Remote Access and then set the RPC_Address (the IP address of the computer that Cassandra is installed on).

If you set these settings correctly during the installation, no further configuration is needed.

However, if you did not enable remote access or make a change, you can manually configure the remote settings for Cassandra.

Note: Use an editor that supports YAML files.

© Exterro, Inc. All rights reserved

To manually configure remote setting for Cassandra:

1. Go to the location that you installed Cassandra.
2. By default, it is "<Drive>**:\Program Files\ AccessData\Cassandra**".
3. Open the **conf** folder.
4. Edit the **cassandra.yaml** file.
5. Search for **rpc_address**:
6. Change the address from local host to the IP or DNS name of the computer running Cassandra.

   For example, change rpc_address: localhost to rpc_address: 10.10.10.10
7. Search for **native_transport_port**:
8. Verify that the setting is: **native_transport_port: 9042** (**or the port you are using**)
9. **Save** and exit the file.
10. **Restart** the **AccessData Cassandra service**.

Configuring a Remote KFF Server

To configure a remote KFF Server:

1. Navigate to the FTK-Central bin folder (typically "<Drive>:\Program Files\ AccessData\Forensic Tools\<version>\bin\").
2. From the bin folder, open **ADG.WeblabSelfHost.exe.config** in a text editor.
3. Find the line **<add key="KFFServerUrl" value="localhost:9042" />.**

   9042 is the default port for Cassandra.
4. If needed, change **localhost** to be the **location IP address** of your KFF server.

   For example, value="10.10.10.10:9042"
5. **Save** and close the file.
6. **Restart** the **Exterro Self Host Service**.

© Exterro, Inc. All rights reserved

Installing KFF Import Utility

To install KFF import utility:

1. Navigate to **KFF_Import_Utility.exe**.
2. Run **KFF_Import_Utility.exe as an administrator**.
3. Click **Next**.
4. Review and accept the license terms and click **Next**.
5. Verify or change the **Destination Folder** and click **Next**.
6. Click **Install**.
7. Click **Finish**.

Importing a CSV using the KFF Import Utility

You can import Hash Sets and KFF Groups by importing a custom CSV file.

To import a CSV using KFF import utility:

1. Open the **KFF Import Utility**.
2. Click the **Browse** button and locate the CSV that you want to import.
3. Click **Open**.
4. Enter package, vendor, version, etc.
5. If you installed Cassandra enabling Remote Access, in the Server address field, you must enter the computer's IP that has Cassandra installed on it, even if it is on the same computer as the import utility. Otherwise, leave it as localhost.
6. Click **Import**.
7. When complete, click **OK**.

© Exterro, Inc. All rights reserved

Verifying a File Using the KFF Import Utility

You can verify Hash Sets and KFF Groups to ensure the correct file is being imported.

To verify a file using KFF import utility:

1. Open the **KFF Import Utility**.
2. Click the **Browse** button and locate the file that you want to import.
3. Enter set name, package, vendor, version, and set status.
4. If you installed Cassandra enabling Remote Access, in the Server address field, you must enter the computer's IP that has Cassandra installed on it, even if it is on the same computer as the import utility. Otherwise, leave it as localhost.
5. Click **Verify**.
6. When complete, the Success window will appear, showing the following details:
7. Group Count, Set Count, Hash Count, Photo DNA Count
8. If you would like to open the log for further examination of the data, select **Yes**. If not, select **No** and the window will close.

Removing Pre-defined KFF Libraries Using the KFF Import Utility

You can remove a pre-defined KFF Library that you have previously imported. You cannot see or remove existing custom KFF data (your own CSVs or manually entered data).

To remove pre-defined KFF libraries using KFF import utility:

1. On the **KFF Server**, open the **KFF Import Utility**.
2. Select the **library** that you want to remove.
3. Click **Remove**.

© Exterro, Inc. All rights reserved

Using the KFF Utility in FTK Central

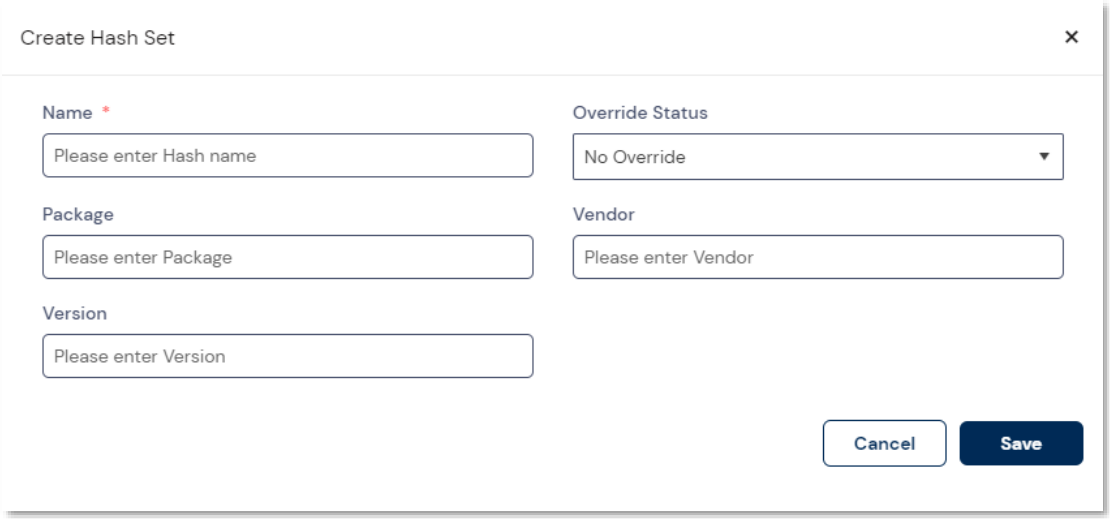
You can use the KFF Utility in FTK Central to create and import hash sets as well as create groups. The functionality from the stand-alone KFF utility has been carried over.

Warning: Apache Cassandra must be installed and configured for this feature to work.

Creating a Hash Set

To create a hash set:

1. From the home page, click on the **Settings** button from the top-right corner.
2. Navigate to the **System Management** tab.
3. Select the **Hash Sets** section.
4. Click **Create Hash Set**.
   - The **Create Hash Set** prompt is displayed.



5. Enter a **Name**.

© Exterro, Inc. All rights reserved

6. Enter any one of the following **Override Status**.
   - **No Override**
   - **Ignore**
   - **Alert**
7. Enter a **Package** name.
8. Enter a **Vendor** name.
9. Enter a **Version**.
10. Click **Save**.

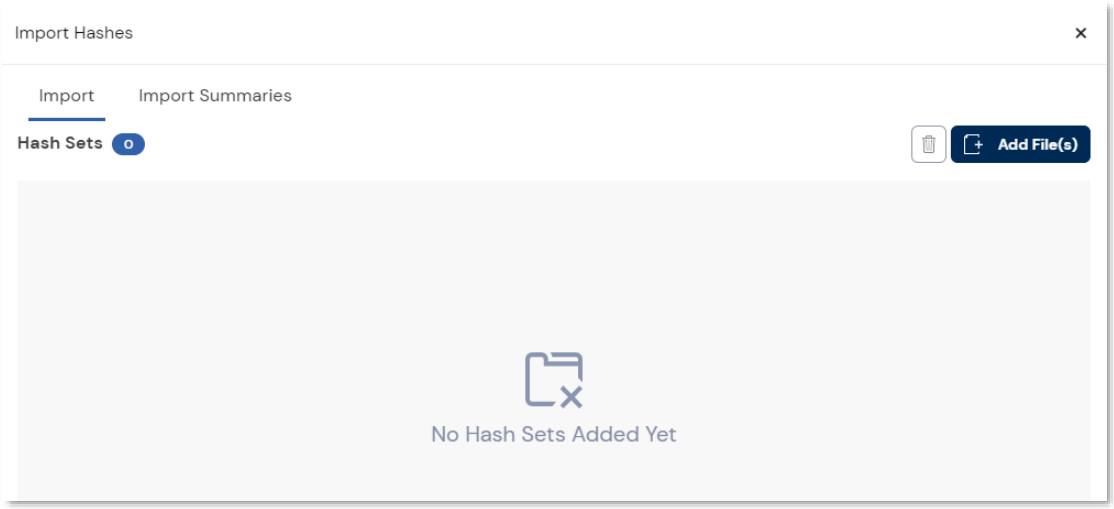
Note: From the **Hash Sets** section, you can click on the **Edit** or **Delete** button to edit or delete hash sets respectively.

© Exterro, Inc. All rights reserved

Importing a Hash Set

To import a hash set:

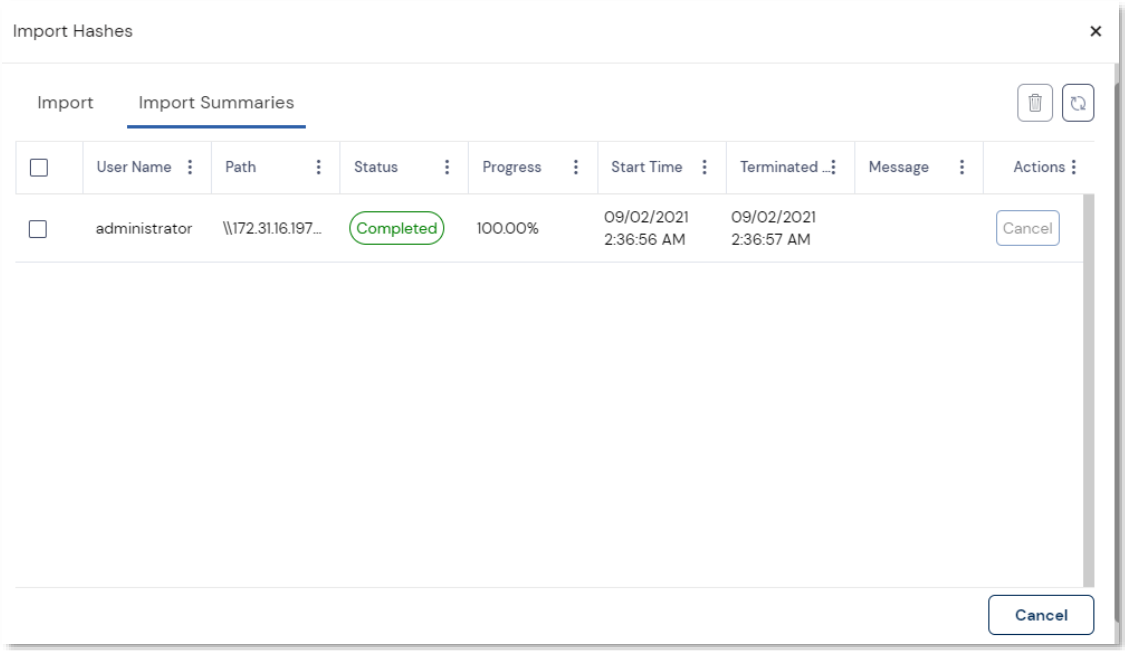
1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Hash Sets**.
4. Click **Import Hashes**.
    - The **Import Hashes** prompt is displayed.



5. Click **Add File(s)**.
6. Enter the location path in the **Server** field.
7. Select the required hash file to be imported.
8. Select anyone of the below **Default Status**:
    - **Alert**
    - **Ignore**
9. Click **Import Data**.

© Exterro, Inc. All rights reserved

- The **Import Summaries** page will be displayed.



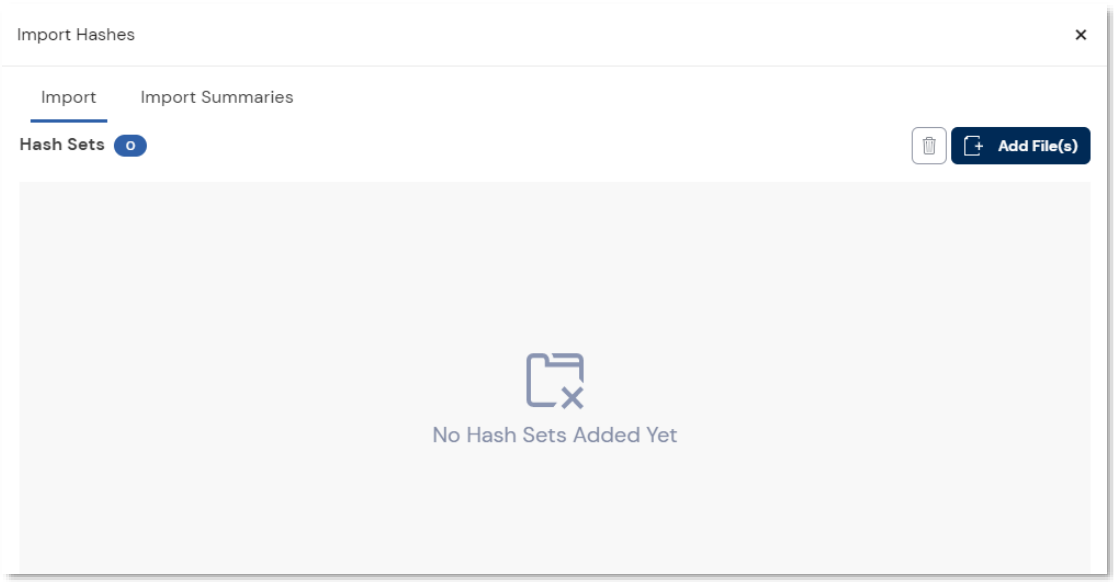
The progress of the import operation will be displayed.

© Exterro, Inc. All rights reserved

Importing a Hash Set from Review Mode

To import a hash set from Review mode:

1. From the Grid, select the records.
2. Right-click on a selected record.
3. Select **Export**.
4. Select any one of the following options:
   - **Checked** – This will export the file in native format.
   - **All to CSV** – This will create a list of files with general metadata information.
5. Click **OK**.
6. From the home page, click **Settings** from the top-right corner.
7. Navigate to the **System Management** tab.
8. Click **Hash Sets**.
9. Click **Import Hashes**.
   - The **Import Hashes** prompt is displayed.



© Exterro, Inc. All rights reserved

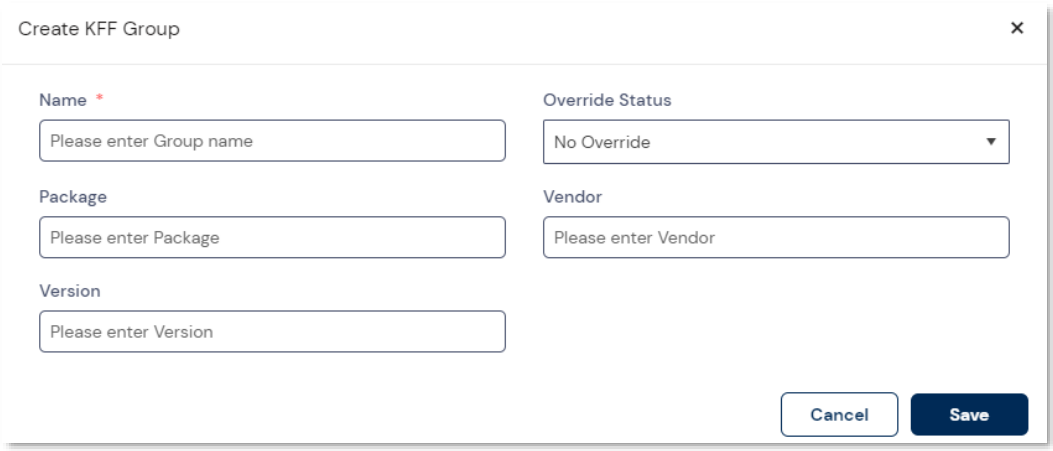
10. Click **Add File(s)**.
11. Enter the location path in the **Server** field.
12. Select the required hash file to be imported.
13. Select anyone of the below **Default Status**:
    - **Alert**
    - **Ignore**
14. Click **Import Data**.

© Exterro, Inc. All rights reserved

Creating a KFF Group

To create a KFF group:

1. From the home page, click **Settings** button from the top-right corner.
2. Navigate to the **System Management** tab.
3. Select the **KFF Groups** section.
4. Click **Create KFF Group**.
   - The **Create KFF Group** prompt is displayed.



5. Enter a **Name**.
6. Select any one of the below provided **Override Status**:
   - **No Override**
   - **Ignore**
   - **Alert**
7. Enter a **Package** name.
8. Enter a **Vendor** name.
9. Enter a **Version**.
10. Click **Save**.

Note: From the **KFF Groups** section, you can click on the **Edit** or **Delete** button to edit or delete KFF groups respectively.

© Exterro, Inc. All rights reserved

Associating Hash Sets to KFF Group

To associate hash sets to KFF group:

1. From the home page, click **Settings** button from the top-right corner.
2. Navigate to the **System Management** tab.
3. Select the **KFF Groups** section.
4. Click on the **+** button against the required KFF group to which the hash set should be associated.
5. Check a specific **Hash Set**.
6. Click **Associate**.

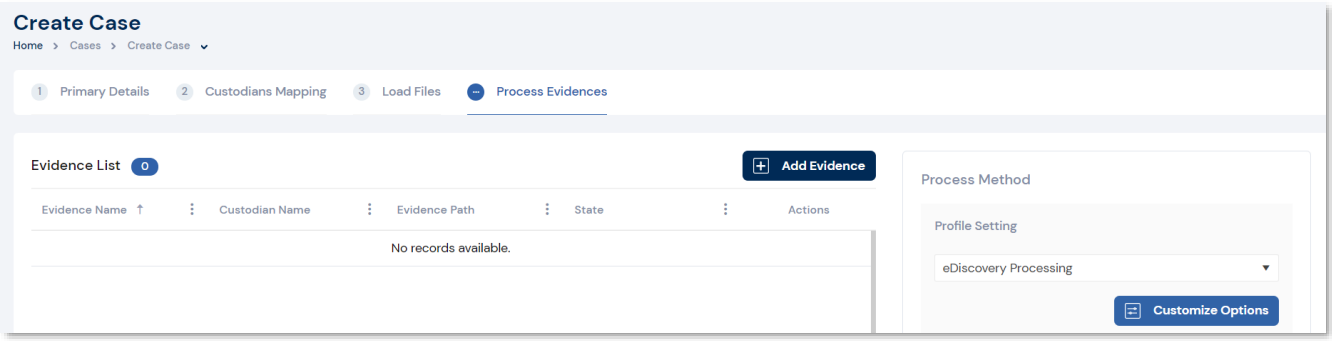
The hash set will now be associated with the selected KFF group.

© Exterro, Inc. All rights reserved

Running KFF Against a Case

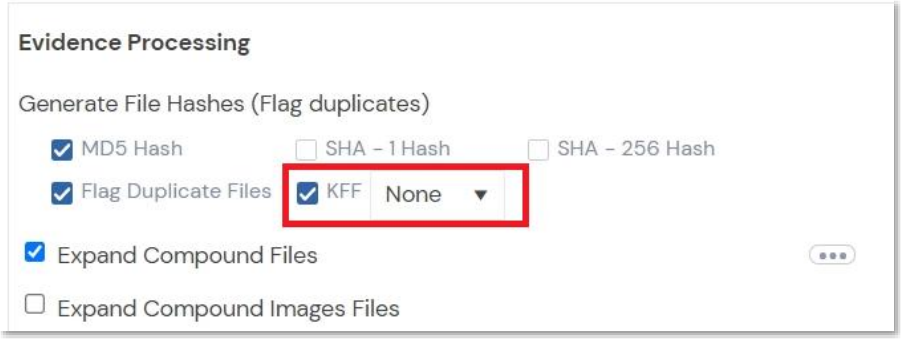
To run KFF import utility:

1. From the Process Evidence page of case creation, click **Customize Options**.



Note: Alternatively, during review, select the desired items, right-click > **Additional Analysis** > **Customize Options**.

2. Select **Document Content Analysis**.
3. Select **KFF**.
4. Click the **drop-down** list.



5. Select a template to use.
6. Click **Apply**.
7. Click **Process Data** or **Run Analysis**.

© Exterro, Inc. All rights reserved

Reviewing KFF Results in a Case

KFF results are displayed in Review.

You can use the following tools to see KFF results:

- KFF Columns. See Using Quick Columns section.
- KFF Facet Filters See Using Facet Filters section.

KFF Facet Filters

You can use the following KFF facets:

- KFF Vendors
- KFF Groups
- KFF Statuses
- KFF Sets

Within a facet, only the filters that are available in the cases are available. For example, if no files with the Alert status are in the case, the Alert filter will not be available in the KFF Status facet.

To apply KFF facets:

1. In the Grid, open the **Filter Facets**.
2. Expand **KFF**.
3. Select your chosen facets.

© Exterro, Inc. All rights reserved

KFF Columns

You can use KFF Quick Columns and sort on KFF values. For example, you can sort on the KFFStatus column to quickly see all the files with the Alert status.

1. From the Review, click the **Quick Column** menu.
2. Select **KFF**.
3. The following columns will appear:
   - **KFF Status**
   - **KFF GroupName**
   - **KFFSet**

Column	Description
KFF Status	Displays the status of the file as it pertains to KFF. The three options are Unknown (0), Ignore (1), and Alert (2). • If you configured the case to skip Ignorable files, these files are not included in the data. • If you configured the case to flag ignorable files, and the Hide Ignorable Quick Filter is activated, these files are in the data but are not displayed.
KFF GroupName	Displays the name created for the KFF Group in the case.
KFFSet	Displays the KFF Hash Set to which the file belongs.

© Exterro, Inc. All rights reserved

Processing iWork Files for Review

To image iWork files:

1. Open a case with iWork files.
2. Select an iWork file.
3. Select the **Annotate** viewer to begin PDF conversion.

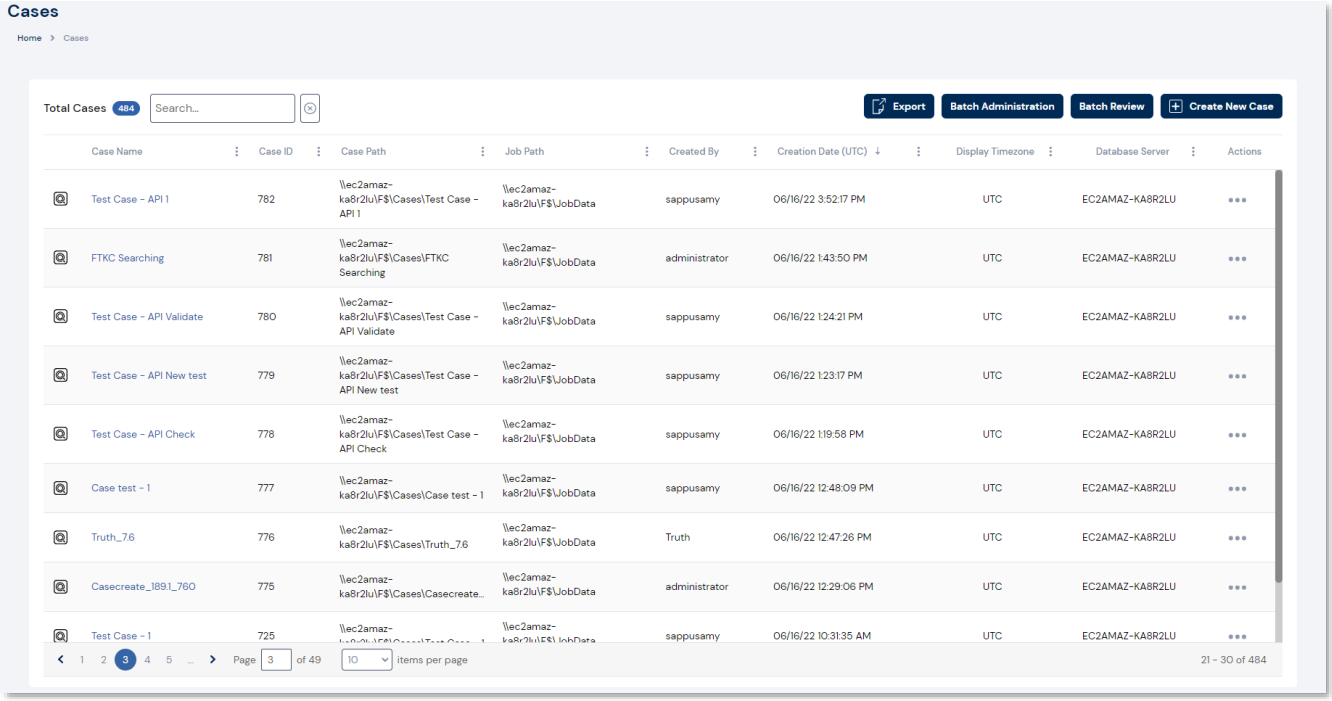
Note: Alternatively, use bulk imaging to efficiently process multiple iWork files. See Bulk Imaging.

4. This will run in the background and store results in the case folder.
5. Once a file is converted, it will be displayed in the viewer.

© Exterro, Inc. All rights reserved

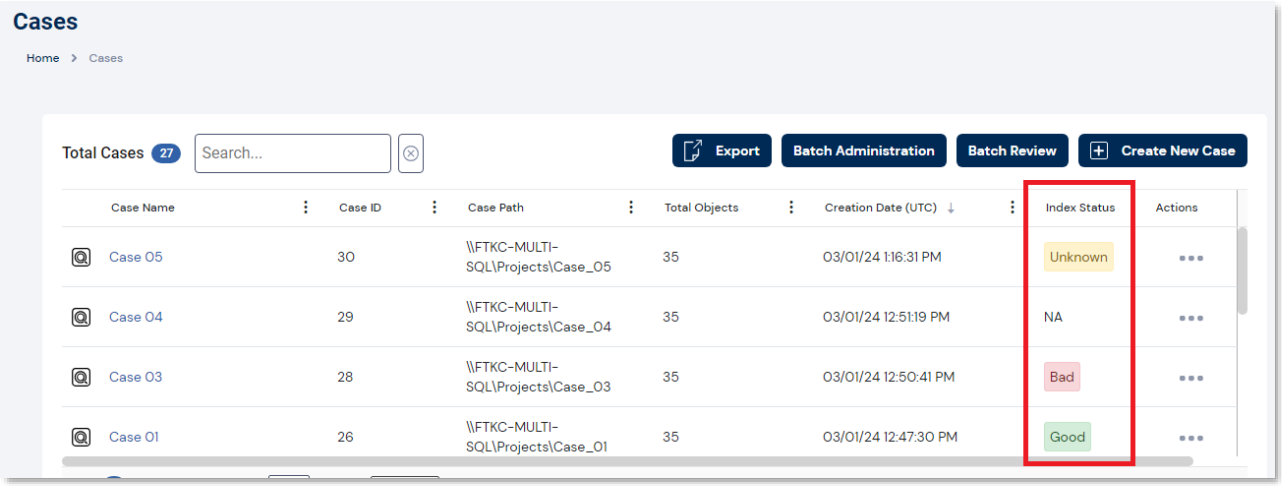
Managing Cases

The Manage cases page provides the list of cases available in the application. This page allows you to access the review portal, view case dashboards, manage load files, custodians, evidence, process data and coding panels associated with a case.



© Exterro, Inc. All rights reserved

You can also check index status of all the cases in the application from the **Index Status** column in this page.



Status	Description
Good	When the case index has yet to be checked.
Bad	When the evidence in the case is processed with a valid search index.
Unknown	When any of the files like (DTX file) are missing in the dts_idx folder. This can be found in the case path after evidence has been processed.
N/A	When the evidence in the case isn't processed with a search index or the dts_idx folder is not generated in the case path.

© Exterro, Inc. All rights reserved

Elements of Managing Cases

Viewing Details about a Case	• Viewing Details about a Case
Opening a Case	• Opening a Case via Case Dashboard • Opening a Case via Case List • Case List Options • Case Dashboard
Case Summary	• Managing Load Files • Managing Custodians • Managing Evidence • Managing Process Data
Coding Panels	• Creating Coding Panel • Reorganizing a Coding Panel • Deleting Coding Panels
Batches	• Batches
Batch Administration Panel	• Viewing Review Set Details • Dashboard: Viewing Case Coding Summary
Creating Review Sets	• Creating Review Sets
Editing Review Sets	• Editing Review Sets
Deleting Review Sets	• Deleting Review Sets
Batch Review Panel	• Checking In/Out a Review Set • Reviewing a Review Set

© Exterro, Inc. All rights reserved

Viewing Details about a Case

You can view the following details about the case within the Case Dashboard:

- Case Overview
- Processing Jobs
- Case Evidence
- Bookmarks and Labels
- File Categories
- Cities (Location)
- Message Applications
- Languages

See Case Dashboard section.

You can view the following details (and edit them) about the case within the Case Summary:

- Case Details
- Evidence List
- Custodians
- Processing Options

See Case Summary section.

© Exterro, Inc. All rights reserved

Opening a Case

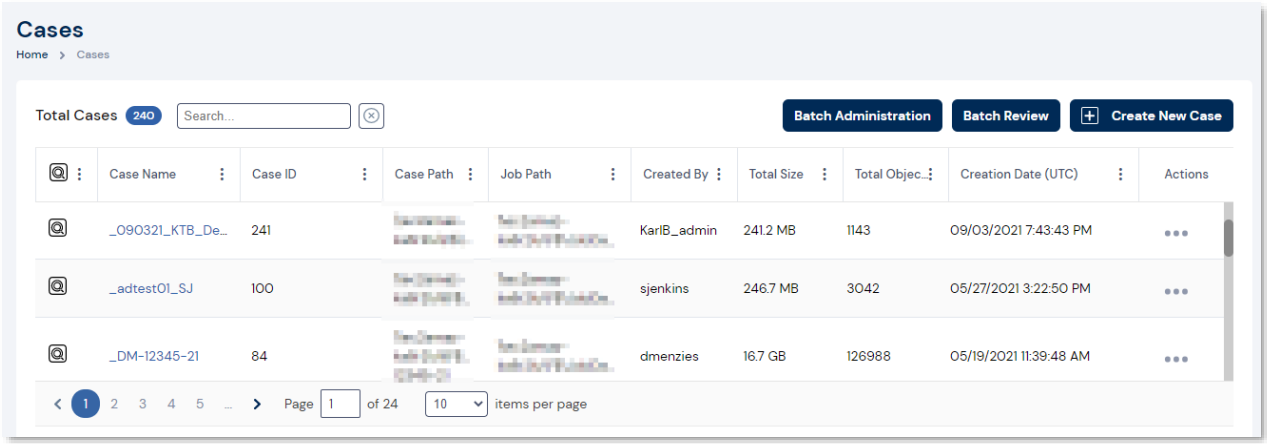
Opening a Case via Case Dashboard

Tip: To filter the grid efficiently, you can simply enter a keyword into the search box

located at the top of any grid and click the search button or press enter.

To open a case via case dashboard:

1. From the home page, click **Case List**.



2. Click on a **Case Name** to load the Case Dashboard. See Case Dashboard section.
3. Click on **Enter Review**.

The Review portal will load with all processed evidence.

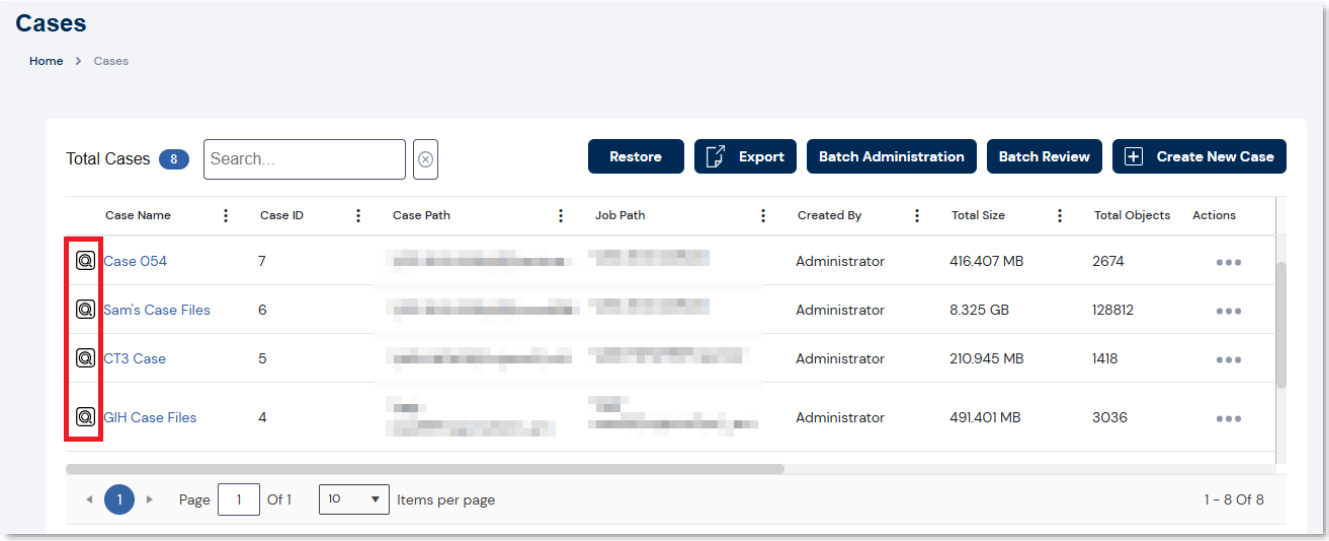
Note: Users will only see the cases that they have been assigned to. Administrators will have access to the full list of cases.

© Exterro, Inc. All rights reserved

Opening a Case via Case List

To open a case via case list:

1. From the home page, click **Case List**.



2. Click on the **Enter Review** icon against the required case.

The Review portal will load with all processed evidence.

Note: Users will only see the cases that they have been assigned to. Administrators will have access to the full list of cases.

© Exterro, Inc. All rights reserved

Opening a Case via Review Mode

To open a case via Review mode:

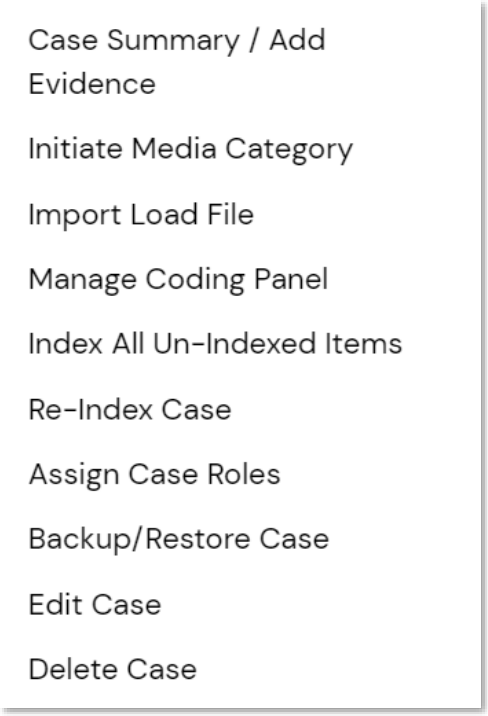
1. Ensure a case is open in Review mode.
2. Click on the drop-down list in the top-left corner.
3. Select a case to load directly in Review mode.

Note: Users can copy the case path within Review mode. Click on the **Copy Case Path** button located near the case drop-down list. The clipboard will now have the case path.

© Exterro, Inc. All rights reserved

Case List Options

You can click on the **Context menu** against the required case to select and perform the following operations.



- **Case Summary / Add Evidence** – To view case summary and add additional evidence.
- **Refresh Index Status** – To manually refresh the 'Index Status' column value for the corresponding case.
- **Merge Index** – To manually perform the 'Merge Index' operation for a case.

Warning: Merged entities continue to display objects belonging to an evidence item even after that evidence has been soft-deleted from the Case Summary page. However, you can regenerate the entity to view the refreshed results on the Entity Management page.

- **Initiate Media Category** – To configure Project VIC/CAID settings for a case. (See Configuring Project Vic/CAID section more details).

© Exterro, Inc. All rights reserved

- **Import Load File** – To import Load files to a case. While you can import load files from the Case List page, it is identical in functionality to importing load files during case creation. (See Case Creation Load Files section).
- **Manage Coding Panel** – To manage coding panels associated to a case.
- **Sync Portable Case** – To synchronize the changes made in the case of FTK Central with the corresponding Portable Case.
- **Index All Un-Indexed Items** – To manually initiate a job for the case to re-index the unindexed items.
- **Re-Index Case** – To delete the existing Index of case and initiate a new Index for the same based on the selected profile.

  ***Note**: Only the Noise words, letters, and columns are considered for reindexing. However, this will not alter the Index counts.*
- **Assign Case Roles** – To assign case-level permissions to users. (See Assigning Roles section for more details).
- **Assign Users/Groups to Case** –To assign users or user groups to the corresponding case.
- **Backup Case** - To Backup a case.
- **Edit Case** – To edit the case name, case path, and job path.

Note: Upon editing a case's path, it takes up to 5 to 10 minutes to reflect the change in the application.

- **Delete Case** – To delete a case.

Note: Upon initiating the Case deletion process, all the jobs associated with the corresponding case will be automatically cancelled before deleting the case.

Tip: You can click on the **Enter Review** button against the required case to directly navigate to the corresponding case's review mode.

© Exterro, Inc. All rights reserved

Case Dashboard

The Dashboard allows you to view important information regarding a case in an easy-to-read visual interface. Additionally, the dashboard allows you to access the Review portal. See Viewing Data section.

Case Overview

The Case Overview panel consists of data pertaining to the case you have clicked on. The details range from:

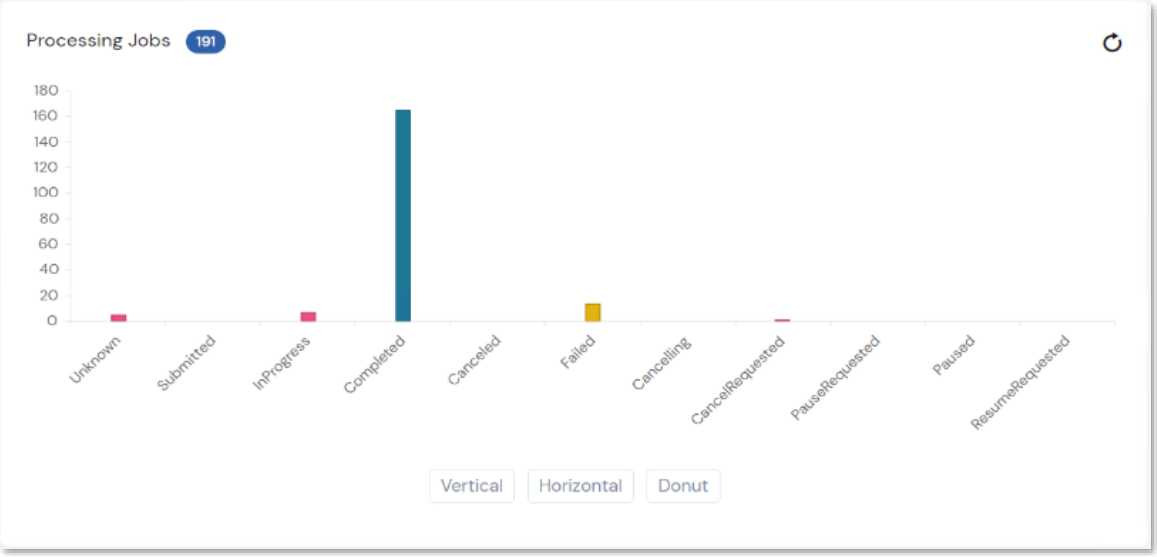
- Case ID
- Case Name
- Creation Date
- Size
- Case Path
- Case Size

© Exterro, Inc. All rights reserved

Processing Jobs

The Process Jobs section visualizes the status of all processing jobs associated with the case. You can toggle between the following options to view the information in different visualization representations:

- Vertical
- Horizontal
- Donut



© Exterro, Inc. All rights reserved

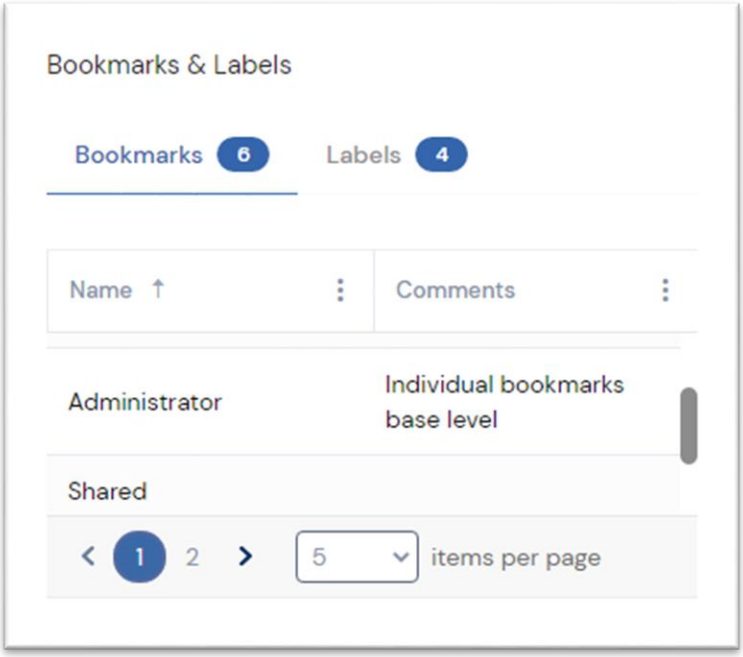
Case Evidence

The Case Evidence panel allows you to see the evidence that has been added to the selected case. This evidence may have custom placeholder images if applied during evidence processing. However, if this option has not been configured then the evidence image placeholder will be generic.

You can toggle the Case Evidence view by clicking on **Grid View**.

Bookmarks & Labels

The Bookmarks & Labels panel provides you with the grid view of all bookmarks and labels available in a case.

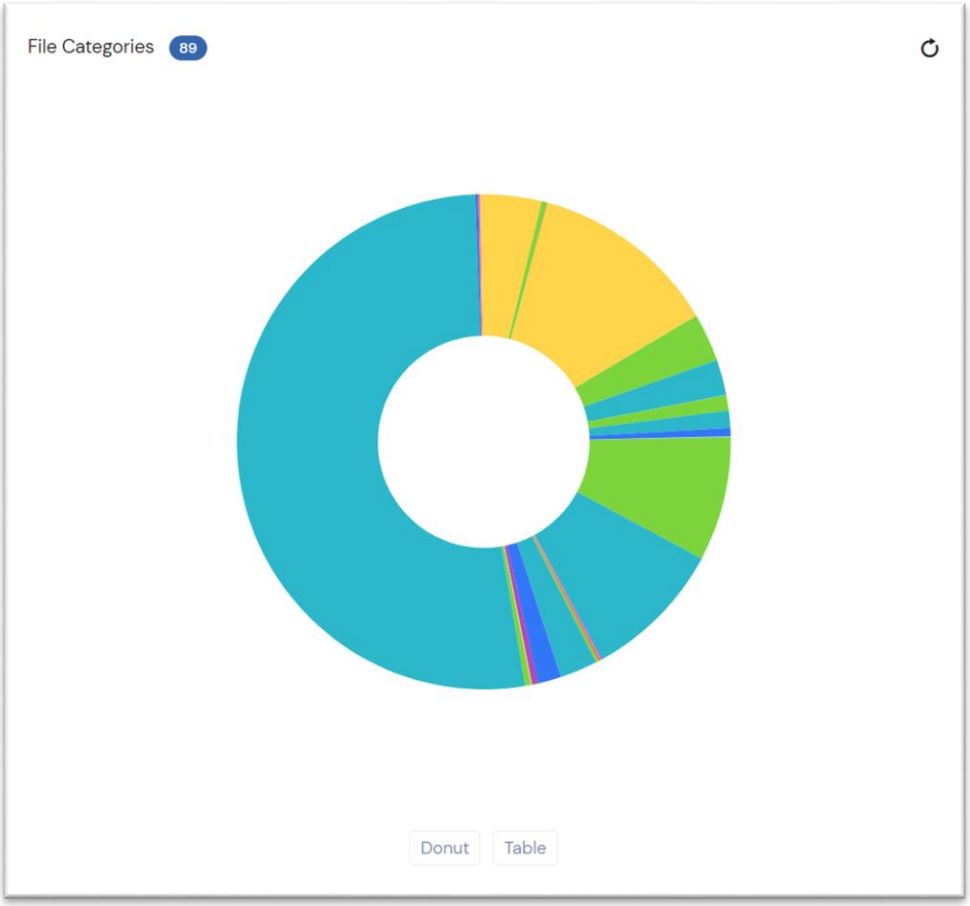


© Exterro, Inc. All rights reserved

File Categories

The File Categories panel provides you with a visualization of all the evidence file types available in a case. The following are the types for views available for File Categories:

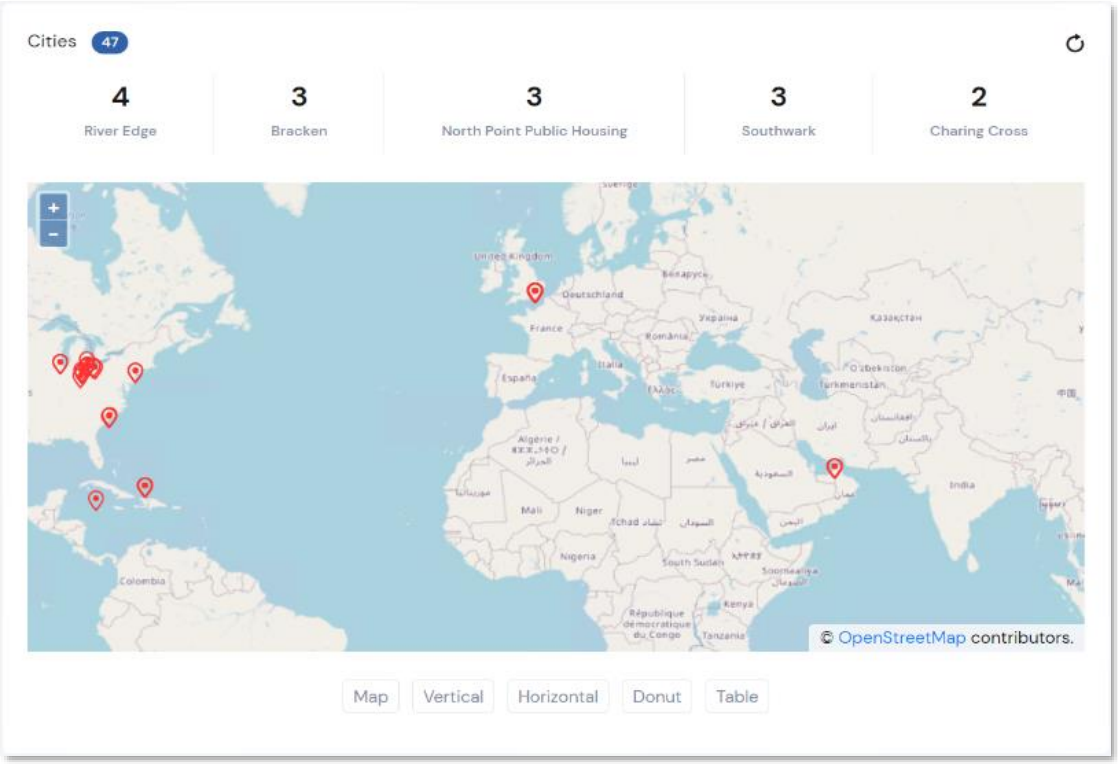
- Donut
- Table/List



© Exterro, Inc. All rights reserved

Cities

The Cities panel provides you a geographical representation of the files that are associated to specific cities. This information is obtained with the use of geographical metadata.



© Exterro, Inc. All rights reserved

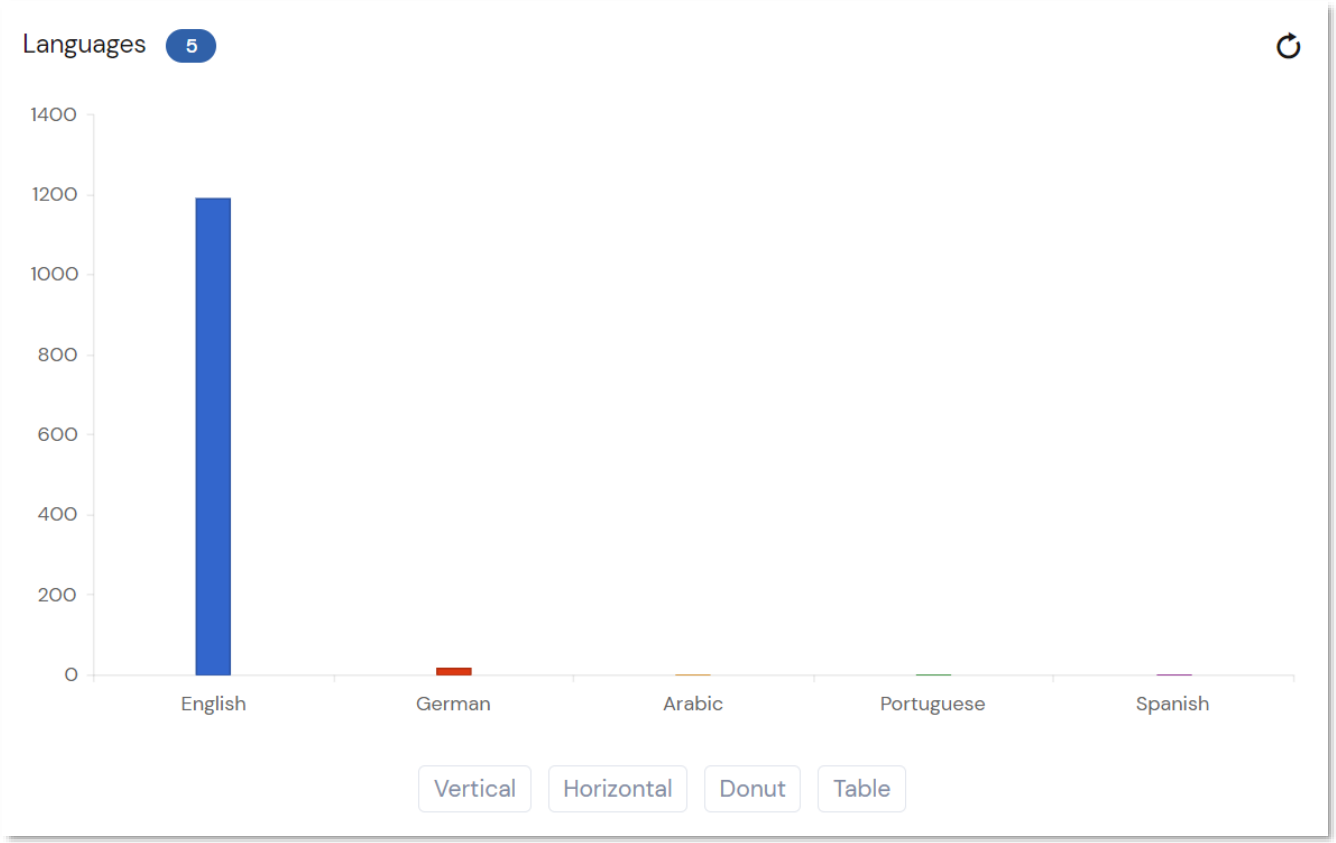
Message Applications

The Message Applications section allows you to have an overview of message application usage found within a dataset.

© Exterro, Inc. All rights reserved

Languages

The Languages panel allows you to see an overview of the languages identified within a case. This will only be populated if the Language Identification processing option is selected at case creation.

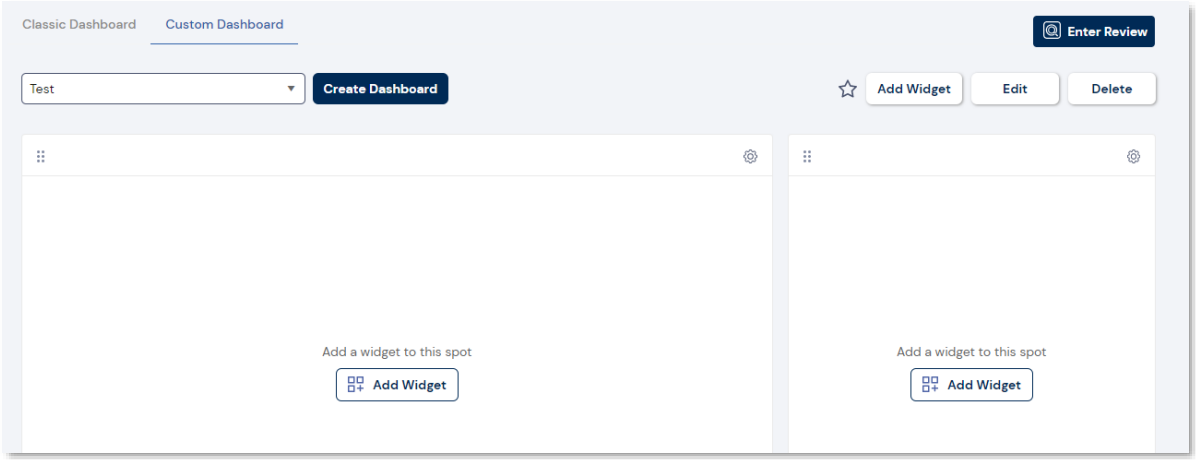


© Exterro, Inc. All rights reserved

Custom Case Dashboards

To create a custom dashboard:

1. From the home page, click **Case List**.
2. Click on the **Case Name**.
   - The **Custom Dashboard** tab will be displayed.



3. Click Create Dashboard.
4. Select a **Layout**.
5. Enter a Dashboard Name.
6. Select the **Access** type.
   - **Public**: Everyone at a case-level can view the dashboard.
   - **Private**: Only the users/user groups selected can view this custom dashboard. These users/user groups must be assigned to the case to be listed.
     - Click the **Select Users / User Groups** drop-down list and check the required users/user groups.
7. Click Create Dashboard.

Tip: You can edit the required custom dashboard by clicking on **Edit** for the selected custom dashboard.

© Exterro, Inc. All rights reserved

To mark a custom dashboard as Favorite:

1. From the home page, click **Case List**.
2. Click on the **Case Name**.
3. Select a **Custom Dashboard** from the drop-down list.
4. Click on the **Favorite** button in the top-right corner.

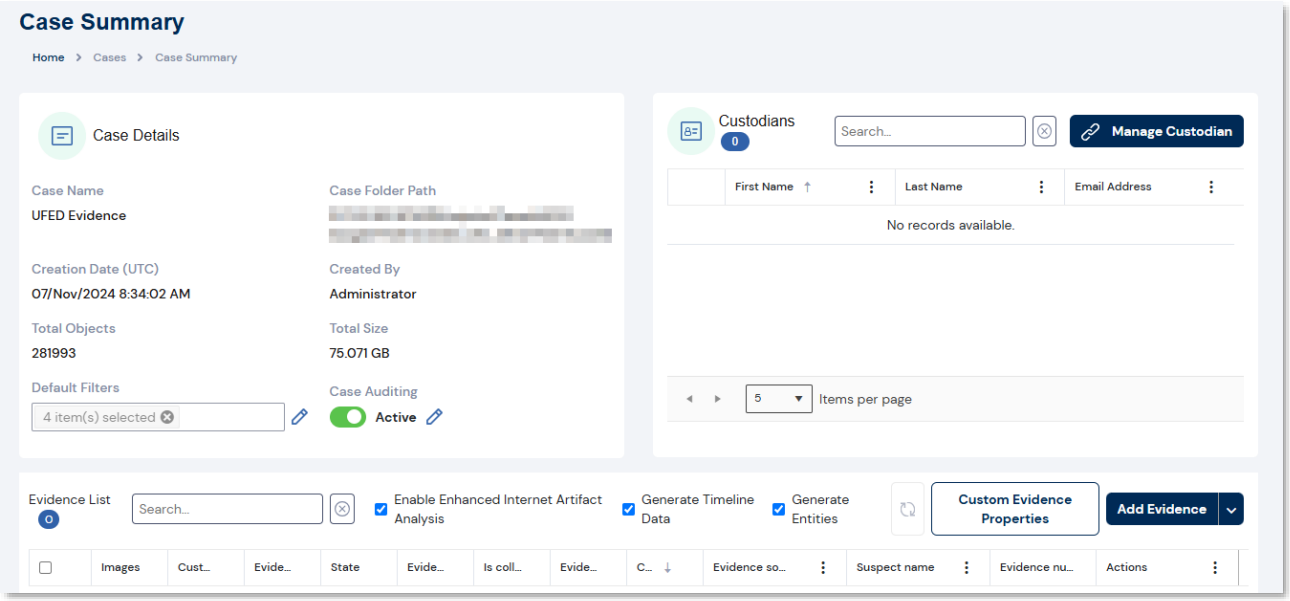
The selected custom dashboard will now be loaded by default.

© Exterro, Inc. All rights reserved

Case Summary

While the Case Dashboard gives you a visualization of case details, the Case Summary section gives you the ability to make changes to a case. The following changes can be made:

- Importing Load Files.
- Managing Custodians.
- Managing Evidence.
- Managing Process Data.
- Managing Default Filters.



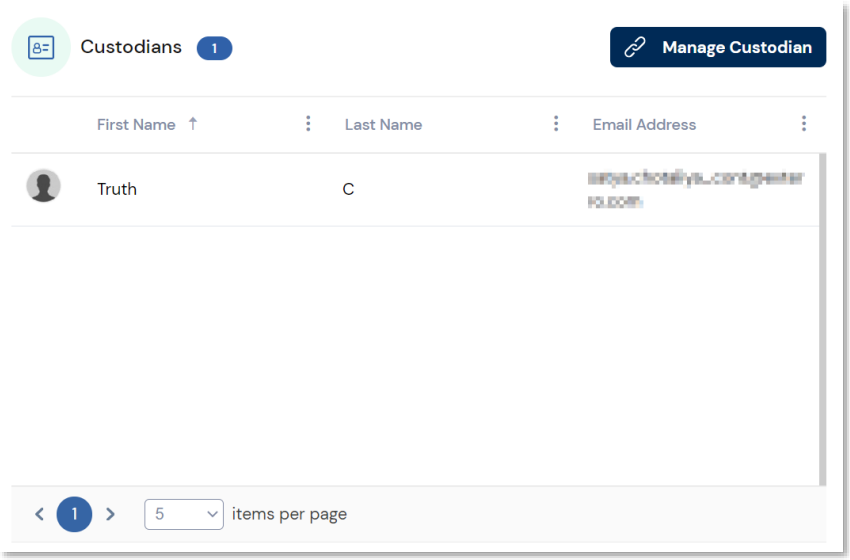
© Exterro, Inc. All rights reserved

General Statistics

The Case Details panel gives you an overview of the Case Name, Case Folder Path, Creation Date, Total Objects, Created By and Total Size.

Managing Custodians

While you can map custodians from the Case Summary page, it is identical in functionality to mapping custodians during case creation. See Case Creation: Custodian Mapping.



Adding a Custodian

Refer Creating a Case: Custodian Mapping section.

Removing a Mapped Custodian

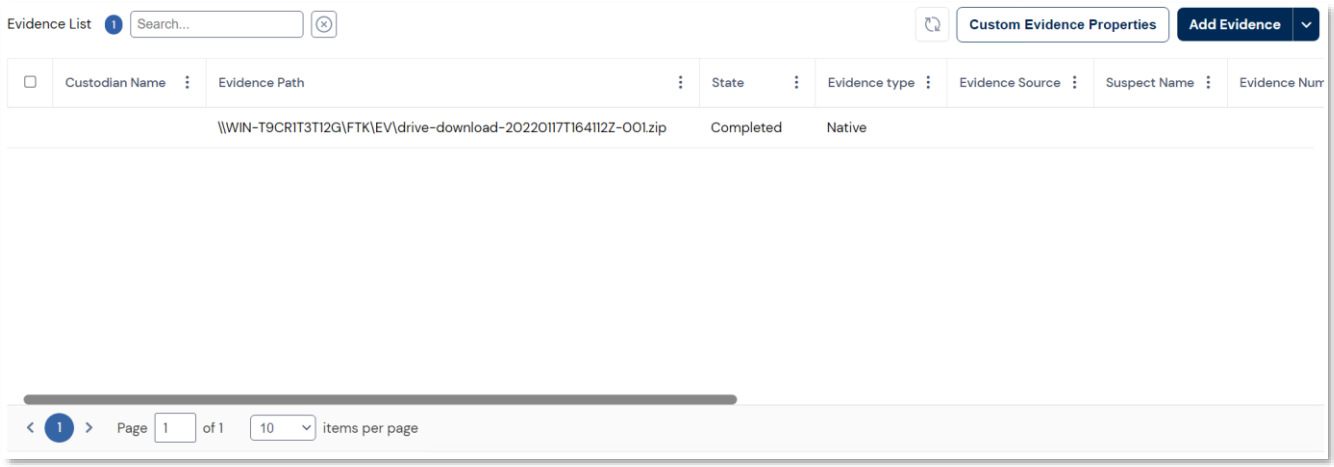
To remove a mapped custodian:

1. Click **Manage Custodian**.
2. Using the **Custodians Mapped** panel, search for the custodian.
3. Click **X**.
4. Click **Save** to finalize custodian removal.

© Exterro, Inc. All rights reserved

Managing Evidence

Similarly, to the process of adding evidence during case creation, you can edit and remove any evidence added to a case using Case Summary.



Adding Additional Evidence

See [Creating a Case: Process Evidence.]

Removing Evidence

Evidence within a case can be deleted during and after a case. However, deleting evidence from a case does not delete the data source itself, rather just the case data associated with the evidence.

To remove evidence:

1. Click on the **context menu** (in the **Actions** column) against the evidence required to be removed.
2. Click **YES**.

Warning: Once deleted, it cannot be undone. All associated labels and bookmarks will be removed.

© Exterro, Inc. All rights reserved

Managing Process Data

After case creation you can use the Process Evidence section to specify the processing profile to use during processing. This processing will take place on any new evidence added to the case.

Processing Data

See Process Evidence.

Managing Default Filters

After case creation you can edit the selected default filters on a case by case basis.

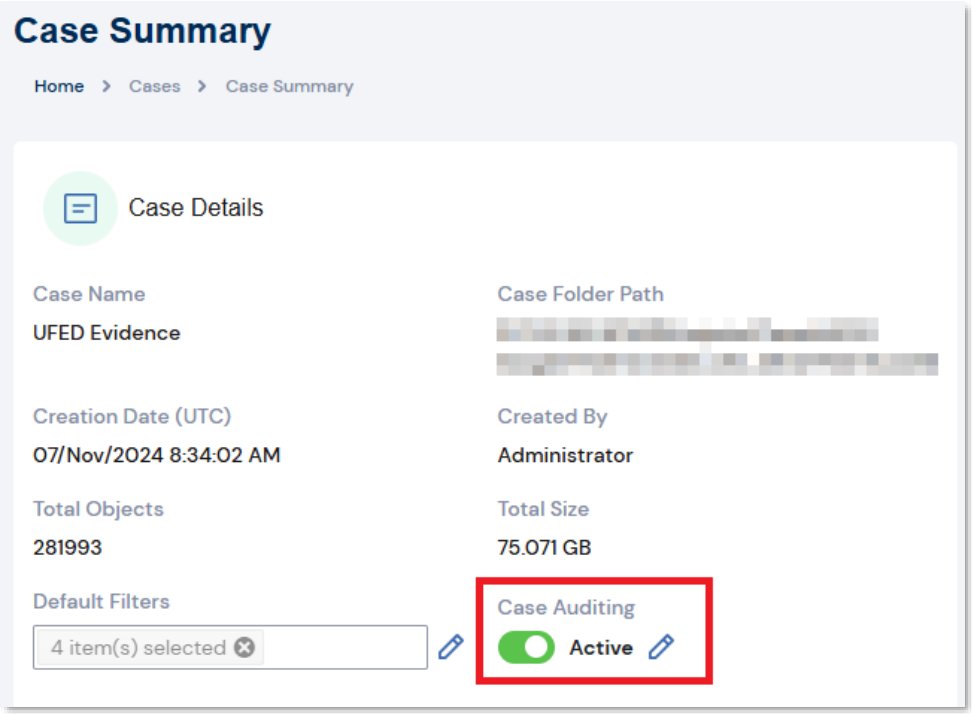
To remove default filters:

1. Click on the **Edit** button.
2. Select the required filters within the drop-down list.
   - Hide Duplicates
   - eDiscovery Refinement
   - Hide Containers
   - Hide Bookmarks
3. Click the **Save** button.

© Exterro, Inc. All rights reserved

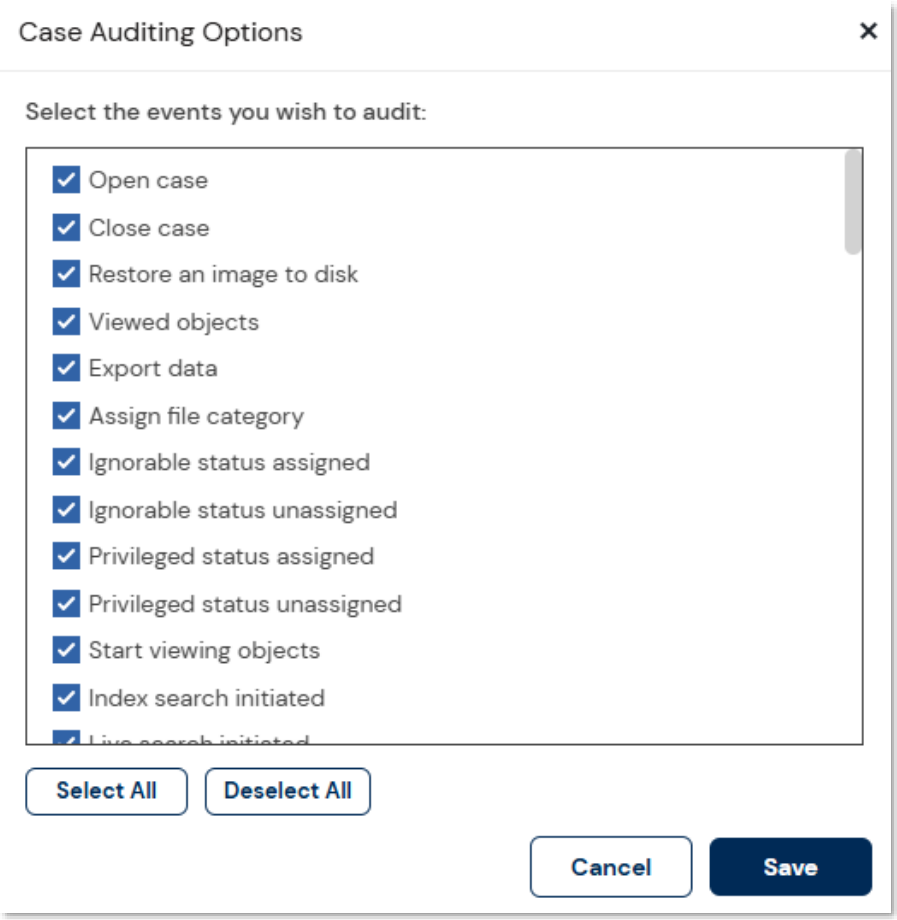
Managing Case Auditing

You can choose to enable or disable the Case Auditing process for a case using the **Case Auditing** toggle in the **Case Summary** page.



© Exterro, Inc. All rights reserved

Also, you can click on the **Edit** icon against the toggle to select the required events for which the auditing should be performed.



© Exterro, Inc. All rights reserved

Coding Panels

Coding is putting values into the fields (columns) of documents. The Coding panel in Review allows you to use coding layouts to change the data of the selected document. Coding layouts can be created from the Case List or during Batch Administration.

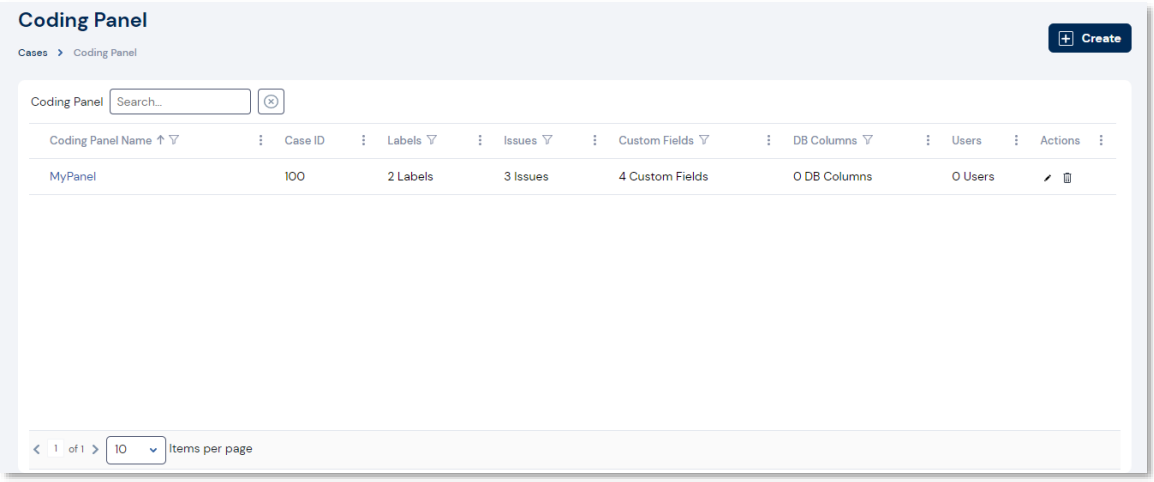
Reviewers with View Coding Layout permissions can code the data of a document using the Coding panel and the mass actions in the Grid panel. Coding allows you to identify descriptive pieces of information that never had metadata, like images that were loaded and need to have dates manually added into the field. The Coding panel in Review allows you to use coding layouts to code the selected document.

© Exterro, Inc. All rights reserved

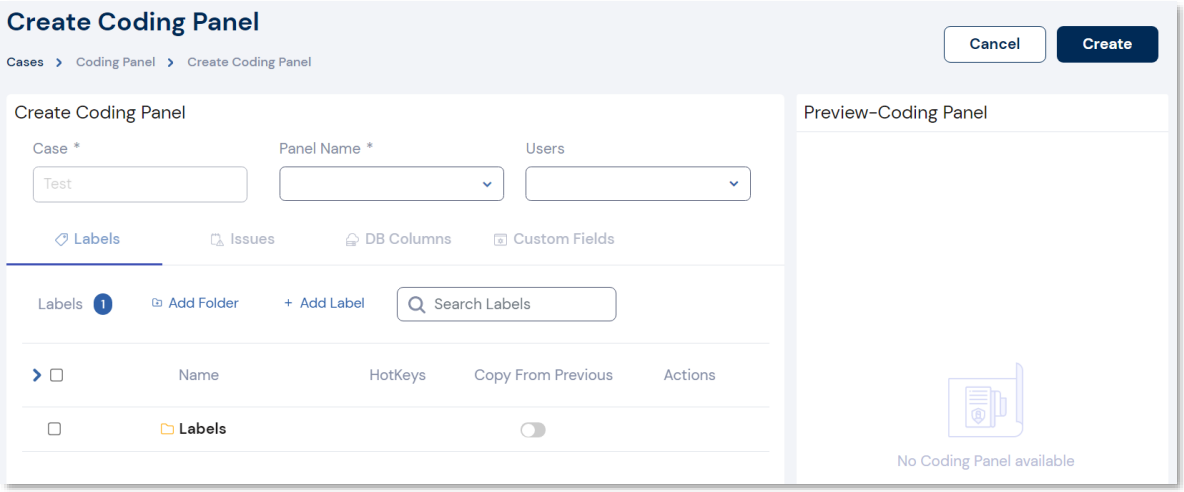
Creating Coding Panel

To create a coding panel:

1. From the home page, click **Case List**.
2. Click on the **context menu** (in the **Actions** column) against the required case.
3. Click the **Manage Coding Panel**.
    - The **Coding Panel** page is displayed.



4. Click **Create**.
    - The **Create Coding Pane** page is displayed.



© Exterro, Inc. All rights reserved

5. Enter a **Panel Name**.
6. Select the **Users** that will have access to the coding panel.
7. Use the sections below to configure new Creating Labels, Creating Issues, Creating DB Columns and Creating Custom Fields.
8. Click **Create**.

Creating Labels

To create a label:

1. Navigate to **Labels** tab.
2. Click on **+ Add Label**.
3. Enter the label's name in the field prompted.
4. Configure the hotkey by selecting a key.
5. Enable **Copy From Previous** option in order to apply the previously made configuration to the current record.
6. Click on the **Save** button .

Notes:

- From the list of labels, you can click **Edit** or **Delete** to edit or remove the label respectively.
- From the list of labels, you can click on the **New Label** button against a label folder to create a child label.

© Exterro, Inc. All rights reserved

Creating Issues

To create an issue:

1. Navigate to **Issues** tab.
2. Click on **+ Add Issues**.
3. Enter the issue's name in the field prompted**.**
4. Configure the hotkey by selecting a key.
5. Enable **Copy From Previous** option in order to apply the previously made configuration to the current record.
6. Click on the **Save** button .

Notes:

- From the list of issues, you can click on the **Edit** or **Delete** button to edit or delete the issue respectively.
- From the list of issues, you can click on the **Add Child Issue** button against the required issue to create a child issue.

© Exterro, Inc. All rights reserved

Creating DB Columns

To create a DB column:

1. Navigate to **DB Columns** tab.
2. Select one or more **DB columns.**

Creating Custom Fields

To create a custom field:

1. Navigate to **Custom Fields** tab.
2. Click on **+ Add Custom Fields**.
3. Enter a custom field **Name**.
4. Select the **Type** of custom field to be created.
5. Checkbox
6. Radio
7. Date
8. Text
9. Number
10. Multi Entry – This option requires users to separate values with a semicolon (;).
11. Enable **Copy From Previous** option in order to apply the previously made configuration to the current record.
12. Enable the **Required** option to force users to enter a value into the custom field before submission.
13. Click **Save.**

Notes:

- From the list of custom fields, you can click on the **Edit** or **Delete** button to edit or remove the field respectively.
- From the list of issues, you can click on the **Add Value** button against the required field to create another field.

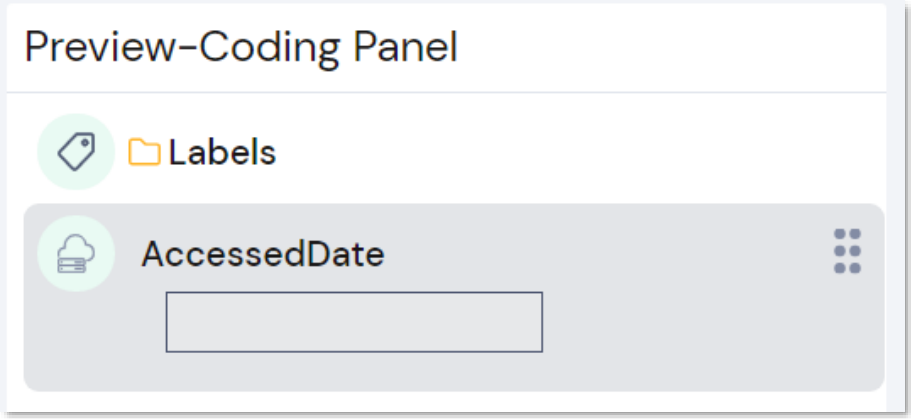
Reorganizing a Coding Panel

To reorganize coding panel layouts:

1. From the home page, click **Case List**.

© Exterro, Inc. All rights reserved

2. Click on the **Context menu** (in the **Actions** column) against the required case.
3. Click on **Manage Coding Panel**.
4. Click on the **Edit** button against the required coding panel.
5. Hover over a coding panel element in the **Preview-Coding Panel** pane.



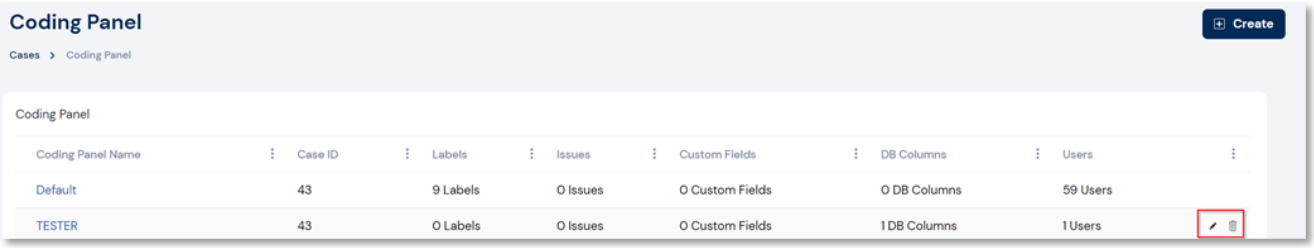
6. Click and drag an element in its desired order.
7. Click **Update**.

© Exterro, Inc. All rights reserved

Deleting Coding Panels

To delete a coding panel:

1. From the home page, click **Case List**.
2. Click on the **Context menu** (in the **Actions** column) against the required case.
3. Click on **Manage Coding Panel**.



4. Click on the **Delete** button .

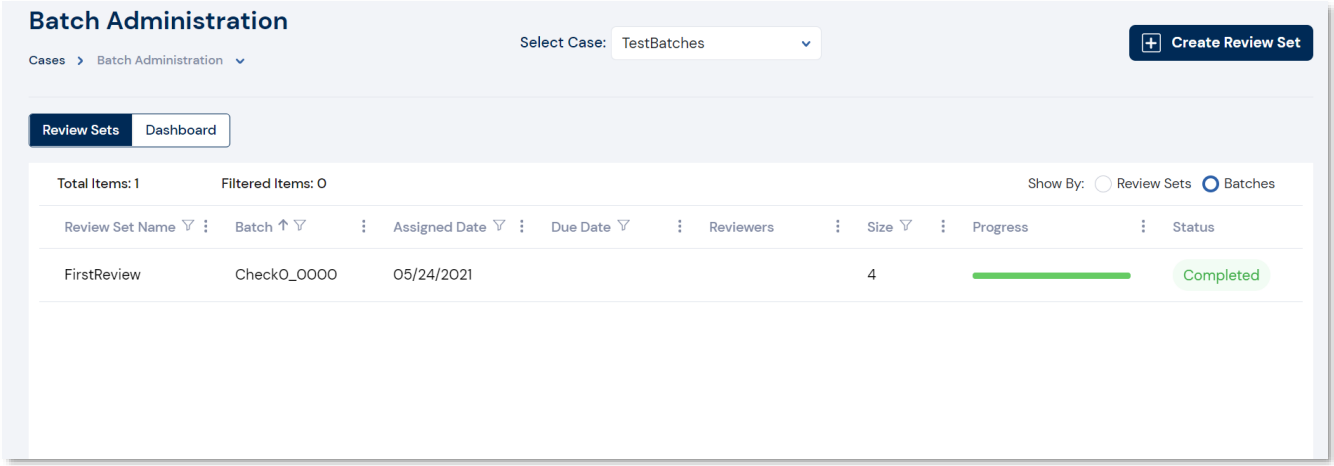
Warning: Clicking on the Delete button will remove the coding panel without prompting any further confirmation.

© Exterro, Inc. All rights reserved

Batches

Batches are review sets of documents that you can check out for coding and then check back in. Batches aid in the work flow of the reviewer. It allows the reviewer to track the documents that have been coded and still need to be coded. Administrators with Manage Review Sets permissions can create and delete review sets.

Batch Administration Panel



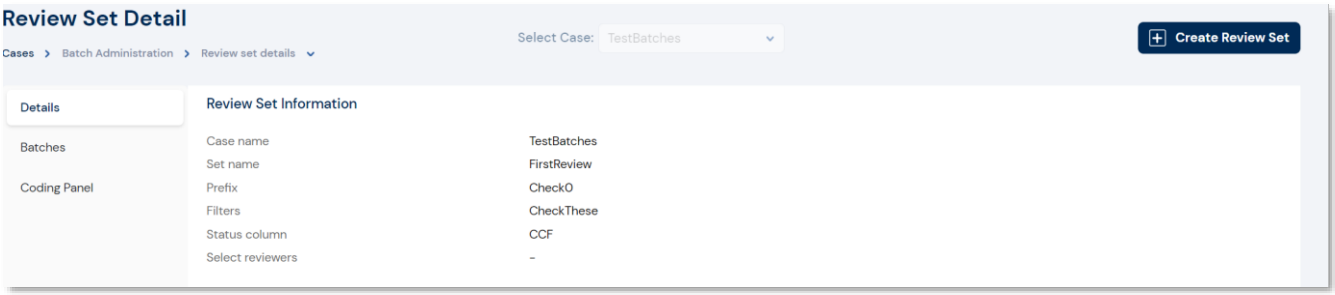
The Batch Administration panel can be accessed from the **Case List tab**. This panel allows users with relevant permissions to create review sets as well as view the progress of existing assigned batches.

© Exterro, Inc. All rights reserved

Viewing Review Set Details

To view review details:

1. Select a case using the drop-down list.
2. Select **Show By: Review Sets**. Selecting Batches will give you an overview of the review sets in a case.
3. Click the **Review Set Name**.
   - The Review Set Detail panel is displayed.



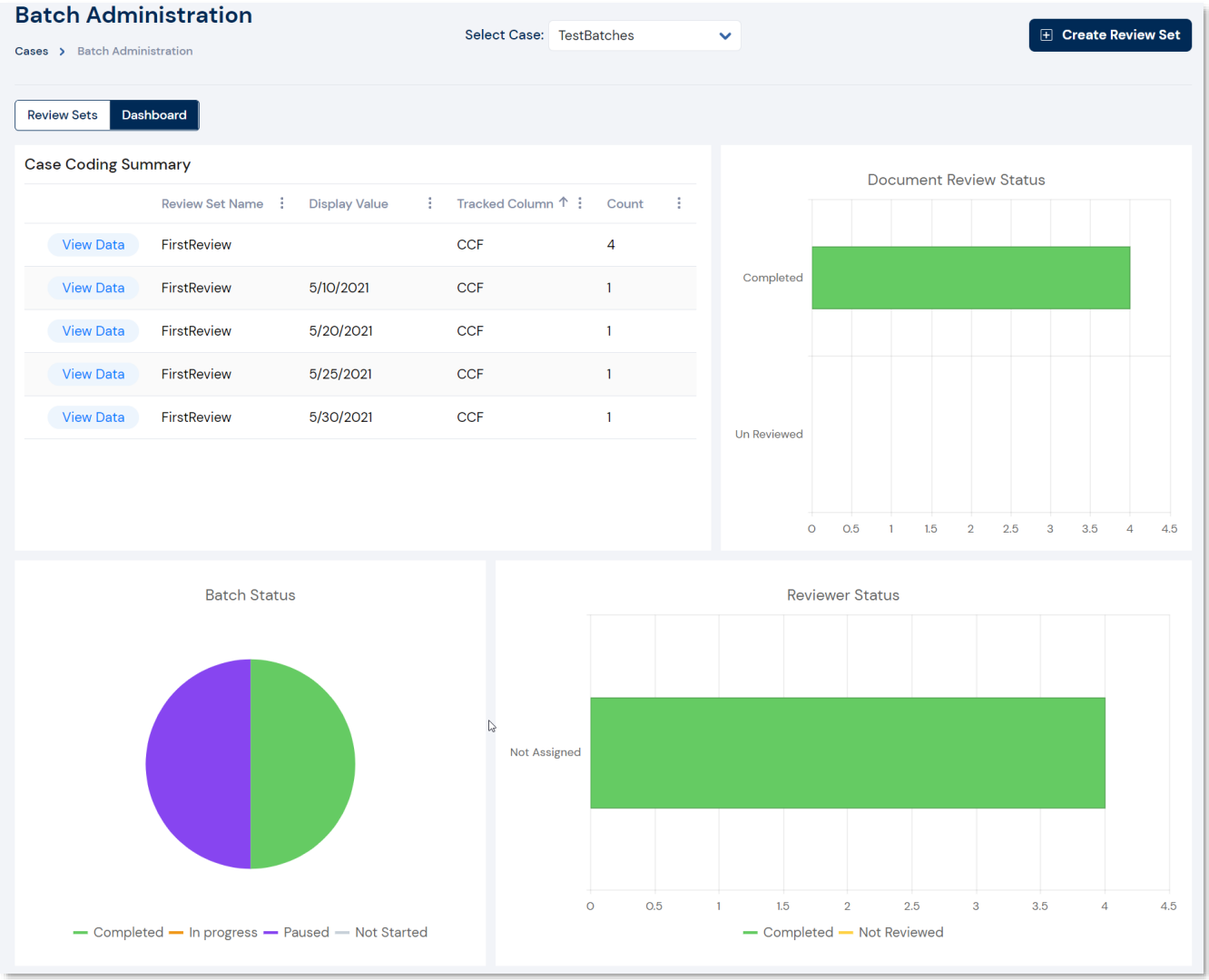
Note: While viewing the batch details in Batch Information or Review Set Detail windows, you can click on **Edit** or **Delete** against the required batch to assign reviewers or delete the batch.

© Exterro, Inc. All rights reserved

Dashboard: Viewing Case Coding Summary

When viewing the Batch Administration panel, you have the ability to see a summary of the Case Coding summary. This overview allows you to see the review sets that were created and even if they were checked in as completed, you are able to view those select documents to finalize them.

- Click Create Review Set to create a new review set.
- Click View Data to view the review set data in Review mode.



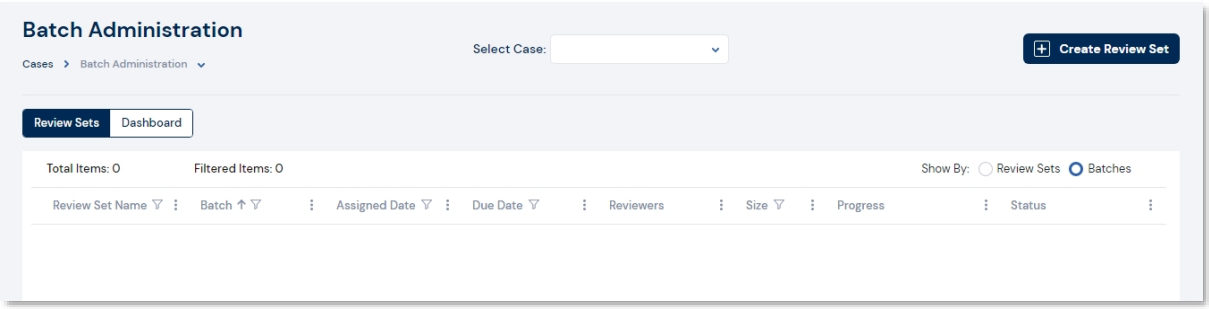
© Exterro, Inc. All rights reserved

Creating Review Sets

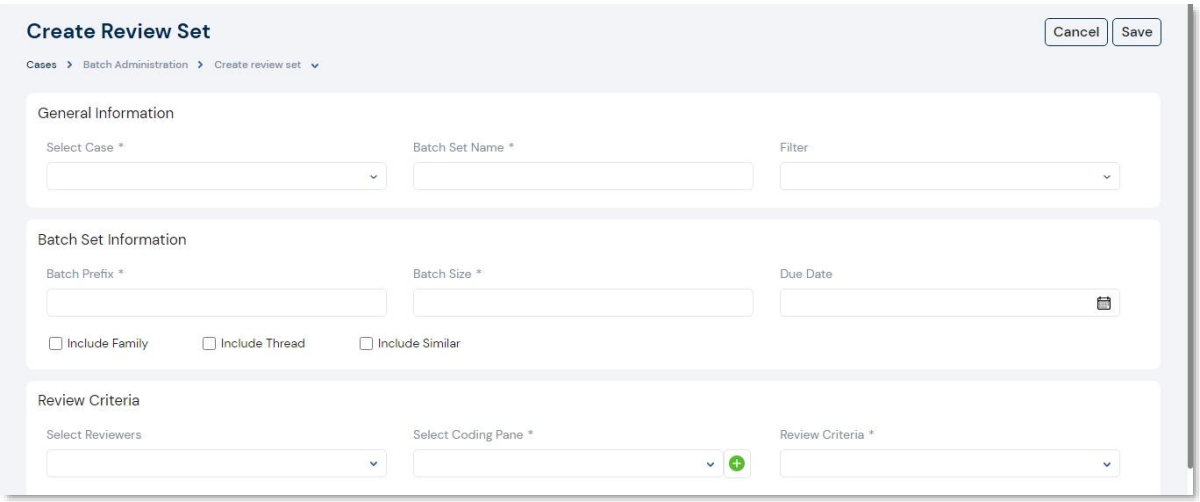
FTK Central allows you to create multiple review sets for cases based on your requirements. This option allows you to assign specific users to batches, which then allow those users to perform review tasks.

To create a review set:

1. From the home page, click **Case List**.
2. Click Batch Administration.
   - The **Batch Administration** window is displayed.



3. Click Create Review Set.
   - The **Create Review Set** page is displayed.



4. Select the required case for which the review set has to be created, using the **Select Case** drop-down field.

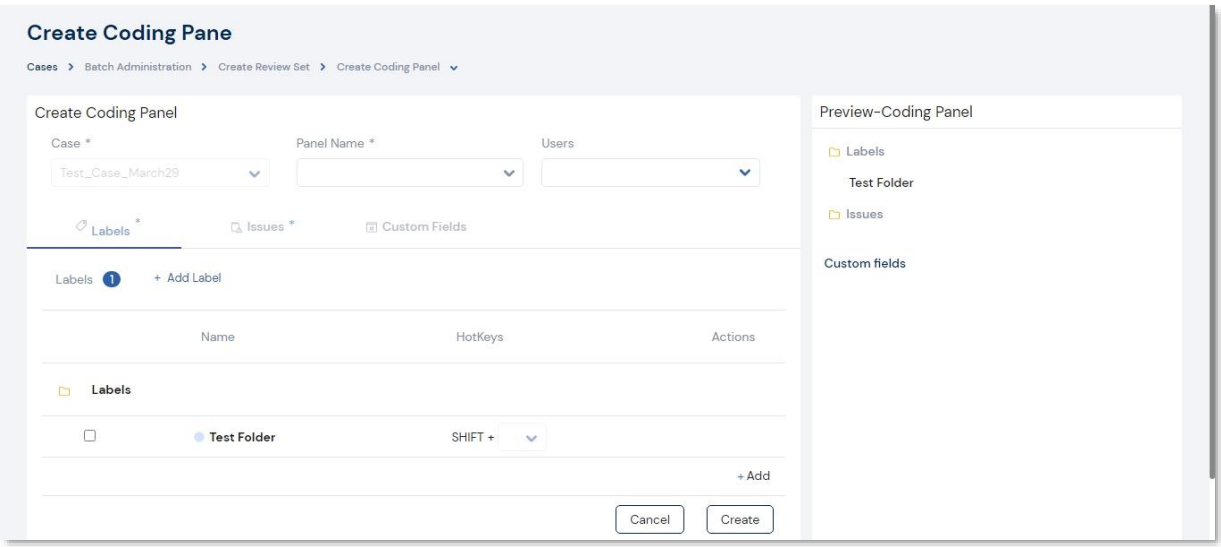
© Exterro, Inc. All rights reserved

5. Provide the **Batch Set Name**.
6. Select the required **Filter** based on which the files in the case should be filtered before adding them to the review set. This can be labels or label groups within a case.
7. Provide the keyword terms in **Batch Prefix** field that should be prefixed to the files in a review set.
8. Provide the file count limit in the **Batch Size** field based on which the number of files for a batch will be automatically allocated.
9. Set the **Due Date** for the review set by clicking on and configuring the date.
10. Enable any or all of the below provided options based on the requirement:
    - **Include Family** – To include the family files.
    - **Include Thread** – To include the related email threads.
    - **Include Similar** – To include similar files.

11. Select the reviewers from the **Select Reviewers** drop-down field intended for the review set.
12. Select the coding pane intended for the review set from the **Select Coding Pane** drop-down field.

© Exterro, Inc. All rights reserved

Note: You can click on (add button) to add a new coding by configuring the **Create Coding Pane** page based your customizations. See Coding Panels section.



13. Select the label criteria from the **Review Criteria** drop-down field. The review process for a file will be considered as completed only if the selected label is applied to the file during review process.
14. Click **Save**.

© Exterro, Inc. All rights reserved

Editing Review Sets

To edit a review set:

1. From Batch Administration page, select a case using the drop-down list.
2. Select **Show By: Review Sets**. Selecting **Batches** will give you an overview of the review sets in a case.
3. Click the **Review Set Name**.
4. The Review Set Detail panel will open with options to view **Details, Batches** and **Coding Panel** details.
5. Click **Batches**.
6. Click the **Edit** button.
7. Make the necessary changes.
8. Click **Update**.

Deleting Review Sets

To delete a review set:

1. From Batch Administration page, select a case using the drop-down list.
2. Select **Show By: Review Sets**. Selecting **Batches** will give you an overview of the review sets in a case.
3. Click the **Review Set Name**.
4. The Review Set Detail panel will open with options to view **Details, Batches** and **Coding Panel** details.
5. Click **Batches**.
6. Click the **Delete** button.
7. Click **OK**.

© Exterro, Inc. All rights reserved

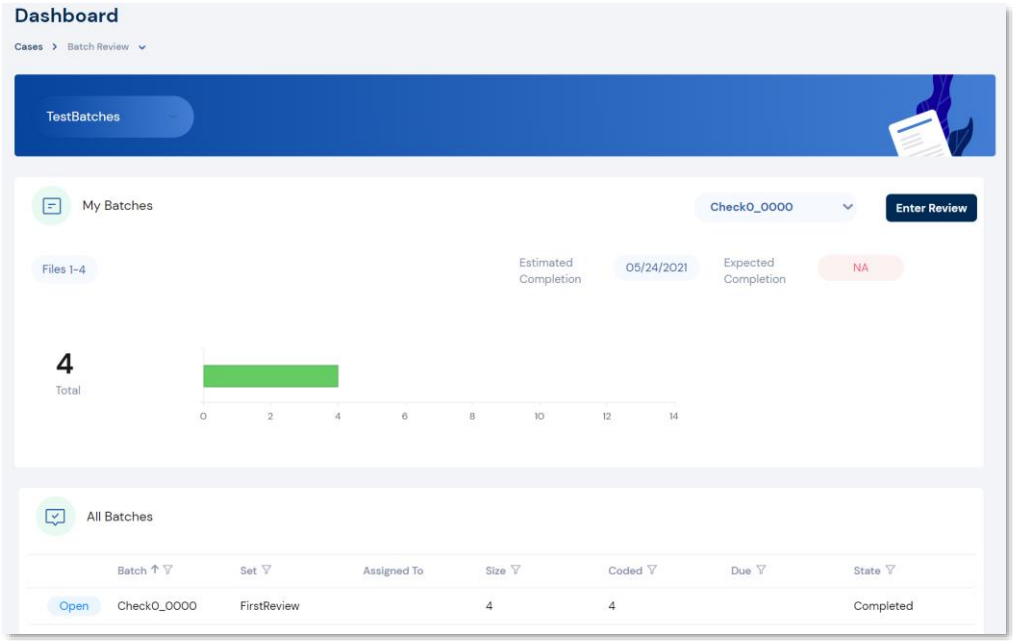
Batch Review Panel

Checking In/Out a Review Set

Reviewers can check out sets of documents for coding. Administrators can create and associate review sets for reviewers. When you are done coding a set of documents, you can check them back in to notify administrators you are done with reviewing the batch.

To check in/out of a review set:

1. From the home page, click **Case List**.
2. Click Batch Review.
   - The **Batch Review** window is displayed.



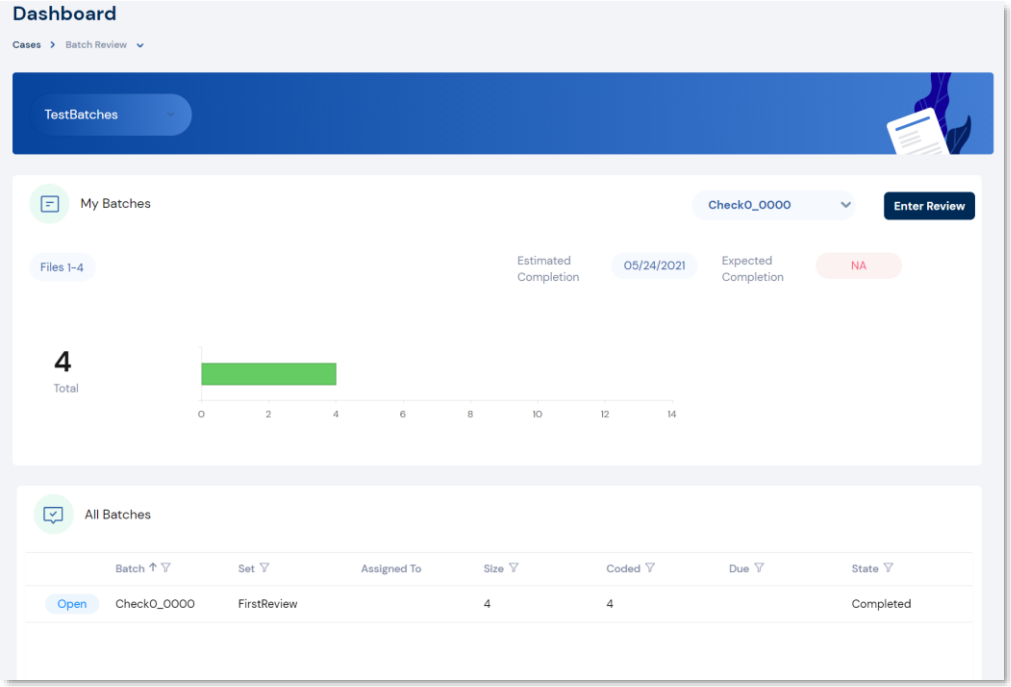
3. Select a case using the drop-down list.
4. The review sets for this case will appear in **All Batches**.
5. In line with the batch, click the **Check Out** button or **Check In** button.

© Exterro, Inc. All rights reserved

Reviewing a Review Set

To review a review set:

1. From the home page, click **Case List**.
2. Click Batch Review.
   - The **Batch Review** window is displayed.



3. Select a case using the drop-down list.
4. The review sets for this case will appear in **All Batches**.

Note: Alternatively, you can select a batch from the **My Batches** drop-down list.

5. Click Enter Review.

Note: Alternatively, click **Open** in line with a batch in **All Batches**.

© Exterro, Inc. All rights reserved

Backup and Restoring Cases

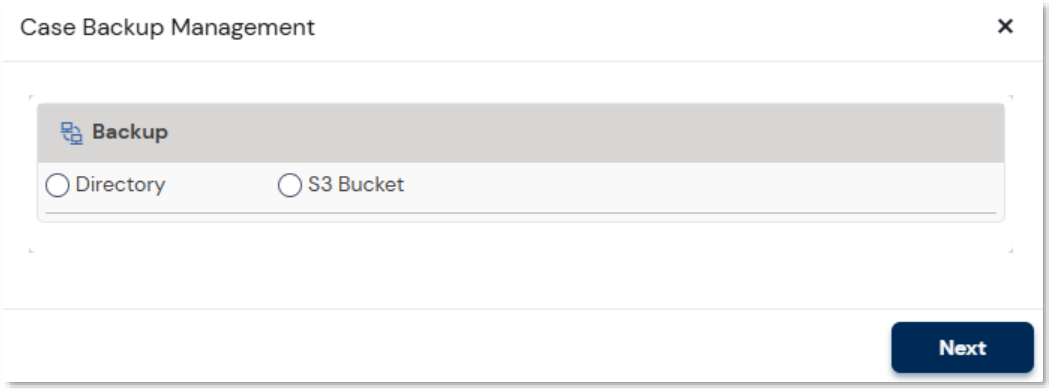
Backup and Restoring Cases

The Backup function copies the case's database table space file to the case folder, then deletes it from the database. This prevents two people from making changes to the same case at the same time, preserving the integrity of the case, and the work that has been done on it. Look for filename DB fn. Backup keeps up to four backups, DB f0, DB f1, DB f2, and DB f3.

Backing up the Cases

To back up a case:

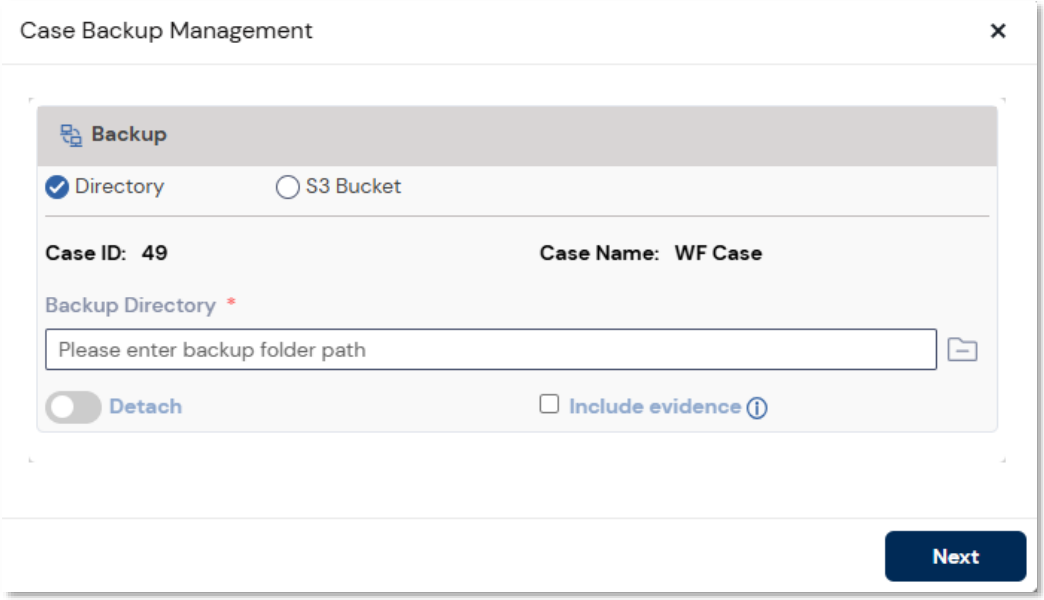
1. From the home page, click **Case List**.
2. Click on the **Actions menu** against the required case.
3. Select **Backup**.
   - The **Case Backup Management** pop-up is displayed.



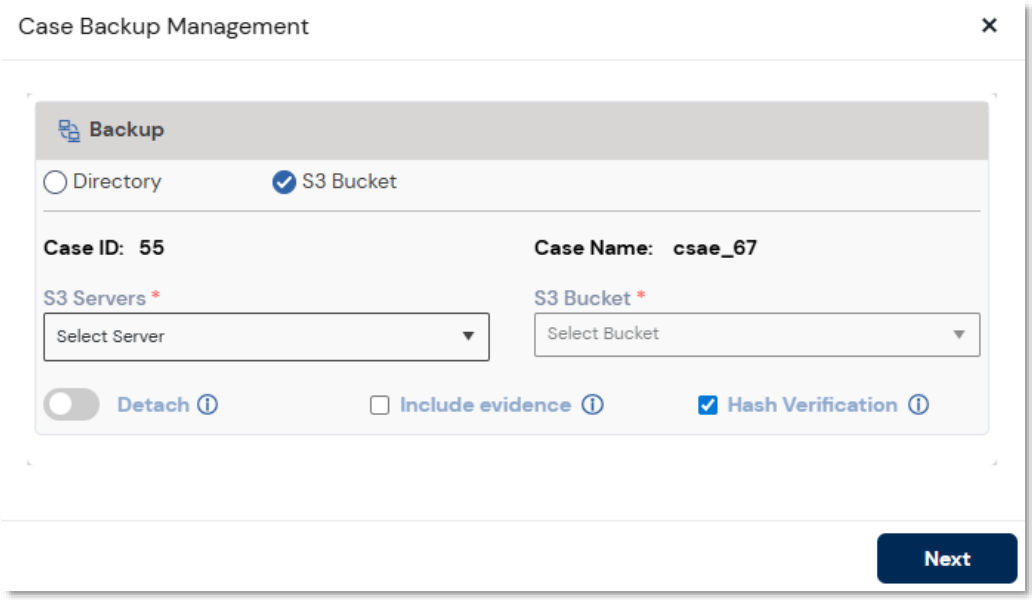
© Exterro, Inc. All rights reserved

4. Select the **Backup** type

- **Directory** – To back up the case in the network directory. You can provide the network path in the **Backup Directory** field or click on the **Browse** button against the field to browse and select the required path.



- **S3 Bucket** – To back up the case in the AWS S3 location. You can select the **S3 Server** and **S3 Bucket** in which the case should be backed up.



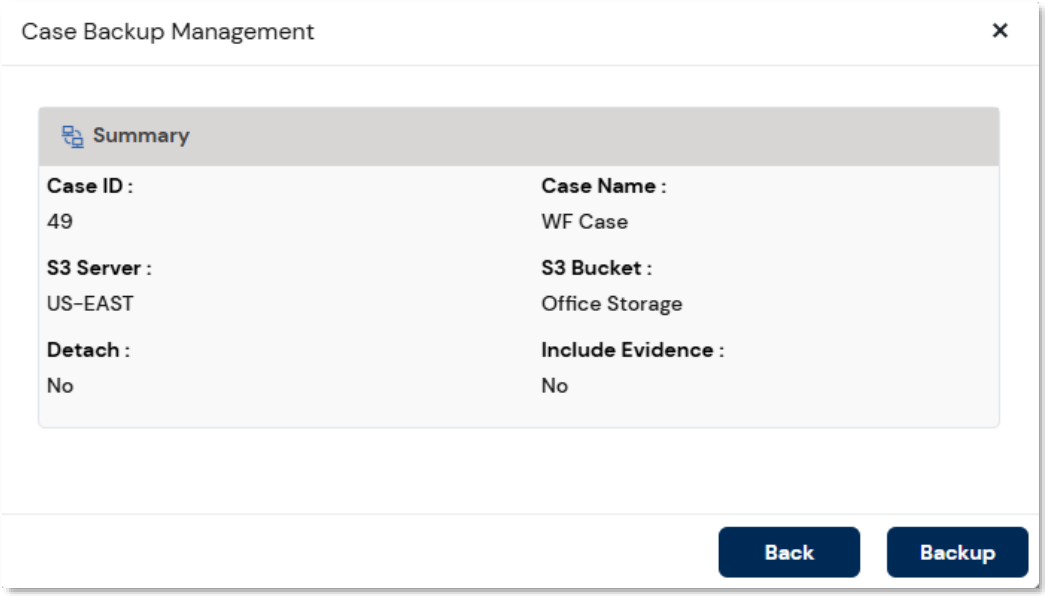
© Exterro, Inc. All rights reserved

5. Enable the **Detach** option if you want to delete the case from the FTK Central after the backup process is completed.
6. Check the **Include Evidence** option if you want to back up the evidence along with the case.
7. Check the **Hash verification** option if you want to verify the hashes of the files backed up into the AWS S3 to ensure data integrity.

Notes:

- The **Hash Verification** option is applicable only while backing up the cases in AWS S3.
- You can download the hash file generated for the case from the **Hash Details** column in the **File Upload Progress** pop-up of **AWS S3 Management**.

8. Click **Next**.
   - The **Summary** of the configurations made will be displayed.



9. Verify the configuration and click on **Backup**.

© Exterro, Inc. All rights reserved

The backup job will be initiated. You can view its progress in the Job Queue. The selected case will have a backup created upon successful execution of the job.

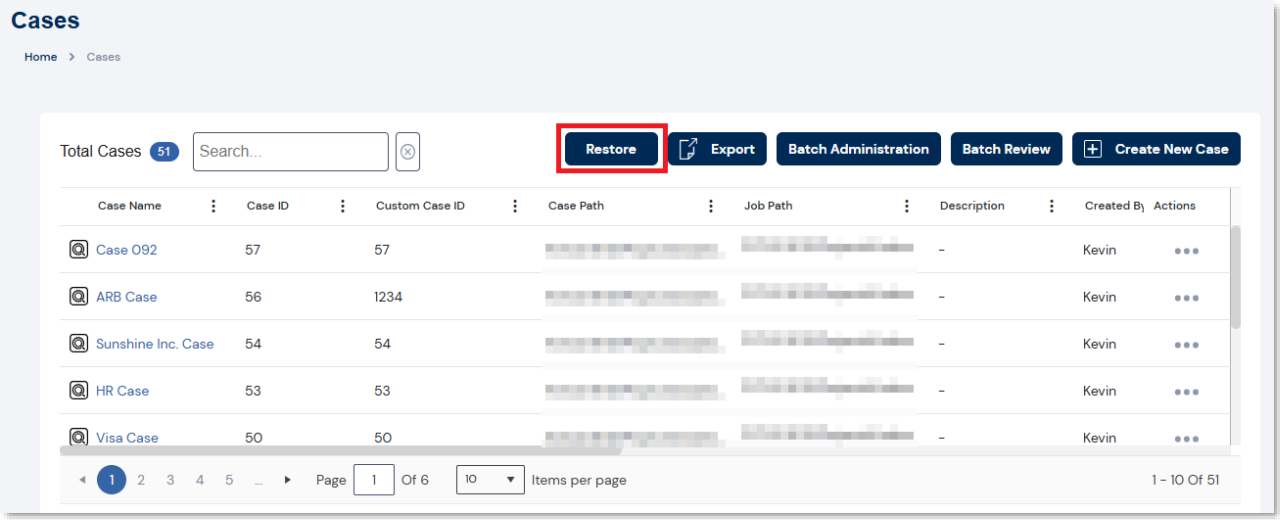
© Exterro, Inc. All rights reserved

Restoring Cases

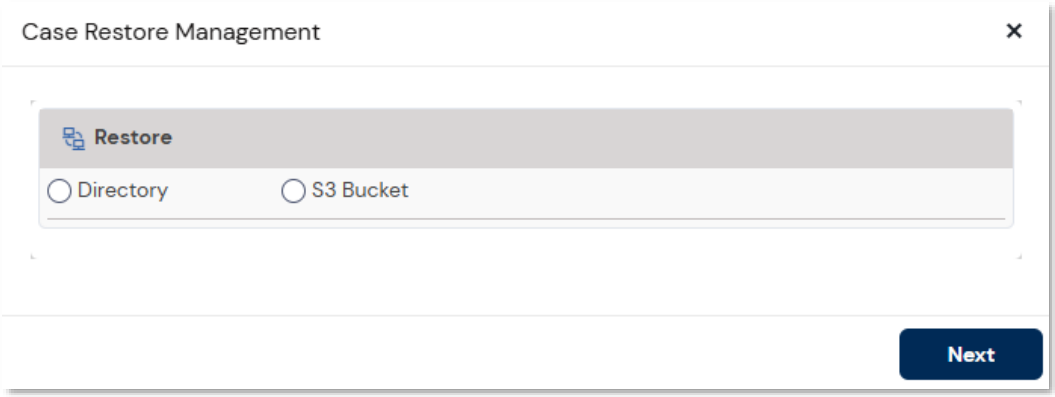
When your case is backed up, it is saved within a folder. FTK Central allows you can restore the case state.

To restore the case:

1. From the home page, click **Case List**.
2. Click on **Restore**.



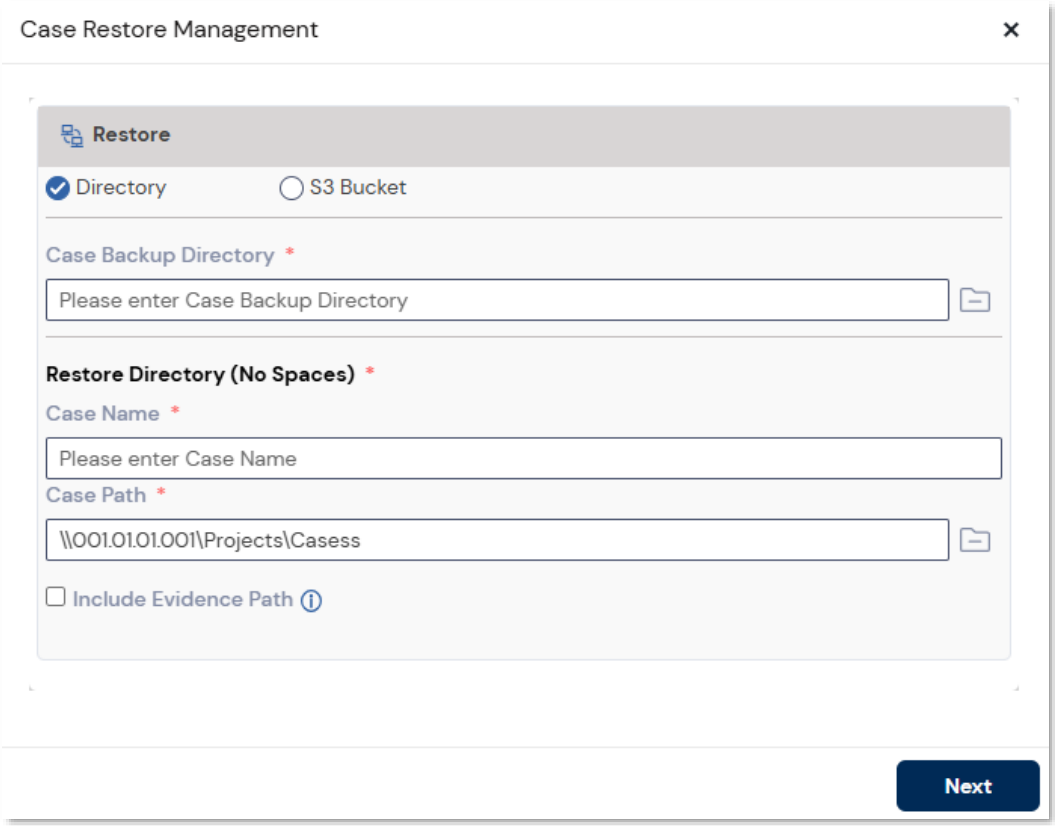
- The **Case Restore Management** pop-up is displayed.



© Exterro, Inc. All rights reserved

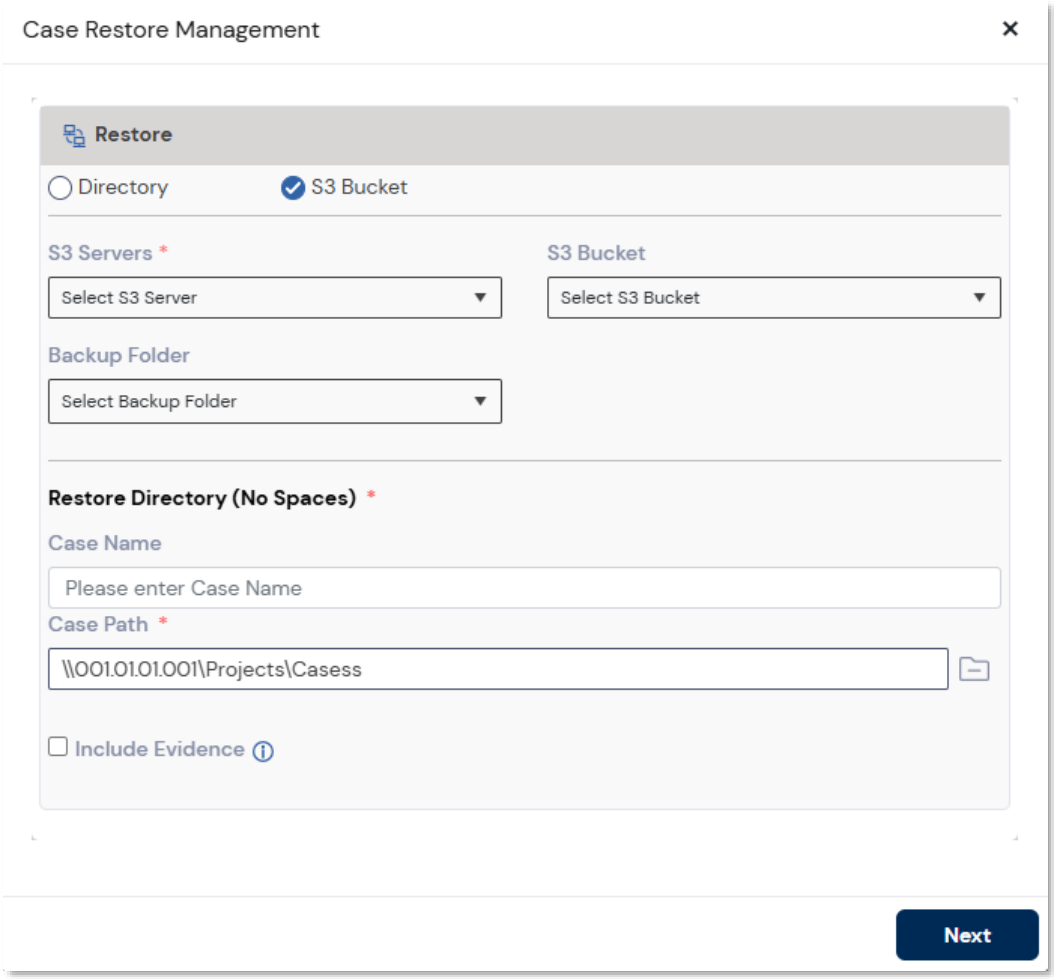
3. Select the **Restore** type.

- **Directory** – To restore the case backed up in the network directory. You can provide the network path in the **Backup Directory** field or click on the **Browse** button against the field to browse and select the path where the case is backed up.



© Exterro, Inc. All rights reserved

- **S3 Bucket** – To restore the case backed up in the AWS S3 location. You can select the **S3 Server, S3 Bucket,** and **Backup Folder** in which the case is backed up.

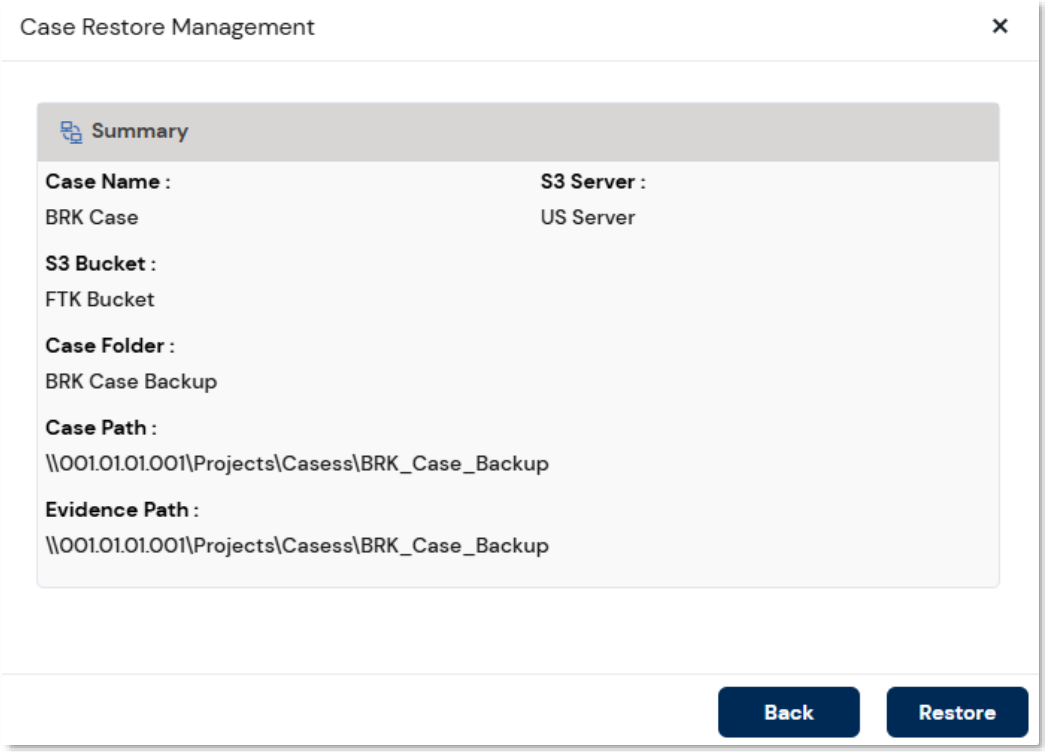


4. The **Case Name** and **Case Path** will be auto populated based on the backed-up case's details. However, you can change it if required.

© Exterro, Inc. All rights reserved

5. Check the **Include Evidence** option if you want to restore the evidence along with the case.
   - Upon checking this option, the **Evidence Path** field is displayed. The value for this field is auto populated based on the backed-up case's details. However, you can change it if required.

6. Click **Next**.
7. The **Summary** of the configurations made will be displayed.



8. Verify the configuration and click on **Restore**.

The restore job will be initiated. You can view its progress in the Job Queue. The selected case will be restored in FTK Central upon successful execution of the job.

© Exterro, Inc. All rights reserved

Viewing Data

Using Review, you can select and examine your data in multiple ways. You can use various panels to examine the data. You use the Panels toggle to select which panel to display.

Elements of Viewing Data

Viewing Documents in the Grid	• File Icons
	• Current File in Viewer
	• Grid Details
	• Selecting Files
	• About the Amount of Data Displayed in Fields
	• Performing Actions in the Grid
	  ○ Productions
	  ○ Additional Analysis
	  ○ DocID
	  ○ Bulk Bookmarking
	  ○ Bulk Labeling
	  ○ Bulk Coding
	  ○ Privileged Files
	  ○ Ignorable Files
	  ○ Bulk Imaging
	  ○ Bulk Native Conversion
	  ○ Export
	  ○ Export to Semantics21
	  ○ Delete
	• Viewing Object Attributes
	  ○ Family
	  ○ Duplicates

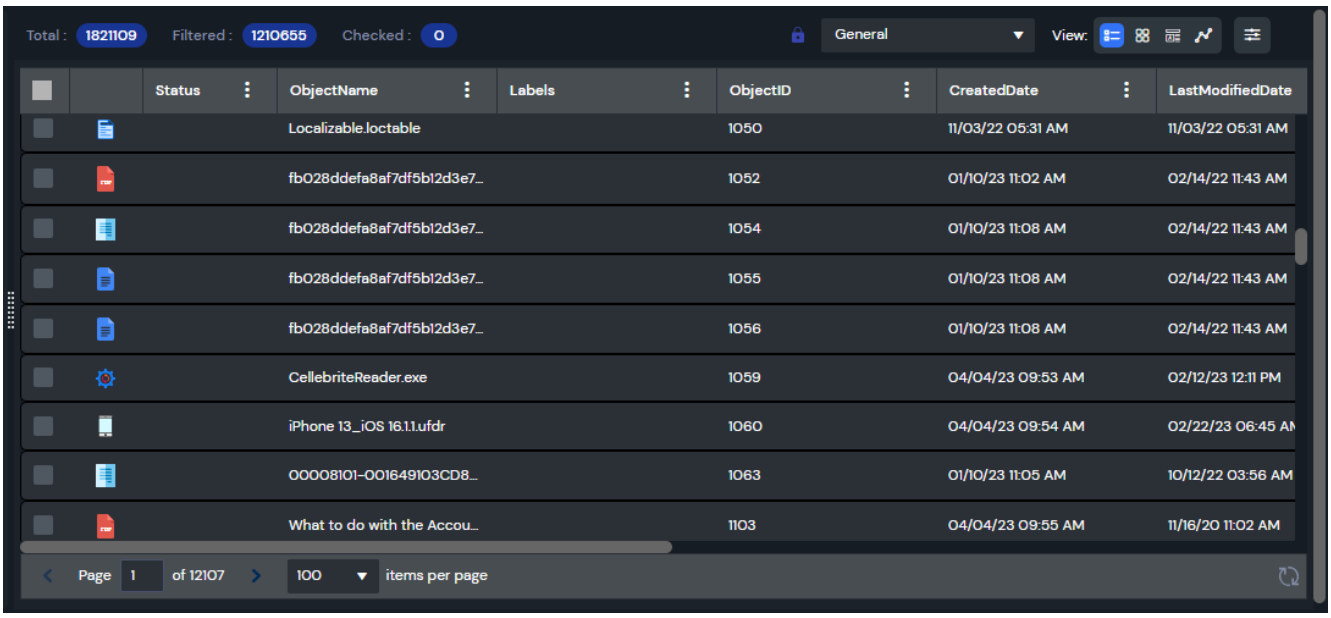
© Exterro, Inc. All rights reserved

	○ MetaData ○ History
Columns	• Using Quick Columns • Provided Quick Columns • Using Custom Columns • Moving Columns in the Grid • Creating Custom Column Sets
Using Views	• Using the Grid View • Using the Thumbnail View ○ Toggling Thumbnail Size
	• Using the Map View ○ Processing Requirements ○ Key Controls ○ Longitude & Latitude ○ Color, Size & Shape ○ Populating Map View with EXIF Data
Using Document Viewing Panels	• Using the Native Panel • Using the Image Panel ○ Buttons and Functions ○ Tabbed Productions ○ Redactions ○ Unitization ○ Restore Original PDF ○ Slip -sheet Maker • Using the Text Panel • Using the MetaData Panel • Using the Desktop Viewer • Using the View Panel on Another Monitor

© Exterro, Inc. All rights reserved

Viewing Documents in the Grid

The Grid panel lists the filtered evidence for a selected case.

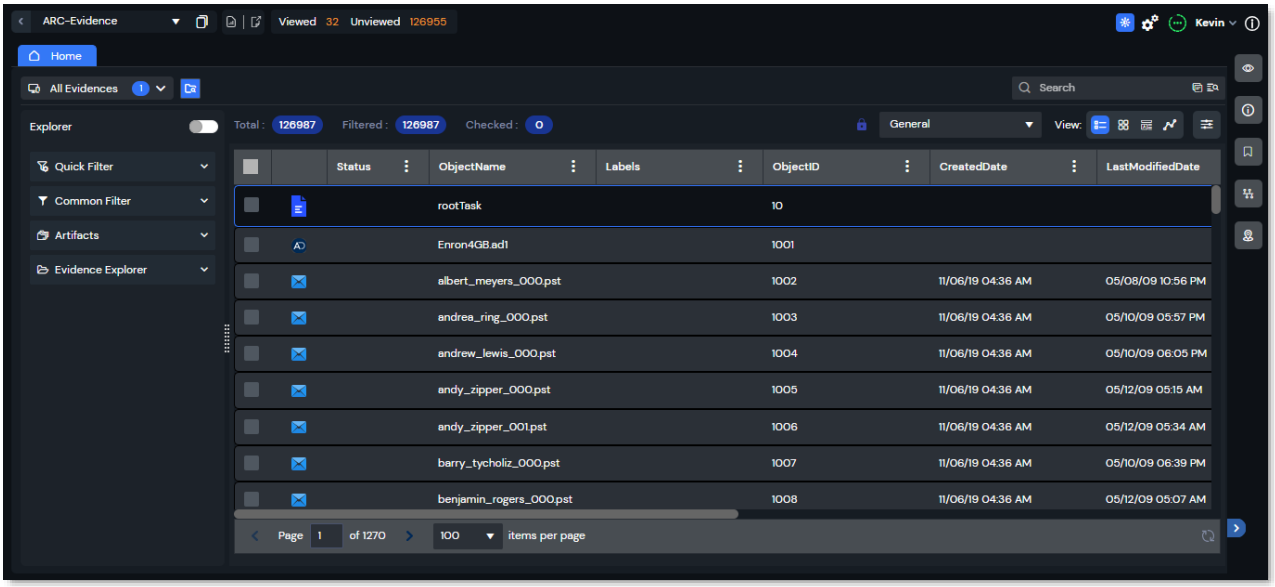


© Exterro, Inc. All rights reserved

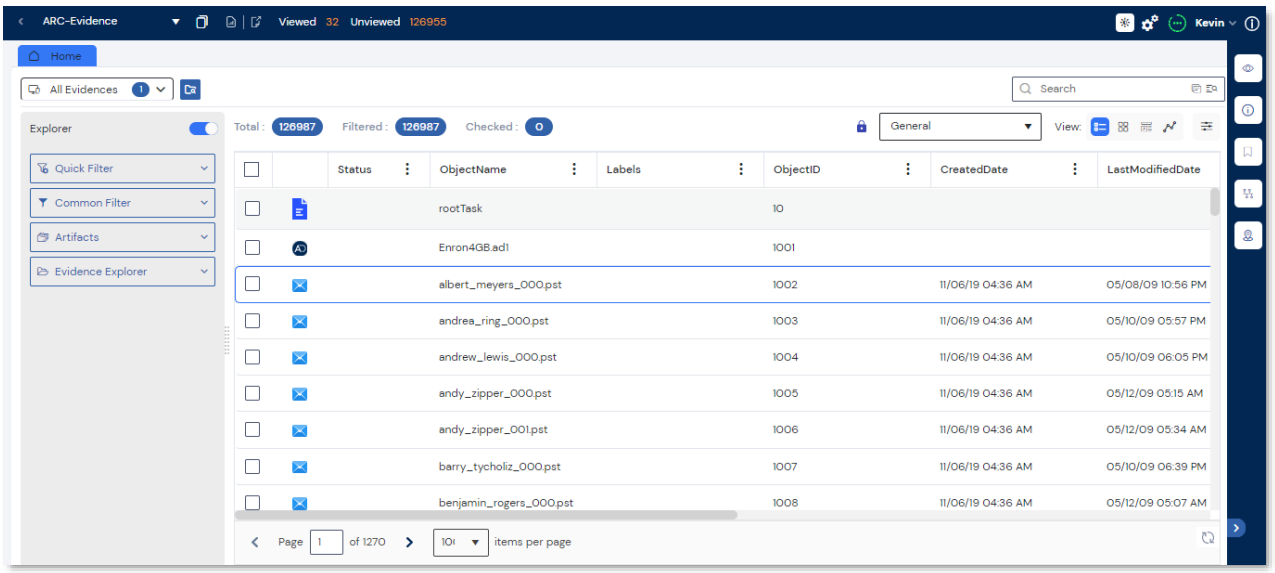
Dark and Light Modes

You can click on or buttons in the top-right corner of the application to access the Light and Dark modes respectively. The Dark mode is enabled by default.

Dark Mode:



Light Mode:



© Exterro, Inc. All rights reserved

File Icons

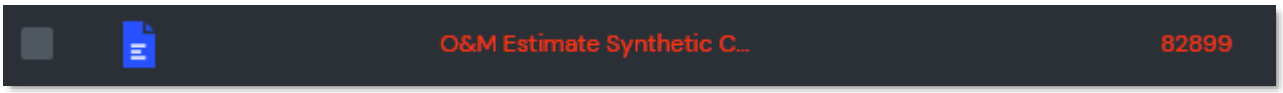
File Types are identified within the file list with icons. Each file type has its own unique file icon to denote what it is.

Note: You can click on the file type icon to download the file in its native format.

File Status

File Statuses are displayed in the grid. Icons are displayed in this column to signal if they are tagged, bookmarked, or deleted items.

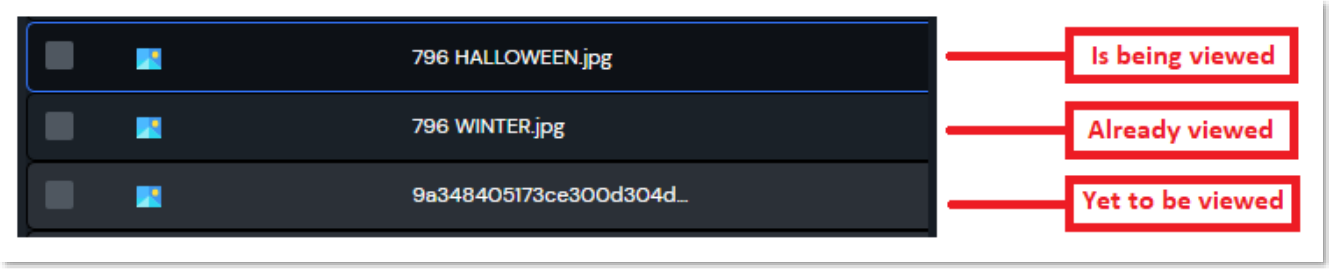
Additionally, the encrypted files in the grid will be highlighted in red.



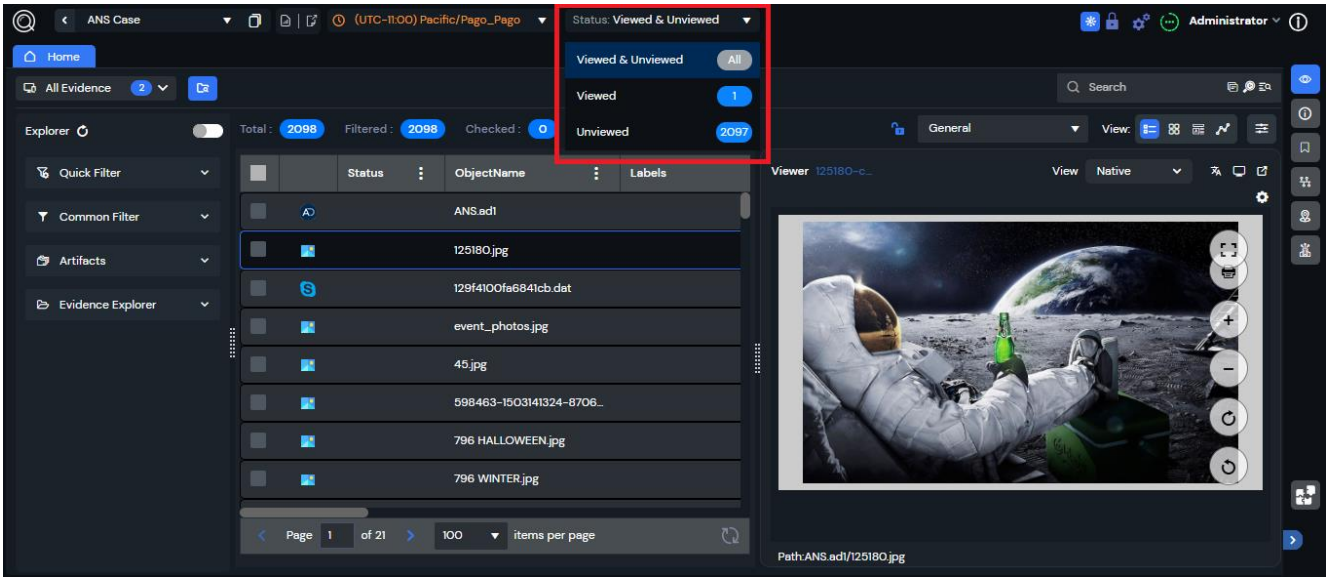
© Exterro, Inc. All rights reserved

Viewed/Unviewed Files

The color codes are differentiated between the viewed and unviewed files in the Item List for easier reference.

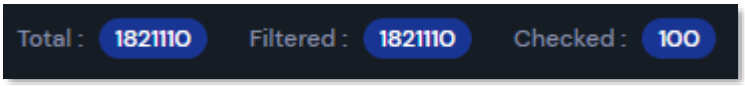


The counts of files that are viewed and unviewed are displayed in the page's header. You can select the required count from the drop-down to filter and view only those files in the Item List.



Grid Details

When using the Grid, the counts for Case Items, Total, Filtered, and Checked Items are displayed at the top of the list.

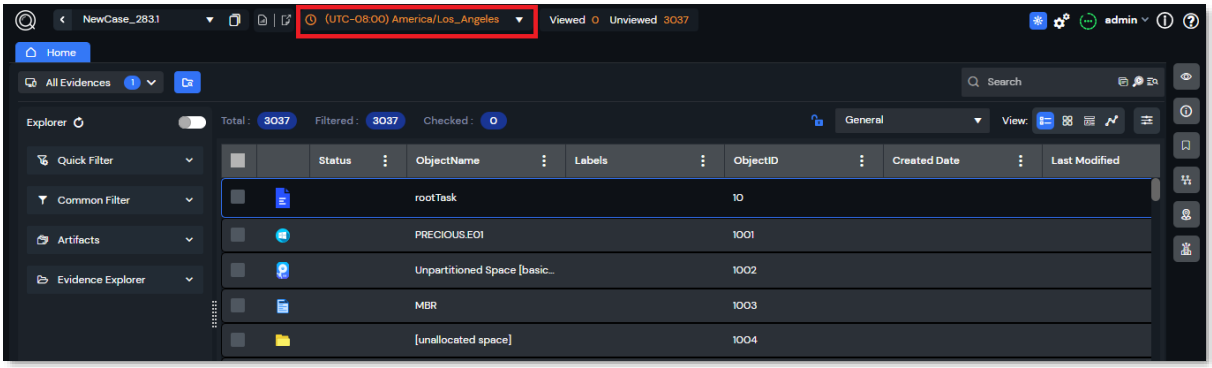


© Exterro, Inc. All rights reserved

Review Page Time Zone

You can now choose to set the required time zone for the Review page. The selected time zone will be reflected only in the Review page and for the user who selected it.

You can perform the action by selecting the required time zone from the drop-down displayed at the top of the Review page.



Notes:

- The time zone selected using this option will not be reflected in the time zone displayed in the Timeline View, which can only be configured at a case level.
- The time zone selected in the Review page will not be changed when the time zone of the case is modified (Edit Case).

© Exterro, Inc. All rights reserved

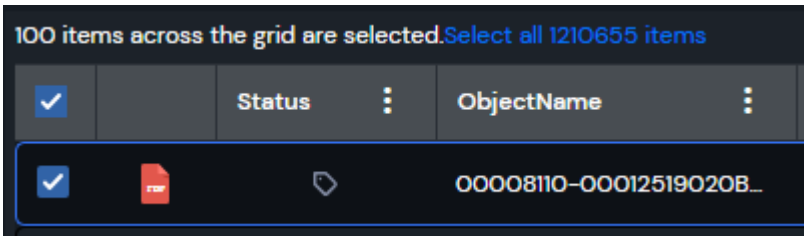
Selecting Files

During review using the Grid, you are able to select files with two methods:

- Select files by checking an item(s) in the file list.
- Select files by clicking on the item in line.

Notes:

- You can hold CTRL while clicking to select multiple files.
- You can select all the files in the list by enabling the checkbox on the column header. Doing so will also provide you an option to select all files in a case.
- The files selected by checking will be retained during the following scenarios:
  - Switching between different cases in the Review page.
  - Navigating to different pages within the application and returning to the Review page.
  - Logging out and logging back into the application and navigating to the Review page.
  - The files checked for a Case in the FTK application will be reflected in the corresponding FTK Central application (Smart View) and vice versa.



© Exterro, Inc. All rights reserved

About the Amount of Data Displayed in Fields

By default, the number of characters that display for a field in the Grid and Coding Panel is limited to 512 characters. Additional characters are truncated.

If fields contain large amounts of data, you may need to remove the column from grid or you can reduce the page size to a smaller size such as 100, 50 or 20 records.

© Exterro, Inc. All rights reserved

Performing Actions in the Grid

During review, you can utilize functions directly from the Grid. These functions range from but not limited to, Productions, Slipsheets and Additional Analysis.

Productions

See Image Panel section.

Creating Productions

To create a production:

1. In the Grid panel, select the records.
2. Right-click on a selected record.
3. Select **Productions** > **Production(s)**.
4. Enter the **Production Name**.
5. Click **Submit Job**.

Restoring Original PDF

To restore original PDF:

1. In the Grid panel, select the records.
2. Right-click on a selected record.
3. Select **Productions** > **Restore Original PDF**.
4. Click **Submit Job**.

Creating a Slipsheet

To create a slipsheet:

1. In the Grid panel, select the records.
2. Right-click on a selected record.
3. Select **Productions** > **Add a Slipsheet**.
4. Enter a **Phrase**.
5. Select the **Metadata**.
6. Click **Submit Job**.

© Exterro, Inc. All rights reserved

Additional Analysis

After evidence has been added to a case and processed, you may wish to perform other analysis tasks. Specific items can also be targeted. Multiple processing tasks can be performed at the same time.

See Creating a Case: Process Evidence.

To perform an additional analysis:

1. In the Grid panel, select the records.
2. Right-click on a selected record.
3. Select **Additional Analysis**.
4. Select any of the below provided **Additional Analysis** processing options:

Processing Options	Description
Optical Character Recognition	To perform OCR on all applicable files. You can configure the setup related to this operation by clicking on the **OCR Options** button. ***Note:*** *You can check the* ***Clear previous OCR*** *option to clear all the text already extracted from the file*
Entity Extraction(Doc. Content)	To specify and extract personal information present in the documents. You can configure the list of entities that should be extracted from the file by clicking on the **EE Options** button.
Language Identification	To identify all the supported languages that are present in the file's content. You can configure the list of languages and the file types that needs to be processed by clicking on the **Language Identification** button.

© Exterro, Inc. All rights reserved

Note: You can choose to run the advanced evidence processing operations for the selected files by clicking on **Customize** and selecting the required processing operations.

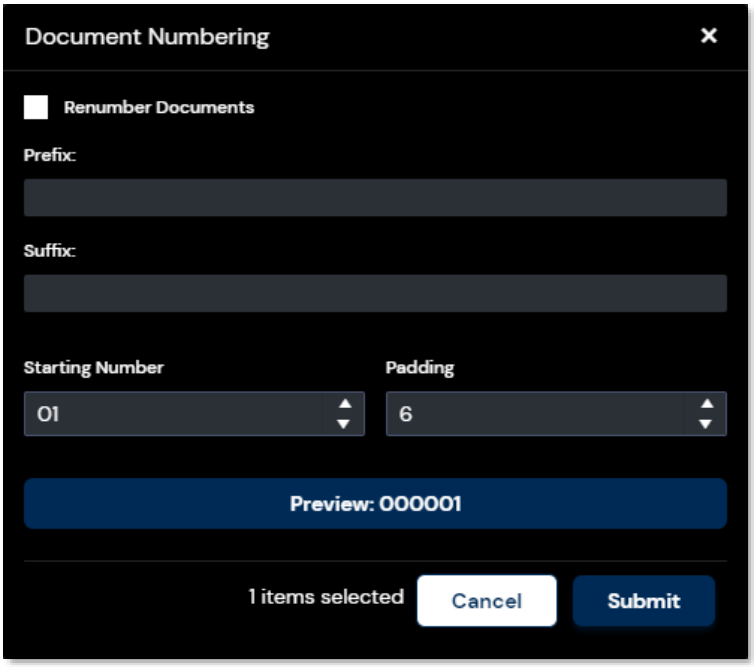
5. Select the specific **Target Items**.
6. Select a **Processing Manager**.
7. Click **Run Analysis**.

© Exterro, Inc. All rights reserved

DocID

To assign a DocID:

1. In the Grid, check a record.
2. Right-click on a selected record.
3. Select **Assign DocID**.
    - The **Document Numbering** prompt is displayed.



Note: You can enable the **Renumber Documents** option to renumber the selected files in order to eliminate gaps and correct incorrect numbering.

© Exterro, Inc. All rights reserved

4. Enter a **Prefix** value for the DocID.
5. Enter a **Suffix** value for the DocID.
6. Enter a **Starting Number**.
7. Enter **Padding** value based on which the zeros will be padded to the starting number.
    - Upon configuring the above values, a preview of configured DocID will be displayed.

Example: If the padding is '1', the starting number will be '01', and if the padding is '2', the starting number will be '001', and so on.

Tip: The **DocID** column can be used during review to easily view documents have been assigned a document ID.

© Exterro, Inc. All rights reserved

Bulk Bookmarking

Refer Working with Bookmarks section.

To apply bulk bookmarking:

1. From the home page, click **Case List**.
2. Select the required case.
3. Click **Enter Review**.
4. Check the required files.
5. Right-click on a checked file.
6. Select **Bulk Bookmarking**.
7. Check the required bookmarks.
8. Select the required options:
    - **No operation** – No changes will be made to the bookmarks.
    - **Assign All Bookmarks** – The bookmarks will be assigned to the selected files.
    - **Un-assign all Bookmarks** – The bookmarks will be unassigned from the selected files.
9. Click **Submit Job**.

© Exterro, Inc. All rights reserved

Bulk Labeling

Refer Working with Labels section.

To apply bulk labeling:

1. From the home page, click **Case List**.
2. Select a case.
3. Click **Enter Review.**
4. Check the required files.
5. Right-click on a checked file.
6. Select **Bulk Labeling**.
7. Check the required labels.
8. Select the required options:
    - **No operation** – No changes will be made to the labels.
    - **Assign All Labels** – The labels will be applied to the selected files.
    - **Un-assign all Labels** - The labels will be unassigned from the selected files.
9. Select the **Additional Options**.
    - **Keep Families Together** - Check to apply the selected label to documents within the same family as the selected documents.
    - **Keep Threads Together** - Check to apply the selected label to all email files related to the selected email file.
    - **Keep Similar Together** - Check to apply the selected bookmark to all documents related to the selected documents.
10. Click **Submit Job**.

© Exterro, Inc. All rights reserved

Bulk Coding

Allows you to apply issues, categories, and other field coding to the selected item. See Coding Panels section.

To perform bulk coding:

1. In the Grid, select the records.
2. Right-click on a selected record.
3. Select **Bulk Coding**.
4. Select the desired Coding Panel using the drop-down list.
5. Enable **Media Category**.
    - Upon enabling this option, a drop-down field is displayed to select the required Media Category option.

6. Select the required options:
    - **No Change** – No changes will be made to the coding.
    - **Assign**– The labels will be applied to the selected coding.
    - **Un-assign** - The labels will be unassigned from the selected coding.

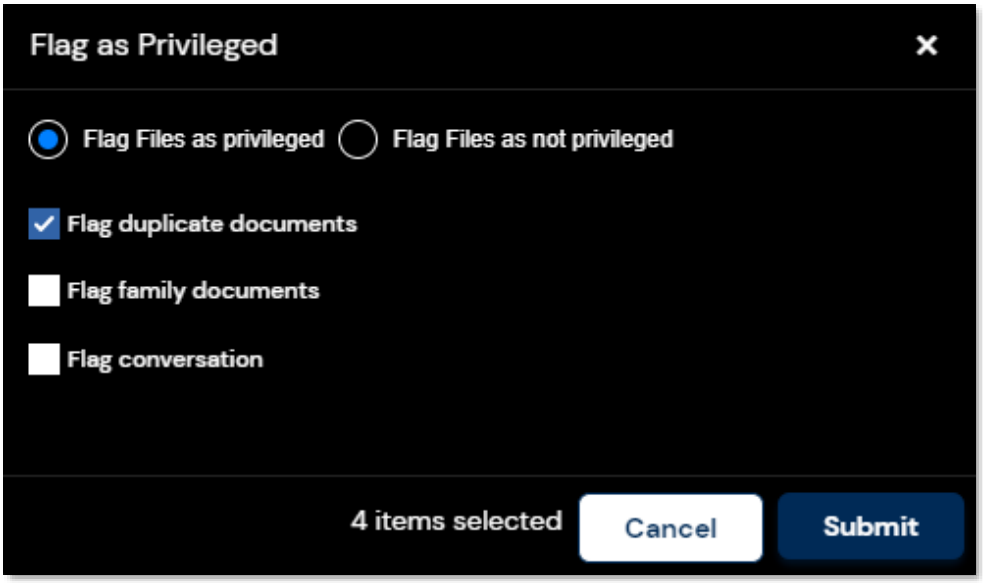
7. Select the **Additional Options**.
    - **Keep Families** - Check to apply the selected coding to documents within the same family as the selected documents.
    - **Keep Threads** - Check to apply the selected coding to all email files related to the selected email file.
    - **Keep Similar** - Check to apply the selected coding to all documents related to the selected documents.
8. Click **Submit Job**.

© Exterro, Inc. All rights reserved

Privileged Files

To flag a file as privileged/not privileged:

1. In the Grid, check a record.
2. Right-click on a selected record.
3. Select **Flag As Privileged**.
    - The **Flag as Privileged** prompt is displayed.



4. Select if the flagged files should be privileged or not.
5. Select the below provided flagging options based on your requirements:
    - **Flag duplicate documents** – Check to apply the selected flag to duplicate documents.
    - **Flag family documents** - Check to apply the selected flag to documents within the same family as the selected documents.
    - **Flag conversation** - Check to apply the selected flag to all emails related to the selected email.
6. Click **Submit**.

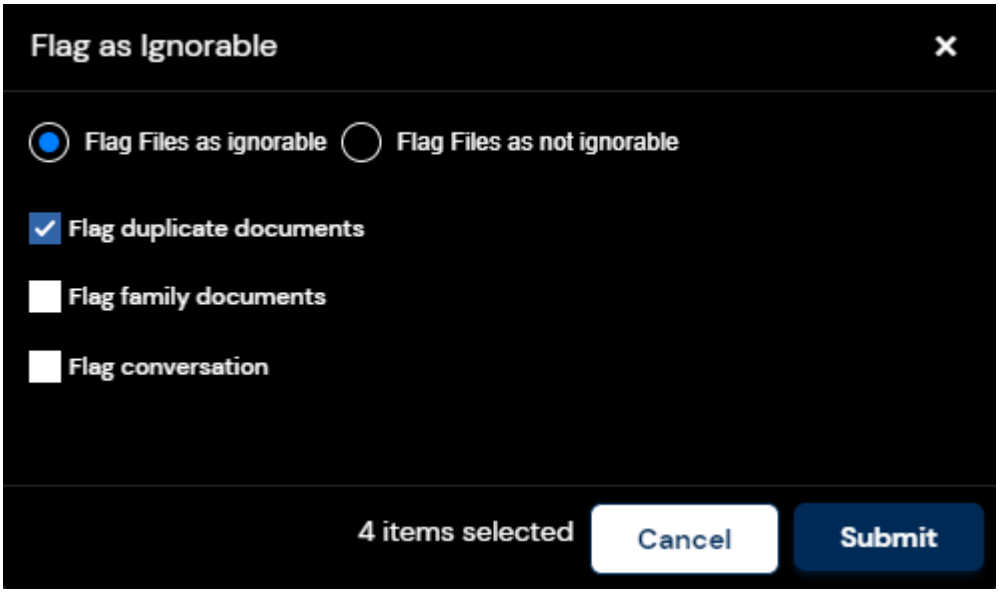
Tip: To classify the files with privileged flag, the **FlaggedPrivileged** column can be used during review.

© Exterro, Inc. All rights reserved

Ignorable Files

To flag a file as ignorable/not ignorable:

1. In the Grid, check a record.
2. Right-click on a selected record.
3. Select **Flag As Ignorable**.
    - The **Flag as Ignorable** prompt is displayed.



4. Select if the flagged files should be ignorable or not.
5. Select the below provided flagging options based on your requirements:
    - **Flag duplicate documents** – Check to apply the selected flag to duplicate documents.
    - **Flag family documents** - Check to apply the selected flag to documents within the same family as the selected documents.
    - **Flag conversation** - Check to apply the selected flag to all emails related to the selected email.

6. Click **Submit**.

Tip: To classify documents with an ignorable flag, the **FlaggedIgnorable** column can be used during review.

© Exterro, Inc. All rights reserved

Bulk Imaging

To perform bulk imaging:

1. In the Grid panel, select the records.
2. Right-click on a selected record.
3. Select **Bulk Imaging**.
4. Select an Image Format.
5. Configure preferences depending on the selected Image Format.
6. Click **Next**.
7. Configure your preferences.
8. Click **Next**.
9. Configure your preferences.
10. Click **Submit Job**.

Bulk Native Conversion

The Imaging process runs automatically when viewing a file in the Image viewer. You can choose to manually run this job for selected/bulk files in advance to make review within the Image viewer faster.

To perform bulk native conversion:

1. In the Grid panel, select the records.
2. Right-click on a selected record.
3. Select **Bulk Native Conversion**.
4. Select **Convert to PDF**.
5. Click **Submit Job**.

© Exterro, Inc. All rights reserved

Download native(s)

To download a file in its native format:

1. In the Grid panel, select the records.
2. Right-click on a selected record.
3. Select **Download native(s)**.

Export to CSV

See Exporting section.

To export data to CSV:

1. In the Grid panel, select the records.
2. Right-click on a selected record.
3. Select **Export to CSV**.

Export Media Categories

To export to media categories:

1. In the Grid, select the records.
2. Right-click on the selected record.
3. Select the required **Export media categories**.
4. Provide the **Export Path** where the files should be exported.
5. Select **Include Media** if the selected records need to be exported in native format.
6. Provide the **Project Vic Case Number.**

Note: Enabling the checkbox against the **Project Vic Case Number** field will allow you to enter the case number without having to select it from the drop-down.

7. Provide the **Contact Name**.
8. Provide the **Contact Title**.
9. Provide the **Contact Phone**.
10. Provide the **Contact Email**.
11. Provide the **Contact Organization**.
12. Click on **Submit Job**.

© Exterro, Inc. All rights reserved

Export to Semantics21

To export to Semantics21:

Note: This option allows users to export relevant data in JSON format which can be seamlessly ingested into Semantics21. The option to reimport (after classification) into FTK Central will be available in a future release.

1. In the Grid, select the records.
2. Right-click on the selected record.
3. Select **Export to Semantics21** > **All Checked/All Filtered**.
4. Select **Include Media** if the selected records need to be exported in native format.
5. Enter an **Export Path**.
6. Enter a **File Name** (JSON file).
7. Click **Export**.

Delete

Warning: The Delete option is applicable only when the value for **Product Type** is set as **Ediscovery** in the App config file.

To delete the files:

1. In the Grid, select the records.
2. Right-click on the selected record.
3. Click on **Delete**.
4. From the **Delete Objects** pop-up, select whether the corresponding family files should be deleted as well (**Include Family** or **Don't Include Family** option).
5. Click **Submit**.

© Exterro, Inc. All rights reserved

Columns

Using Quick Columns

You use columns to display specific data properties about evidence items. You can sort, filter, customize, and reposition the columns of information in the Grid pane. There are many pre-configured fields that you can display as columns.

To use quick column:

1. In the Grid, click the **Columns** drop-down list**.**
2. Click on any of the provided quick columns.
3. The column changes will be made immediately in the Grid.

Tip: By default, the file type filters will have automatic columns assigned when toggled. This option can be turned off by toggling the **padlock** button.

© Exterro, Inc. All rights reserved

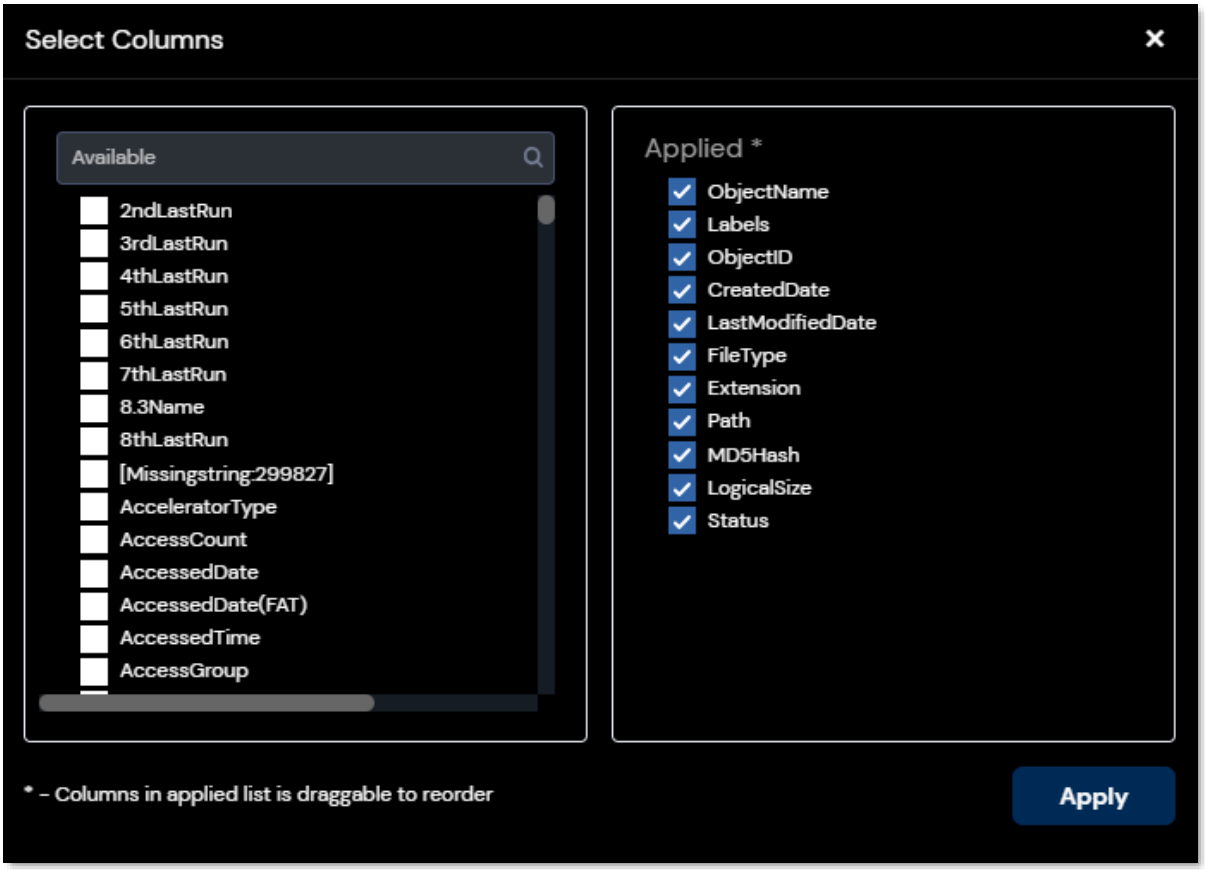
Provided Quick Columns

You can refer to the Default Columns KB article.

Using Custom Columns

To use custom column:

1. In the Grid, click the **Columns** drop-down list**.**
2. Click on **Select**.
3. Select the required columns by checking them.



4. Click **Apply**.

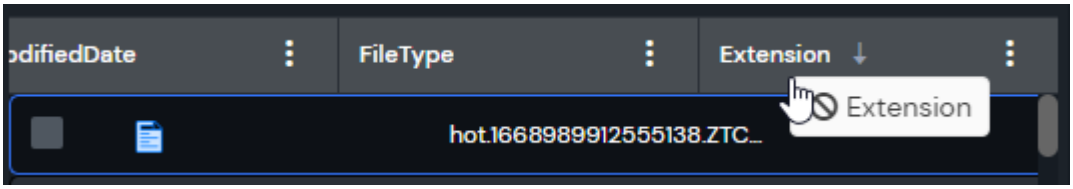
The columns will now update in the Grid.

© Exterro, Inc. All rights reserved

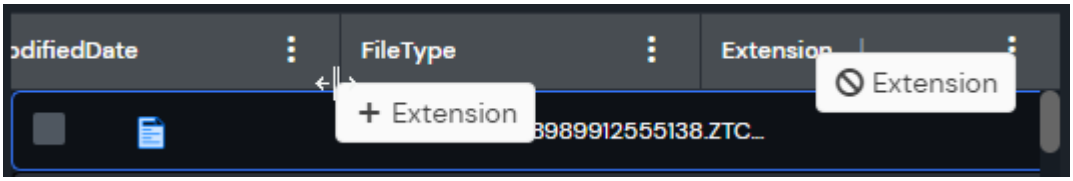
Moving Columns in the Grid

To move column in Grid:

1. In the Grid, find the column that you would like to move.
2. Click and hold.



3. Drag this column where you would like to move it to.
   - You will notice a marker where the column is being held against.



4. Unclick to set the column in place.

© Exterro, Inc. All rights reserved

Using Views

You can use different pre-configured views to help you review data.

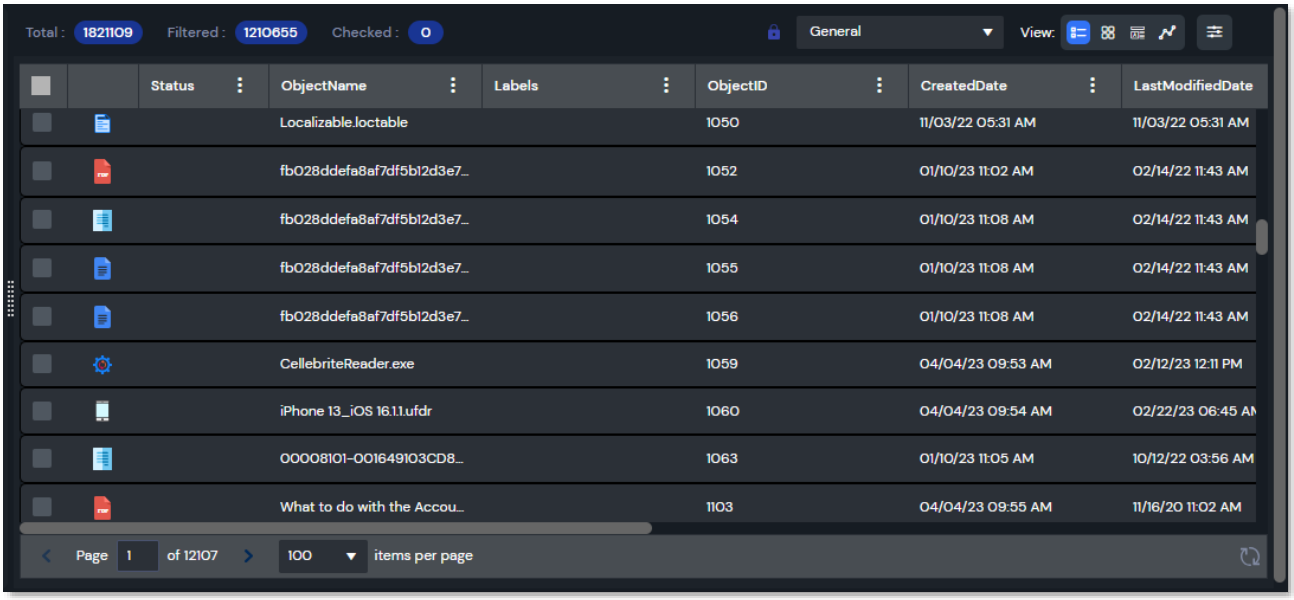
- - See Using the List Viewer section.
- - See Using the Thumbnail Viewer section.
- - See Using the Smart Grid Viewer section.
- - See Using the Timeline Viewer section.

Note: Whenever you change views, the File List is refreshed.

© Exterro, Inc. All rights reserved

Using the List View

The List View displays all objects in a case with the relevant metadata columns automatically applied.



Note: You can click on the **Refresh** icon to load the updated file list.

Tip: The 'Files List' section supports nested sorting options for multi-column sorting. While doing so, the headers of the sorted columns will be numbered based on the sorting hierarchy

© Exterro, Inc. All rights reserved

Using the Thumbnail View

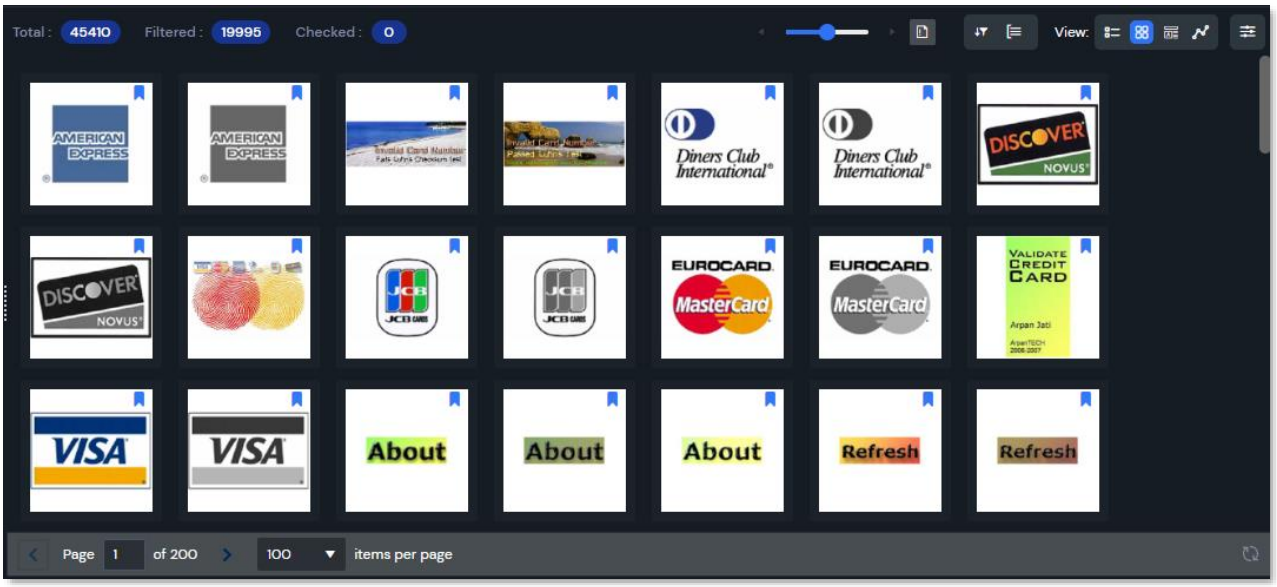
The Thumbnail View allows you to see rows of thumbnail images of the graphic files or video files in your case. While you can view thumbnails, bulk operations can be run using the right-click context menu. You can double click on the file to view the file's content in **Native** view.

Additionally, multiple thumbnails can be selected using keyboard shortcuts:

- **CTRL + A** can be used to select all visible thumbnails.
- **CTRL + Clicking** can be used to select specific thumbnails.
- **SHIFT + Clicking** can be used to select all thumbnails between two thumbnails.

Click on **Thumbnail View** to access this view.

Note: Image thumbnails are generated only when choosing the processing option: **Generate Image Thumbnails**.

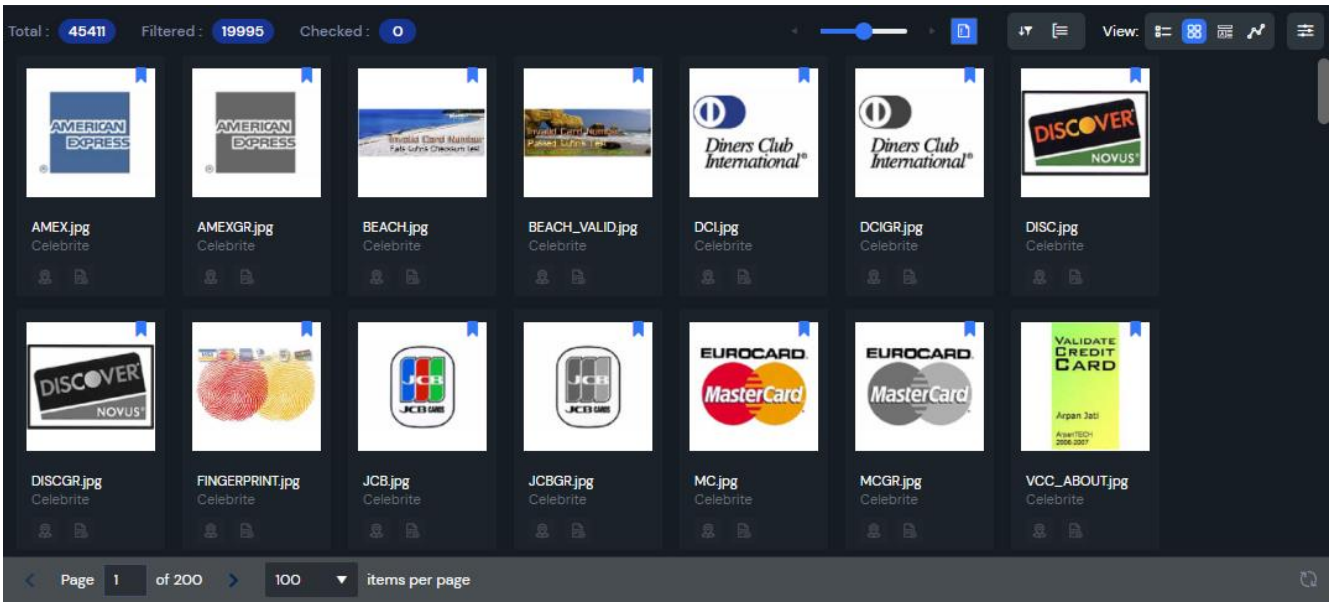


Notes: The Thumbnail view is applicable only to images and videos. A blank thumbnail will be displayed for any other filetypes.

© Exterro, Inc. All rights reserved

Thumbnails Info

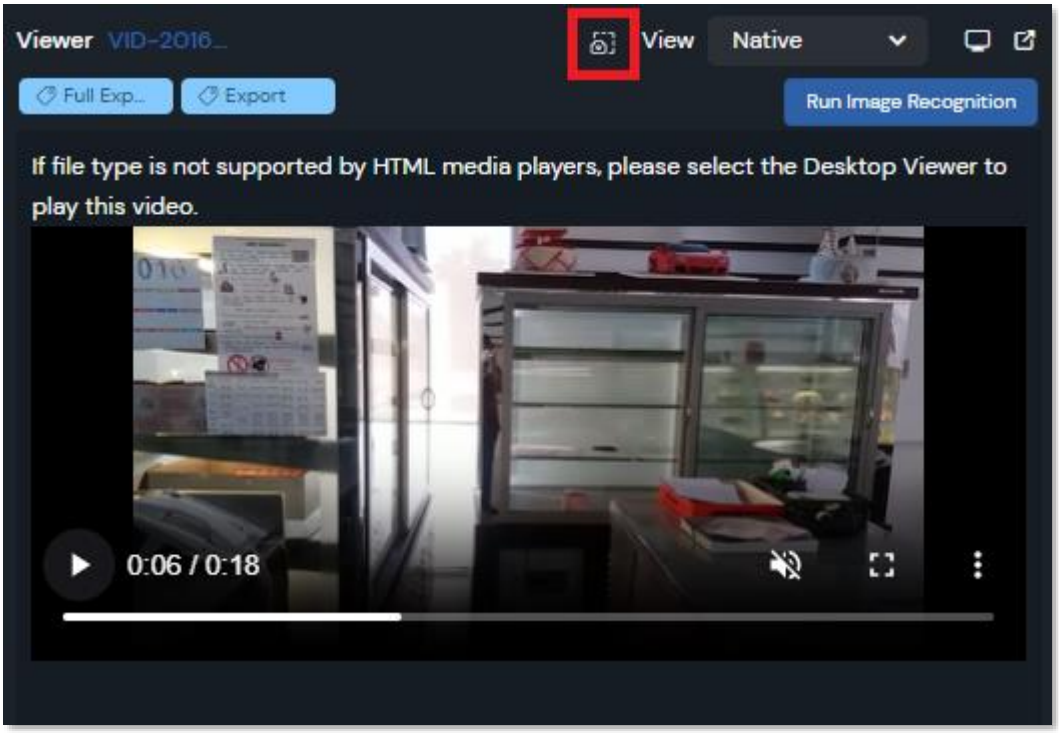
You can view the thumbnails of the files along with the corresponding details, click on the **Show Thumbnail Info** button.



© Exterro, Inc. All rights reserved

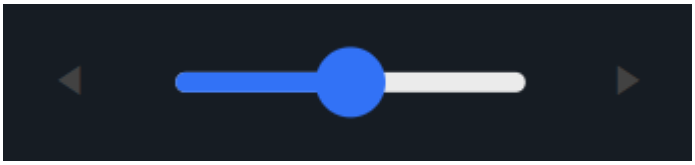
Custom Thumbnail

You can set custom thumbnails for the videos displayed in the 'Thumbnail View'. This action can be performed by pausing the video at the required moment in the viewer and clicking on the **Capture Thumbnail** button.



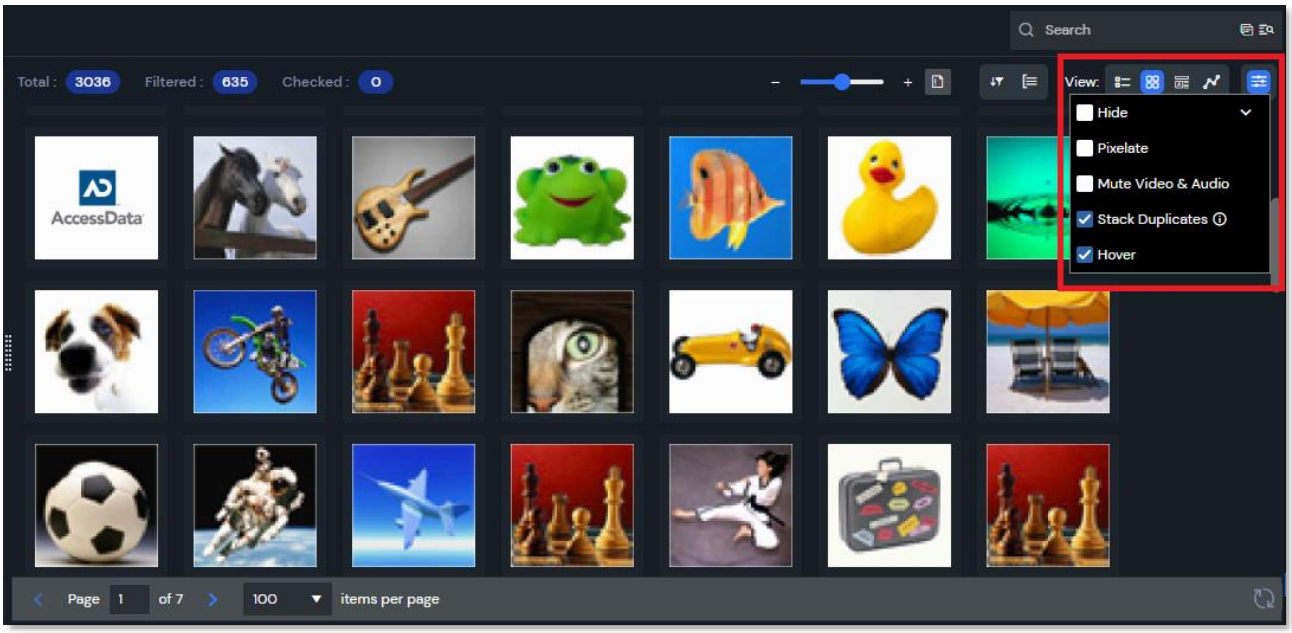
Toggling Thumbnail Size

You can resize the Thumbnails by adjusting the Thumbnail Size bar.



© Exterro, Inc. All rights reserved

Thumbnail Settings



You can click on the **Thumbnail Settings** button to access and make use of the following options:

Option	Description
Hide	To hide the objects that are viewed or tagged. **Note:** This feature is also applicable to the List View and Smart Grid View as well.
Pixelate	To automatically pixelate the images that are categorized using CAID/VIC.
Mute Video & Audio	To automatically mute the sound when the multimedia objects are opened in Viewer.
Stack Duplicates	To stack the duplicate objects based on the Hash values.

© Exterro, Inc. All rights reserved

Option	Description
Hover	Hover over the required file in the 'Thumbnail View' to view the enlarged version of the thumbnail image (of multimedia files) along with the below details: • Object Name • EXIF image model • Location of the file (If available)

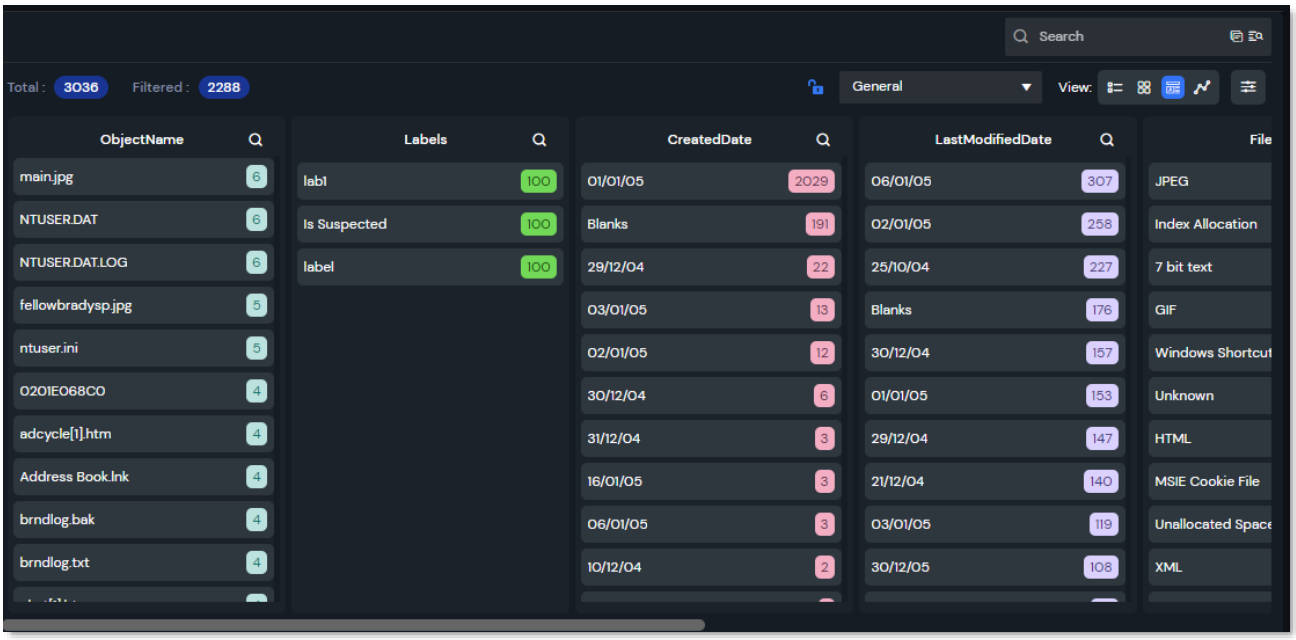
Note: The following options selected for the thumbnail view will be automatically saved and retained across sessions:

- Hide Thumbnails
- Pixelate Thumbnails
- Mute Video & Audio
- Stack Duplicates
- Hover to Preview
- Show Thumbnail Info
- Thumbnail Size

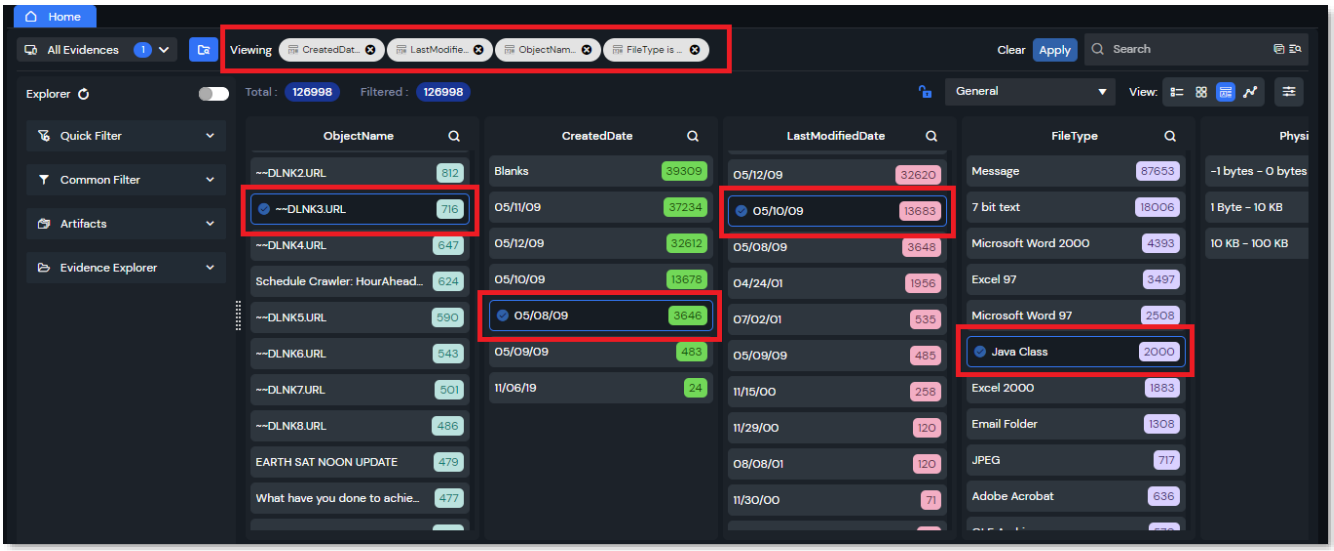
© Exterro, Inc. All rights reserved

Using the Smart Grid View

Smart Grid View in the Exterro FTK Central application automatically groups all the metadata values and displays them in corresponding columns for easier filtering and reviewing purposes.

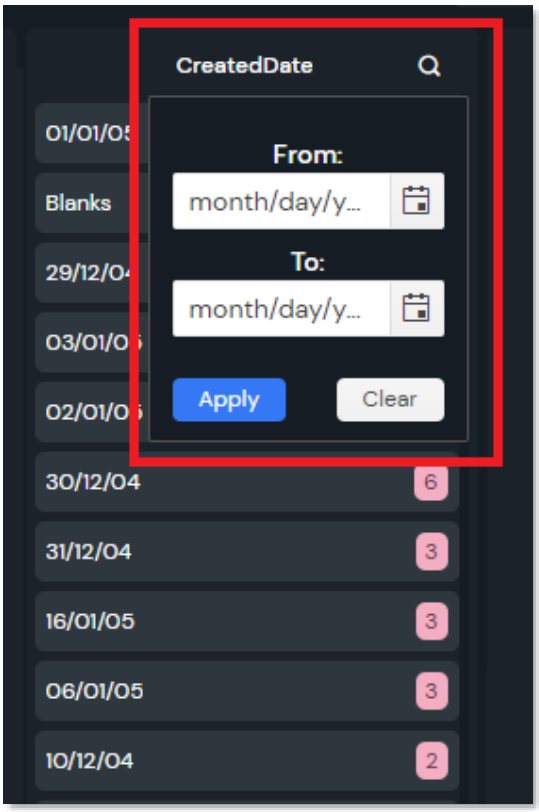


All the file metadata details are categorized in multiple scrolling grids. You simply need to click and select all the values required to form a filter query and click on Apply to view the resulting set of files.



© Exterro, Inc. All rights reserved

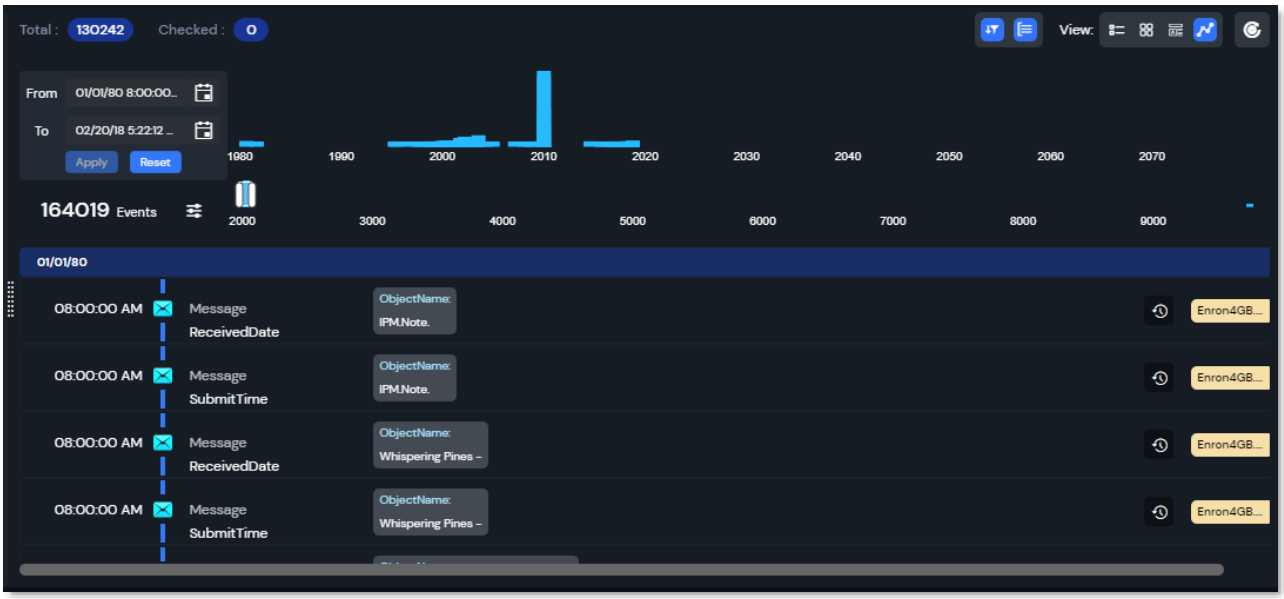
Moreover, you click on against the required column's header to filter values of each column.



© Exterro, Inc. All rights reserved

Using the Timeline View

In the Timeline View, all the files in the evidence are categorized based on its date and time within the specified range.



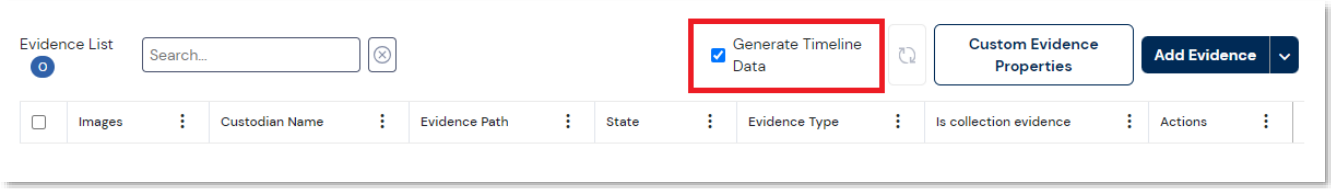
© Exterro, Inc. All rights reserved

Generating Timeline Data

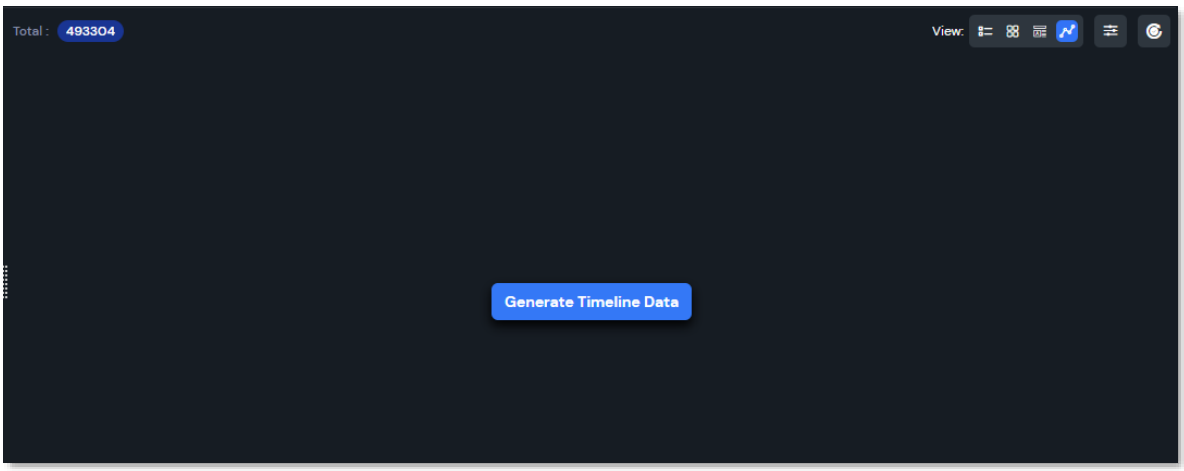
To generate the timeline data:

You can generate the timeline data using any of the following methods:

- You can automatically generate the Timeline data for the case files by enabling the **Generate Timeline Data** option (in the Process Evidence section) while creating a case.

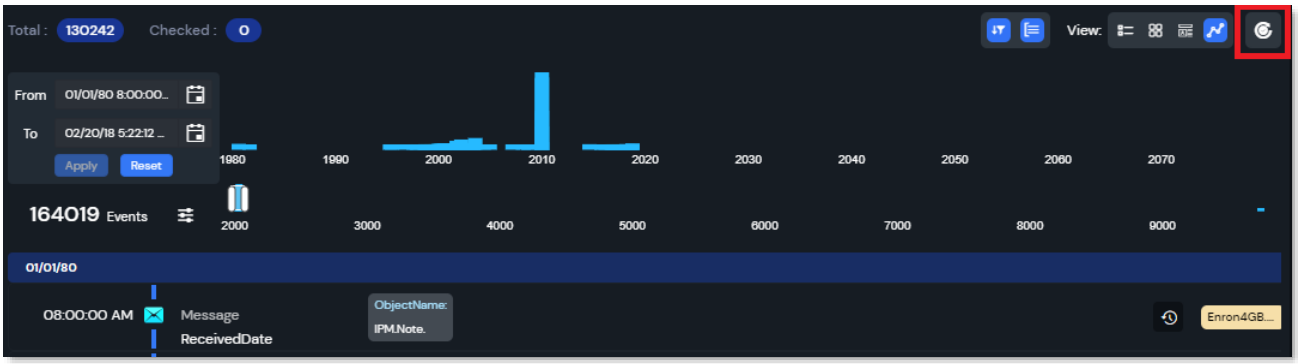


- When the **Timeline** view is not automatically generated (during case creation), click on the **Generate Time Data** button.



© Exterro, Inc. All rights reserved

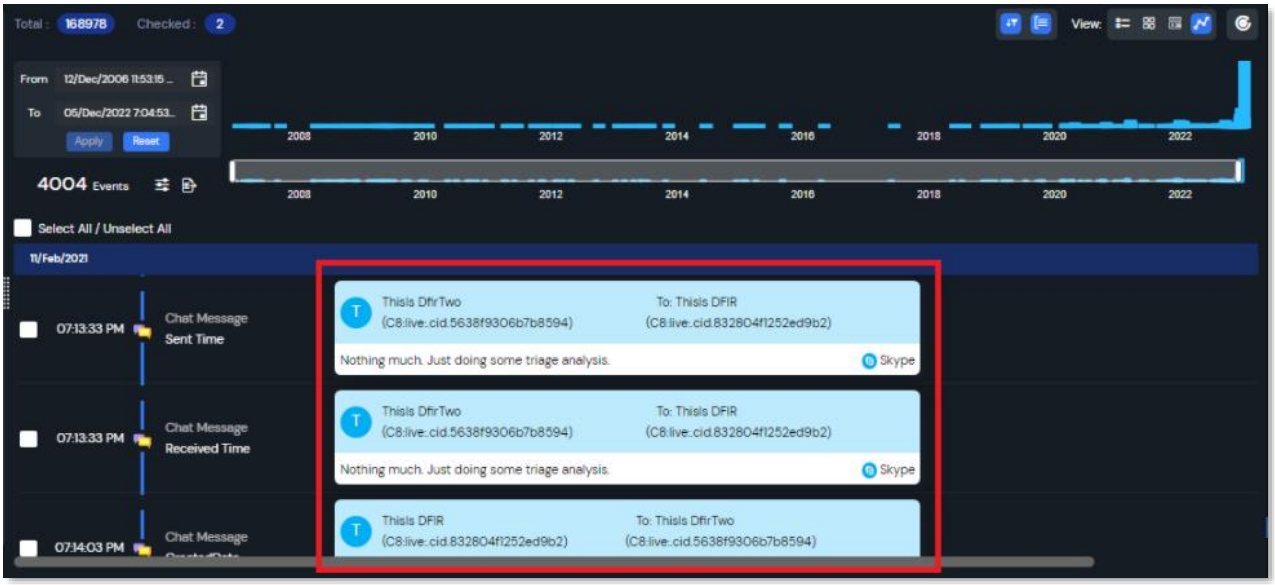
- When the timeline data is already generated, you can click on the **Generate Timeline Data** button from the top-right corner of the **Timeline** view.



© Exterro, Inc. All rights reserved

Notes: The user interface of the chats displayed in the Timeline View is a bit different compared to the other file types. This is made to provide you with the following details about the chat in this view for easier reviewing purposes:

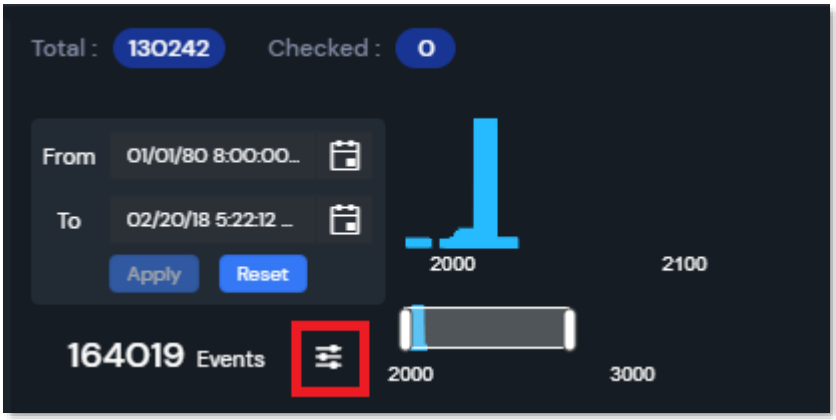
- Message Sender
- Message Recipient
- Message Body
- Source Application
- Attachments



© Exterro, Inc. All rights reserved

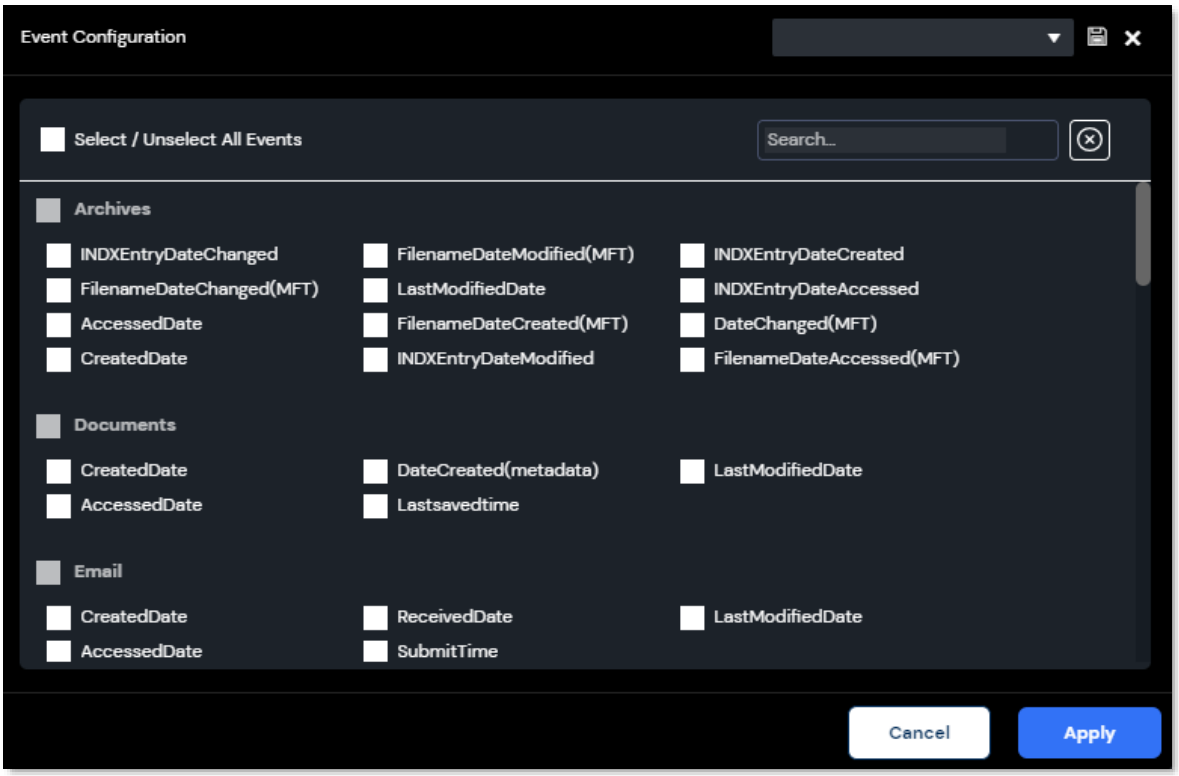
Event Configuration:

Instead of displaying all event updates made for a file, you can choose to filter out the required set of events using **Event Configuration**.



© Exterro, Inc. All rights reserved

You can configure the events by clicking on and selecting the required events from the **Event Configuration** pop-up.



Notes:

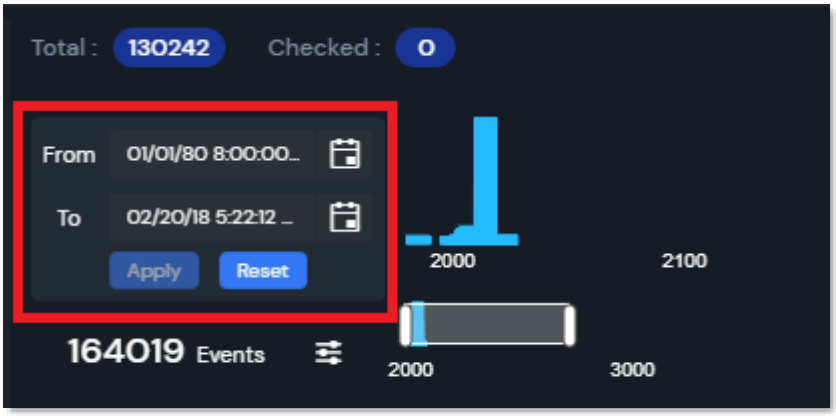
- You can save the events selected intended to be used later by clicking on the **Save New** button in the top-right corner of the **Event Configuration** pop-up.
- The saved event configurations can be access from the drop-down field in the top-right corner of the **Event Configuration** pop-up.

© Exterro, Inc. All rights reserved

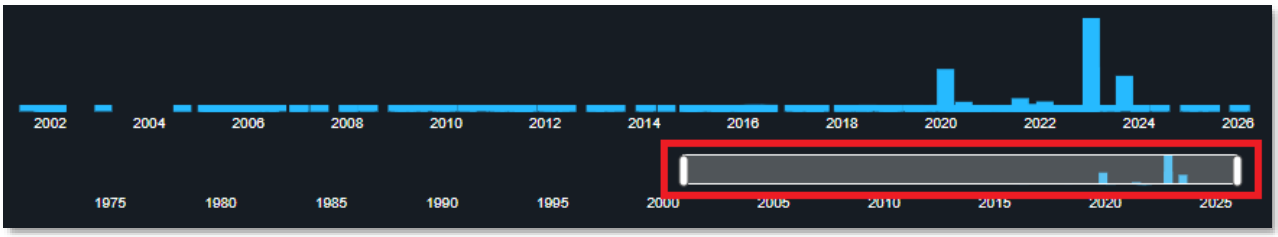
Filtering the file events based on Timeline:

You can specify the date range to in the Timeline View to filter and view only the corresponding set of files. You can do so, by any of the following methods:

- Configuring the **From** and **To** date fields and click on **Appy**:



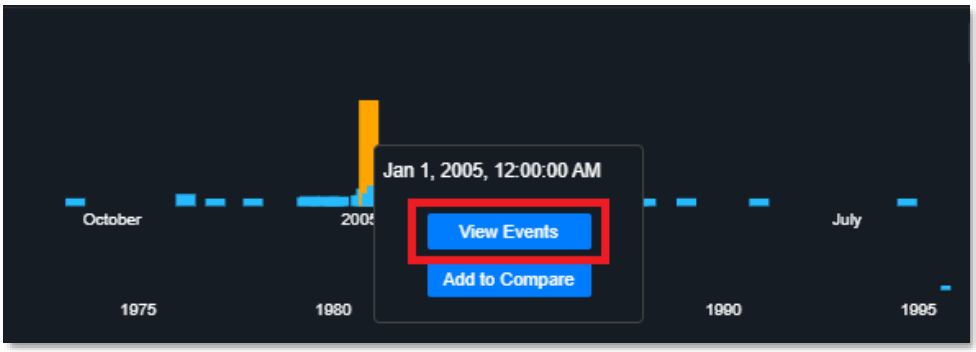
- Adjusting the timeline bar by clicking and dragging the indicators:



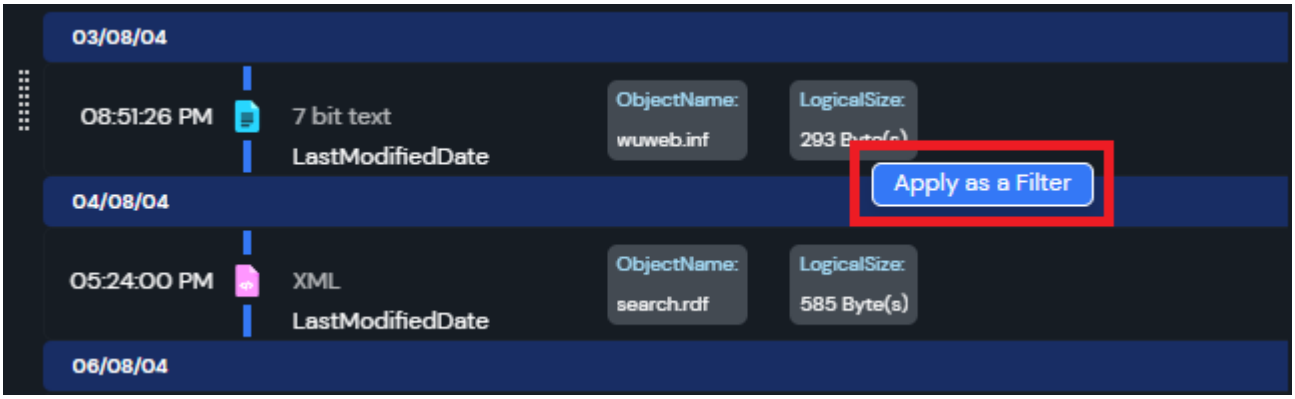
Note: You can click on the **Reset** button to reset the timeline filters applied.

© Exterro, Inc. All rights reserved

- Click on the specific bar graph and select **View Events**.



- Click on any of the events from the list and select **Apply as a Filter** to filter and view all the files with the same event value.

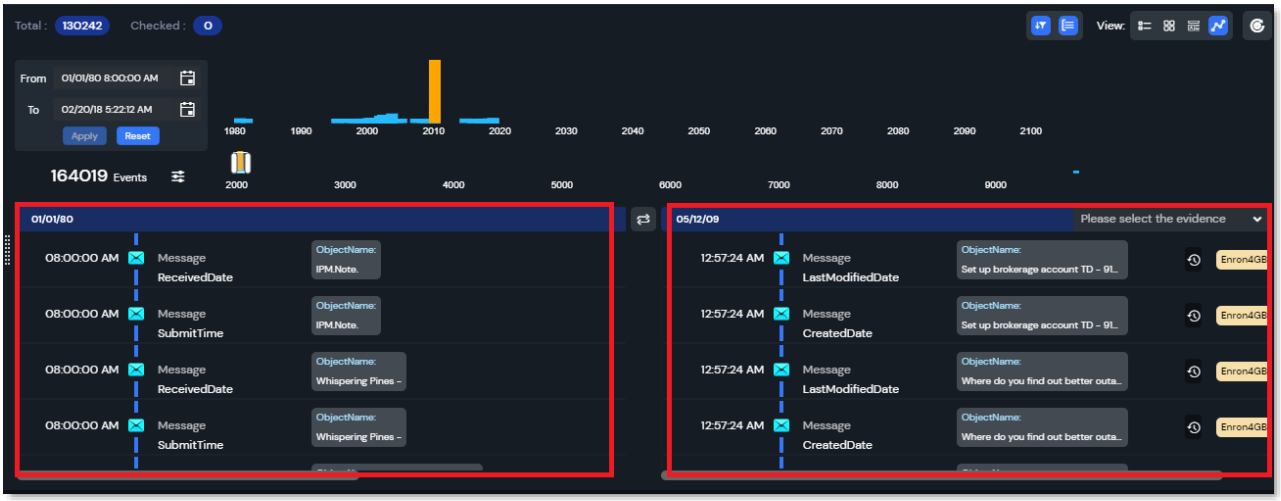


© Exterro, Inc. All rights reserved

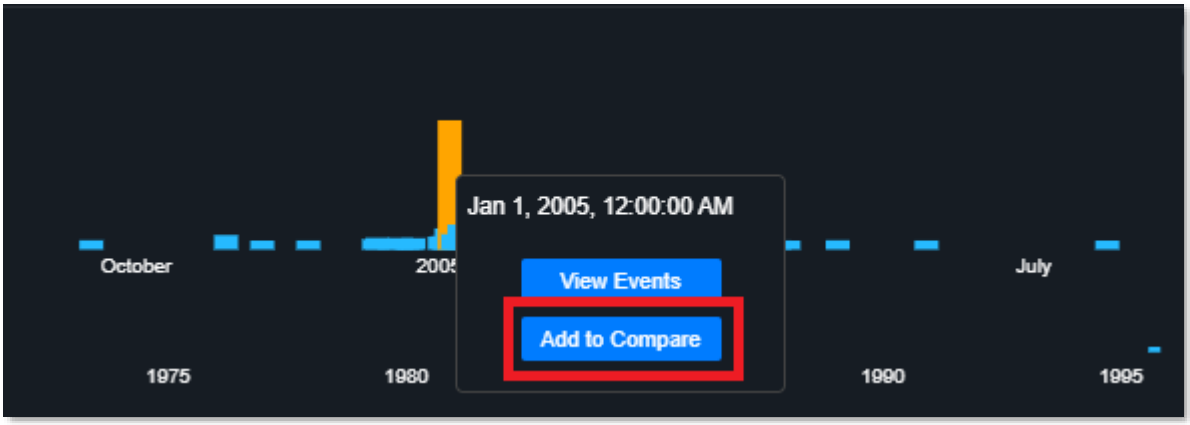
Comparing the File Events

To compare the file events based on Timeline:

You can compare the file list filtered using two different timelines and compare them for your reviewing purpose.



To perform the action, click on any of the bar graphs from the timeline and select **Add to Compare**.

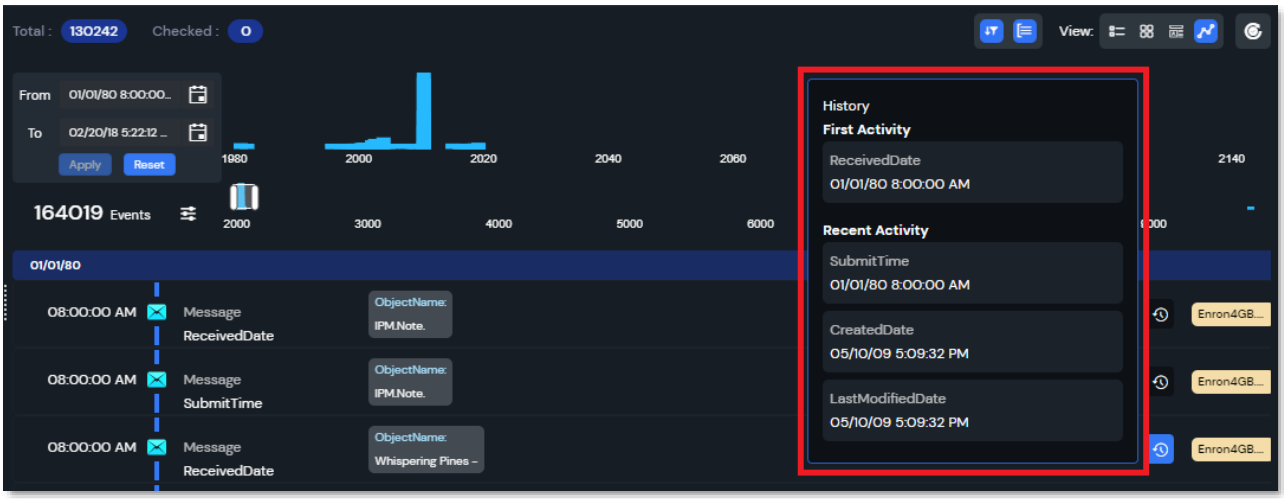


Note: During the comparison, you can click on the Sync scroll button to synchronize the scrolling between the two file lists.

© Exterro, Inc. All rights reserved

Document History

You can view the document's history i.e., the date and time when the changes, updates, or modifications were made to the file by clicking on the **History** button against the required document.



Exporting the Timeline File Events

To export the Timeline events:

You can export the required events from the **Timeline View** by following the below steps:

1. Select the required events from the Timeline View
2. Right-click and select the **Export to Excel** option.
3. Select any one of the below options to perform the operation:

- **Download without Native Files** - To generate the report consisting of all timeline event details in XLSX format.
- **Include Native Files** - To download a ZIP file consisting of the XLSX report along with all the native files. You can click the hyperlinks from the report to view the corresponding native file.

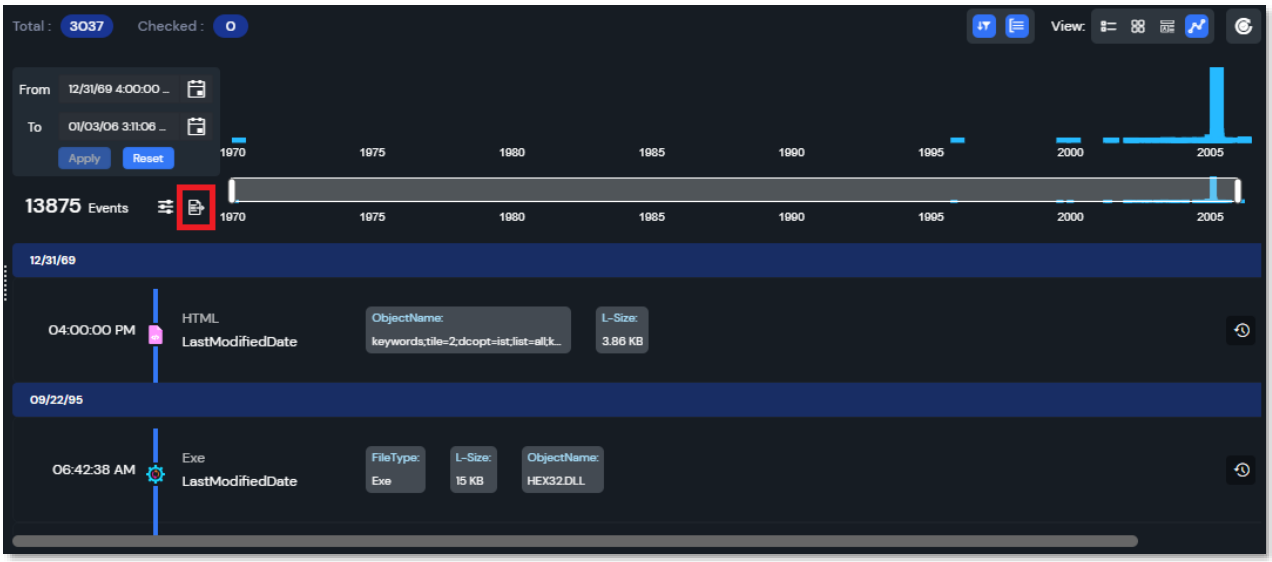
© Exterro, Inc. All rights reserved

Generating the Timeline Report

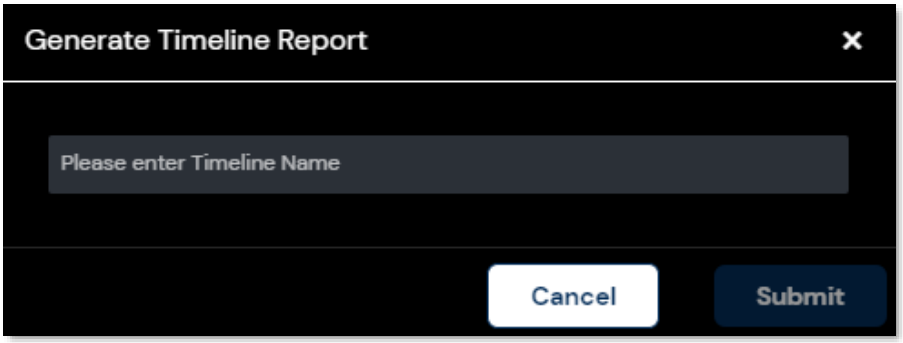
To generate the Timeline Report:

You can generate the entire timeline events as a report by following the below steps:

1. Click on the **Generate timeline report** button.



- The **Generate Timeline Report** pop-up is displayed.



2. Enter the **Timeline Name** and click on **Submit**.

A job will be initiated to generate the report. Upon job completion, you can download the report from the Job Queue.

© Exterro, Inc. All rights reserved

Viewing the Panels

FTK Central consists of the following types of panels intended to provide users with wide range of options and features to effectively filter and view the specific sets of data for reviewing:

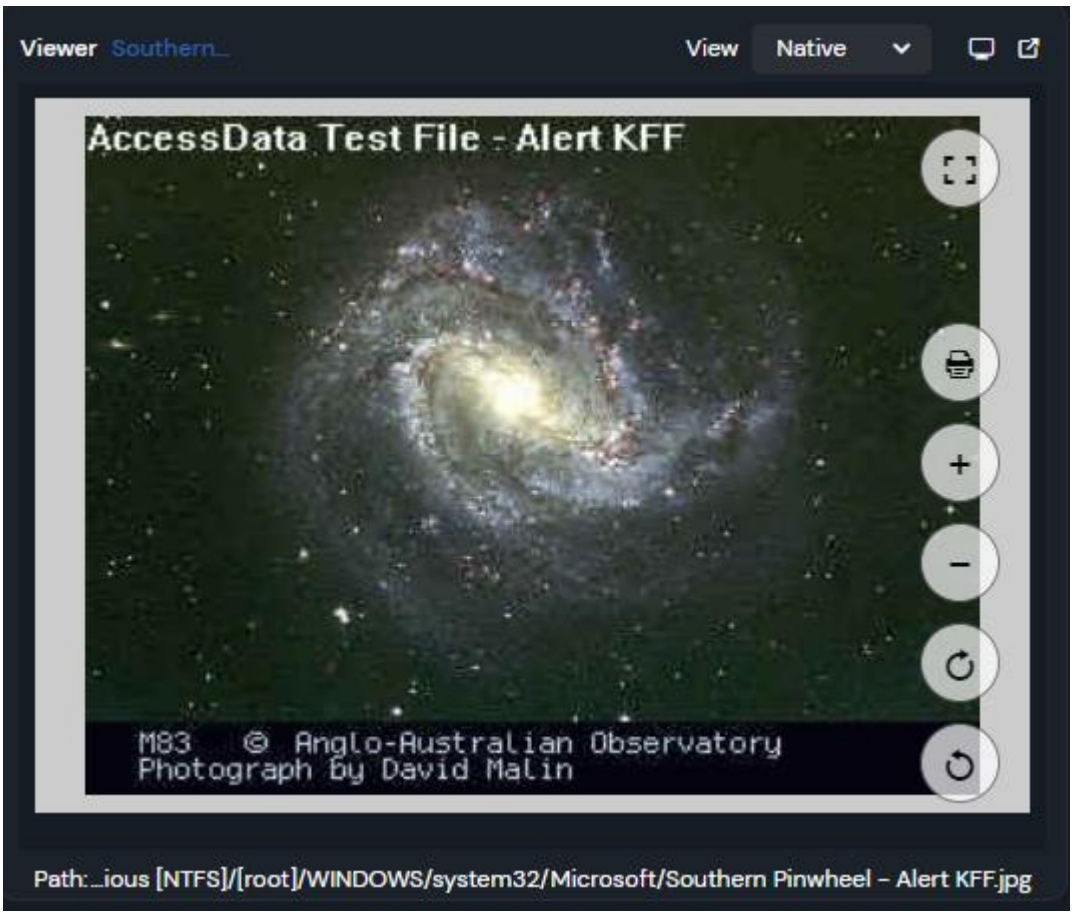
- Viewer
- Info
- Tags
- Mini Timeline
- Maps

© Exterro, Inc. All rights reserved

Viewer

This viewer displays the file's content in its **Native**, **Image**, or **Text** format.

You can open this viewer by double clicking on the file in the item list or click on



Note: You can click on the **Pop Out** button to open the viewer in a new pop-up.

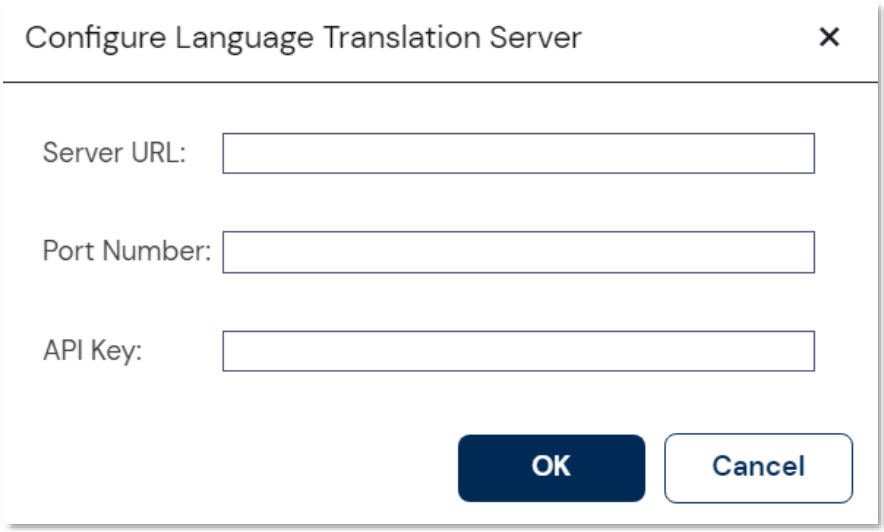
Refer the Using Document Viewing Panels section for detailed information on the **Viewer** panel.

© Exterro, Inc. All rights reserved

Language Translation

You can translate the content of the file displayed in the viewer by following the below steps:

1. Click on **Configure Translation Server** from the viewer.
   - The **Configure Language Translation Server** pop-up is displayed.



2. Provide the following information:
   - Server URL
   - Port Number
   - API Key

3. Upon configuring the server details, click on the **Translate** button to translate the file's content to English.

Note: The **Translate** button will be enabled only for the file types supported for language translation in FTK Central

A job will be initiated to perform the translation. You can view the translated version of the file from the **Translated** view.

© Exterro, Inc. All rights reserved

Info

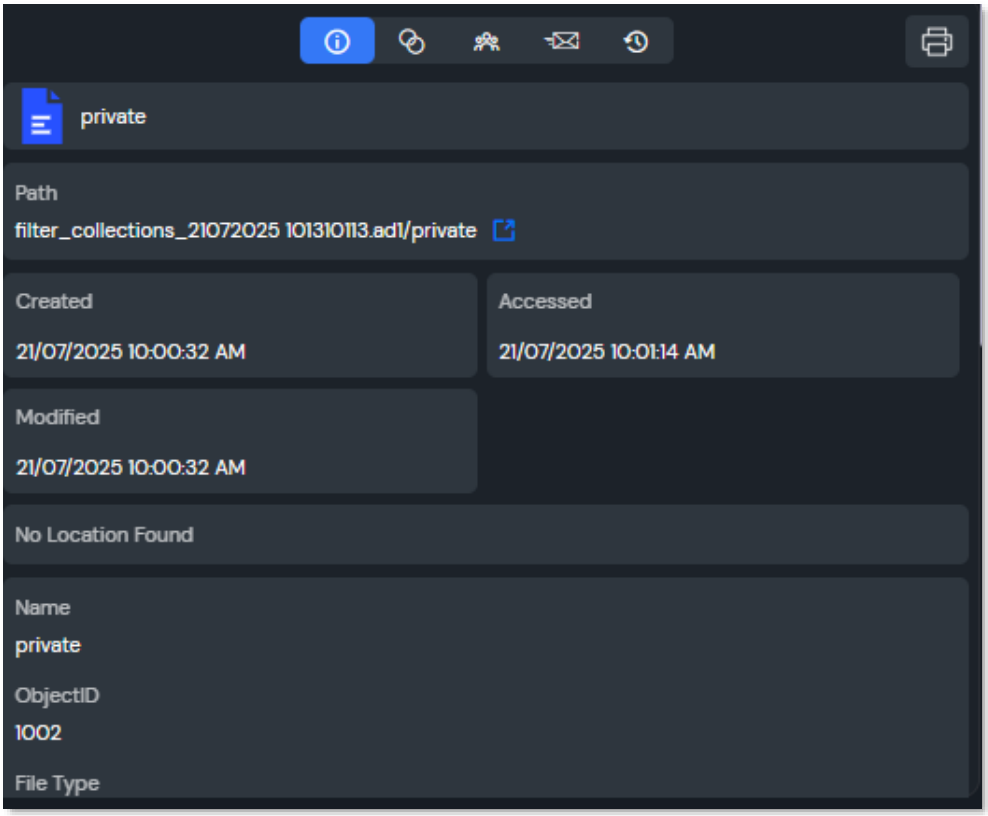
Upon clicking on the **Info** panel, you will be able to see all information associated with the file itself.

All the file related information is categorized in the below sections:

Info

This section displays all the metadata of the selected file.

You can click on the **Open in new tab** button against the **Path** field to view all the files present in the selected location path. This detail will be opened in a separate tab within the application.



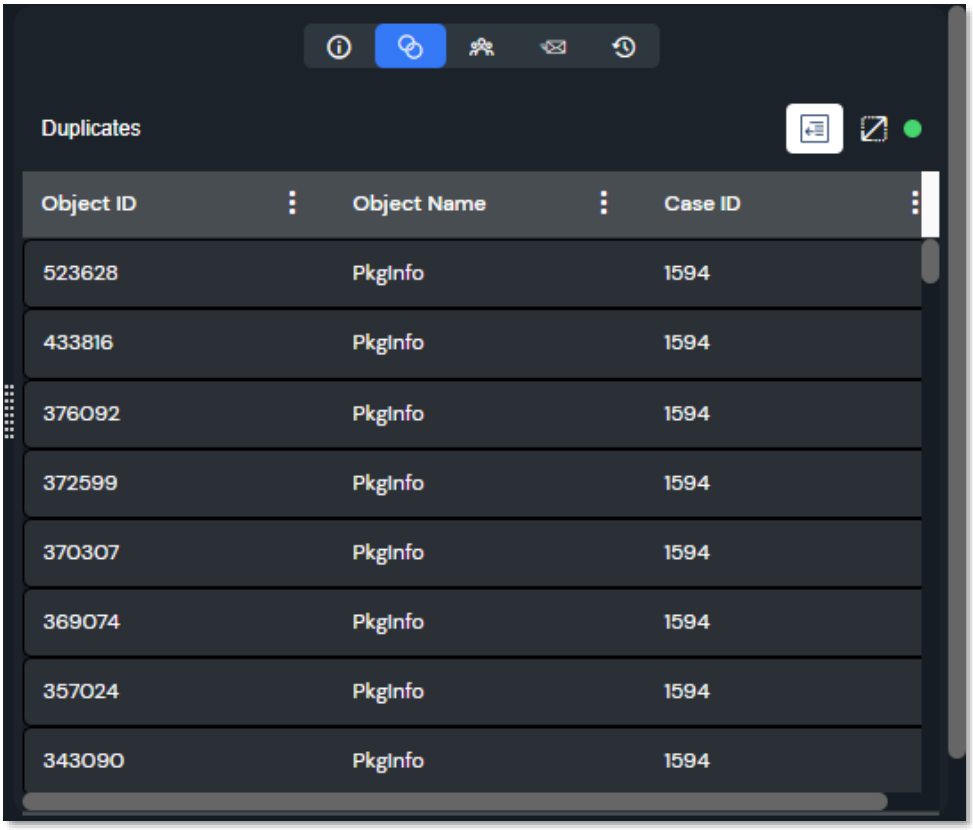
Note: You can click on the **Print** button to print the metadata details of the selected file.

© Exterro, Inc. All rights reserved

Clicking on any of the date field values will open the Mini Timeline panel to view the file's timeline events.

Duplicates

Duplicate files will appear in its own panel and clicking on the **Object ID** will display the files in the Grid.



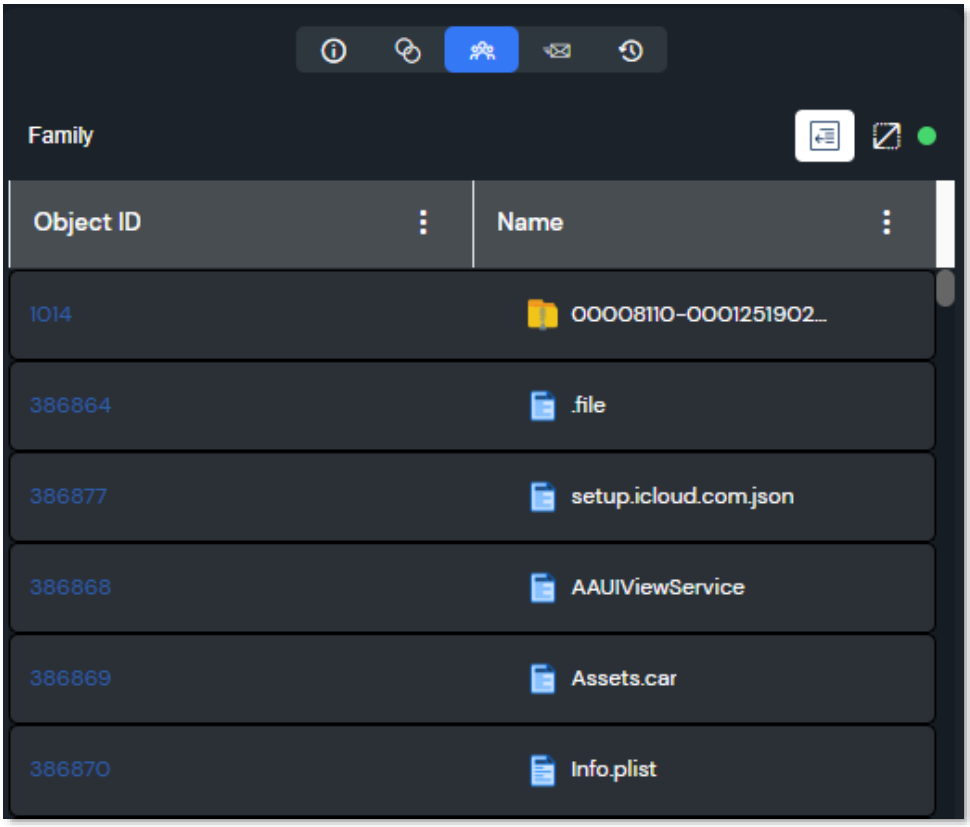
Tip: Click the **Original File** button to go **back to original** file when actively viewing Family, Duplicate files or Email Threads.

Note: You can click on the **Maximize** button to open the viewer in a new pop-up.

© Exterro, Inc. All rights reserved

Family

Parent and child files will appear in the Family section. Clicking on the **Object ID** will display the files in the Grid.



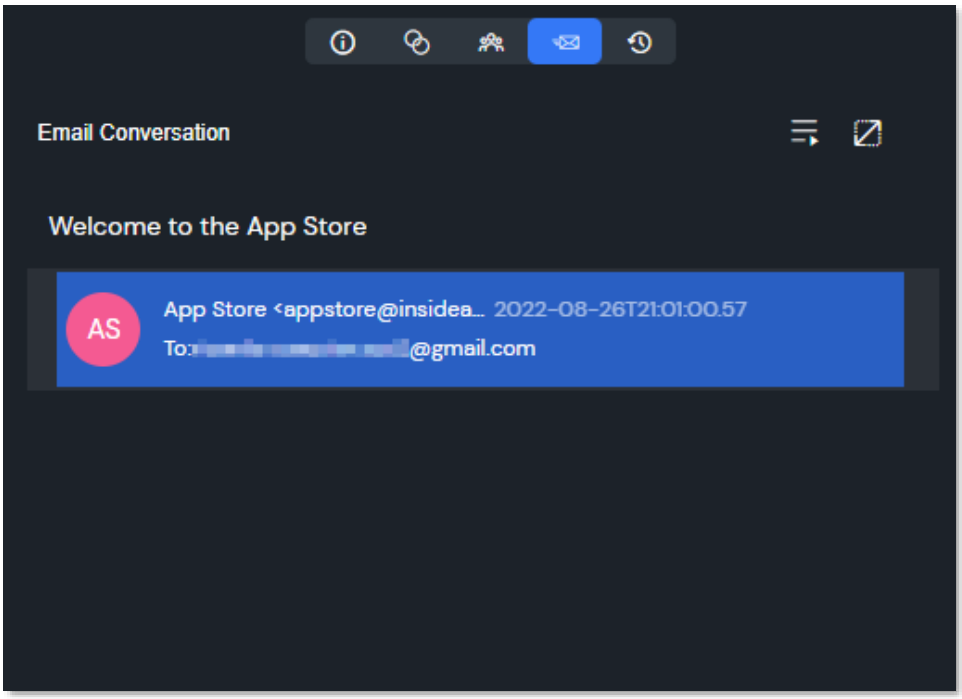
Tip: Click the **Original File** button to go **back to original** file when actively viewing Family, Duplicate files or Email Threads.

Note: You can click on the **Maximize** button to open the viewer in a new pop-up.

© Exterro, Inc. All rights reserved

Email Conversation

Email conversations will be shown in its entirety when a user has identified an email with a conversation thread. Additionally, any attachments will be displayed; the attachment icon allows users to go directly to the attachment if available.



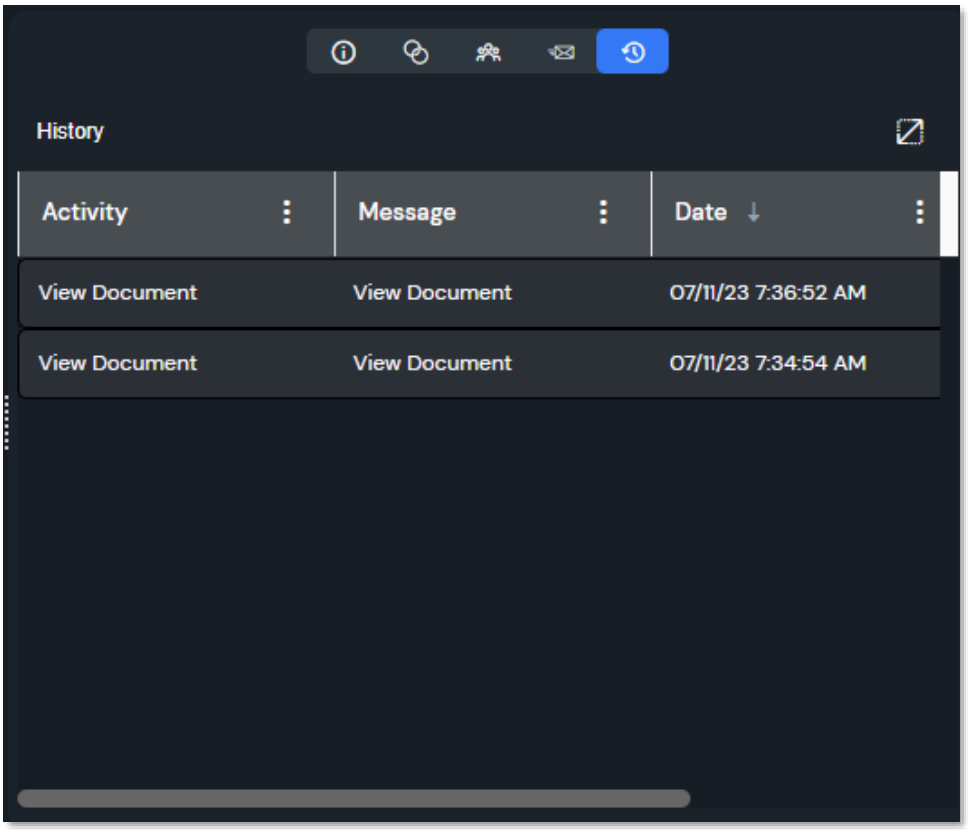
Tip: Click the **Original File** button to go **back to original** file when actively viewing Family, Duplicate files or Email Threads.

Note: You can click on the **Maximize** button to open the viewer in a new pop-up.

© Exterro, Inc. All rights reserved

History

While reviewing, the application will record any actions made involving all files. Using the History section allows you to see what user actions have been made towards a specific file. These user actions range from viewing, exporting and other review related actions.

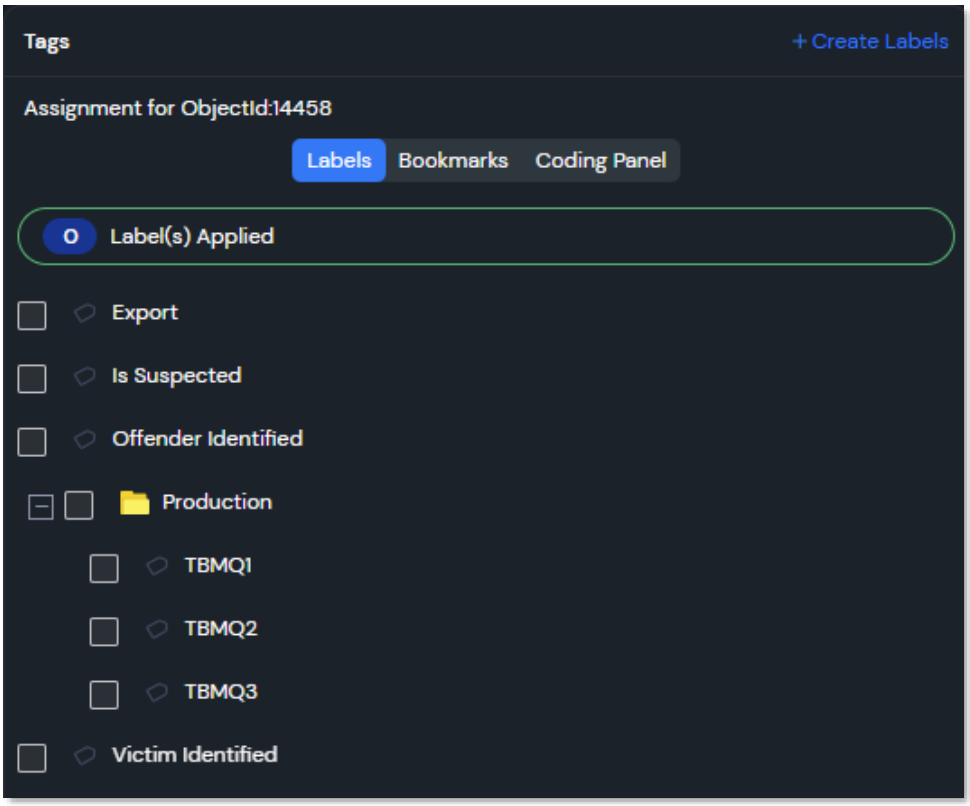


Note: You can click on the **Maximize** button to open the viewer in a new pop-up.

© Exterro, Inc. All rights reserved

Tags Panel

The **Tags** panel provides the list of Labels, Bookmarks, and Coding panels (configured in the application) intended for the review process.



Refer the following sections to make use of the corresponding features:

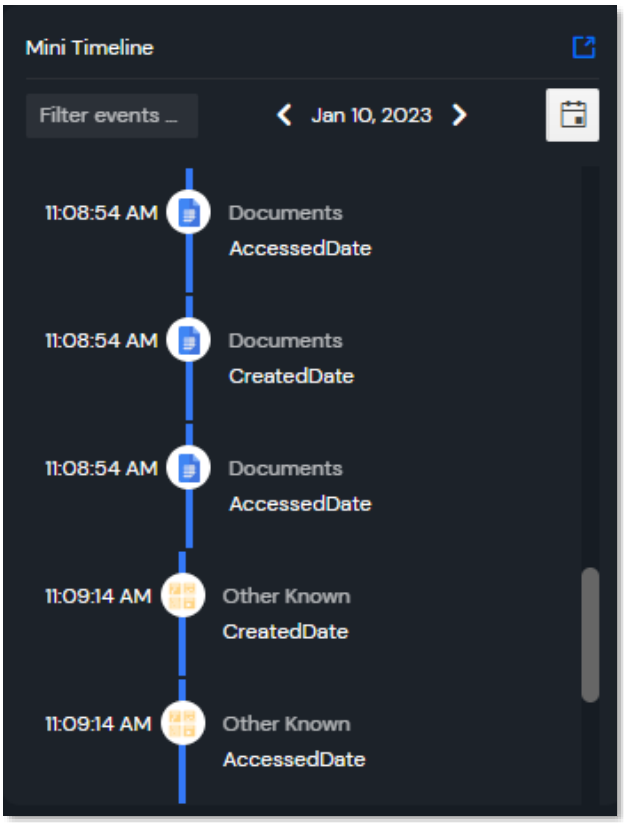
- Working with Labels
- Working with Bookmarks
- Coding Panels within Review

© Exterro, Inc. All rights reserved

Mini Timeline

Warning: The data for this panel will be generated only upon selecting a date value from the **Info** panel of a file.

The Mini Timeline provides you with the list of all events processed for the selected file. Upon clicking a date value in the **Info** panel, the **Mini Timeline** panel will be opened, and the corresponding event will be highlighted. You can click on the **Toggle calendar** button to select the specific date and view the corresponding events processed on that date.

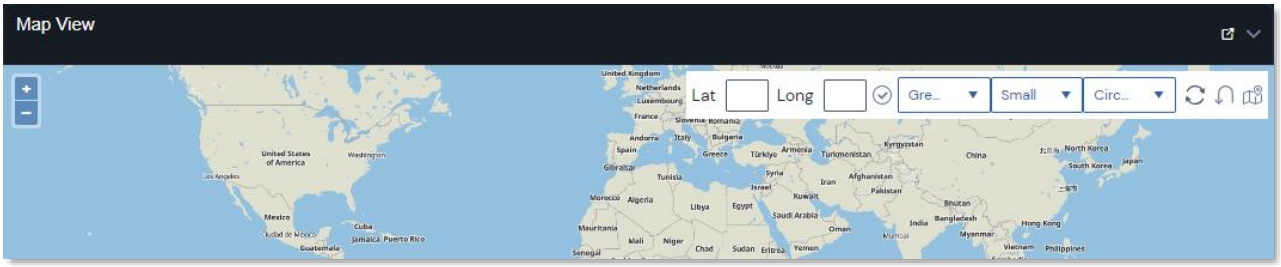


© Exterro, Inc. All rights reserved

Maps

The Map View allows you to view a map with real-world geographic location of evidence items that have geolocation information associated with them. This lets you understand where certain activities/actions took place.

- If you have photos in the evidence that have GPS data in the EXIF data, you can see where those photos were taken.



Processing Requirements

- Clicking on the **Popout Map** button will display the map in a new window with an enlarged view.
- The geolocation data is automatically processed, there is no processing option to select.
- Refer Processing Options section.

© Exterro, Inc. All rights reserved

Key Controls

Photos with GPS information in the EXIF data. If you have photos in the evidence that have GPS data in the EXIF data, you can see where those photos were taken.

Longitude & Latitude

You can enter a custom latitude and longitude should they have any need to. It can be helpful in situations where there may be some relation with two cases or evidence files.

Color, Size & Shape

Customizations are key controls, especially when you have your own preferences. Specifically, you can change the color, size and shape of location pointers.

Populating Map View with EXIF Data

To populate map view with EXIF data:

1. Ensure a case is loaded with existing geolocation data.
2. Click the **Map View** button.

© Exterro, Inc. All rights reserved

Entity Management Dashboard

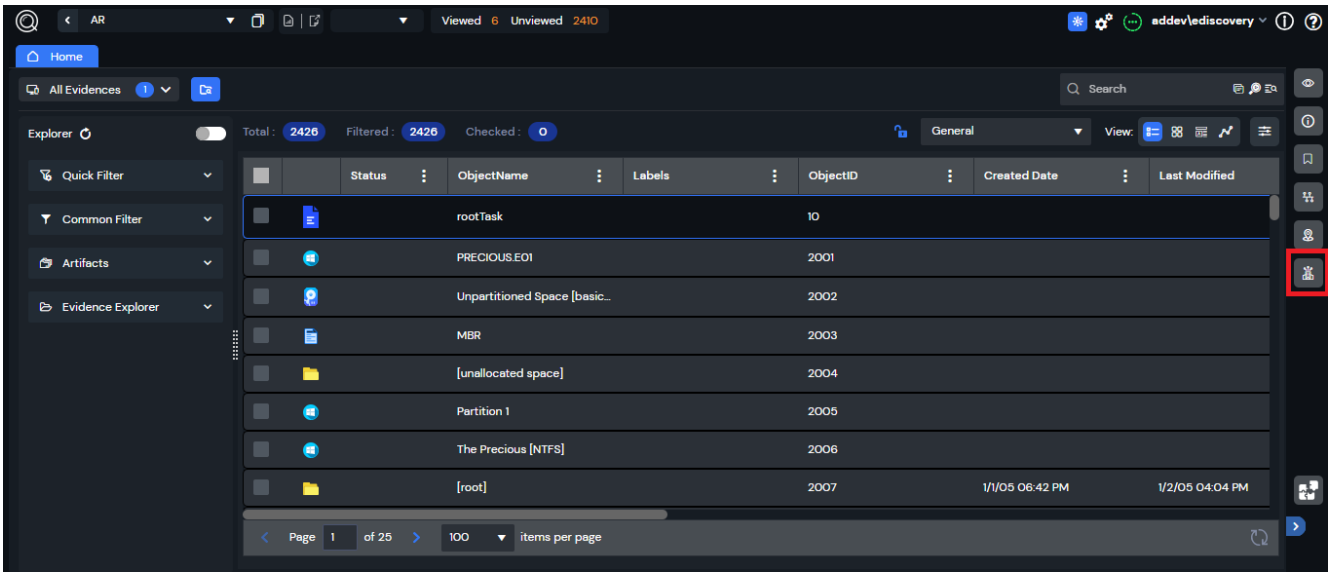
The Entity Management feature allows you to track and analyze people (entities) and their details involved in your cases. This feature automatically processes all case files to identify and categorize entities along with their details such as phone numbers, email addresses, and social media profiles.

The following are the key highlights of this feature:

- **Entity Normalization:** The system identifies and links different aliases of a person using common details (primarily phone numbers) and merges a single entity profile. FTK identifies social handles and communication data which is subsequently merged into a primary entity. A parent-child relationship is formed
- **Entity Management:** You can manually create new entities and merge multiple entities directly from the dashboard. You can identify if any of the entities were manually created or automatically identified from the 'Status' column.
- **Interaction Filtering:** You are provisioned with the ability to filter communication based on the chat applications and 'To' and 'From' dates. This filtering option allows you to apply a filter directly to the Item List and review the results.
- **Social Analyzer:** Communication Analysis: Communication flows within a case are visually represented in a flowchart-like diagram Visual indicators within the dashboard show whether communications between entities were one-directional or bidirectional.

© Exterro, Inc. All rights reserved

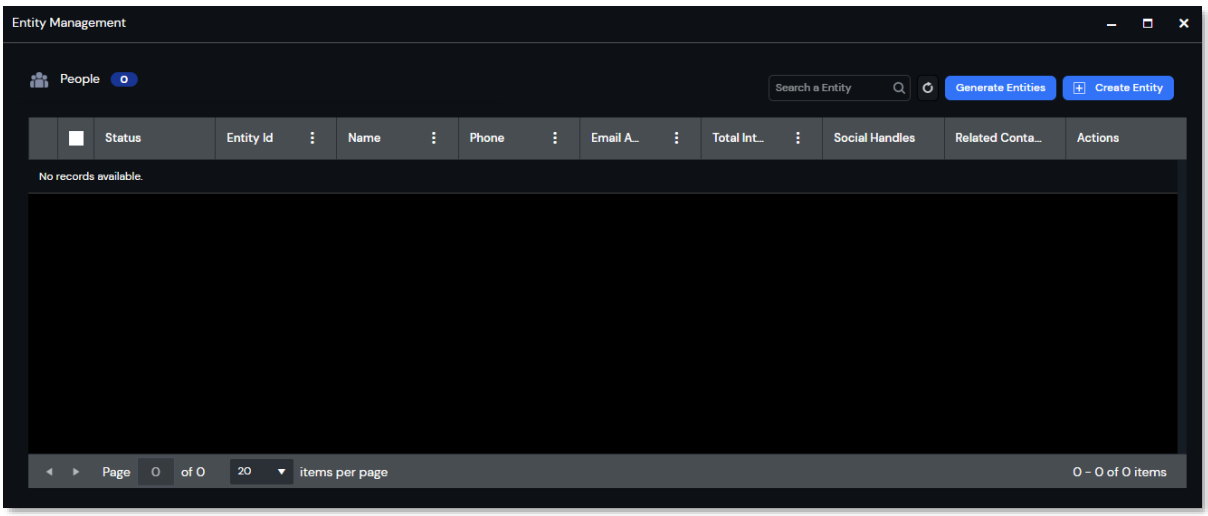
You can click on the icon from the Review page to access the Entity Management Dashboard.



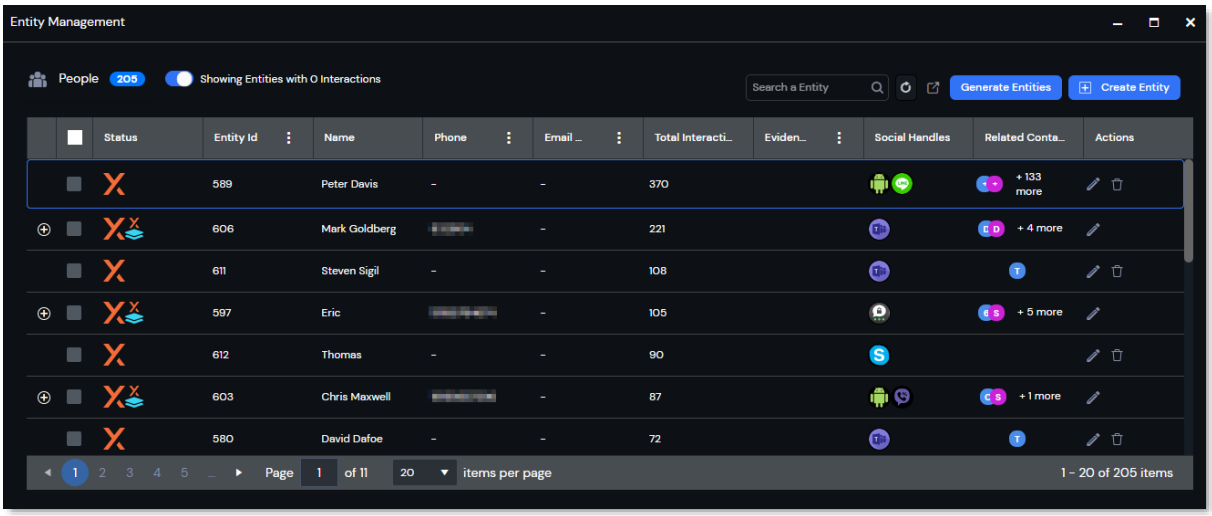
© Exterro, Inc. All rights reserved

Generating Entities

Upon clicking on the icon, the **Entity Management** pop-up will be displayed. You can click on the **Generate Entities** button to generate the entities based on the case files.



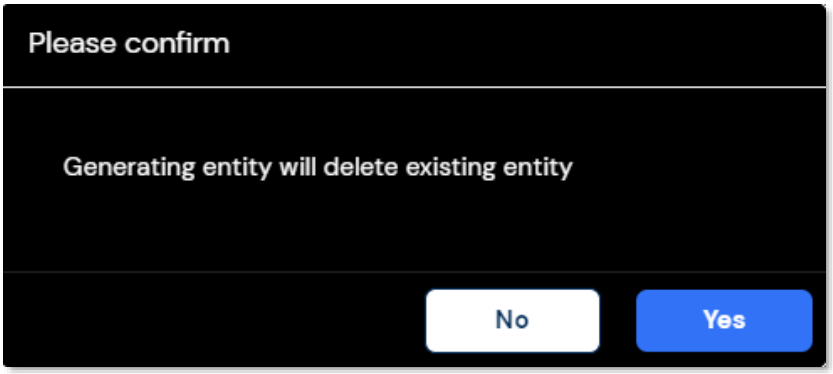
However, the entities will be automatically generated for the cases enabled with the **Generate Entities** option while creating/editing the case.



You can choose to show/hide the entities without any interactions by enabling/disabling the **Showing entities with 0 interactions** option in the dashboard.

© Exterro, Inc. All rights reserved

Note: You can choose to regenerate the entities list in the dashboard by clicking on the Generate Entities button once again. However, the already generated list of entities will be deleted before performing the action.



Note: You can edit or delete the required entities from dashboard by clicking on the **Edit** or **Delete** icons respectively.

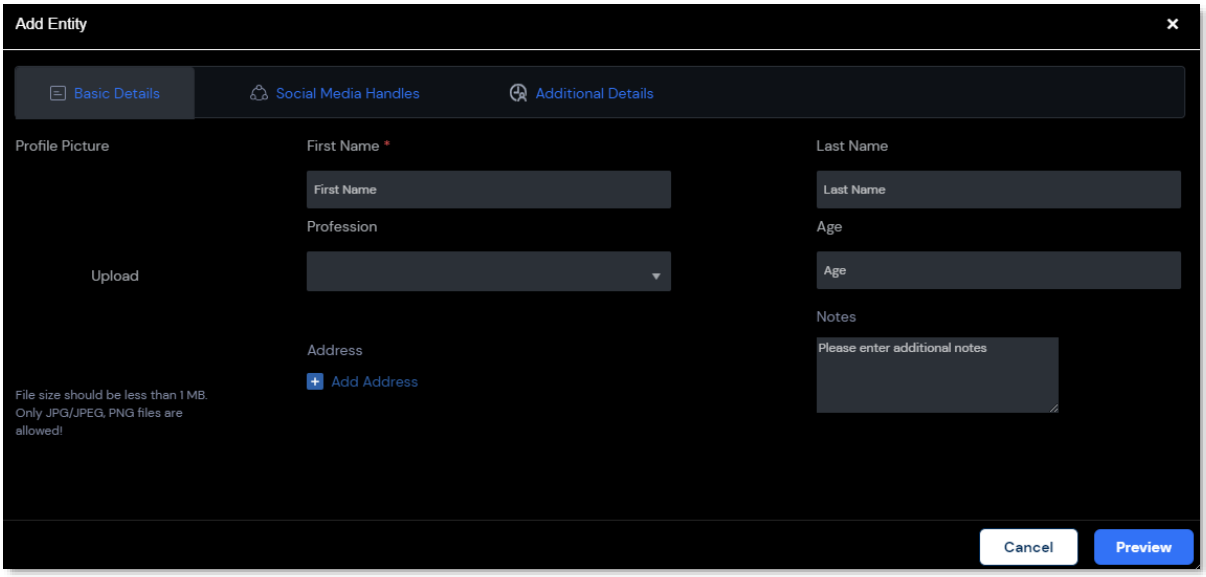
© Exterro, Inc. All rights reserved

Creating Entities

Entity Management also allows you to create a list of your own entities with the corresponding details that have relevance to the case.

To create entities:

1. From the **Entity Management Dashboard**, click on **Create Entity**.
   - The **Add Entity** page is displayed.

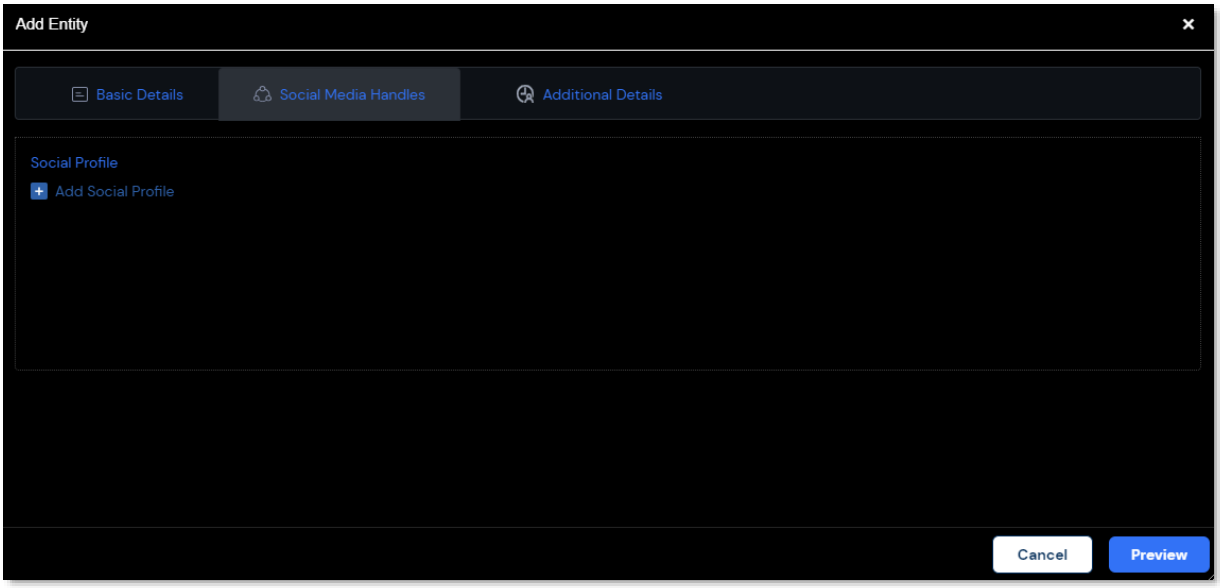


2. Enter the following details of the entity in the **Basic Details** section:
   - Name
   - Age
   - Address
   - Profession
   - Additional notes about the entity.

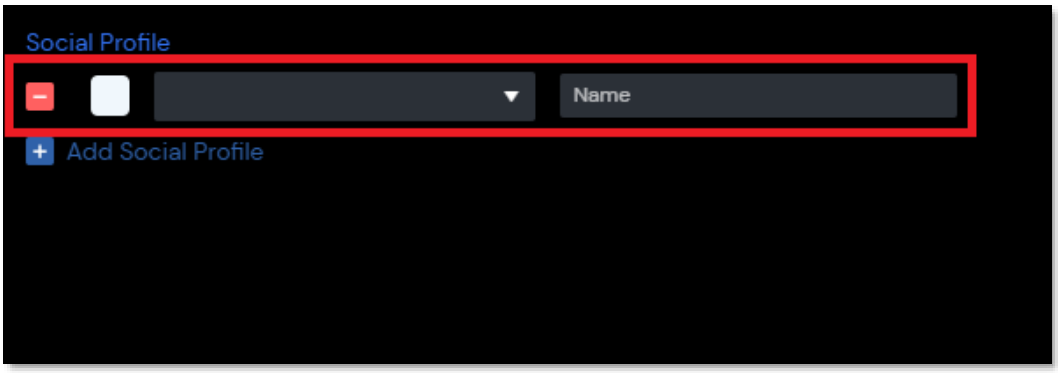
Note: You can also upload a picture of the entity by clicking on the **Upload** option against the **Profile Picture** field.

© Exterro, Inc. All rights reserved

3. Navigate to the **Social Media Handles** section.



4. Click on **Add Social Profile**.
   - The below field will be displayed.

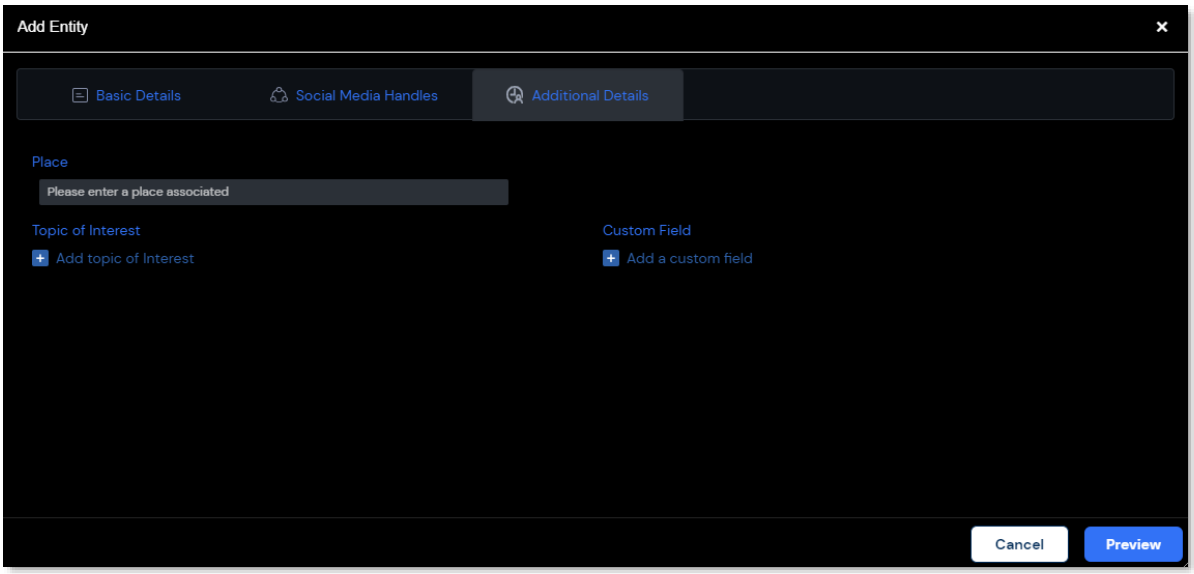


5. Select the social media application from the drop-down field and enter the corresponding account name.

Note: You can add multiple social media handles by clicking on the **Add Social Profile** button for the required number of times.

© Exterro, Inc. All rights reserved

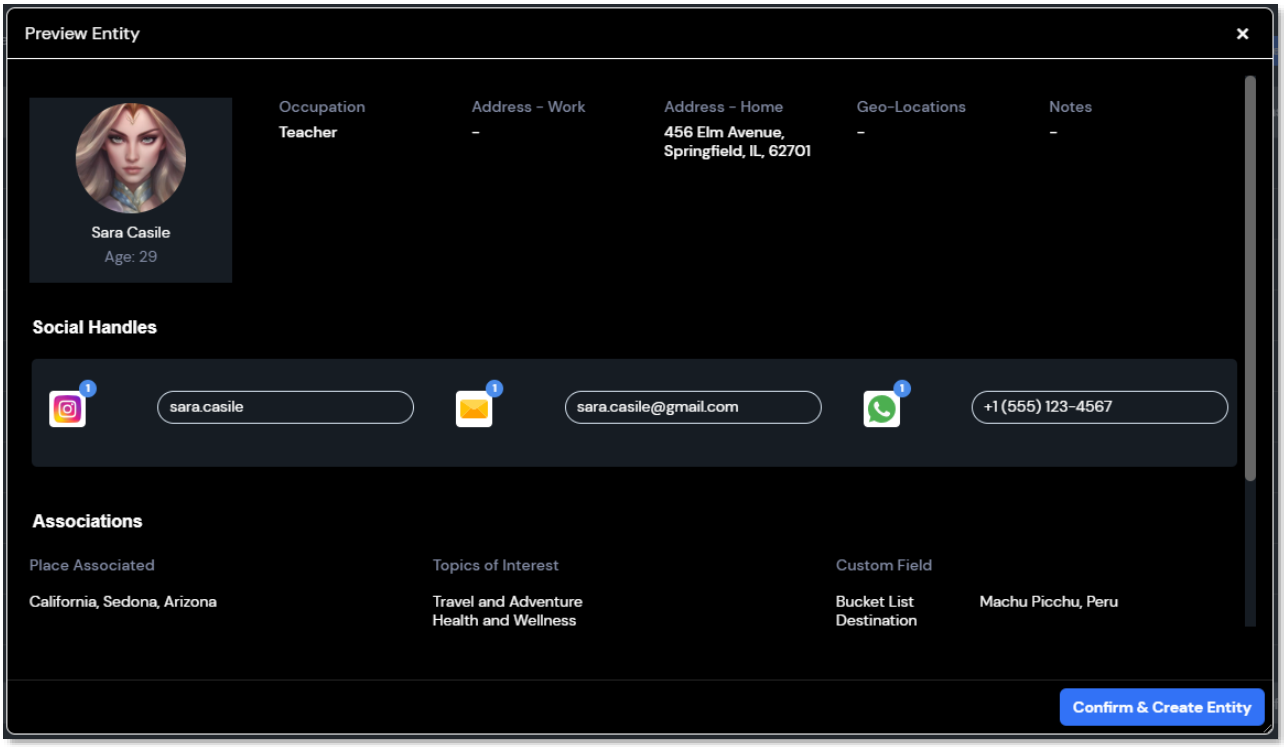
6. Navigate to the **Additional Details** section.



7. Enter the **Place** associated with the user.
8. Click on the **Add topic of interest** option to provide the corresponding information.
9. Click on the **Add a custom field** option to add the custom field and value that should be displayed in the **Entity Managed Dashboard**.

© Exterro, Inc. All rights reserved

10. Click on the **Preview** button.
    - A preview of the entity with all the configured information will be displayed.



11. Upon verification, click on the **Confirm & Create Entity** button to create the entity.

The entity will be created and displayed in the **Entity Management Dashboard**.

The following icons are displayed in the **Status** column of **Entity Management Dashboard** to distinguish between the user created entities and FTK Central created entities:

- - User Created Entities
- - FTK Created Entities

© Exterro, Inc. All rights reserved

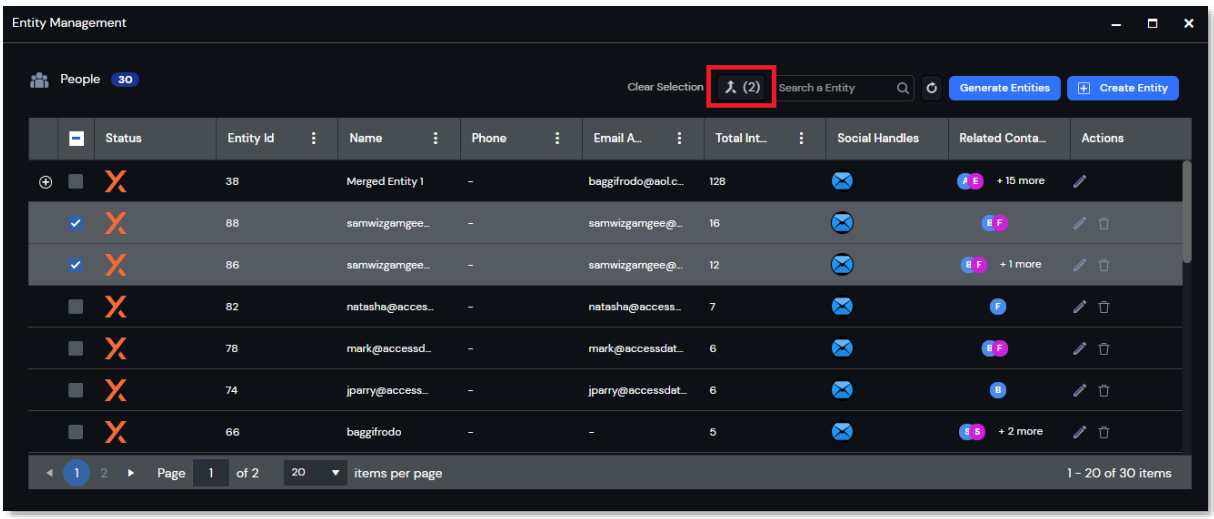
Merging and Unmerging Entities

Note: You can sort the entities to segregate and view the merged and standalone entities by clicking on the **Status** column header in the dashboard.

To merge the entities:

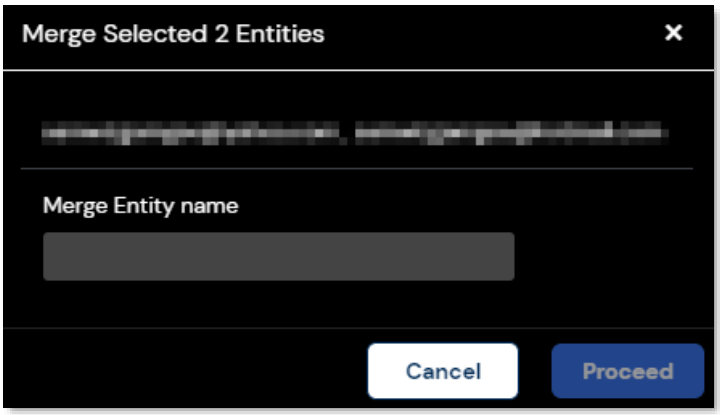
1. From the Entity Management Dashboard select two or more entities.
2. Click on the **Merge Entities** button.

Note: The **Merge Entities** button will be displayed only upon selecting two or more entities.



© Exterro, Inc. All rights reserved

- The **Merge Selected Entities** pop-up is displayed.



3. Enter the **Merge Entity Name**.
4. Click **Proceed**.

The selected entities will be merged into one single entity and displayed in the dashboard.

The following icons are displayed in the **Status** column of **Entity Management Dashboard** to distinguish between the entities that are merged by the user and FTK Central application:

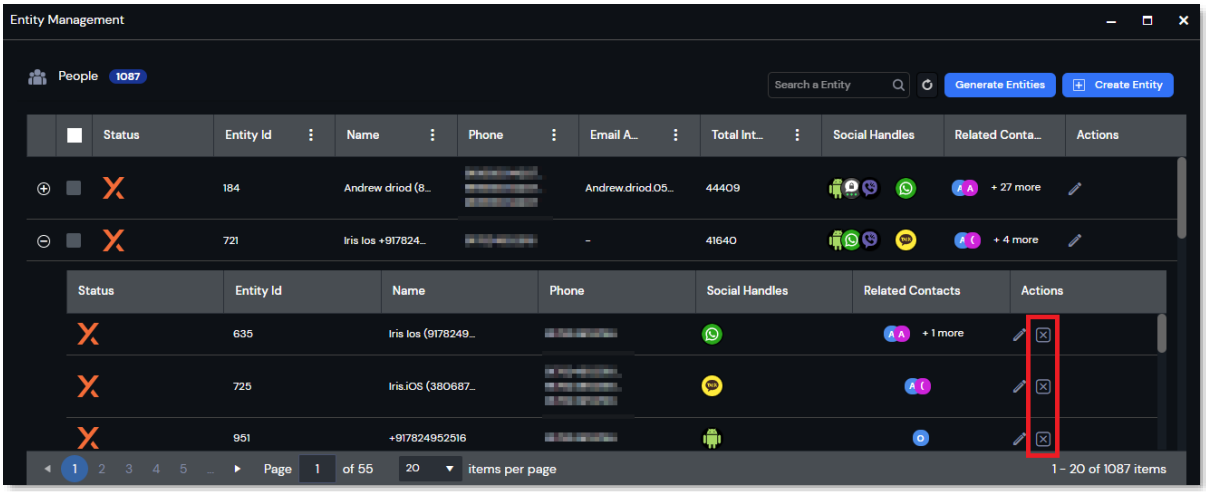
- - Merged by the FTK Central application.
- - Merged by the user.

Warning: Merged entities continue to display objects belonging to an evidence item even after that evidence has been soft-deleted from the Case Summary page. However, you can regenerate the entity to view the refreshed results on the Entity Management page.

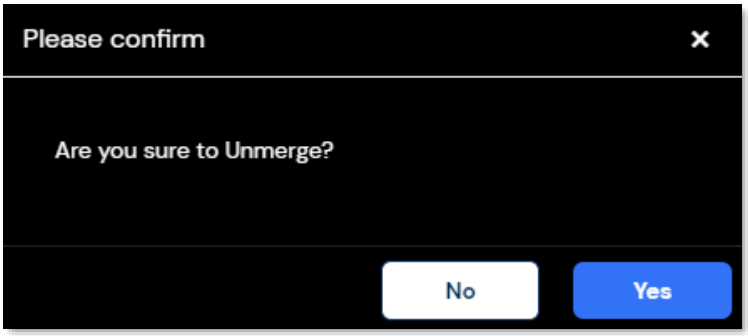
© Exterro, Inc. All rights reserved

To unmerge the entities:

1. From the Entity Management Dashboard, click on the **Expand Details** icon against the required (merged) entity.



2. Click on the **Unmerge Entity** icon against the entity that should be unmerged.
   - The **Please confirm** pop-up is displayed.



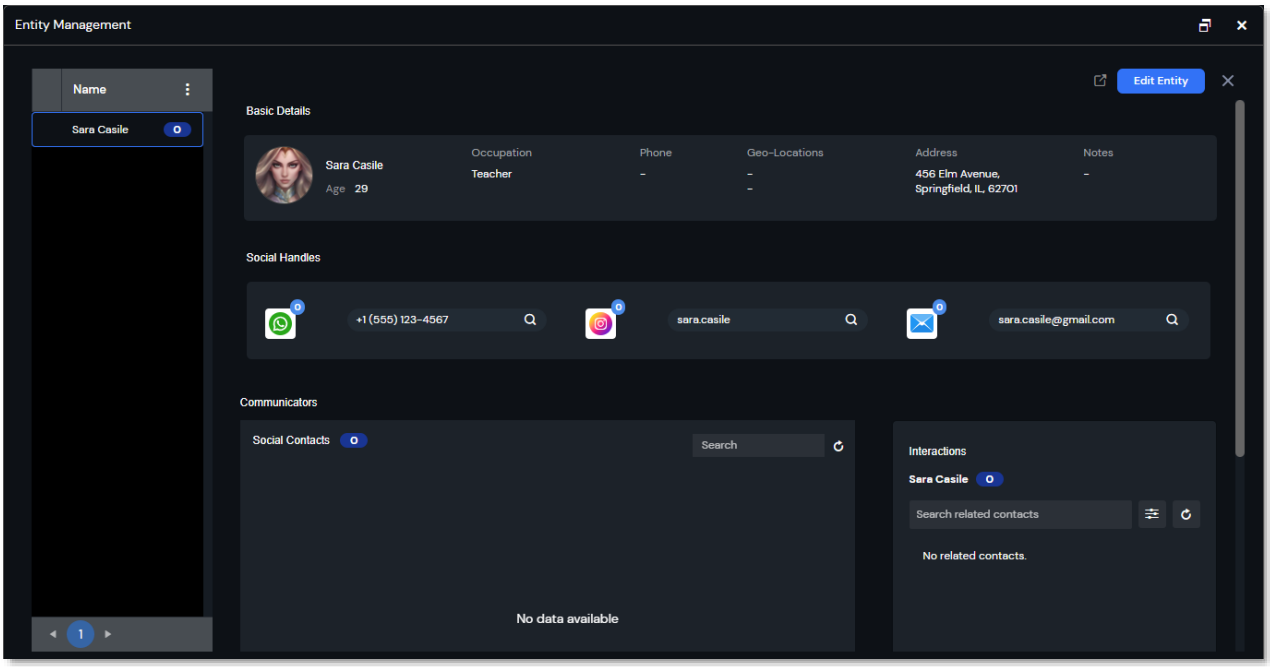
3. Click on **Yes**.

The corresponding entity will be unmerged and maintained as a separate entity in the dashboard.

© Exterro, Inc. All rights reserved

Viewing the Entity Details

You can click on the required entity from the dashboard to access the details of a specific entity.

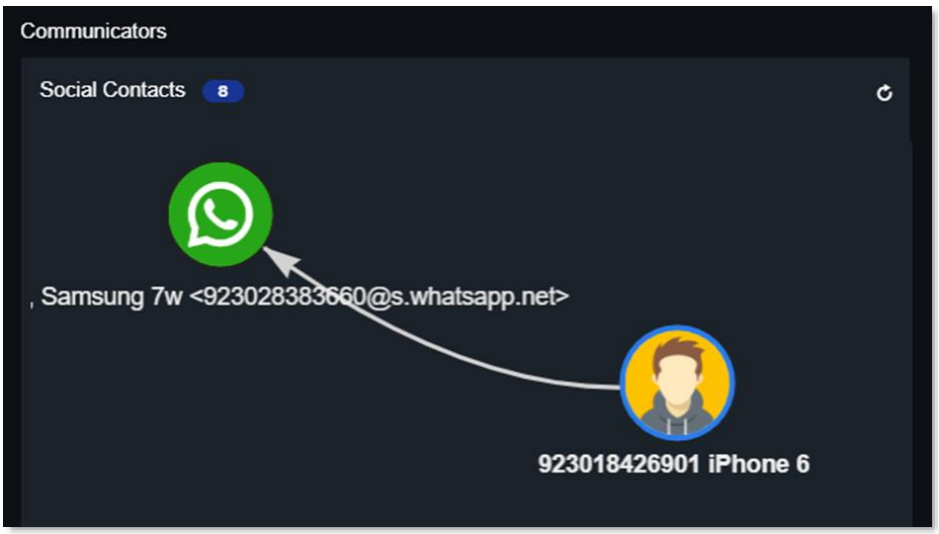


Upon clicking on the entity, the details page will be displayed consisting of the entity's basic details and social handles. Moreover, you can make use of this section to perform a communication analysis between the entities.

© Exterro, Inc. All rights reserved

This can be achieved by using both the **Communicators** and **Interactions** sections. Upon selecting the required entities from the **Interactions** section, the **Communicators** section will generate a graphical representation of communications flow between the entities.

Furthermore, you can click on the entity to view the modes of communication flow i.e. the social handles via which the communication was established.



Note: You can select the required entity from the left pane (**Name** section) to view the corresponding details.

© Exterro, Inc. All rights reserved

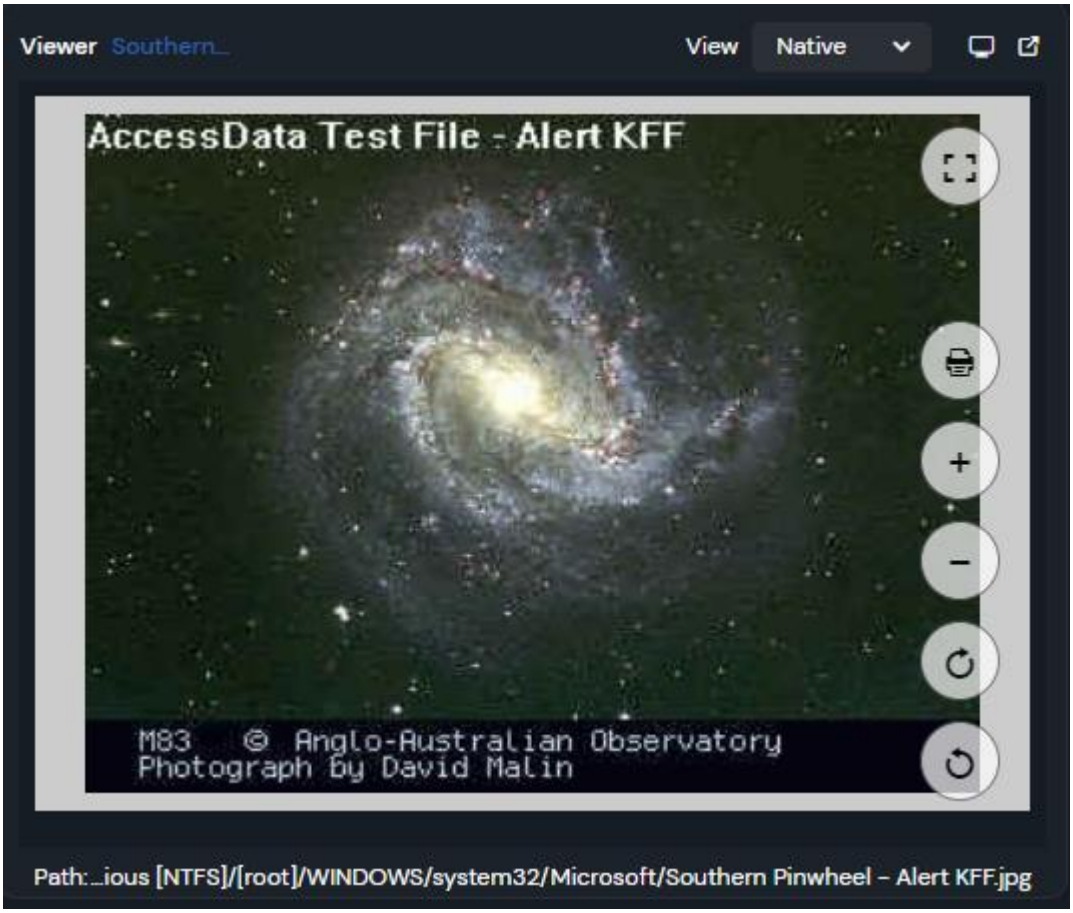
Using Document Viewing Panels

You can use different pre-configured document viewing panels to visualize data.

- See Native Panel section
- See Image Panel section
- See Text Panel section
- See View Panel on Another Monitor section

Using the Native Panel

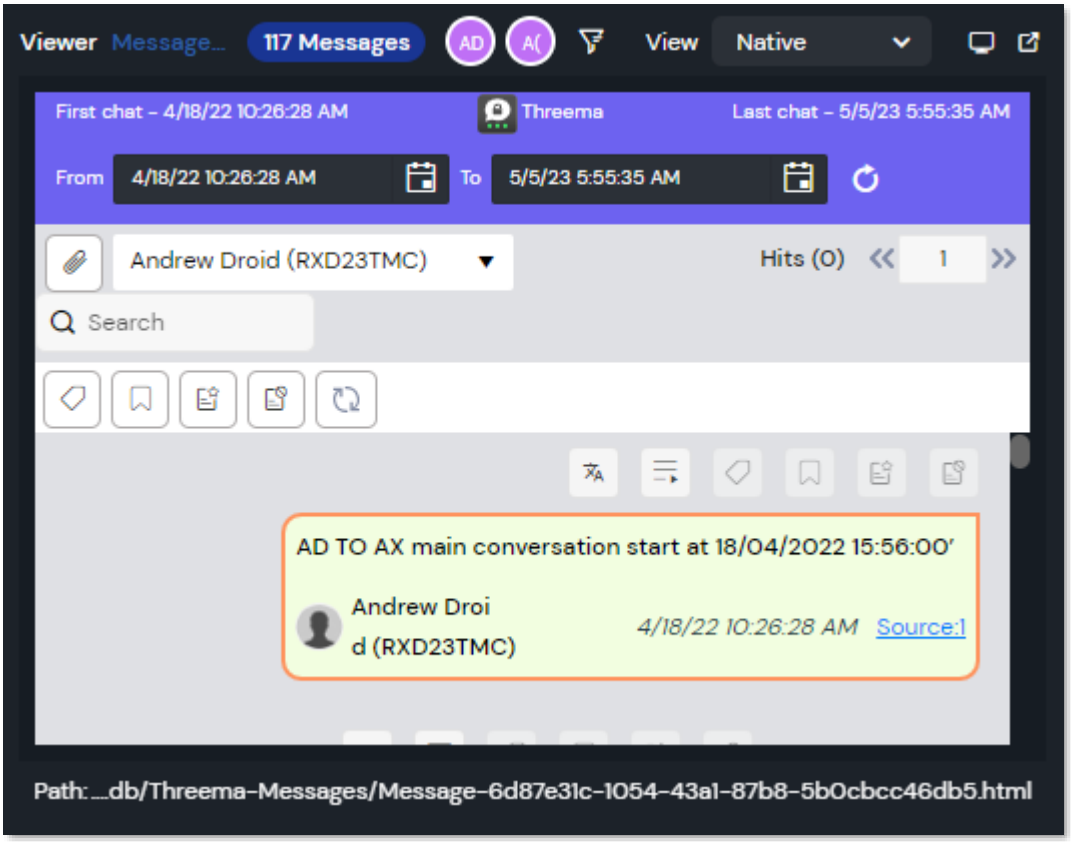
You can click the **Native** view to display the file in its native format.



© Exterro, Inc. All rights reserved

Chat Applications:

The Native View of the Chat conversations has been enhanced to provide users with a near native experience of the source chat application for easy reviewing.



All the individually collected chat files will be consolidated to display the entire conversation thread. You can make use of the **From** and **To** date filters to filter and view only the chats sent/received within a specified time period.

You can click on the **Select this chat on the Item List** button to navigate to and view the corresponding individual file in the Item list.

© Exterro, Inc. All rights reserved

The following information are displayed in the Native view's header specifically for chat conversions:

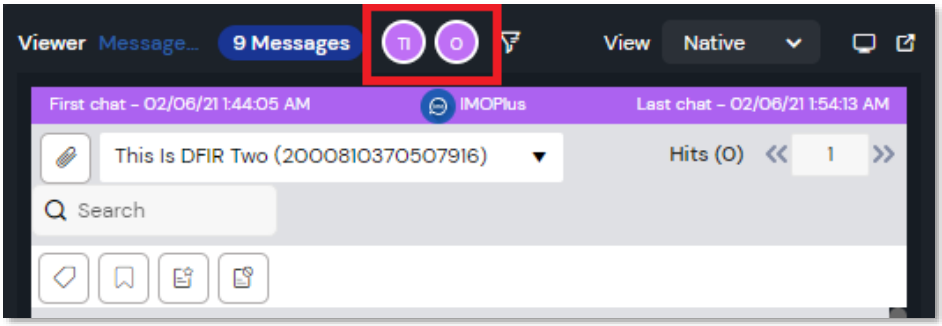
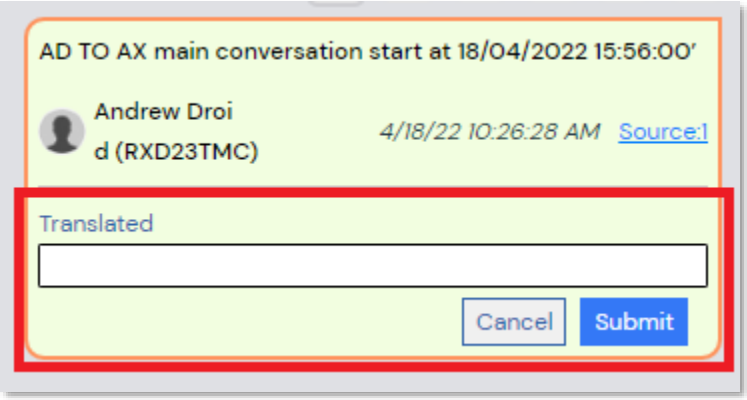
- The chat application's name.
- The total number of messages present in the selected conversation.
- The participants of the conversation.
- The date and time of the first and last chats in the Conversation.
- The 'Attachment(s)' button to click and view all the attachments in the conversation.

Note: While viewing the attachments, you can click on the **Filter conversations around this attachment** button to navigate and view the chat associated with the attachment in the Native view.

For chat applications, you are provided with the following options to performing the corresponding operations in the Native viewer:

Options	Description
Label	To label a chat conversation.
Bookmark	To bookmark a chat conversation.
Flag as Privileged	To Flag a chat as privileged.
Flag as Ignorable	To Flag a chat as ignorable.
Participant Details	To view the details of the participants involved in the conversation. The initials of the participants will be displayed in the header of the viewer.

© Exterro, Inc. All rights reserved

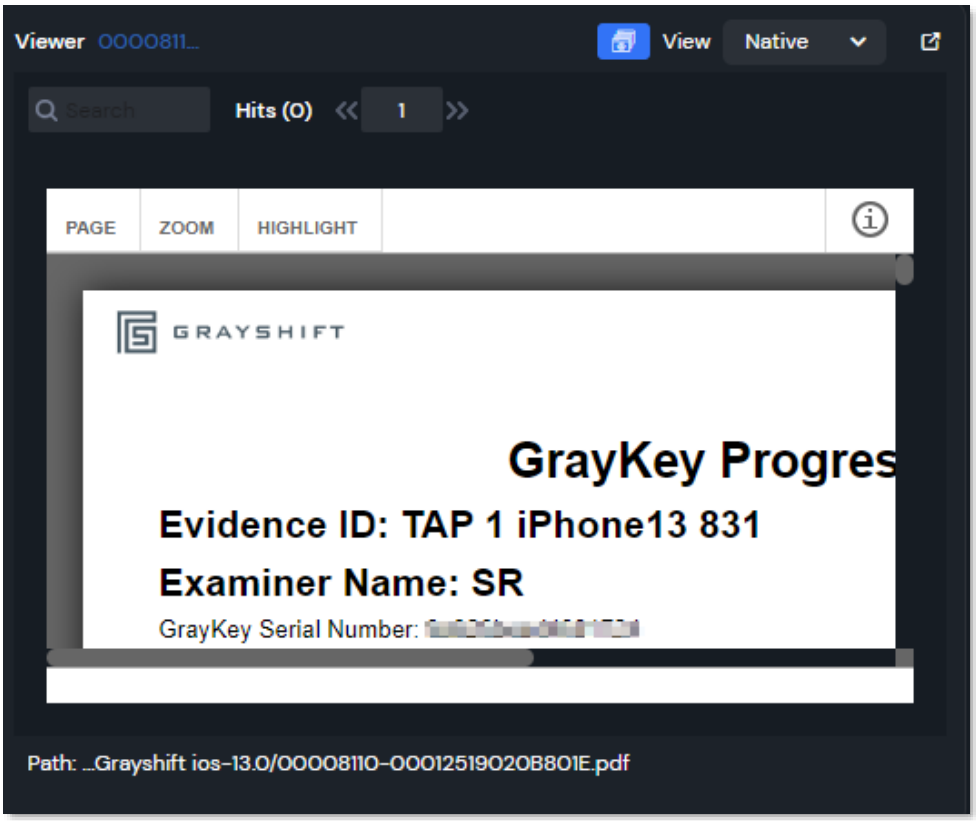
Options	Description
	Example: 
Attachments	To View attachments shared in the particular chat.
Translate Manually	To manually provide the translated content of the messages in the viewer. 

© Exterro, Inc. All rights reserved

Alternative View

Click on to enable the **Alternative View** mode in the **Native** viewer.

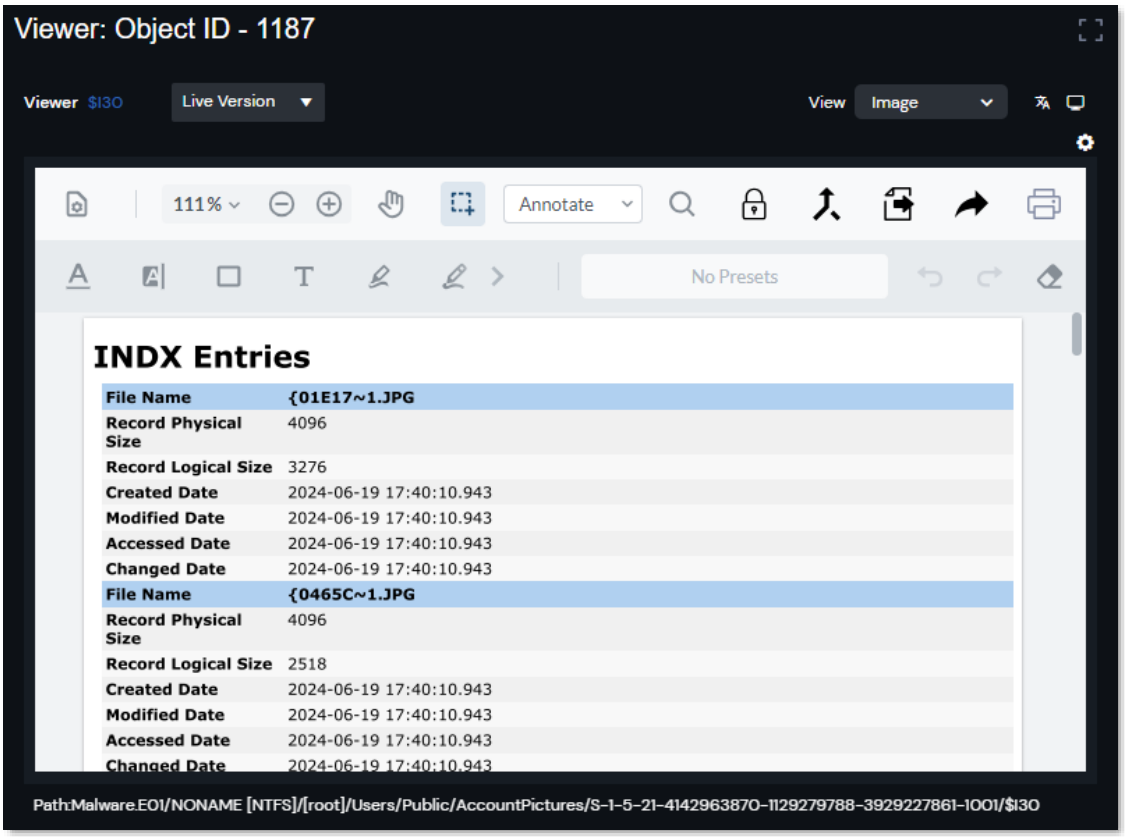
Note: This option is applicable only for PDF and Word file types.



© Exterro, Inc. All rights reserved

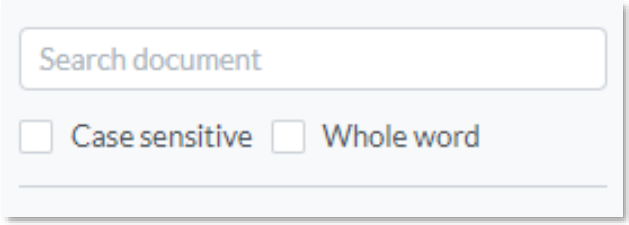
Using the Image Panel

When viewing documents in **Image** view, you will see a variation of icons and buttons. These options are useful for different processes such as creating tabbed productions, redactions, branding, unitization and having the ability to restore a document.

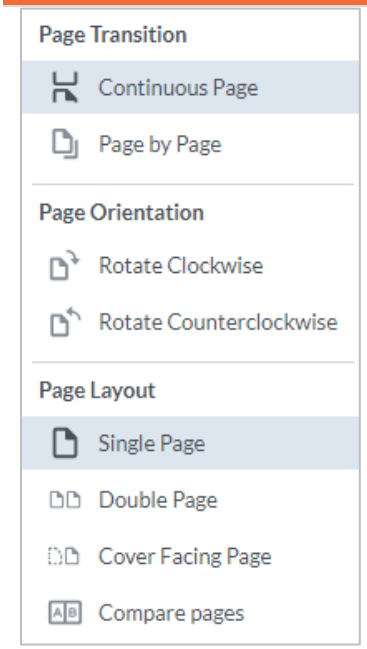


© Exterro, Inc. All rights reserved

Buttons and Functions

Buttons	Description and uses
	Find in Document – Allows users to search for words and phrases in the selected file. 
	Page Toggle – Allows users to go to pages quickly without having to cycle each page.
	Zoom in and Out – You can click on the increase ( ) or decrease ( ) button to zoom in or zoom out of the file displayed in the viewer. You can also use the drop-down list to select a specific pre-set percentage.
	Print - Ability to print a document as is or with annotations.
	Additional Tools – Ability to move between multiple pages. Rotate a document clockwise and anticlockwise. Additionally, view Document Properties.

© Exterro, Inc. All rights reserved

Buttons	Description and uses
	
	Highlight Text – Allows text to be highlighted within a document.
	Write Text - Lets users type text over a document.
	Stamping – Stamp predefined value on a document.
	Redact Area – Main redaction tool. Allows users to pick a color for the redaction area.
	Burn in Redaction – Action to ensure redactions are held in place.
	Restore Document – Restores documents back to original state.
	Unitize Document – Allows documents to have document breaks, deletion of pages, moving of pages and rotation of pages.
	Create Tabbed Production – Creates a child document which can be a holder for redactions or other edits.

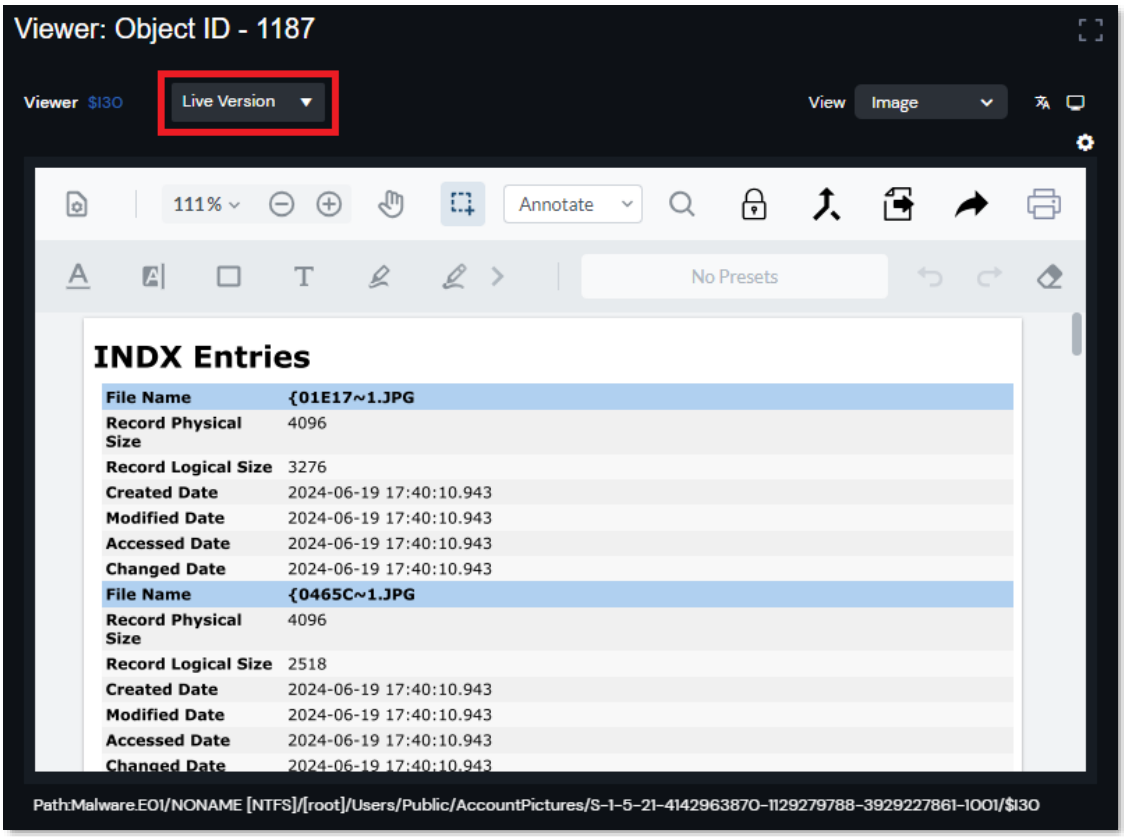
© Exterro, Inc. All rights reserved

Buttons	Description and uses
	Draw Rectangle – To draw rectangles (in required color and thickness) in the file.
	Draw Ellipse – To draw ellipses (in required color and thickness) in the file.
	Draw Line – To draw lines (in required color and thickness) in the file.
	Draw Scribble – To scribble (in required color and thickness) in the file.

© Exterro, Inc. All rights reserved

Live Version

The live version drop-down consists of the redacted and produced versions of the selected file (if applicable). Selecting the required version of file from the drop-down will display the modifications (redactions, annotations, etc.) made to the file or the produced format of the file.



© Exterro, Inc. All rights reserved

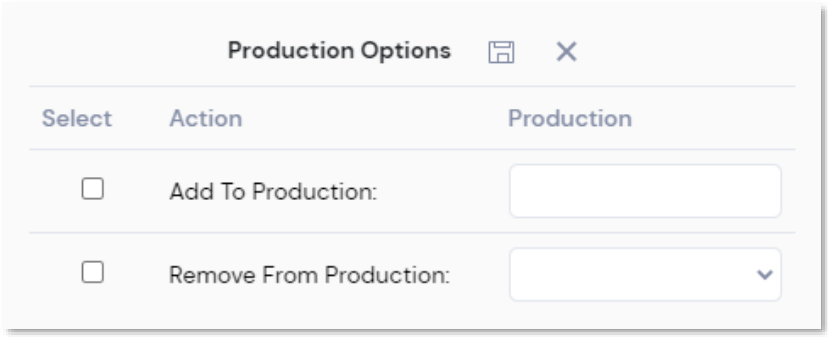
Tabbed Productions

FTK Central facilitates expert document preparation, with tabbed production options for creating multiple versions of a document without adding additional documents to a case. This is ideal when redactions are required on a document. It must be done prior to any editing as users will be able to toggle between different versions of a document.

Creating a Tabbed Production

To create a tabbed production:

1. Select the required file from the list view.
2. Select **Image** in the **Viewer**.
3. Click on .
    - The **Production Options** prompt will be displayed.



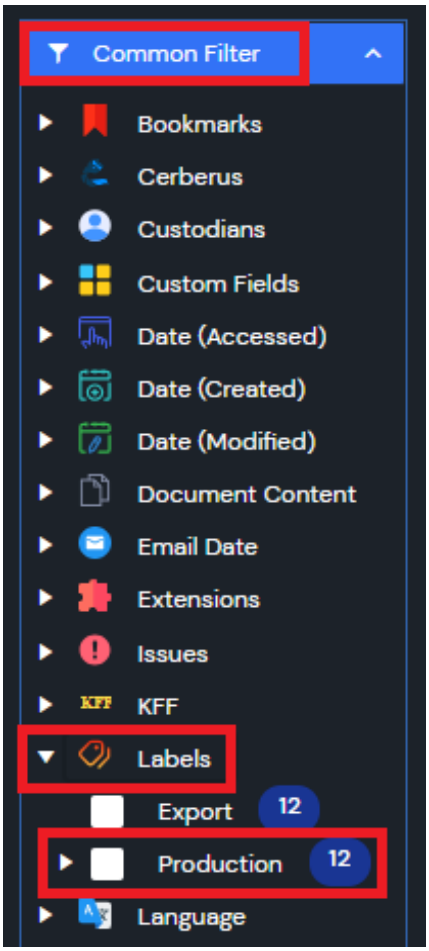
4. Enable the **Add To Production** field and provide a name against it.
5. Click the **Save** button.

© Exterro, Inc. All rights reserved

Filtering productions

To filter production:

1. In the Grid, click the **Common Filter** from the left pane.
2. Navigate to **Labels** > **Production**.



3. Select the required production label.

© Exterro, Inc. All rights reserved

Redactions

There may be cases that require redaction of documents for various reasons. FTK Central gives you the freedom to redact documents as you wish.

Tip: You can use the following columns to identify the corresponding information:

- **DocIsRedacted** - To identify documents that have been redacted.
- **DocRedactionMigrated** - To identify documents that have migrated redactions from a legacy application.

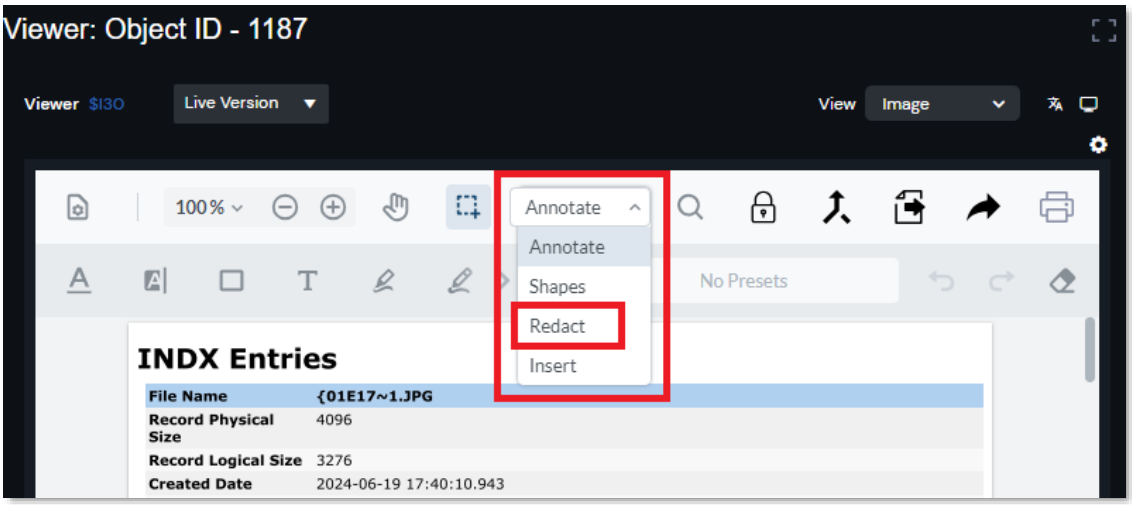
Note: Any processes beyond this point require users to work on **Live Version** of their document and then save them as tabbed productions.

© Exterro, Inc. All rights reserved

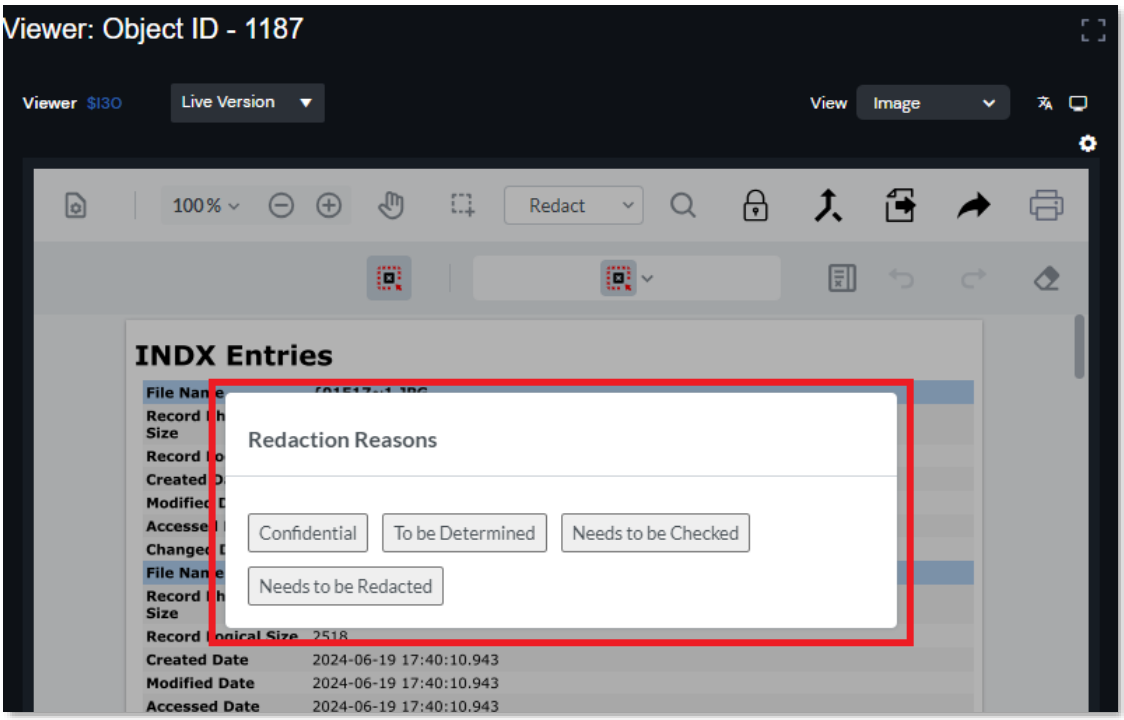
Manual Redaction

To perform redaction manually:

1. Click the Image in the Viewer.
2. Select the **Redact** option from the drop-down.

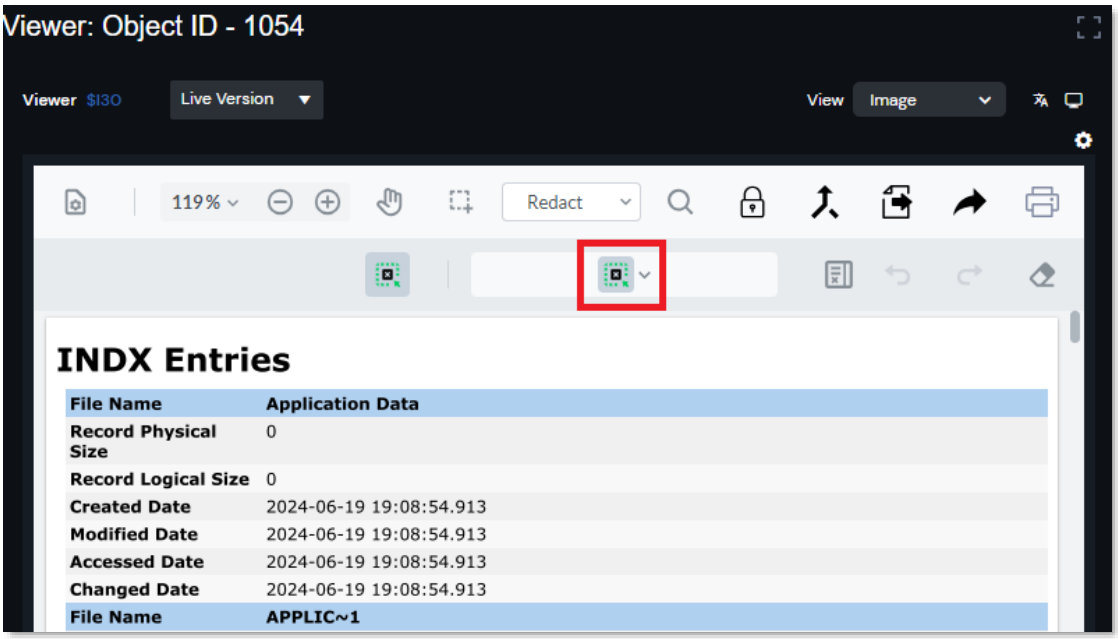


- The **Redaction Reasons** pop-up is displayed.



© Exterro, Inc. All rights reserved

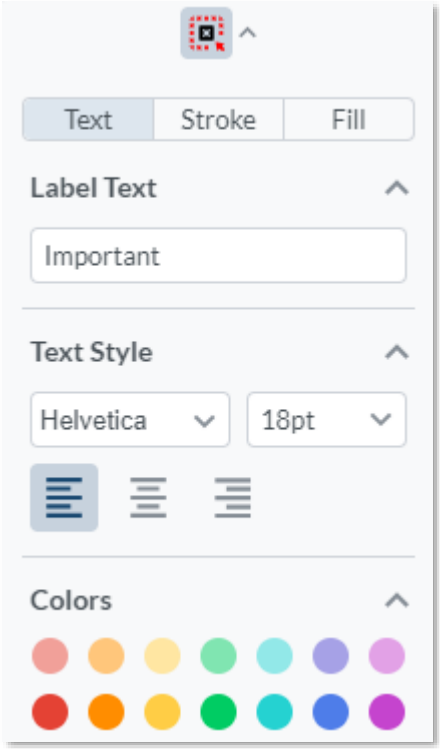
3. Select the required redaction reason.
4. Click on the **Mark for redaction** icon to configure the redaction settings.



© Exterro, Inc. All rights reserved

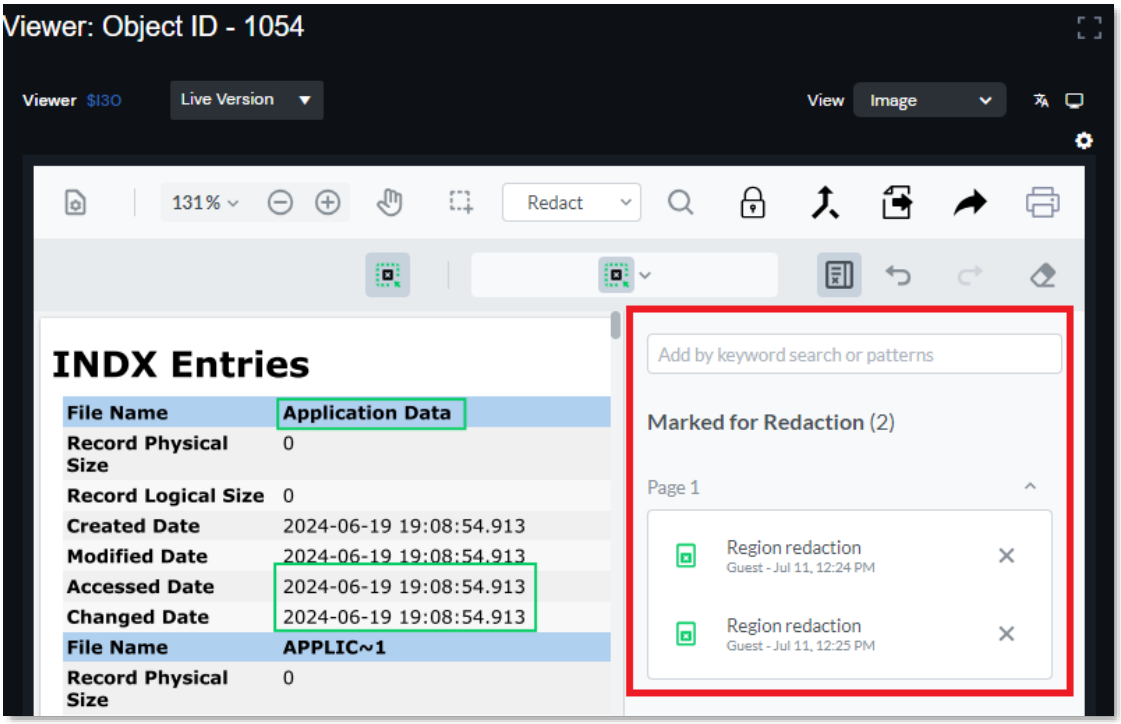
5. Configure the below provided redaction settings based on your requirements:

- Text – You can configure the label text, font, and color that should be used for redaction.
- Stroke -
- Fill -



© Exterro, Inc. All rights reserved

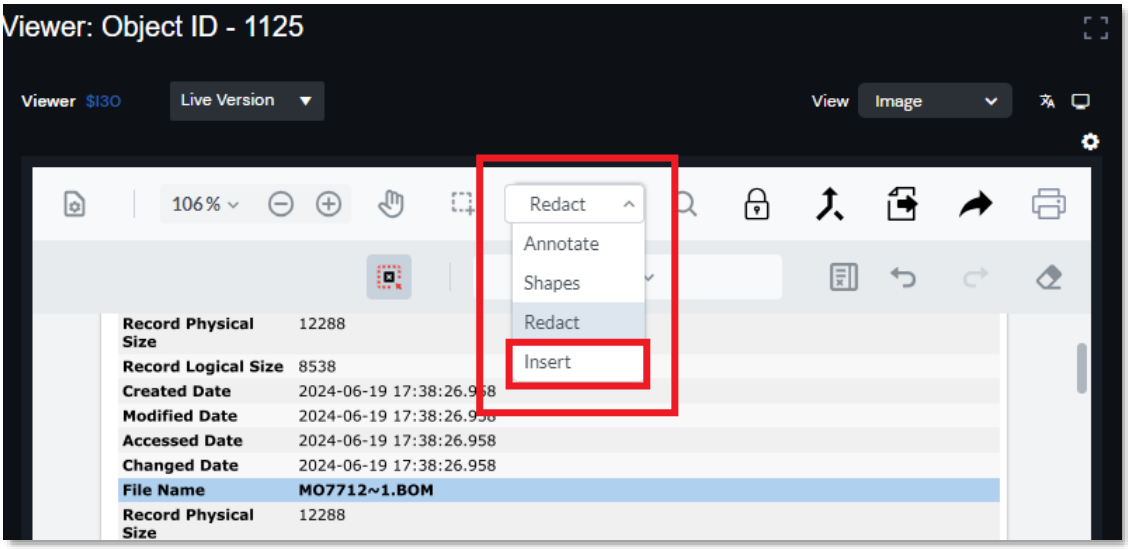
6. Upon configuration, click and drag on the file content to apply the redaction.
   - The **Marked for Redaction** pane will be displayed to list out the redactions done in file.



Note: You can hide/show the panel by clicking on the **Redaction Panel** icon.

© Exterro, Inc. All rights reserved

7. Select the Insert option from the drop-down menu.



8. Click on the **Rubber Stamp** icon and select the required stamp from the drop-down
9. Use the cursor to place the stamp at the required position and click on it to apply the stamp.

Note: You can click on to lock the applied redactions and stamps in the provided location to avoid changing it later.

© Exterro, Inc. All rights reserved

Automatic Redaction

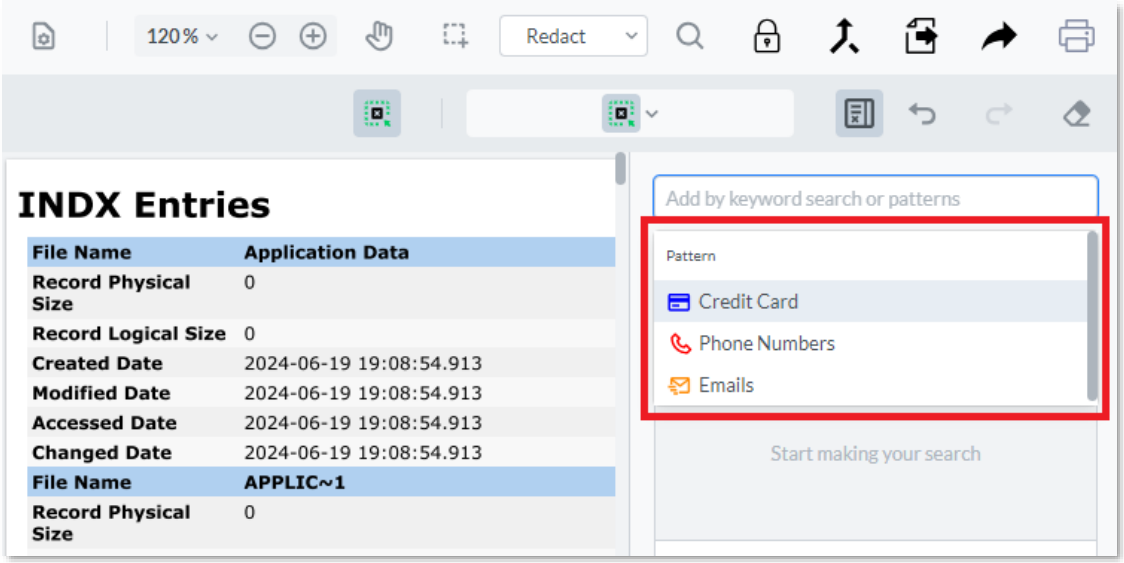
The image view allows you to automatically identify, locate, and redact specific information present across the file.

To automatically redact specific information in the file:

1. Upon selecting the **Redact** option from the **Image View** drop-down, click on the **Redaction Panel** icon
2. Search for the required keyword or provide the required regex pattern in the Redaction Panel.

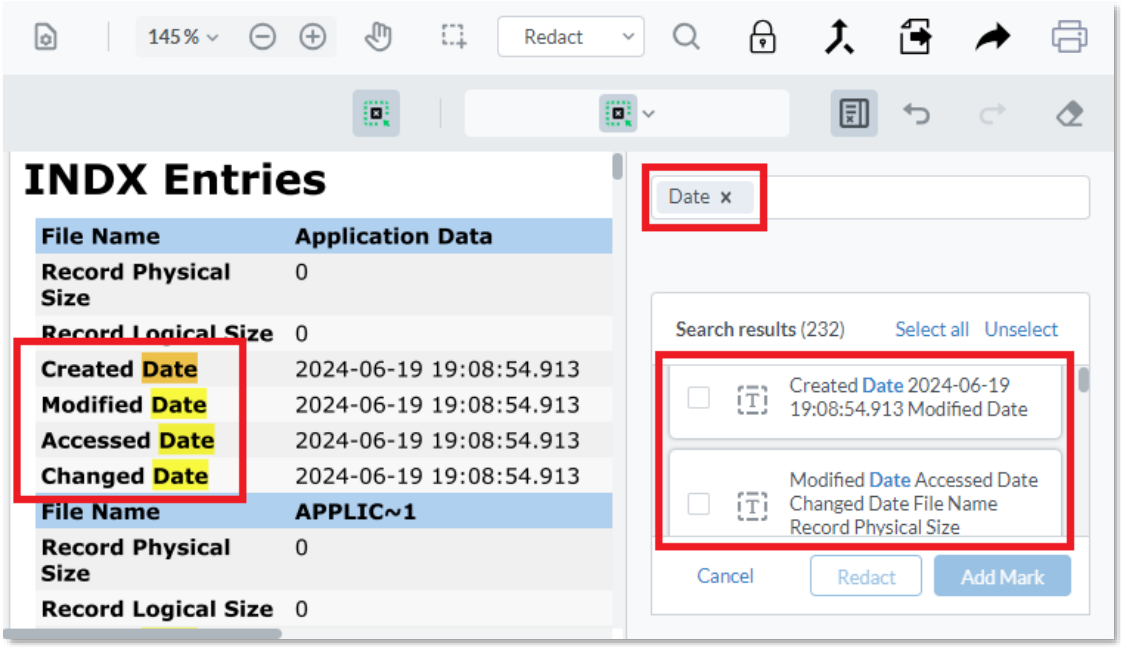
Tip: By default, the regex patterns to identify the following entities will be displayed while trying to perform the search operation. You can click on the required pattern to search and identity the corresponding information in the file:

- Credit Card
- Phone Numbers
- Emails



© Exterro, Inc. All rights reserved

3. The keywords will be highlighted in the document (left pane) and its occurrences will be listed in the Redaction Panel (right pane).



4. Select the required occurrences from the Redaction Panel and click on any of the following buttons to perform the corresponding action:

- **Redact** – The selected content will be redacted, and the changes will be burned into the file.
- **Add Mark** – The selected content will be marked for redaction. You can burn the redactions later by clicking on the **Burn in Redactions** button.

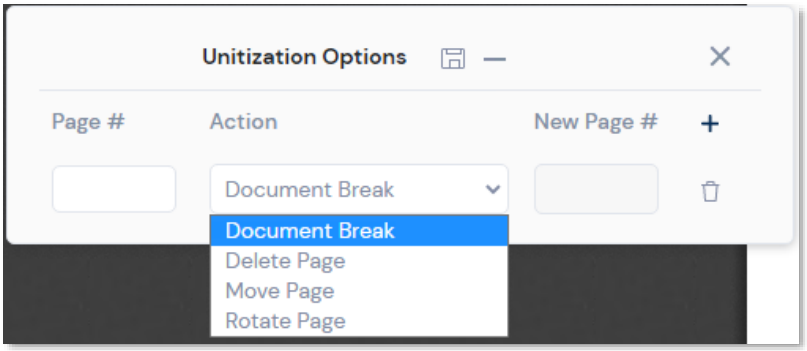
© Exterro, Inc. All rights reserved

Unitization

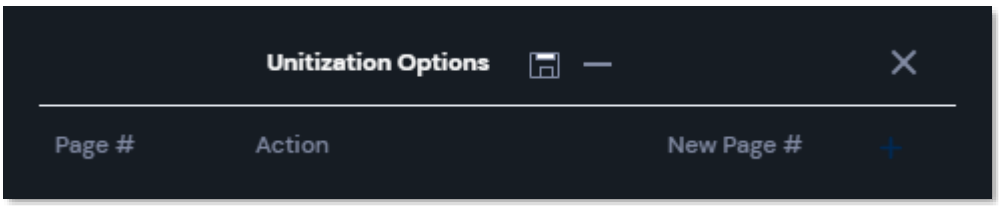
FTK Central allows you to split or merge imaged documents into child documents by using the process of unitization.

To reorder a document:

Unitization allows users to edit documents visually by giving the ability to create document breaks, delete, move and rotate pages.



1. Click the **Image** in the Viewer.
2. Click the **Unitization** button.
   - The **Unitization Options** prompt is displayed.



3. Click **+**.
4. Select the required **Action**.
5. Enter the **New Page #** based on which the selected **Action** should be performed.
6. Click the **Save** button.

© Exterro, Inc. All rights reserved

Restore Original PDF

There may be times where the documents reviewed have been incorrectly processed and/or poorly reviewed by a user. FTK Central allows users to restore documents as they were first processed within a case.

To restore original PDF:

1. Click the **Image** in the Viewer.
2. Click .
3. The restore process will begin.

Slip-sheet Maker

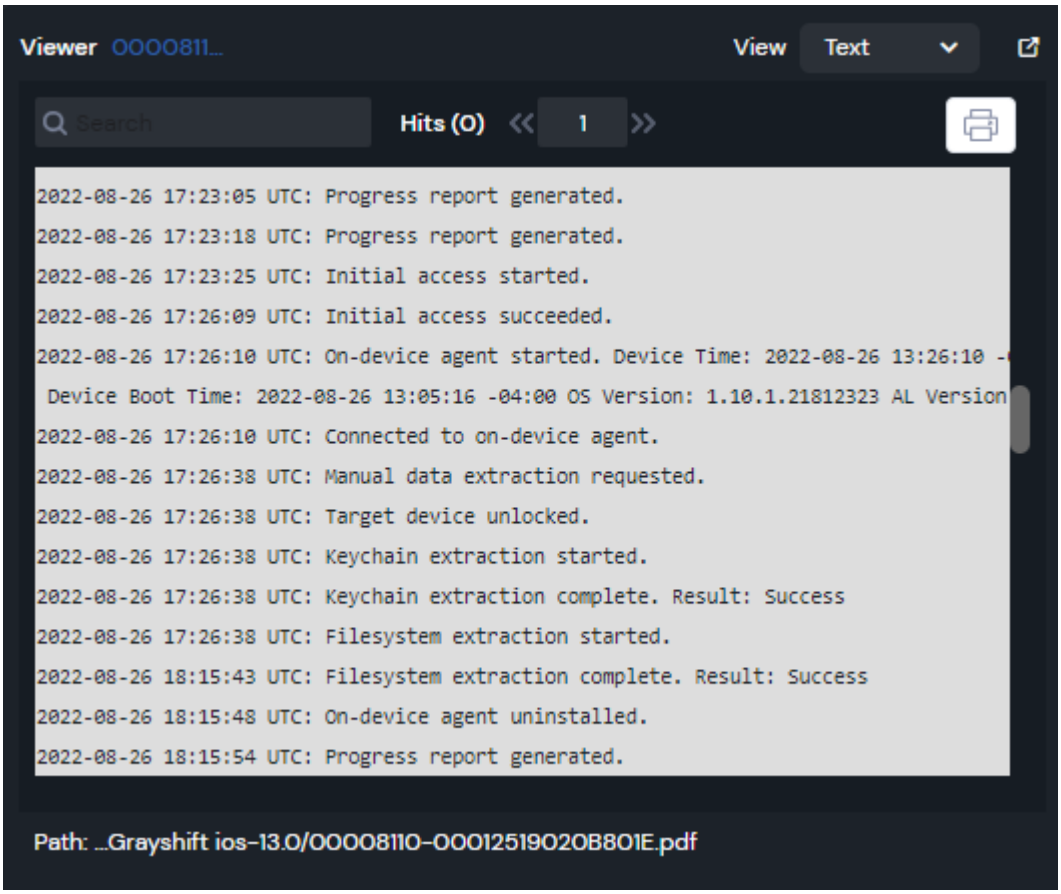
Custom Slipsheets allow users to automatically replace pages in a document or across a case during the review process.

See Performing Actions In the Grid: Productions section.

© Exterro, Inc. All rights reserved

Using the Text Panel

Upon clicking on **Text** view, you can view the text content extracted from the selected file.



Tip: OCR text will appear in this panel.

Using the Viewer Panel on Another Monitor

During the review process, you may need to use the viewer on another monitor or on a smaller scale. Snapping out the viewer allows you to use the panel as you wish.

Click the **Pop Out** button to create a new browser window strictly for the viewer.

© Exterro, Inc. All rights reserved

Using the Desktop Viewer

Users can utilize the FTK Central viewer to review a multitude of file types, however it can be a timely task when reviewing multimedia file types as certain file types require conversion. The Desktop view (FTK Plus Lite viewer) allows users to review file types instantly using a barebones version of FTK Plus without any prior conversion.

Users that do not currently have access to this viewer will be prompted to download it when attempting to open this viewer within the FTK Central UI. The installer will be downloaded from the FTK Central app server.

Click the **Desktop viewer** button to open the external viewer.

Moreover, the FTK Central Desktop Viewer supports multiple sessions, based on the workflow below:

- **While using multiple sessions via multiple browsers:** One desktop viewer will be generated for each browser, displaying the content of the corresponding session.
- **While using multiple sessions via multiple tabs in the same browser:** One desktop viewer will be generated for the browser and the content in the viewer will be updated/changed based on the tabs selected.

Please refer to the FTK Plus User Guide for more usage information; FTK Plus Lite viewer functionality is not limited when used with FTK Central.

© Exterro, Inc. All rights reserved

Exporting

Within the Review portal, you can export files in native format or a file list without having to use the export wizard. This export will create a CSV file with item list details maintaining the current column layout. Additionally, users have the option to utilize the export wizard to create images and load files with specific parameters.

Elements of Exporting

Exporting Grid to CSV	• Exporting Grid to CSV
Export Wizard	• AD1 – Optional Configuration • Native – Optional Configuration • Load Files – Optional Configuration • Imaging – Optional Configuration • Text – Optional Configuration • Numbering – Optional Configuration • Summary

Exporting Grid to CSV

To export Grid to CSV format:

1. In the Grid, Right-click on the file list.
2. Click **Export to CSV**.

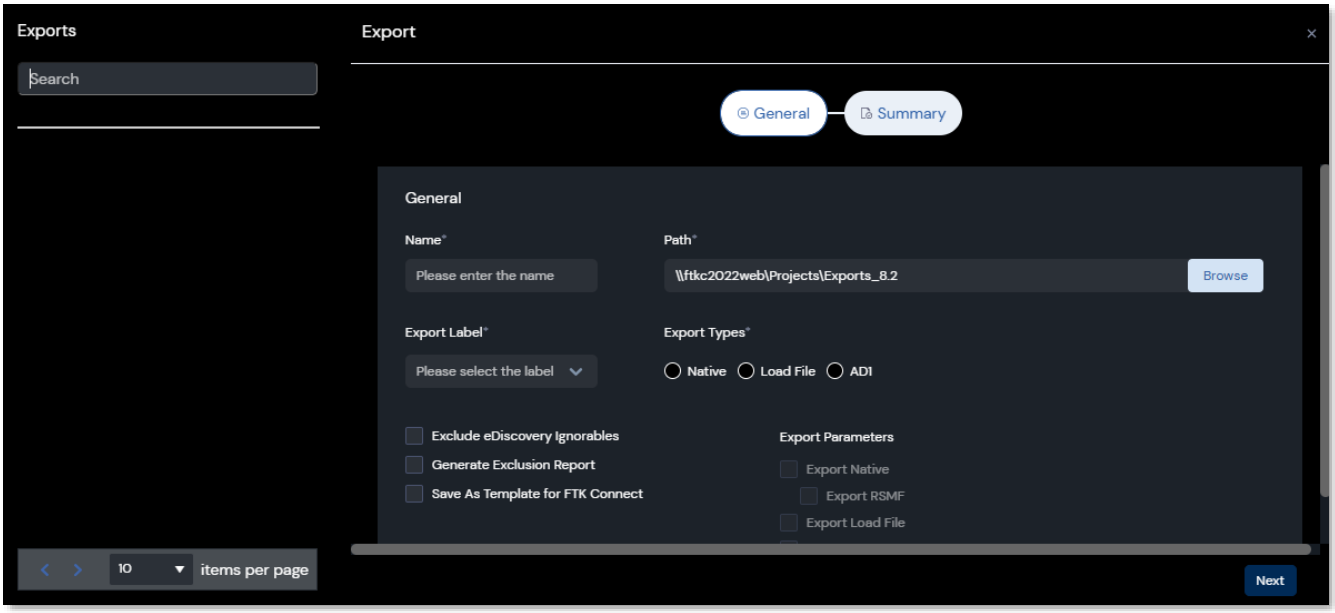
The CSV export will begin but the operation may take some time to complete depending on the file size.

© Exterro, Inc. All rights reserved

Export Wizard

You can export files that you find in an investigation to process and distribute to other parties. For example, you can export files that may need further review by external resources.

You can click on to access the Export Wizard.



© Exterro, Inc. All rights reserved

To export using the export wizard:

1. In the Grid, click the **Export** button.
   - The **General** section in the Export dialog will be displayed.
   - Specific to an open case, **Previous Exports** will be displayed.

2. Provide the export file **Name**.
3. Provide the file location **Path** where the exported file(s) should be stored.
4. Select the labels for the **Export Labels** field, only the files with these selected labels applied will be added to the exported file.
5. Select any one of the below provided **Export Types**:
   - **Native** – To export the files into their original file type.
   - **Load File** – To export the files in a load file format.
   - **AD1/L01** – To export the files in AD1/L01 file format.

6. Enable the following option based on your requirements:
   - **Exclude eDiscovery Ignorables** – To exclude the duplicates, containers, and eDiscovery refinement files during the export process.
   - **Generate Exclusion Report** – To generate a report consisting of the details related to the files that were excluded from the exported files list.
   - **Save as Template for FTK Connect -** To save specific export options as a template and use it within FTK Connect.

Note: The templates created using this option can be selected only during FTK Connect exports.

   - **Copy from Previous Export –** To reuse existing export parameters from a previous export.

7. Select the **Export Parameters**.

   - **Native –** To export all files in their native formats.

© Exterro, Inc. All rights reserved

- **RSMF –** To export all the chat and conversations in the Relativity Short Message Format (RSMF).

- **Images –** To export all files in the image format.
- **Text –** To export all files in the text format.
- **Load File –** To export all files in the load file format.

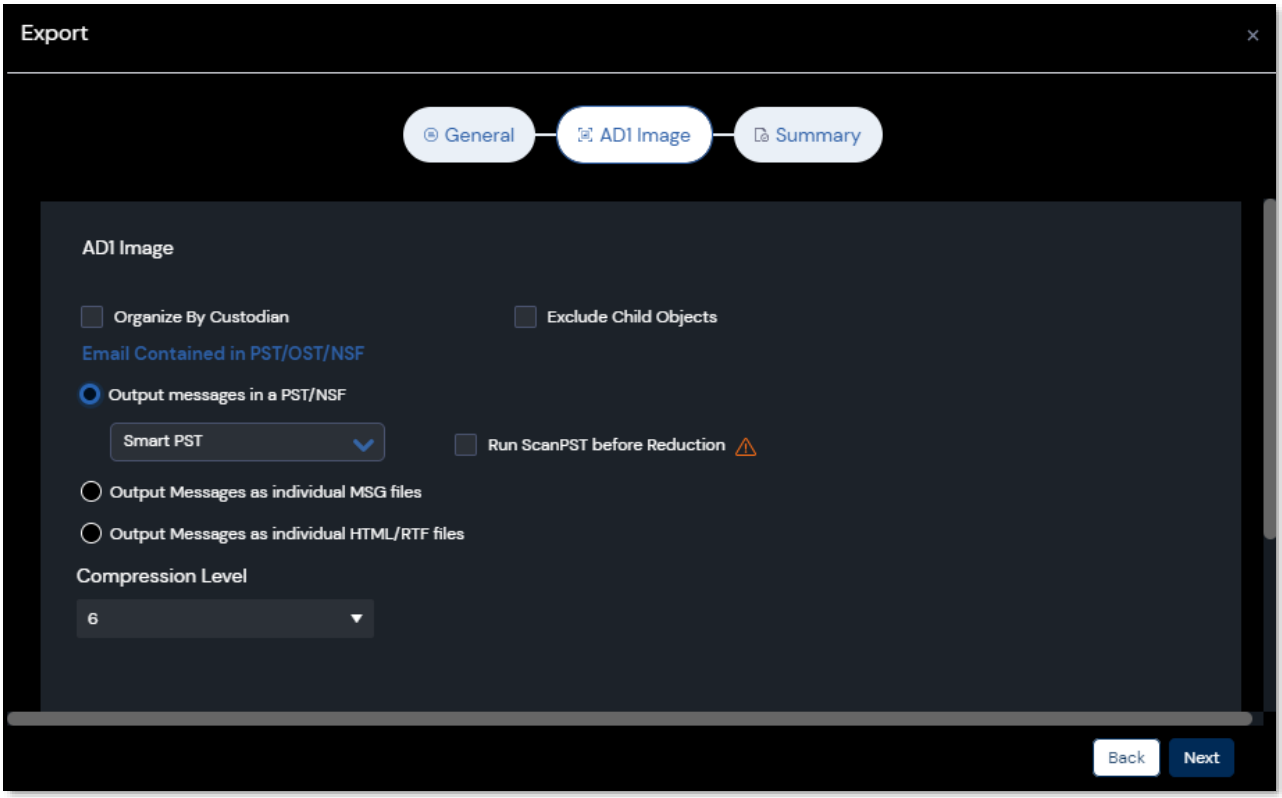
Note: Upon exporting the chats and conversations in RSMF format (**Export RSMF** option), the messages translated in FTK Central will not be displayed in the exported RSMF JSON file.

8. Click **Next**.

You will be navigated to the next section based on the selections made for **Export Types** and **Export Parameters** fields in the next section.

© Exterro, Inc. All rights reserved

AD1 – Optional Configuration



Note: These configuration options will only appear if **AD1** was set as the Export Type within the **General** export wizard configuration.

To configure AD1 options:

1. If required select **Organize by Custodian**.
    - When this option is checked, associated outputs will be stored in folders named after a custodian(s).
2. If required select **Exclude Child Objects**.

© Exterro, Inc. All rights reserved

3. Select any of the following options for **Email Contained in PST/OST/NSF**.
   - **Output message in PST/NSF**
     a) **New PST** – This option is recommended when there are only a few files present for export.
     b) **Reduced PST** – This option is recommended when there are a large number of files present for export.
     c) **Smart PST** – Upon selecting this option, the application will calculate the number of files and selects the best option (**New PST** or **Reduced PST**) to perform the operation with faster results.
        i) **Run ScanPST before Reduction** - Upon selecting this option, the application will attempt to recover and fix the structure of the corrupted PST files.

Note: The **Run ScanPST before Reduction** option will be displayed only when the **Smart PST** or **Reduced PST** option is selected.

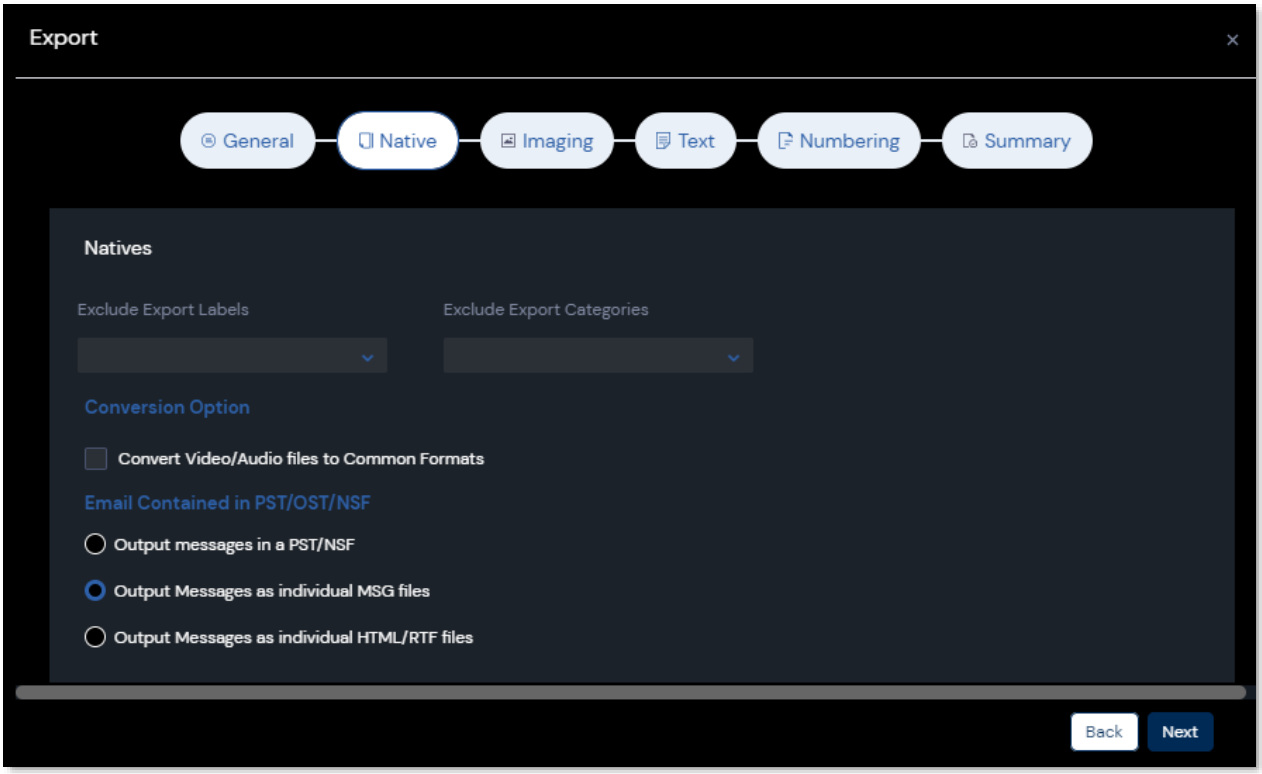
   - **Output Messages as individual MSG files**.
   - **Output Messages as individual HTML/RTF files**.

Note: When creating AD1 exports, the **Estimated Export Size** is shown in the summary page. This information may take some time to load depending on the size of the export.

4. Select a **Compression Level**.
   - By default, the compression level will be set to 6.
   - A compression level of 0 will have no compression.
   - A compression level of 9 will have the highest level of compression. This will create the smallest file but will take the longest to create.

© Exterro, Inc. All rights reserved

Native – Optional Configuration



Note: These configuration options will be displayed only when the **Native** or **Load file** option is selected for the **Export Types** field in the **General** section.

© Exterro, Inc. All rights reserved

To configure native file options:

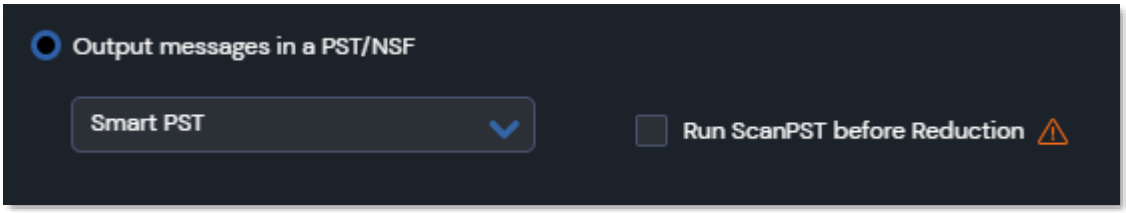
1. Select **Exclude Export Labels**.
2. Select **Exclude Export Categories**.
3. Enable the **Convert Video/Audio files to Common Formats** option if you want to export the audio and video files into the MP3 and MP4 formats respectively.

Note: When this option is enabled, all audio and video files in different formats (other than MP3 and MP4) will be converted to MP3 and MP4 formats respectively and stored in the **Converted files** folder after the export.

However, this conversion process will not be performed for the files that are already in MP3 and MP4 formats and such files will be stored outside the **Converted files** folder.

© Exterro, Inc. All rights reserved

4. Select any one of the following options for **Email Contained in PST/OST/NSF**.
   - **Output message in PST/NSF**



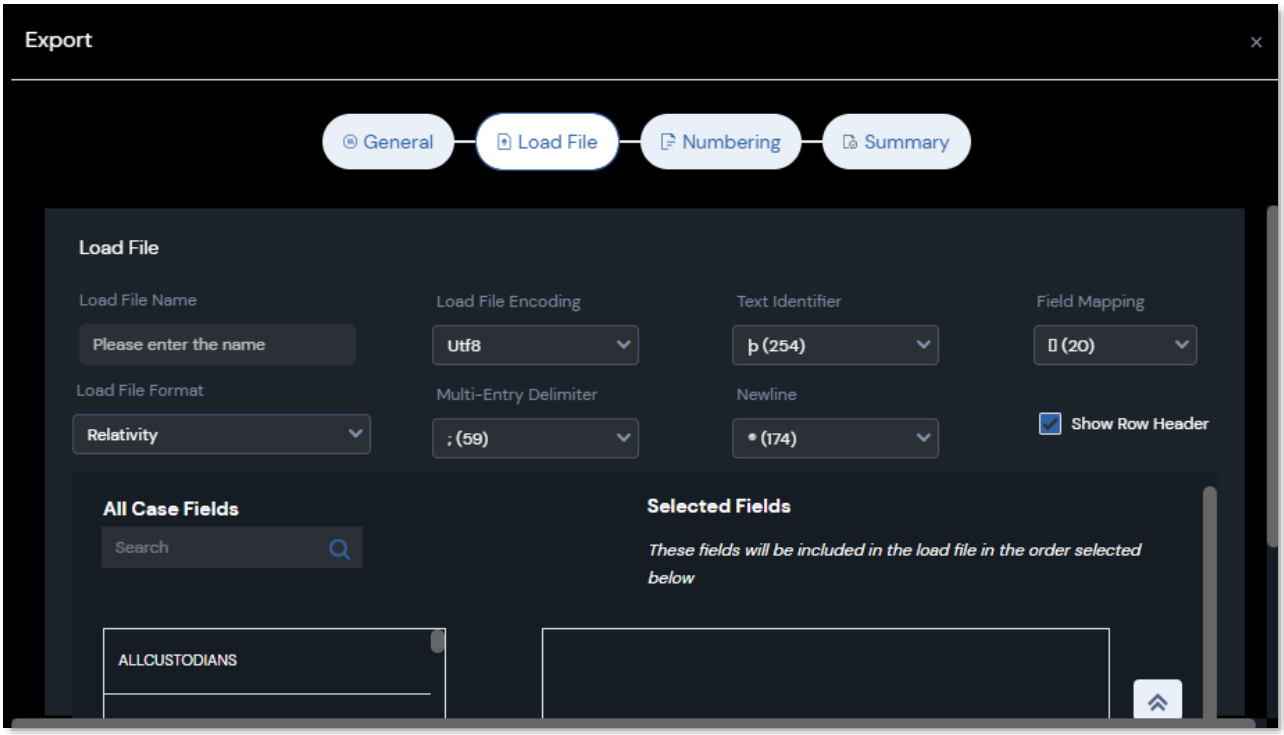
- **New PST** – This option is recommended when there are only a few files present for export.
- **Reduced PST** – This option is recommended when there are a large number of files present for export.
- **Smart PST** – Upon selecting this option, the application will calculate the number of files and select the best option (**New PST** or **Reduced PST**) to perform the operation with faster results.
  i) **Run ScanPST before Reduction** - Upon selecting this option, the application will attempt to recover and fix the structure of the corrupted PST files.

Note: The **Run ScanPST before Reduction** option will be displayed only when the **Smart PST** or **Reduced PST** option is selected.

- **Output Messages as individual MSG files**.
- **Output Messages as individual HTML/RTF files**.

© Exterro, Inc. All rights reserved

Load Files – Optional Configuration



Note: These configuration options will only appear if the **Load File** option was selected within the **General** export wizard configuration.

© Exterro, Inc. All rights reserved

To configure load file options:

1. Select a **Load File Name.**
2. Select a **Load File Format**.

- Select all files to be included in the load file.

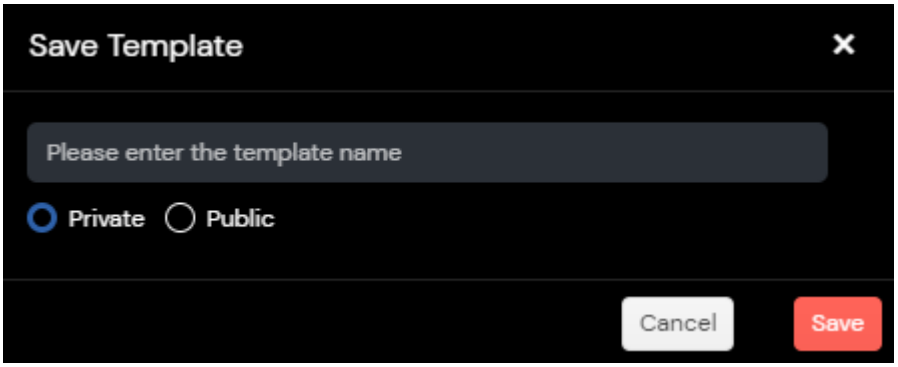
Note: Alternatively, you can select any of the **Default Templates** present at the bottom of the page:

- FTK Central Export Template
- FTK Central Email Export Template
- Relativity Export Template
- Relativity Email Export Template
- Direct Relativity Export Template
- DOJ_CART Standard
- MQ-LTemplate

© Exterro, Inc. All rights reserved

To save a load file template:

1. Select the fields you want included in the load file.
2. Click on the **Save Template** button.
    - The **Save Template** pop-up is displayed.



3. Provide a template name.
4. Select any of the below options:

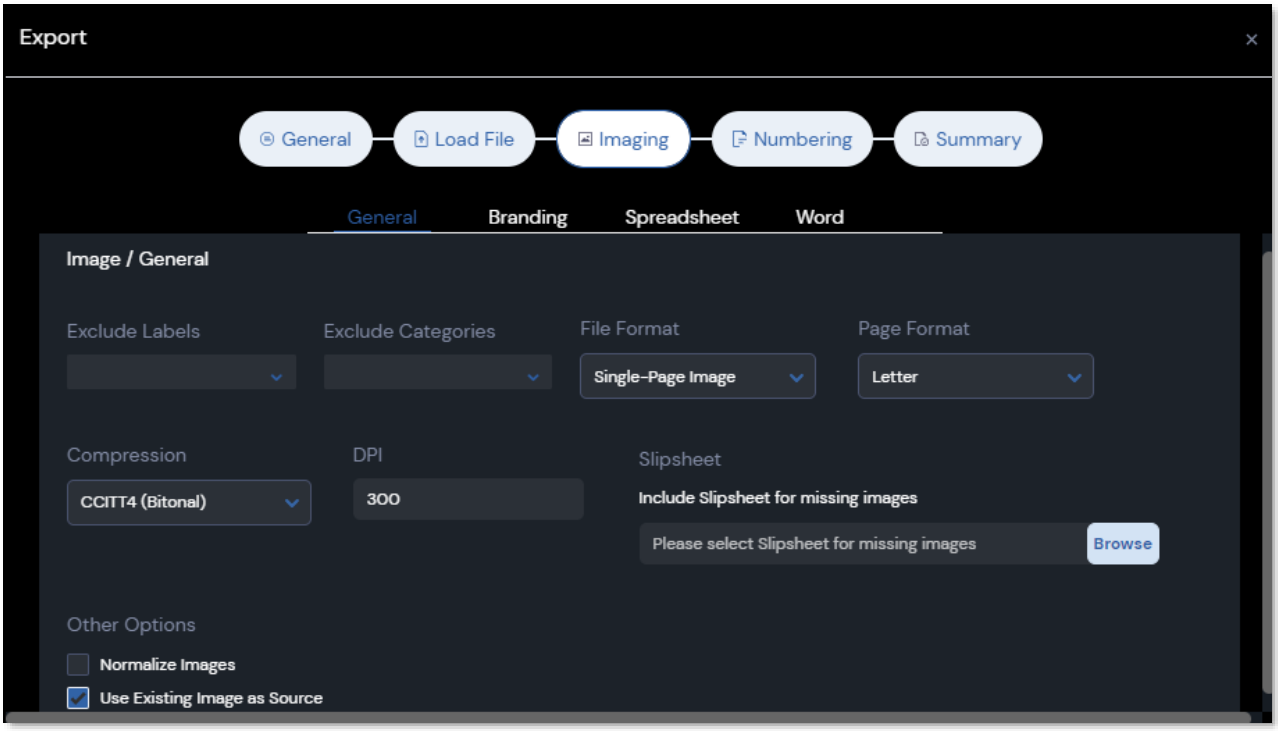
- **Private** – The load file template will be made accessible only for the user who create it.
- **Public** – The load file template will be made accessible by all users with export permissions.

5. Click on the **Save** button.

Note: You can update and overwrite the user created templates but cannot save over a system default template.

© Exterro, Inc. All rights reserved

Imaging – Optional Configuration



Note: These configuration options will only appear if **Export Images** was selected within the **General** export wizard configuration.

To configure imaging options:

1. Select **Image/General** configurations.
2. Set any other configurations:

© Exterro, Inc. All rights reserved

General:

- Exclude labels
- Excluded Categories
- File format
- Page format
- Placeholder images for missing images
- Other options
- Normalize images
- Produces searchable pdf

Branding:

- Watermark
- Header/Footer

Spreadsheet:

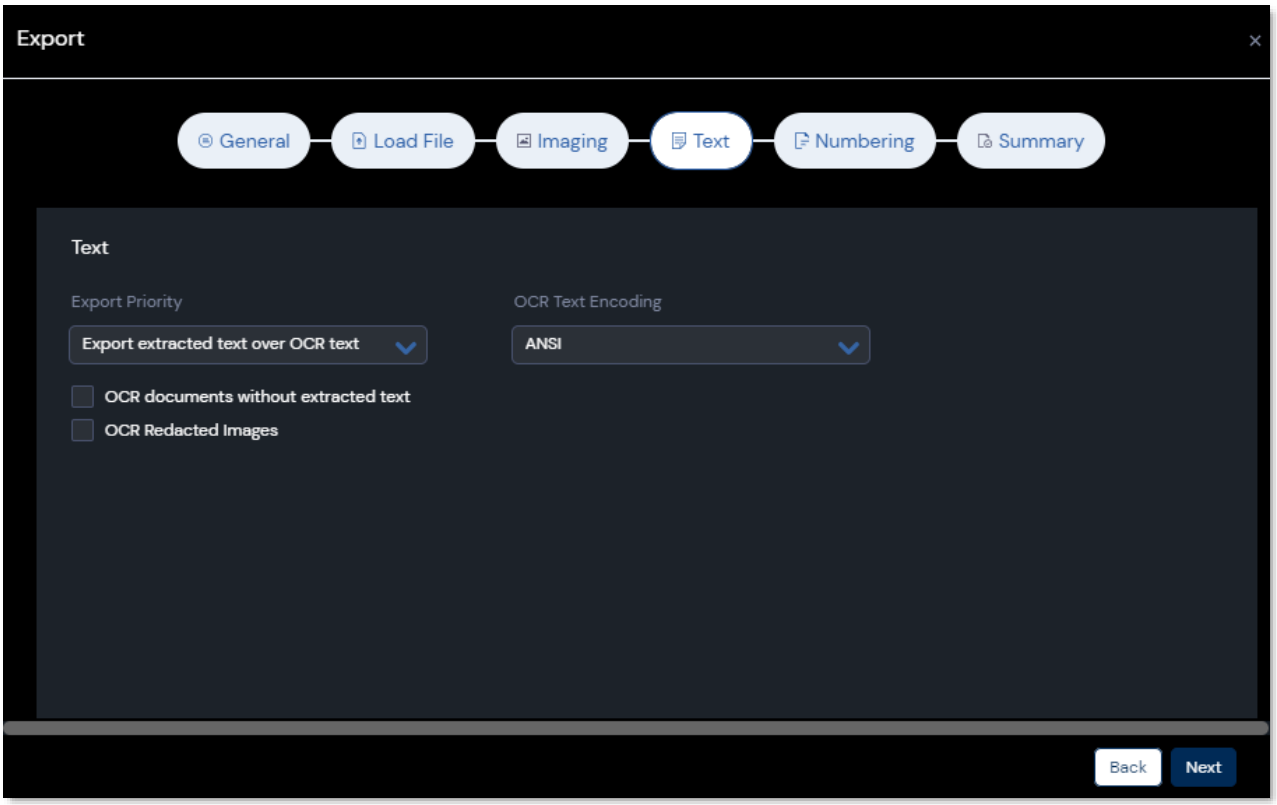
- General Excel Imaging Options
- Page
- Printing
- Formula Substitutions

Word

- General Word Imaging Options
- Formula Substitutions
- Page

© Exterro, Inc. All rights reserved

Text – Optional Configuration



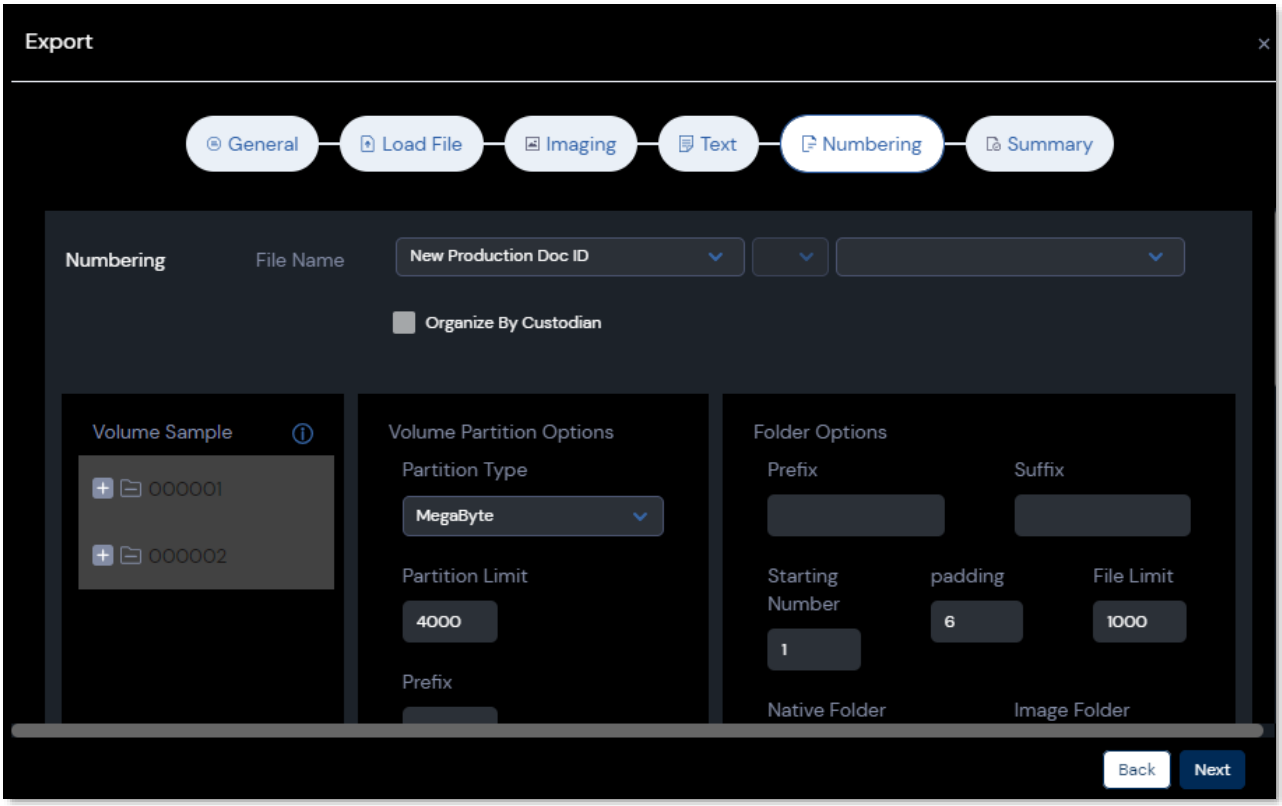
Note: These configuration options will be displayed only when the **Export Text** option was selected within the **General** export wizard configuration.

To configure text options:

1. Select **Export Priority**.
2. Select **OCR Text Encoding**.
3. If required, select **OCR documents without extracted text**.
   - Choosing this option will evaluate each item for the existence of text content, if none is found, the document will be OCR'ed.
4. If required, select **OCR Redacted Images**.
   - Choosing this option will OCR images that have been redacted.

© Exterro, Inc. All rights reserved

Numbering – Optional Configuration



To configure numbering options:

1. Verify the **Volume Sample**.
2. Configure the **File Name** by selecting a field in the first list. This cannot be empty.
    - New Production Doc ID
    - Original Doc ID
    - Original File Name
    - Original File Name with Original Path
        - If this option is selected, the preceding lists will be disabled.

© Exterro, Inc. All rights reserved

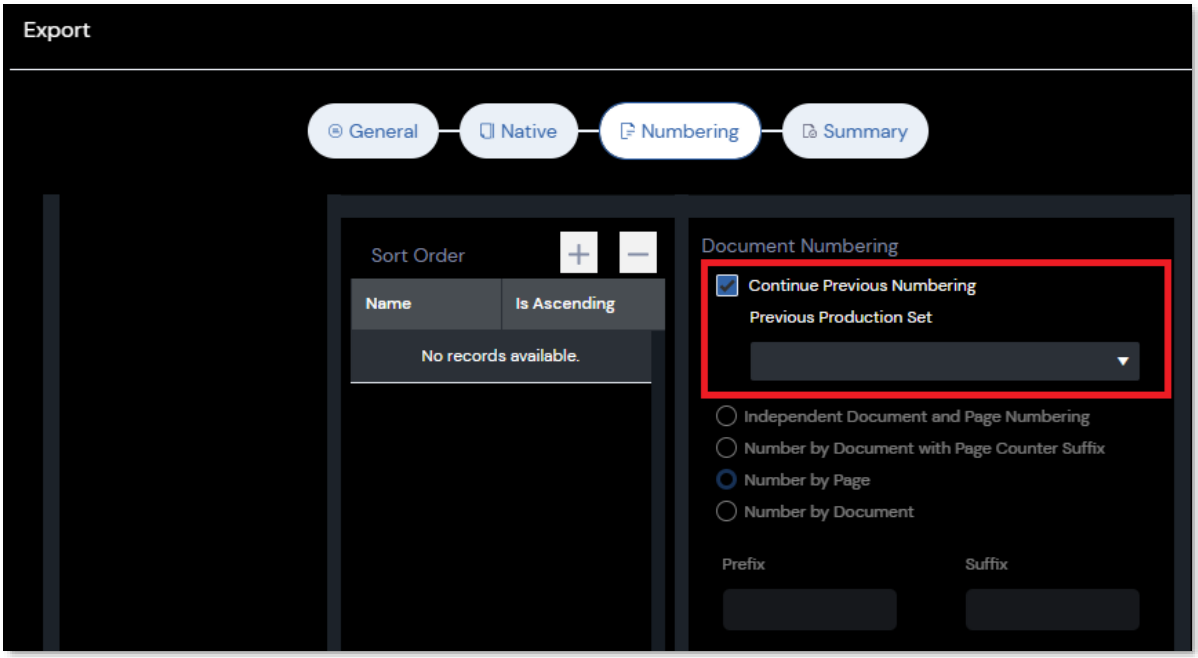
- Additionally, **Volume Partition Options, Folder Options, Sort Order** and **Document Numbering Options** will be disabled.
- **Organize By Custodian** can be toggled when selecting Original File Name with Original Path. When this option is checked, associated outputs will be stored in folders named after a custodian(s).

- Alternatively select any other columns fields.

3. If required, select a **delimiter option** followed by an additional file name column field value.
4. Select **Volume Partition Options**.
5. Select **Folder Options**.
6. Select a **Sort Order**.
7. Select **Document Numbering**.
   - Independent Document and Page Numbering.
   - Number by Document with Page Counter Suffix.
   - Number by Page.
   - Number by Document.

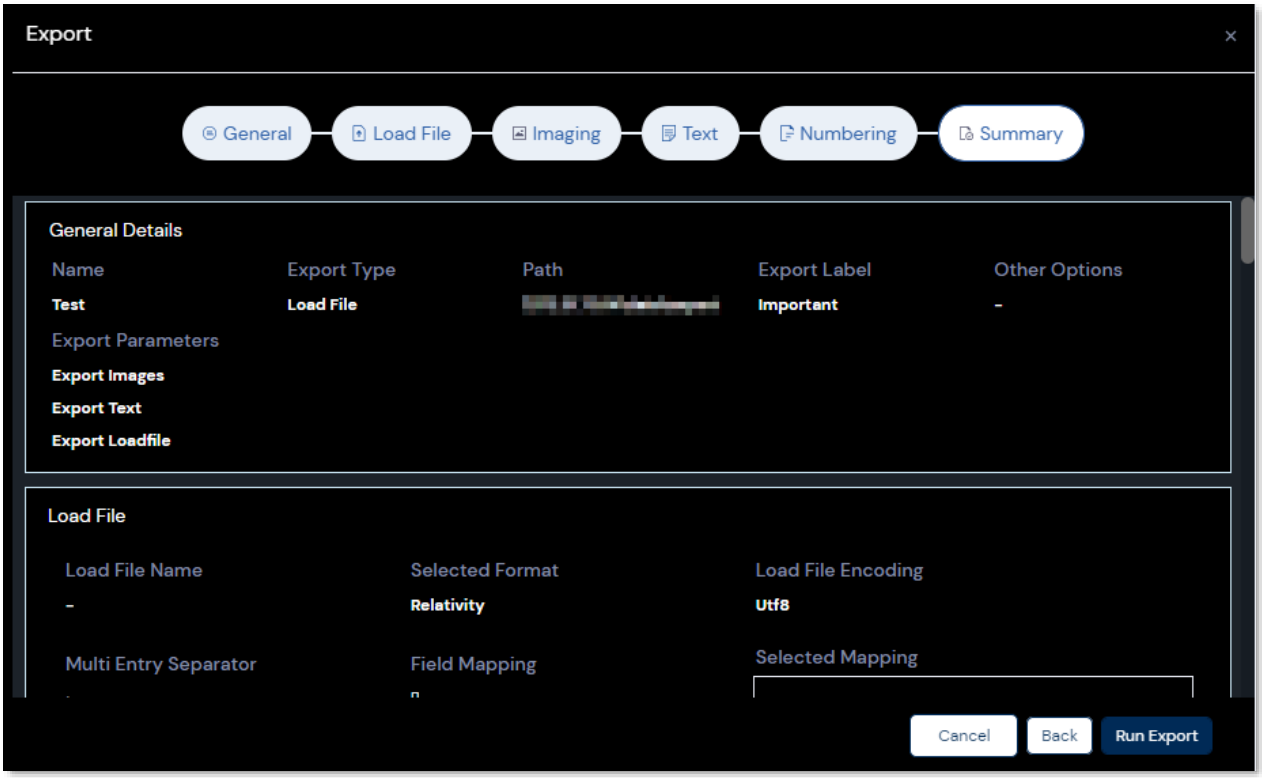
© Exterro, Inc. All rights reserved

Note: You can also choose to continue the numbering from an existing production by enabling the **Continue Previous Numbering** option and selecting the required **Production set** from the dropdown.



© Exterro, Inc. All rights reserved

Summary



Click **Run Export** to start the exporting process.

© Exterro, Inc. All rights reserved

Reviewing Cases

While using FTK Central, you are able to use the review portal. This portal allows you to filter and search data while being able to label and book mark any data of interest to then create summary reports.

Elements of Reviewing Cases

Filtering	• Types of Filers • Exclusion Filter • Quick Filter • Common Filter • Artifacts Filter • Evidence Explorer • Column Filters
Searching	• Simple Searching • Relationships • Advanced Searching
Working with Labels	• Creating Labels • Editing Labels • Deleting Labels • Applying Labels • Creating Label Groups • Editing Label Groups • Filtering for Labels
Working with Bookmarks	• Creating Bookmarks • Editing Bookmarks • Deleting Bookmarks • Applying Bookmarks

© Exterro, Inc. All rights reserved

	• Bulk Bookmarking • Filtering for Bookmarks
Sharing Tags	• To share Tags
Creating Reports	• Report Types • Creating a Detail Report • Creating a Search Term Report • Exporting Reports • Viewing and Downloading Completed Reports

© Exterro, Inc. All rights reserved

Filtering

Filters let you leverage item attributes to locate specific data very quickly. They reduce the amount of time that you must examine data because they can narrow a large data set down to a very specific focus. You can also use filters to exclude data that you do not want displayed. For example, if you only want to see encrypted items, you can apply a filter to show you those. If you do not want to see files that were created after a certain date, you can also use a filter to exclude those files from being displayed.

Types of Filters

The following are the different types of filters that can be used to filter files in the Review page:

Filter Type	Description
Predefined Filters	Predefined Facet Filters are filters that Exterro has created. For example, there is a predefined filter called Graphic Files that limits the displayed data to graphics files only. You cannot delete or modify a predefined filter,
Quick Filters	Quick Filters allow you to use commonly used filters without having to find them yourself. These filters are considered as commonly used filters within the review process.
Nested Filters	A nested filter is a filter that contains filters within it. Nested filters let you leverage several filters together to accomplish a specific goal. Nested filters prevent you from having to create a complicated custom filter each time you need to use multiple filters together. For example, a simple nested filter could include both Graphic Files and KFF Alert Files as filters. **Simply select multiple filters.**

© Exterro, Inc. All rights reserved

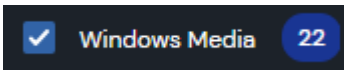
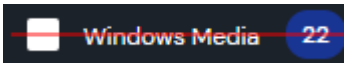
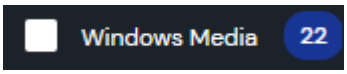
Filter Type	Description
Search Filters	Search filters are added to a live search or an index search. They limit a search to only display results that match the criteria contained within the search. **Simply run a search and apply a filter.**
Exclude Filters	This option allows users to exclude the selected file types from being displayed in the File List.

© Exterro, Inc. All rights reserved

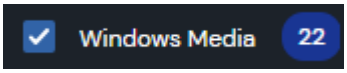
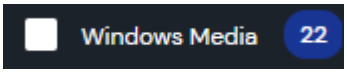
Exclusion Filter

You can make use of the exclusion filter by enabling the **Explorer** toggle.

When the Explorer toggle is enabled:

Action	Filter Representation	Description
Click on the checkbox the first time		The inclusion filter is enabled i.e., only the selected file types will be displayed in the Item List.
Click on the checkbox the second time		The exclusion filter is enabled i.e., file types other than the selected file types will be displayed in the file list.
Click on the checkbox the third time		The filter is disabled

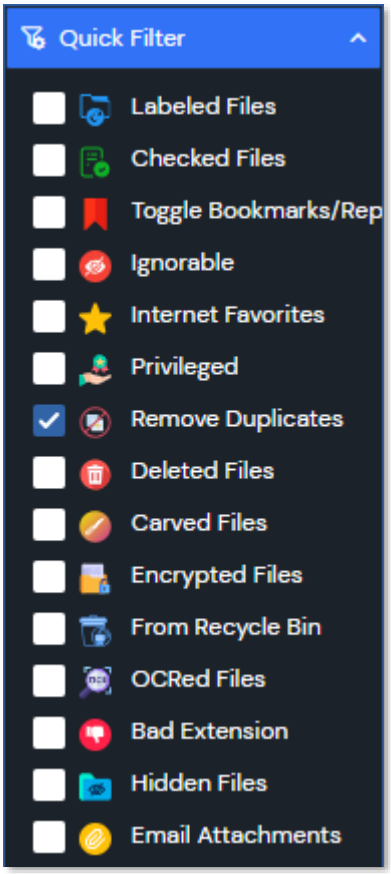
When the Explorer toggle is disabled:

Action	Filter Representation	Description
Click on the checkbox the first time		The inclusion filter is enabled i.e., only the selected file types will be displayed in the Item List.
Click on the checkbox the second time		The filter is disabled

© Exterro, Inc. All rights reserved

Quick Filter

Quick Filter provides you with the predefined set of filter types to aid you during review.



You can access the filters by expanding the **Quick Filter** section from the **Explorer** pane.

Filters
• Bad Extension
• Bookmarks
• Carved Files
• Checked Files
• Deleted Files
• Ediscovery Refinement

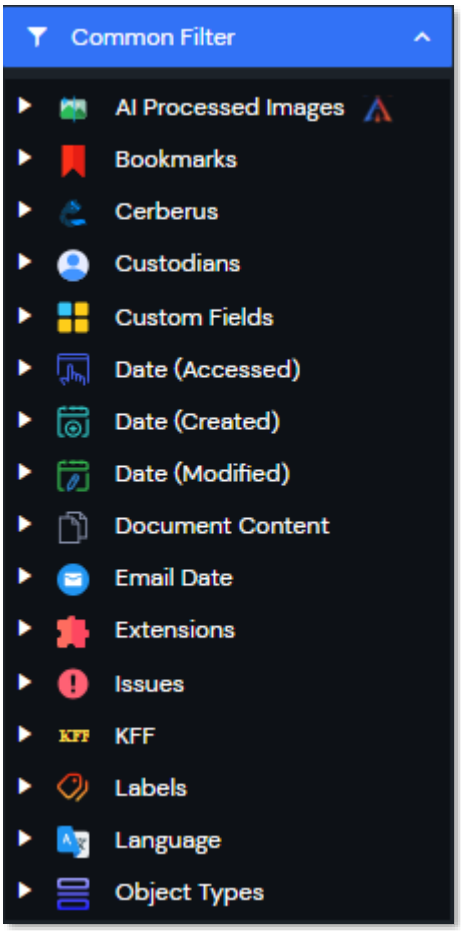
© Exterro, Inc. All rights reserved

Filters
• Email Attachments
• Encrypted Files
• From Recycle Bin
• Geo Location
• Hidden Files
• Ignorable
• Internet Favorites
• Labeled Files
• OCRed Files
• Privileged
• Remove Containers
• Remove Duplicates
• Remove Notes and Bookmark Files
• Translated Files

© Exterro, Inc. All rights reserved

Common Filter

The filter section provides you with all the common filtering options related to the files present in a case.



Filters
AI Processed Images
Bookmarks
Cerberus
Custodians

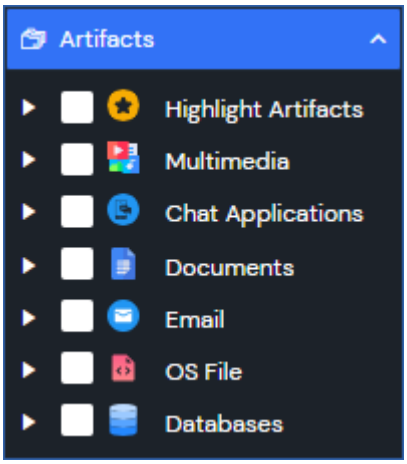
© Exterro, Inc. All rights reserved

Filters
Custom Fields
Date (Accessed)
Date (Created)
Date (Modified)
Document Content
Email Date
Extensions
Issues
KFF (Known File Filters)
Labels
Language
Object Types
Production Sets
Size
Status
Viewed Status

© Exterro, Inc. All rights reserved

Artifacts Filter

This section provides you with the list of filters grouped up based on the corresponding file types.



Filter Group

Highlight Artifacts

- Search Keywords
- Passwords
- From Recycle bin
- User accounts
- Last logged on users
- Desktop Items
- Most Recent commands
- RDP events
- Device information
- Apple Wifi locations

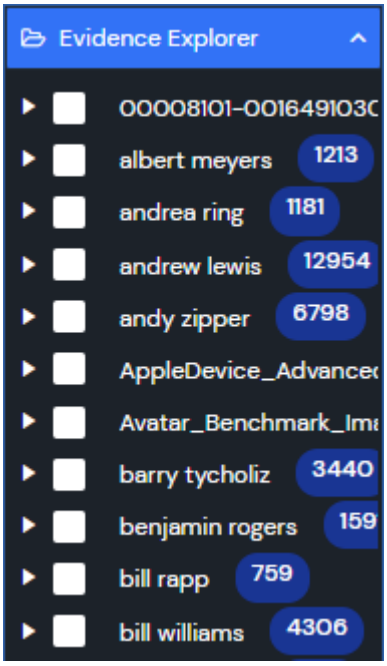
© Exterro, Inc. All rights reserved

Filter Group
• Significant Locations • Parked Location • Map search location • Google Maps location • Sim Card Information • UFDR Extraction Summary • XRY Extraction Summary • UFD Extraction Summary • iOS Connected Account Information • iOS Device Information
Mobile
Chat Applications
Documents
Email
Multimedia
OS Files
System Summary
Databases
OS Info
Geolocation
Internet & Browsers

© Exterro, Inc. All rights reserved

Evidence Explorer

This section lists all the evidence present in a case. You can select the required evidence to view only the files associated with it.



© Exterro, Inc. All rights reserved

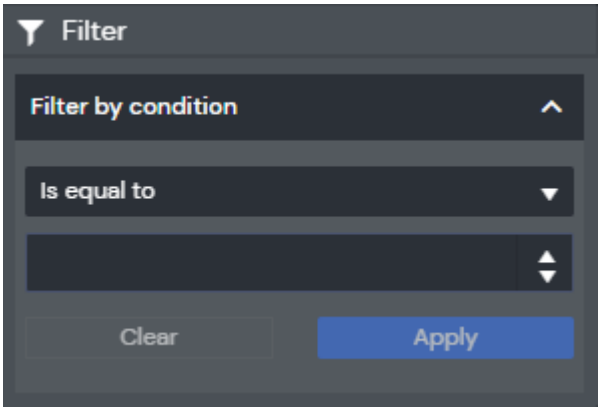
Column Filters

While in the process of reviewing records using the Files List, there may be times where you may want to filter the contents of a specific column. An example would be filtering the column for extensions. You can click the Filter icon located on each column to then create a filter of your own.

Upon clicking the Filter icon, you will be prompted with a filter creation window. It is simple to use and only requires a custom value to be filtered. The following are the two types of filtering used in columns:

Filter by condition:

The following table lists the possible operators that can be found in the filter options. The operators available depend upon what property is selected.



Operator	Description
Contains	Searches for a text string that contains the value that you have entered in the value field. This operator is available for text string filtering.
StartsWith	Searches for a text string that starts with the value that you have entered in the value field. This operator is available for text string filtering.
EndsWith	Searches for a text string that ends with a value that you have entered in the value field. This operator is available for text string filtering.

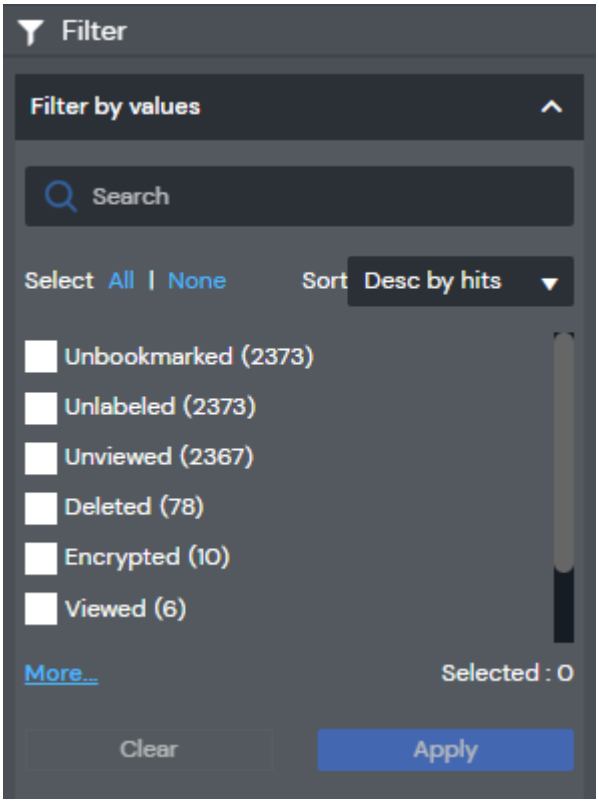
© Exterro, Inc. All rights reserved

Operator	Description
Is equal to	Searches for a value that equals the property selected. This operator is available for almost all value filtering and is the default value.
Is not equal to	Searches for a value that does not equal the property selected. This operator is available for almost all value filtering.
Is greater than or equal to	Searches for a value that is greater than and/or equal to the property selected. This operator is available for numerical value filtering.
Is greater than	Searches for a value that is greater than the property selected. This operator is available for numerical value filtering.
Is less than or equal to	Searches for a value that is less than and/or equal to the property selected. This operator is available for numerical value filtering.
Is less than	Searches for a value that is less than the property selected. This operator is available for numerical value filtering.
Is Empty	Searches and retrieves records for which no values are present in the corresponding column.
Is Not Empty	Searches and retrieves records for which the corresponding column is not empty.

© Exterro, Inc. All rights reserved

Filter by values:

This column filter type will display all the values present in the corresponding column from which you can select and filter the required values.



© Exterro, Inc. All rights reserved

To apply a column filter:

1. In the Grid navigate to the Grid.
2. Click the **Context menu** button against the required column header.
3. Click the **Filter** button.
   - **Filter by Condition** – allows users to filter using an applicable condition type such as the date.
   - **Filter by Values** – allows users to filter using the values present in the column such as an object name or extension.

Note: You can also search for records with blank values by selecting the 'Blank' value from the column filter.

4. Configure the filter and click **Apply**.

© Exterro, Inc. All rights reserved

Searching

You can use searching to help you find files of interest that are relevant to your case. After you perform a search, you can save your search or share your search with groups. Then, you can filter your result set to further cull down evidence. As you find relevant files, you can tag the files with Labels, Issues, or Categories for further review or for export.

When you search data, you use search phrases to find relevant evidence. A search phrase is any item that you would receive a search hit on, such as a word, a number, or a grouping of words or numbers.

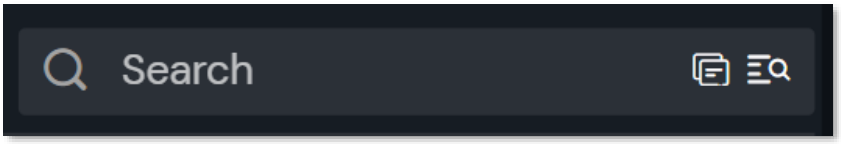
You can search for text that is either in the metadata of the file or in the body of a file. You can also select a column in the Grid and filter on that specific column.

When you start a search, be mindful of the items in the list that you are starting with. For example, if you have applied a facet filter to show only DOC files, and you search for a text string that you think is in a PDF file, it will not find it. However, the same is not true for column filters. If you have applied a column filter to show only DOC files and you search for a text string that you think is in a PDF file, it will locate the file, regardless of the previous column filter application.

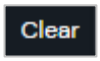
© Exterro, Inc. All rights reserved

Simple Searching

The Index Search Bar is where you can conduct a query of the Text Index. Index Search allows for fast searching based on keywords. Your evidence must be indexed in order to perform index searches. Indexing can be done either when evidence is added to your case or later. While indexing takes longer when you add evidence items, it is well worth it if you later need to do a search. This search is very quick and produces case specific results rapidly.



To perform the basic search, provide the required search term in the search bar and click on or press Enter.

Note: After performing a search, you can click on against the required search term to remove it or click the **Clear**  button to remove all the search terms.

Relationships

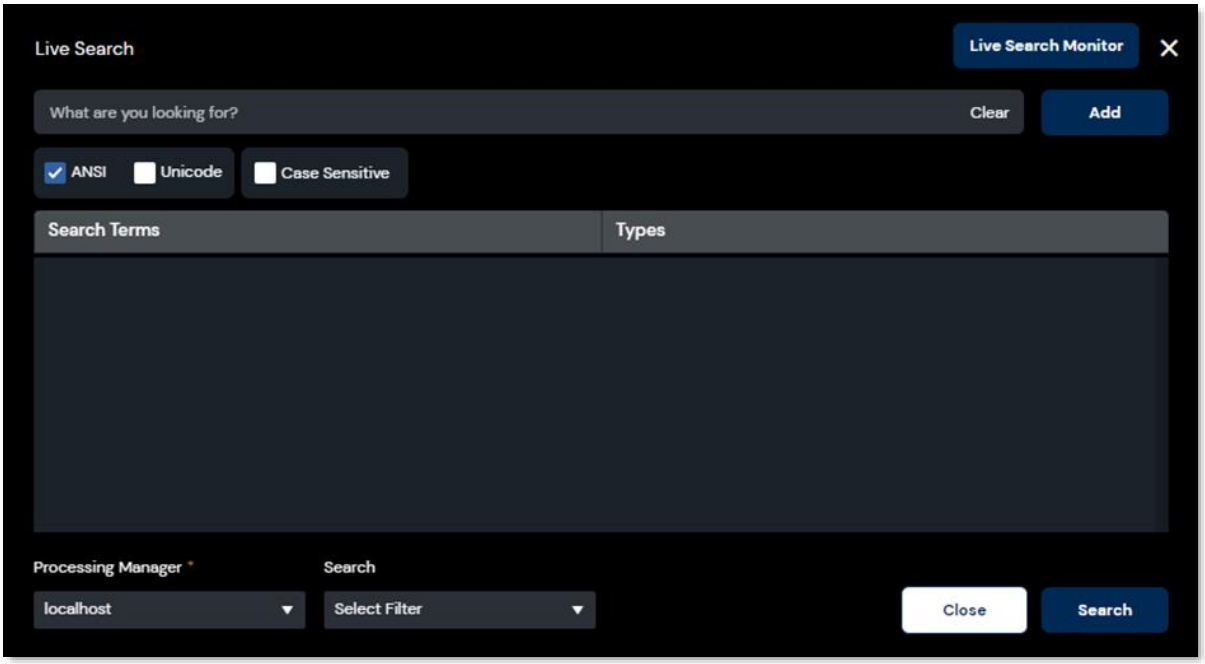
While performing search you can click the **Relationships** button and select any of the following options based on which the results should be displayed.

- **Duplicates** - To display the duplicate files.
- **Family** – To display the family files.
- **Near Duplicates** -To display the files that are almost similar to the original file.

© Exterro, Inc. All rights reserved

Live Search

FTK Central brings you 'Live Search', a feature that enables you to perform quick and effective search operations over case files via bit-by-bit comparison. A live search is effective because it can find patterns of non-alphanumeric characters, including those that are not generally indexed. This search is best suited for searching and filtering through unindexed case files. . (FTKC-24859)

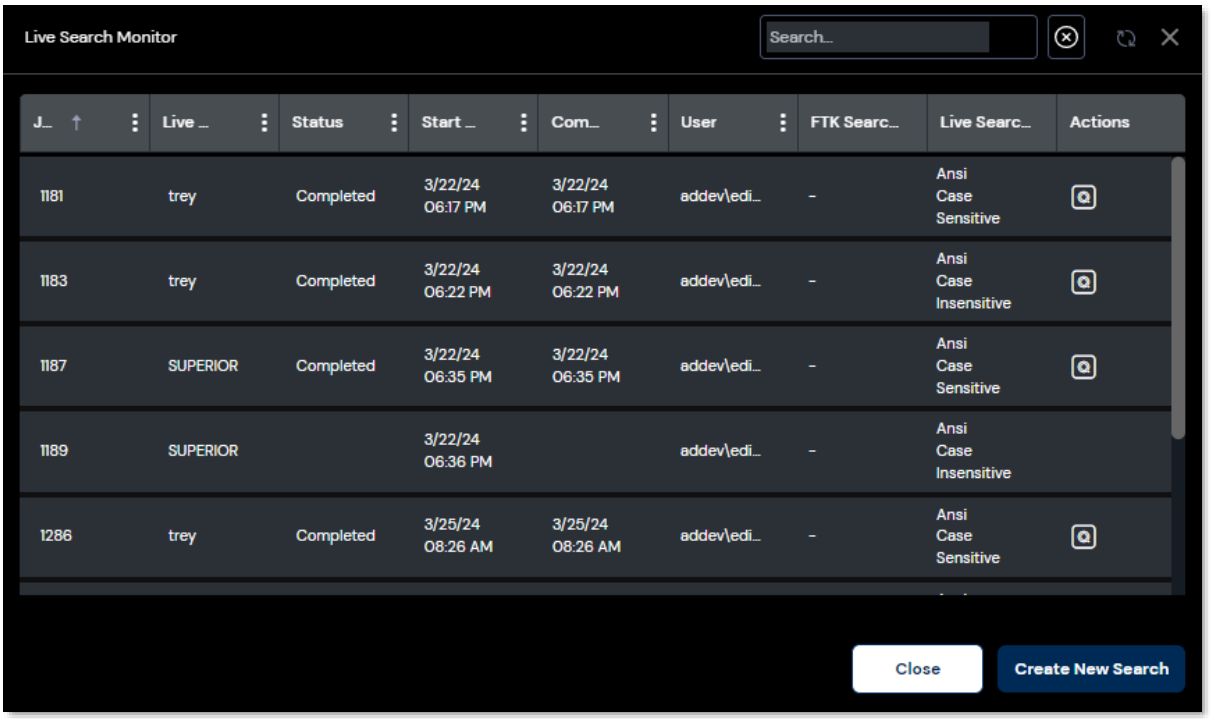


You can click on the **Live Search** button against the search bar to access the **Live Search** pop-up and provide the required list of keywords to perform the search operation.

This search feature enables you to retrieve results based on ANSI (American National Standards Institute), Unicode, and Case Sensitive terms present in the case files.

© Exterro, Inc. All rights reserved

Each Live Search performed in the Review page will be processed as a job. You can view the status of such jobs by clicking on the **Live Search Monitor** button from the **Live Search** pop-up.

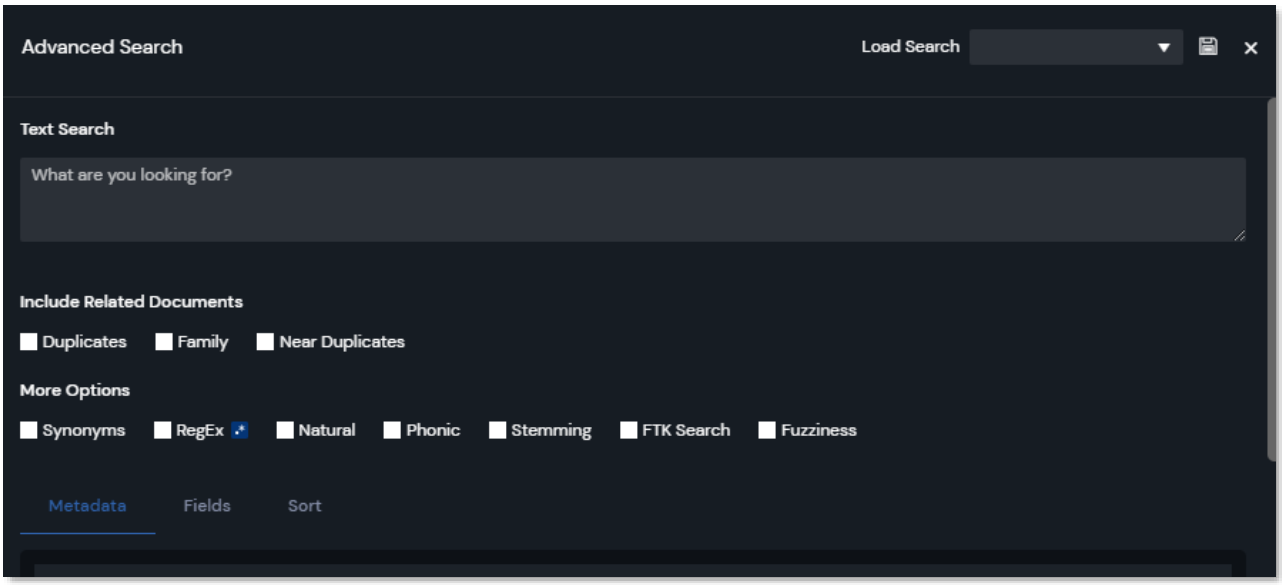


Once the jobs are processed, you can click on to view the corresponding search results in the Review page.

© Exterro, Inc. All rights reserved

Advanced Searching

FTK Central Advanced Search allows you to perform a detailed search and obtain relevant results using the multiple filters and search options available in this feature.



© Exterro, Inc. All rights reserved

To perform an advanced search:

1. In the Grid, click the **Advanced Search** button against the search tab.
   - The **Advanced Search** prompt is displayed.

- Configure the required filtering options based on the below descriptions.

Options	Descriptions
Include Related Documents	Allows users to search within duplicates, family or near duplicates.
Synonyms	To search and display all the files containing the keywords that have the same meaning as the provided search term. For example, searching for 'duplicate' will also find 'copy'.
Regex	To filter all the files based on the ReGex term entered.
Natural	Search term is run as it is displayed.
Phonic	To search and display files containing words that sounds like the specified keyword. For example, searching for 'Smith' will also find 'Smithe' and 'Smythe'.
Stemming	To search and display the files containing the inflected words of the specified keyword. For example, searching for 'dye' will also find 'dying'.
FTK Search	Utilizes DTSearch and does not search fielded values.
Fuzziness	To filter and display the files consisting of terms that are similar in spelling (or characters) to the specified search term. For example, searching 'serach', 'serch', 'sarch, will also find 'search'. You can set the Fuzziness level based on the below options: ▪ **Little Fuzzy** ▪ **Very Fuzzy**

© Exterro, Inc. All rights reserved

Options	Descriptions
	Fuzzy logic search; it is looking for similar documents but not exact equals, called homologous files. An example would be two word processor documents, with a paragraph added in the middle of one.

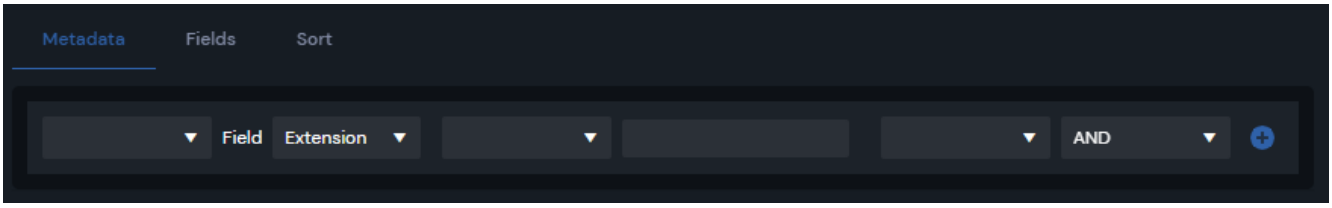
- Click **Search**.

Note: After performing a search, you can click on ✕ against the required search term to remove it or click on **Clear** Clear to remove all the search terms.

© Exterro, Inc. All rights reserved

To perform a Search using Metadata, Fields, and Sort:

Metadata:

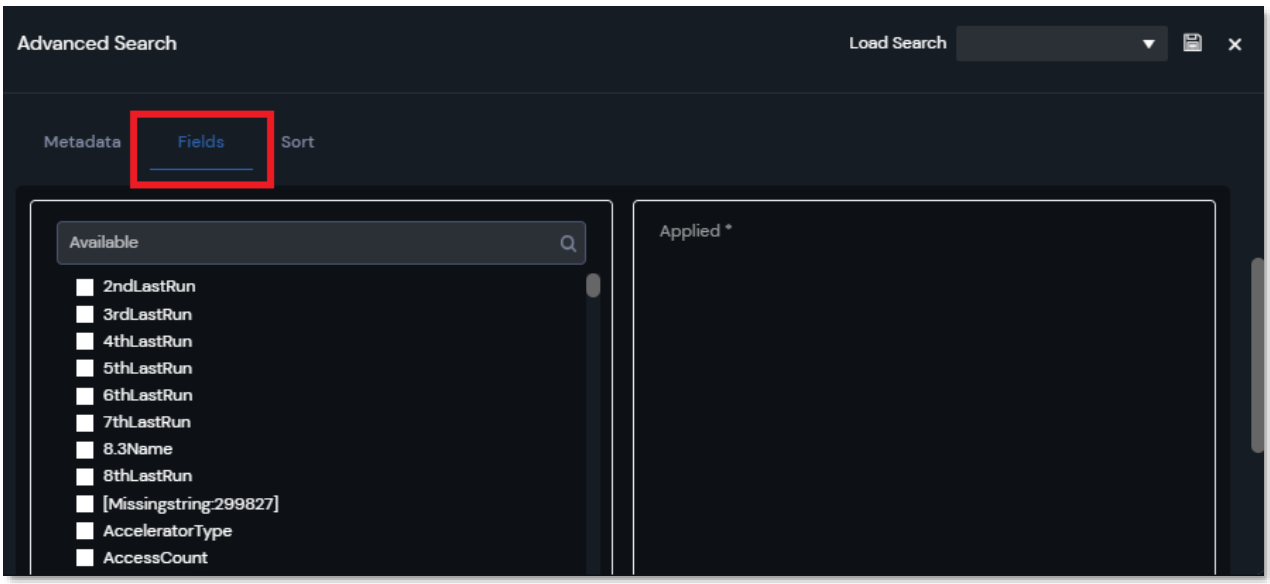


1. Select the opening parentheses (if required) from the first drop-down.
2. Select the **Field** name from the drop-down.
3. Select the field operator.
4. Enter the field value.
5. Select the closing parentheses (if required).
6. Select an Boolean Operator if required.
7. Click the on the **Apply** button to add an additional field search if required.

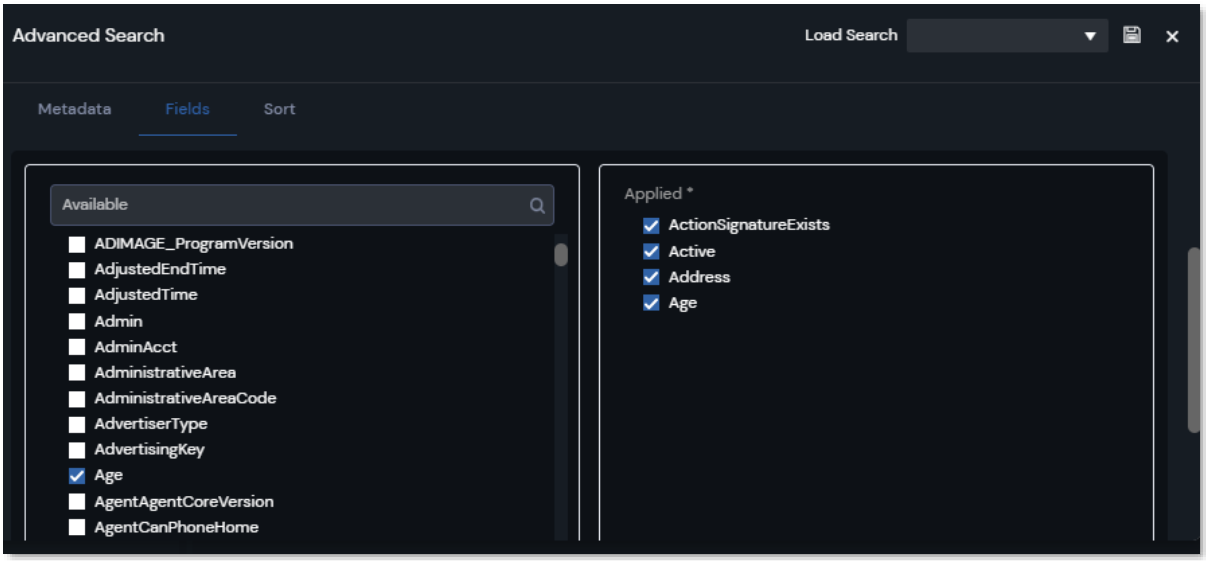
© Exterro, Inc. All rights reserved

Field:

8. Select the **Field** tab.



9. Select the columns to be filtered from the right-side section.
   - The selected columns will be displayed in the **Applied** (left-side) section.

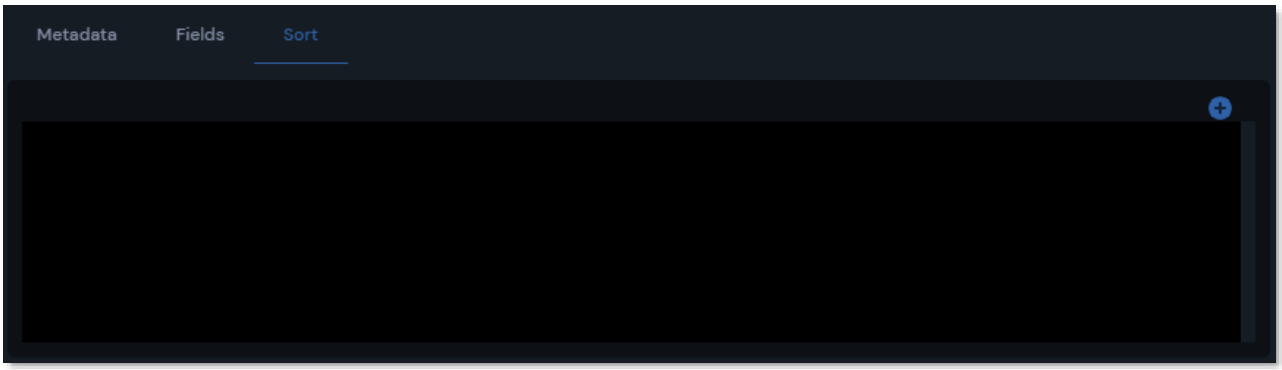


© Exterro, Inc. All rights reserved

10. Drag and drop the required columns in the **Applied** section to reorder it based on which the columns will be displayed after the search is performed.

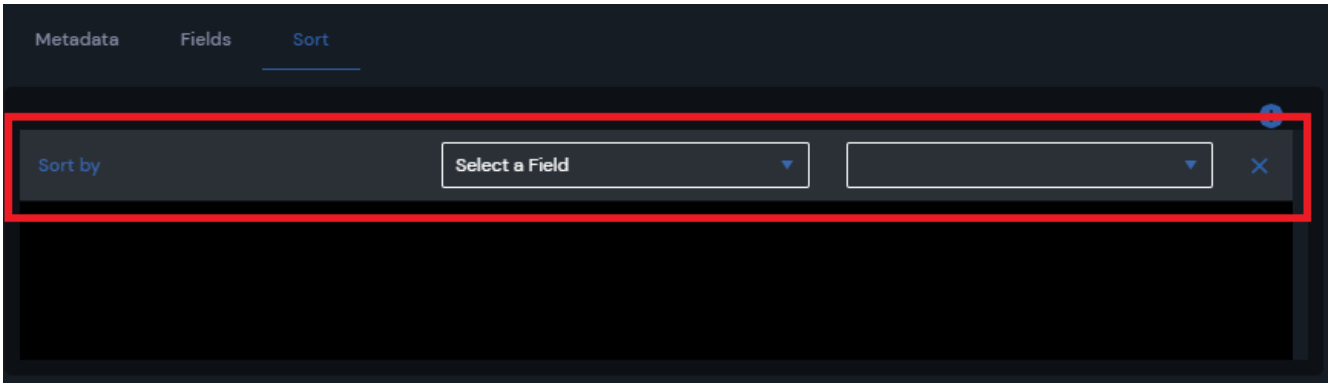
Sort:

11. Click on the **Sort** tab.



© Exterro, Inc. All rights reserved

12. Click the on the **Apply** button to add a column sort preference if required.
    - The **Sort by** field is displayed.



13. Select the field name and the sort preference in the field against it
14. Click **Search**.

© Exterro, Inc. All rights reserved

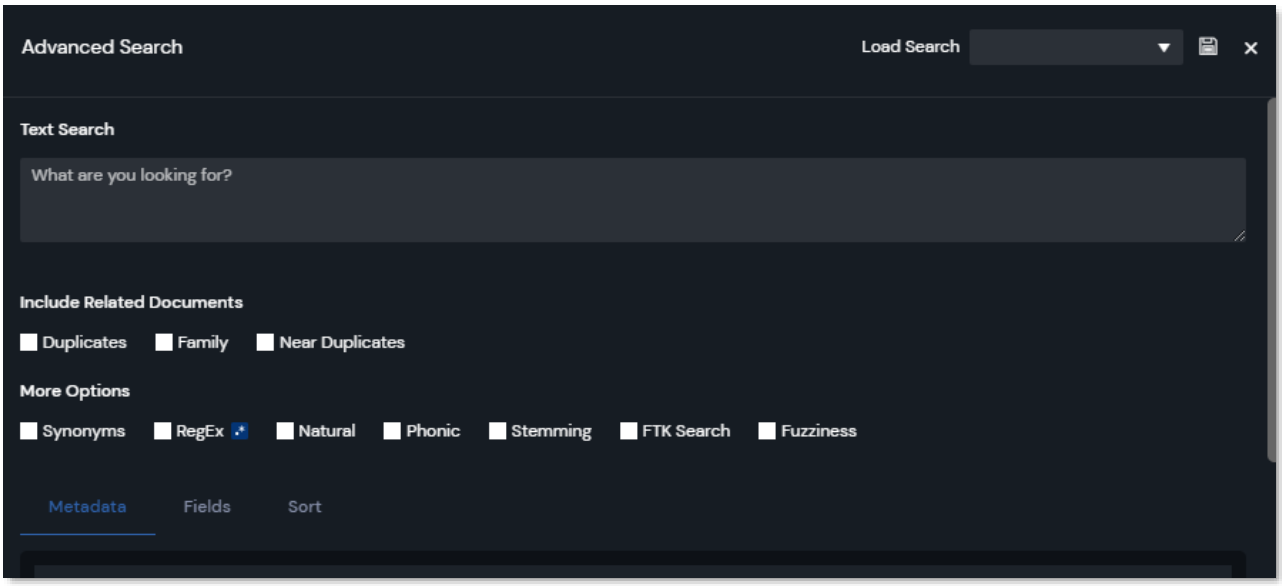
To expand search terms:

You can use expand search terms to add related words and phrases to a search. For example, when you are searching for "text", the function will display:

Search Term Categories:

Default	Include Related	Include Specific	Include General
School text	School text	Column	Book
Schoolbook	Schoolbook	Cookie	Matter
Text edition	Text edition	Copy	Passage
Textual matter	Textual matter	Crammer	School text
Textbook	Textbook	Draft	Schoolbook

1. In the Grid, click the **Advanced Search** button against the search tab.
   - The **Advanced Search** prompt is displayed.

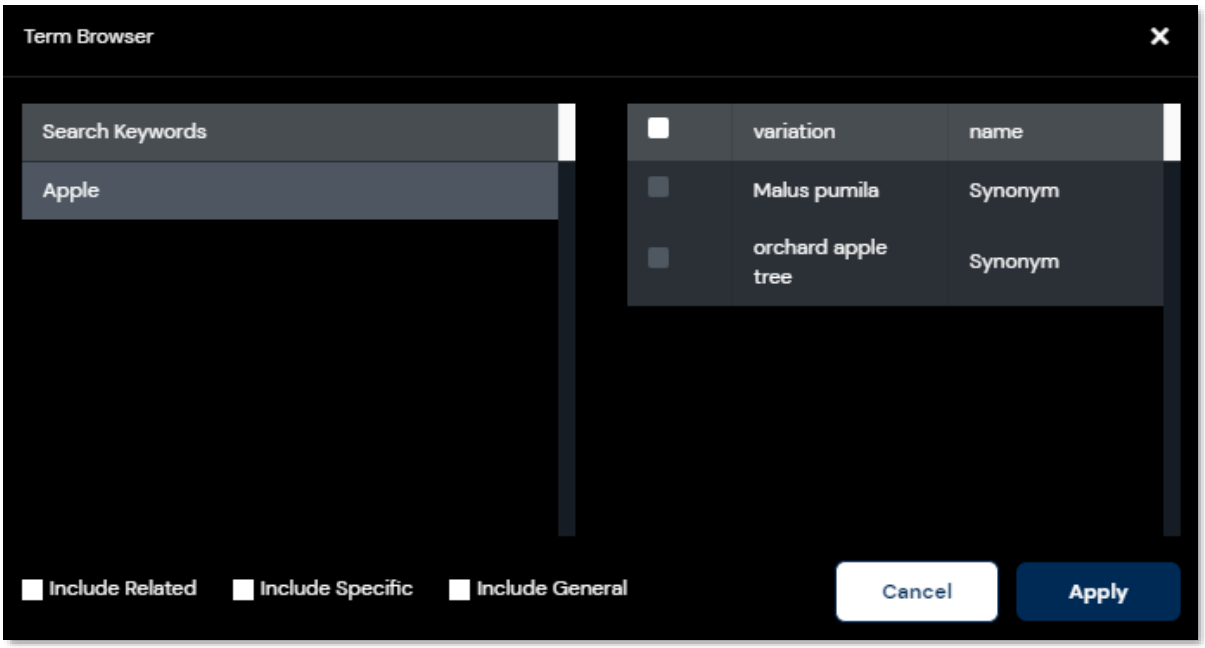


© Exterro, Inc. All rights reserved

2. Provide the **Text Search** term.
3. Click **Expand Search Terms**.

Warning: The **Expand Search Terms** button will be displayed only upon providing the terms for **Text Search** field.

- The **Term Browser** will be displayed.



4. Select the required search term.
5. Check the required variation terms.
6. Enable the required search term category:
   - **Include Related**
   - **Include Specific**
   - **Include General**
7. Click **Apply**.

© Exterro, Inc. All rights reserved

To save a search:

You can save any advanced search that you design in the Advanced Search Builder. All saved searches are stored in the Advanced Search Builder. You can use saved searches to run past searches again.

1. In the Grid, click the **Advanced Search** button against the search tab.
   - The **Advanced Search** prompt is displayed.

2. Configure the required search terms and filters.

3. Click the **Save Search** button.
   - The **Save Search** section is displayed.

4. Provide the **Search Name**.
5. Configure the following fields to set the accessibility and visibility of the search based on your preference:
   - **User Permission:**
     - **Private** – To be displayed and accessed only for the user who created it.
     - **Public** – To be displayed and accessed by all the users.
   - **Case Permission:**
     - **Case** - The saved search will be accessible only within the selected case.
     - **Global** - The saved search will be accessible for all cases.

Note: The **View Save Global Search** permission is required to use the **Case Permission** option.

6. Click to save the search term and perform the search operation.
7. Click to save the search term.

© Exterro, Inc. All rights reserved

© Exterro, Inc. All rights reserved

To load a search:

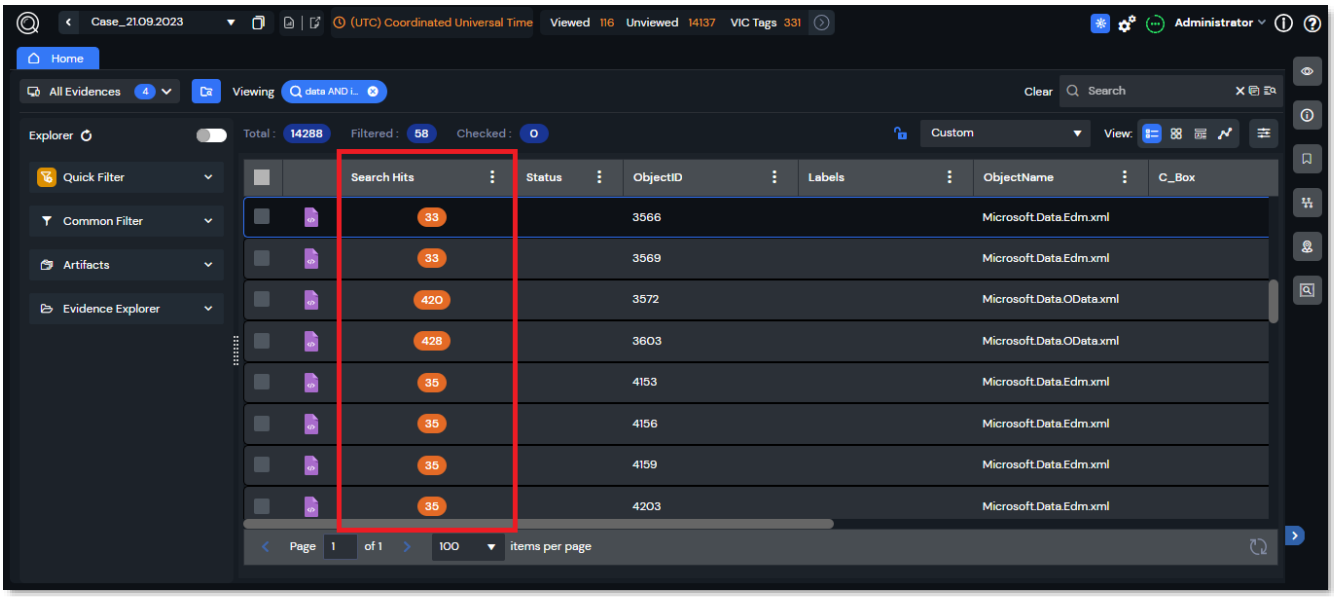
1. In the Grid, click the **Advanced Search** button against the search tab.
   - The **Advanced Search** prompt is displayed.

2. Select the required saved search from the **Load Search** drop-down field.
3. Click **Search**.

© Exterro, Inc. All rights reserved

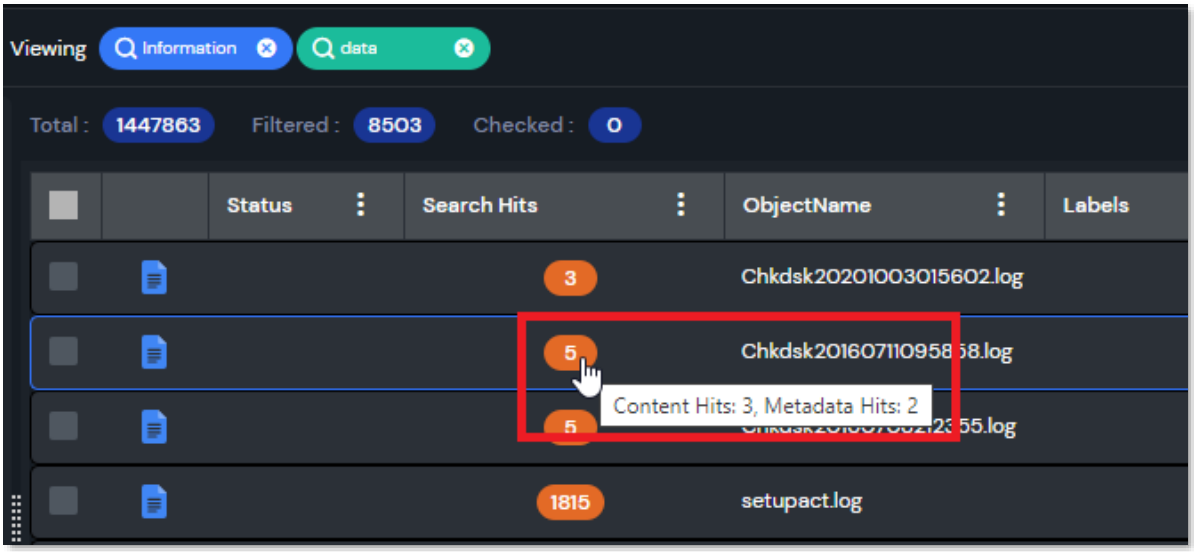
Search Hits Column

Upon performing the search operation, this column will be displayed to provide you with the search hit count in each file i.e., the number of occurrences of the search terms in each file.



Hovering over the count in the column would display the following segregated details:

- **Content Hits** – The number of hits in the file's content.
- **Metadata Hits** – The number of hits in the file's metadata.



© Exterro, Inc. All rights reserved

Search Term Excerpt Report

The Search Term Excerpt Report is one of the most vital features required for a reviewer to easily seek out the important information and files related to a case.

Upon performing a search, this report will be generated to display the search results along with a brief snippet, phrase, or summary of content related to the keyword. With this, you can have a quick overview of the result's content, helping you to decide whether the result is likely to contain the information you're searching for.

Example:

Scenario: *You're investigating a case involving unauthorized financial transactions and need to find communications related to transaction approvals.*

Search Keyword: *"transaction approval"*

Original Email Content: *"Following our discussion, Jane Doe has authorized the transaction approval for the new vendor payment system. Please proceed with the necessary paperwork to finalize this process."*

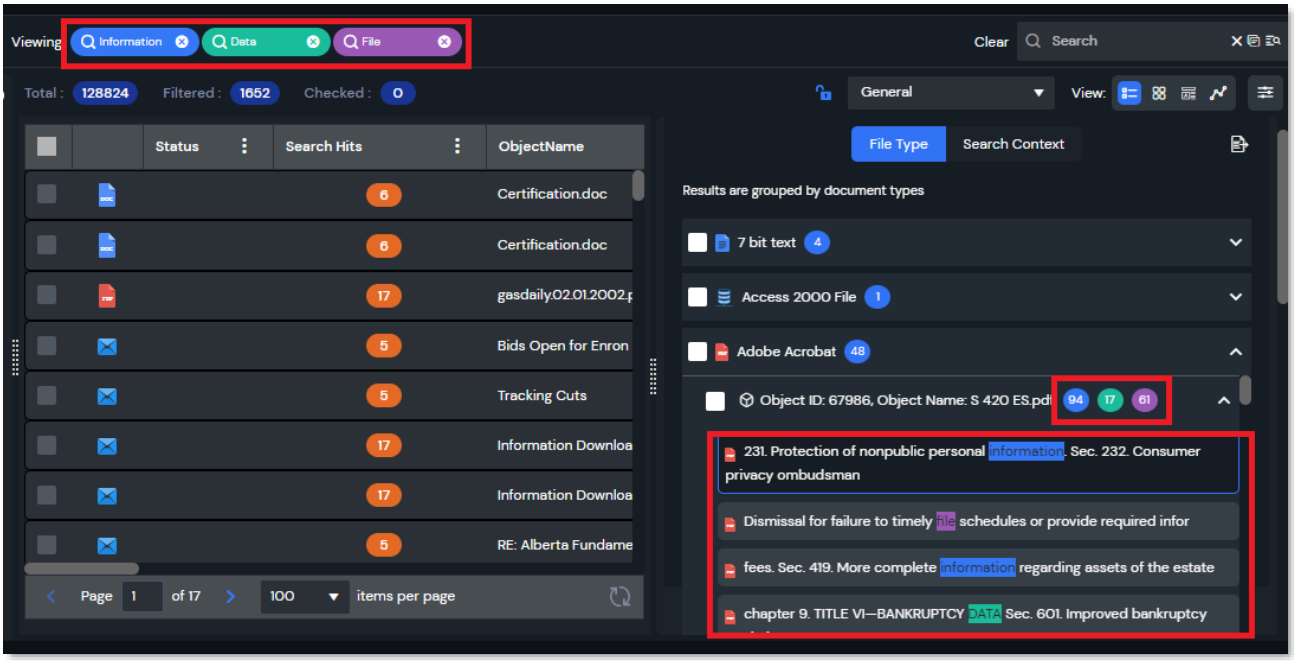
Search Result Excerpt: *"...Jane Doe has authorized the* ***transaction approval*** *for the new vendor payment system..."*

© Exterro, Inc. All rights reserved

You can view the search excerpts report by clicking on the **Search Term Excerpt Report** icon from the right pane after the search operation is performed.

Warning: The **Search Term Excerpt Report** icon will be displayed only after the search operation is completed.

You can use multiple keywords for performing search operations, and each keyword and its count value will be highlighted in a distinct color in the report. This will be automatically performed every time you add a new search keyword.



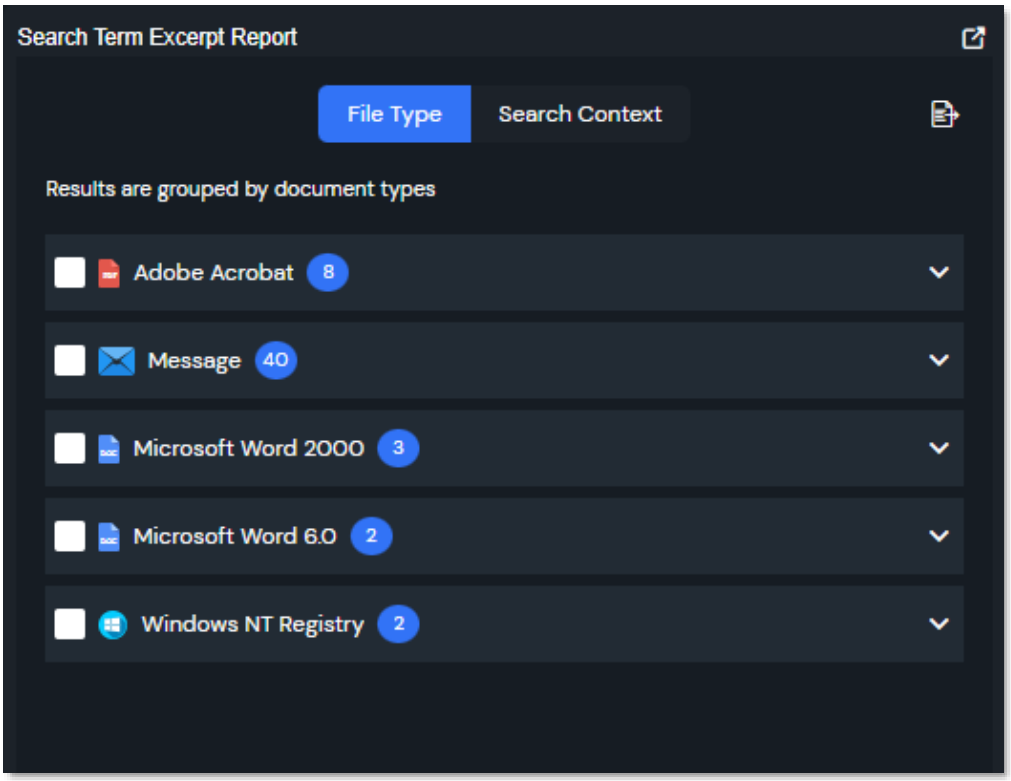
You also can select the required files from this report and perform the following operations:

- Bulk Bookmarking
- Bulk Coding
- Bulk Labeling
- Flag as Privileged
- Flag as Ignorable

© Exterro, Inc. All rights reserved

File Type Report

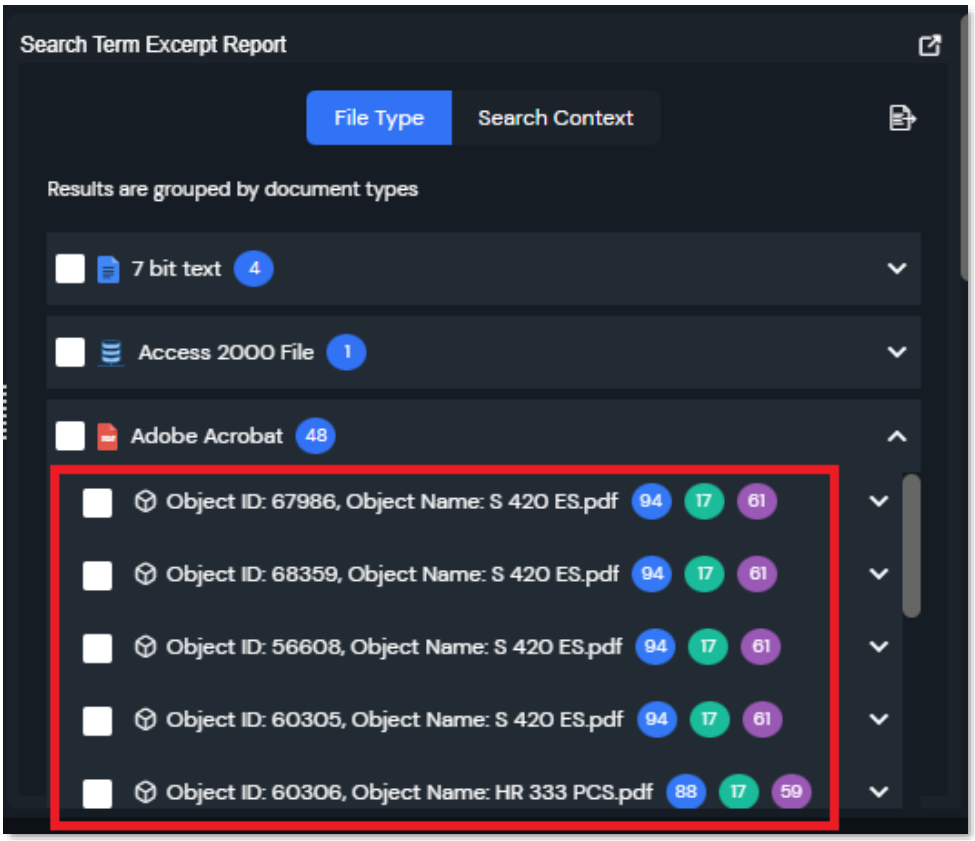
The **File Type** section in the **Search Term Excerpt Report** lists out all the search result files grouped within corresponding file types.



© Exterro, Inc. All rights reserved

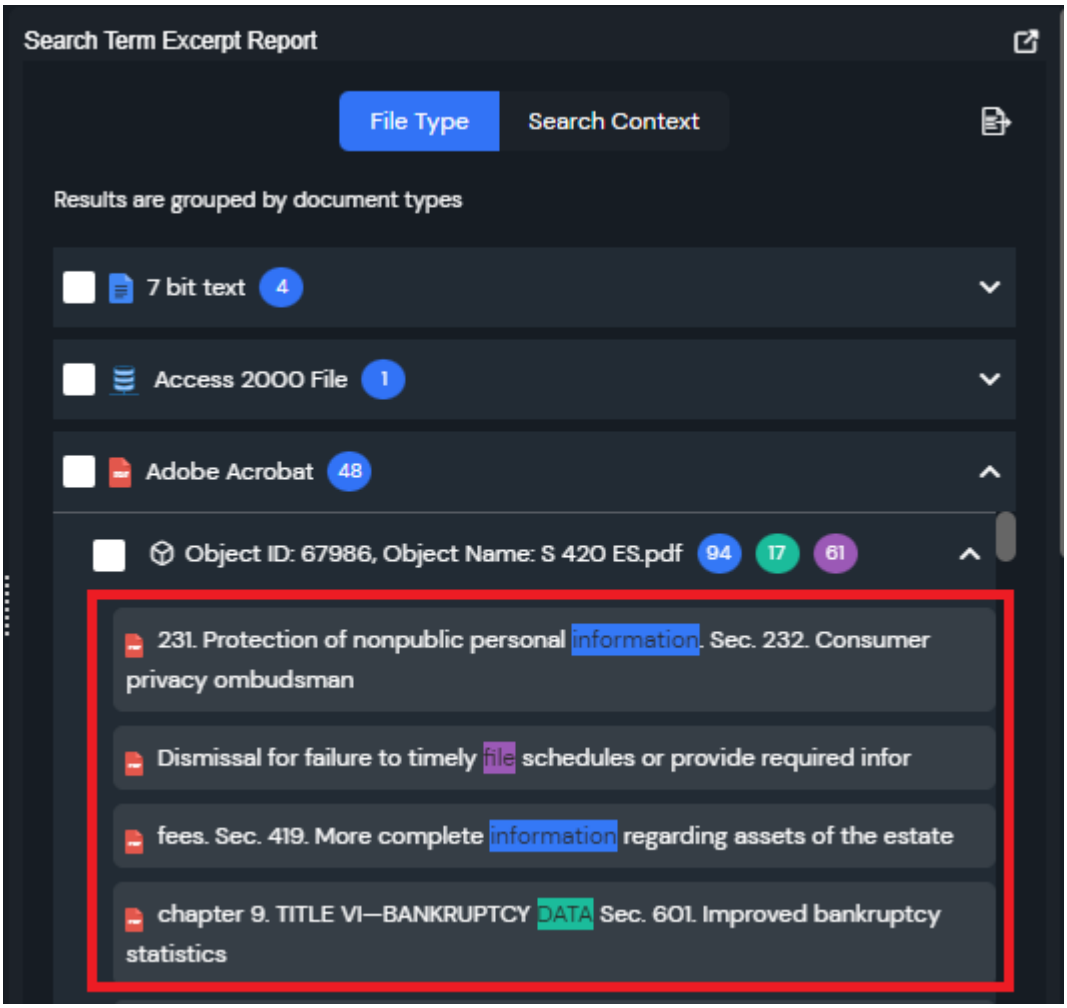
To review the files from File Type section:

1. From the File Type section of the report, expand the required file types to view all the corresponding files.



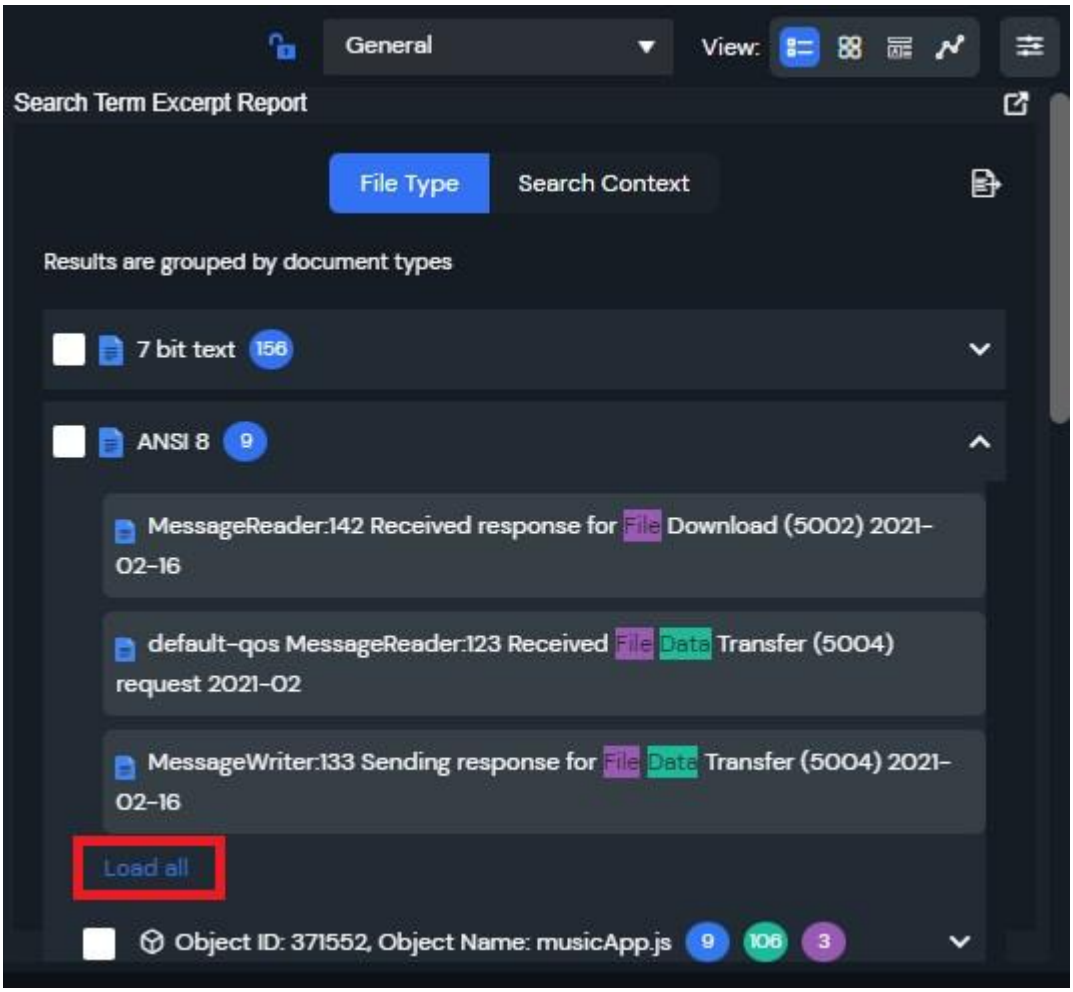
© Exterro, Inc. All rights reserved

2. Expand each file to view the highlighted search results within the phrase to view the contextual information.



© Exterro, Inc. All rights reserved

Note: Upon expanding a file type group consisting of more than 100 files, only the first 100 files in the list will be displayed. You can click on the **Load all** button to load and view the remaining files.



© Exterro, Inc. All rights reserved

3. Click on the required files to view the content in the Viewer on the corresponding page where the excerpt is available.

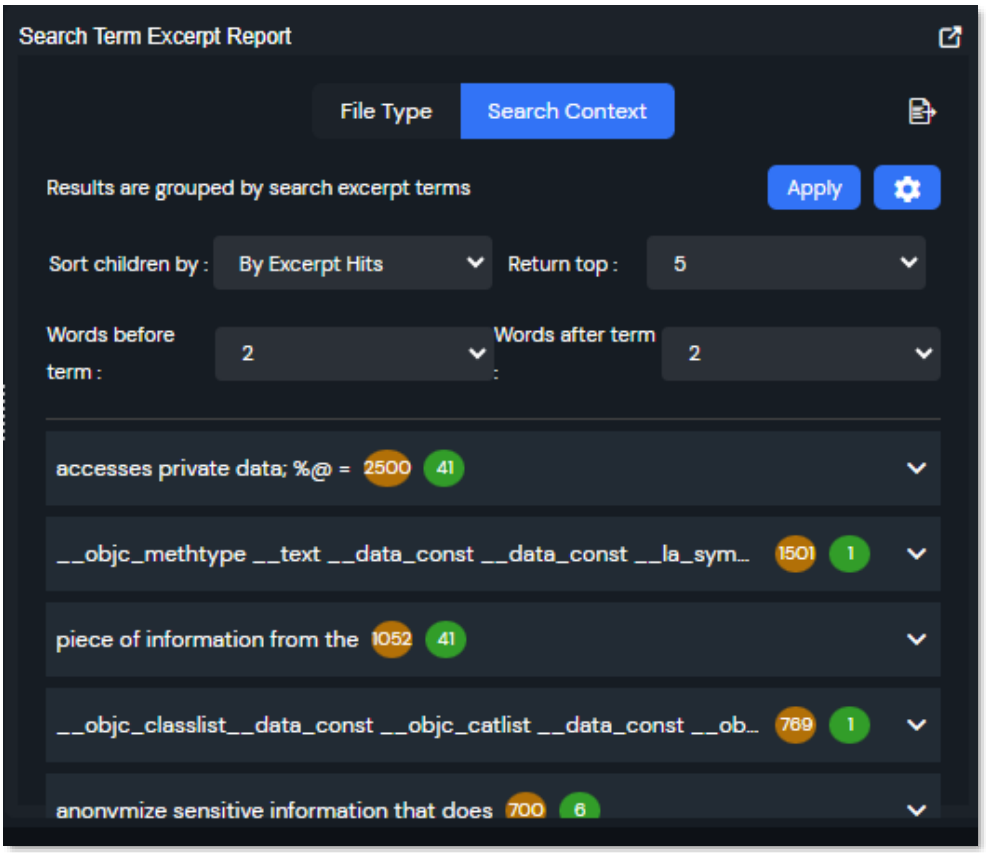
Notes:

- The Chat Conversation and Chat Message files will be opened in the Native viewer whereas all other file types will be opened in the Text Viewer.
- The files indicated with the icon mean the keywords are present in the metadata information of the file. So, when you click on a file with the icon, the Info Viewer will be opened instead of Native viewer.
- You can export the report by clicking on the **Export Search Term Report** button.

© Exterro, Inc. All rights reserved

Search Context Report

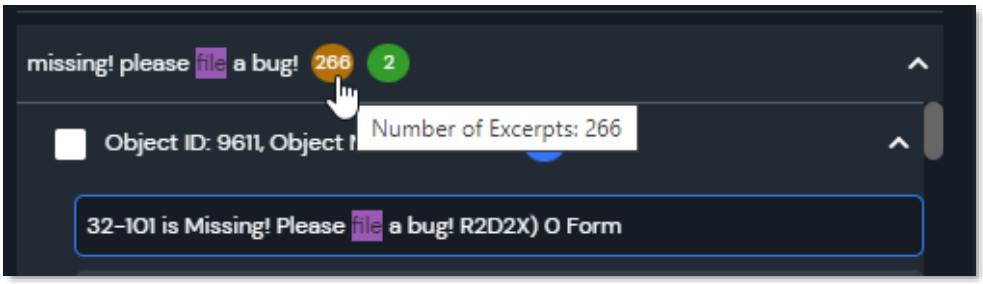
The **Search Context** section in **Search Term Excerpt Report** groups the files based on the most reiterated excerpts (phrases or snippets) consisting of the search term.



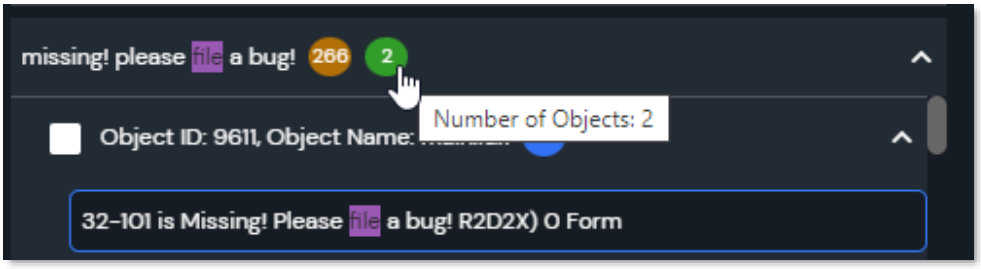
© Exterro, Inc. All rights reserved

The following count will be displayed against the excerpts listed in the section:

- **Number of Excerpts** – This count indicates the number of occurrences of the corresponding excerpt across the search result files.



- **Number of Objects** – This count indicates the number of files within which the excerpts are available.

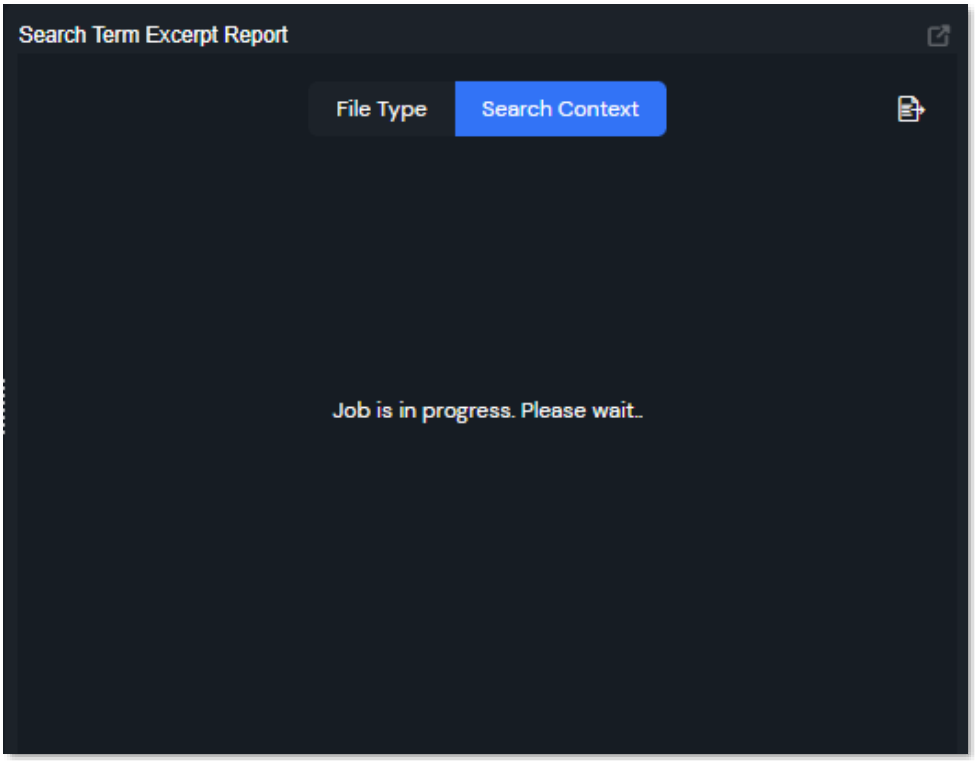


© Exterro, Inc. All rights reserved

Warning: A job will be triggered for the **Search Context** section of the report during the following scenarios:

- when you navigate to the section for the first time after the search is performed.
- After applying filters in the section.

The information will be loaded and displayed after job completion.



© Exterro, Inc. All rights reserved

To filter the files in the Search Context section:

1. From the **Search Context** section, configure the following options based on your requirements:

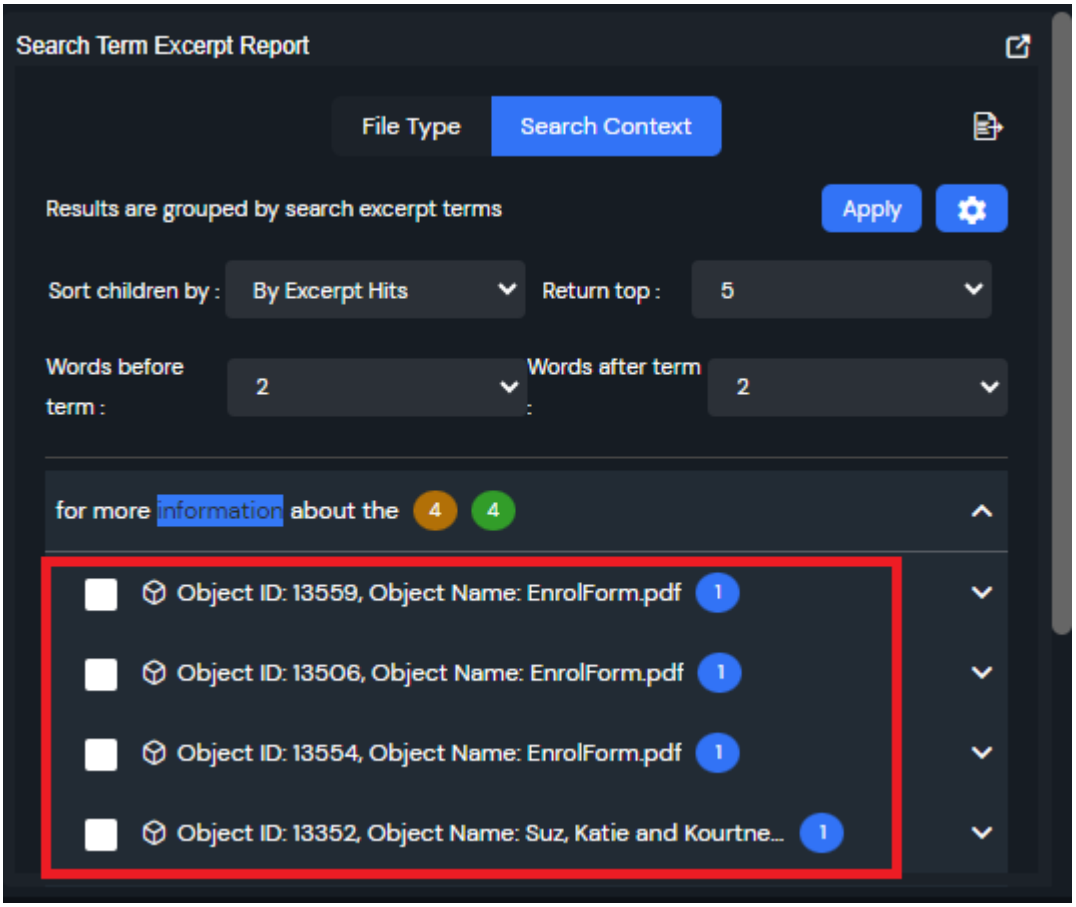
- **Sort children by** – To sort the excerpts list based on any one of the following options:
  - **By Excerpt Hits:** To sort the excerpts from the most to least number of hits in the search results.
  - **By Object ID:** To sort the excerpts based on the file's ID (object ID)
  - **By Document Type:** To sort the excerpts based on the document types listed in the Explorer pane.
- **Return top** – Select the number of excerpts that should be displayed in the section.
- **Words before term** – The limit of words that should precede the provided keyword.
- **Words after term** – The limit of words that should follow up with the provided keyword.

2. Click on Apply.

© Exterro, Inc. All rights reserved

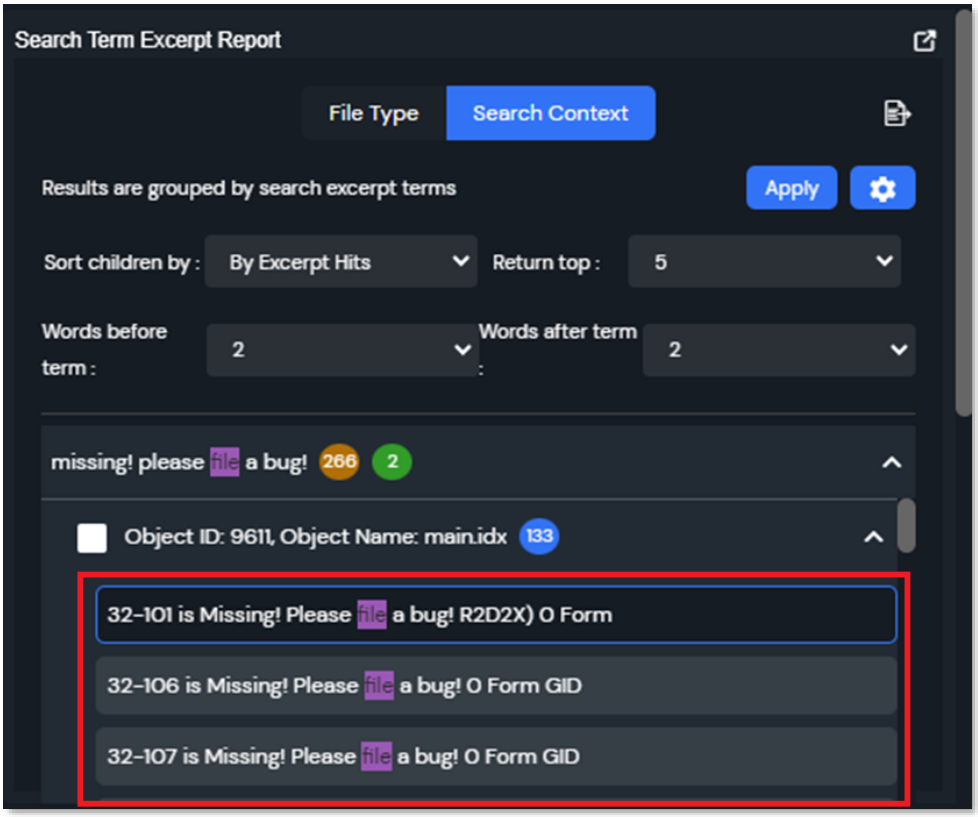
To view the files from the Search Context section:

1. Expand the excerpt listed in the section to view the list of files.



© Exterro, Inc. All rights reserved

2. Expand the required file to view the list of keyword excerpts in it.



3. Click on the required file to view the information in the Viewer on the corresponding page where the excerpt is available.

Note: The Chat Conversations and Chat Messages file types will be opened in the Native viewer whereas all other file types will be opened in the Text Viewer.

© Exterro, Inc. All rights reserved

Working with Labels

Labels let you group files in the way that makes the most sense to you. Initially, there are no default labels. All are customized. Labels you create are saved locally and you have complete control over them within your case.

Creating Labels

To create a label:

1. In the Grid, click the **Show Tags Panel** button.
    - The **Tag Configuration** pop-up is displayed.
2. Click the **Settings** button.
3. Click **+ Create Labels**.
4. Select the **Labels** tab.
5. Click **+ Add Label**.

Tip: Click the on a label folder to create a label specifically in the folder. This button will appear when you hover over a label folder.

6. Enter a Label **Name**.
7. Click the **Save** button.

© Exterro, Inc. All rights reserved

Editing Labels

To edit a label:

1. In the Grid, click the **Show Tags Panel** button.
    - The **Tag Configuration** pop-up is displayed.
2. Click **+Create Labels**.
3. Select **Labels** tab.
4. Click on the label name and edit it.
5. Click **Update**.

Deleting Labels

Warning: Deleting labels will remove them from the document(s). This cannot be undone.

To delete a label:

1. In the Grid, click the **Show Tags Panel** button.
    - The **Tag Configuration** pop-up is displayed.
2. Click **+Create Labels**.
3. Select **Labels** tab.
4. Click the **Delete** button against the required label.

© Exterro, Inc. All rights reserved

Applying Labels

To apply a label:

1. In the Grid, select the records requiring labeling.
2. Check or highlight these records.
3. Click the **Show Tags Panel** button.
4. Select the **Labels** tab.
5. Check the required label.

Tip: Checking a label folder will apply all child labels as well as any child labels located in sub folders.

Any changes made will now be applied.

Note: To remove a label, uncheck the selected label. To remove all child labels, uncheck the label group.

© Exterro, Inc. All rights reserved

Creating Label Groups

To create a label group:

1. In the Grid, click the **Show Tags Panel** button.
    - The **Tag Configuration** pop-up is displayed.
2. Click **+ Create Labels**.
3. Select **Labels** tab.
4. Click **Add Folder**. This will create a root folder.

Tip: To create a sub group, click the icon in line with the parent group.

5. Click **Save**.

Editing Label Groups

To edit a label group:

1. In the Grid, click the **Show Tags Panel** button.
    - The **Tag Configuration** pop-up is displayed.
2. Click **+ Create Labels**.
3. Select **Labels** tab.
4. Click on the folder name and edit it.
5. Click **Update**.

Any changes made will now be applied.

© Exterro, Inc. All rights reserved

Filtering for Labels

See Filtering section.

To filter a label:

1. In the Grid, click on **Common Filter** from the **Explorer** pane.
2. Expand the **Labels** folder.
3. Select a label or label group(s).

The Grid will update to show only these labels.

Working with Bookmarks

A Bookmark is a group of files that you want to reference in your case. These are user-created and the list is stored for later reference, and for use in the report output. You can create as many bookmarks as needed in a case. Bookmarks can be nested within other bookmarks for convenience and categorization purposes.

Bookmarks help organize the case evidence by grouping related or similar files. For example, you can create a bookmark of graphics that contain similar or related graphic images. The Tags tab lists all bookmarks that have been created in the current case. Bookmarks only apply to the case they are created in.

© Exterro, Inc. All rights reserved

Creating Bookmarks

To create a bookmark:

1. In the Grid, click the **Show Tags Panel** button.
    - The **Tag Configuration** pop-up is displayed.
2. Select the **Bookmarks** tab.
3. Click **+ Create Bookmarks**.
4. Enter the bookmark **Name** and **Comment**.
5. Click **Save** .

The bookmark will now be created.

© Exterro, Inc. All rights reserved

Editing Bookmarks

To edit a bookmark:

1. In the Grid, click the **Show Tags Panel** button.
    - The **Tag Configuration** pop-up is displayed.
2. Click the **Bookmarks** tab.
3. Click **+ Create Bookmarks**.
4. Click on the required bookmark and make changes to the Name and Comment.
5. Click **Update**.

Any changes made will now be applied.

Deleting Bookmarks

To delete a bookmark:

1. In the Grid, click the **Show Tags Panel** button.
    - The **Tag Configuration** pop-up is displayed.
2. Click the **Bookmarks** tab.
3. Click **+ Create Bookmarks**.
4. Click the **Delete** button against the bookmark to be deleted.
5. Click **Yes** in the confirmation pop-up.

© Exterro, Inc. All rights reserved

Applying Bookmarks

To apply bookmark:

1. In the Grid, select the records requiring bookmarking.
2. Click the **Show Tags Panel** button.
3. Select **Bookmarks**.
4. Check the required bookmark.
5. Any changes made will now be applied.

Note: To remove a bookmark, uncheck the selected bookmark.

Bulk Bookmarking

Refer Performing Actions from the Grid section.

Filtering for Bookmarks

Refer Filtering section.

To filter a bookmark:

1. In the Grid, click on **Common Filter** from the **Explorer** pane.
2. Navigate to **Bookmarks**.
3. Expand the bookmark folder.
4. Select a bookmark(s).

The Grid will update to show only these bookmarks.

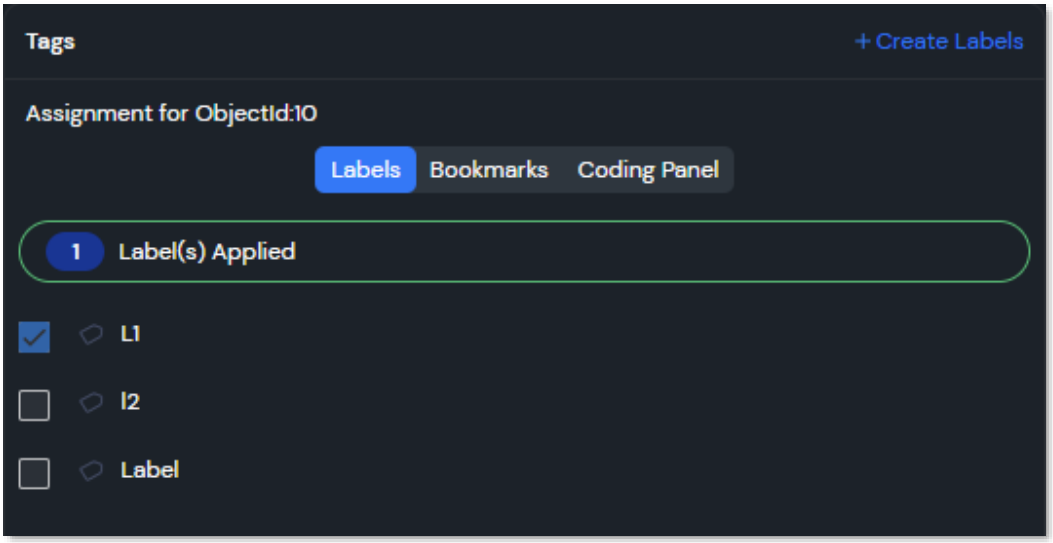
© Exterro, Inc. All rights reserved

Sharing Tags

You can share the labels, issues, and custom fields created for other users in order to be utilized during the review process. Using the **Apply Users & Groups** function allows you to share these tags with users to edit and use within the case and coding panel.

To share tags:

1. In the Grid, click on the **Tags** button.
    - The **Tags** panel is displayed.



2. Click **+ Create Labels**.
3. Select **Labels, Issues,** or **Custom Fields** section.
4. Select the required label, issues, or custom fields.
5. Click **+ Apply Users & Groups**.
6. In the **Users & User Groups** dialog, select the required users or user groups.
7. Click **Save**.

The user or user groups can now access the selected labels, issues, or custom fields in the case and within the coding panel.

© Exterro, Inc. All rights reserved

Creating Reports

You can create a case report about the relevant information of a case any time during or after the investigation and analysis of a case. Reports can be generated in different formats, including HTML and PDF. The PDF report is designed specifically for printing hard copies with preserved formatting and correct organization. The HTML report is better for electronic distribution.

Note: Click the **Reports** button to access reporting functionality.

© Exterro, Inc. All rights reserved

Report Types

- **Detail Report**: Standard FTK Report
- **Processing Reports**:
  - Data Volume Report – Category Overview, Evidence List, Encrypted File List, Case Breakout and Processing Exceptions.
  - File De-Duplication Report – De-Duplication Information and File Duplicates.
  - Email De-Duplication Report – De-Duplication Information and Email Duplicates.
  - Processing Error Report: General Processing Errors.
- **Event Reports**: Event Audit Log – User events-based report.
- **Search Reports**:
  - Search Term Report – Search terms associated with a case.
  - Detailed Search Report: Active search query report. Users must have an active keyword search before this option is available.
- **Additional Reports:**
  - Email Recipient Count Reports – A report consisting of the User Name, Email Domain, Email Address, and Item Count of all the custodians in the case.

Warning: During mail composition, when a sender manually types in the email address of the recipient instead of selecting it from the suggestion drop-down, the name of the recipient will not be displayed for that email.

Hence, the recipient's name of such email files will not be displayed in the **Email Recipient Count Report** generated from the FTK Central application.

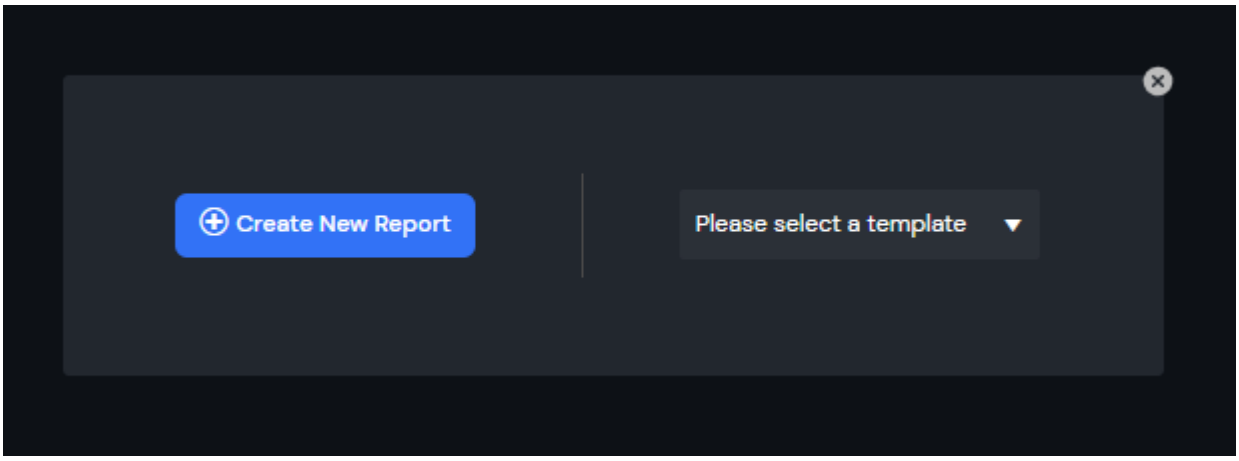
© Exterro, Inc. All rights reserved

Creating a Detail Report

You can create a detail report about the relevant information of a case any time during or after the investigation and analysis of a case. Reports can be generated in different formats, including DOCX and PDF. The PDF report is designed specifically for printing hard copies with preserved formatting and correct organization.

To create a Detail Report:

1. From the home page, click **Case List**.
2. Select the required case.
3. Click **Enter Review**.
4. Click on the **Reports** button.
5. Click **Detail Report**.

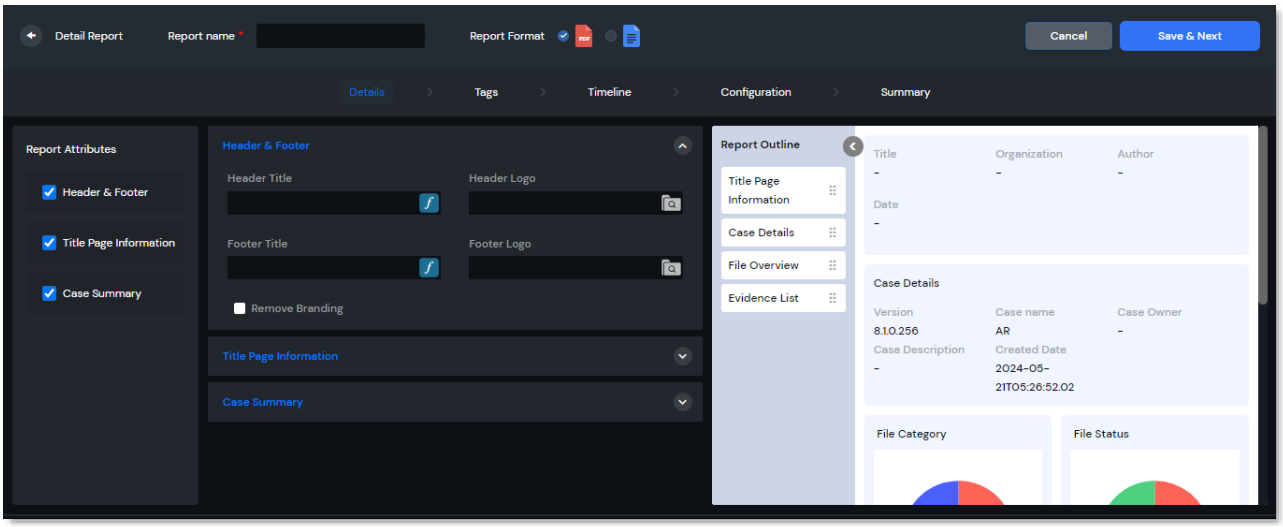


6. Click on **Create New Report**.

Note: You can also choose to select a template from the right side to create a report based on the configurations made for a previously created report.

© Exterro, Inc. All rights reserved

- The Detail Reports creation page is displayed.



7. Enter a **Report Name**.
8. Select a **Report Format**.

From this page, you can configure the report details (left pane) while simultaneously previewing (right pane) the impacts made to the report. This process is further explained in the following sections:

- Report Configurations
- Report Preview

© Exterro, Inc. All rights reserved

Report Configuration

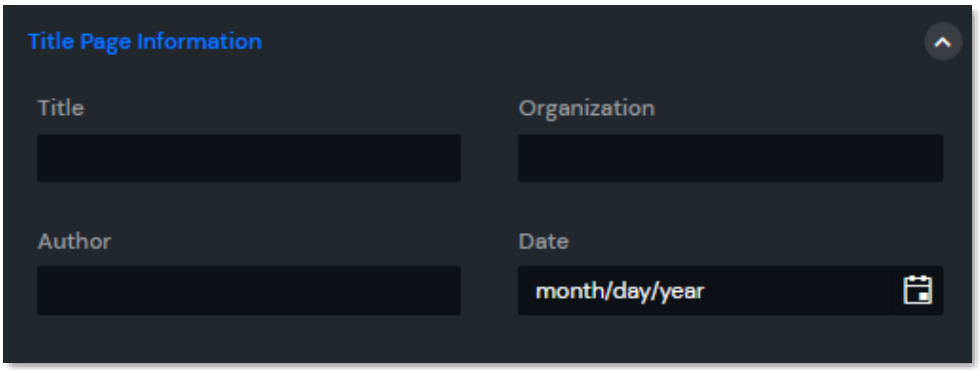
You can navigate to and configure the required details for the report from the following sections:

Details:

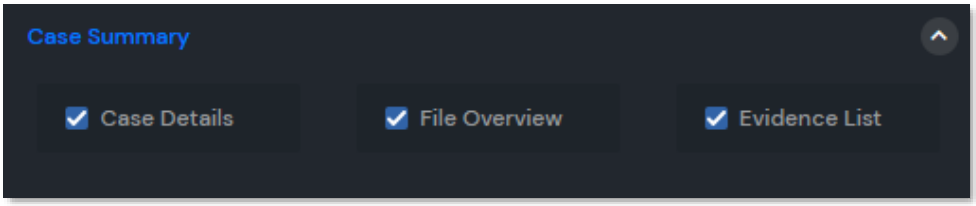
1. From the **Details** section, select any of the following **Report Attributes** that should added to the report:
   - Header and Footer
   - Title Page Information
   - Case Summary
2. Configure the following details for **Header & Footer** section:
   - **Header Title** – Enter the title that should be displayed in the header of the report. You can click on the **Font Styler** icon to configure the style, size, and color of the header font.
   - **Header Logo** – Click on the browse icon to browse and select the image file that should be used as a logo in the header of the report.
   - **Footer Title** – Enter the title that should be displayed in the footer of the report. You can click on the **Font Styler** icon to configure the style, size, and color of the footer font.
   - **Footer Logo** – Click on the browse icon to browse and select the image file that should be used as a logo in the footer of the report.
   - **Remove Branding** – Enable this option if you want to remove the 'Powered by exterro' branding from the report.

© Exterro, Inc. All rights reserved

3. Configure the following details for **Title Page Information** section:
   - **Title** – Enter the title of the report.
   - **Organization** – Enter the organization associated with the report.
   - **Author** – Enter the author of the report.
   - **Date** – Select the date that should be displayed in the report.



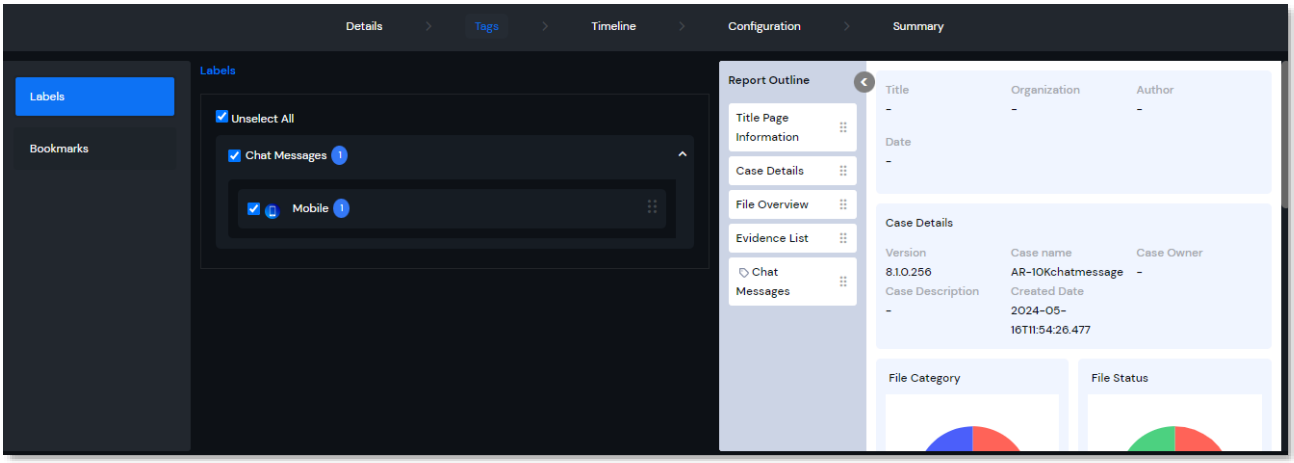
4. Select any of the following information from the **Case Summary** section that should be displayed in the report:
   - **Case Details** – To display the case related information (case name, case owner, created date, etc.) in the report.
   - **File Overview** – To display the 'File Category' and 'File Status' charts consisting of the file types information.
   - **Evidence List** – To display the information related to the evidence of the case.



5. Click **Save & Next**.

© Exterro, Inc. All rights reserved

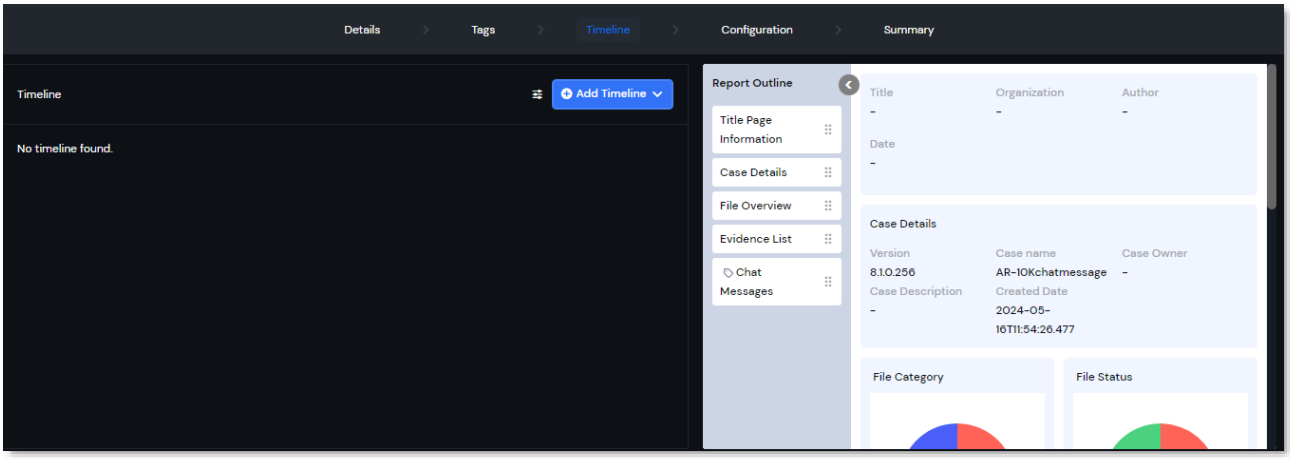
Tags



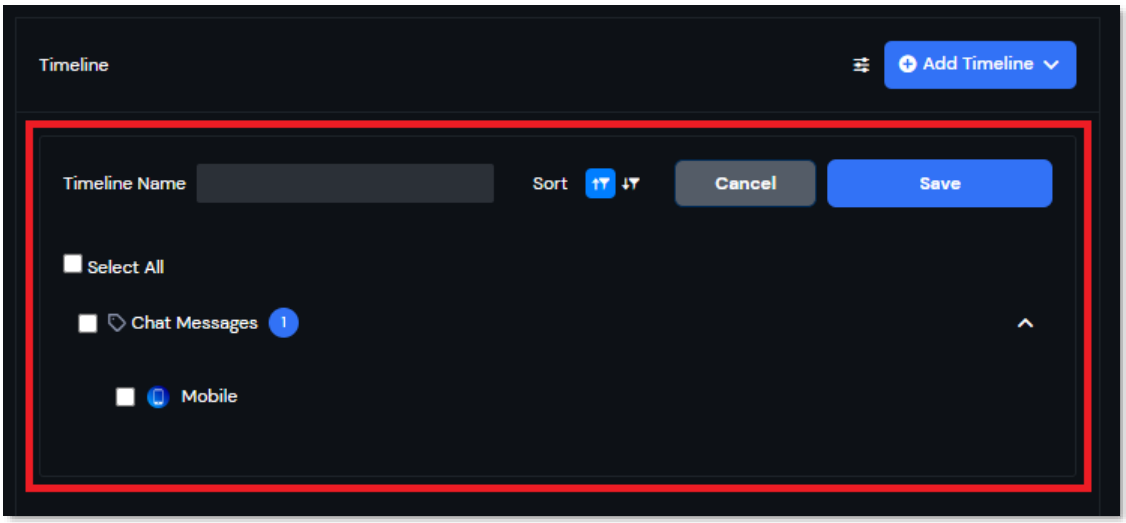
6. From the **Tags** section, expand the required **Labels** or **Bookmarks** from the corresponding sections.
7. Select the file types that should be added to the report.
8. Click **Save & Next**.

© Exterro, Inc. All rights reserved

Timeline



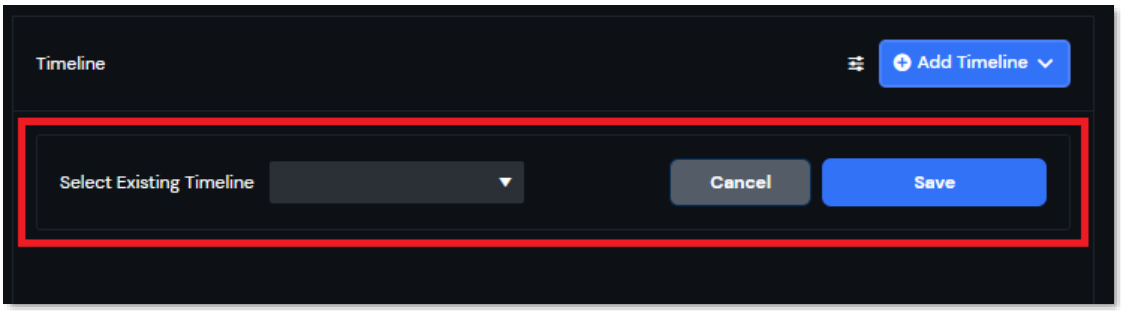
9. From the **Timeline** section, click on **Add Timeline** and select any of the below options:
   - **Create New Timeline** – To create a new timeline event based on the files labeled in the case.



Note: You can choose whether the timeline event should be sorted in ascending or descending order using the **Sort** field.

© Exterro, Inc. All rights reserved

- **Add Existing Generated Timeline** – To add the timelines that are already created from the Timeline View.



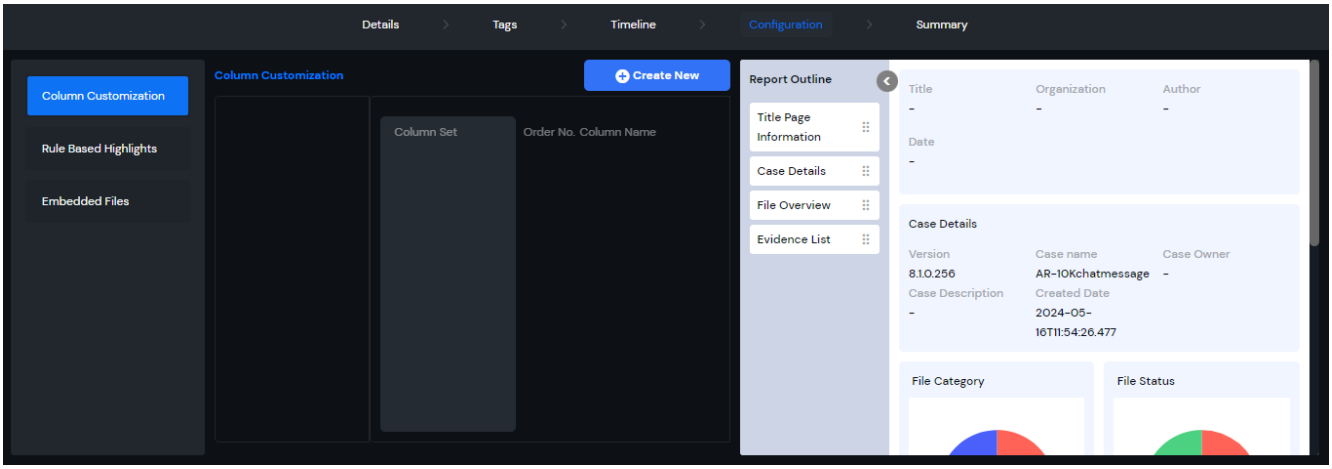
Notes:

- You can click on the **Event Configuration** button to configure specific set of events that should be displayed in the report.

10. Click **Save**.
11. Click **Save & Next**

© Exterro, Inc. All rights reserved

Configuration

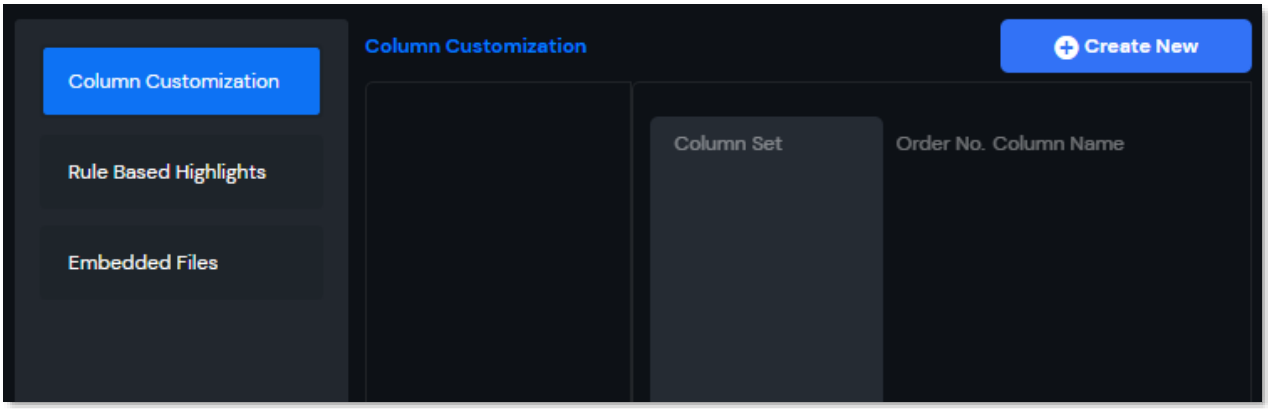


This section consists of the following options to perform the corresponding operations:

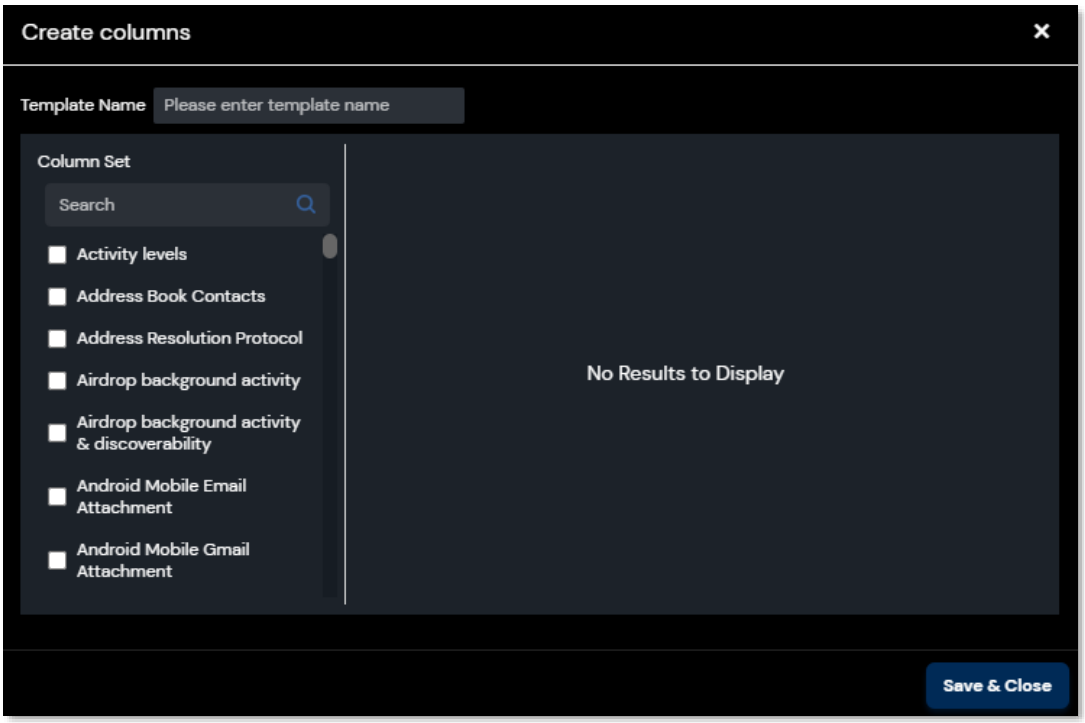
© Exterro, Inc. All rights reserved

Column Customization:

The **Column Customization** option allows users to use predefined column sets or create custom sets to be included within a report.



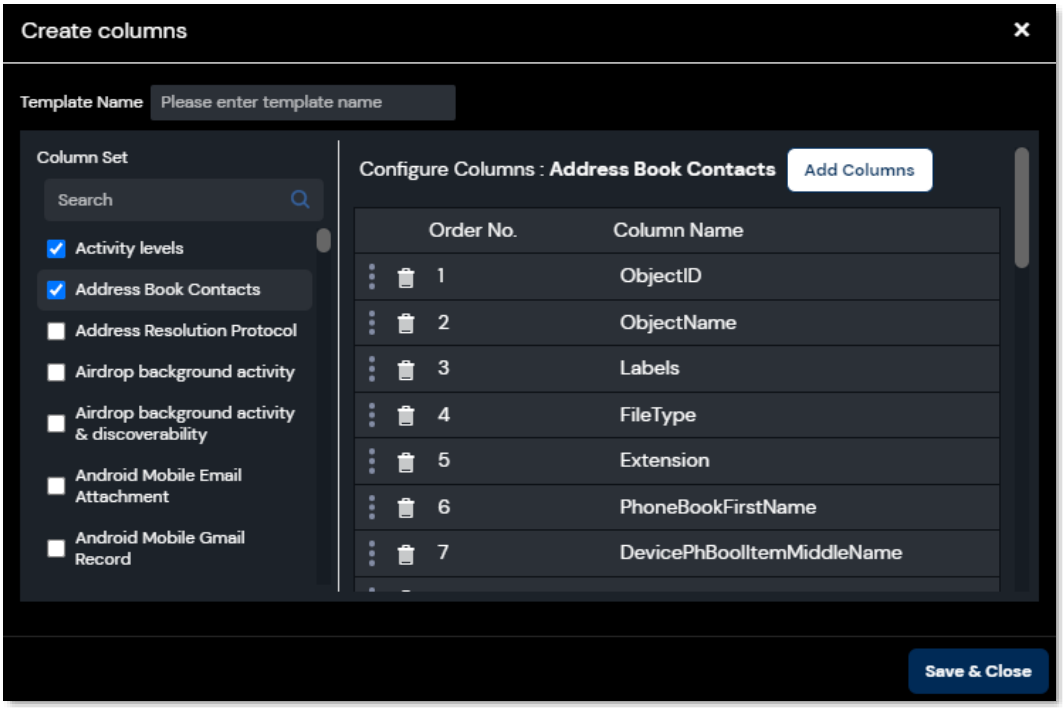
I. From the **Column Customization** section, click **Create New**.
II. The **Create columns** pop-up is displayed.



III. Enter a **Template name**.

© Exterro, Inc. All rights reserved

IV. Select the required **Column Set**.



V. Click and drag any columns within the **Configure Columns** list to reorder them.
   i. Alternatively, click the **delete** button to remove any columns from the predefined list.

VI. Click **Add Columns**.

VII. Using the **Search** functionality, locate any required columns and check them.

VIII. Click and drag any columns within the **Applied** list to reorder them.

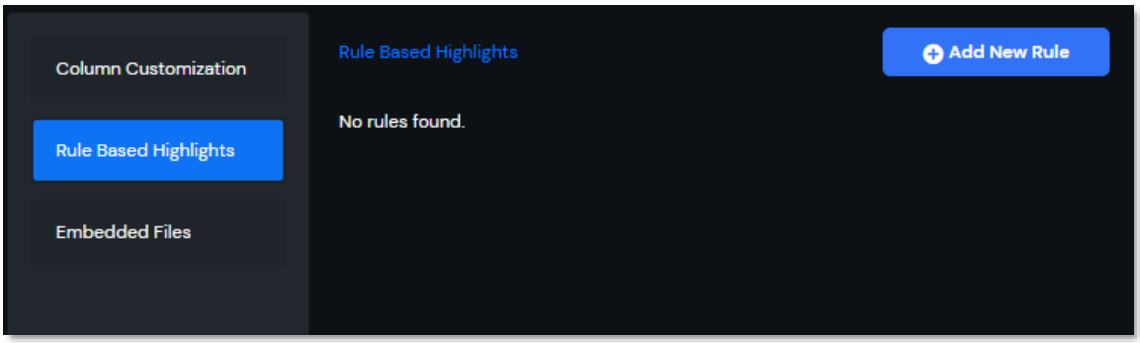
IX. Click **Apply**.

X. Click **Save & Close**.
   - The custom column sets selected for the report will be available in the **Column Set** section.
   - If additional changes need to be made to the created set, click the **Edit** icon against the required column set.

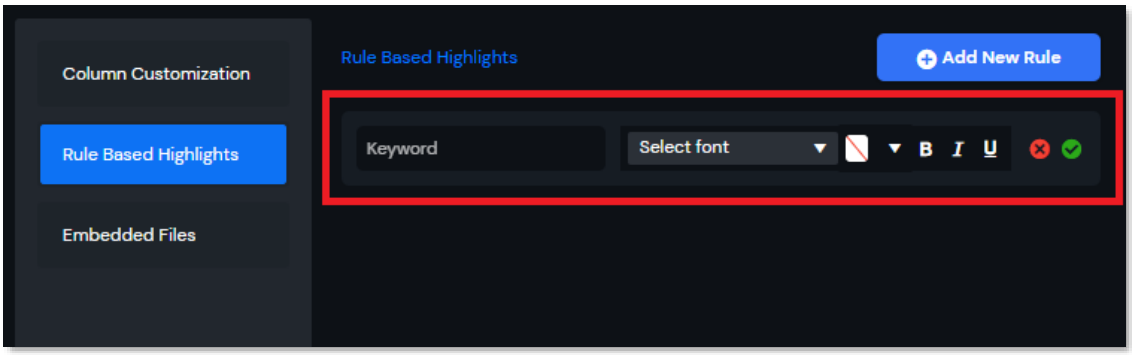
© Exterro, Inc. All rights reserved

Rule Based Highlights:

The **Rule Based Highlights** option allows you to configure a list of keywords that should be automatically highlighted within the files that are added to the report.



I. From the **Rule Based Highlights** section, click **Add New Rule**.
   - The below provided field will be displayed.



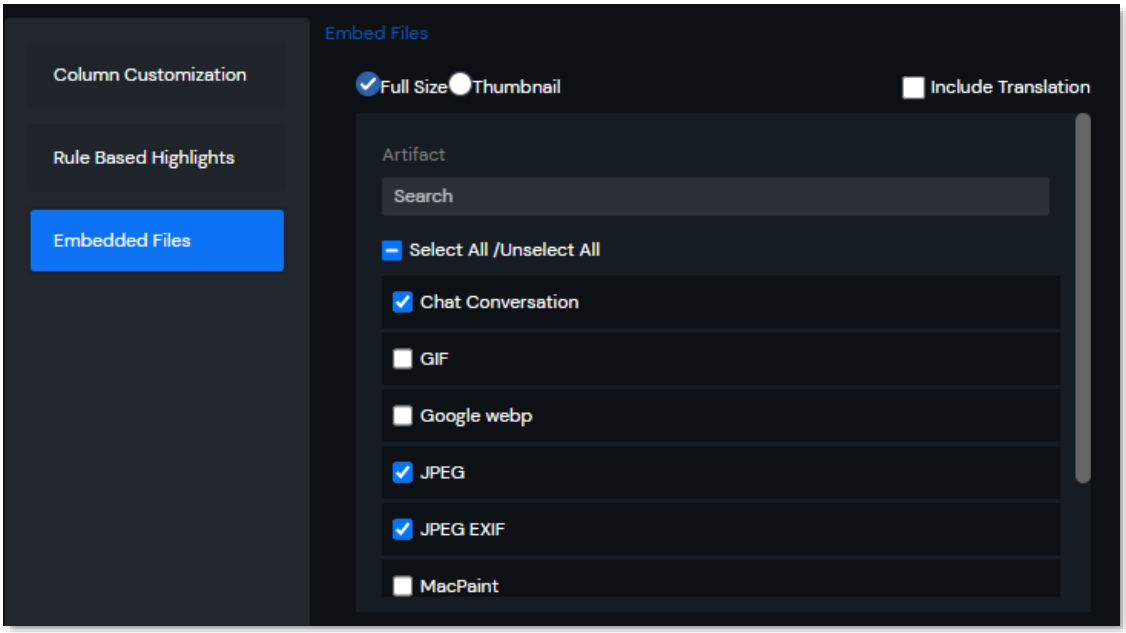
II. Enter the keyword that should be highlighted.
III. Select the keyword's font.
IV. Select the highlight color from the drop-down.
V. Click to save the keyword.

Note: You can add multiple keywords to be highlighted by clicking on the **Add New Rule** button and configure the keywords for the required number of times.

© Exterro, Inc. All rights reserved

Embedded Files:

The **Embedded Files** option allows you to embed the required type of files to the report.



I. From the **Embedded Files** section, select any one of the following embed format:
   - **Full Size** - The entire file will be embedded in the report along with its details enabling you to view the file content in the report itself.
   - **Thumbnail** - The thumbnails will be displayed against the corresponding files listed in the report. You can click on the thumbnail to open and view the corresponding files exported along with the report.

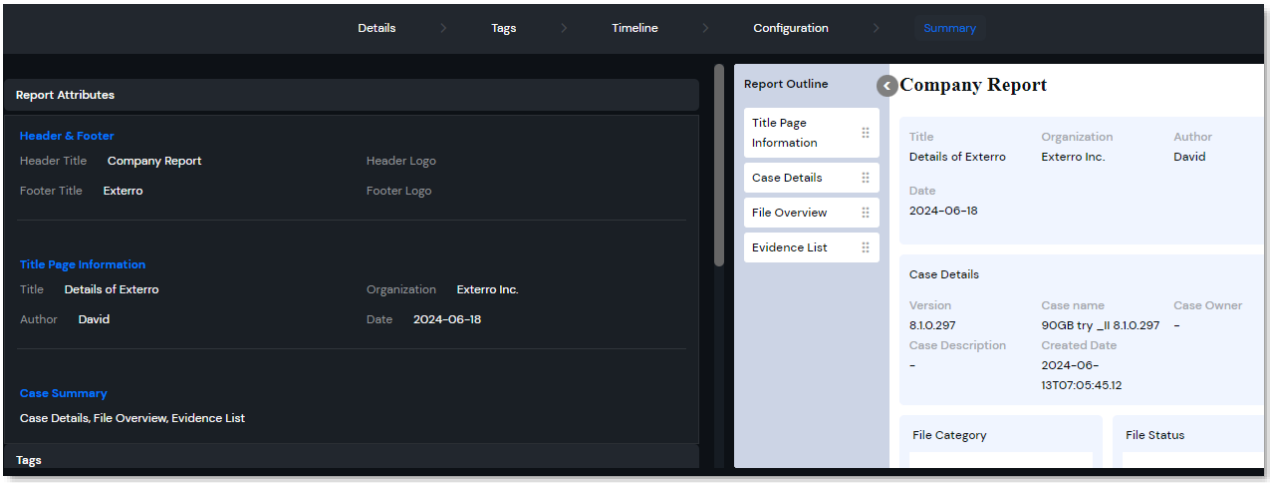
II. Select the required artifacts that should be embedded to the report.

12. Check the **Include Translation** option if you want to add the translated file along with the original file in the report.
13. Click **Save & Next**

© Exterro, Inc. All rights reserved

Summary

This section displays a summary of all the configurations made for the Detail Report.



14. Verify and ensure that all the configurations made to the report are correct.

Note: You can refer to the preview section (right pane) to get an idea of how the details in the generated report will be displayed.

15. Click **Generate Report**.

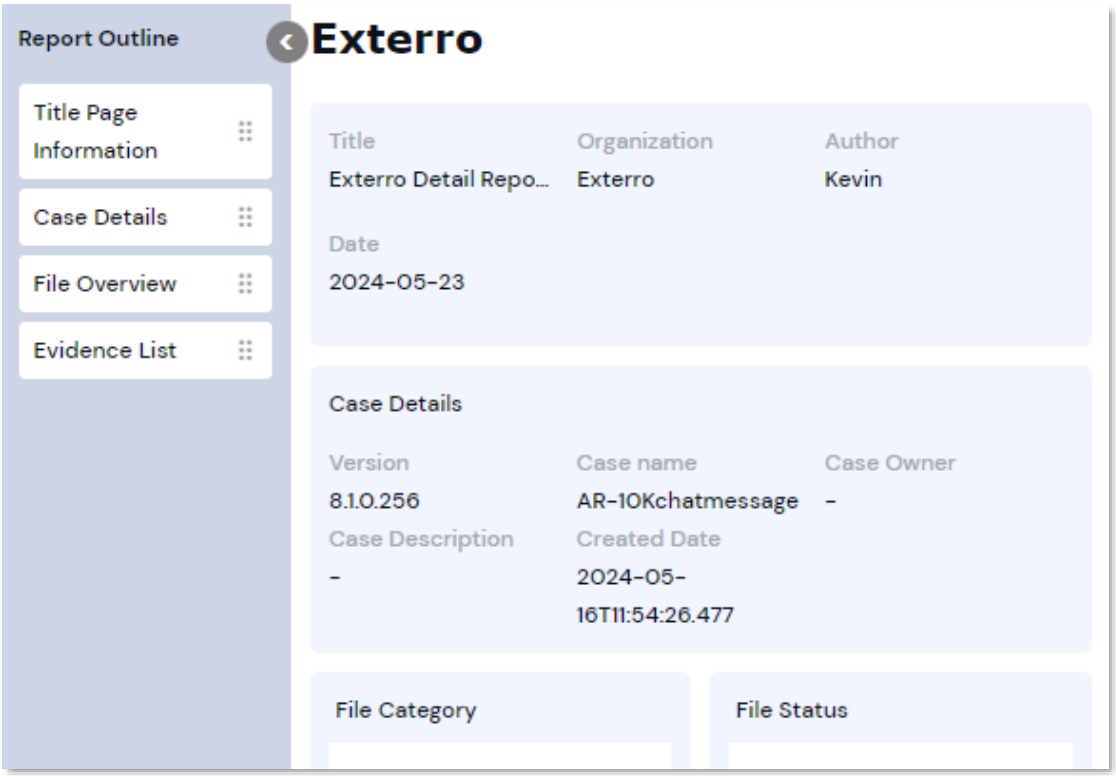
A job will be initiated to generate the report. Upon job completion, you can download the report from the Completed Reports.

If the volume of the report exceeds 1GB, the entire report should be accessed from the provided file path. Only the PDF will be downloaded locally.

© Exterro, Inc. All rights reserved

Report Preview

The Preview pane is displayed constantly in the right pane of the Detail Report creation page. This helps you to have a quick look at the report while simultaneously configuring it.



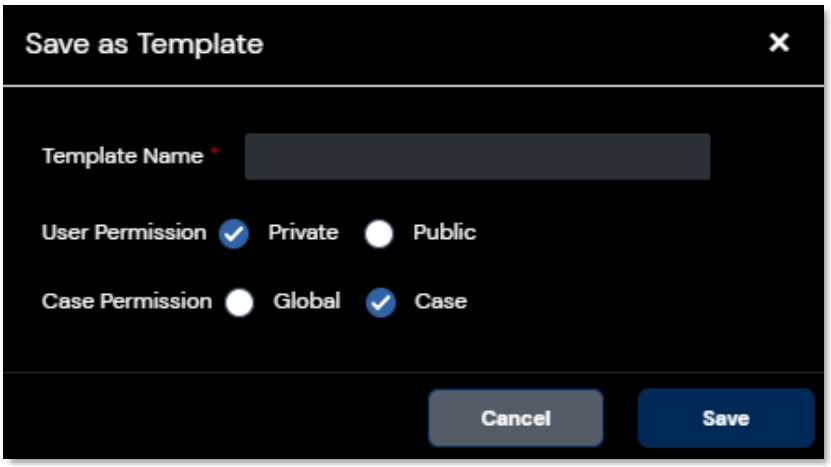
You can click and drag on the sections displayed in the **Report Outline** pane to rearrange the sections in the Detail Report.

© Exterro, Inc. All rights reserved

Report Template

To create a report template:

1. From the Summary section during report creation, click **Save as Template**.
   - The **Save as Template** pop-up is displayed.



2. Enter the **Template Name**.
3. Select any one of the below options for the **User Permission** field:

   - **Private** – Enable this option if you want the template to be accessible only by yourself.
   - **Public** – Enable this option if you want the template to be accessible by all users.

4. Select any one of the below options for the **Case Permission** field:

   - **Global** – Enable this option if you want the template to be accessible by all users.
   - **Case** – Enable this option if you want the template to be accessible only by the users associated with the case.

5. Click **Save**.

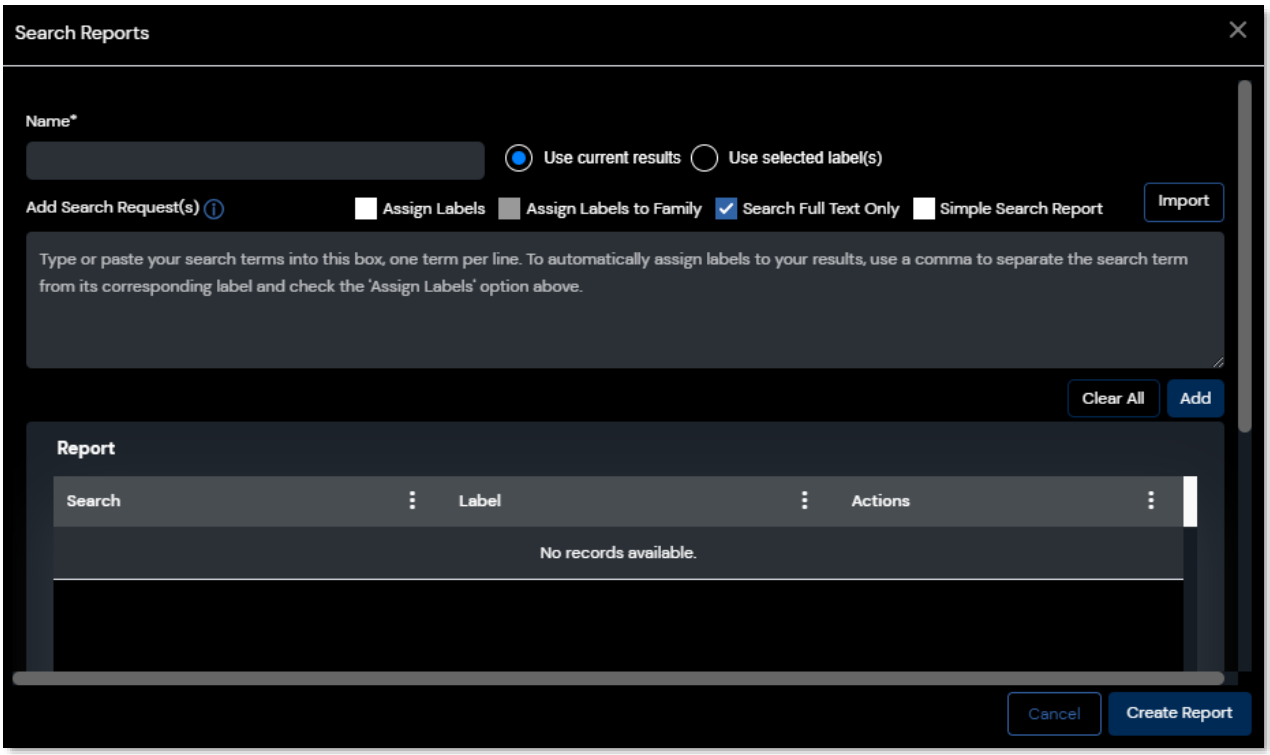
The template will be created and can be selected while creating the Detail Report.

© Exterro, Inc. All rights reserved

Creating a Search Term Report

To create a search term report:

1. From the home page, click **Case List**.
2. Select the required case.
3. Click **Enter Review**.
4. Click on the **Reports** button.
5. Click **Search Term Report**.
   - The **Search Reports** prompt is displayed.



6. Enter a **Name.**
7. Select any of the below searching options:
   - **Use current results** – To generate search report for files filtered in the Review page.
   - **User selected label(s)** – To generate the search report for the files associated with the selected labels.

© Exterro, Inc. All rights reserved

8. Enter **Search Requests**.
Alternatively, click Import to select a text file of predefined search terms and labels.

Syntax - <Search_term>, <label_name>

Example – *Official, Priority*

Note: The dtSearch syntax should be followed.

9. Click **Add**.
10. Check **Assign Labels** to automatically apply labels to the corresponding search results.
11. Check **Assign Labels to Family** to automatically apply labels to the family files associated with the corresponding search results.

Warning: The **Assign Labels to Family** option will be disabled by default and will be enabled only upon checking on the **Assign Labels** option.

12. Check **Search Full Text Only** to run the search only across the files' content i.e. the search will not be performed across the files' metadata details.
13. Check **Simple Search Report** to create a simplified search term report. When this option is checked, a report with only the number of hits and size for each search term will be created.
14. Click **Create Report**.
15. Click **View Completed Reports** from the **Generate Report** prompt to view the completed search term report with the relevant hit types:
    - **Docs with Hits -** The number of documents in the searchable set that contain the search term.
    - **Docs with Hits + Family -** The number of documents that are returned by the search, plus the number of attachment family files associated with it.
    - **Size (MB)** – The size of the documents, if exported as native files.
    - **Total Hits -** The total number of hits within the documents returned. ***Example:*** *43 hits within 10 documents.*
    - **Unique Docs with Hits** - The number of documents in the searchable set returned by only that specific term. If more than one term returns a particular document, that document is not counted as a unique hit.

© Exterro, Inc. All rights reserved

- **Unique Family Docs -** The number of family documents in the search results that only contain a specific term. If more than one term appears in a particular document family, it is not counted as a unique hit.
- **Family Emails –** The total number of hits in emails
- **Family Attachments –** The total number of hits in any email attachment.
- **Unique Emails without Attachments -** The number of emails in the searchable set returned by only that specific term. If more than one term returns a particular email, that email is not counted as a unique email.

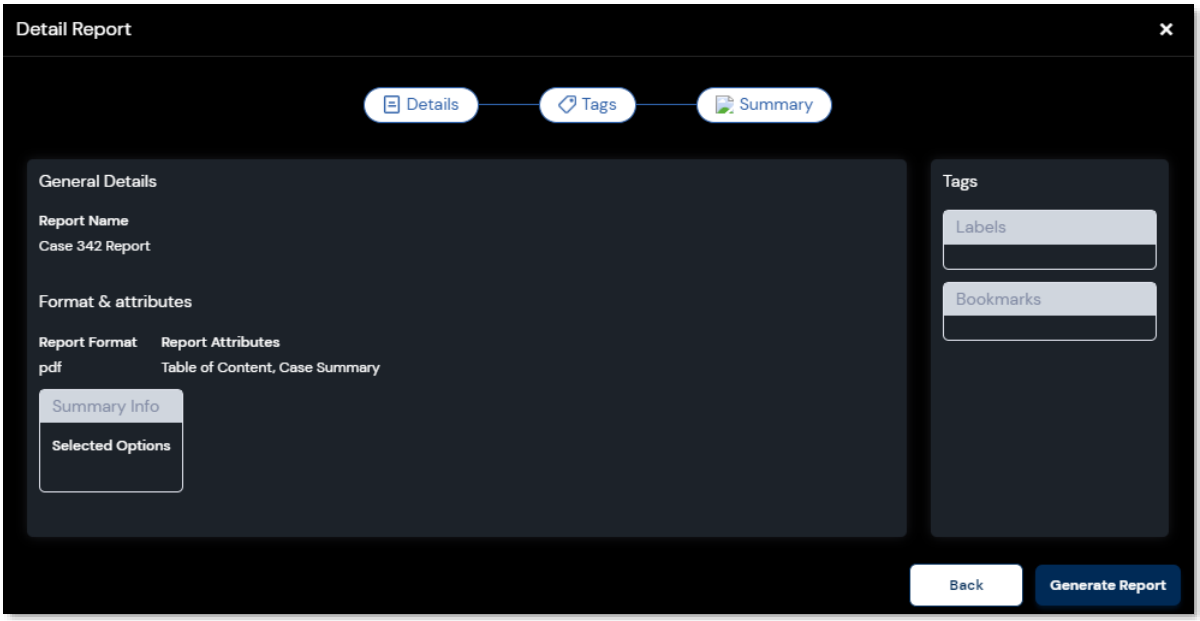
© Exterro, Inc. All rights reserved

Exporting Reports

To export a report:

1. From the **Generate Report** prompt, click on any type of reports.
   - The report configuration prompt is displayed.

2. Configure the required information in all the sections and proceed by clicking on **Save & Next**.
3. Click on **Generate Report** to generate the selected report.

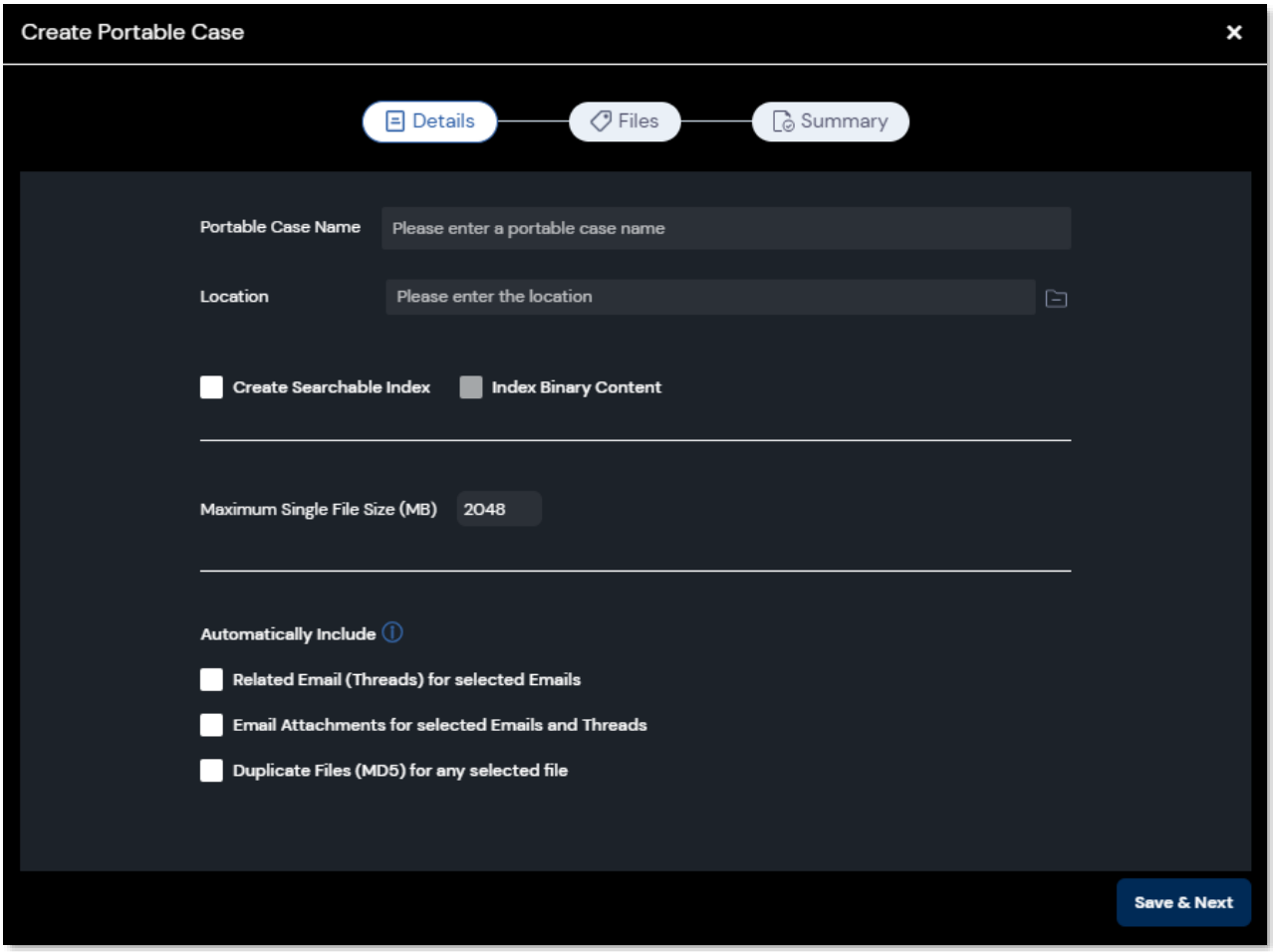


The job intended for exporting the report will be initiated.

© Exterro, Inc. All rights reserved

Portable Case

Portable Cases enable the investigator to export or share specific items from FTK for review in a "portable" FTK Portable Case instance running on a system without any licensing restrictions. However, only consisting of a limited feature set. For example, quick searches will be available, but advanced search is not.



© Exterro, Inc. All rights reserved

Prerequisites

1. The system that will host the "portable" FTK Portable Case must have Microsoft .NET Framework 4.7.2 and Visual C++ 2013 Redistributable already installed.
2. The FTK Portable Case system does not need to have full version of FTK Portable Case installed. The FTK Portable Case binaries come bundled with the exported data by default.

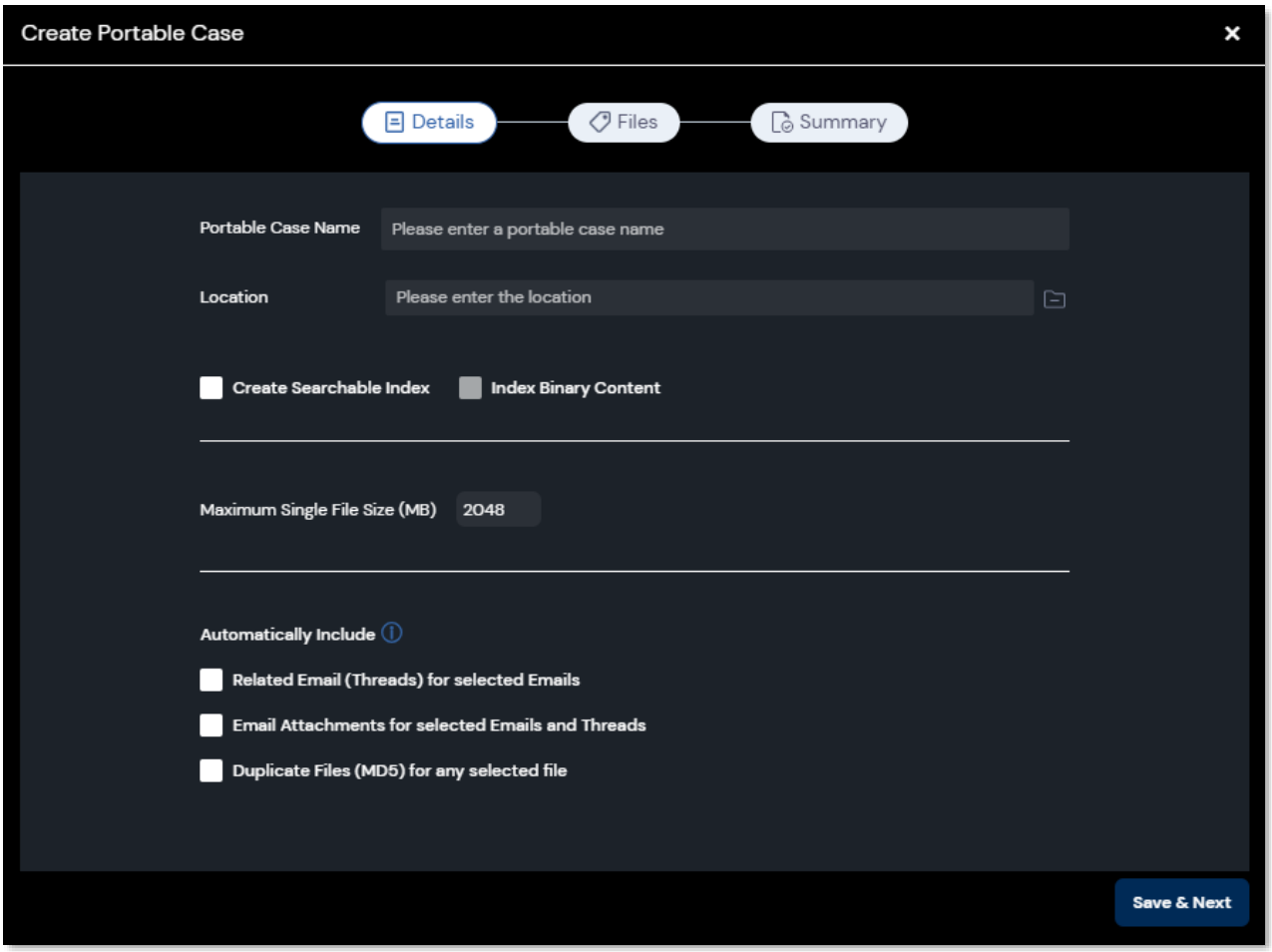
Note: When a Portable Case is being opened, it will install both VLC and OutsideX if they are not already present.

© Exterro, Inc. All rights reserved

Creating a Portable Case

To create a Portable Case:

1. From the home page, click on **Case list**.
2. Select the required case.
3. Click **Enter Review**.
4. Click on the **Reports** button.
5. Select **Create Portable Case**.
    - The **Create Portable Case** pop-up is displayed.



© Exterro, Inc. All rights reserved

Details:

6. Enter the Portable Case Name.
7. Browse and select the location where the Portable Case should be generated.
8. Check **Create Searchable Index**.
    - This will create a new index for the sub-set of items to be included in the portable case. This is not the same index as the case.
9. Enable the **Index Binary Content** option to index the binary values of the file.

Note: The **Index Binary Content** option will be enabled only upon selecting the **Create Searchable Index** option.

10. Enter the value for **Max Single File Export Size** (MB).
    - This will limit the files being exported for the portable case. If a limit of 2048 MB is set, any files bigger than this will not be added to the portable case.
11. Check the following options for the **Automatically Include** field on to include the corresponding files to the Portable Case:
    - **Related Emails (Threads)** - To include only the email threads related to the selected emails.
    - **Email Attachments** - To include only the email attachments of the selected emails.
    - **Duplicate Files (MD5)** - To include the duplicate files of the selected files.
12. Click **Save & Next**.

© Exterro, Inc. All rights reserved

Files:

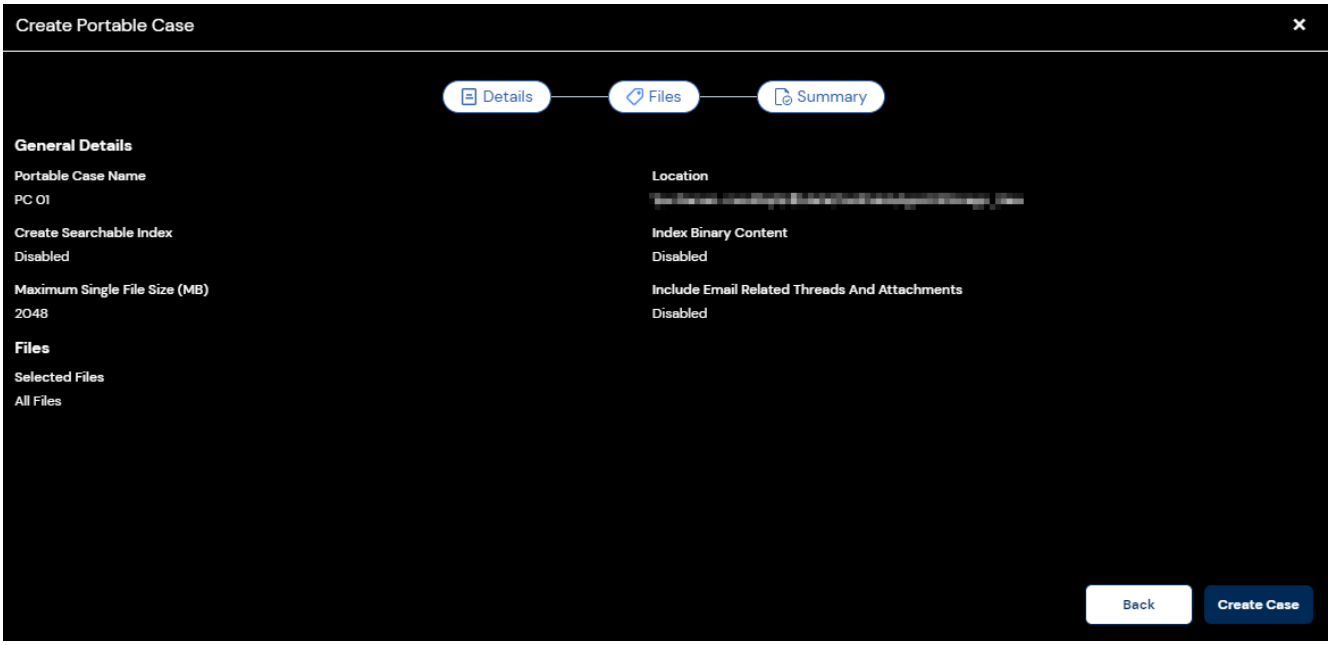
13. Select any one of the below options to add files to the Portable Case:

- **All Files** – To add all the files in the case to the Portable Case.
- **Checked Files** – To add the files that are checked in the Review page.
- **Filtered Files** – To add the files that are filtered in the Review page.
- **Tagged Files** – To add the files that are labeled or bookmarked.

14. Click **Save & Next**.

© Exterro, Inc. All rights reserved

Summary:



15. Ensure if all the configurations made for Portable Case are correct in the **Summary** section.
16. Click **Create Case**.

© Exterro, Inc. All rights reserved

Opening a Portable Case

1. Navigate to the folder where the Portable Case is generated.
2. Double click on **Launch FTK Portable Case** file.

Note: The Portable Case will attempt to install any additional packages if required.

3. The Portable Case will be opened.

Opening a Portable Case with an existing FTK Portable Case instance

Note: This is applicable only if the portable cases are created without enabling the Include FTK Plus option.

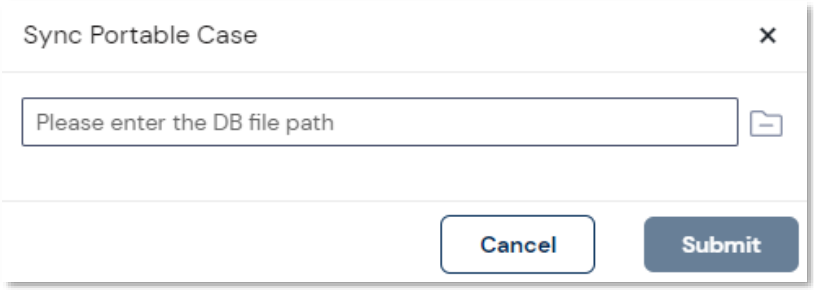
1. Navigate to a Portable Case folder.
2. Double click on **Launch FTK Portable Case** file.
3. Click on **Explore Portable Data File**.
4. Navigate to another **data.db** file associated with a portable case and click Open to view the portable case.

Note: Typically, **data.db** files are stored within the root directory of a portable case.

© Exterro, Inc. All rights reserved

Syncing a Portable Case with FTK Central

1. Login to the FTK Central application.
2. Click on **Case List**.
3. Click on the **Actions** menu against the required case.
4. Click **Portable Case Sync**.
   - The **Sync Portable Case** pop-up is displayed.



5. Select the **.db** file located in the root directory of the portable case.
6. Click **Submit**.

© Exterro, Inc. All rights reserved

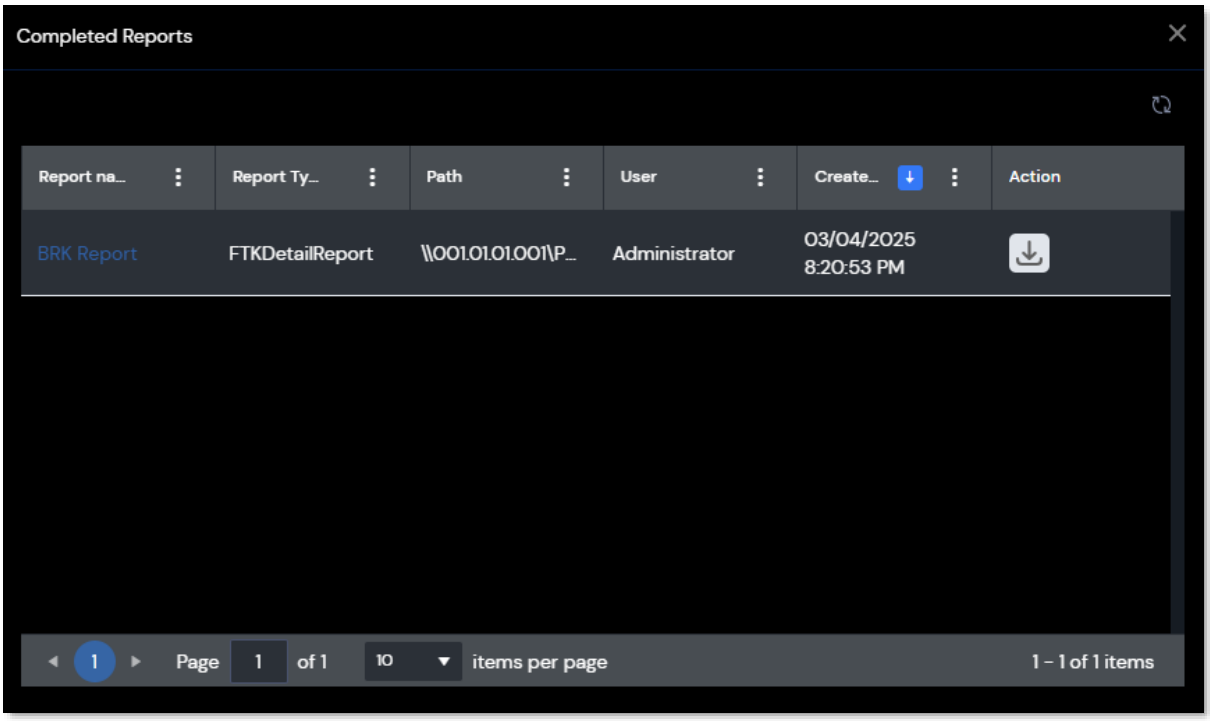
Viewing and Downloading Completed Reports

To view and download a completed report:

1. From the **Generate Report** prompt, click on **View Completed Reports**.

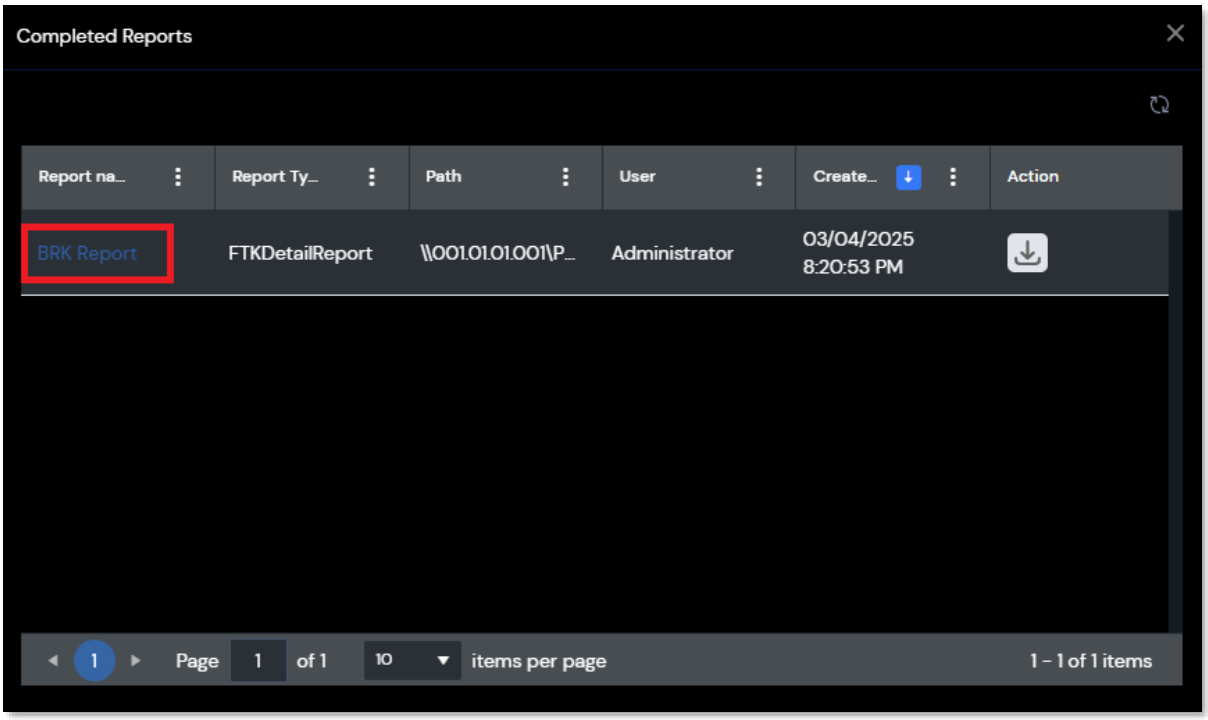
© Exterro, Inc. All rights reserved

- The **Completed Reports** pop-up is displayed.

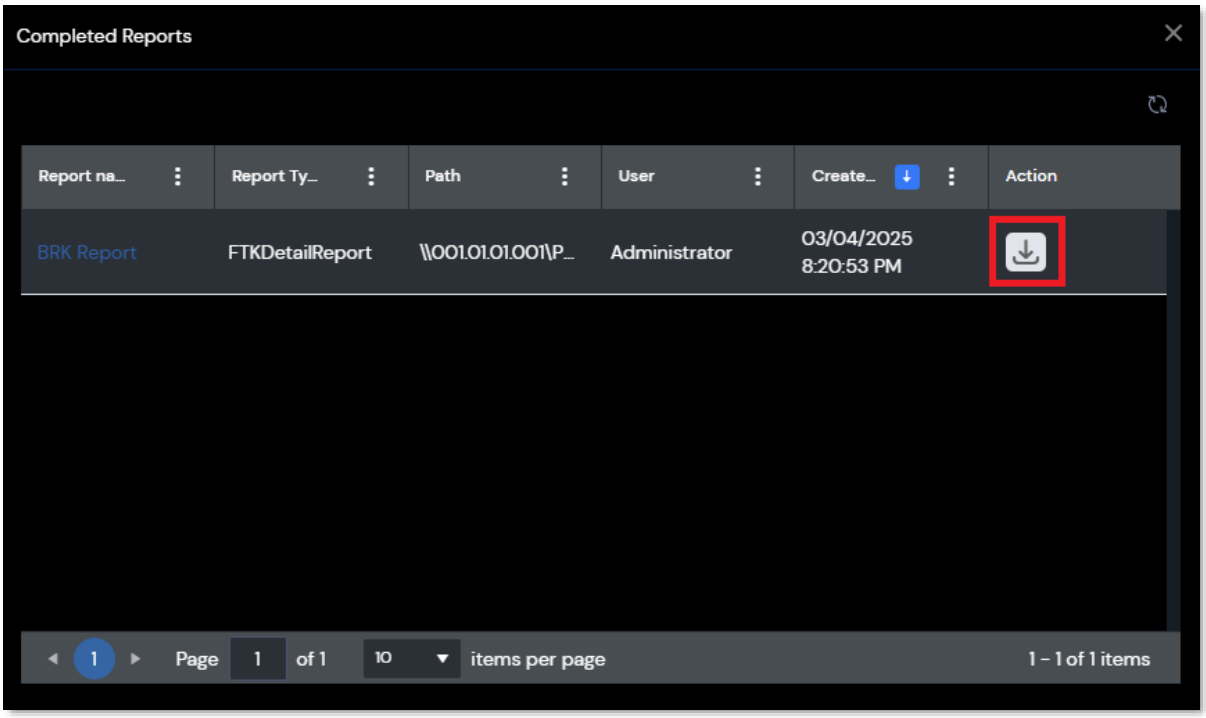


© Exterro, Inc. All rights reserved

2. Click on the **Report Name** to open and view the file in the browser tab**.**



3. Click on the **Download** button to download the file**.**



© Exterro, Inc. All rights reserved

Coding Panels within Review

Coding is putting values into the fields (columns) of documents. The Coding panel in Review allows you to use coding layouts to change the data of the selected document. Coding layouts can be created from the Case List or during Batch Administration.

Reviewers with View Coding Layout permissions can code the data of a document using the Coding panel and the mass actions in the Grid panel. Coding allows you to identify descriptive pieces of information that never had metadata, like images that were loaded and need to have dates manually added into the field. The Coding panel in Review allows you to use coding layouts to code the selected document.

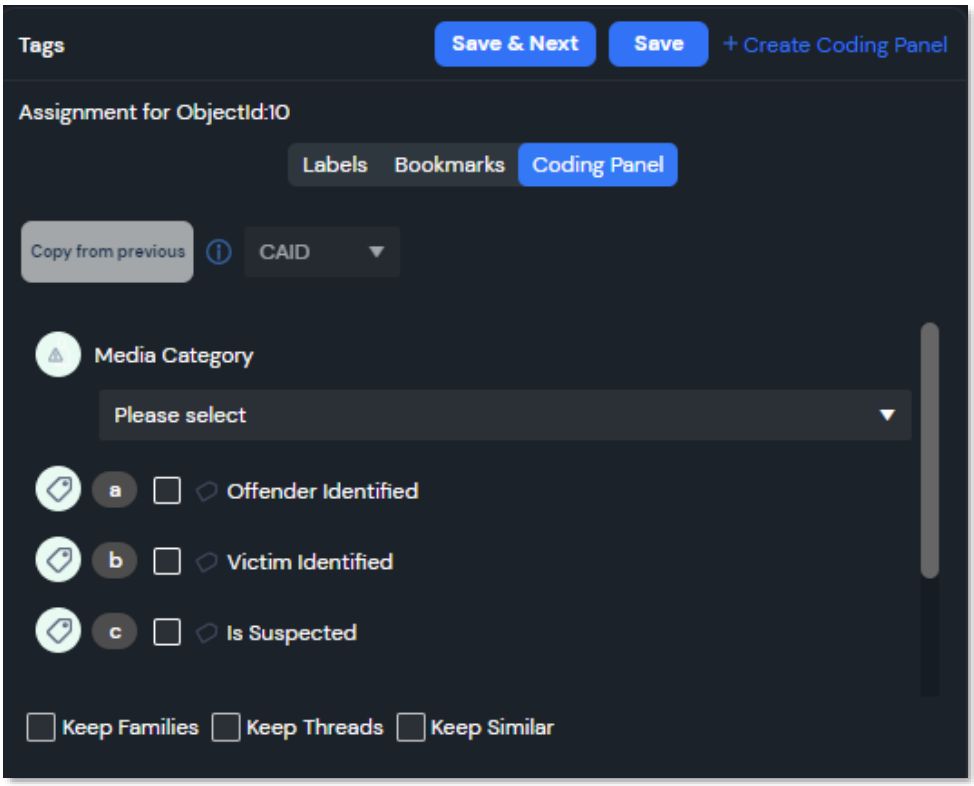
Creating Coding Panel

To create a coding panel:

1. From the home page, click **Case List**.
2. Select a Case.
3. Click **Enter Review**.
4. Click on the **Show Tags Panel** button.

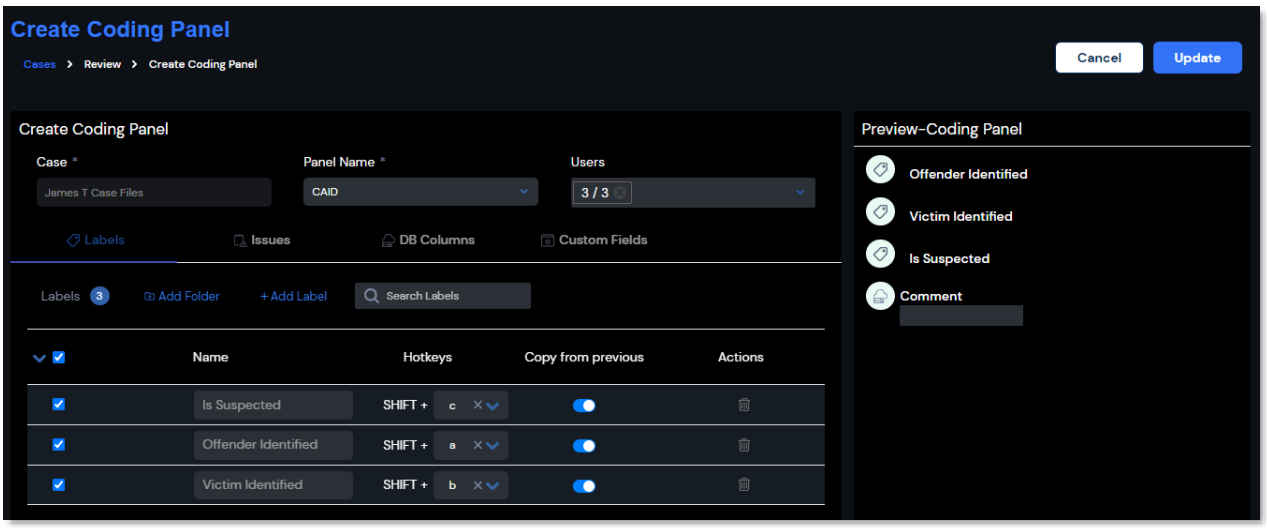
© Exterro, Inc. All rights reserved

5. Select the **Coding Panel** tab.



© Exterro, Inc. All rights reserved

6. Click **+ Create Coding Panel.**
    - The **Create Coding Panel** page is displayed.



7. Select the **Panel Name**.
8. Select the **Users** that will have access to the coding panel.
9. Use the sections below to configure new Creating Labels, Creating Issues, Creating DB Columns and Creating Custom Fields.
10. Click **Create**.

© Exterro, Inc. All rights reserved

Creating Labels

To create a label:

1. Navigate to **Labels** tab.
2. Click on **+ Add Label**.
3. Enter the label's name in the field prompted.
4. Configure the hotkey by selecting a key against the **SHIFT +** field.
5. Enable **Copy From Previous** option in order to apply the previously made configuration to the current record.
6. Click on the **Save** button .

Notes:

- From the list of labels, you can click on **Delete** to remove the label.
- From the list of labels, you can click on the **New Label** button against a label folder to create a child label.
- From the list of labels, you can click on the **New Folder** button against a label folder to create a child folder.

© Exterro, Inc. All rights reserved

Creating Issues

To create an issue:

1. Navigate to **Issues** tab.
2. Click on **+ Add Issues**.
3. Enter the issue's name in the field prompted**.**
4. Configure the hotkey by selecting a key against the **SHIFT +** field.
5. Enable **Copy From Previous** option in order to apply the previously made configuration to the current record.
6. Click on the **Save** button .

Notes:

- From the list of issues, you can click on the **Delete** button to delete the issue.
- From the list of issues, you can click on the **Add Child Issue** button against the required issue to create a child issue.

Creating DB Columns

To create a DB column:

1. Navigate to **DB Columns** tab.
2. Select one or more **DB columns.**

© Exterro, Inc. All rights reserved

Creating Custom Fields

To create a custom field:

1. Navigate to **Custom Fields** tab.
2. Click on **+ Add Custom Fields**.
3. Enter a custom field **Name**.
4. Select the **Type** of custom field to be created.
   - Checkbox
   - Radio
   - Date
   - Text
   - Number
   - Multi Entry – This option requires users to separate values with a semicolon (;).
5. Enable **Copy From Previous** option in order to apply the previously made configuration to the current record.
6. Enable the **Required** option to force users to enter a value into the custom field before submission.
7. Click **Save.**

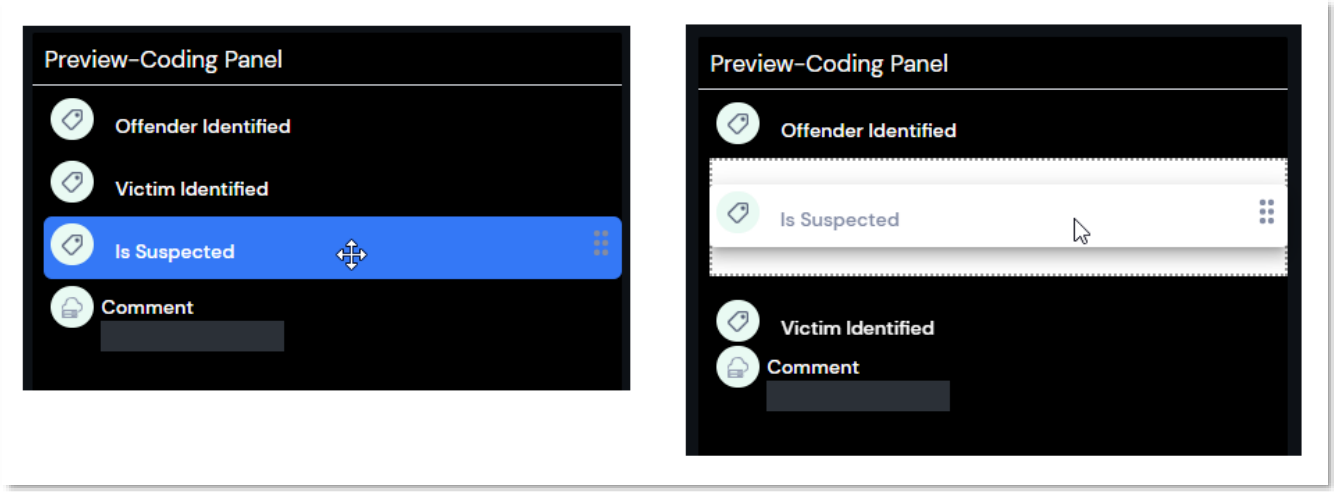
Note: From the list of custom fields, you can click on the **Delete** button to remove the field.

© Exterro, Inc. All rights reserved

Reorganizing a Coding Panel

To reorganize coding panel layouts:

1. From the home page, click **Case List**.
2. Click on the required case.
3. Click on **Enter Review**.
4. Click on the **Show Tags Panel** button.
5. Select the **Coding Panel** tab.
6. Click **+ Create Coding Panel.**
7. Hover over a coding panel element in the **Preview-Coding Panel** pane.



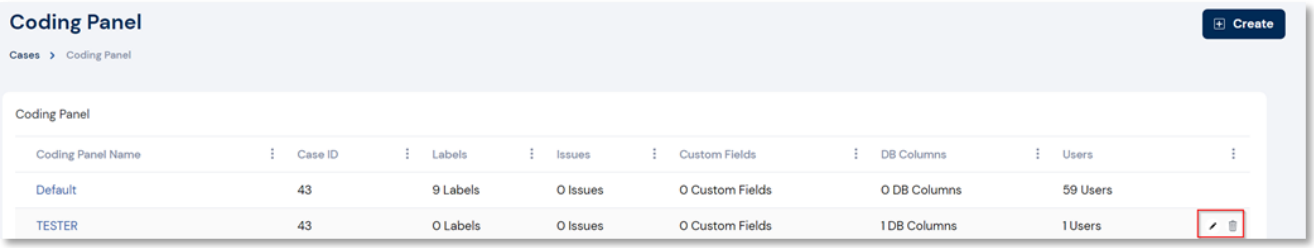
8. Click and drag an element in its desired order.
9. Click **Update**.

© Exterro, Inc. All rights reserved

Deleting Coding Panels

To delete a coding panel:

1. From the home page, click **Case List**.
2. Click on the **Context menu** (in the **Actions** column) against the required case.
3. Click on **Manage Coding Panel**.



4. Click on the **Delete** button .

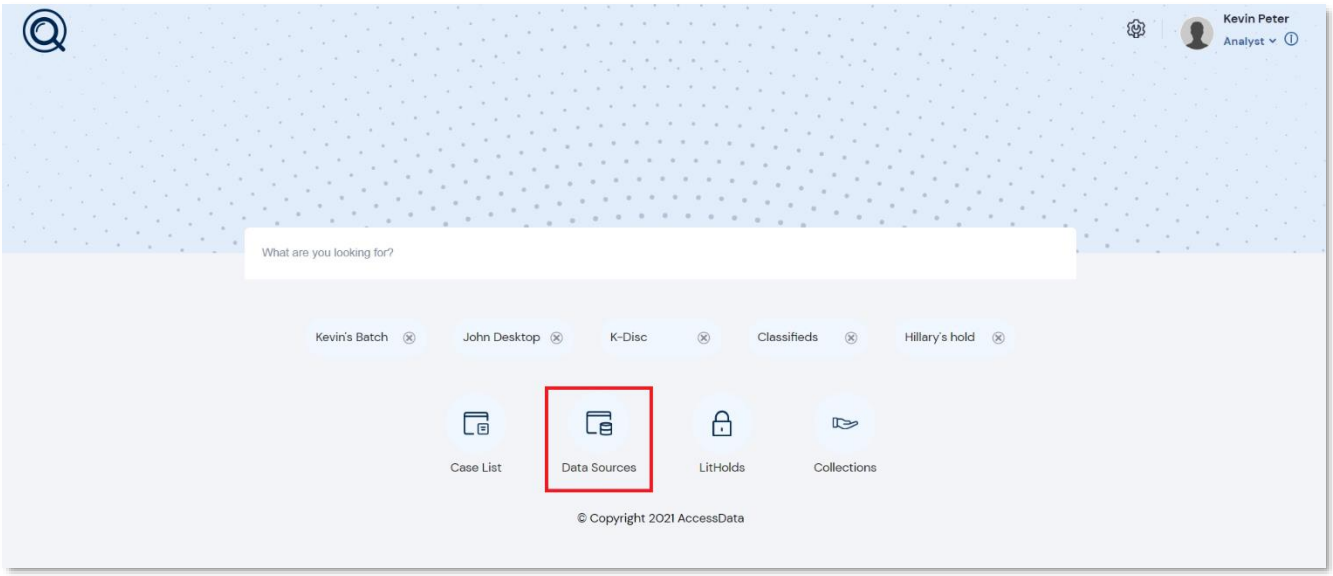
Warning: Clicking on the Delete button will remove the coding panel without prompting any further confirmation.

© Exterro, Inc. All rights reserved

Data Sources

Data Sources are the sources of data relevant to a case during electronic discovery or security investigation. The data can include electronically stored information on employees, system management computers, and can refer to people, Network shares, Domino or Exchange email accounts, or other public repositories associated with the person.

The Data Sources module allows you to add, define, delete and edit data sources. Once data sources have been configured, data can be collected remotely and then processed.



© Exterro, Inc. All rights reserved

Managing Data Sources

FTK Central supports data management and collection from 11 different data sources and the details to manage the data sources are provided in the upcoming sections.

Elements of Managing Data Sources

Network Share	• Adding Network Share data sources • Importing Network Shares data sources from CSV • Mapping Network Share to custodians • Editing Network Share data sources • Deleting Network Share data sources
Computer	• Adding Computer data sources • Importing Computer data sources from CSV • Mapping Computer to custodians • Editing Computer data sources • Deleting Computer data sources • Creating Endpoint Reports
Gmail	• Adding Gmail data sources • Mapping Gmail data sources to custodians • Editing Gmail data sources • Deleting Gmail sources
Google Drive	• Adding Google Drive sources • Mapping Google Drive data sources to custodians • Editing Google Drive data sources • Deleting Google Drive sources
OneDrive	• Adding OneDrive sources • Mapping OneDrive data sources to Custodians • Editing OneDrive data sources

© Exterro, Inc. All rights reserved

	• Deleting OneDrive sources
Microsoft Teams	• Adding Microsoft Teams sources • Editing Microsoft Teams data sources • Deleting Microsoft Teams sources
Slack	• Adding Slack data sources • Editing Slack data sources • Deleting Slack data sources
SharePoint	• Adding SharePoint data sources • Editing SharePoint data sources • Deleting SharePoint data sources
Exchange	• Adding Online/Office 365 data sources • Adding Exchange data sources • Mapping Exchange data sources to custodians • Editing Exchange data sources • Deleting Exchange data sources
Box	• Adding Box data sources • Editing Box data source • Deleting Box data source

Tip: To filter the grid efficiently, you can simply enter a keyword into the search box

located at the top of any grid and click the search button or press enter.

© Exterro, Inc. All rights reserved

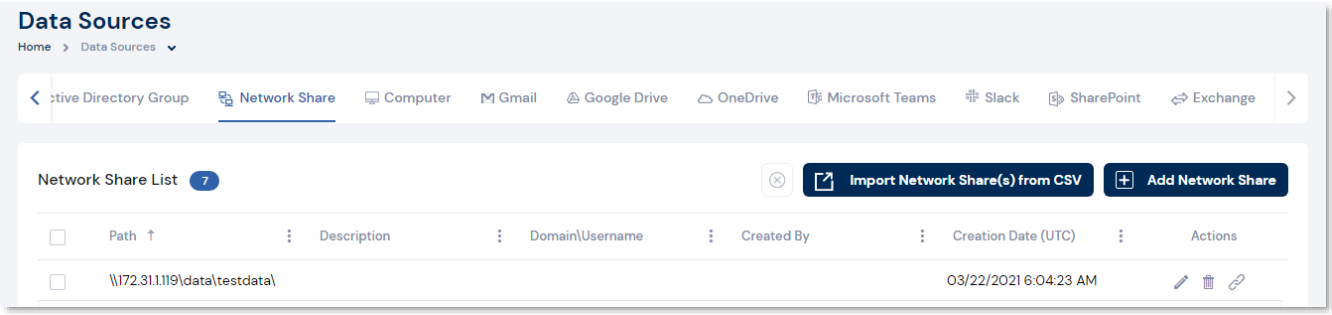
Network Share

Shares are network folders on which the person may possess read and write access permissions. You can add or remove shares from this page, edit a share path, or add and edit a share's locality and description.

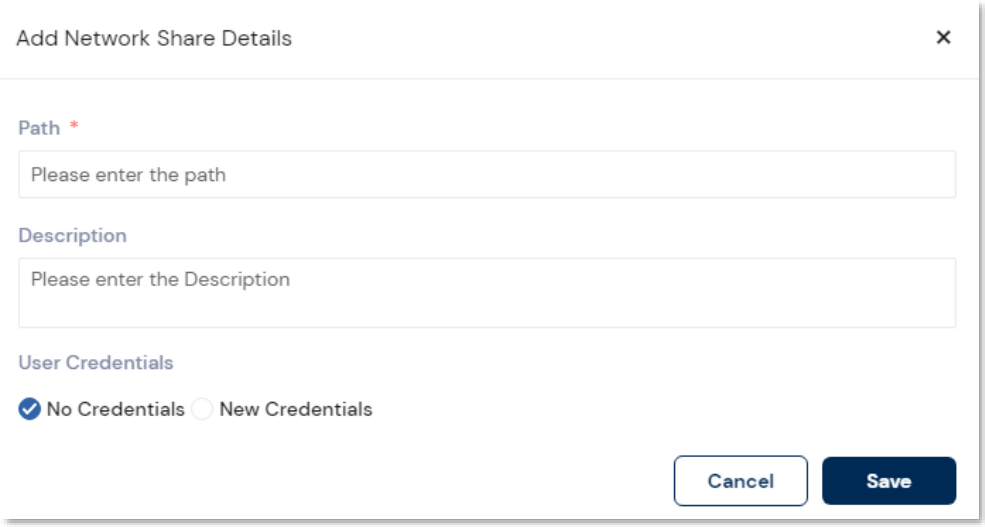
Adding Network Share data sources

To add a Network Share data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Network Share**.



3. Click **Add Network Share**.
   - The **Add Network Share Details** pop-up is displayed.



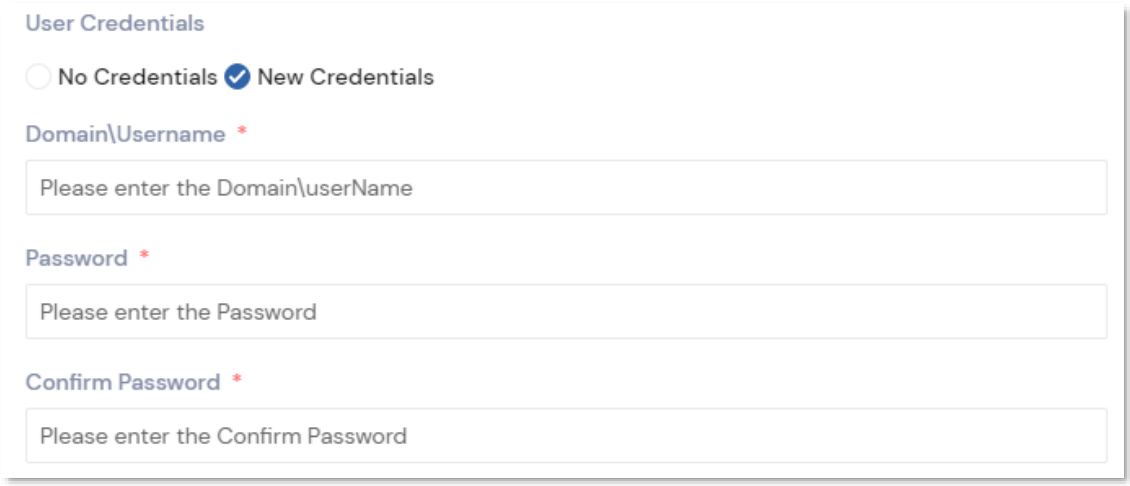
© Exterro, Inc. All rights reserved

4. Enter the **Path** of a network share.

5. Provide a **Description**.

6. Choose **No Credentials** if you don't want any authentication to access it or **New Credentials** to set a username and password for it.

Note: The below steps are to be performed for configuring new credentials.



i. Provide a **Domain/Username** for the network share.

ii. Provide a **Password**.

iii. Repeat the same password in **Confirm Password** field.

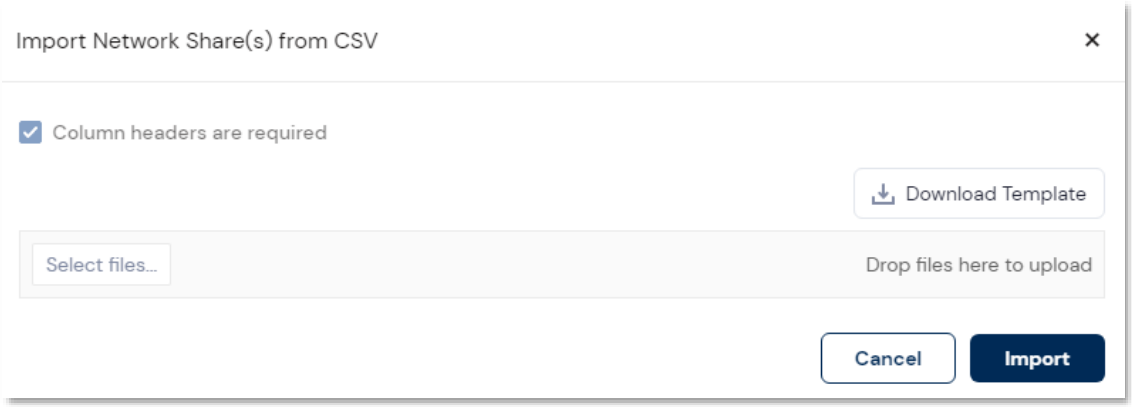
7. Click **Save**.

© Exterro, Inc. All rights reserved

Importing Network Share from CSV

To add a Network Share data source from CSV:

1. From the home page, click **Data Sources**.
2. Navigate to **Network Share**.
3. Click **Import Network Share(s) from CSV**.
    - The **Import Network Share(s) from CSV** pop-up is displayed.



4. Click **Select files**.
5. Select the required file or drag and drop the file to be uploaded.
6. Click **Import**.

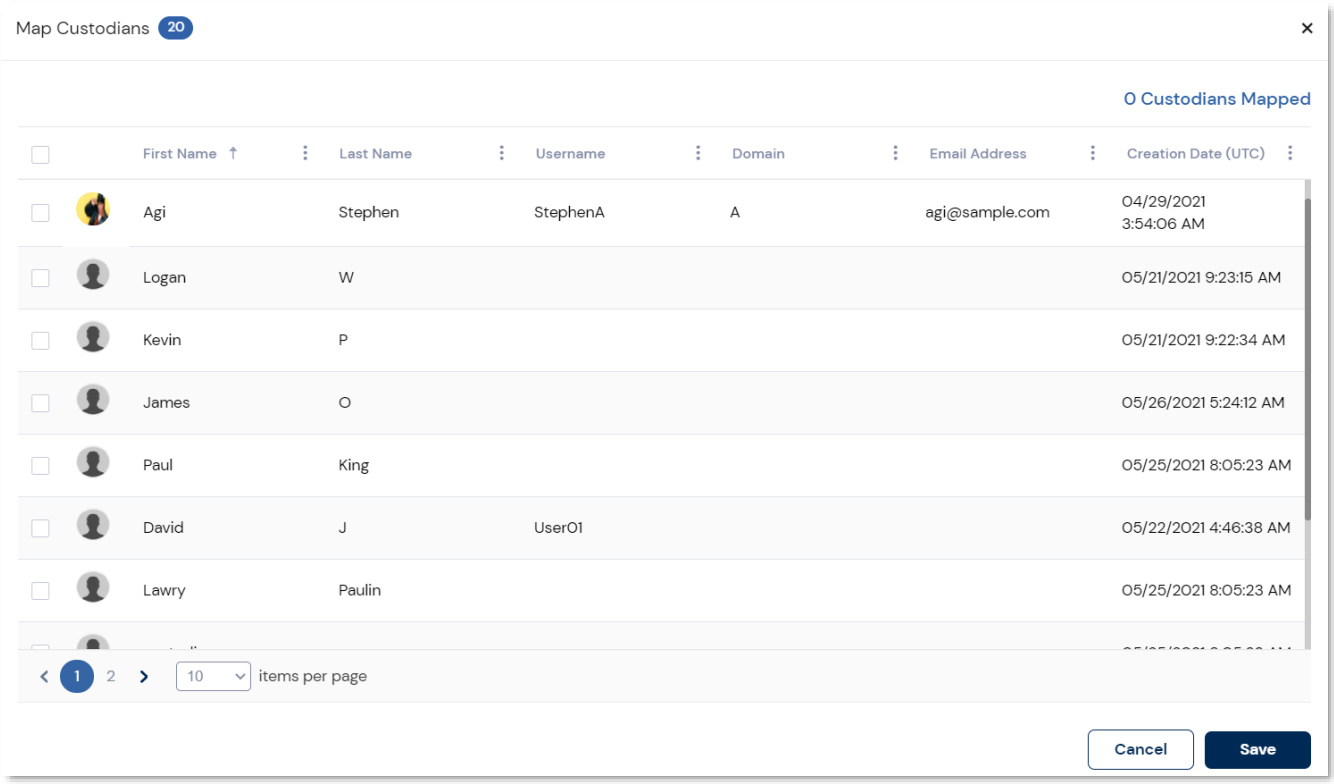
Note: You can click on **Download Template** fill in the details of the network share and upload it for the application to read the network shares to be imported.

© Exterro, Inc. All rights reserved

Mapping Network Shares data sources to Custodians

To map a Network Share data source to custodians:

1. From the home page, click **Data Sources**.
2. Navigate to **Network Share**.
3. Click **Map Custodian** against the data source to be mapped.
   - The **Map Custodians** pop-up is displayed.



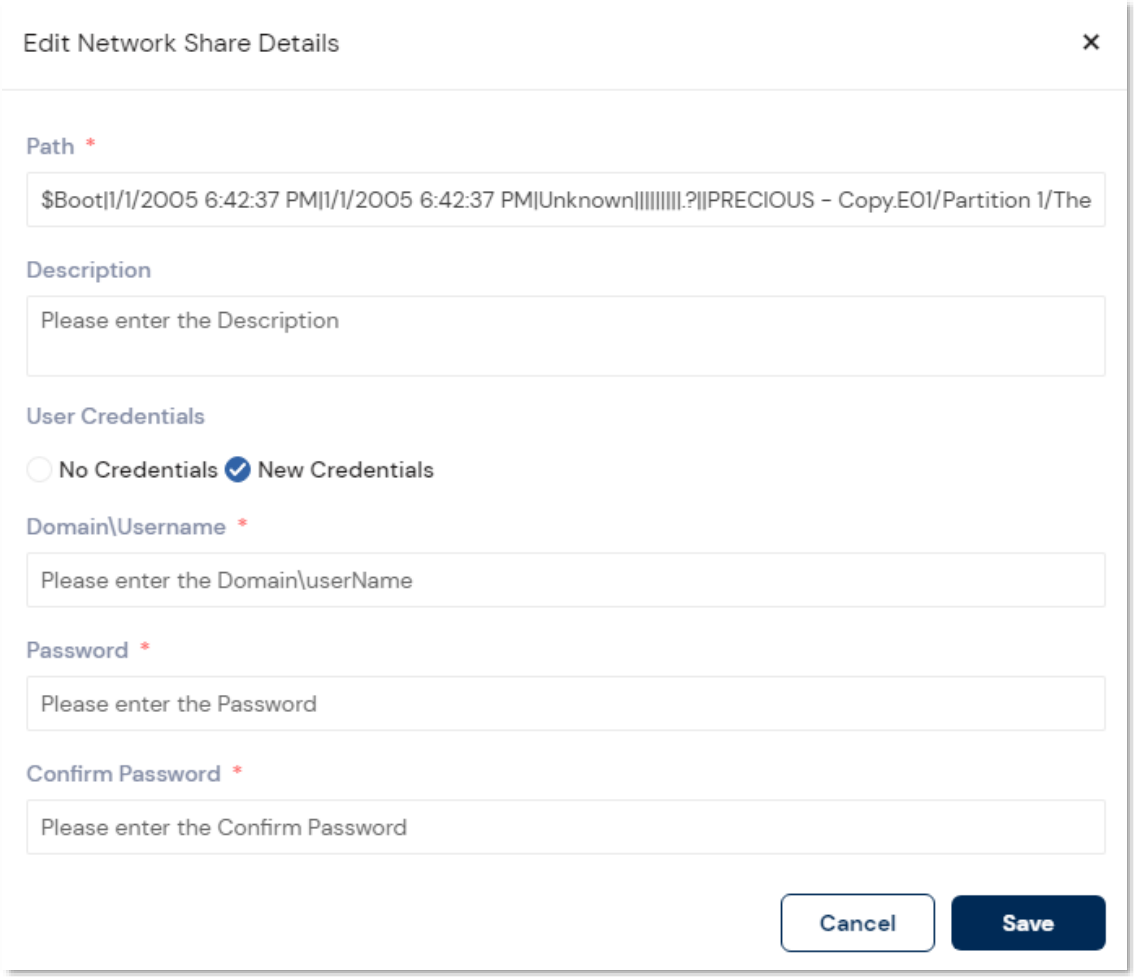
4. Select the required custodians by enabling the checkbox against it.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Editing Network Share data sources

To edit a Network Share data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Network Share**.
3. Click **Edit** against the data source to be edited.
   - The **Edit Network Share Details** pop-up is displayed.



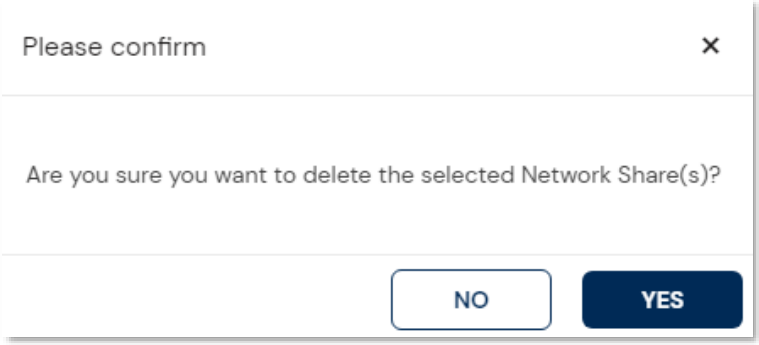
4. Make the necessary changes.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting Network Share data sources

To delete a Network Share data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Network Share**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.

© Exterro, Inc. All rights reserved

Computer

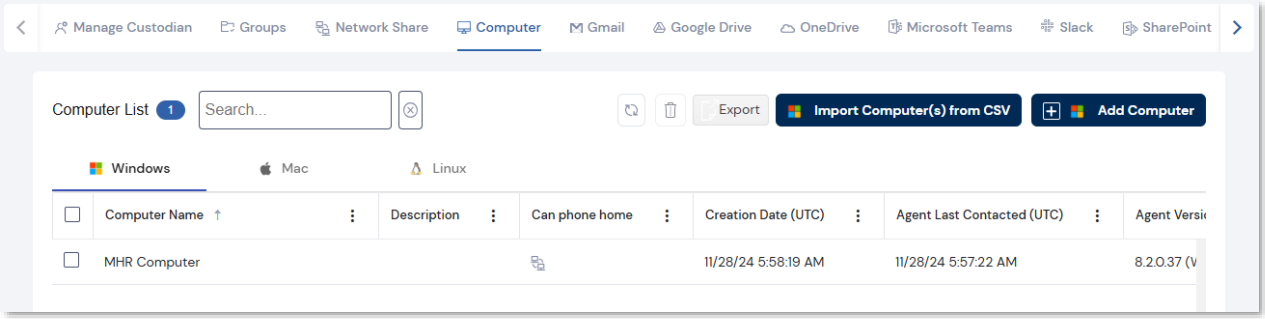
One of the primary sources of evidence used in a case originates on workstations (or nodes) managed by a person. You can add or remove computers from this page, edit a share path, or add and edit a computer's information and description.

Adding Computer data sources

Note: These steps are not applicable for Mac Agents, as they are automatically registered once they have been installed.

To add a computer data source:

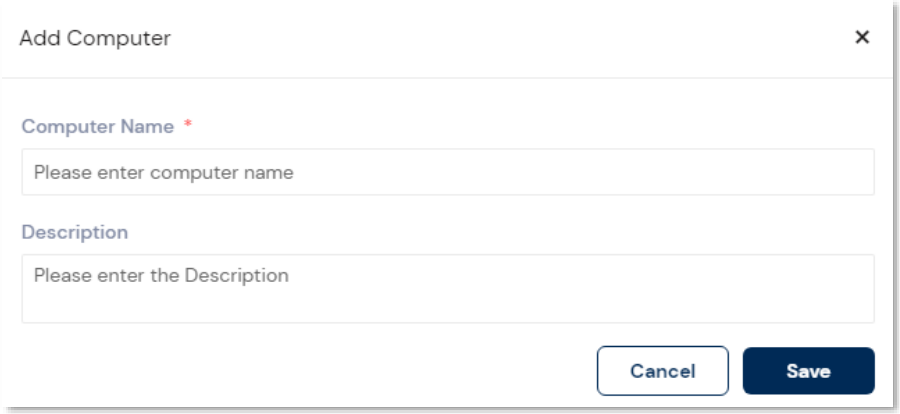
1. From the home page, click **Data Sources**.
2. Navigate to **Computer**.



3. Select the **Windows** or **Linux** section.

© Exterro, Inc. All rights reserved

4. Click **Add Computer**.
   - The **Add Computer** pop-up is displayed.



5. Provide a name for the computer in **Computer Name** field.
6. Provide a description for the computer in **Description** field.
7. Click **Save**.

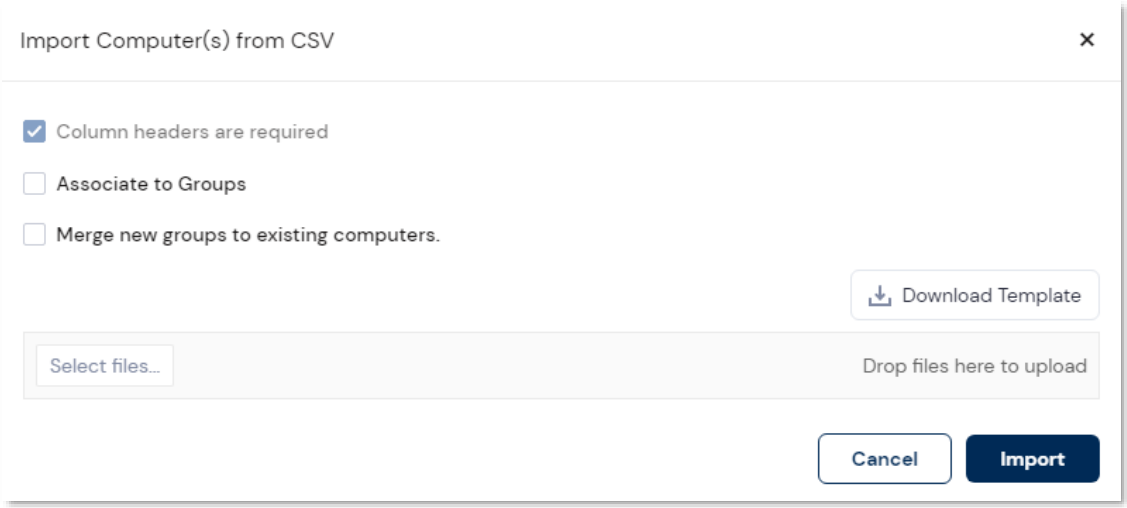
© Exterro, Inc. All rights reserved

Importing Computer data sources from CSV

Note: These steps are not applicable for Mac Agents, as they are automatically registered once they have been installed.

To import computer data sources from CSV:

1. From the home page, click **Data Sources**.
2. Navigate to **Computer**.
3. Select the **Windows** or **Linux** section.
4. Click **Import Computer(s) from CSV**.
   - The **Import Computer(s) from CSV** pop-up is displayed.



5. Click **Select files**.
6. Select the required file or drag and drop the file to be uploaded.
7. Enable the checkbox against **Associate to Groups** to associate groups to computers.
8. Enable the checkbox against **Merge new groups to existing computers** to associate new groups to computers that were previously added by CSV import.
9. Click **Import**.

Note: You can click on **Download Template** fill in the details of the network share and upload it for the application to read the network shares to be imported.

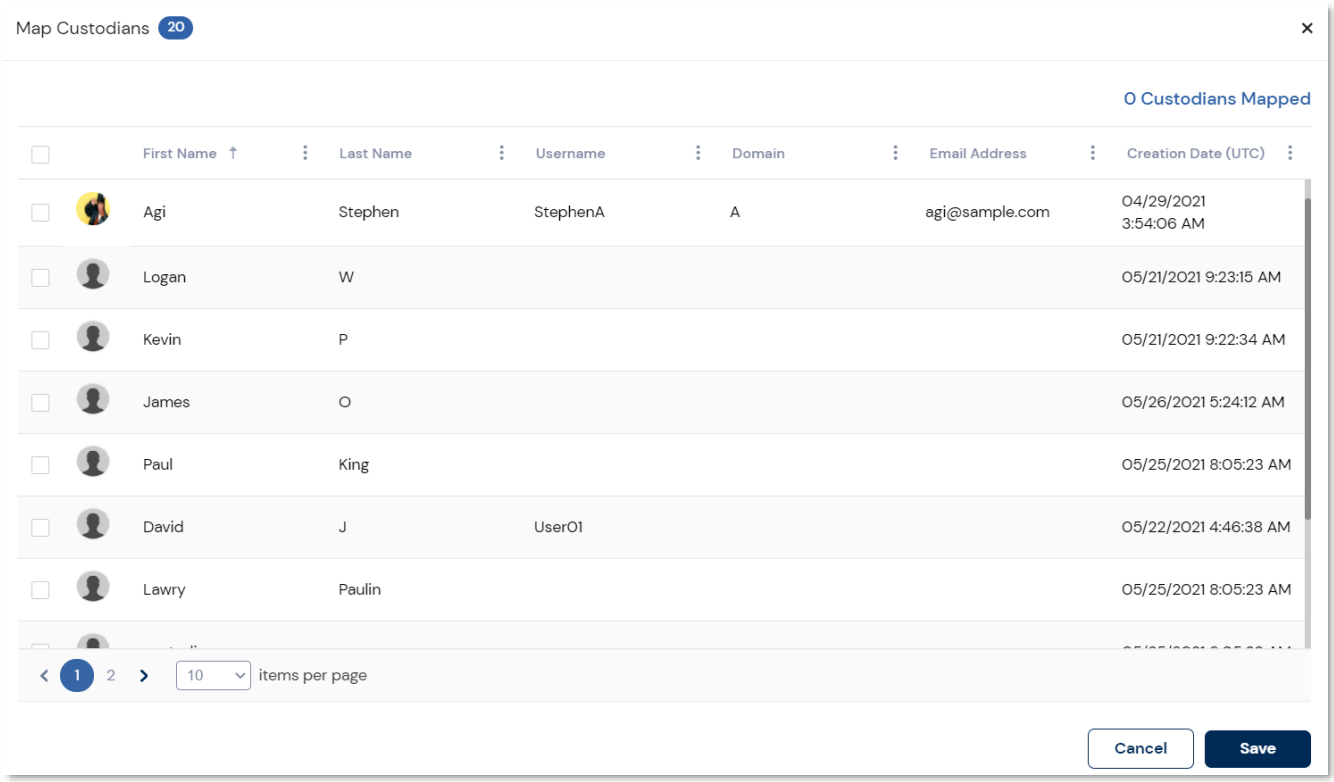
© Exterro, Inc. All rights reserved

Mapping Computer data sources to Custodians

Note: These steps are not applicable for Mac Agents, as they are automatically registered once they have been installed.

To map a computer data source to custodians:

1. From the home page, click **Data Sources**.
2. Navigate to **Computer**.
3. Select either **Windows** or **Linux** section.
4. Click **Map Custodian** against the data source to be mapped.
   - The **Map Custodians** pop-up is displayed.



5. Select the required custodians by enabling the checkbox against it.
6. Click **Save**.

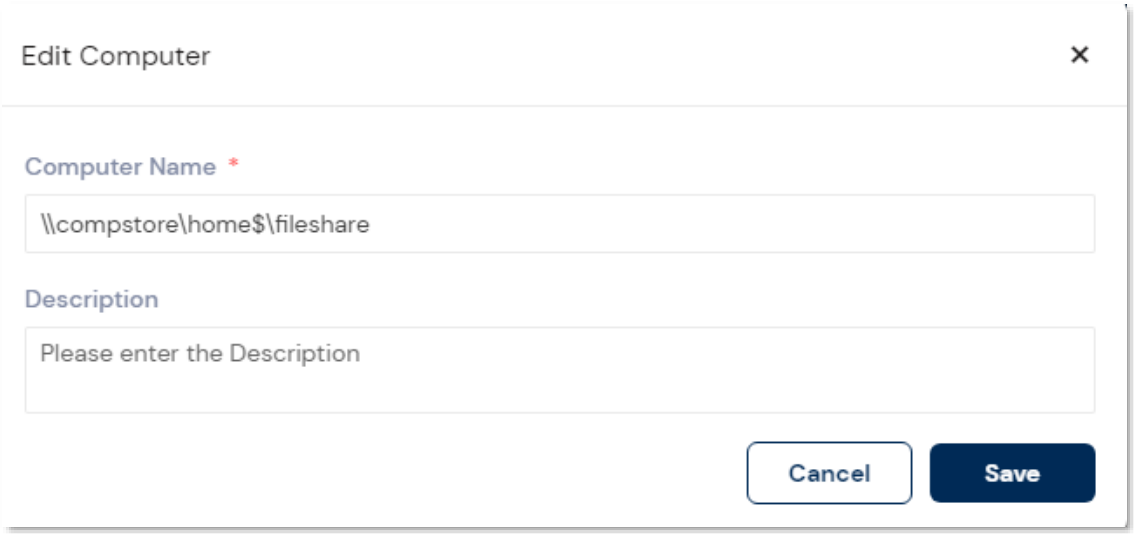
© Exterro, Inc. All rights reserved

Editing Computer data sources

Note: These steps are not applicable for Mac Agents, as they are automatically registered once they have been installed.

To edit a computer data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Computer**.
3. Select the **Windows** or **Linux** section.
4. Click **Edit** against the data source to be edited.
   - The **Edit Computer** pop-up is displayed.



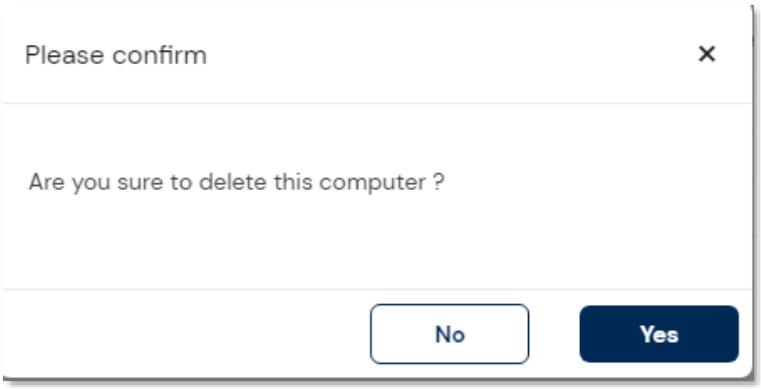
5. Make the necessary changes.
6. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting Computer data sources

To delete a computer data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Computer**.
3. Select the **Windows, Mac,** or **Linux** section.
4. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.



5. Click **Yes**.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.

© Exterro, Inc. All rights reserved

Creating Endpoint Reports

To create an endpoint report from data sources:

1. From the homepage, click **Data Sources**.
2. Click **Computer**.
3. Select the **Windows, Mac,** or **Linux** section.
4. Click **Export**.
5. Select any of the following report types:
   - **HTML**
   - **CSV**
   - **PDF**

The report will be created, listing the computers and their associated columns.

Tip: To create a report of specific endpoints, ensure computers have been filtered using the columns available. If this is not followed, a report will feature all computers listed in Data Sources.

© Exterro, Inc. All rights reserved

Gmail

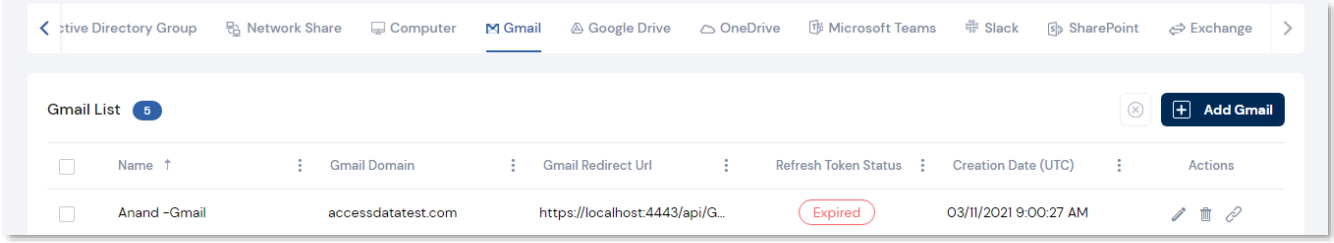
You can configure the application to collect data from Gmail at a domain (administrative) level. Administrators can collect from individual accounts without needing individual credentials. The service account must be used for collections.

Tip: If you have updated your FTK Central environment with an existing Data Source, ensure they are removed and reconfigured.

Adding Gmail data sources

To add a Gmail data source:

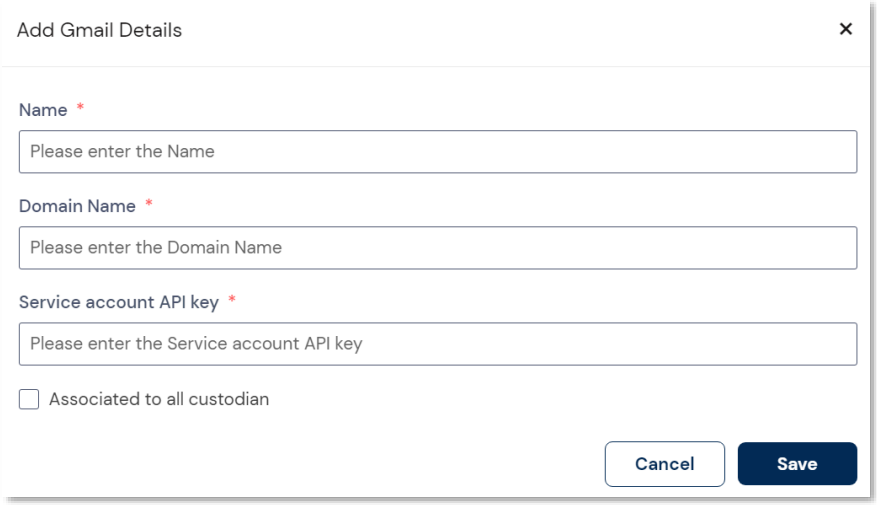
1. From the home page, click **Data Sources**.
2. Navigate to **Gmail**.



3. Click **Add Gmail**.

© Exterro, Inc. All rights reserved

- The **Add Gmail Details** pop-up is displayed.



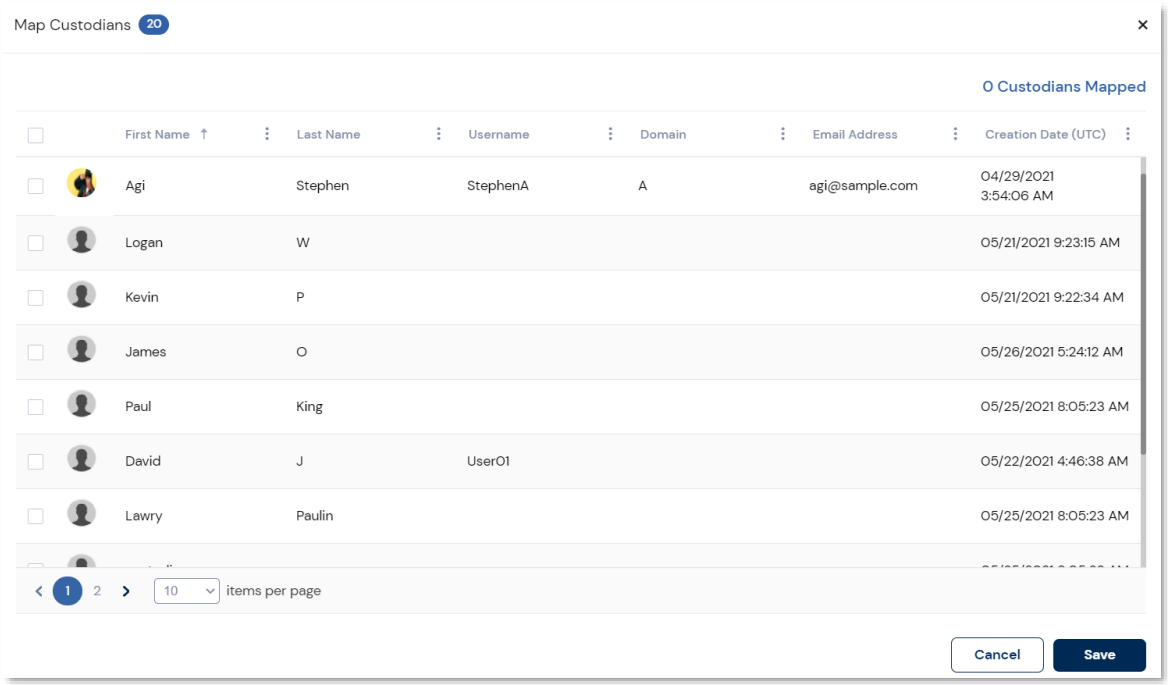
4. Provide a **Name** for the Gmail.
5. Enter the **Domain Name.**
6. Enter the **Service account API key**.
7. Select the **Associated to all custodians** to associate all the custodians to the server.
8. Click **Save**.

© Exterro, Inc. All rights reserved

Mapping Gmail data sources to Custodians

To map a Gmail data source to custodians:

1. From the home page, click **Data Sources**.
2. Navigate to **Gmail**.
3. Click **Map Custodian** against the data source to be mapped.
   - The **Map Custodians** pop-up is displayed.



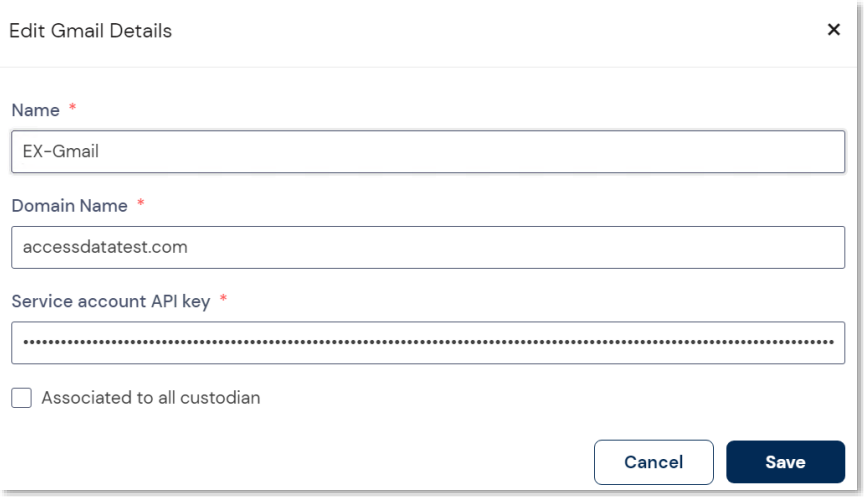
4. Select the required custodians by enabling the checkbox against it.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Editing Gmail data sources

To edit a Gmail data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Gmail**.
3. Click **Edit** against the data source to be edited.
   - The **Edit Gmail Details** pop-up is displayed.



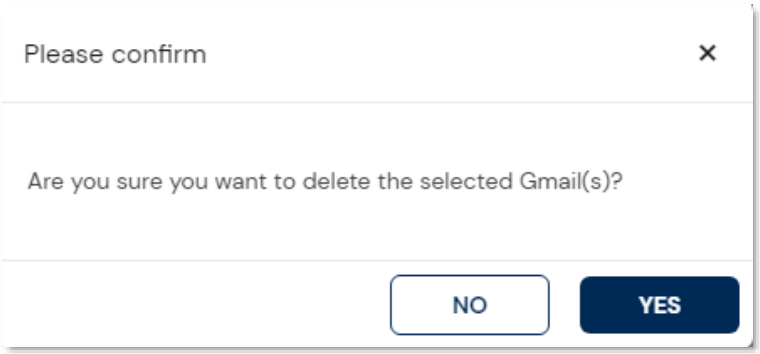
4. Make the necessary changes.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting Gmail data sources

To delete a Gmail data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Gmail**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.

© Exterro, Inc. All rights reserved

Google Drive

You can configure the application to collect files from a Google Drive. Once you have configured the application to collect from your Google Drive, you can choose to collect from this source with a collection job. The service account must be used for collections.

Tip: If you have updated your FTK Central environment with an existing Data Source, ensure they are removed and reconfigured.

Notes:

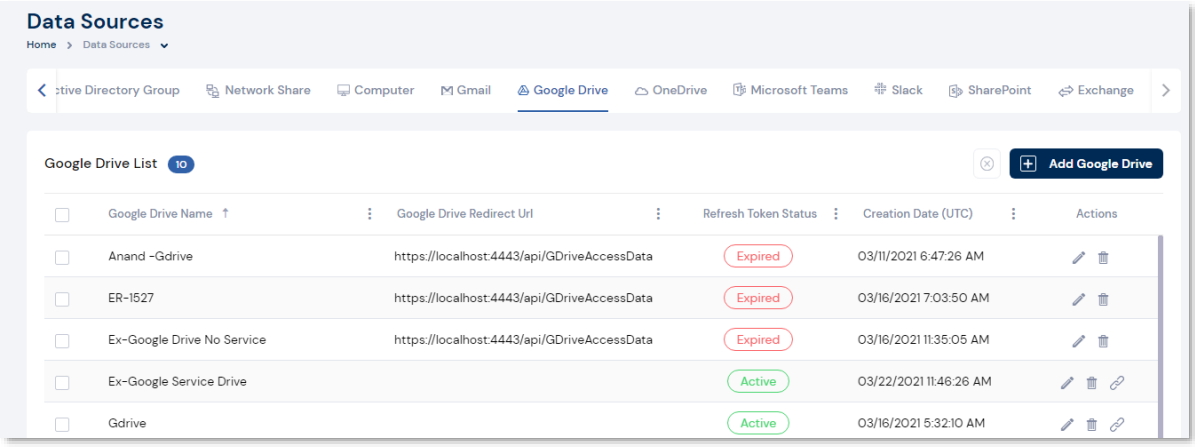
- When the user runs a Report only collection for Google Drive, native Google files (Docs, Spreadsheets, Slides, and Forms) do not count against a user's storage quota and show as zero bytes.
- Google does not expose the size of the native files from Google Drive and hence only the file size is downloaded when file is downloaded (File Scan Collection/Non report only scenario).

© Exterro, Inc. All rights reserved

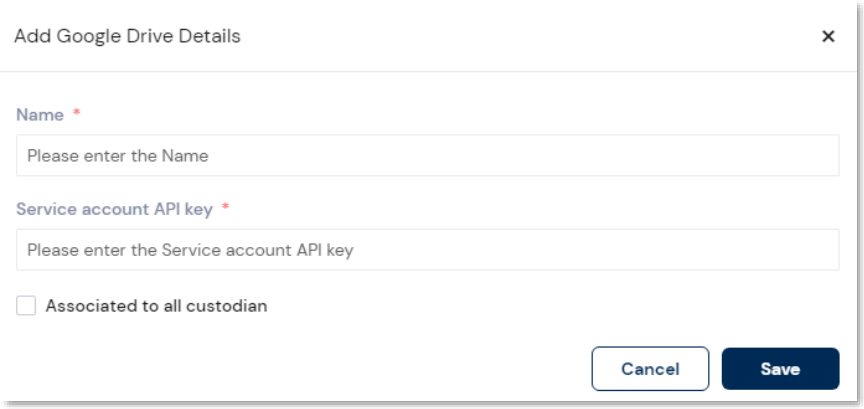
Adding Google Drive data sources

To add a Google Drive data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Google Drive**.



3. Click **Add Google Drive**.
   - The **Add Google Drive Details** pop-up is displayed.



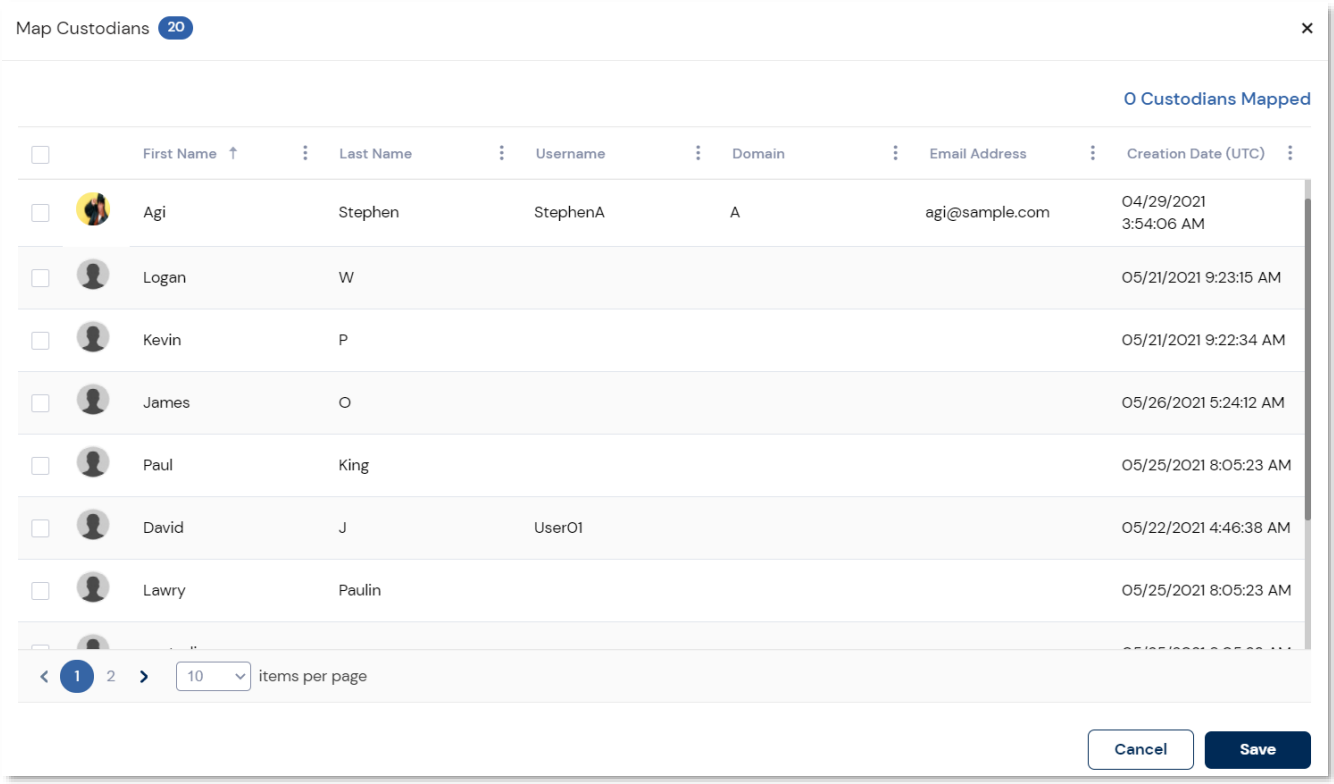
4. Provide a **Name** for the Google Drive.
5. Enter the **Service account API key**.
6. Select the **Associated to all custodians** to associate all the custodians to the server.
7. Click **Save**.

© Exterro, Inc. All rights reserved

Mapping Google Drive data sources to Custodians

To map a Google Drive data source to custodians:

1. From the home page, click **Data Sources**.
2. Navigate to **Google Drive**.
3. Click **Map Custodian** against the data source to be mapped.
   - The **Map Custodians** pop-up is displayed.



4. Select the required custodians by enabling the checkbox against it.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Editing Google Drive data sources

To edit a Google Drive data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Google Drive**.
3. Click **Edit** against the data source to be edited.
   - The **Edit Google Drive Details** pop-up is displayed.

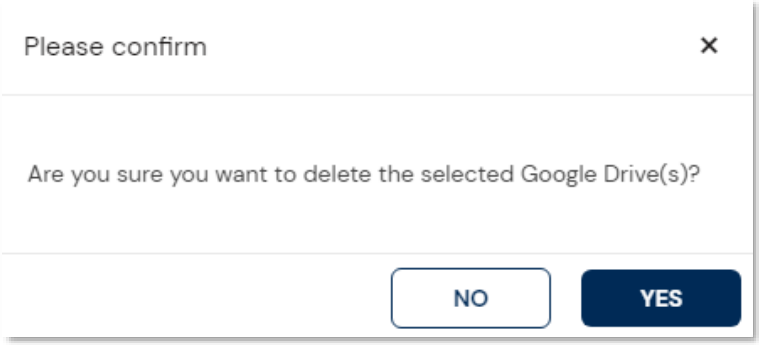
4. Make the necessary changes.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting Google Drive data sources

To delete a Google Drive data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Google Drive**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.

© Exterro, Inc. All rights reserved

OneDrive

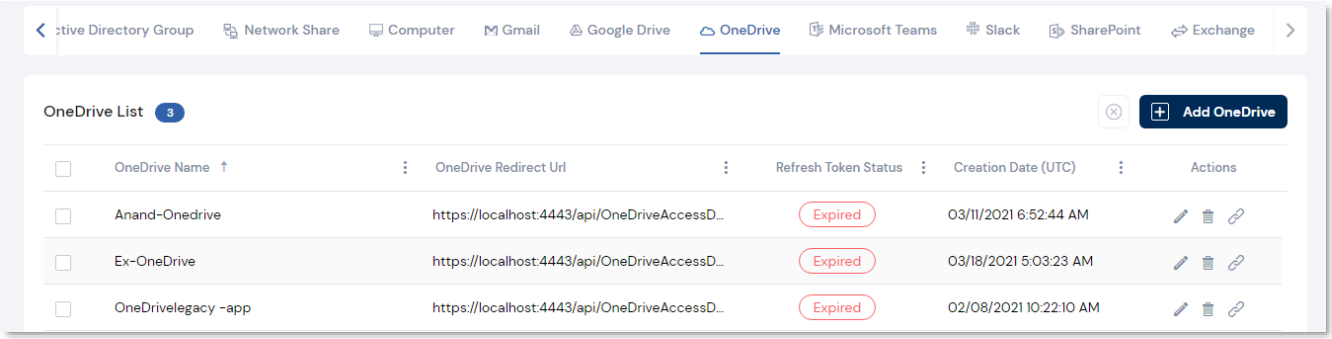
You can configure the application to collect all files from a OneDrive. Once you have configured the application to collect from your OneDrive, you can choose to collect from this source with a collection job. If attempting to collect from GCC environments please refer to the Office 365 Credentials section.

Tip: If you have updated your FTK Central environment with an existing Data Source, ensure they are removed and reconfigured.

Adding OneDrive data sources

To add a OneDrive data source:

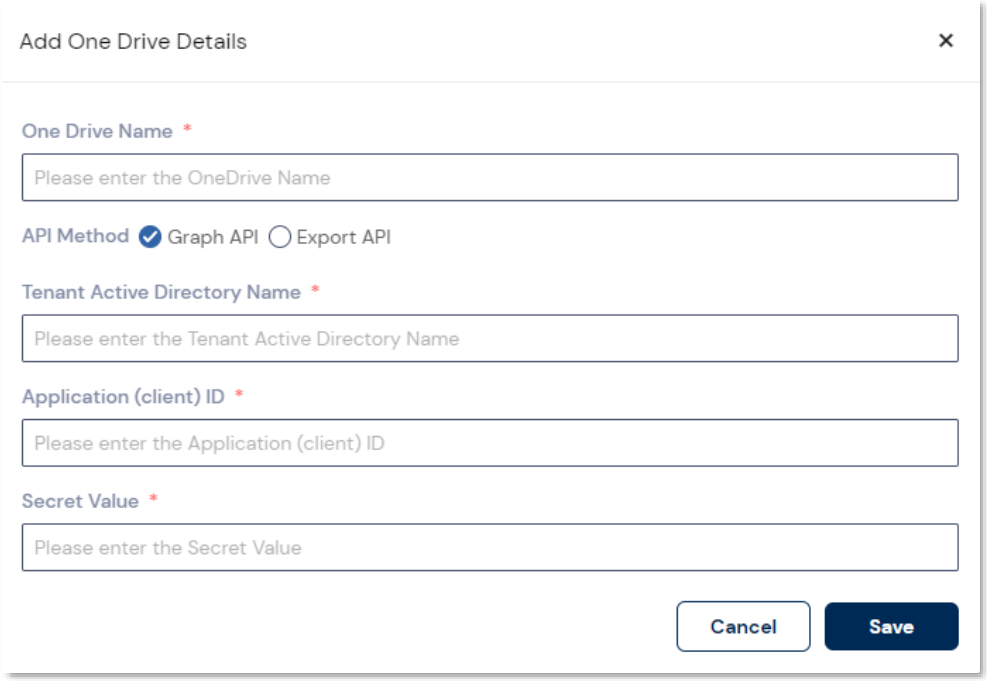
1. From the home page, click **Data Sources**.
2. Navigate to **OneDrive**.



3. Click **Add OneDrive**.

© Exterro, Inc. All rights reserved

- The **Add OneDrive Details** pop-up is displayed.



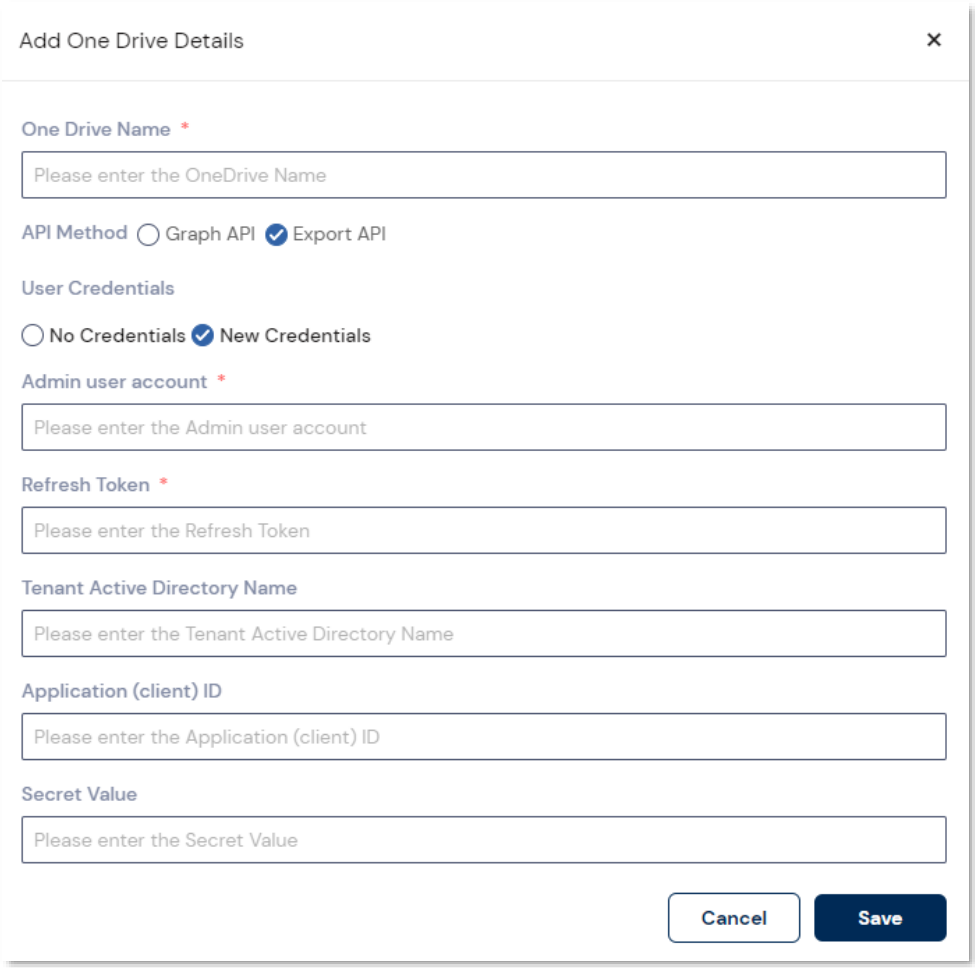
4. Enter a **OneDrive Name**.
5. Choose the API Method.
   a) Graph API:
      i. Enter the **Tenant Active Directory Name**.
      ii. Enter the **Application (client ID)**.
      iii. Enter the **Secret Value**.

© Exterro, Inc. All rights reserved

b) Export API:

i. Choose the **User Credentials**.

- No Credentials – This will fetch the credentials configured in the System Management > Manage Credentials page.
- New Credentials – Select this to configure users with new credentials.



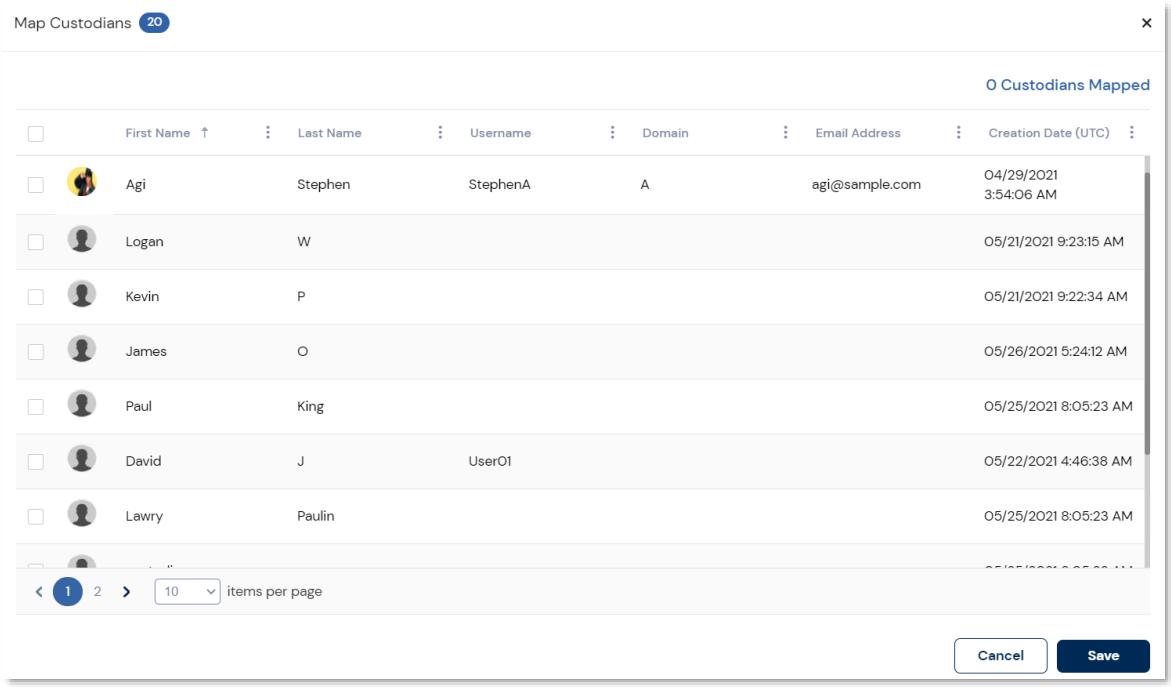
6. Click **Save**.

© Exterro, Inc. All rights reserved

Mapping OneDrive data sources to Custodians

To map a OneDrive data source to custodians:

1. From the home page, click **Data Sources**.
2. Navigate to **OneDrive**.
3. Click **Map Custodian** against the data source to be mapped.
   - The **Map Custodians** pop-up is displayed.



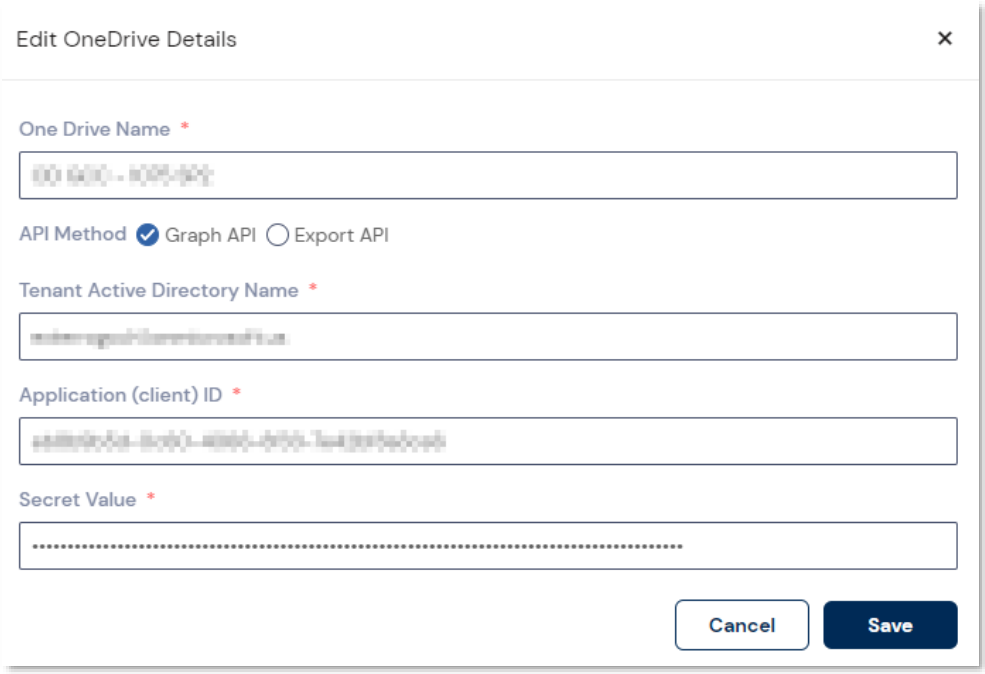
4. Select the required custodians by enabling the checkbox against it.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Editing OneDrive data sources

To edit a OneDrive data source:

1. From the home page, click **Data Sources**.
2. Navigate to **OneDrive**.
3. Click **Edit** against the data source to be edited.
   - The **Edit OneDrive Details** pop-up is displayed.



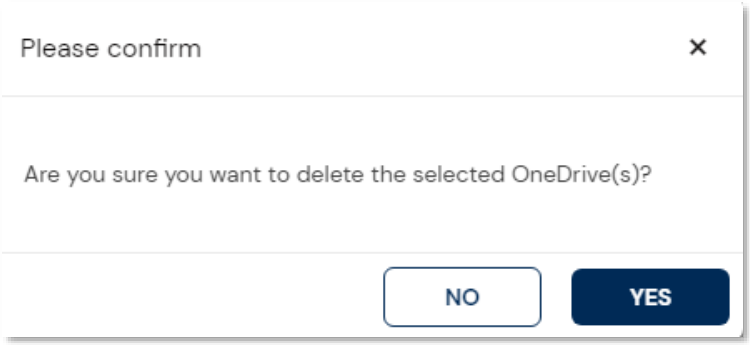
4. Make the necessary changes.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting OneDrive data sources

To delete a OneDrive data source:

1. From the home page, click **Data Sources**.
2. Navigate to **OneDrive**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.

© Exterro, Inc. All rights reserved

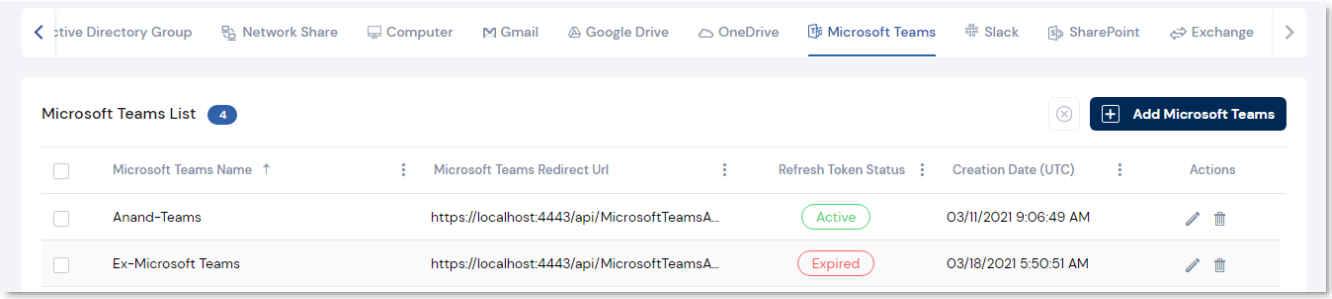
Microsoft Teams

You can configure the application to collect files Microsoft Teams business user accounts. You can add, edit, or delete multiple accounts from this page. If attempting to collect from GCC environments please refer to the Office 365 Credentials section.

Adding Microsoft Teams data sources

To add a Microsoft Teams data source:

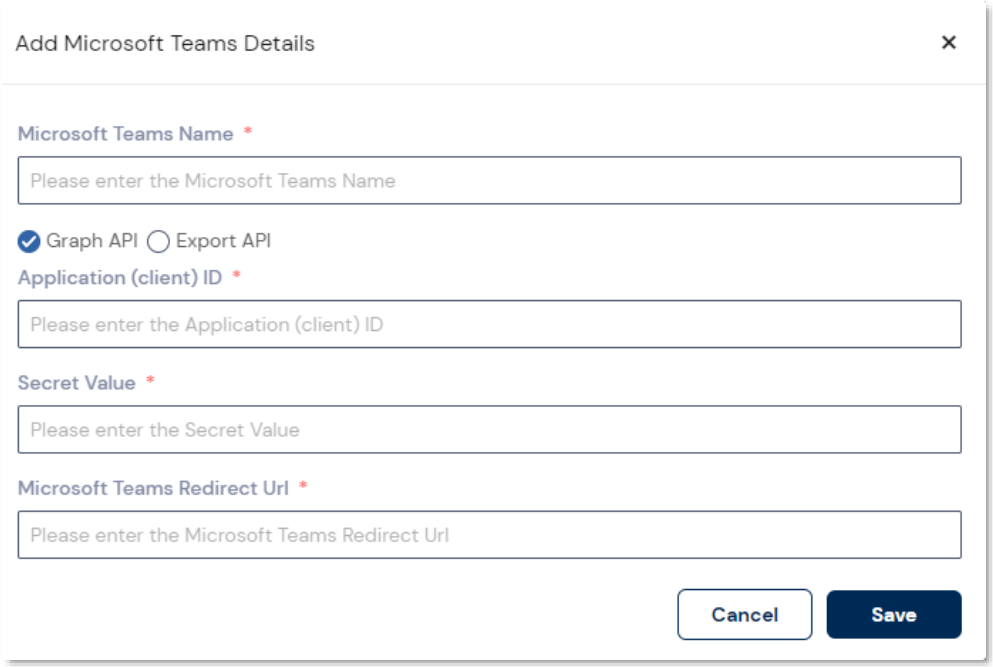
1. From the home page, click **Data Sources**.
2. Navigate to **Microsoft Teams**.



3. Click **Add Microsoft Teams**.

© Exterro, Inc. All rights reserved

- The **Add Microsoft Teams Details** pop-up is displayed.



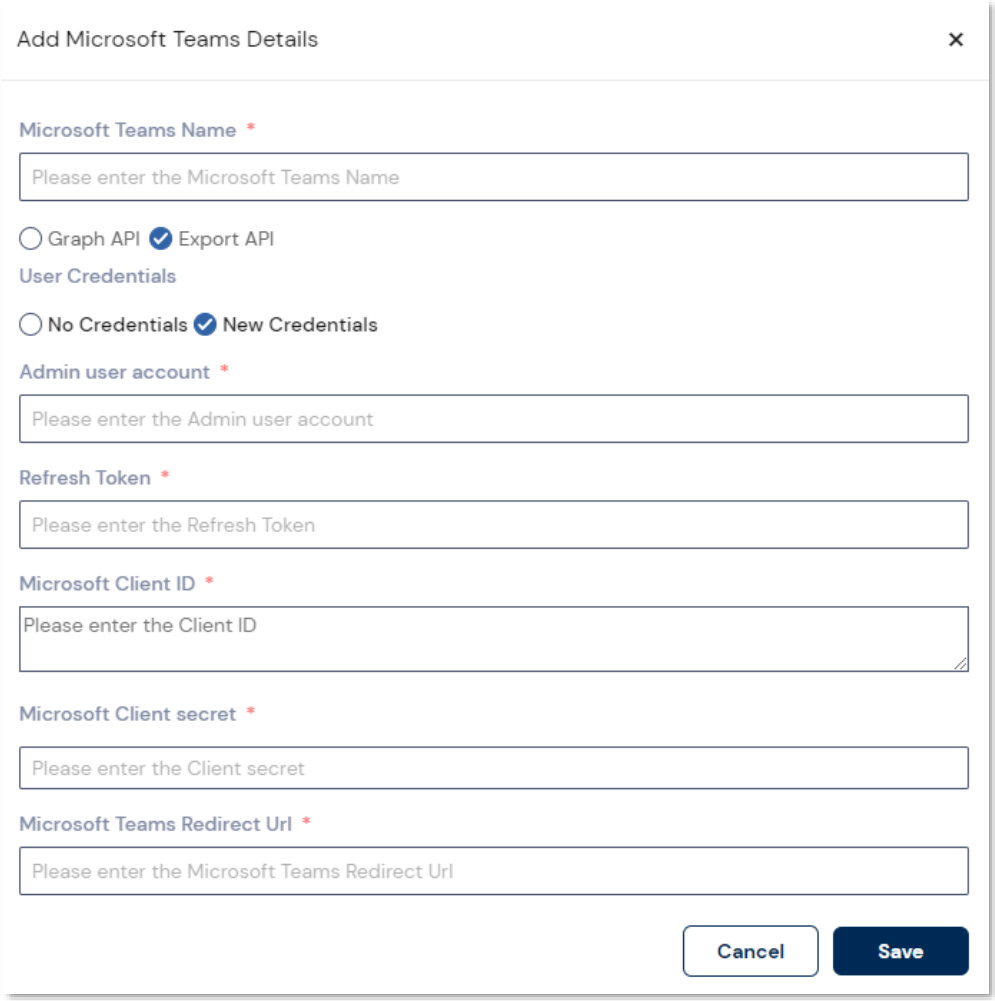
4. Enter a **Microsoft Teams Name**.
5. Select the API Method.
   a) Graph API:
      i. Enter the **Application (client ID)** of the Microsoft Teams.
      ii. Enter the **Secret Value** of the Microsoft Teams.
      iii. Enter the **Redirect URL** of the Microsoft Teams.

© Exterro, Inc. All rights reserved

b) Export API:

i. Choose the **User Credentials**.

- No Credentials – This will fetch the credentials configured in the System Management > Manage Credentials page.
- New Credentials – Select this to configure users with new credentials.



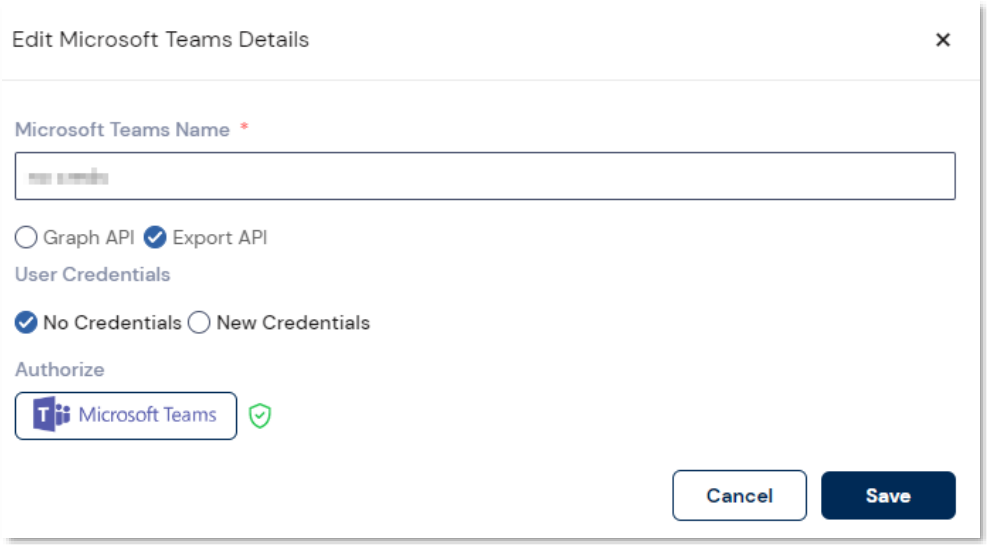
6. Click **Save**.

© Exterro, Inc. All rights reserved

Editing Microsoft Teams data sources

To edit a Microsoft Teams data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Microsoft Teams**.
3. Click **Edit** against the data source to be edited.
   - The **Edit Microsoft Teams Details** pop-up is displayed.



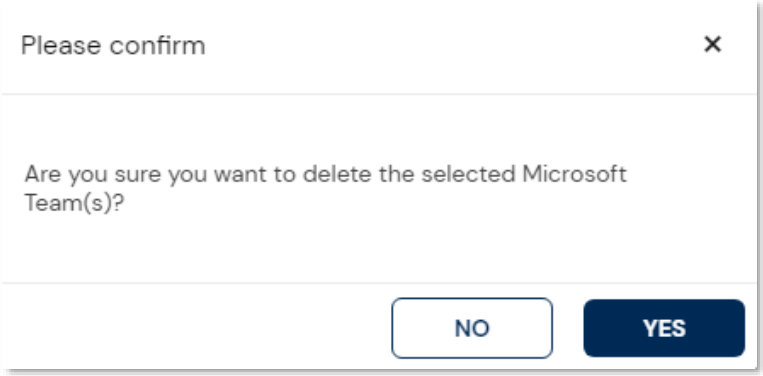
4. Make the necessary changes.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting Microsoft Teams data sources

To delete a Microsoft Teams data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Microsoft Teams**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.

© Exterro, Inc. All rights reserved

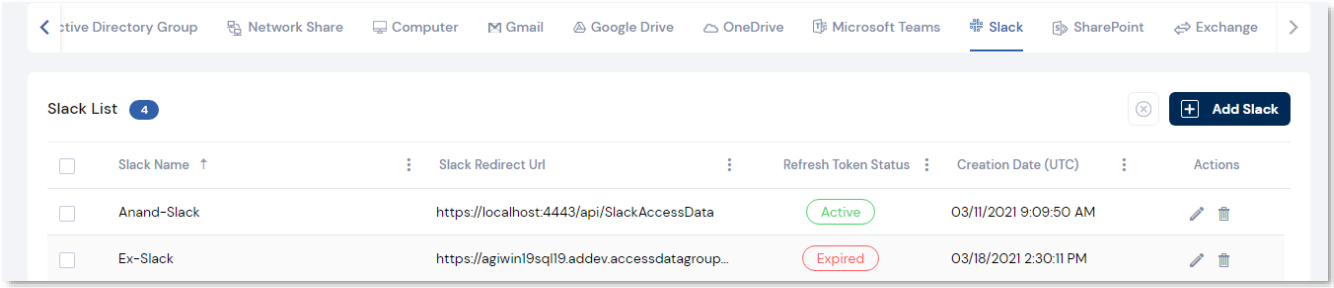
Slack

You can configure the application to collect files from Slack business user accounts. You can add, edit, or delete multiple accounts from this page.

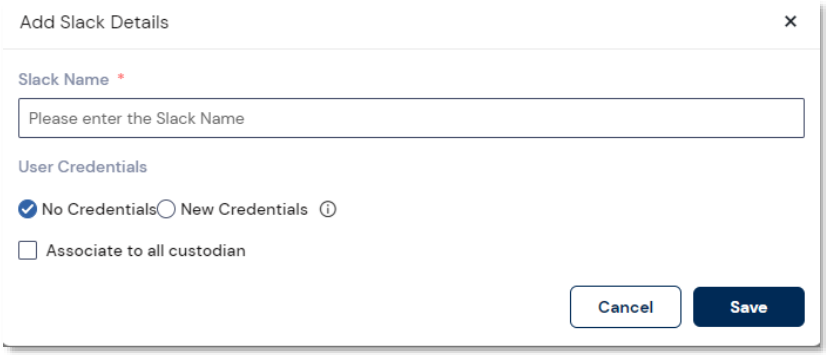
Adding Slack data sources

To add a Slack data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Slack**.



3. Click **Add Slack**.
   - The **Add Slack Details** pop-up is displayed.

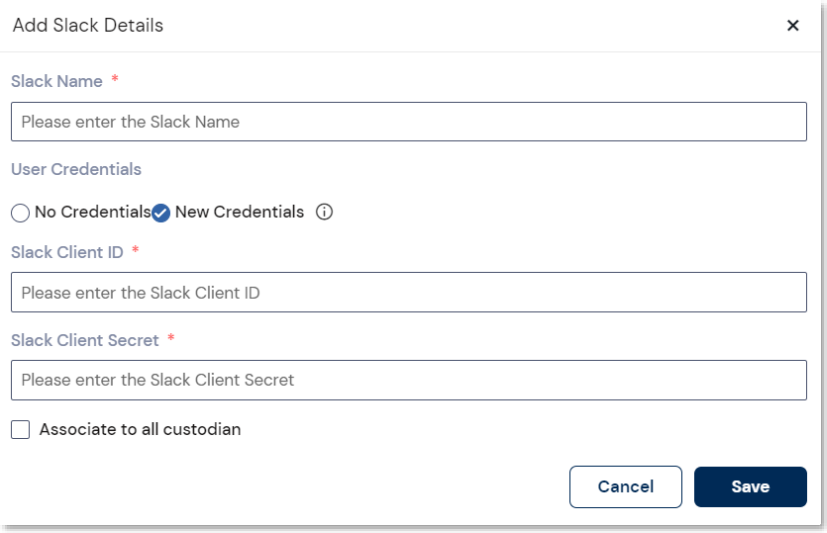


4. Provide the **Slack Name**.
5. Select one of the following options for the **User Credentials** field:
   - **No Credentials:** The settings configured in **System Management** > **Configuration** > **Manage Credentials** > **Slack Credentials** will be used.

© Exterro, Inc. All rights reserved

- **New Credentials:** Provide the following information:
  - Slack Client ID
  - Slack Client Secret

Note: You are recommended to contact the Exterro Team to get the values of the Slack Client ID and Slack Client Secret.



Note: Use **New Credentials** only if your organization has enabled the **Block Files Download** option in Slack.

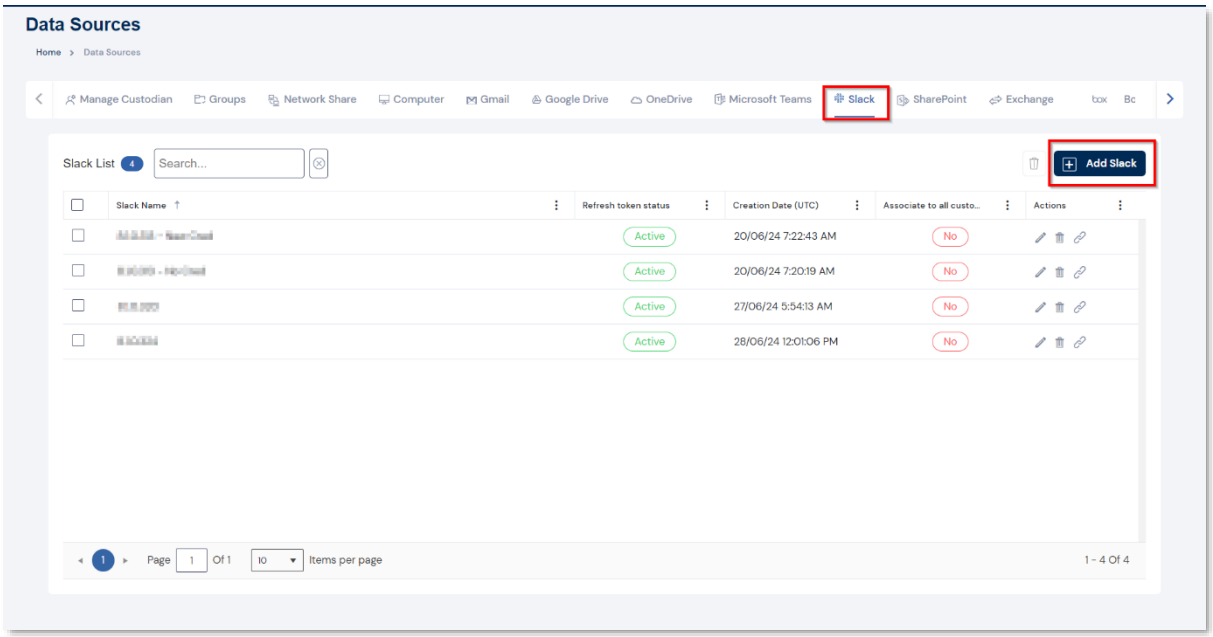
6. Select **Associate to all custodian** checkbox to associate the created Slack data source to all the custodians.

© Exterro, Inc. All rights reserved

Authorizing Slack data sources

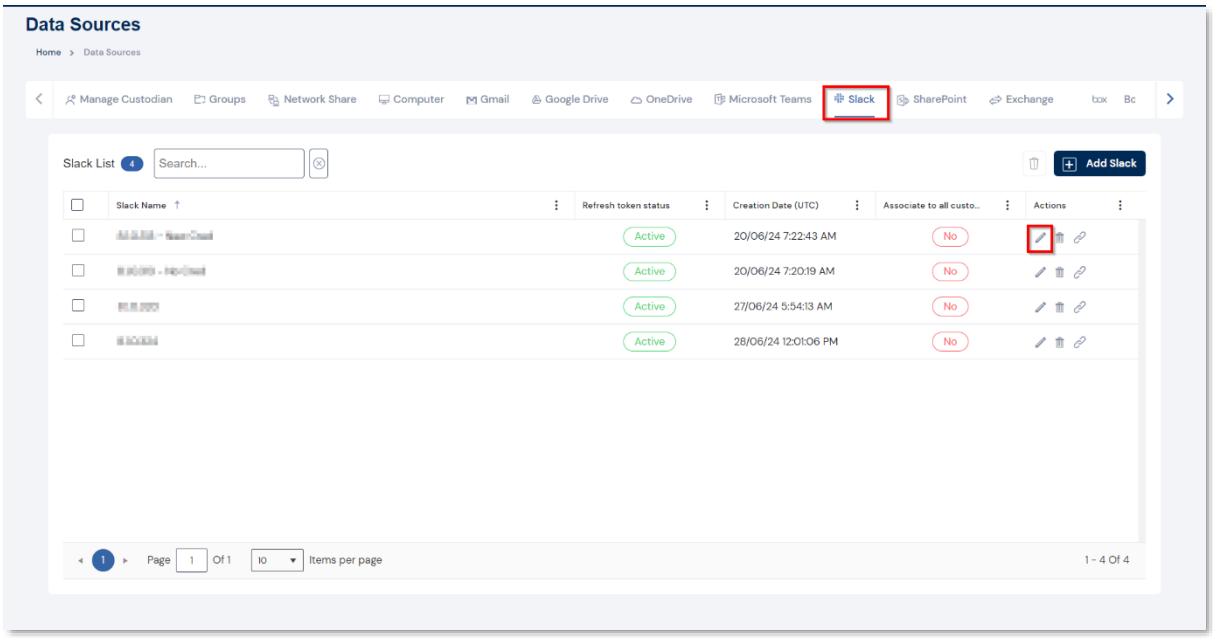
To authorize the Slack data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Slack**.
3. Click on **Add Slack**.

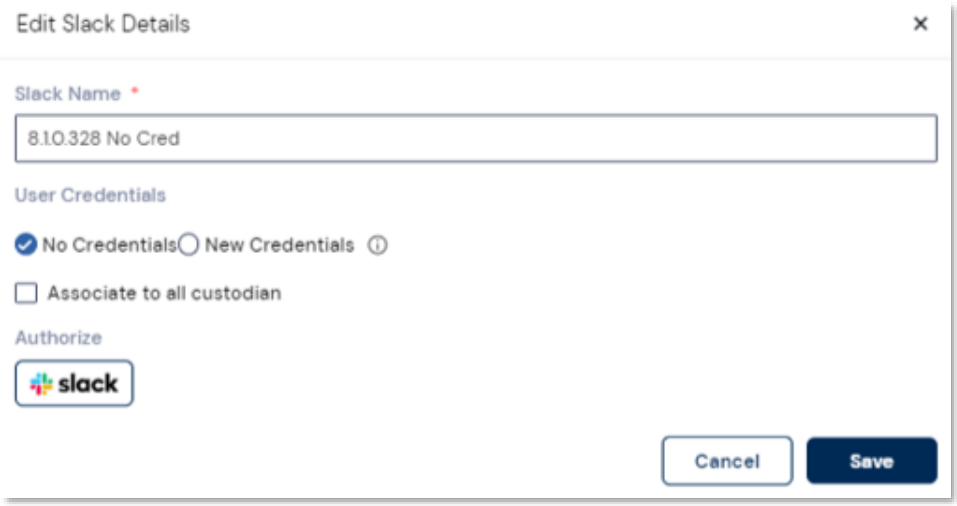


© Exterro, Inc. All rights reserved

4. Click **Edit** icon against the existing Slack data source.



- The **Edit Slack Details** pop-up is displayed.



5. Click on the **Slack** icon to initiate the authorization process.
6. Provide the **Organization Domain** and click **Continue**.

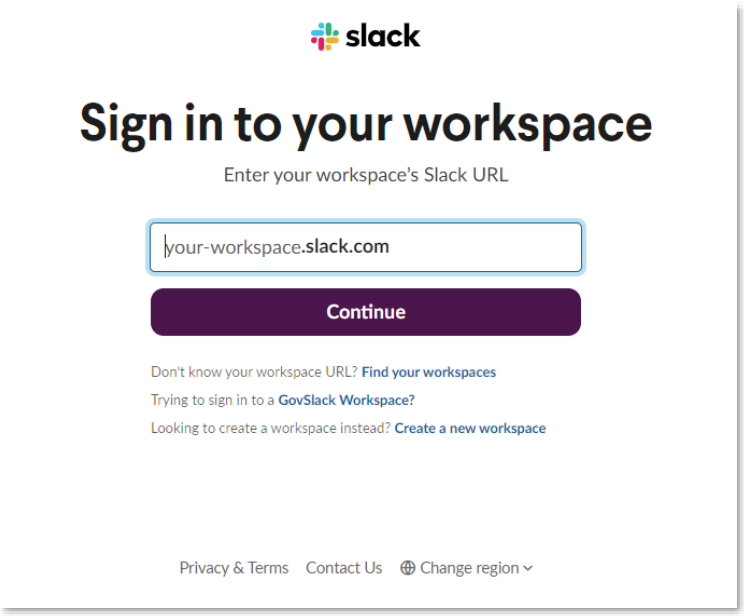
© Exterro, Inc. All rights reserved

Note: For Enterprise Licenses, the **Organization Domain** is required because the Slack App is an administrative application that cannot be installed for individual workspaces within an organization.

7. Login with the Organization Owner account credentials.

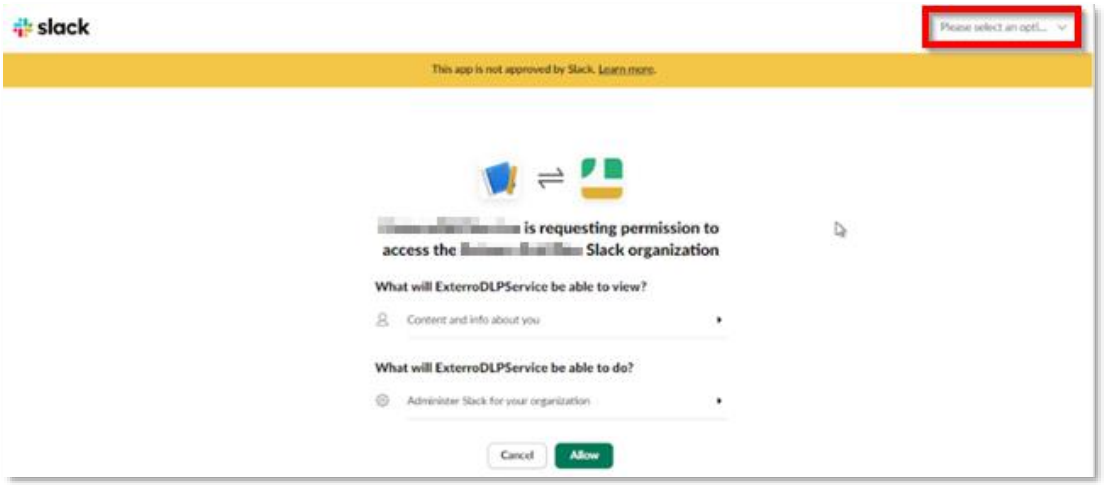
Note: To successfully configure the Slack app, the service account must have **Organization Owner** permissions due to the elevated scopes required, including **discovery:read**.

It is important to note that revoking the **org owner** permission for the service account will invalidate the installed Slack app.



© Exterro, Inc. All rights reserved

8. Enter your organization's Slack workspace name. You can select the workspace name from the drop-down menu located in the top right corner of the Slack authorization screen.



9. Once the Workspace is selected, click on **Allow**.

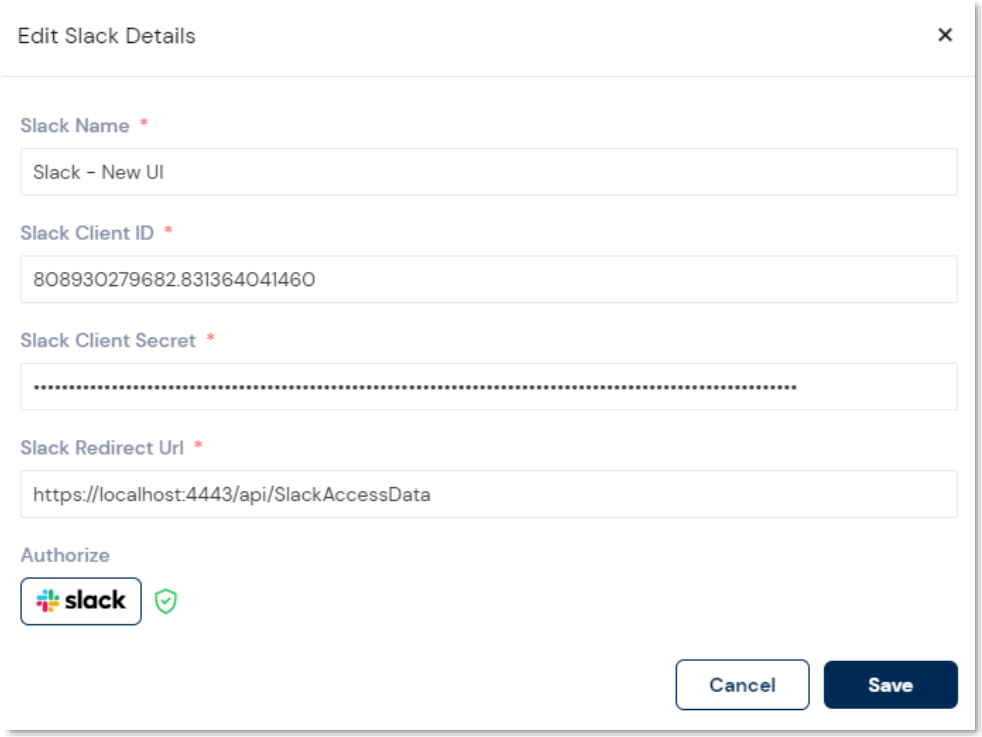
Note: Upon clicking **Allow**, access permissions for the Slack data source are granted, enabling integration with the selected workspace.

© Exterro, Inc. All rights reserved

Editing Slack data sources

To edit a Slack data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Slack**.
3. Click **Edit** against the data source to be edited.
   - The **Edit Slack Details** pop-up is displayed.



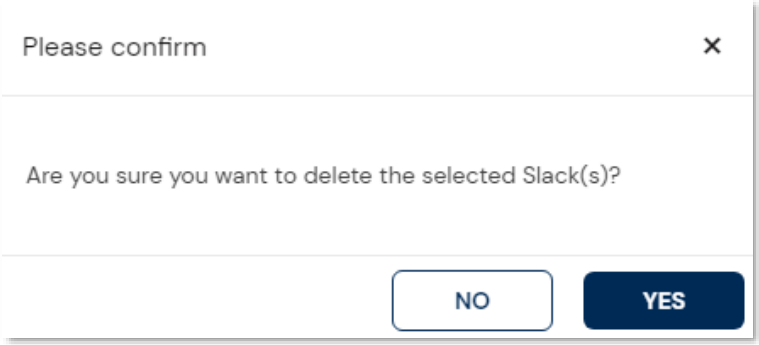
4. Make the necessary changes.
5. Click **Slack** and authorize the account and to establish a successful connection.
6. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting Slack data sources

To delete a Slack data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Slack**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.

© Exterro, Inc. All rights reserved

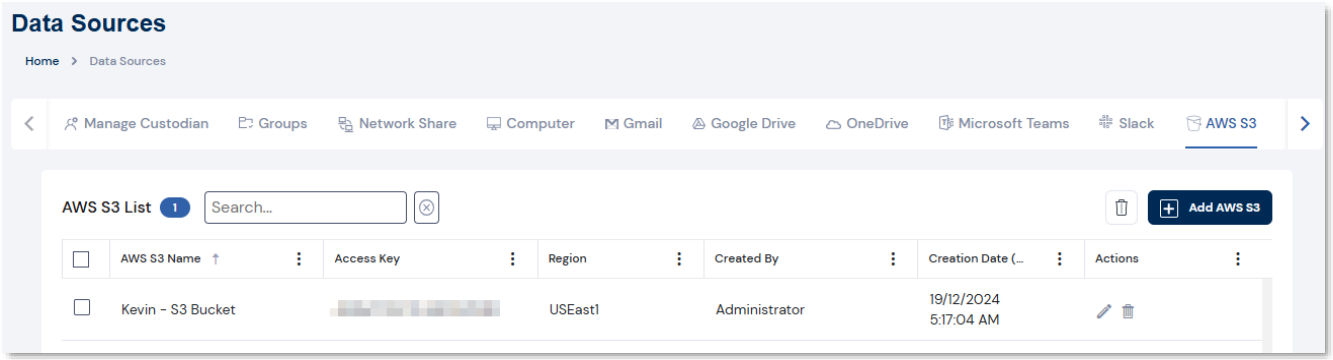
AWS S3

You can configure the application to collect files from the Amazon Web Services (AWS) S3 buckets. You can add, edit, or delete multiple accounts from this page.

Adding AWS S3 data sources

To add an AWS S3 data source:

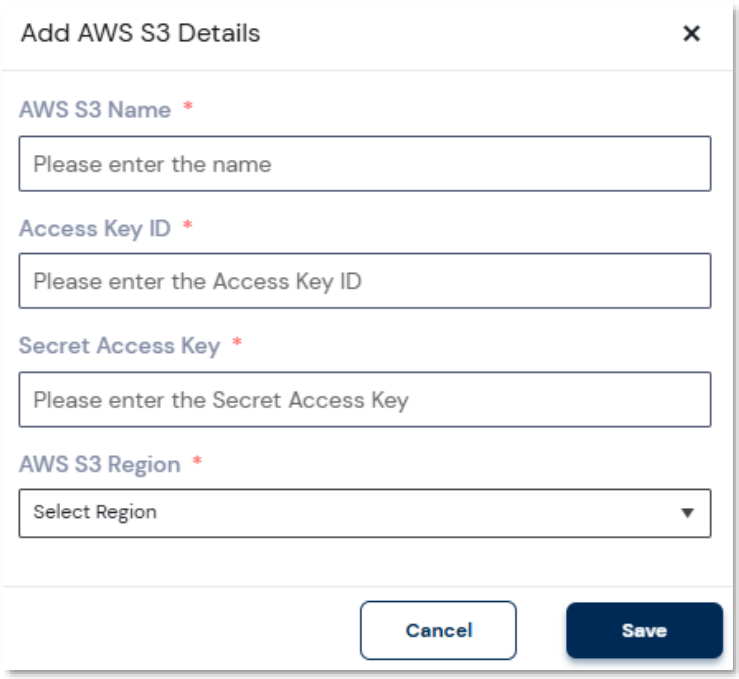
1. From the home page, click **Data Sources**.
2. Navigate to **AWS S3**.



3. Click **Add AWS S3**.

© Exterro, Inc. All rights reserved

- The **Add AWS S3 Details** pop-up is displayed.



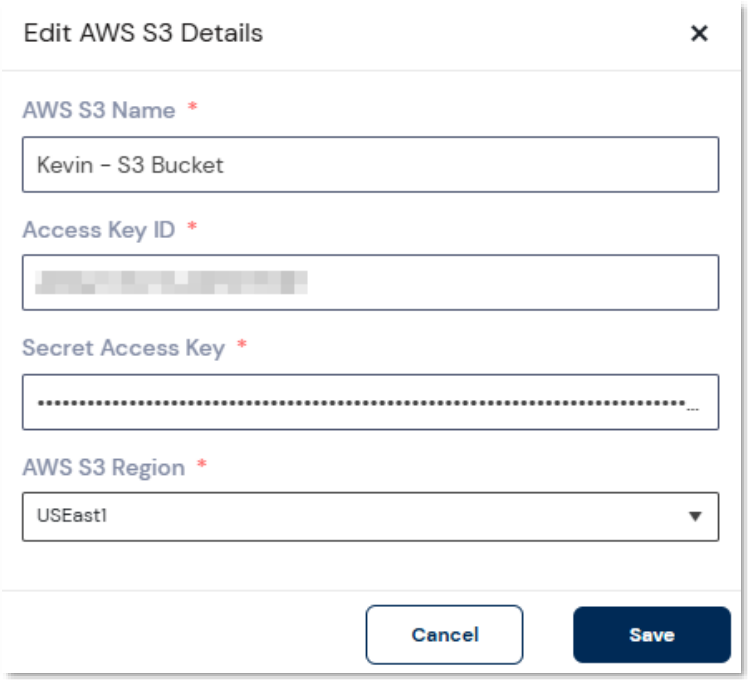
4. Provide the **AWS S3 Name**.
5. Provide the **Access Key ID**.
6. Provide the **Secret Access Key**.
7. Select the **AWS S3 Region**.
8. Click **Save**.

© Exterro, Inc. All rights reserved

Editing AWS S3 data sources

To edit an AWS S3 data source:

1. From the home page, click **Data Sources**.
2. Navigate to **AWS S3**.
3. Click **Edit** against the data source to be edited.
   - The **Edit AWS S3 Details** pop-up is displayed.



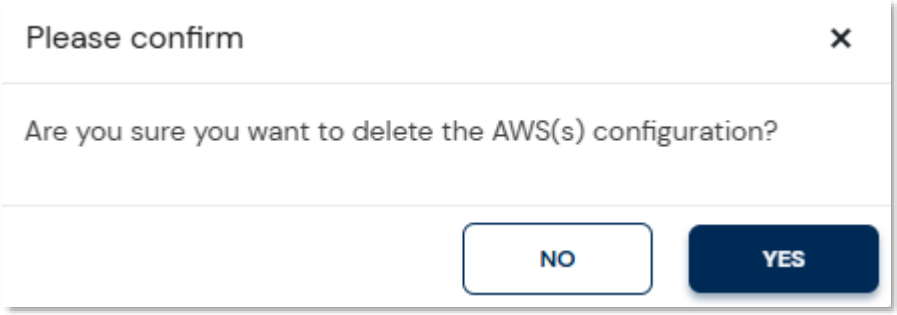
4. Make the necessary changes.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting AWS S3 data sources

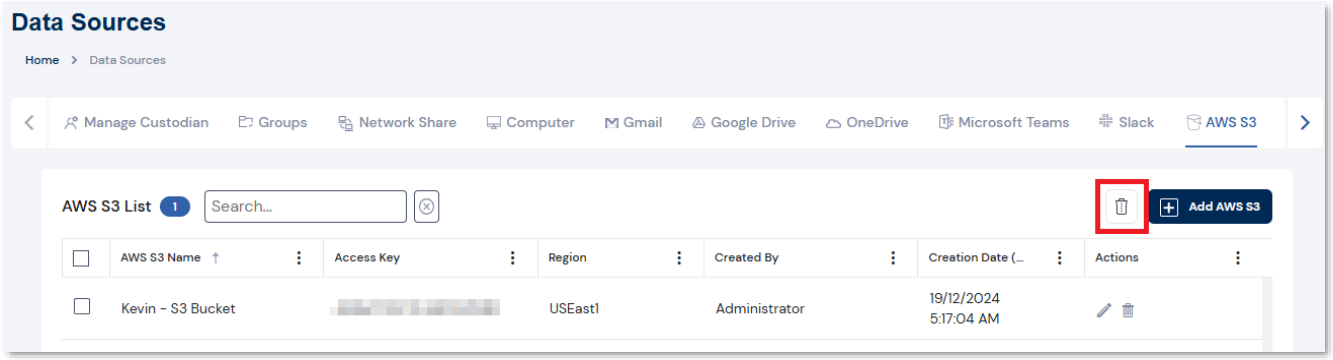
To delete an AWS S3 source:

1. From the home page, click **Data Sources**.
2. Navigate to **AWS S3**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.



© Exterro, Inc. All rights reserved

SharePoint

You can configure the application to collect from document libraries, wikis, blogs, calendars, contacts, announcements, surveys, and discussion boards on team and individual sites of SharePoint. The following are the versions supported:

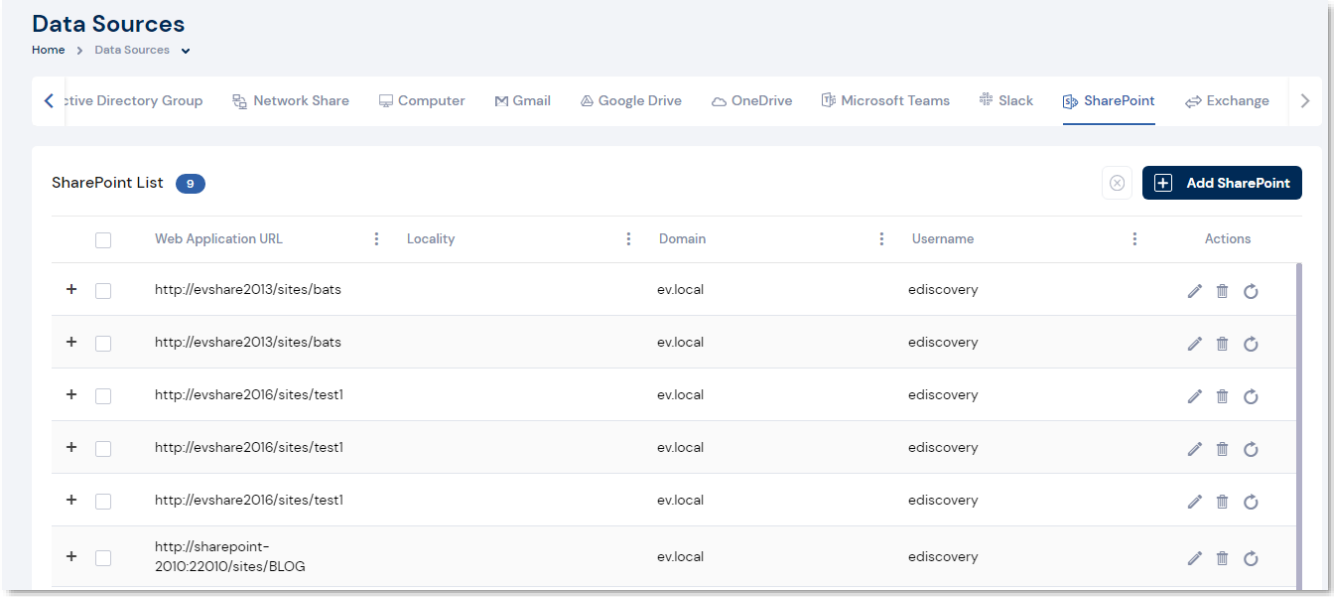
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013
- Microsoft SharePoint 2016
- Office 365
- OneDrive for Business (Collection of personal OneDrive accounts is not supported.)

If attempting to collect from GCC environments please refer to the Office 365 Credentials section.

Adding SharePoint data sources

To add a SharePoint data source:

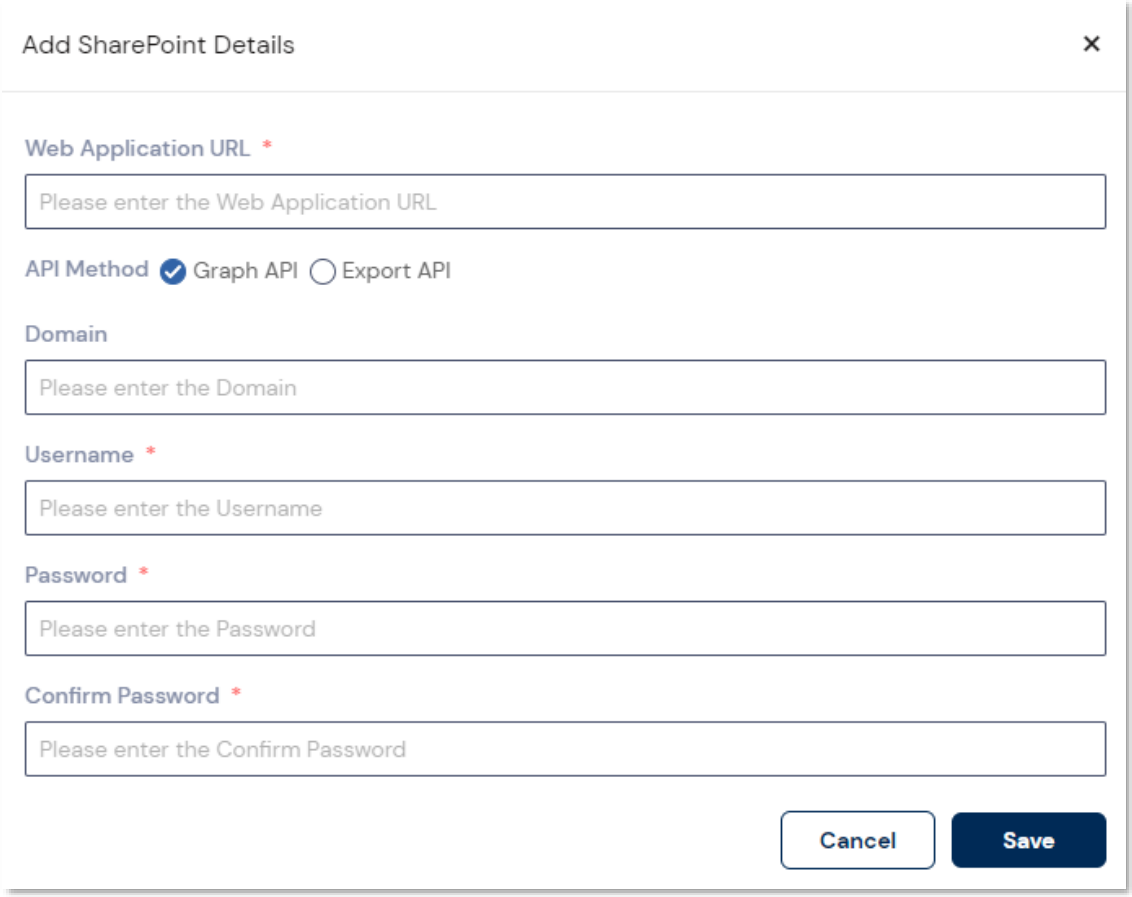
1. From the home page, click **Data Sources**.
2. Navigate to **SharePoint**.



3. Click **Add SharePoint**.

© Exterro, Inc. All rights reserved

- The **Add SharePoint Details** pop-up is displayed.



Note: You must configure the 'Default Case Path' in the Case Defaults section to display the SharePoint Subsite.

© Exterro, Inc. All rights reserved

4. Enter the **Web Application URL**.
   - The value of this field is typically be formatted as the following: http://[Address]:[Port]

     where [Address] is the host name or IP address of the system hosting the SharePoint Web Application. You can optionally use the [Port] address if you are connecting to a specific SharePoint web application. If you provide a URL that does not specify the port, port 80 is used.

     If you specify a root path, such as http://server_name/, when you run the Collection, you can select SharePoint site URLs that may exist within sub sites off of the root path.

     For example, you could include URLs of any blogs, discussion boards, document libraries, or wikis within the specified root path.

     If you specify a SharePoint path to a particular organization's department, you can include the blogs, discussion boards, document libraries, or wikis just within that department site. For example, the path may look like http://server_name/sites/marketing
5. Choose the **API Method**.
   c) Graph API:

   i. Enter the **Domain**.

   - (Optional) If the user account entered in the Username field is a domain user account, the domain must be specified; otherwise leave this field blank.

   ii. Enter the **Username**.

   - Lets you specify the username of an account that is granted Full Read access to SharePoint.

   iii. Enter the **Password**.

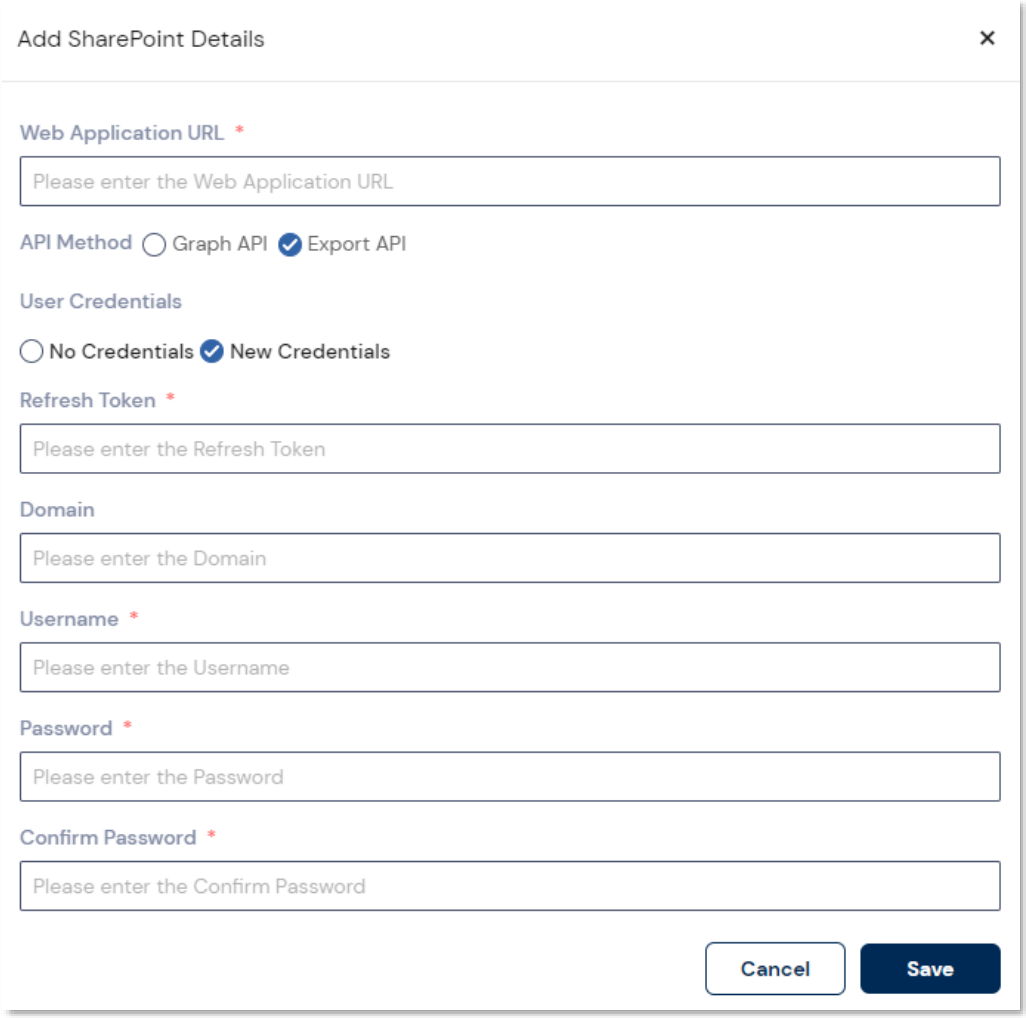
   iv. Repeat the same password in **Confirm Password** field.

© Exterro, Inc. All rights reserved

d) Export API:

i. Choose the **User Credentials**.

- No Credentials – This will fetch the credentials configured in the System Management > Manage Credentials page.
- New Credentials – Select this to configure users with new credentials.



6. Click **Save**.

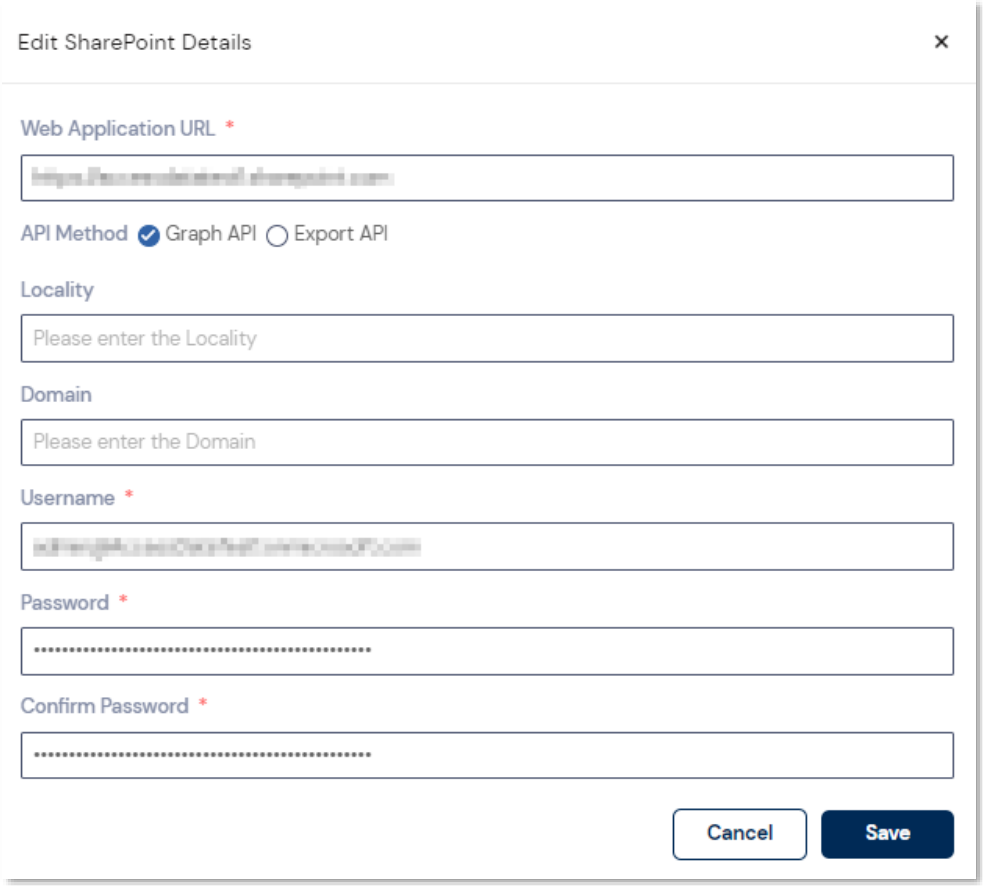
Note: Update the **RefreshSharepointDatasourceIntervalInDays** field in the **ADG.WeblabSelfHost.exe.config** file to automatically synchronize the SharePoint sub sites.

© Exterro, Inc. All rights reserved

Editing SharePoint data sources

To edit a SharePoint data source:

1. From the home page, click **Data Sources**.
2. Navigate to **SharePoint**.
3. Click **Edit** against the data source to be edited.
   - The **Edit SharePoint Details** pop-up is displayed.



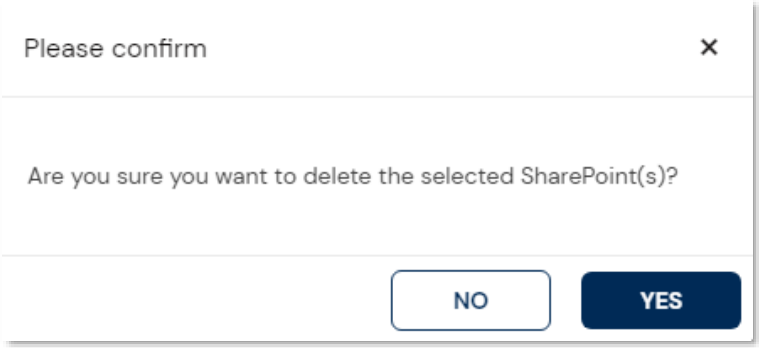
4. Make the necessary changes.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting SharePoint data sources

To delete a SharePoint data source:

1. From the home page, click **Data Sources**.
2. Navigate to **SharePoint**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.

© Exterro, Inc. All rights reserved

Exchange

You can configure the application to collect data from your Microsoft Exchange server which includes email, calendars, contacts, faxes, and voice mail. The following are the versions supported:

- Exchange 2010 SP1
- Exchange 2013
- Exchange 2016
- Exchange EAC (2019)
- Office 365

Note: Exchange Online Basic Authentication deprecation is in progress (31st December 2022) and if already disabled will need to be enabled here: https://portal.office.com/adminportal/home/ to continue with any collections.

If attempting to collect from GCC environments please refer to the Office 365 Credentials section.

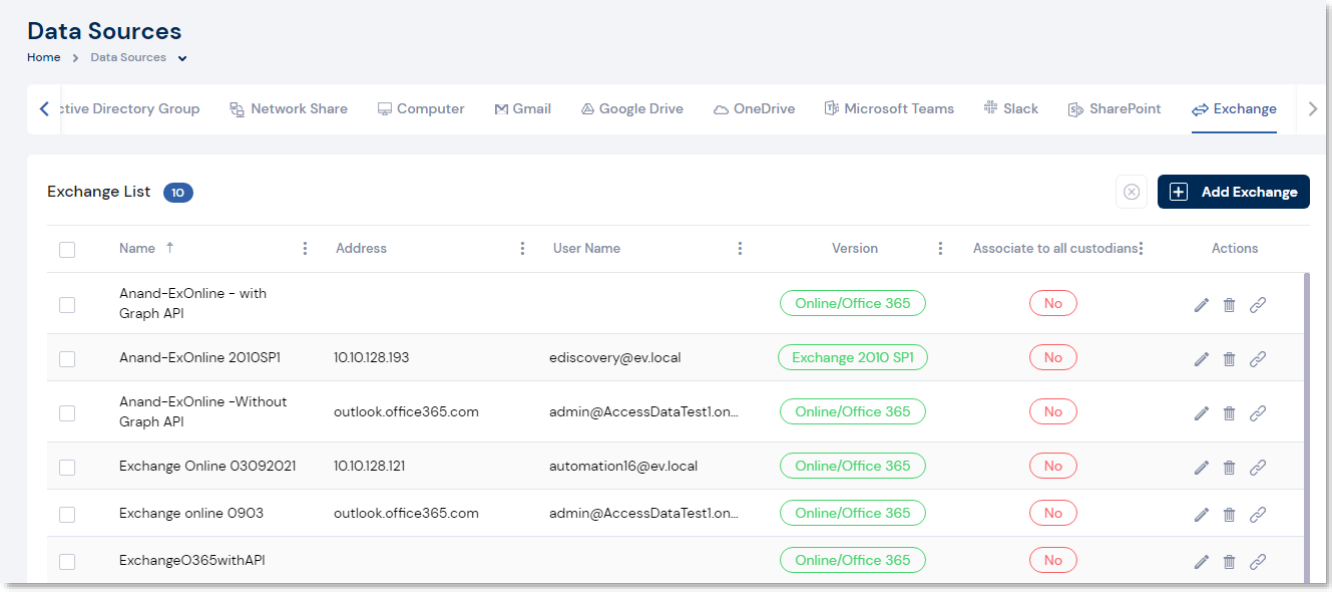
© Exterro, Inc. All rights reserved

Adding Online/Office 365 data sources

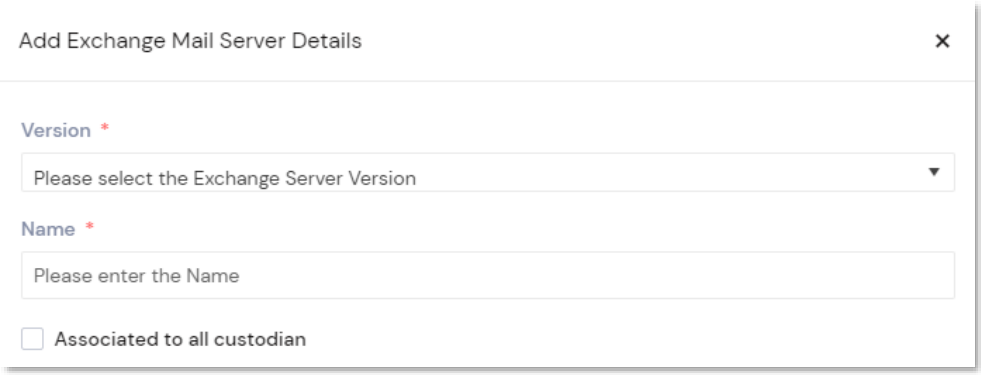
EWS API Method

To add an Online/Office 365 data source (EWS API Method):

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.

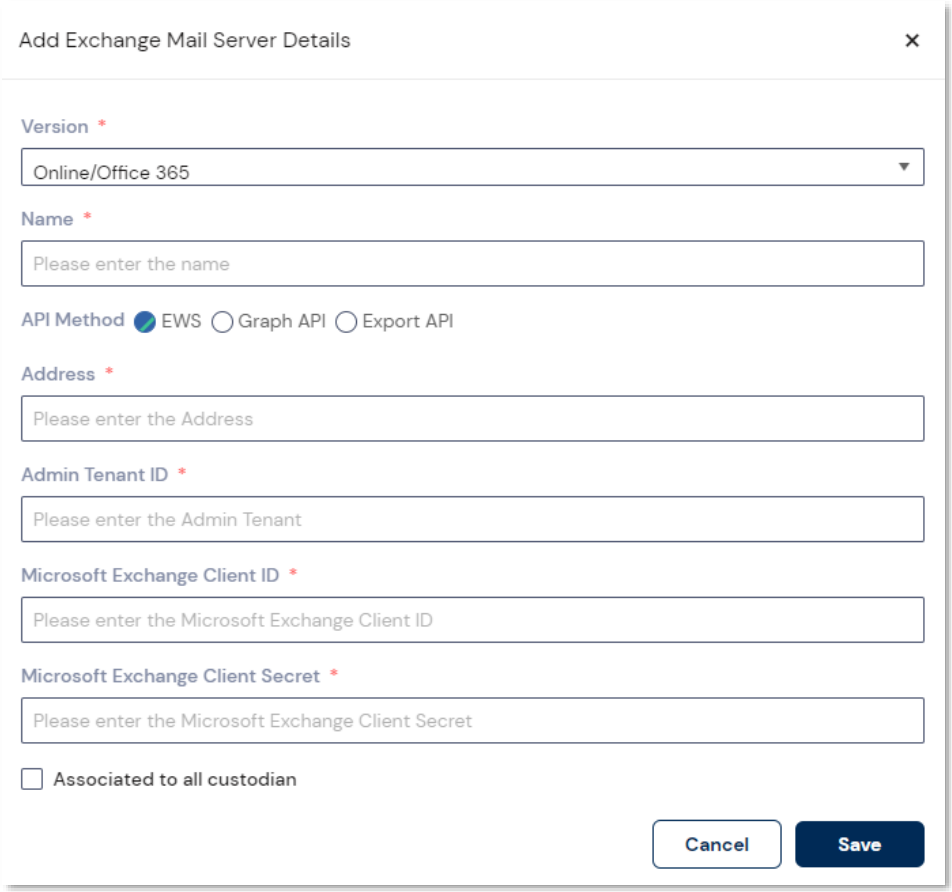


3. Click **Add Exchange**.
   - The **Add Exchange Mail Server Details** pop-up is displayed.



© Exterro, Inc. All rights reserved

4. Select **Online/Office 365** as the **Version** from the drop-down.
5. Enter a **Name** for the Exchange Server.
6. Select the **EWS** option for **API Method** field.



7. Enter the IP address of the Exchange Server in **Address**.
8. Enter the **Tenant ID** in the **Admin Tenant ID** field.

Note: The **Admin Tenant ID** field corresponds to the Primary Domain value.

9. Enter the **Microsoft Exchange Client ID**.
10. Enter the **Microsoft Exchange Client Secret**.
11. Select the **Associated to all custodian** checkbox to associate all the custodians to the server.

Note: If you have previously associated individual custodian to a server, this action will overwrite the associations of the individual custodian.

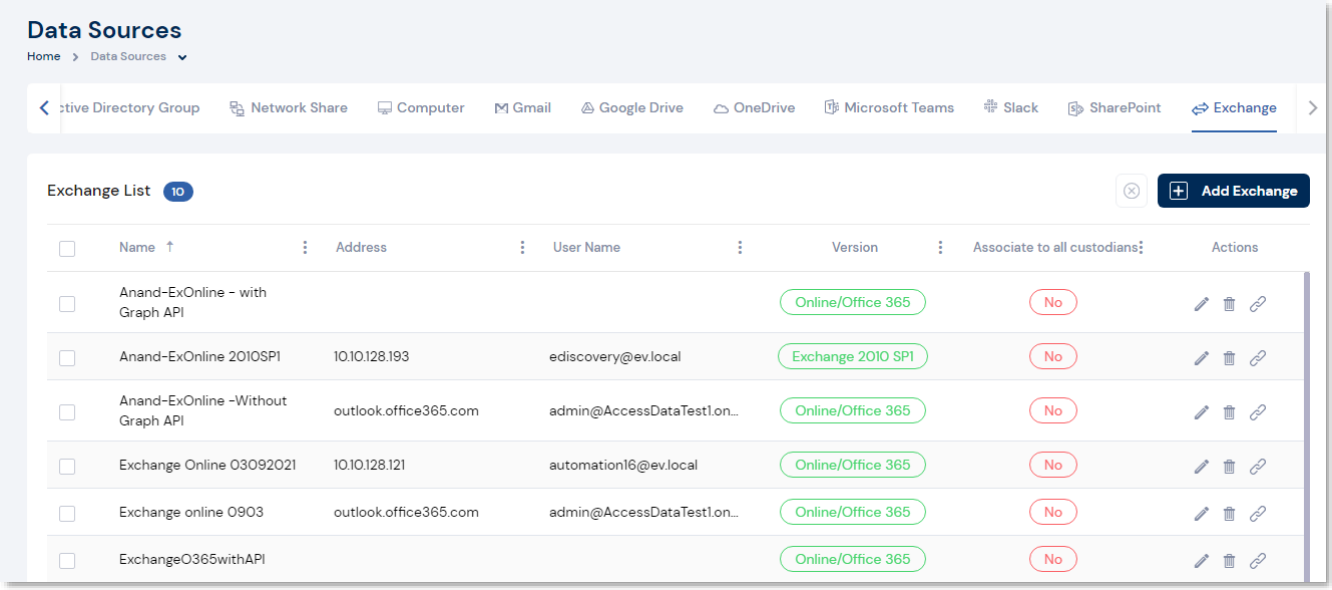
12. Click **Save**.

© Exterro, Inc. All rights reserved

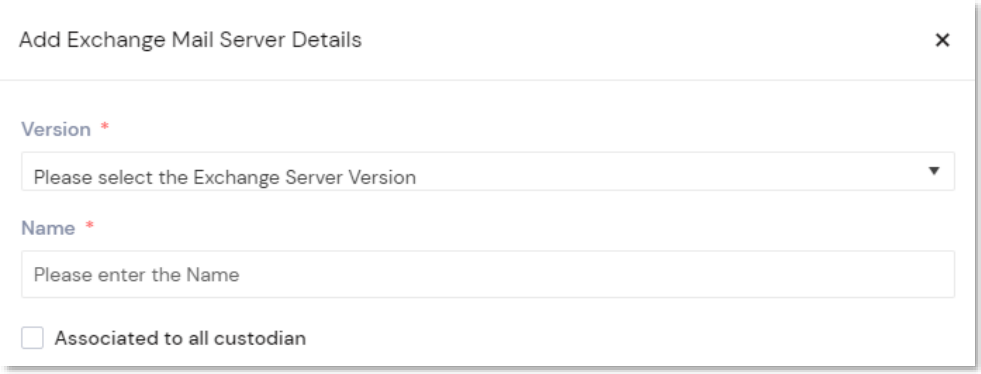
Graph API Method

To add an Online/Office 365 data source (Graph API Method):

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.

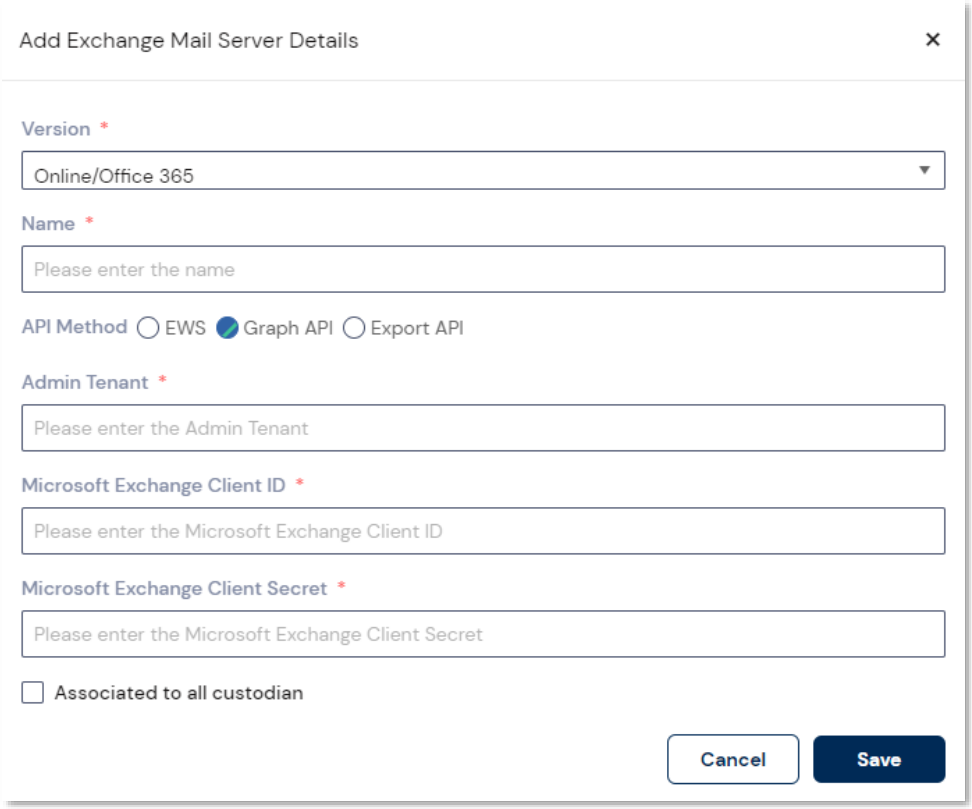


3. Click **Add Exchange**.
   - The **Add Exchange Mail Server Details** pop-up is displayed.



© Exterro, Inc. All rights reserved

4. Select **Online/Office 365** as the **Version** from the drop-down.
5. Enter a **Name** for the Exchange Server.
6. Select the **Graph API** option for the **API Method** field.



7. Enter the **Tenant ID** in the **Admin Tenant** field.

Note: The **Admin Tenant ID** field corresponds to the Primary Domain value.

8. Enter the **Microsoft Exchange Client ID**.
9. Enter the **Microsoft Exchange Client Secret**.
10. Select the **Associated to all custodian** checkbox to associate all the custodians to the server.

Note: If you have previously associated individual custodian to a server, this action will overwrite the associations of the individual custodian.

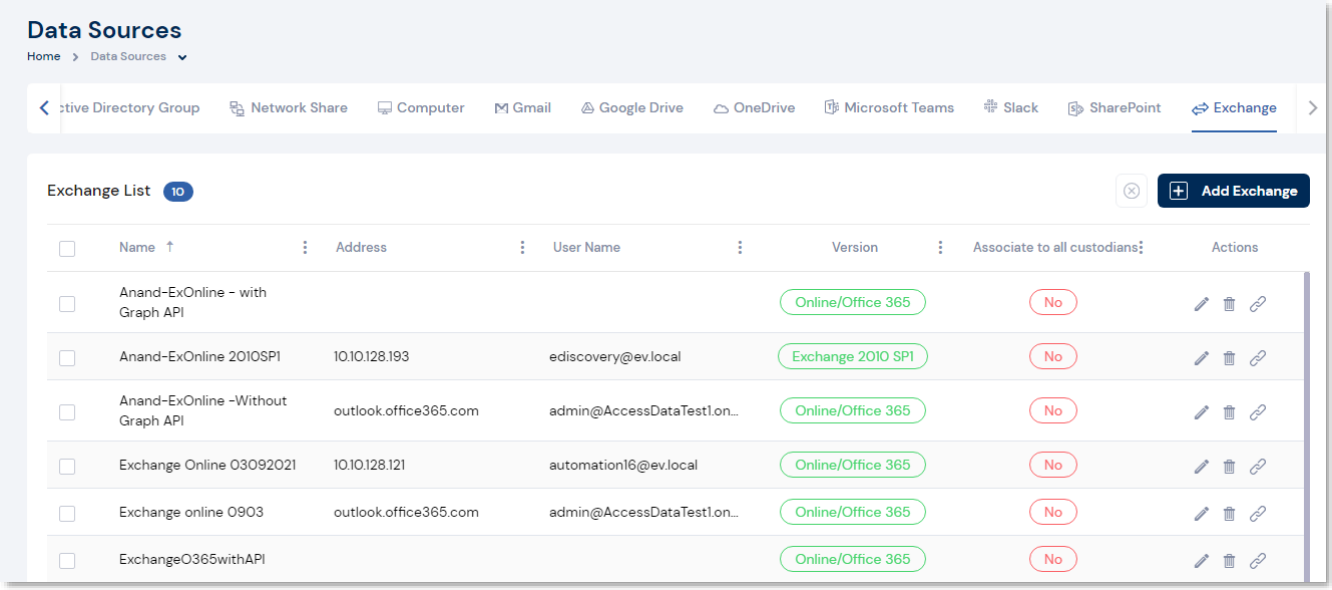
11. Click **Save**.

© Exterro, Inc. All rights reserved

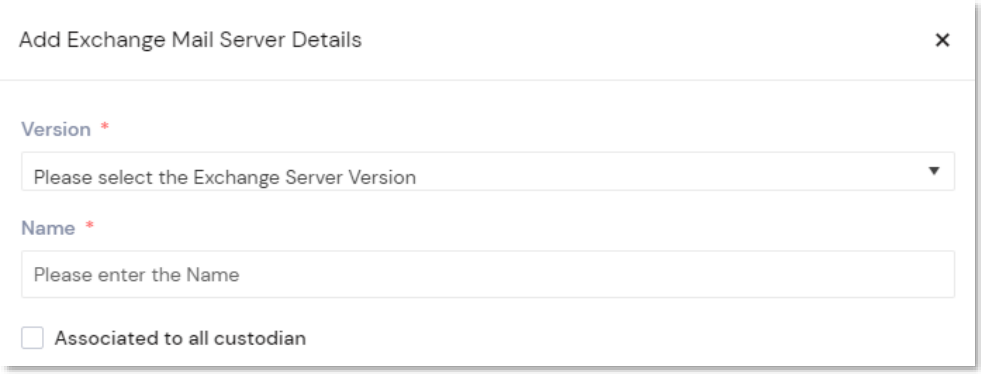
Export API Method

To add an Online/Office 365 data source (Export API Method):

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.

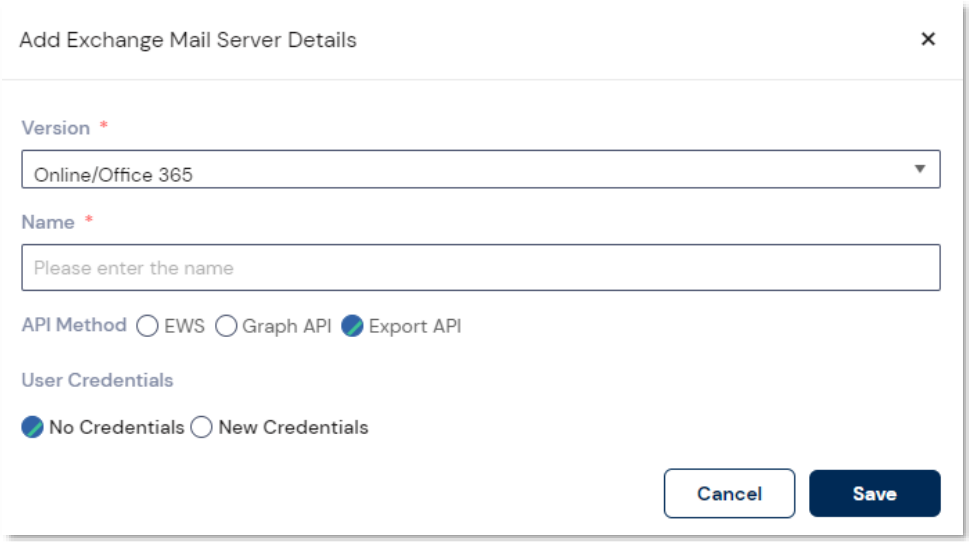


3. Click **Add Exchange**.
   - The **Add Exchange Mail Server Details** pop-up is displayed.



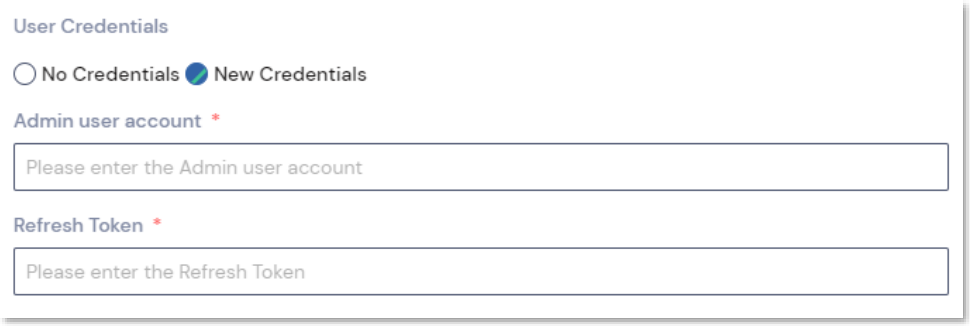
© Exterro, Inc. All rights reserved

4. Select **Online/Office 365** as the **Version** from the drop-down.
5. Enter a **Name** for the Exchange Server.
6. Select the **Export API** option for the **API Method** field.



© Exterro, Inc. All rights reserved

7. Select the any one of the below options for **User Credentials** field:
   - **No Credentials** – Select this option to create the data source without specific account credentials.
   - **New Credentials** – Select this option to create the data source for a specific user account. Upon enabling this option, the following fields will be displayed.



   - **Admin user account** – Provide the admin user account's email address.
   - **Refresh Token** – Provide the corresponding accounts Refresh Token.

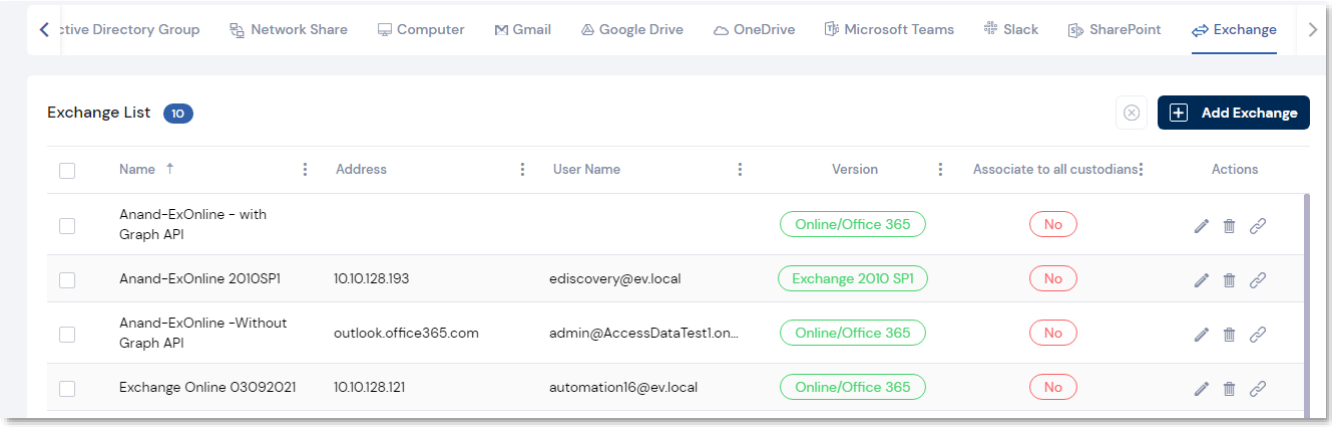
8. Click **Save**.

© Exterro, Inc. All rights reserved

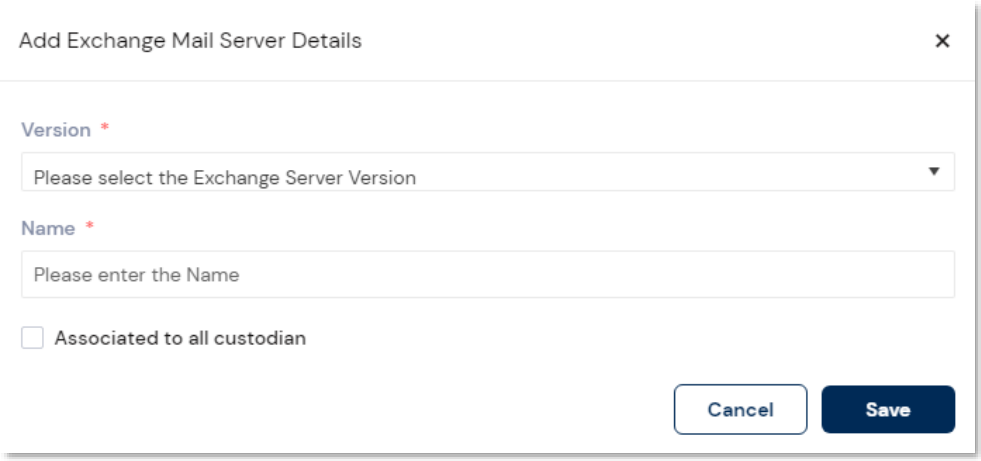
Adding Exchange data sources

To add an Exchange data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.

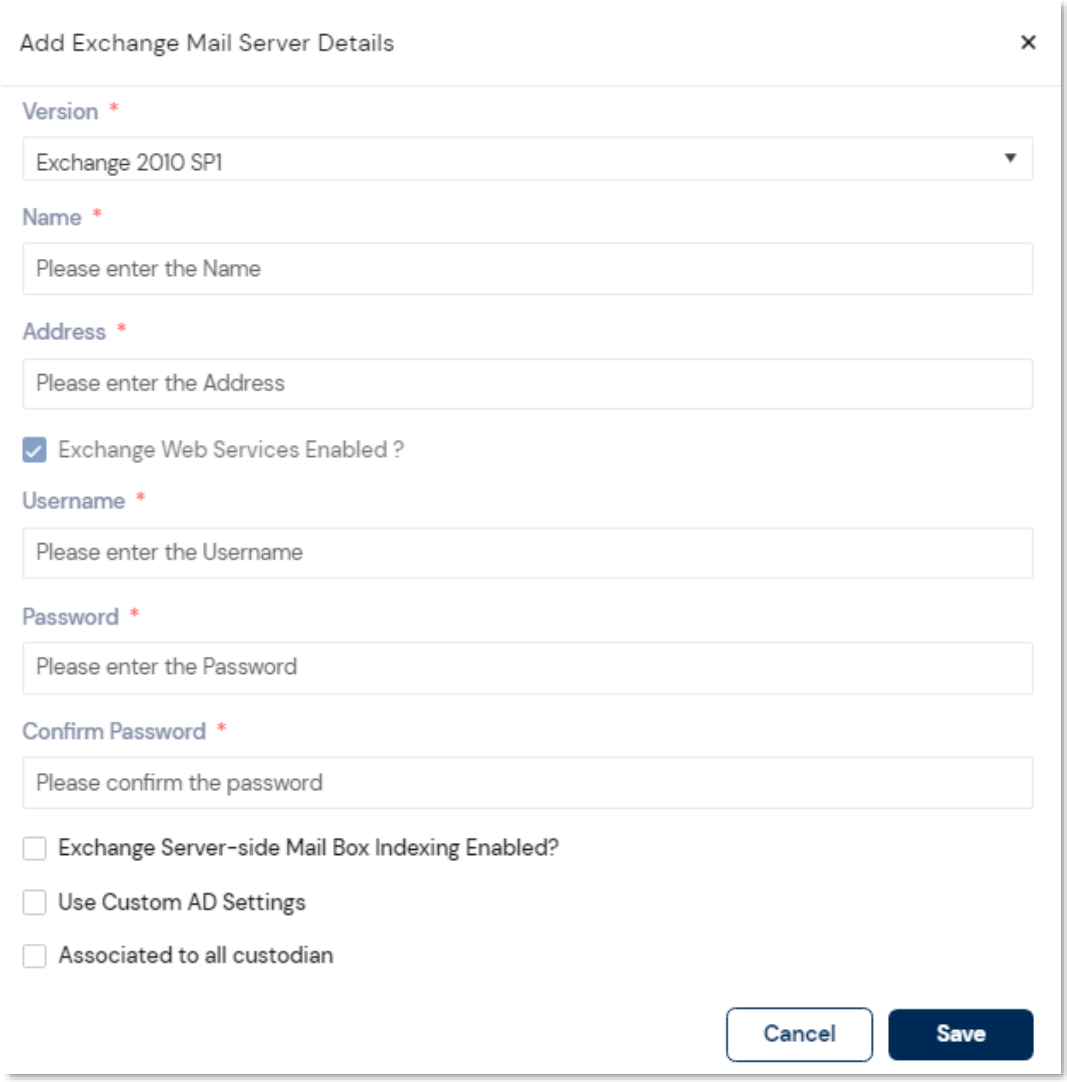


3. Click **Add Exchange**.
   - The **Add Exchange Mail Server Details** pop-up is displayed.



4. Select Exchange 2010 SPI, Exchange 2013, Exchange 2016, or Exchange 2019 as the **Version** from the drop-down.

© Exterro, Inc. All rights reserved



5. Enter a **Name** of the Exchange Server.
6. Enter the **Address**.
7. Enter the **Username**.
8. Enter the **Password**.
9. Repeat the same password in **Confirm Password** field.

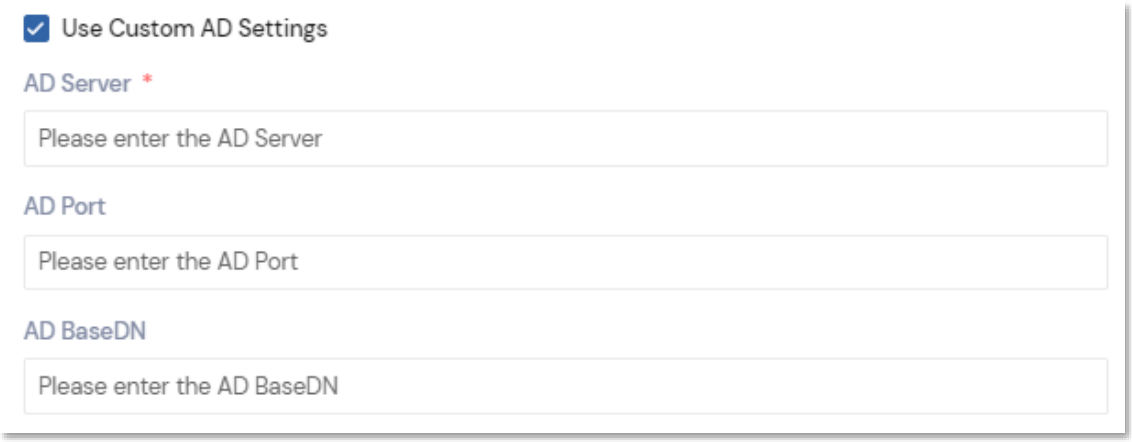
© Exterro, Inc. All rights reserved

10. You can select the **Exchange Server-side Mail Box Indexing Enabled?** checkbox if you have indexing enabled on the server.

Warning: If you want to use filters on the data collected, you must have this action checked.

11. Enable the **Use Custom AD Settings** checkbox to use a custom active directory instead of the local active directory server.

Note: By default, the application uses the local Active Directory server. If you have an advanced scenario, such as a cross-domain scenario, you can select to this option and specify the AD Server, AD Port, AD BaseDN settings.



12. Select the **Associated to all custodians** to associate all the custodians to the server.

Note: If you have previously associated individual custodian to a server, this action will overwrite the associations of the individual custodian.

13. Click **Save**.

© Exterro, Inc. All rights reserved

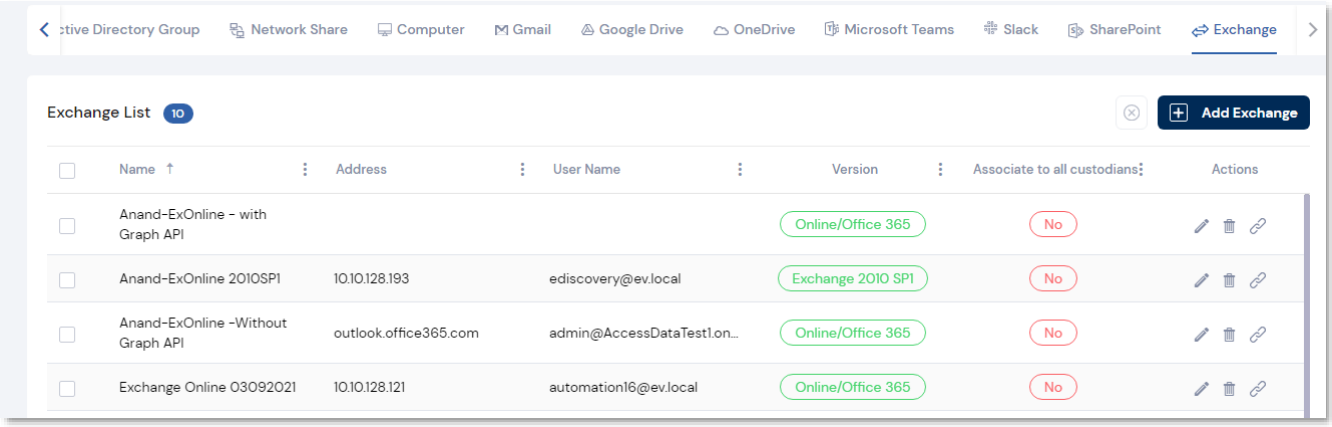
Adding On-Premise Exchange data sources (EAC)

Notes:

- FTK Central supports collection for the Exchange 2019 version.
- Refer to the Exterro Exchange Admin Center (EAC) - Configuration Guide.

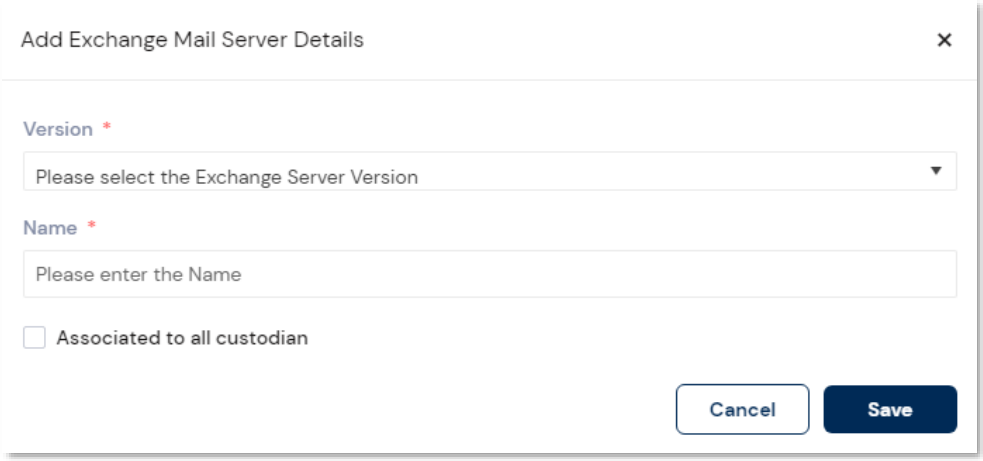
To add an On-Premise Exchange data source (EAC):

14. From the home page, click **Data Sources**.
15. Navigate to **Exchange**.

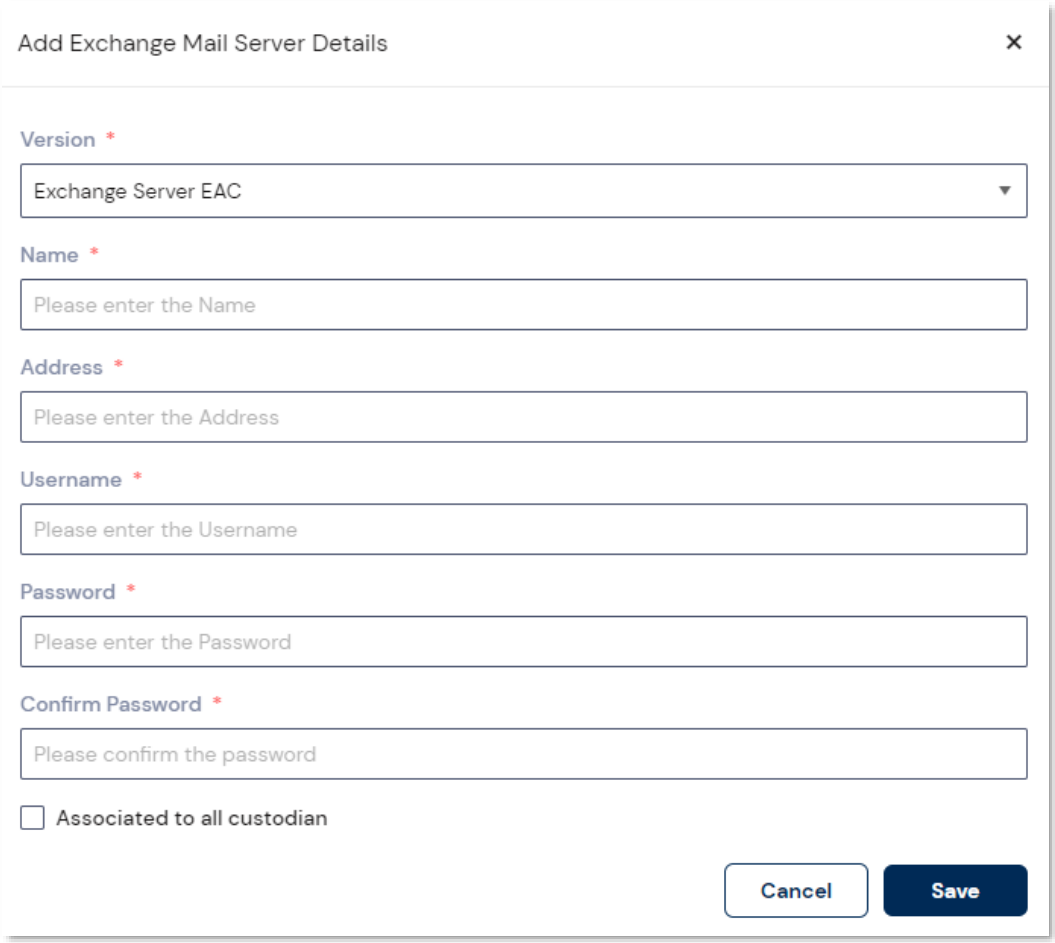


© Exterro, Inc. All rights reserved

16. Click **Add Exchange**.
    - The **Add Exchange Mail Server Details** pop-up is displayed.



17. Select Exchange EAC as the **Version** from the drop-down.



© Exterro, Inc. All rights reserved

18. Enter a **Name** of the Exchange Server.
19. Enter the **Address**.
20. Enter the **Username**.
21. Enter the **Password**.
22. Repeat the same password in **Confirm Password** field.
23. Select the **Associated to all custodians** to associate all the custodians to the server.

Note: If you have previously associated individual custodian to a server, this action will overwrite the associations of the individual custodian.

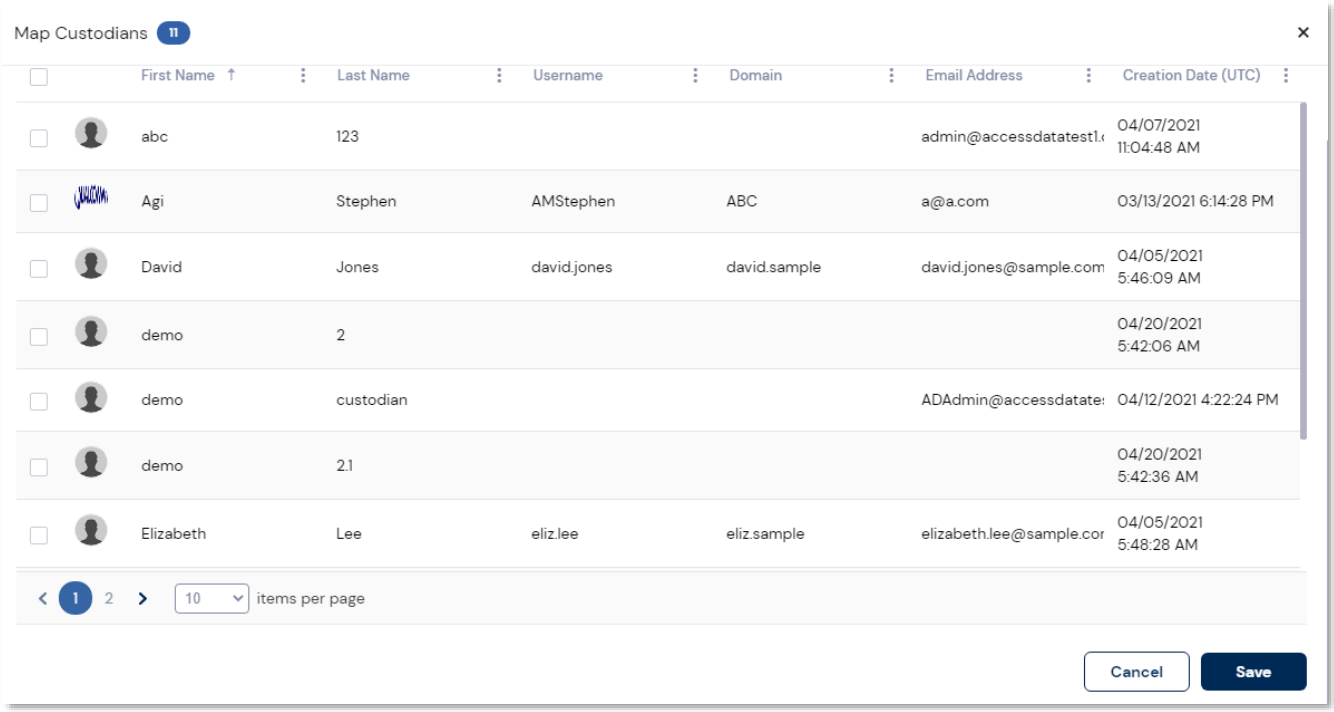
24. Click **Save**.

© Exterro, Inc. All rights reserved

Mapping Exchange data sources to Custodians

To map an Exchange data source to custodians:

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.
3. Click **Map Custodian** against the data source to be mapped.
   - The **Map Custodians** pop-up is displayed.



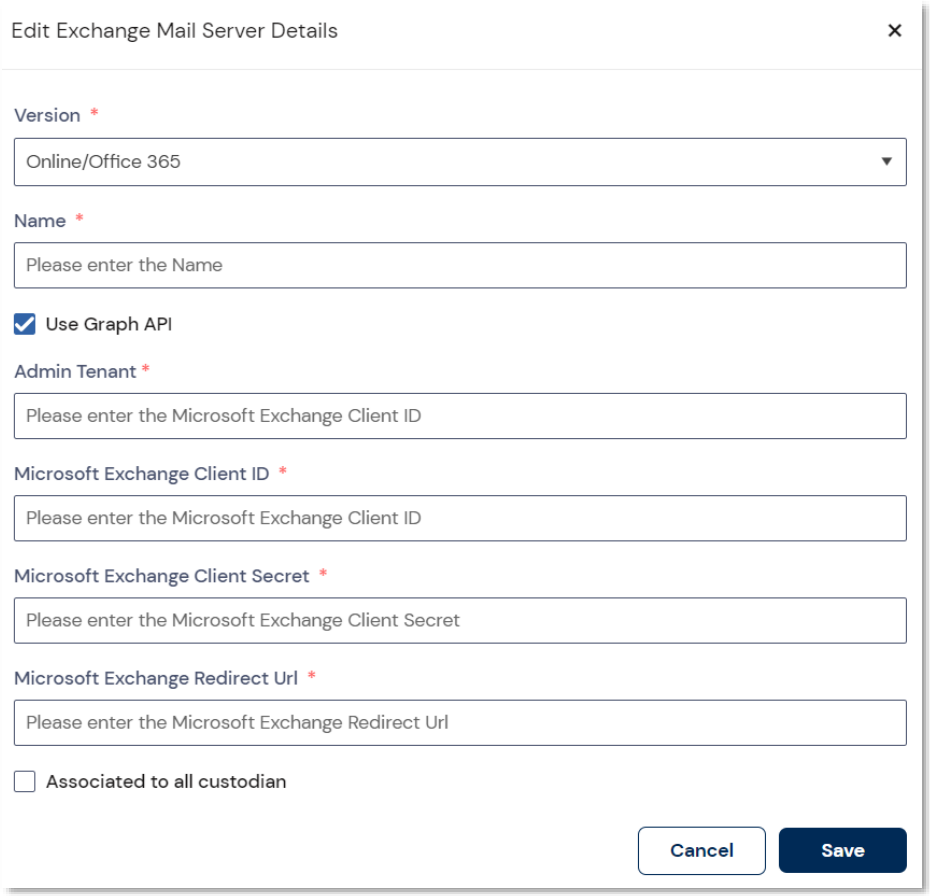
4. Select the required custodians by enabling the checkbox against it.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Editing Exchange data sources

To edit an Exchange data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.
3. Click **Edit** against the data source to be edited.
   - The **Edit Exchange Mail Server Details** pop-up is displayed.



Note: The fields displayed may vary based on the Exchange data source type.

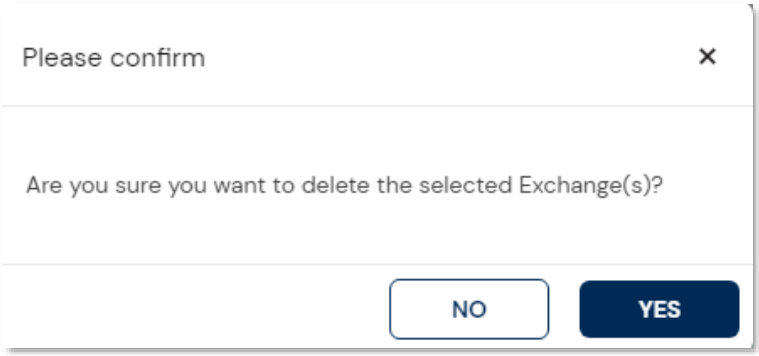
4. Make the necessary changes.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting Exchange data sources

To delete an Exchange data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Exchange**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

Note: You can also perform bulk deletion of data sources by clicking the checkbox against it and clicking on **Delete**.

© Exterro, Inc. All rights reserved

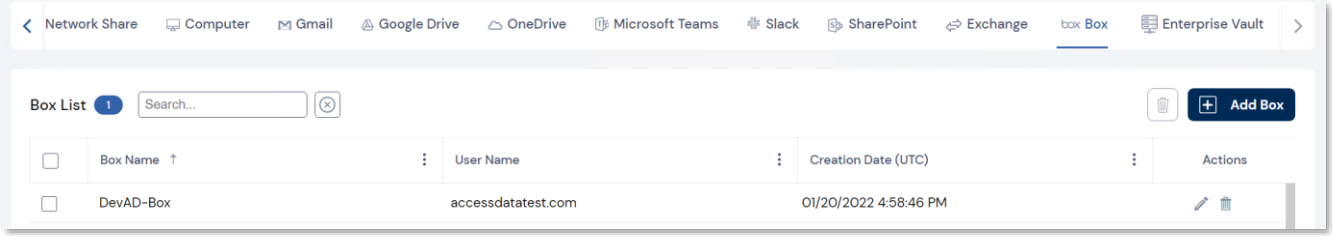
Box

You can configure the application to collect structured and unstructured data from Box. You can add, edit, or delete multiple accounts from this page.

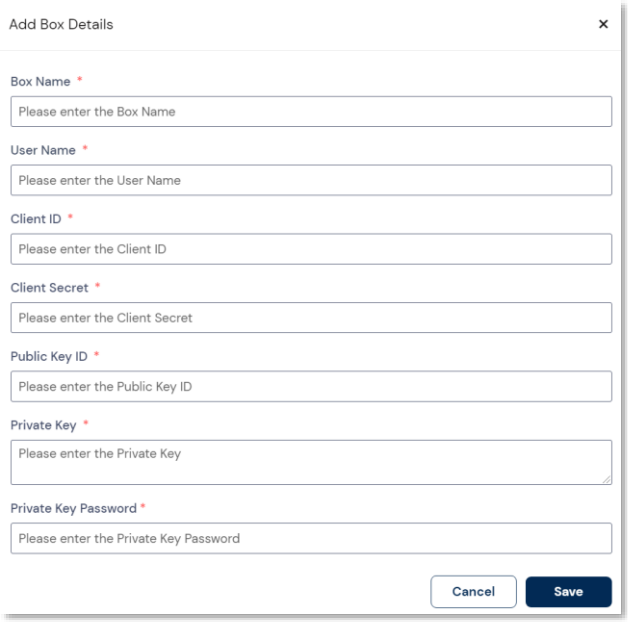
Adding Box data sources

To add a Box data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Box**.



3. Click **Add Box**.
   - The **Add Box Details** pop-up is displayed.



4. Provide a **Name** for Box.

© Exterro, Inc. All rights reserved

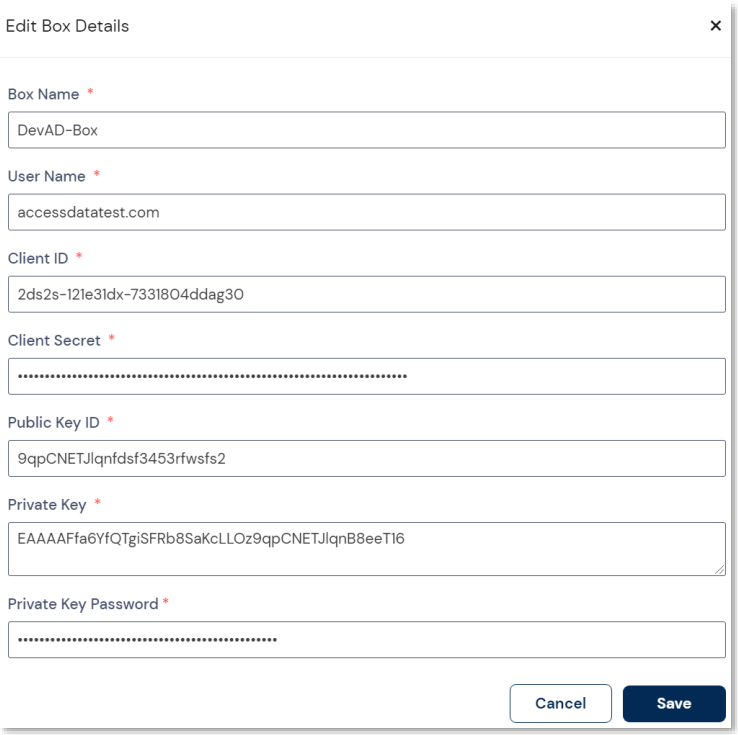
5. Enter the **User Name.**
6. Enter the **Client ID**
7. Enter the **Client Secret**.
8. Enter the **Public Key ID**.
9. Enter the **Private Key**.
10. Enter the **Private Key Password**.
11. Click **Save**.

© Exterro, Inc. All rights reserved

Editing Box data sources

To edit a Box data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Box**.
3. Click **Edit** against the data source to be edited.
   - The **Edit Box Details** pop-up is displayed.



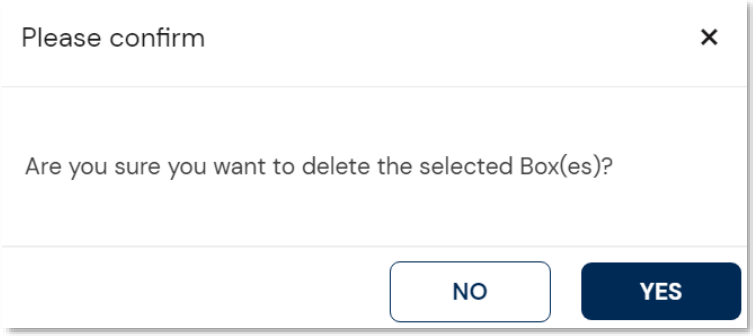
4. Make the necessary changes.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting Box data sources

To delete a Box data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Box**.
3. Click **Delete** against the data source to be deleted.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.

© Exterro, Inc. All rights reserved

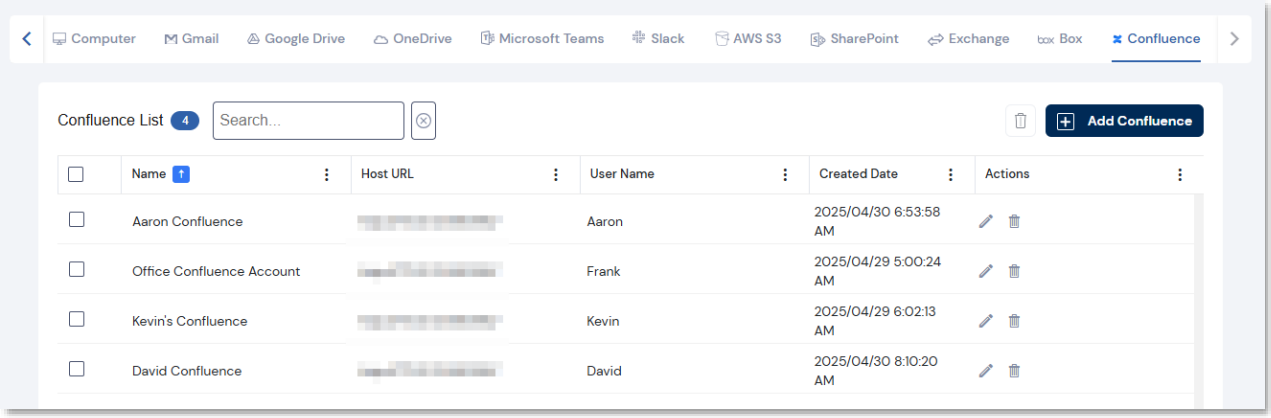
Confluence

You can configure the application to collect data from Confluence. You can add, edit, or delete multiple accounts from this page.

Adding Confluence data sources

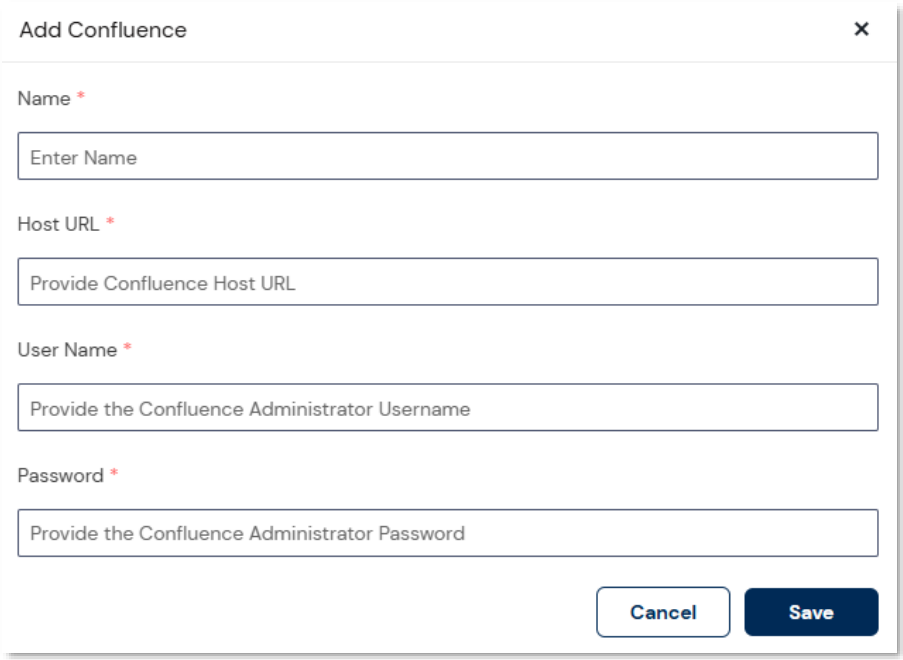
To add a Confluence data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Confluence**.



© Exterro, Inc. All rights reserved

3. Click **Add Confluence**.
   - The **Add Confluence** pop-up is displayed.



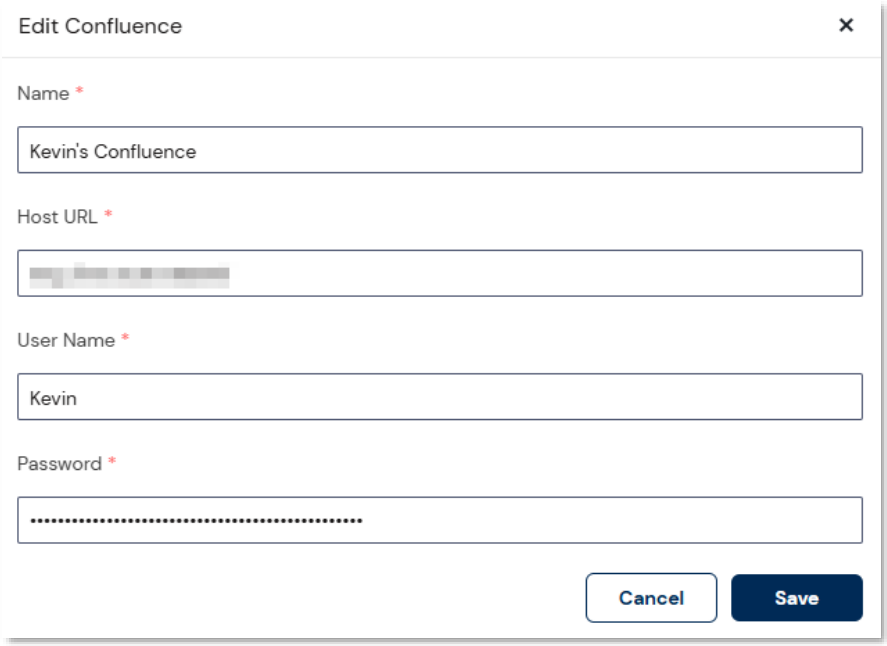
4. Provide a **Name** for the Confluence account.
5. Enter the **Host URL.**
6. Enter the **User Name.**
7. Enter the **Password**.
8. Click **Save**.

© Exterro, Inc. All rights reserved

Editing Confluence data sources

To edit a Confluence data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Confluence**.
3. Click **Edit** against the data source to be edited.
   - The **Edit Confluence** pop-up is displayed.



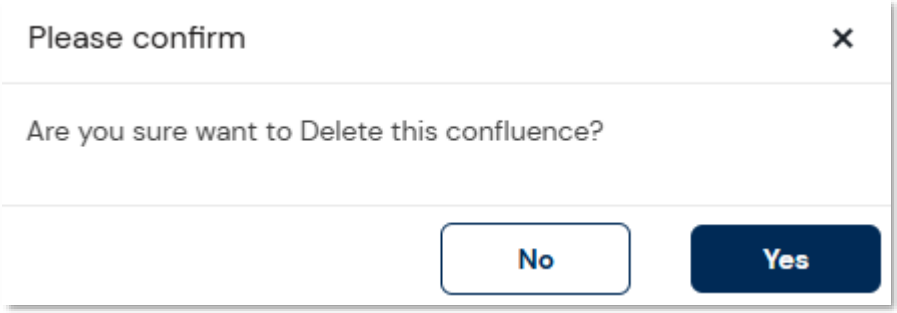
4. Make the necessary changes.
5. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting Confluence data sources

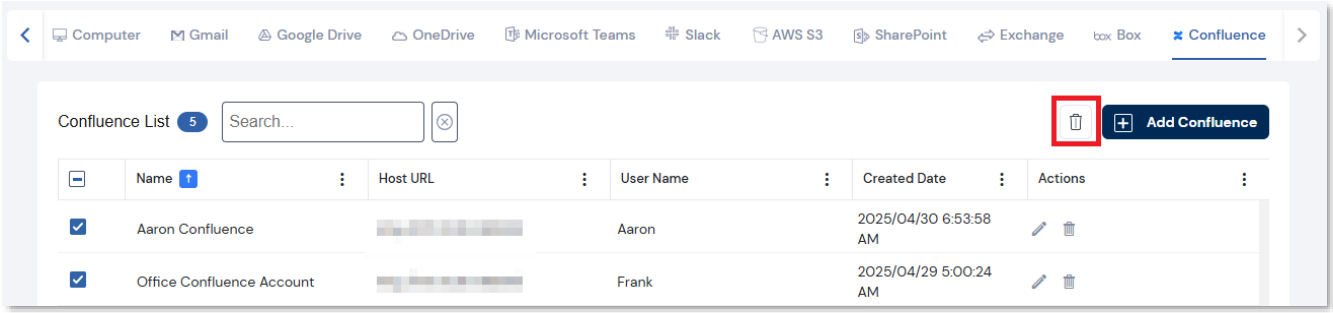
To delete a Confluence data source:

1. From the home page, click **Data Sources**.
2. Navigate to **Confluence**.
3. Click **Delete** against the data source to be deleted.
   - The confirmation pop-up is displayed.



4. Click **Yes**.

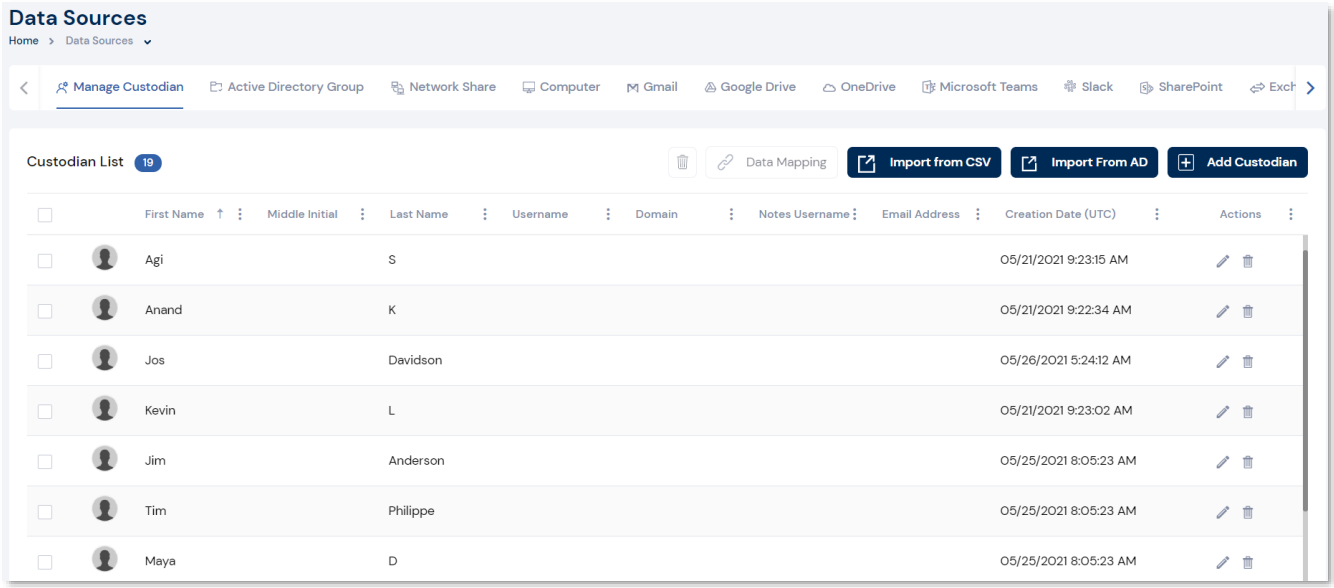
Note: You can also perform bulk deletion of the data source by enabling the checkbox against it and clicking on **Delete**.



© Exterro, Inc. All rights reserved

Custodians

Custodian refers to any identified user who may have data relevant to a case under consideration during electronic discovery. This can include electronically stored information (ESI) on employee or management computers, and can refer to computers, shares, email, or other public repositories associated with the user.



© Exterro, Inc. All rights reserved

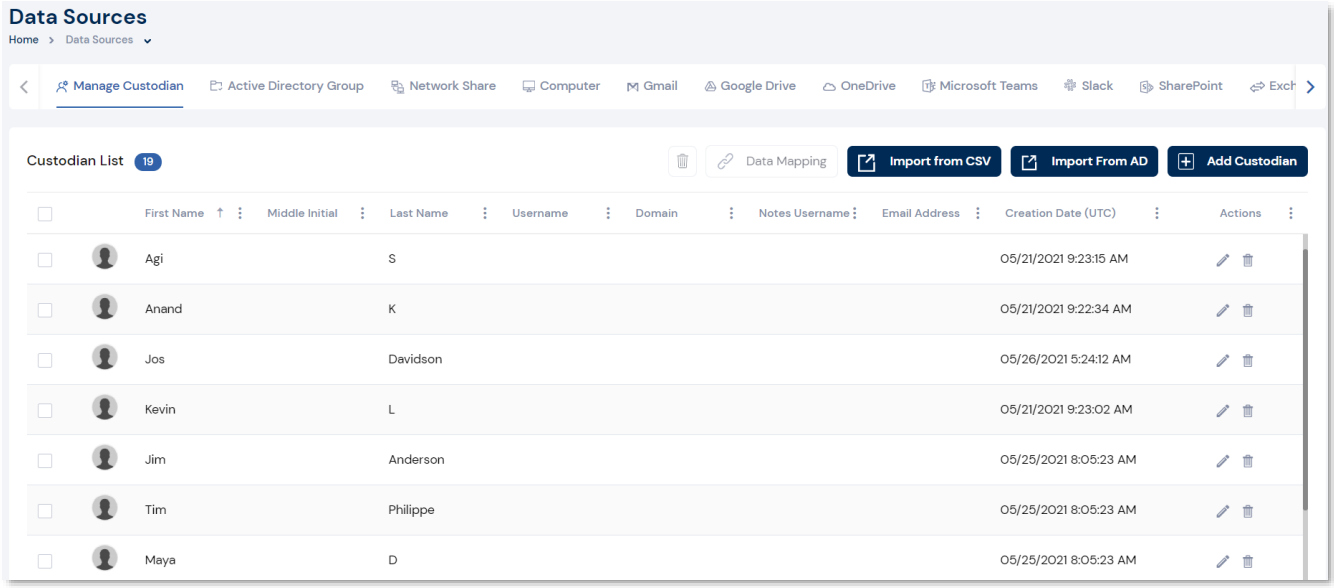
Managing Custodians

FTK Central allows you to add custodians, import custodians via CSV files, import custodians from active directories, add data sources to the custodians, and also to edit or delete them as required.

Adding Custodians

To add a custodian:

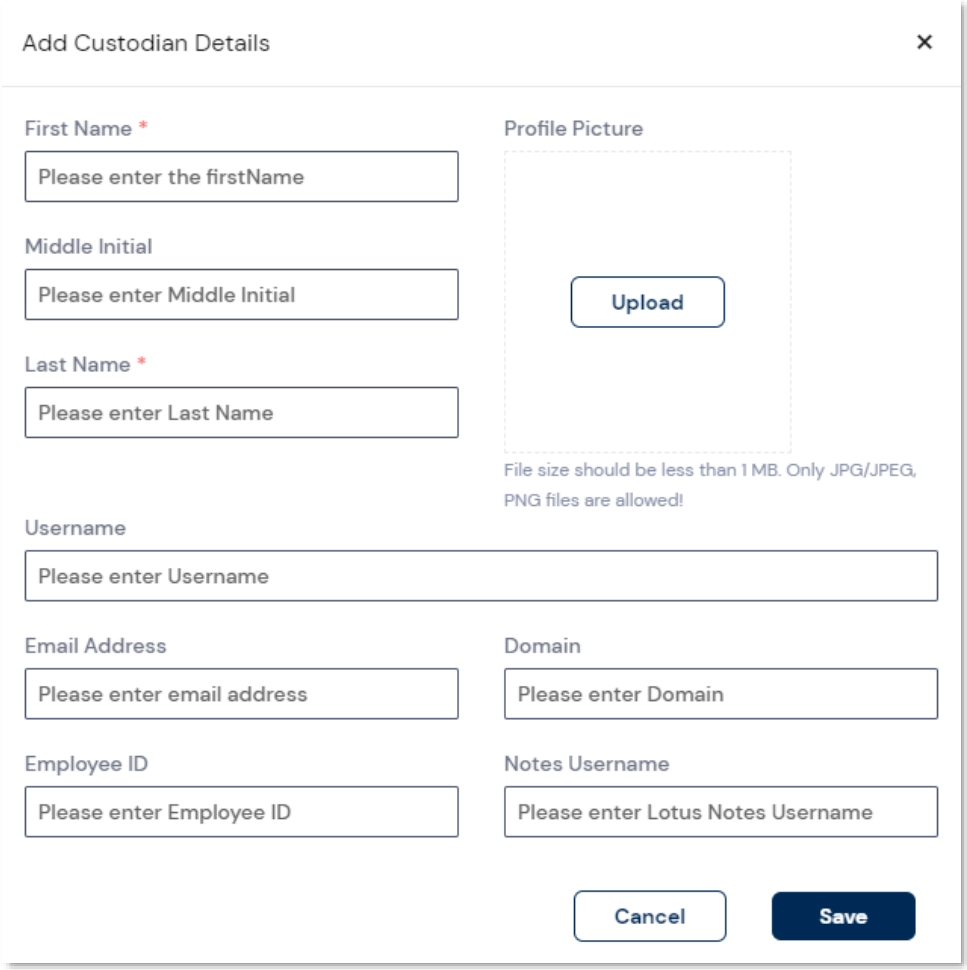
1. From the home page, click **Data Sources**.
   - The **Manage Custodian** page is displayed.



2. Click **Add Custodian**.

© Exterro, Inc. All rights reserved

- The **Add Custodian Details** pop-up is displayed.



3. Enter the custodian's **First Name**, **Middle Initial** and **Last Name**.
4. Click **Upload** and add the profile picture of the custodians.
5. Provide a **Username** of the custodian.
6. Enter the custodian's **Email Address.**
7. The network **Domain** to which the custodian belongs.
8. Enter the custodian's **Employee ID**.
9. The **Notes Username** of the custodian as it appears in their Lotus Notes Directory.
10. Click **Save**.

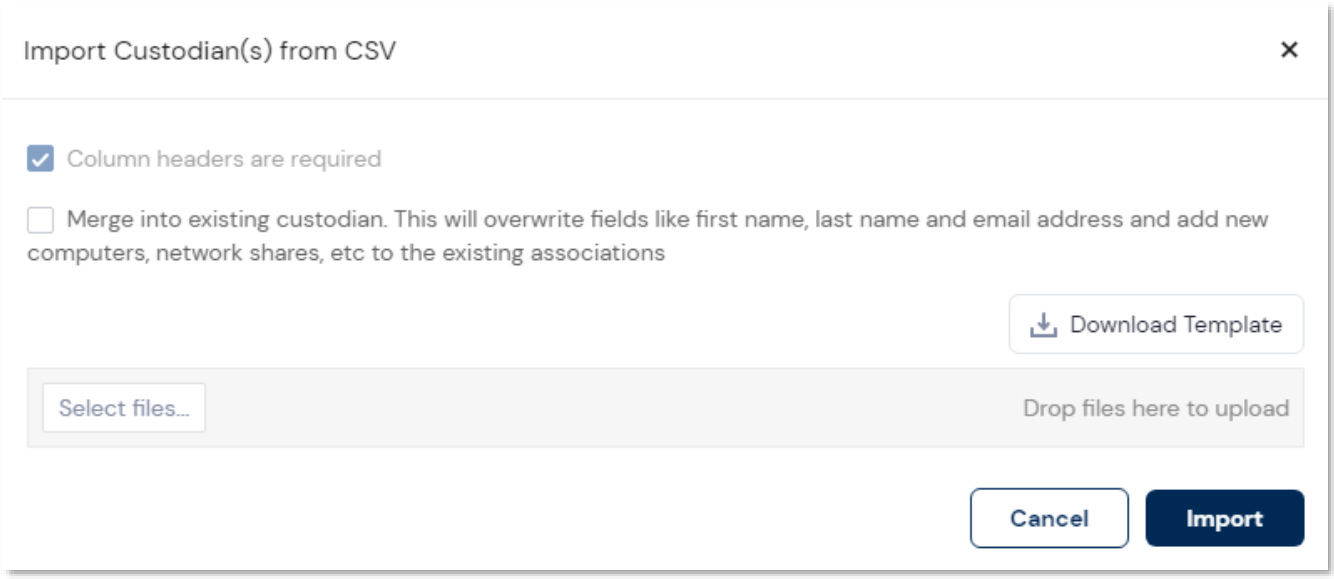
© Exterro, Inc. All rights reserved

Importing Custodians from CSV

You can also import a list of custodians into the system from a CSV file.

To import custodians from CSV:

1. From the home page, click **Data Sources**.
2. Click **Import from CSV**.
   - The **Import Custodian(s) from CSV** pop-up is displayed.



3. Click **Select files**.
4. Select the required file or drag and drop the file to be uploaded.
5. Choose if you want the entries in the CSV to overwrite the information of existing custodians.
6. Click **Import**.

Note: You can also click on **Download Template** and fill in the necessary details and upload to import them to the application.

© Exterro, Inc. All rights reserved

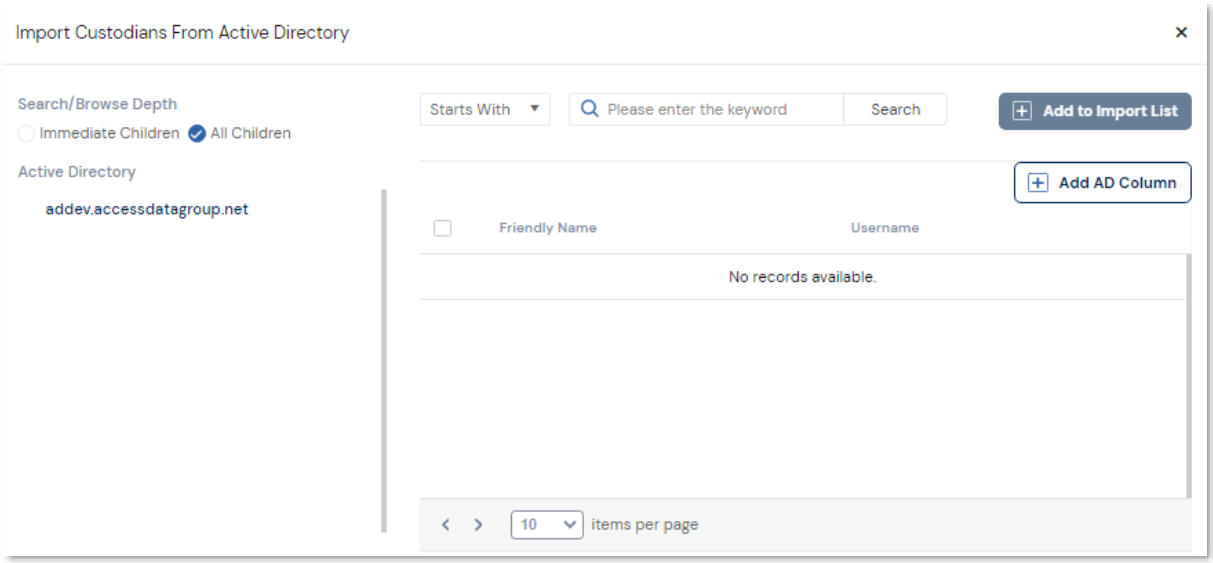
Importing Custodians from Active Directory (AD)

You can also import custodians from Active Directory. The custodian information is automatically taken from the Active Directory. However, you can edit the custodian information later if required.

Warning: You must perform the Active Directory configuration before proceeding to import custodians from it.

To import custodians from an Active Directory:

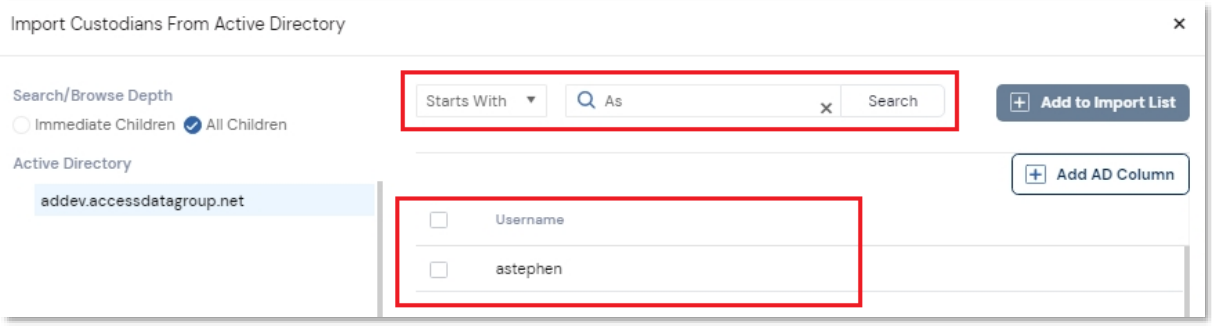
1. From the home page, click **Data Sources**.
2. Click **Import from AD**.
   - The **Import Custodian From Active Directory** pop-up is displayed.



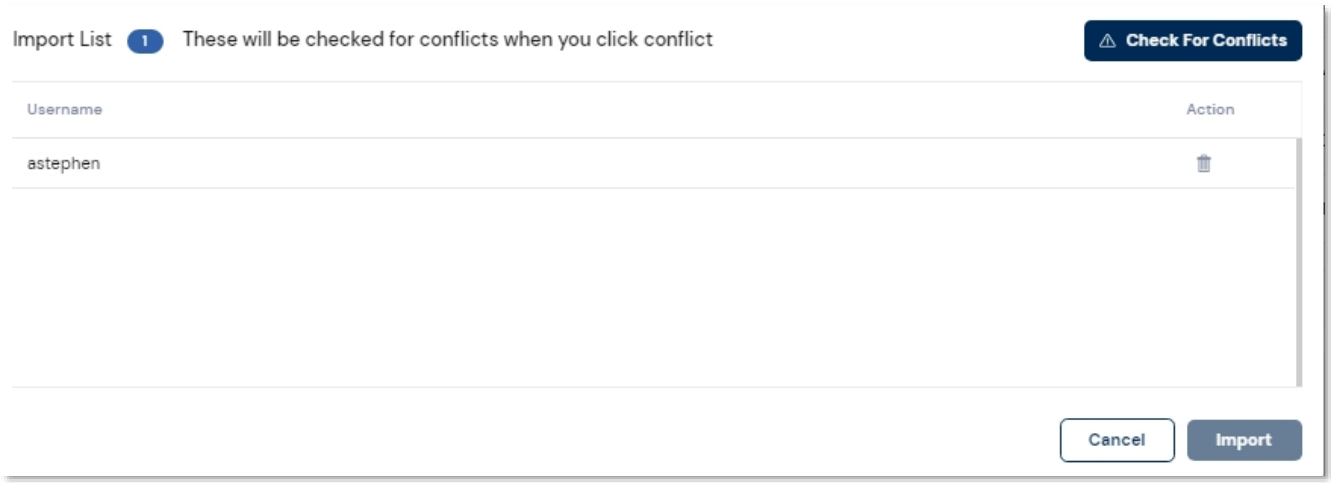
3. Select the **Search/Browse Depth** as required.
   - **Immediate Children** – Select this to take the immediate subfolders of the specified path and import each of those subfolders' content as a unique evidence item. You can automatically create a custodian based on the child folder's name (if the child folder has a first and last name separated by a space) and have it associated with the data in the subfolder.
   - **All Children** – Select this to take all the folders of the specified path and imports all the files.
4. Select the **Active Directory**.
5. Select the custodians from the right-pane.

© Exterro, Inc. All rights reserved

Note: You can also search and select the required custodians.

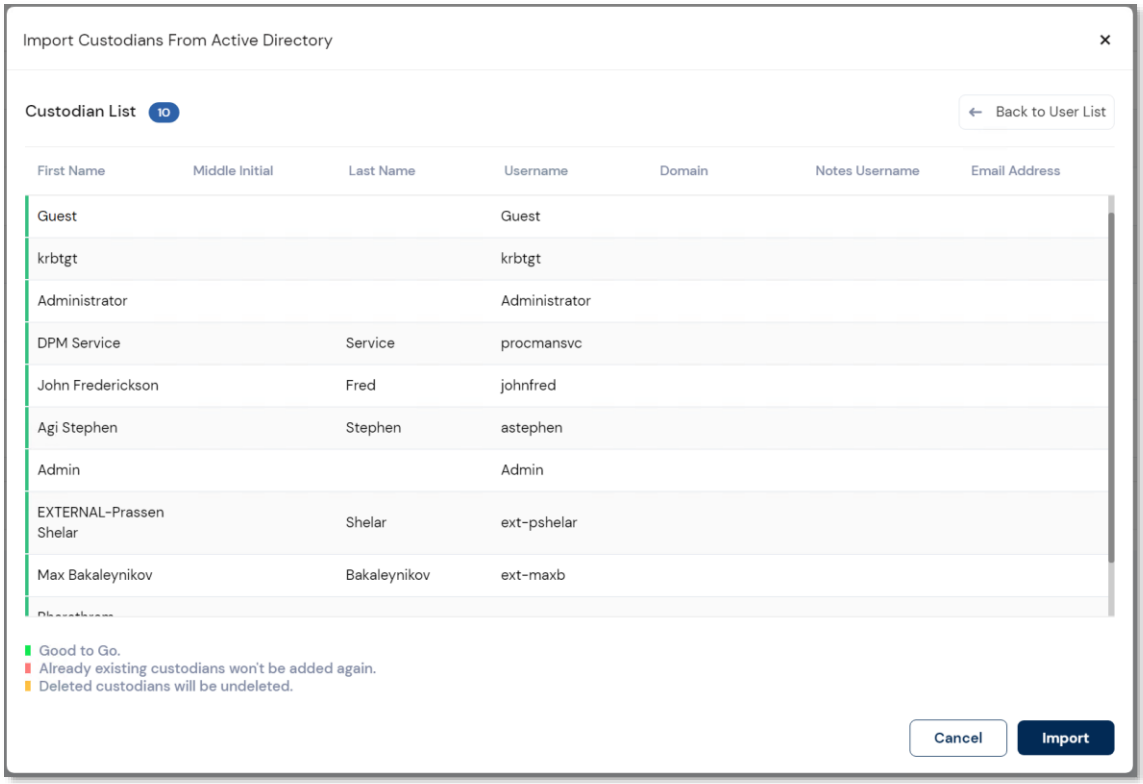


6. Click **Add to Import List**.
   - The selected users will be displayed in the Import List section.



© Exterro, Inc. All rights reserved

7. Click **Check For Conflicts**.

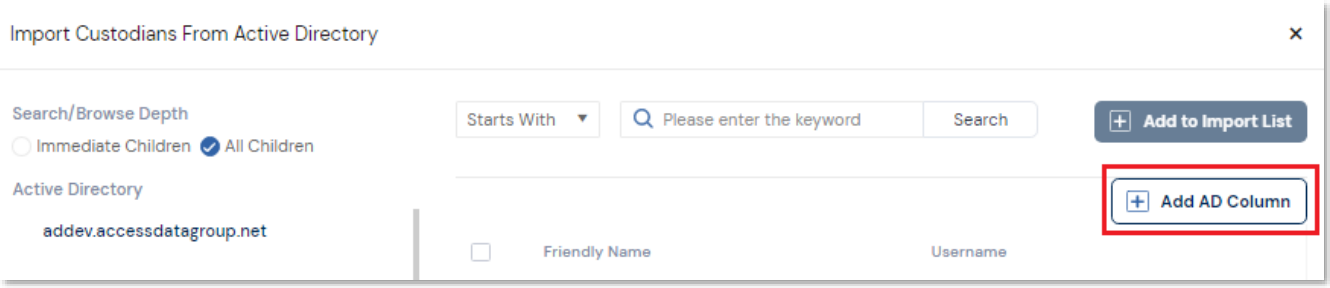


8. Click **Import**.

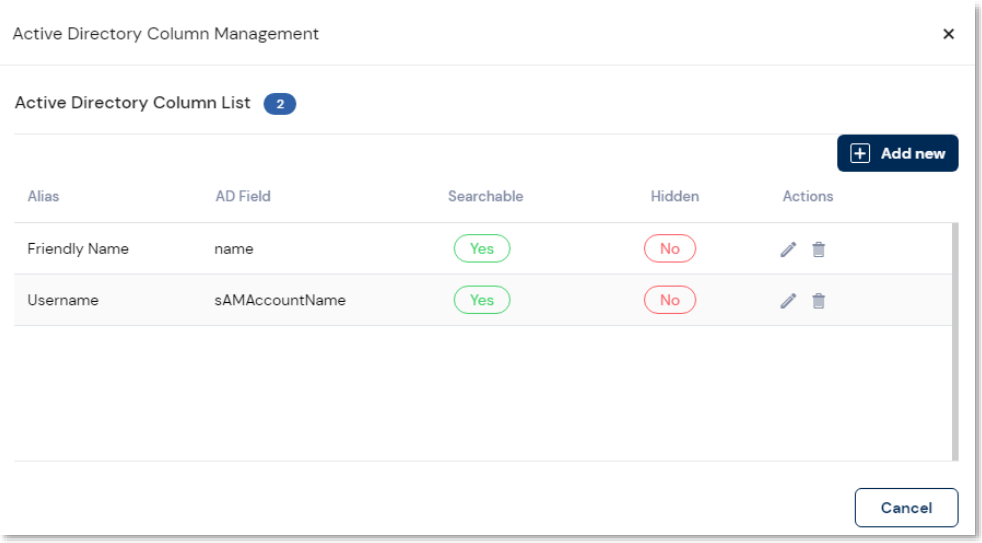
© Exterro, Inc. All rights reserved

To import additional active directory column:

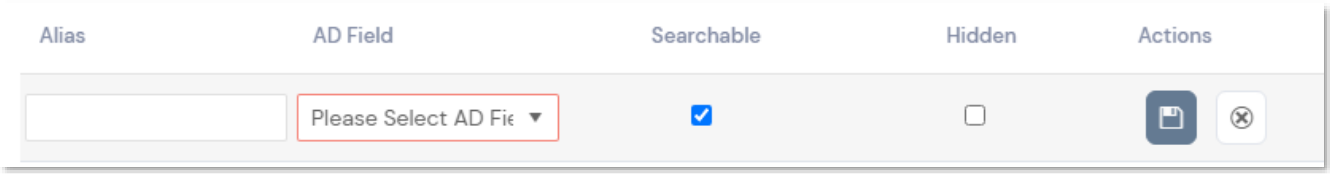
1. Click **Add AD Column** to add additional information to the Active Directory.



- The **Active Directory Column Management** pop-up is displayed.



2. Click **Add new**.
   - The below screen will be displayed.



3. Enter the **Alias** name for the Active Directory.

© Exterro, Inc. All rights reserved

4. Select the **AD Field** from the drop-down.
5. Enable the **Searchable** checkbox to make the column searchable.
6. Enable the **Hidden** checkbox to hide the column for the users.
7. Click **Import** .
8. Click **Import**.

Editing Custodians

To edit a custodian information:

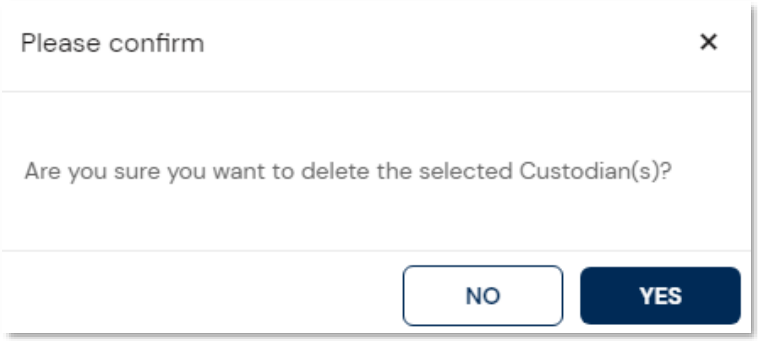
1. From the home page, click **Data Sources**.
2. Click **Edit** against the custodian to be edited.
3. Make the necessary changes.
4. Click **Save**.

© Exterro, Inc. All rights reserved

Deleting Custodians

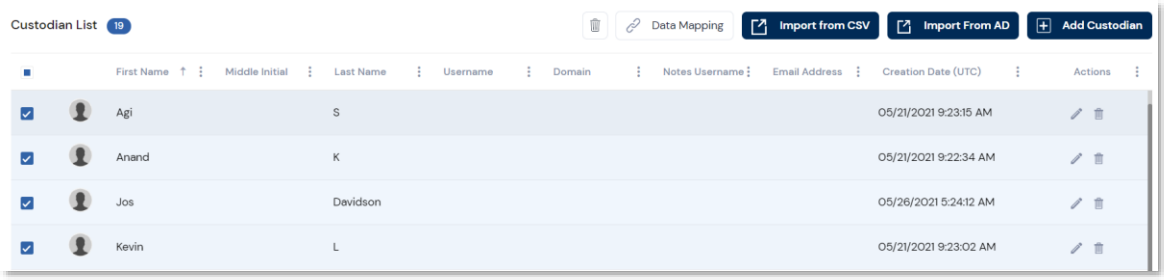
To delete a custodian:

1. From the home page, click **Data Sources**.
2. Click **Delete** against the custodian to be deleted.
   - The **Please confirm** pop-up is displayed.



3. Click **YES**.

Note: You can also perform bulk deletion of the custodians, by enabling the checkbox against it and clicking on **Delete** .



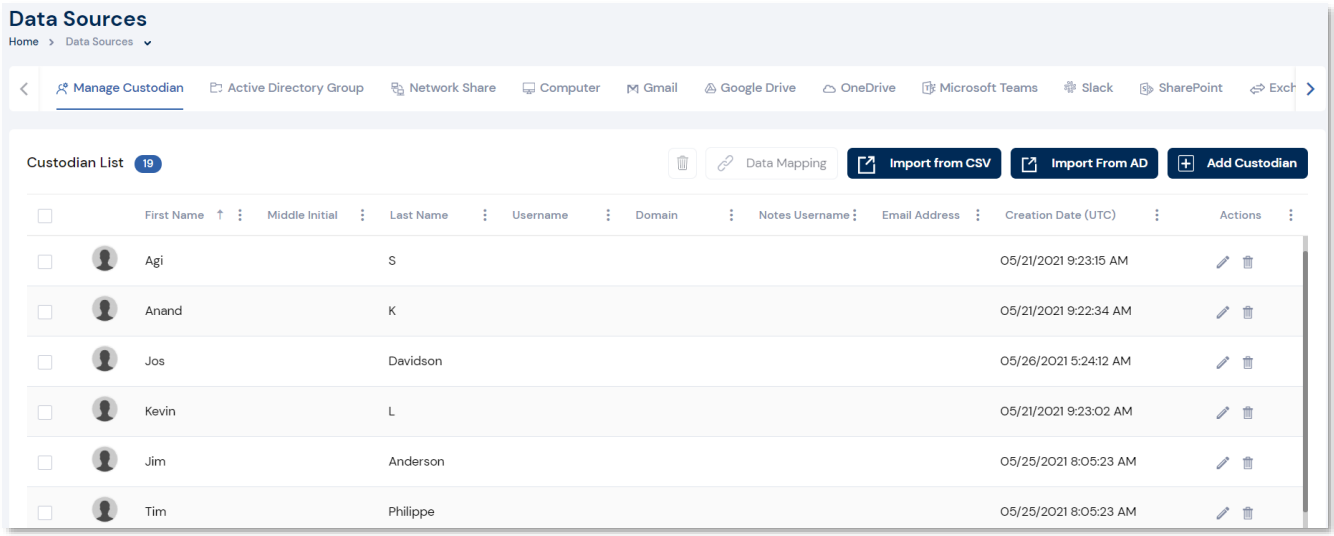
© Exterro, Inc. All rights reserved

Mapping Data to Custodians

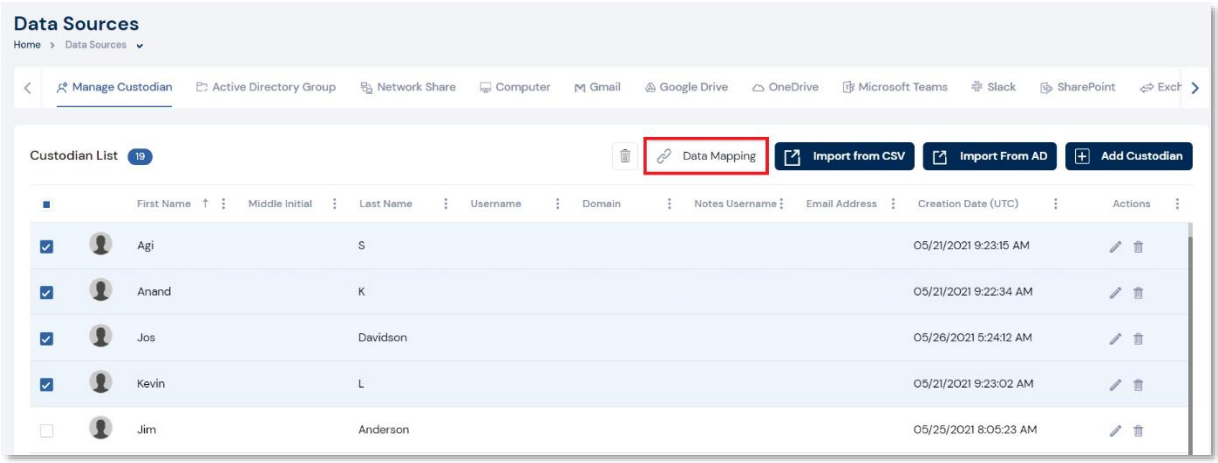
Data Mapping is the process of associating custodians with the data sources applicable for them. You can associate one or more data sources to a custodian.

To map data sources for a custodian:

1. From the home page, click **Data Sources**.
   - The **Manage Custodian** page is displayed.

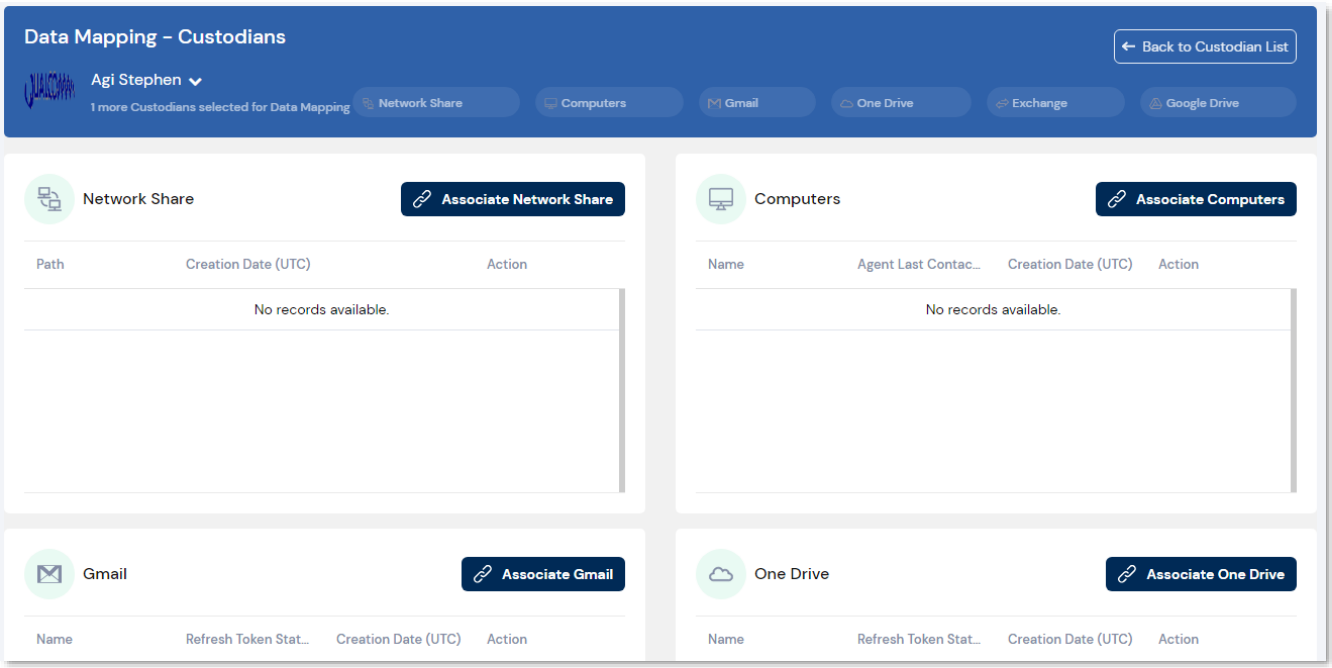


2. Select the required custodians from the list.



© Exterro, Inc. All rights reserved

3. Click **Data Mapping**.
   - The **Data Mapping – Custodians** page is displayed.



4. Click the associate data source icon for the required data source.
   - The map data source pop-up is displayed.

5. Select any of the existing data source.
6. Click **Save**.

Notes:

- You can also create a new data source by clicking the **Add** button from the map data source pop-up.
- You can associate a custodian to more than one data source types.
- Additionally, while reviewing you can view two additional columns to see which custodian is associated to a document (Custodian) as well as other custodians who have held a deduplicated document (AllCustodian). While these columns have been introduced, the review mode will not relist any deduplicated documents for each custodian, rather just the first custodian associated.

© Exterro, Inc. All rights reserved

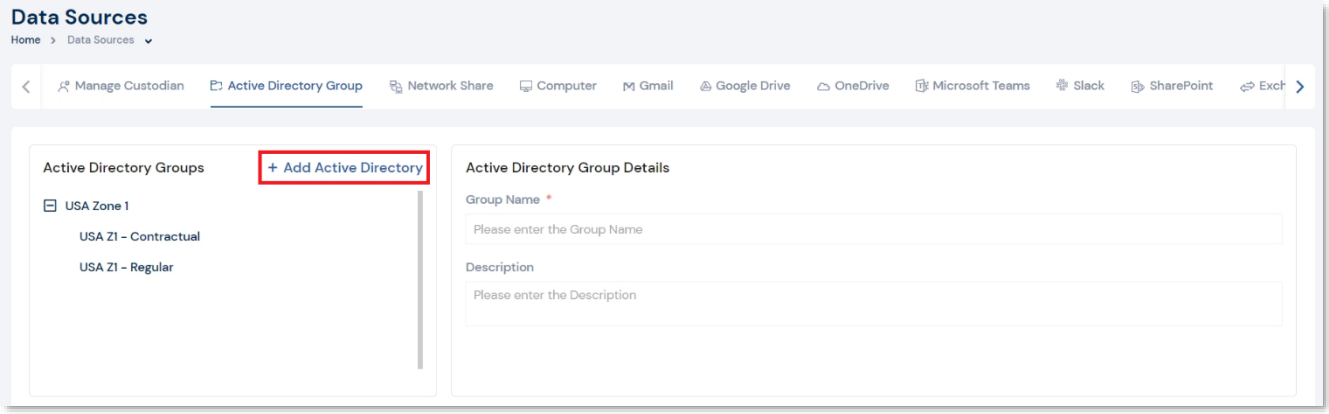
Managing Active Directory Group

FTK Central allows you to group more than one Active Directories under one group to organize it easily. Linking multiple active directories with similar requirements under one group makes it easier to provide permissions and manage them.

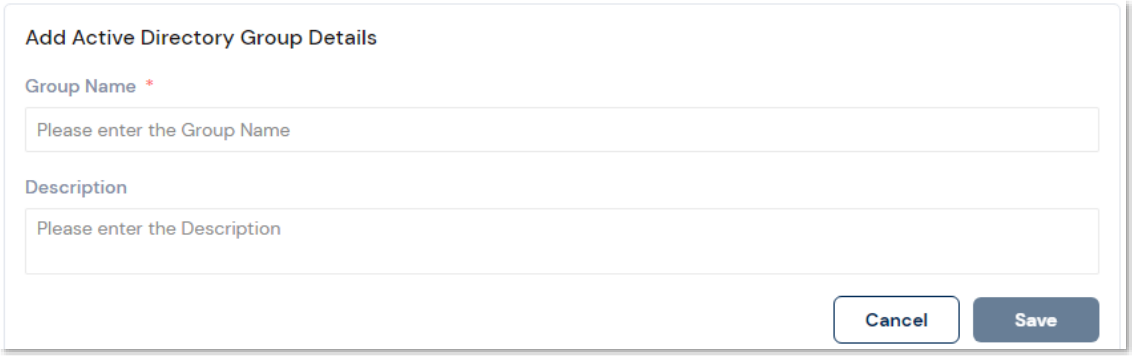
Adding Active Directory Group

To add an active directory group:

1. From the home page, click **Data Sources**.
2. Navigate to the **Active Directory Group** tab.
3. Click **Add Active Directory**.



- The **Add Active Directory Group Details** page is displayed.



4. Provide a name for the active directory in **Group Name**.

© Exterro, Inc. All rights reserved

5. Provide a **Description** for the group.
6. Click **Save**.

Notes:

- From the Active Directory Groups section, you can select a group and click **Add** against it to add a sub-group to it.
- From the Active Directory Groups section, you can select a group/sub-group and click **Edit** to update the information.
- From the Active Directory Groups section, you can select a group/sub-group and click **Delete** to remove it.

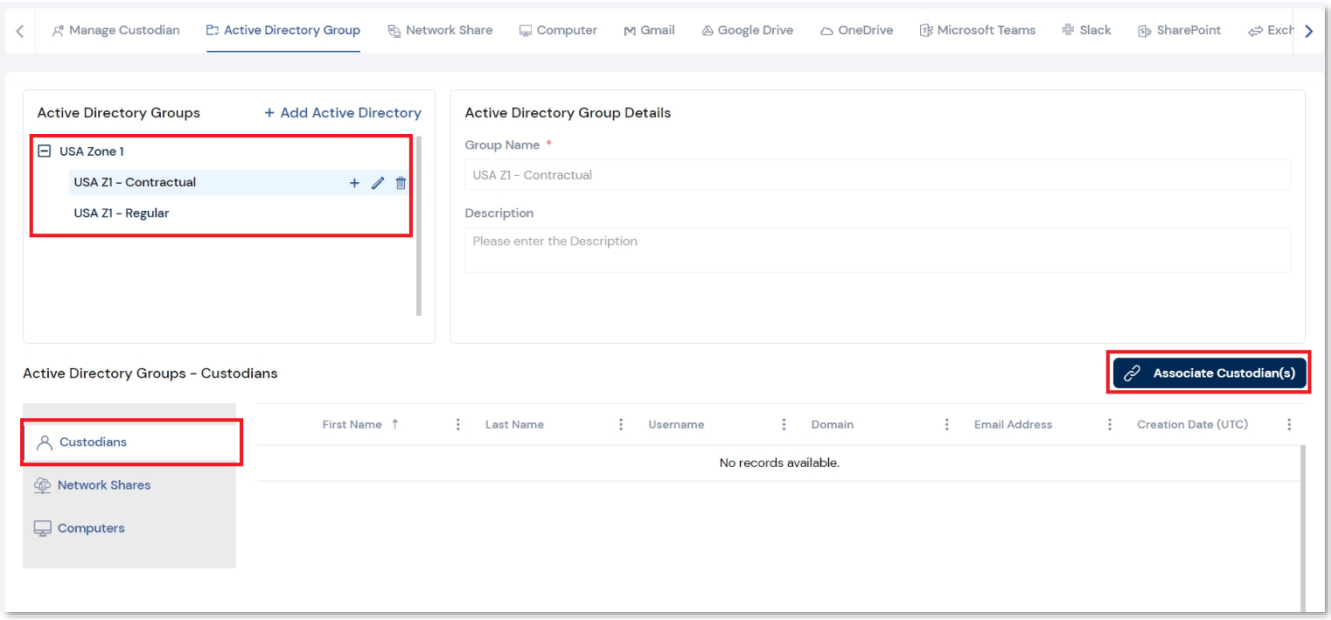
© Exterro, Inc. All rights reserved

Associating Active Directories

Associating custodians with active directory group

To associate custodians to an active directory group:

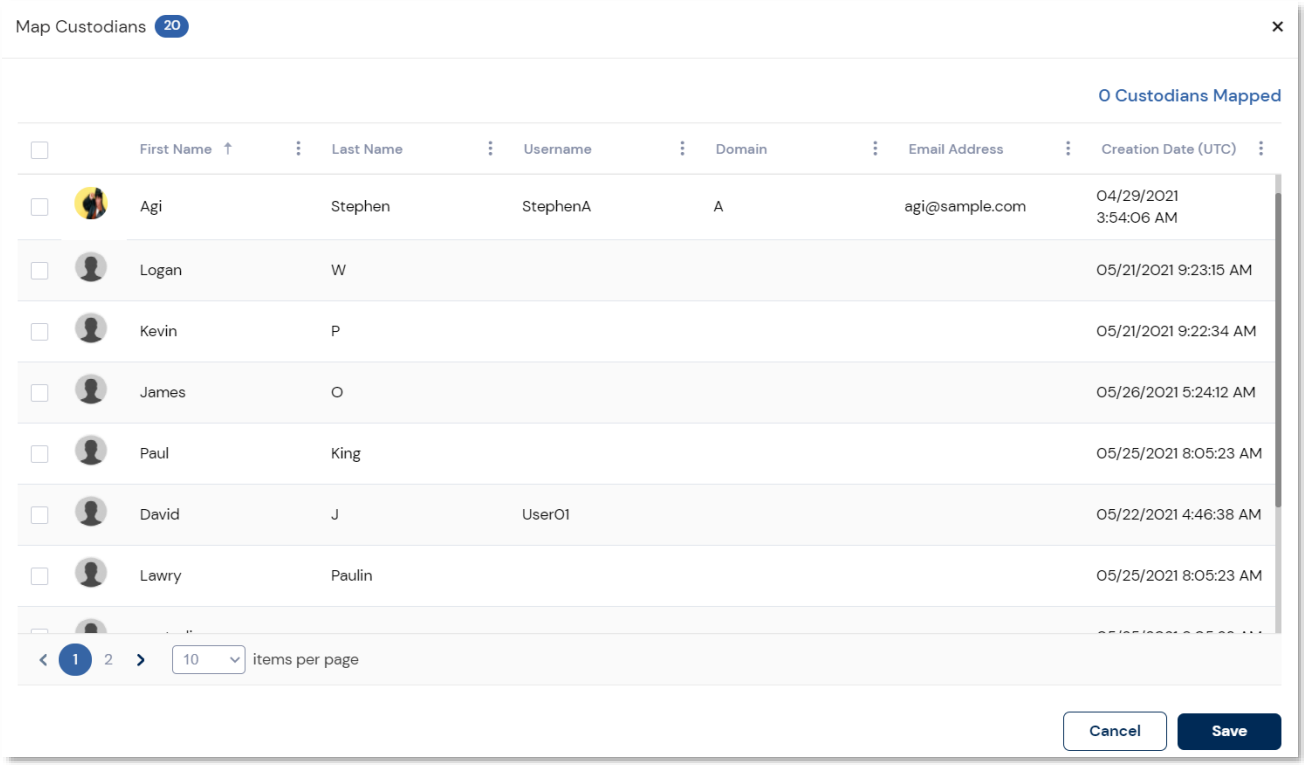
1. From the home page, click **Data Sources**.
2. Navigate to the **Active Directory Group** tab.
3. Click on the required active directory group/sub-group.



4. Click **Associate Custodian(s)**.

© Exterro, Inc. All rights reserved

- The **Map Custodians** pop-up is displayed.



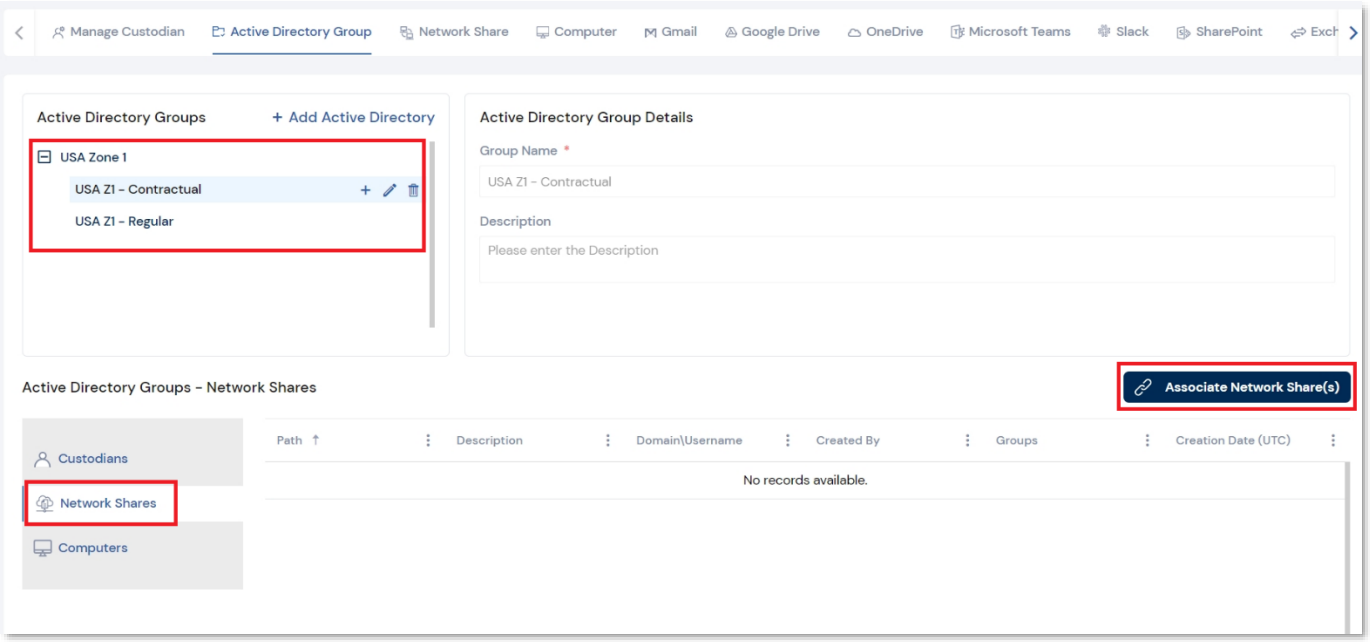
5. Select the required custodians by enabling the checkbox against them.
6. Click **Save**.

© Exterro, Inc. All rights reserved

Associating computers with active directory group

To associate computers to an active directory group:

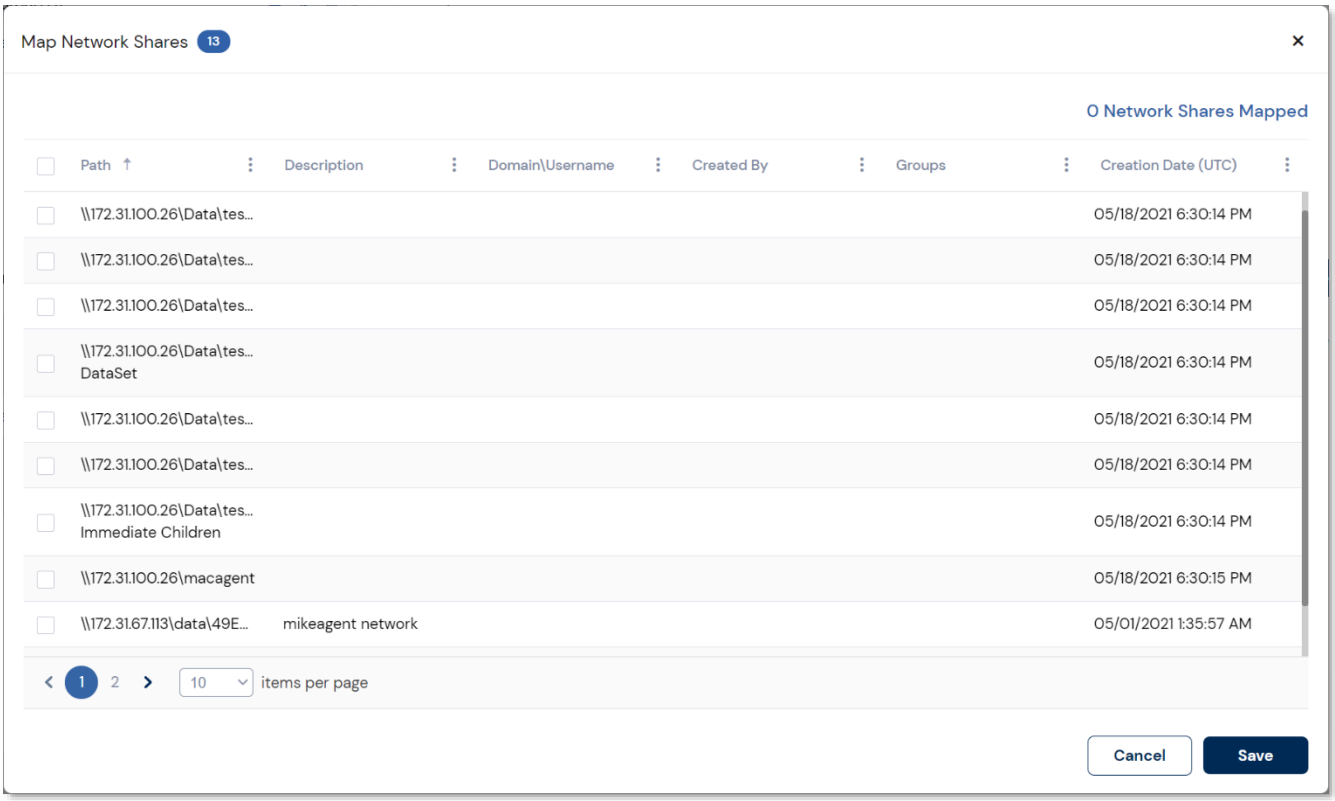
1. From the home page, click **Data Sources**.
2. Navigate to the **Active Directory Group** tab.
3. Click on the required active directory group/sub-group.



4. Click **Associate Network Share(s)**.

© Exterro, Inc. All rights reserved

- The **Map Network Shares** pop-up is displayed.



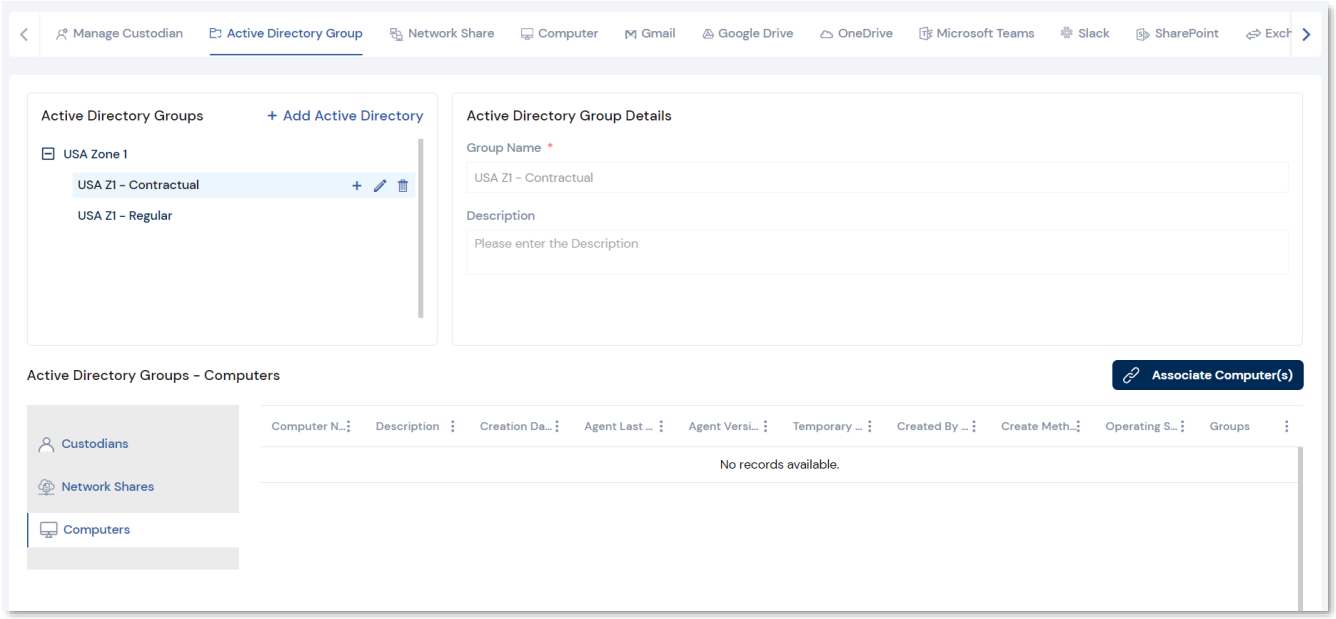
5. Select the required custodians by enabling the checkbox against them.
6. Click **Save**.

© Exterro, Inc. All rights reserved

Associating custodians with active directory group

To associate custodians to an active directory group:

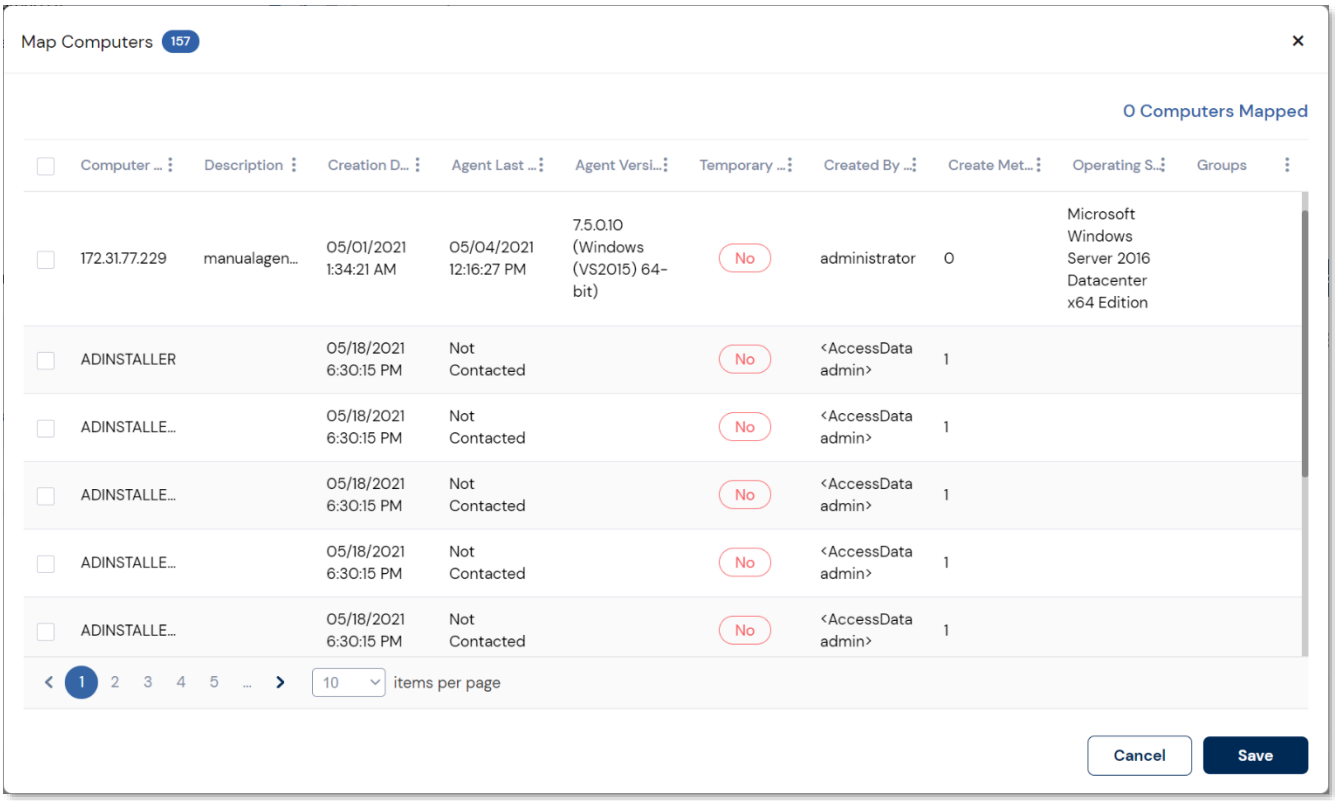
1. From the home page, click **Data Sources**.
2. Navigate to the **Active Directory Group** tab.
3. Click on the required active directory group/sub-group.



4. Click **Associate Computer(s)**.

© Exterro, Inc. All rights reserved

- The **Map Computers** pop-up is displayed.

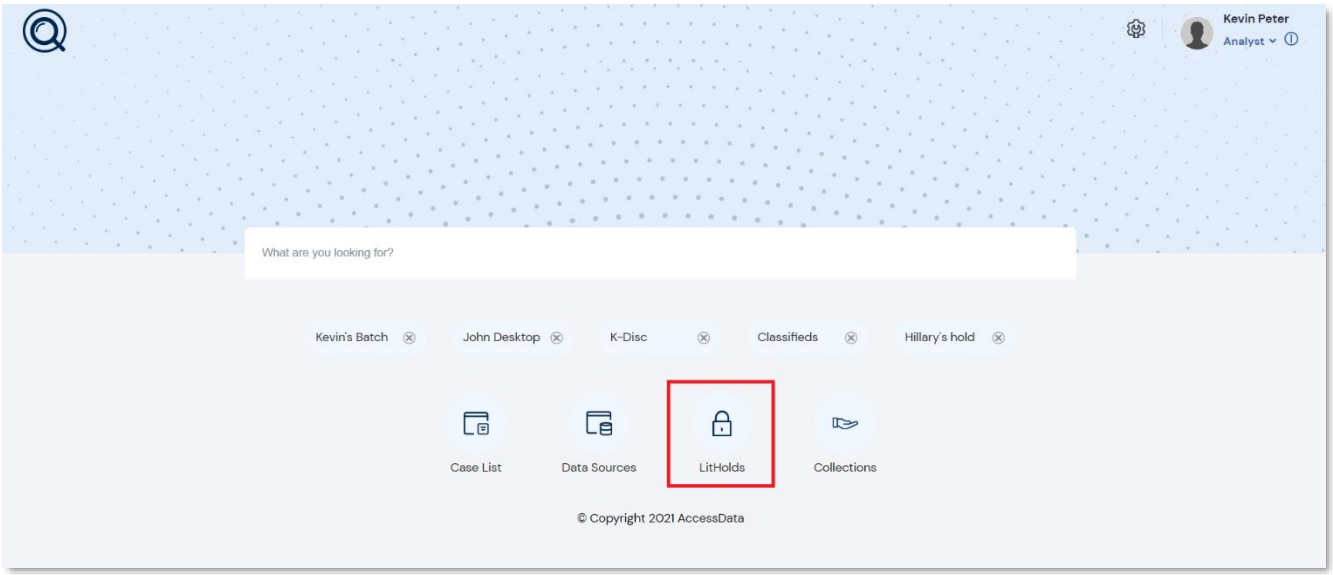


5. Select the required custodians by enabling the checkbox against them.
6. Click **Save**.

© Exterro, Inc. All rights reserved

LitHolds

The Litigation Hold (LitHolds) is a notification management system that efficiently handles all aspects and stages of the litigation hold process within your enterprise. The lit hold features offer email notification templates and interview question templates, reports, histories, reminders, acceptance records, interview response records, and centralizes the relevant data in one location.



© Exterro, Inc. All rights reserved

Elements of LitHolds

Configuring LitHolds	• General LitHold Configuration
	• Managing IT Staff
	  ○ Adding IT Staff
	  ○ Adding IT Staff Group
	  ○ Mapping users to IT Staff Group
	• Managing Approver
	  ○ Adding Approver Group
	  ○ Mapping users to Approver Group
	• Adding Email Templates
	• Documents Templates
	  ○ Creating document templates
	  ○ Adding document to templates
	• Creating Interview Templates

Managing LitHolds	• Creating LitHolds • Viewing LitHolds • Editing LitHolds • Deleting LitHolds • Approving LitHolds • Deactivating LitHolds • Activating LitHolds • Resubmitting LitHolds • Viewing Custodians Responses
Generating Reports	• Hold Summary Report • Custodian Details Report • Hold Details Report • Hold Custodians Report

© Exterro, Inc. All rights reserved

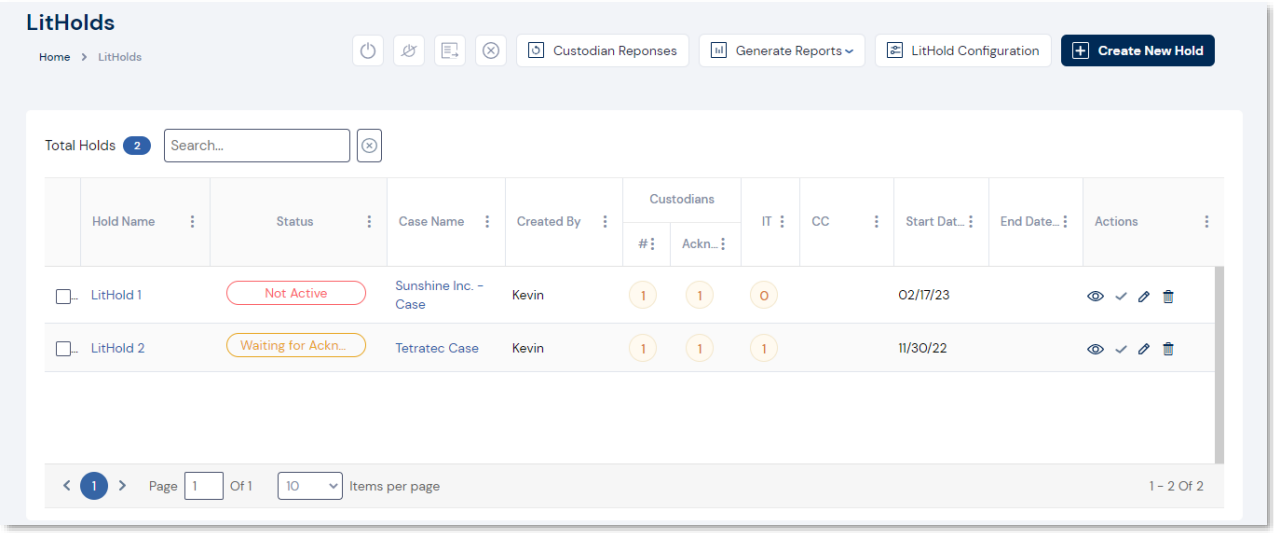
Configuring LitHolds

Before you create litigation holds, you need to configure the following Litigation Hold general settings.

LitHold Configuration

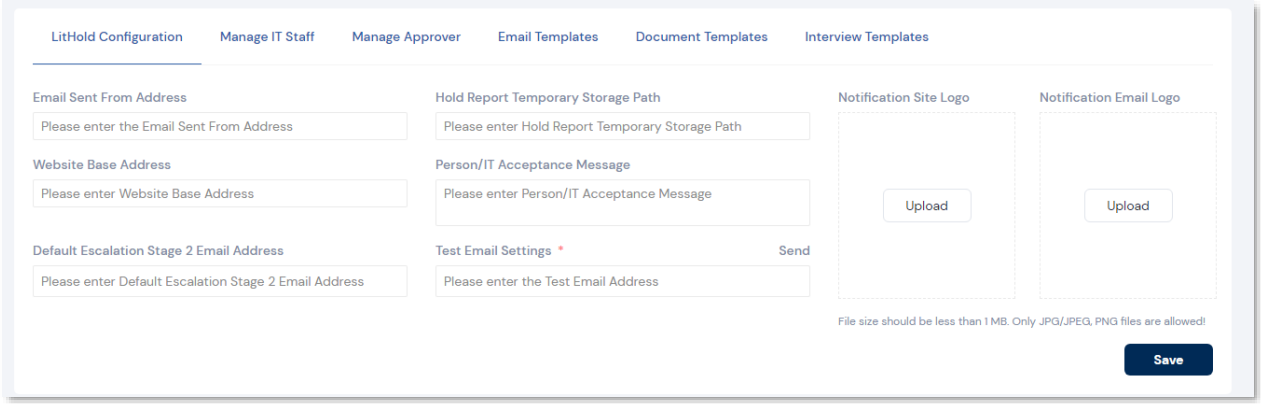
To configure the general lithold settings:

1. From the home page, click **LitHolds**.
   - The Manage page of LitHolds is displayed.



2. Click **LitHold Configuration**.
   - The **LitHold Management** page is displayed.

© Exterro, Inc. All rights reserved



3. Provide the sender's email address in **Email Sent From Address** field.
4. Provide the temporary storage location for reports data in **Hold Report Temporary Storage Path** field.
5. Click **Upload** and choose the **Notification Site Logo** to be uploaded.
6. Click **Upload** and choose the **Notification Email Logo** to be uploaded.
7. Provide the base address of the server running Lit Hold in **Website Base Address**.

Note: The base address includes the protocol and server name, but not the application or the page that is currently displayed. For example, http://<server_name_or_IP_address>/.

8. Provide the **Person/IT Acceptance Message**.

Note: This message is displayed at the bottom of the Person and IT Staff Hold Notification pages, just above the Accept button. This acts as an acknowledgement message, for example, "By clicking accept you agree to the terms set forth."

9. Provide the **Default Escalation Stage 2 Email Address**.

Notes: You can set two levels of escalation policies for person hold acceptance.

- Stage One: If a custodian doesn't accept the hold within a number of specified days, the first escalation email is sent to their manager.
- Stage Two: After a specified number of days, the next escalation is sent to the email address specified in **Default Escalation Stage 2 Email Address** field.

© Exterro, Inc. All rights reserved

10. Provide an email address in **Test Email Settings** and click **Send** to check if you can receive emails.
11. Click **Save**.

© Exterro, Inc. All rights reserved

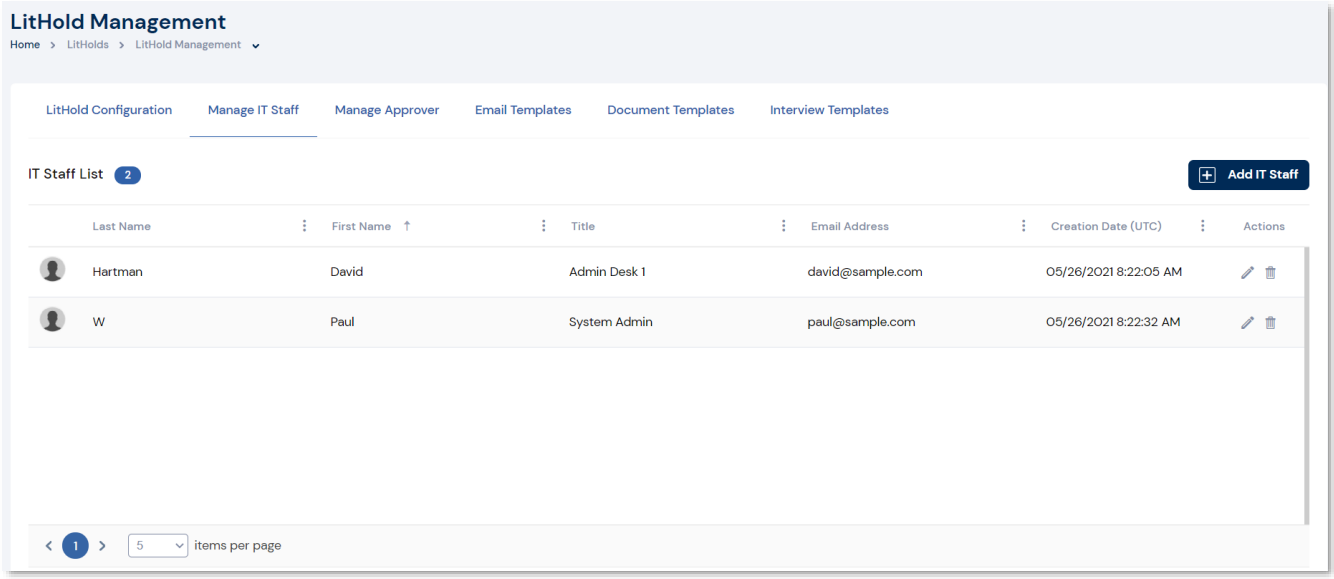
Managing IT Staff

The IT Staff are those individuals in an organization that work with the organization's file aging. During a lit hold, they can receive notifications about lit holds.

Adding IT Staffs

To add an IT staff:

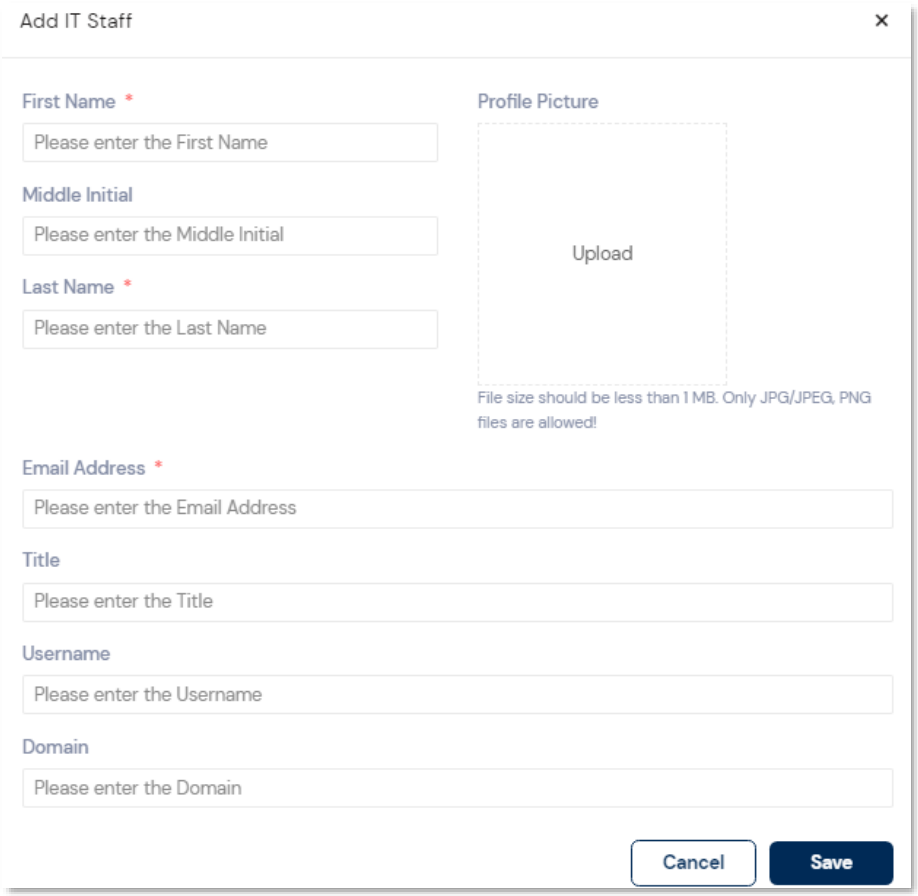
1. From the home page, click **LitHolds**.
2. Click **LitHold Configuration**.
3. Navigate to **Manage IT Staff** tab.



4. Click **Add IT Staff**.

© Exterro, Inc. All rights reserved

- The **Add IT Staff** pop-up is displayed.



5. Enter the First Name, Middle Initial and Last Name of the IT Staff.
6. Enter the **Email Address**, **Title** and **Username** of the IT Staff.
7. Enter the **Domain**.
8. Click **Upload** and choose the **Profile Picture** of the IT Staff.
9. Click **Save**.

Notes:

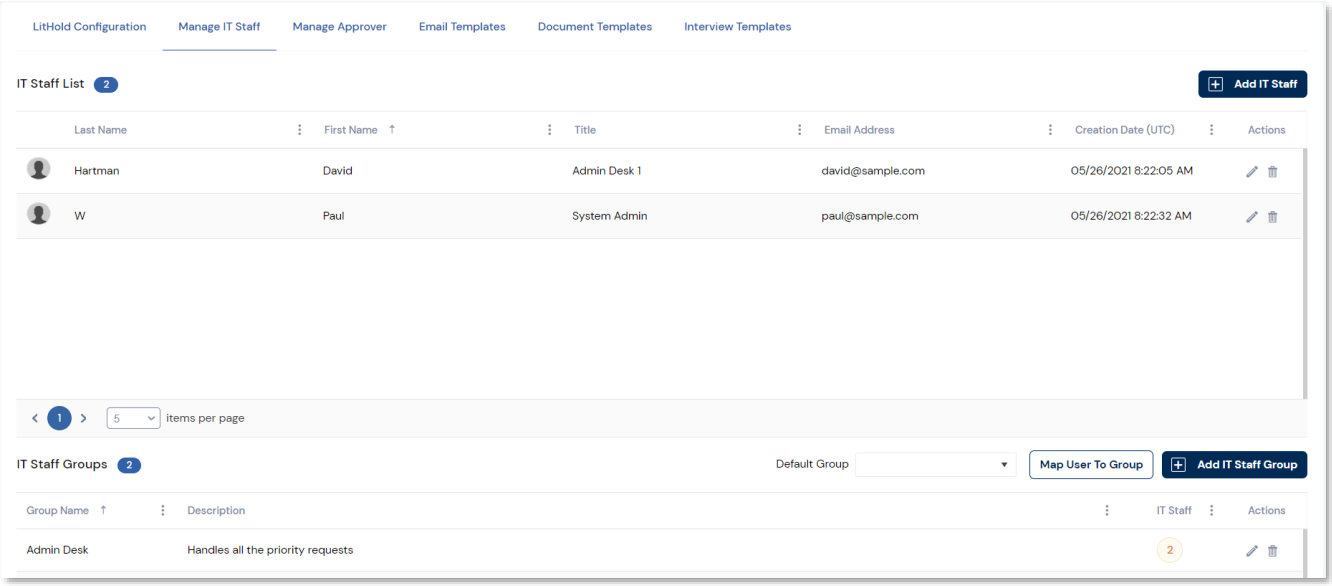
- From the IT Staff list, you can click **Edit** against the IT Staff member to edit the staff information.
- From the IT Staff list, you can click **Delete** against the IT Staff member to delete the staff.

© Exterro, Inc. All rights reserved

Adding IT Staff Groups

To add an IT staff group:

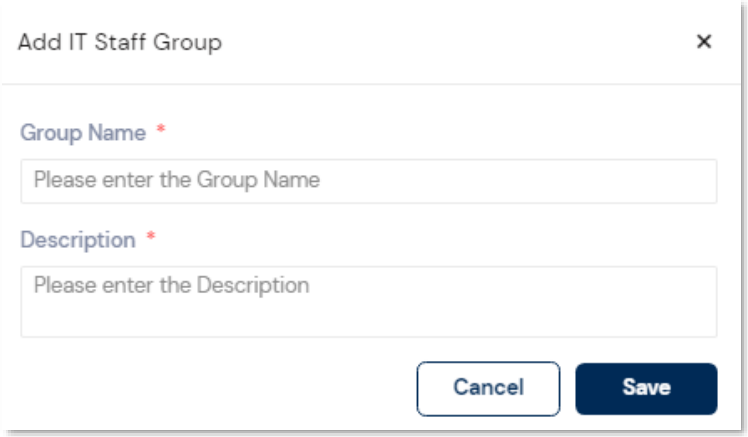
1. From the home page, click **LitHolds**.
2. Click **LitHold Configuration**.
3. Navigate to **Manage IT Staff** tab.



4. Click **Add IT Staff Group**.

© Exterro, Inc. All rights reserved

- The **Add IT Staff Group** pop-up is displayed.



5. Enter the Group Name.
6. Enter the group Description.
7. Click **Save**.

Notes:

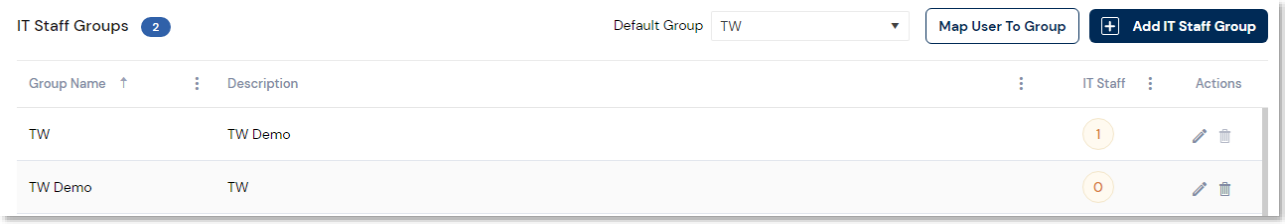
- From the IT Staff Groups list, you can click **Edit** against the IT Staff group to edit it.
- From the IT Staff Groups list, you can click **Delete** against the IT Staff member to delete it.

© Exterro, Inc. All rights reserved

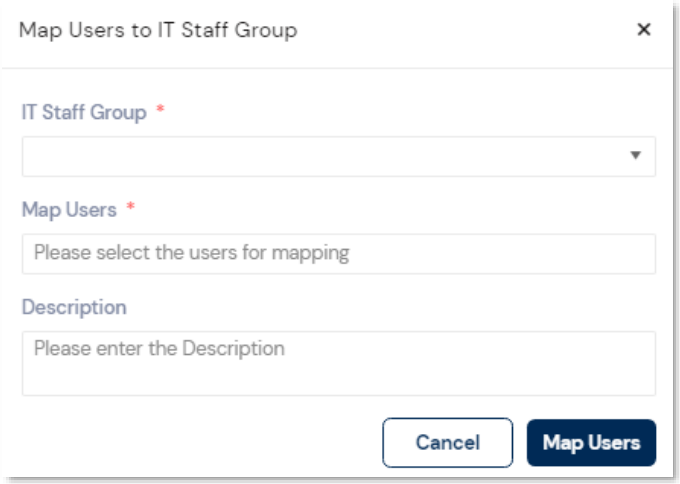
Mapping users to IT Staff Group

To map users to IT staff group:

1. From the home page, click **LitHolds**.
2. Click **LitHold Configuration**.
3. Navigate to **Manage IT Staff** tab.



4. Click **Map User To Group**.
   - The **Map Users to IT Staff Group** pop-up is displayed.



5. Select the IT Staff Group from the drop-down.
6. Select the users from Map Users field.
7. Provide a Description.
8. Click **Map Users**. The newly created IT Staff group will be displayed.

Note: You can choose a default group from the list of groups displayed upon clicking the **Default Group** option.

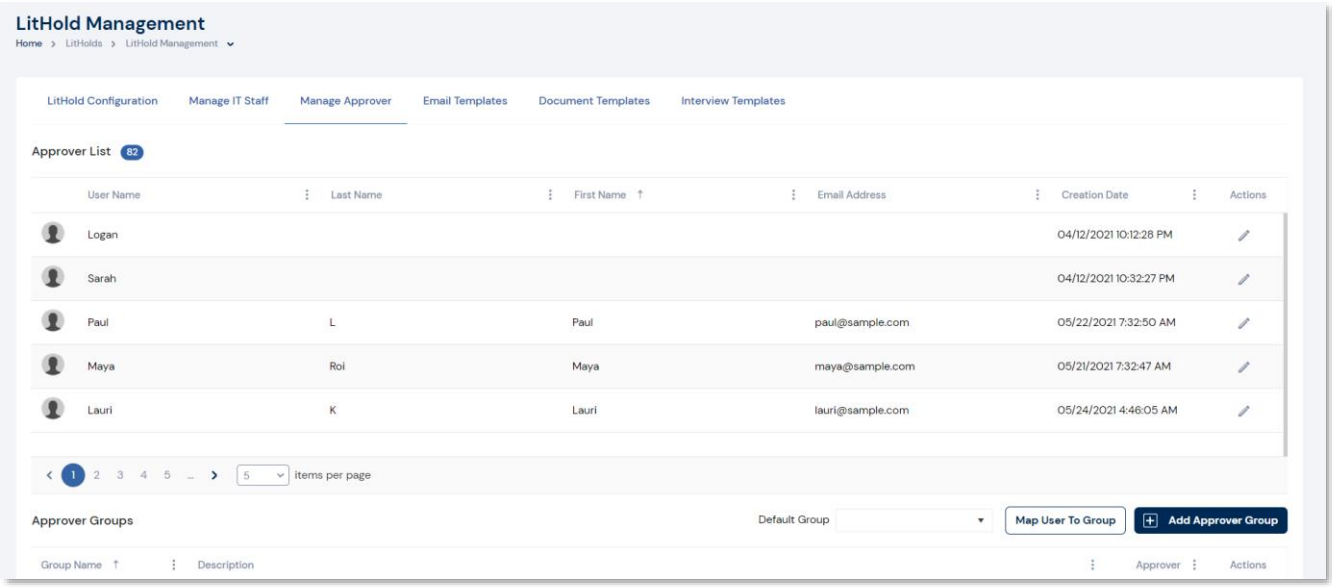
© Exterro, Inc. All rights reserved

Managing Approver

Adding Approver Groups

To add approver group:

1. From the home page, click **LitHolds**.
2. Click **LitHold Configuration**.
3. Navigate to **Manage Approver** tab.

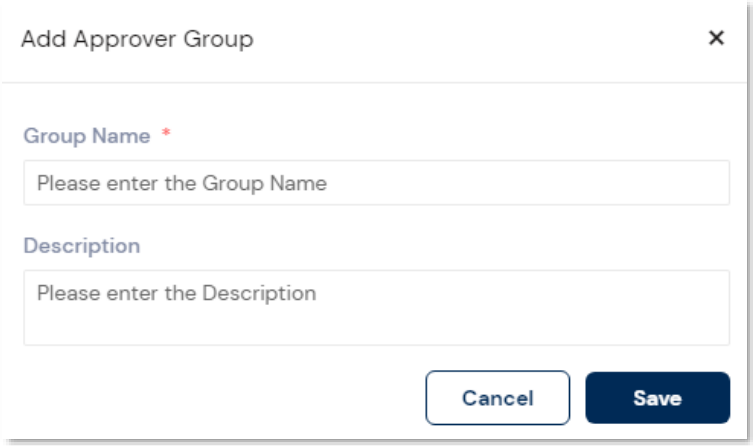


Note: You can click **Edit** against the approver to edit it.

4. Click **Add Approver Group**.

© Exterro, Inc. All rights reserved

- The **Add Approver Group** pop-up is displayed.



5. Provide a **Group Name** and **Description**.
6. Click **Save**.

Notes:

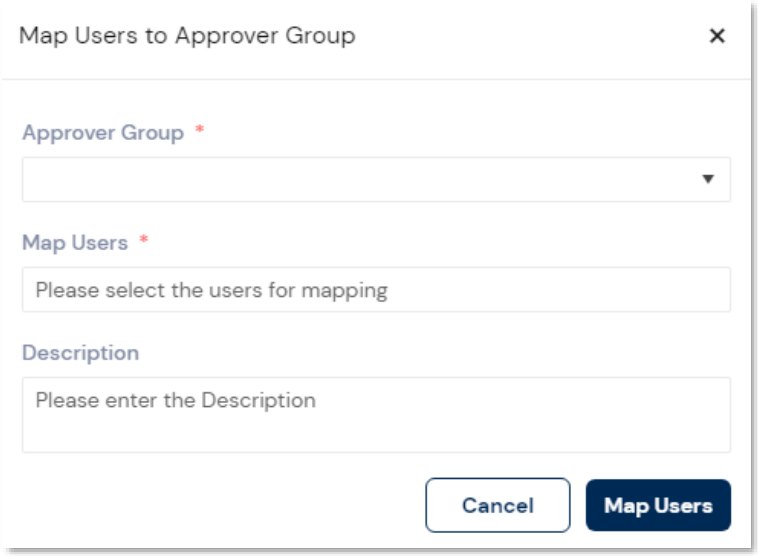
- From the Approvers group list, you can click **Edit** against the approver group to edit it.
- From the Approvers group list, you can click **Delete** against the approver group to delete it.

© Exterro, Inc. All rights reserved

Mapping users to Approver Group

To map users to approver group:

1. From the home page, click **LitHolds**.
2. Click **LitHold Configuration**.
3. Navigate to **Manage Approver** tab.
4. Click **Map User To Group**.
   - The **Map Users to Approver Group** pop-up is displayed.



5. Select the Approver Group from the drop-down.
6. Select the users from Map Users field.
7. Enter the Description.
8. Click **Map Users.**

© Exterro, Inc. All rights reserved

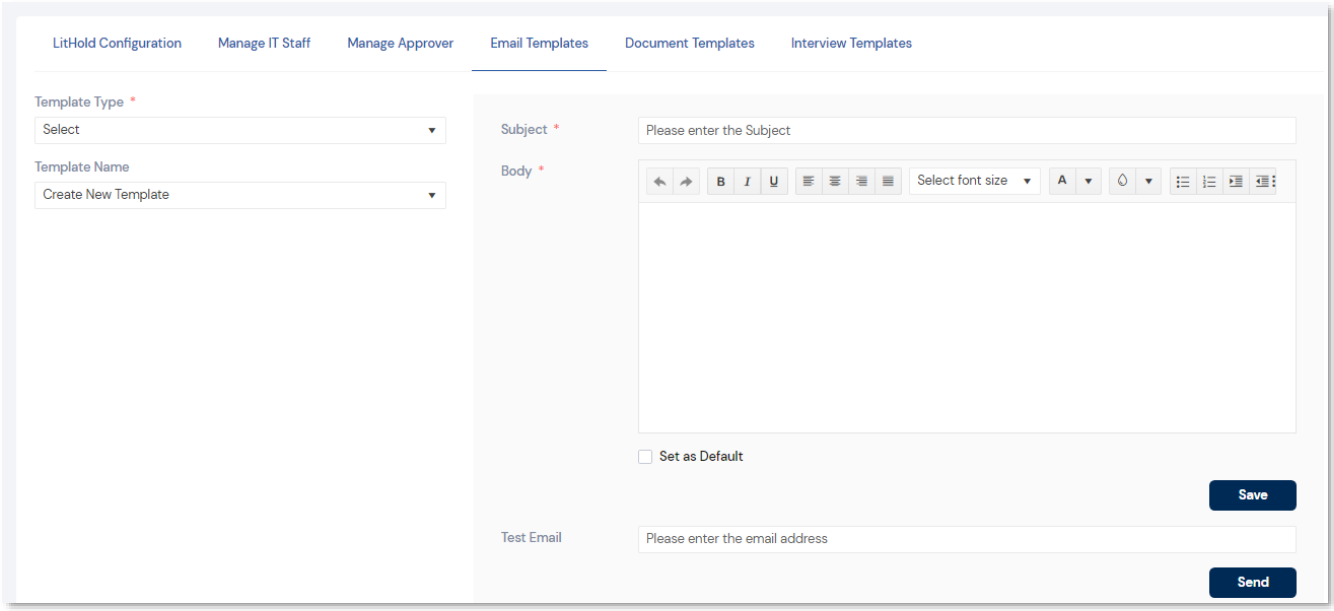
Email Templates

Lit holds send email notifications to custodians, IT Staff, and the Hold Approver informing them of the status and events of the lit hold. When creating a lit hold, you must specify the text of these email notifications. To expedite this process, you can store and use text in email templates. When you create a lit hold, you can choose the template that you want to use.

Adding email templates

To create a new email template:

1. From the home page, click **LitHolds**.
2. Click **LitHold Configuration**.
3. Navigate to **Email Templates** tab.



© Exterro, Inc. All rights reserved

- Select any of the following **Template Type**.

Email Template Type	Purposes
Approval	Sent to the litigation hold manager for their approval.
Hold Acceptance	Sent to the Custodian describing the parameters of the hold, and linking them to the Landing Page where they can view the Stop aging Letters and acknowledge receipt of the litigation hold.
Hold Reminder	Reminds the Custodian that they are still involved a litigation hold.
Hold Termination	Notifies the Custodian that their participation in the litigation hold is no longer necessary.
Person Questions Changed Reminder	You may change the interview questions of a hold. This is the email template that will remind Custodians of the change in interview questions and that they need to re-answer them.
Stop Aging Acceptance	Sent to the IT Staff members to accept the corresponding LitHold.
Stop Aging Reminder	Reminds the IT Staff members that they are still involved a litigation hold.
Stop Aging Termination	Notifies the IT Staff members that their participation in the litigation hold is no longer necessary.
Hold Escalation Stage One	When a custodian doesn't accept the hold within a number of specified days, the first escalation email is sent to their manager. This is the email template for a Stage One Escalation.
Hold Escalation Stage Two	After a specified number of days, the next escalation is sent to the specified email address. This is the email template for a Stage Two Escalation.
Self Collection Notification	
Self Collection Reminder	
Self Collection Termination	

© Exterro, Inc. All rights reserved

4. Select an existing template or **Create New Template** from the **Template Name** drop-down.
5. Enter the email **Subject** for the email template.
6. Enter the email **Body** for the email template.

Note: To set this email template as default for the selected Template type, you can enable **Set as Default** option.

7. Click **Save**.

Note: You can provide the **Test Email** address and click **Send** to test if the email notifications are received as intended.

© Exterro, Inc. All rights reserved

Documents Templates

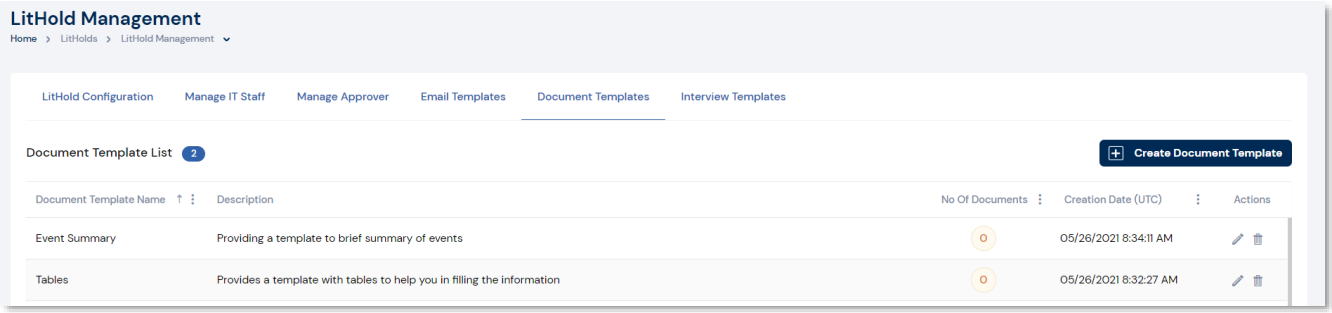
These are any supporting documents that you want to attach to the litigation hold notification emails.

To do so, you have to first create a document template and add a document to it.

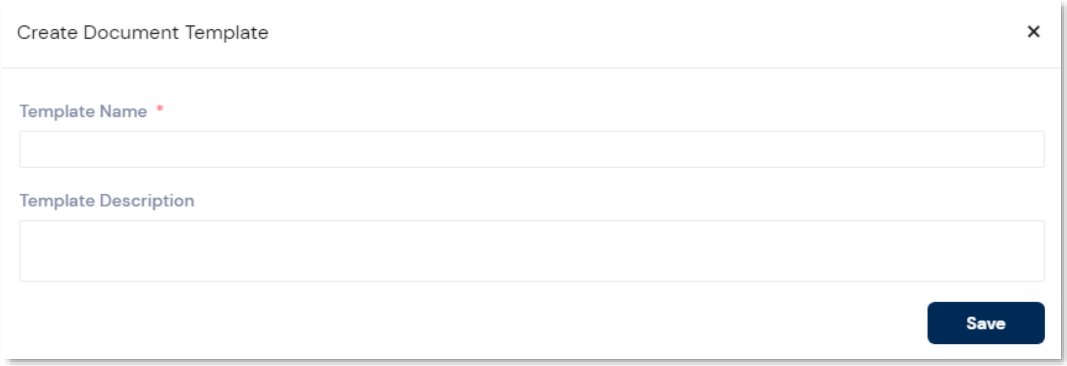
Creating document templates

To create a document template:

1. From the home page, click **LitHolds**.
2. Click **LitHold Configuration**.
3. Navigate to **Document Templates** tab.



4. Click **Create Document Template**.
   - The **Create Document Template** pop-up is displayed.



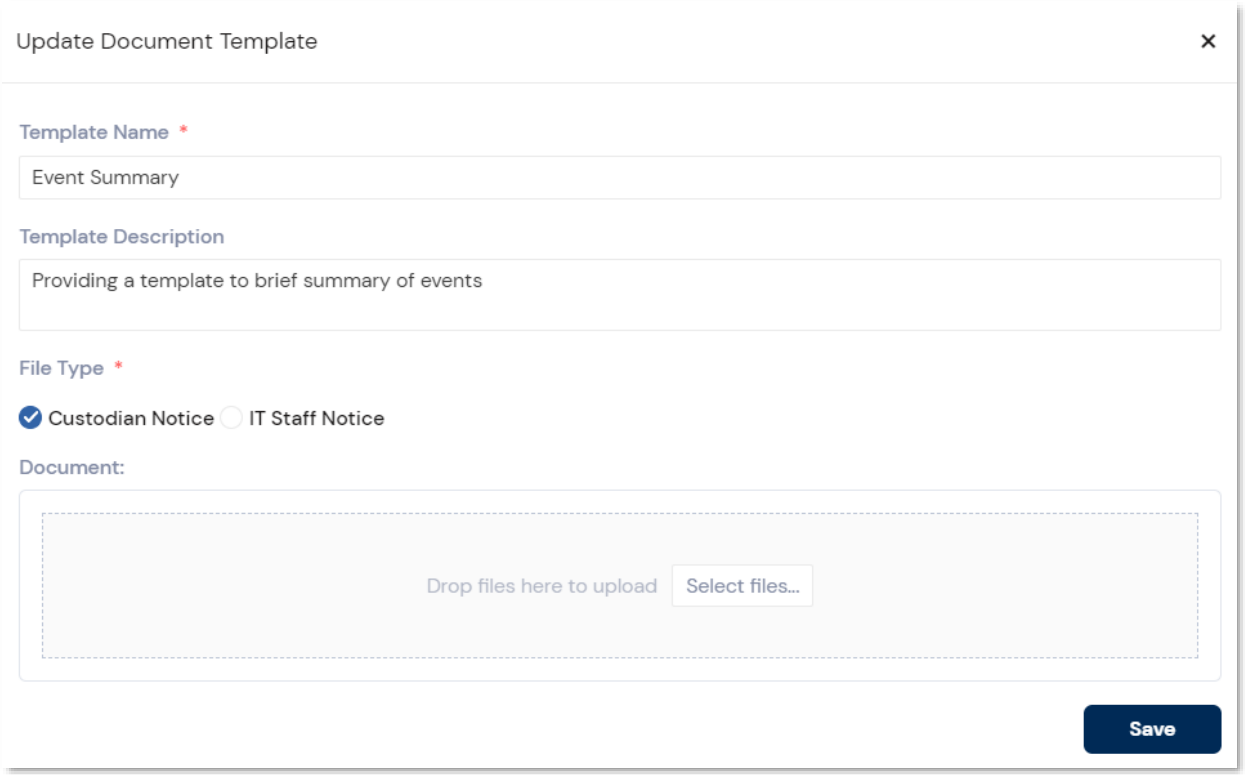
5. Enter the **Template Name**.
6. Enter the **Template Description**.
7. Click **Save**.

© Exterro, Inc. All rights reserved

Adding document to templates

To add a document to template:

1. From the home page, click **LitHolds**.
2. Click **LitHold Configuration**.
3. Navigate to **Document Templates** tab.
4. Click **Edit** against the document template
   - The **Update Document Template** pop-up is displayed.



© Exterro, Inc. All rights reserved

5. Select any one **File Type** as explained below**:**
6. **Custodian Notice**: To attach the documents and questionnaires corresponding to the Custodians.
7. **IT Staff Notice**: To attach the documents and questionnaires corresponding to the IT staffs.
8. Click **Select files** to upload the file.
9. Click **Save**.

Note: From the Document Template list, you can click **Delete** against the document template to delete it.

© Exterro, Inc. All rights reserved

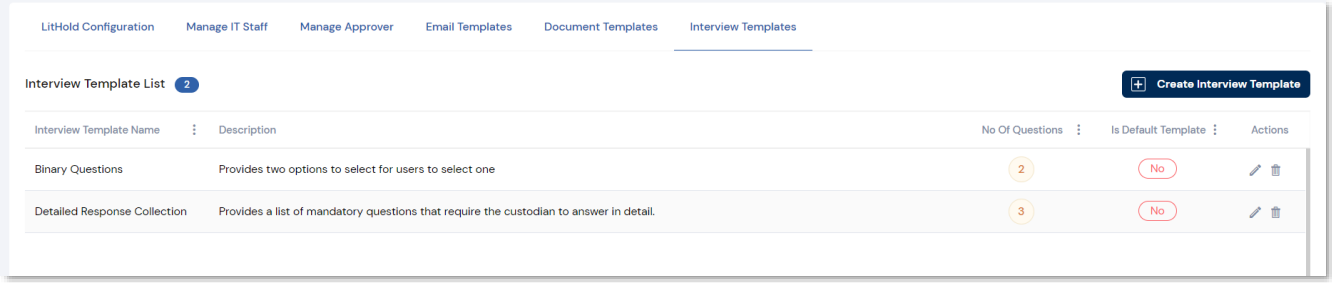
Interview Templates

When you create a lit hold, you have the option of specifying interview questions. These interview questions are given to custodians when they accept a lit hold.

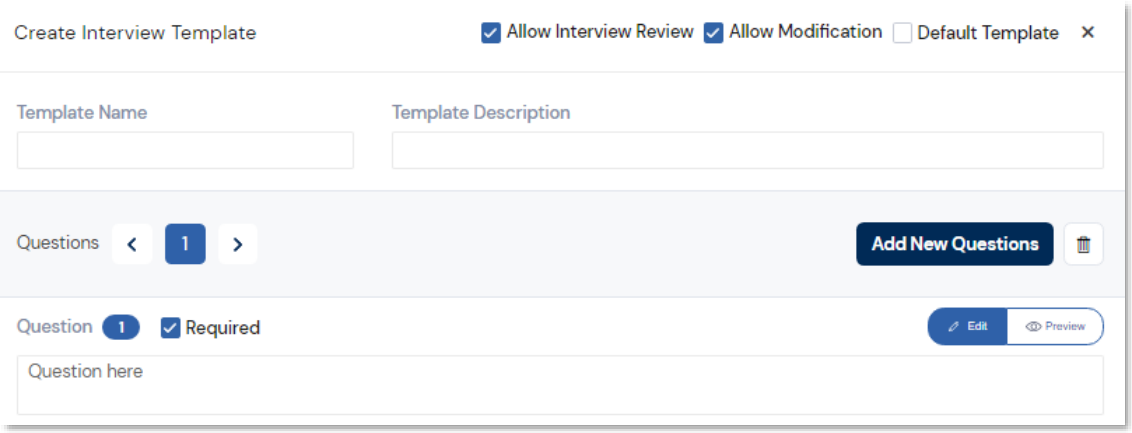
Creating Interview templates

To create an interview template:

1. From the home page, click **LitHolds**.
2. Click **LitHold Configuration**.
3. Navigate to **Interview Templates** tab.



4. Click **Create Interview Template**.
   - The **Create Interview Template** pop-up is displayed.



5. Enable the **Allow Interview Review** to allow custodians to review the Interview after completing.

© Exterro, Inc. All rights reserved

6. Enable **Allow Modification** option to allow custodians to modify the Interview after completing.

Warning: This option will be applicable only when the **Allow Interview Review** option is enabled.

7. Provide a **Template Name**.
8. Provide a **Template Description**.
9. Enter the **Question**.

Note: You can enable the **Required** checkbox to make it mandatory.

10. Select the question **Type** as required**.**
    - Text – To provide a text box for the custodian to write a response.
    - Checkbox – To request the custodian to select one or more options.
    - Radio button– To request the custodian to select any one of the options.

Note: Upon selecting Checkbox or radio button, you can click **Add** to add options or **Remove** to remove an existing option. Also, you can select **Add 'Other' option** to add other as an option.

11. Click **Add New Questions** to add another question and repeat as required.

Note: At any point, you can select a question and click **Delete** to delete it or click **Reset** to clear the complete questionnaire.

© Exterro, Inc. All rights reserved

12. Click **Create Template**.

Notes:

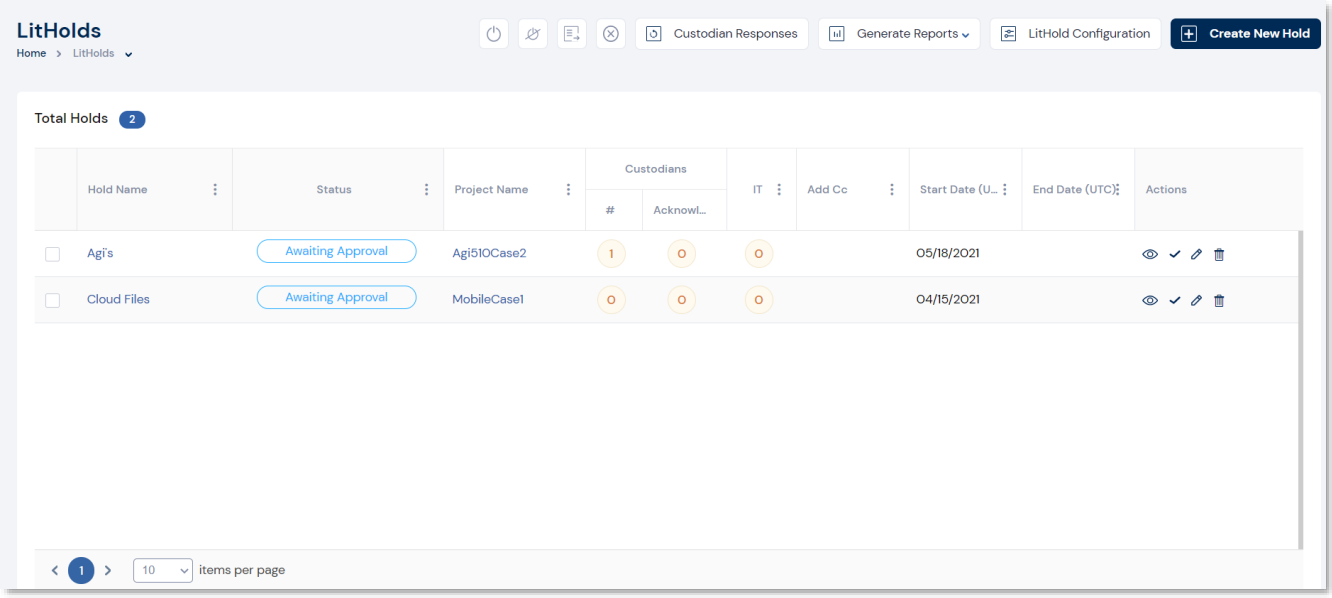
- Enable the **Default Template** option to set this as the default interview template.
- From the interview template list, you can click **Edit** against the Interview template to edit it.
- From the interview template list, you can click **Delete** against the interview template to delete it.

© Exterro, Inc. All rights reserved

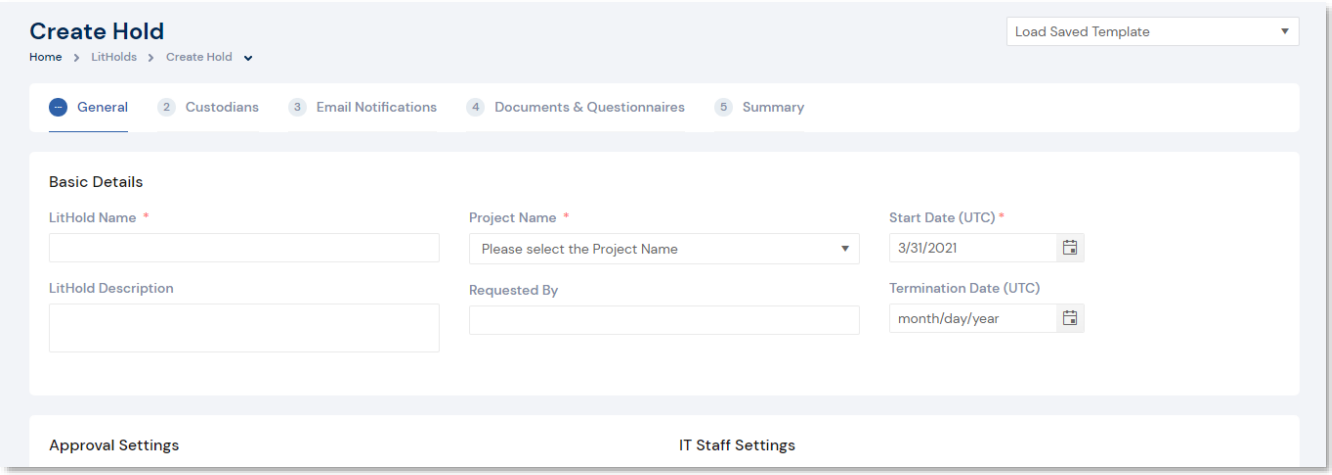
Creating LitHolds

To create a lithold:

1. From the home page, click **LitHolds**.
   - The Manage page of LitHolds is displayed.

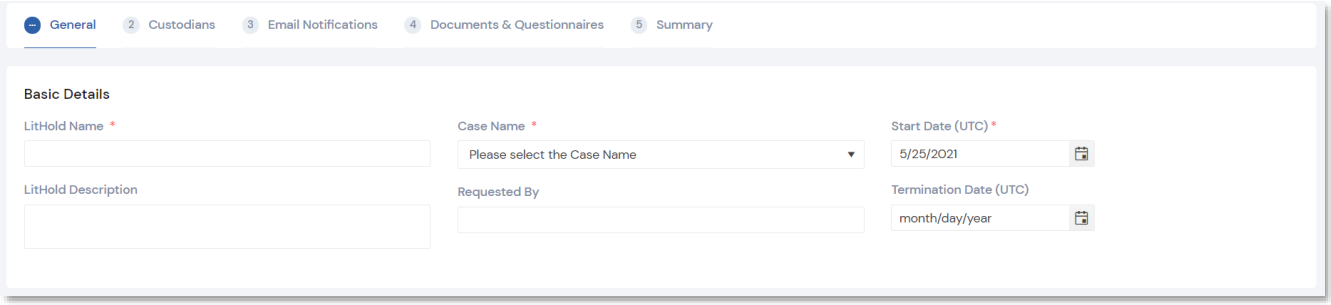


2. Click **Create New Hold**.
   - The **Create Hold** page is displayed.



© Exterro, Inc. All rights reserved

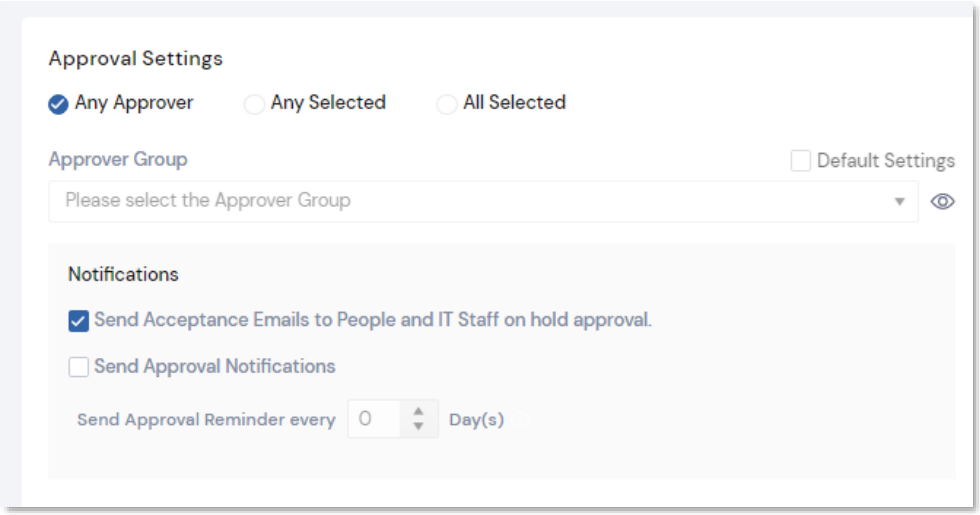
General - Basic Details



3. Enter the **LitHold Name**.
4. Select the **Case Name** from the drop-down.
5. Select the **Start Date (UTC)** of the LitHold.
6. Provide a brief about the hold in **LitHold Description**.
7. Enter the requester name in the **Requested By** field.
8. Select the **Termination Date (UTC)** to close the hold.

© Exterro, Inc. All rights reserved

General – Approval Settings



9. Select one approver from the options listed below:
   - **Any Approver** – Selecting this will allow any approver to approve the litigation hold. If you select this option, no Approval Notifications are sent.
   - **Any Selected** - Selecting this will allow any user belonging to the **Approver Group** to approve the hold.
   - **All Selected** – Selecting this will require all the users belonging to the **Approver Group** to approve the hold.

10. Select the **Approver Group** from the drop-down.

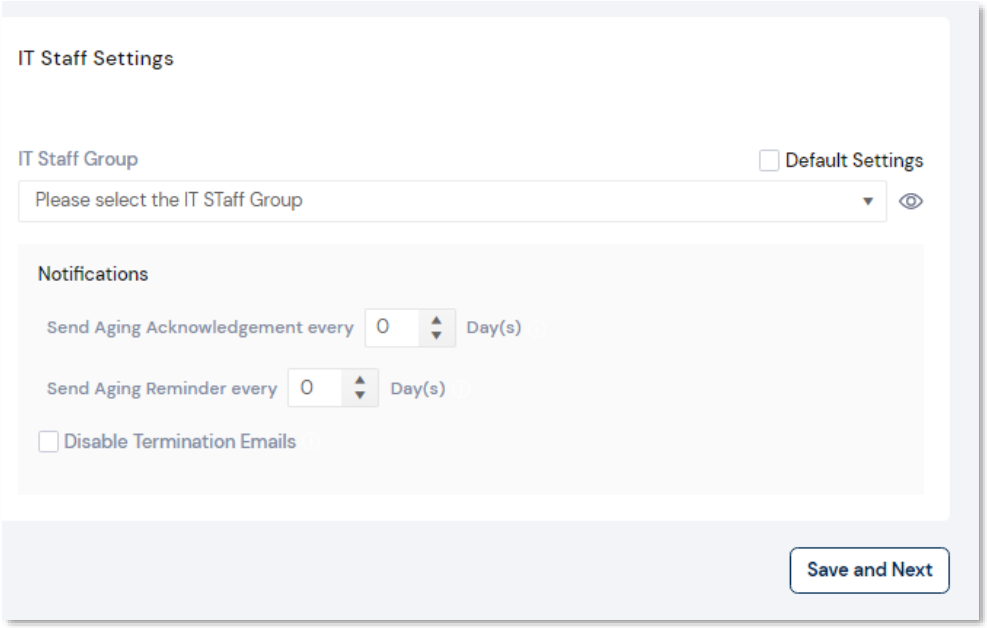
Warnings:

- The **Approver Group** option will be enabled only when the approver value is selected as 'Any Selected' or 'All Selected'.
- You can enable the **Default Settings** option to use the values that are defined in LitHold Configuration.

© Exterro, Inc. All rights reserved

11. Select the required email **Notifications** for the approver.
    - Select **Send Acceptance Emails to People and IT Staff on hold approval** to send email notifications to the hold approvers and IT Staffs.
    - Select **Send Approval Notifications** to send the hold approval notifications.
    - Set the number of days to remind the approver, against the **Send Approval Reminder every** field.

General - IT Staff Settings



12. Select the **Default Settings** to use the configured default IT staff settings.
13. Select the required **IT Staff Group** from the drop-down.

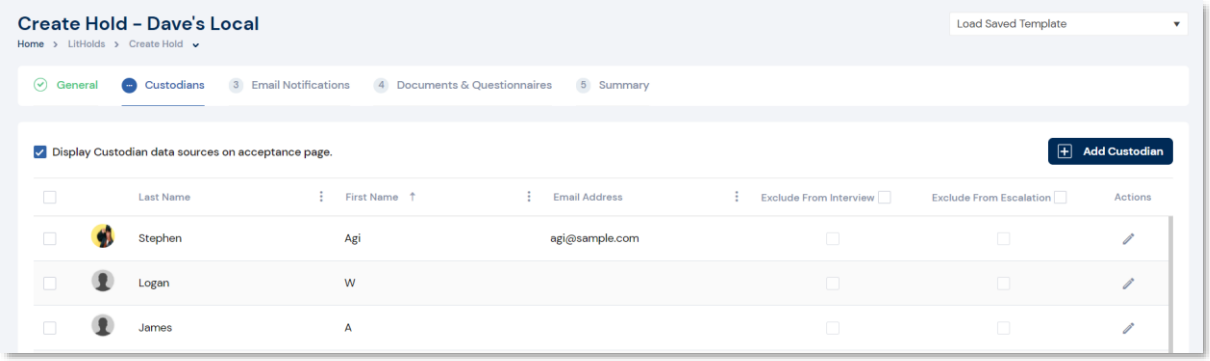
Note: IT Staffs are the individuals that you want to inform that data, for example emails and files stored on the network, must be preserved during the hold. These individuals are notified when a LitHold is created and must acknowledge that they have a role in the lit hold. They are also notified with reminders and when the lit hold is terminated.

© Exterro, Inc. All rights reserved

14. Select the number of days against **Send Aging Acknowledgement every** to resend the hold to members who have not acknowledged every number of specified days.
- Select the number of days against **Send Aging Reminder every** to send the reminder email notification.
- Enable the **Disable Termination Emails** option to disable the termination email notifications that is sent to the members of the IT Staff group.

15. Click **Save and Next**.

Custodians



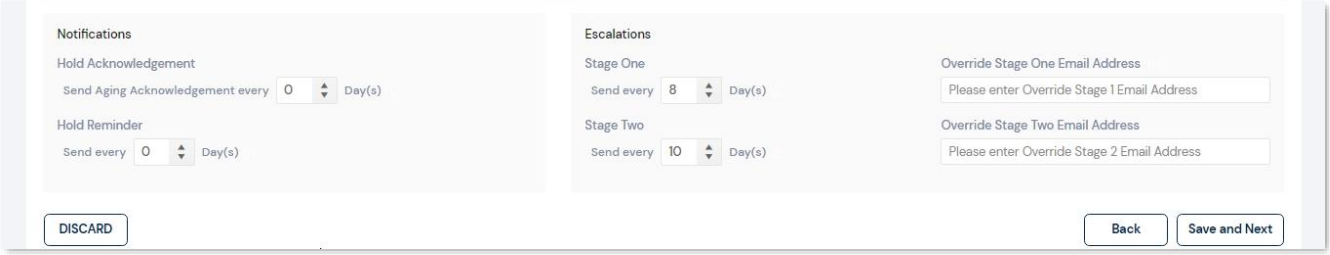
16. You can enable **Display Custodian data sources on acceptance page** option to display the data source of the custodian in the acceptance page.
17. Select the required **Custodians** by enabling the checkbox against it.
18. Select the custodians and enable **Exclude From Interview** column to exclude them from the interview.
19. Select the custodians and enable **Exclude From Escalation** column to exclude them from the escalation.

Notes:

- You can click the **Add Custodian** button to create and add a new custodian.
- You can click **Edit** against the custodian to edit the custodian details.

Custodian Notifications & Escalations

© Exterro, Inc. All rights reserved



20. Set the number of interval days to send the notification for **Hold Acknowledgement**.
21. Set the number of interval days to send the notification for **Hold Reminder**.
22. Set the number of interval days to send the escalation email notifications in **Stage One** and **Stage Two**.

Notes: You can also override the email address for escalation email notification in stage one and stage two fields. i.e.,

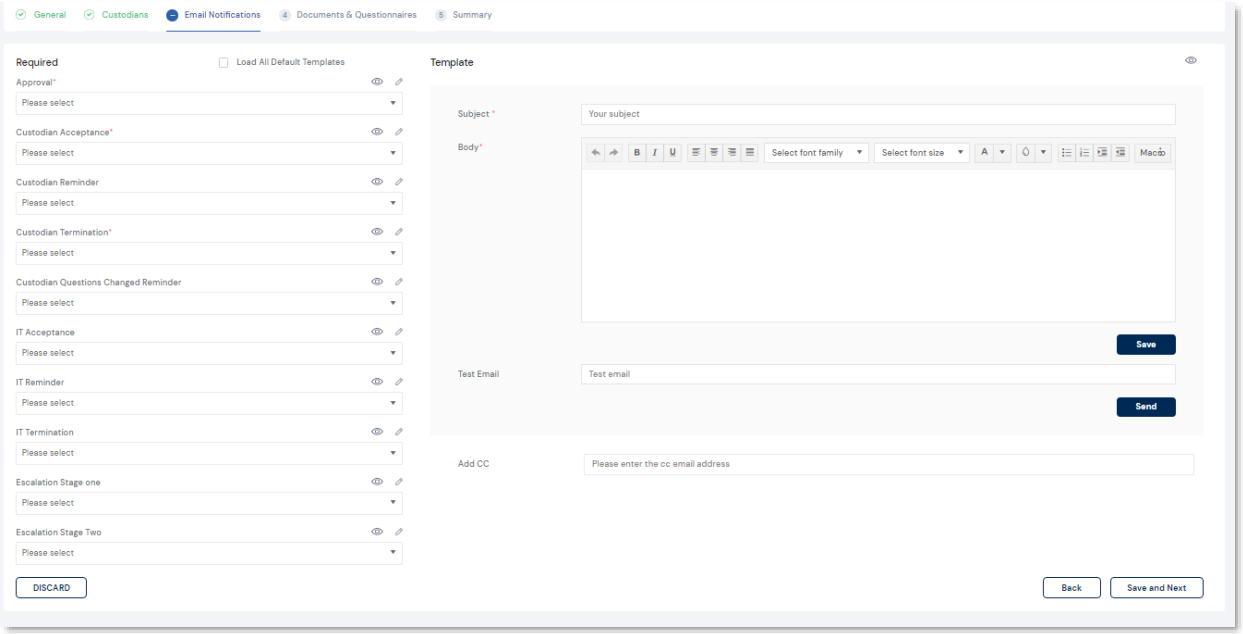
- **Override Escalation Stage One Email Address:** When specified, this email address will be used instead of the manager's email address as specified in Active Directory.
- **Override Escalation Stage Two Email Address:** After a specified number of days, the next escalation is sent to the specified email address

23. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Email Notifications

Lit holds send email notifications to people, IT Staff, and the Hold Approver informing them of the status and events of the lit hold. When you create a lit hold, you can choose the template that you want to use create your own custom email templates. You can edit or delete.



24. You can enable **Load All Default Templates** to use the default templates or select the required email template.

Notes:

- The email content of the selected template is displayed on the right pane for you to view.
- Click the **View** to view the corresponding content in email view.
- You can modify the **Subject** and **Body** of the email notification from the right pane and click **Save**.
- You can provide the **Test Email** address and click **Send** to test if the email notifications are received as intended.

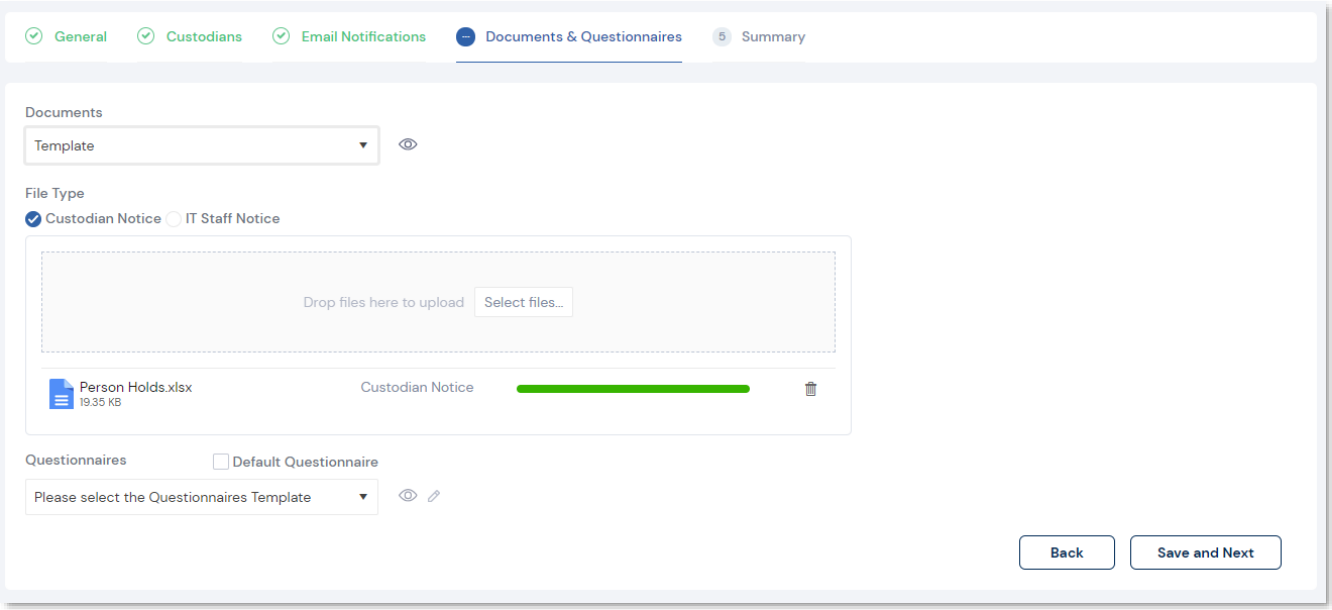
© Exterro, Inc. All rights reserved

25. Add the email address of the CC recipients in **Add CC**. You can also add multiple email addresses separated with commas (,).

26. Click **Save and Next**.

Documents and Questionnaires

Documents are any supporting documents that you want to attach to the litigation hold notification emails.



27. Select the documents template from the **Documents** drop-down field.

Note: The document attached to the template will be automatically loaded in the **File Type**. However, you can click **Delete** to delete the file and manually add it.

28. Select a questionnaire from the **Questionnaires** drop-down.

© Exterro, Inc. All rights reserved

Notes:

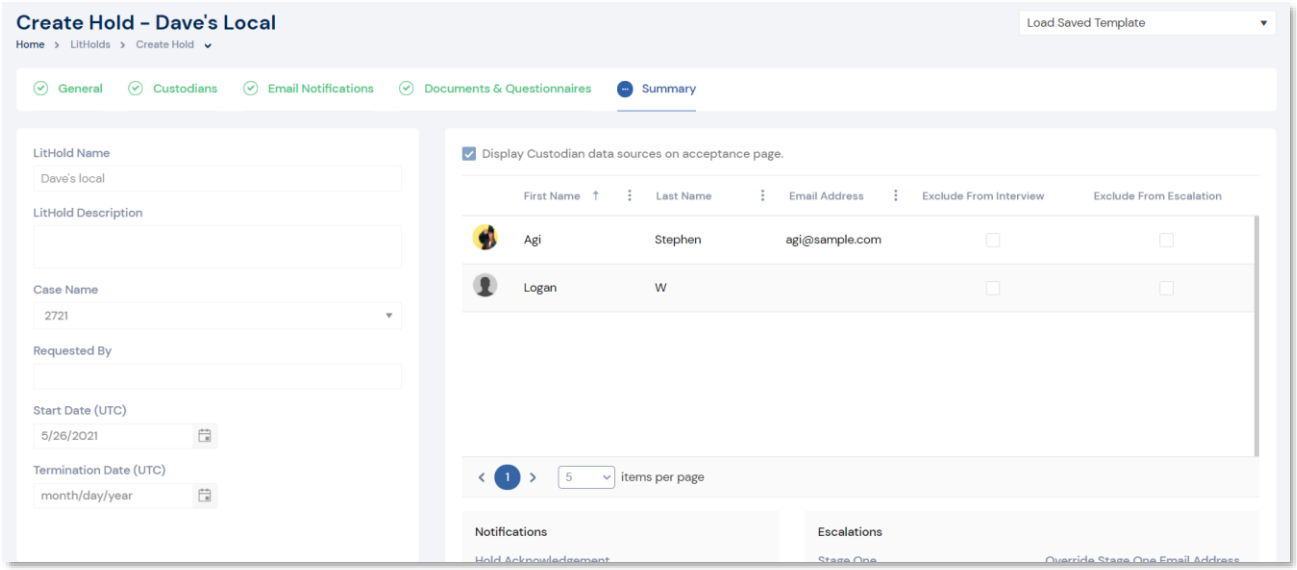
- You can enable **Default Questionnaires** to use the default questionnaire.
- You can click **View** to view the selected questionnaire.
- You can click **Edit** to edit the selected questionnaire.

Tip: You can also select the document templates and add the file type documents as well.

29. Click **Save and Next**.

Summary

30. Review and ensure the provided information is correct.



31. Click **Submit LitHold**.

Note: You can click **Save as Template** to save the hold as a template.

© Exterro, Inc. All rights reserved

Approving LitHolds

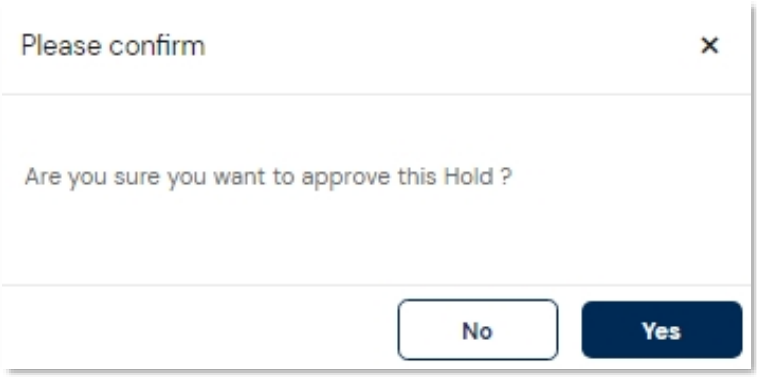
A litigation hold will be initiated only after approving it. Based on the approvers configured during creation, any or all the users will have to approve the hold.

Tip: To filter the grid efficiently, you can simply enter a keyword into the search box

located at the top of any grid and click the search button or press enter.

To approve a lithold:

1. From the home page, click **LitHolds**.
2. Click **Approve** against the hold to be approved.
   - The **Please confirm** pop-up is displayed.



3. Click **Yes**.

© Exterro, Inc. All rights reserved

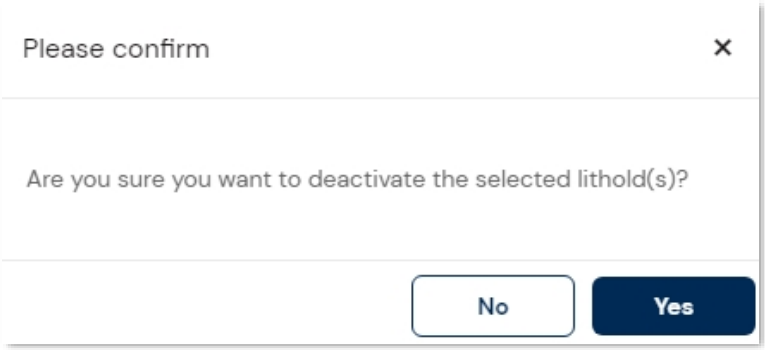
Deactivating LitHolds

Deactivating a hold does not terminate or delete the hold; instead, the hold is "paused" or made not active, regardless of any pending actions. It is to be noted that while a hold is deactivated, scheduled email notifications, such as reminders, are no longer sent. You can re-activate the hold anytime later.

Warning: When you deactivate a hold, custodians and IT staff do not receive termination notices.

To deactivate a lithold:

1. From the home page, click **LitHolds**.
2. Select the required holds by enabling the check box against it.
3. Click **Deactivate** .
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

© Exterro, Inc. All rights reserved

Activating LitHolds

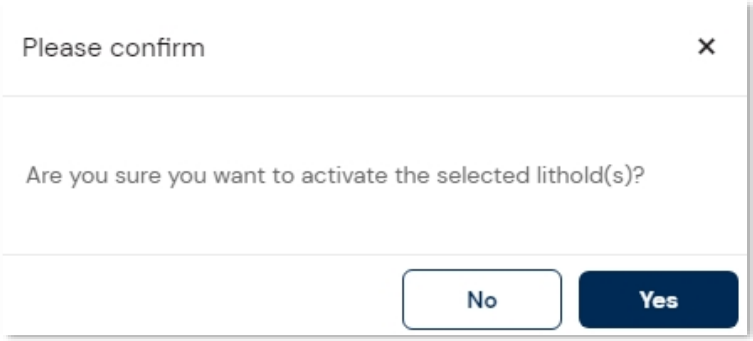
You can activate a deactivated hold to resume the hold to normalcy.

Warnings:

- When you activate a hold, custodians and IT staff do not receive termination notices.
- Upon activating a deactivated hold, the hold will be moved to 'Awaiting Approval' status again.

To activate a lithold:

1. From the home page, click **LitHolds**.
2. Select the required holds by enabling the check box against it.
3. Click **Activate** .
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

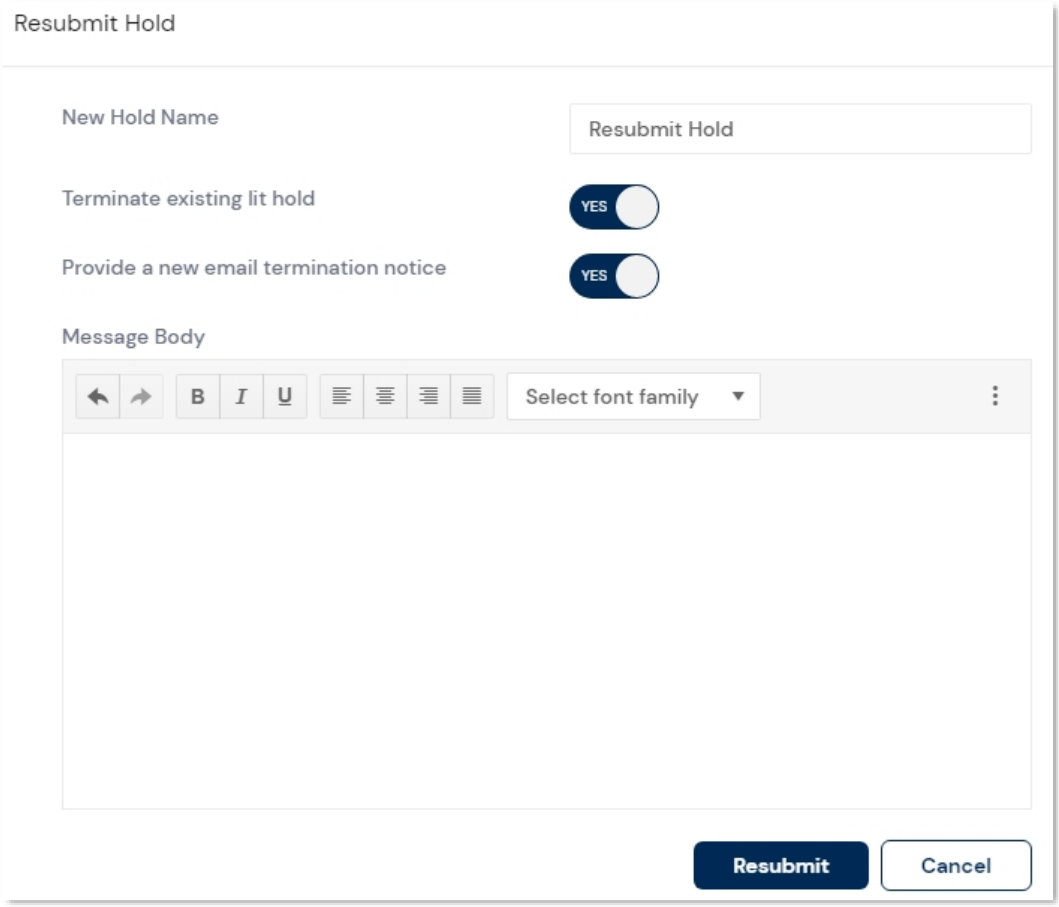
© Exterro, Inc. All rights reserved

Resubmitting LitHolds

Resubmitting a hold creates a new copy of the hold and sets it back to its original state so that all actions must be performed again. You can use this to replace a hold that is already in place or clone an existing hold and leave the original hold intact.

To resubmit a lithold:

1. From the home page, click **LitHolds**.
2. Select the required holds by enabling the check box against it.
3. Click **Resubmit** .
   - The **Resubmit Hold** pop-up is displayed.



4. Enter the **New Hold Name**.

© Exterro, Inc. All rights reserved

5. Enable **Terminate existing lit hold** if you want to deactivate the original hold after creating a new one.
6. Enable **Provide a new email termination notice** if you want to send a notification email on this.
7. Provide the **Message Body** for the email to explain that the previous hold has been replaced.
8. Click **Resubmit**.

Warnings:

- You will be able to enable **Provide a new email termination notice** only if **Terminate existing lit hold** is enabled.
- The Message Body section will be enabled only if **Provide a new email termination notice** is enabled.

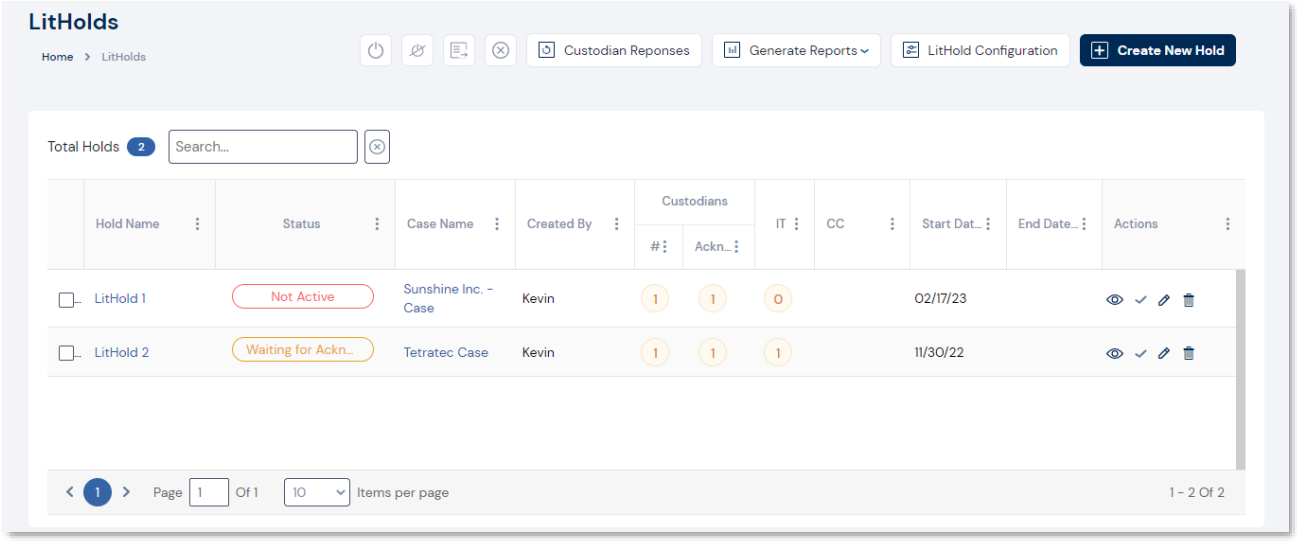
© Exterro, Inc. All rights reserved

Viewing LitHolds

This page allows you to view the overall status of a highlighted hold, which includes the status of the hold, number of IT Staff or custodians along with the actions they completed for the hold and a chronological log of every events of the hold.

To view a lithold:

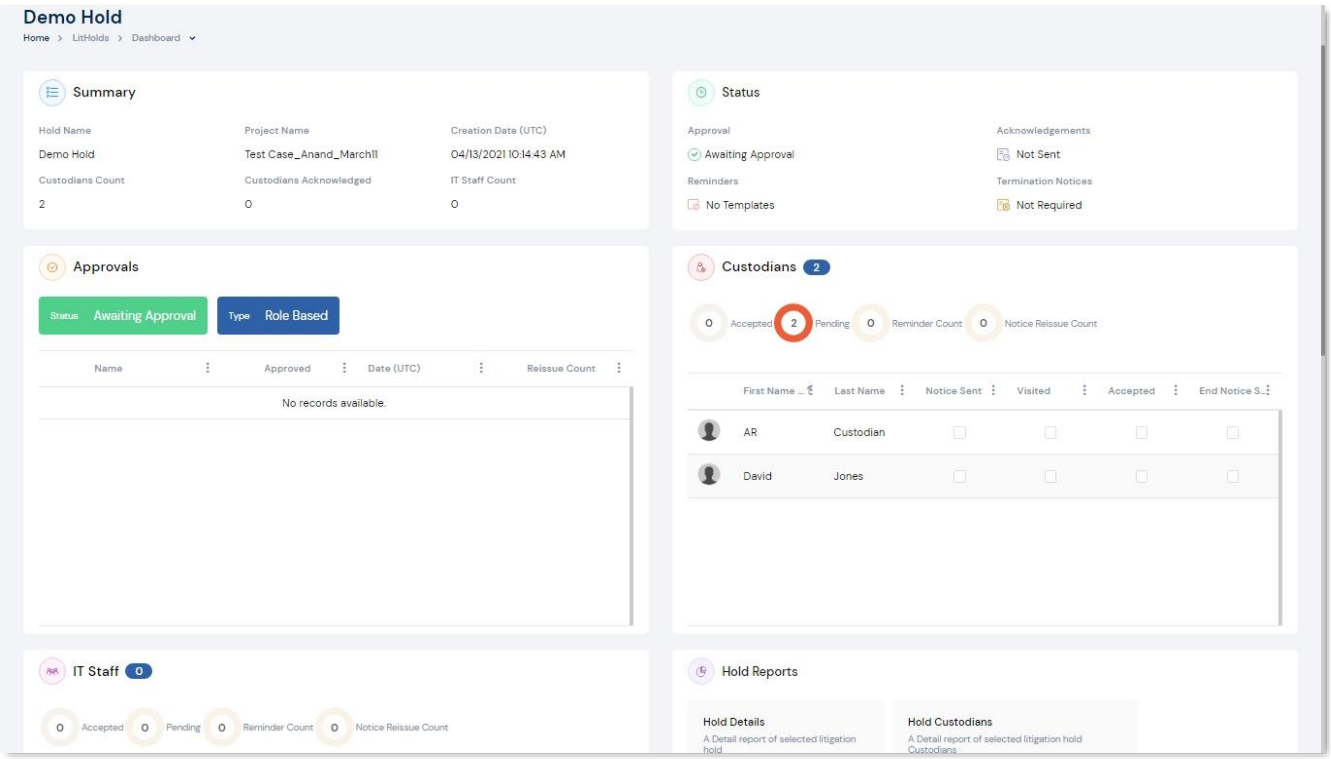
1. From the home page, click **LitHolds**.
   - The Manage holds page is displayed.



2. Click **View** against the hold to be viewed.

© Exterro, Inc. All rights reserved

- The **Dashboard** of the corresponding hold is displayed.

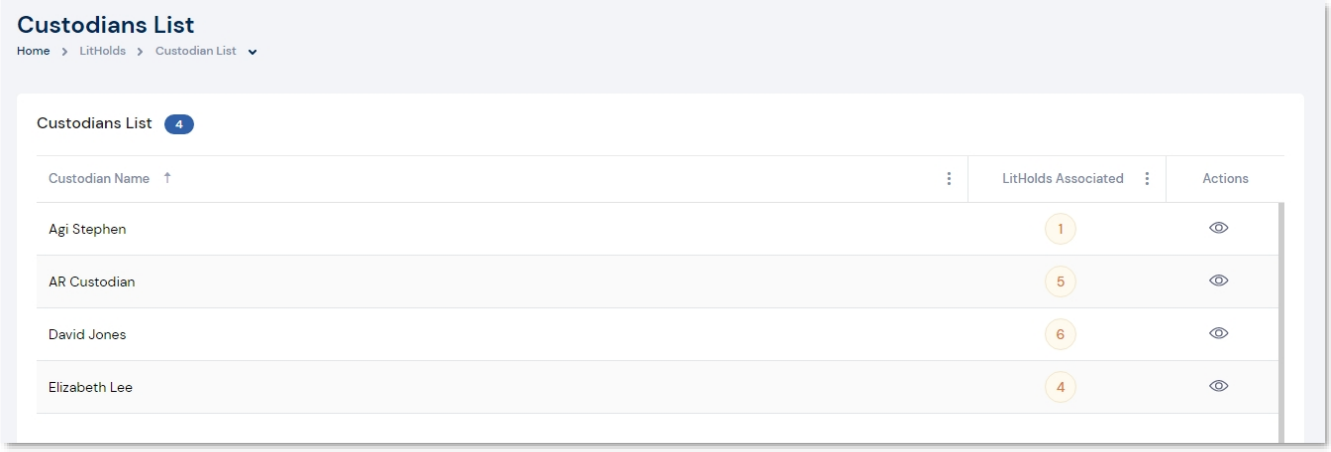


© Exterro, Inc. All rights reserved

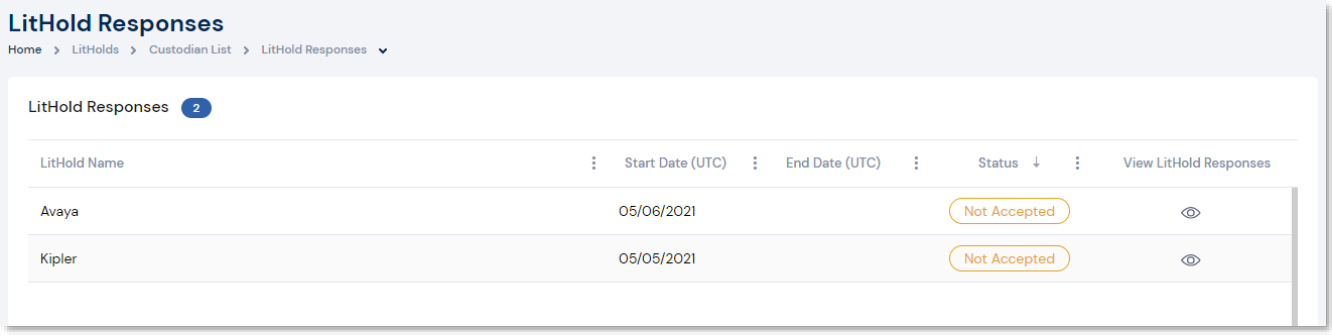
Viewing Custodian Responses of a LitHold

To view the responses of the custodians:

1. From the home page, click **LitHolds**.
2. Click **Custodian Responses**.
   - The associated **Custodians List** is displayed.



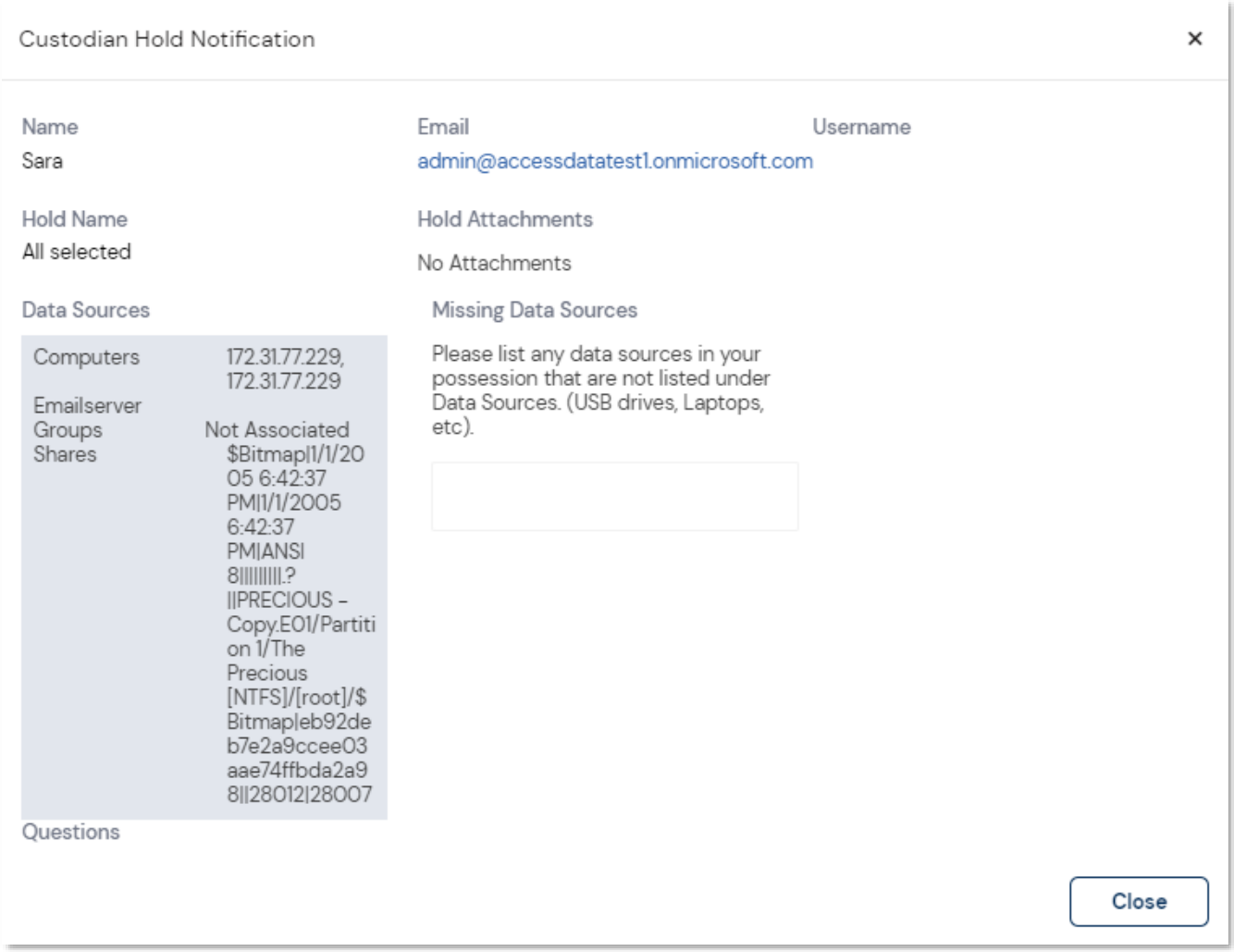
3. Click **View** against the required custodian.
   - The **LitHold Responses** page listing the holds associated with the custodian is displayed.



4. Click **View** against the required hold name.

© Exterro, Inc. All rights reserved

- The **Custodian Hold Notification** pop-up is displayed.



© Exterro, Inc. All rights reserved

Generating Reports for LitHolds

You can generate various predefined reports with summary or detailed information about litigation holds in the application. You can generate the following 4 types of reports for LitHolds:

- Hold Summary report
- Custodian Details report
- Hold Details report
- Hold Custodians report

Tip: The downloaded reports will also be available in the Case Folder Path.

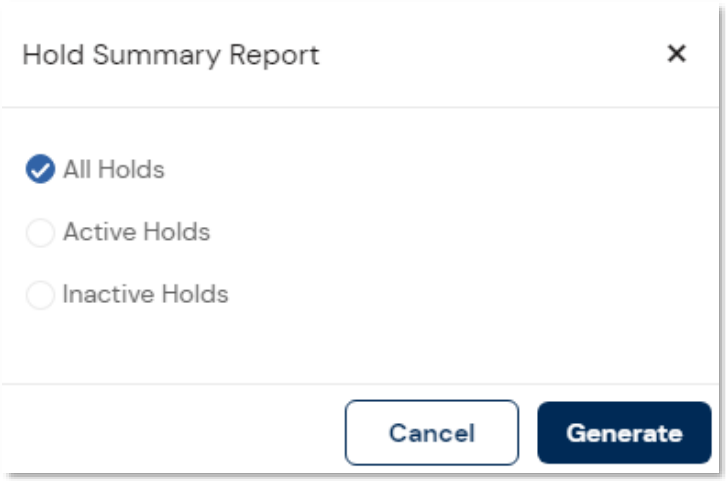
Hold Summary report

This report provides you an overview of all litigation holds in the application. Additionally, this report lists their approval and acceptance status, associated case, and when it was created. Along with it, number of custodians and IT Staff associated with a litigation hold, and the current stage of approval are furnished in the report.

© Exterro, Inc. All rights reserved

To generate hold summary report:

1. From the home page, click **LitHolds**.
2. Click **Generate Reports**.
3. Click **Hold Summary Report**.



4. Select any of the following as required:
   - All Holds – To generate the report of all the holds in the application.
   - Active Holds - To generate the report of all Active holds in the application.
   - Inactive Holds - To generate the report of all Inactive holds in the application.

5. Click **Generate** to downloaded in the report in **.xlsx** format.

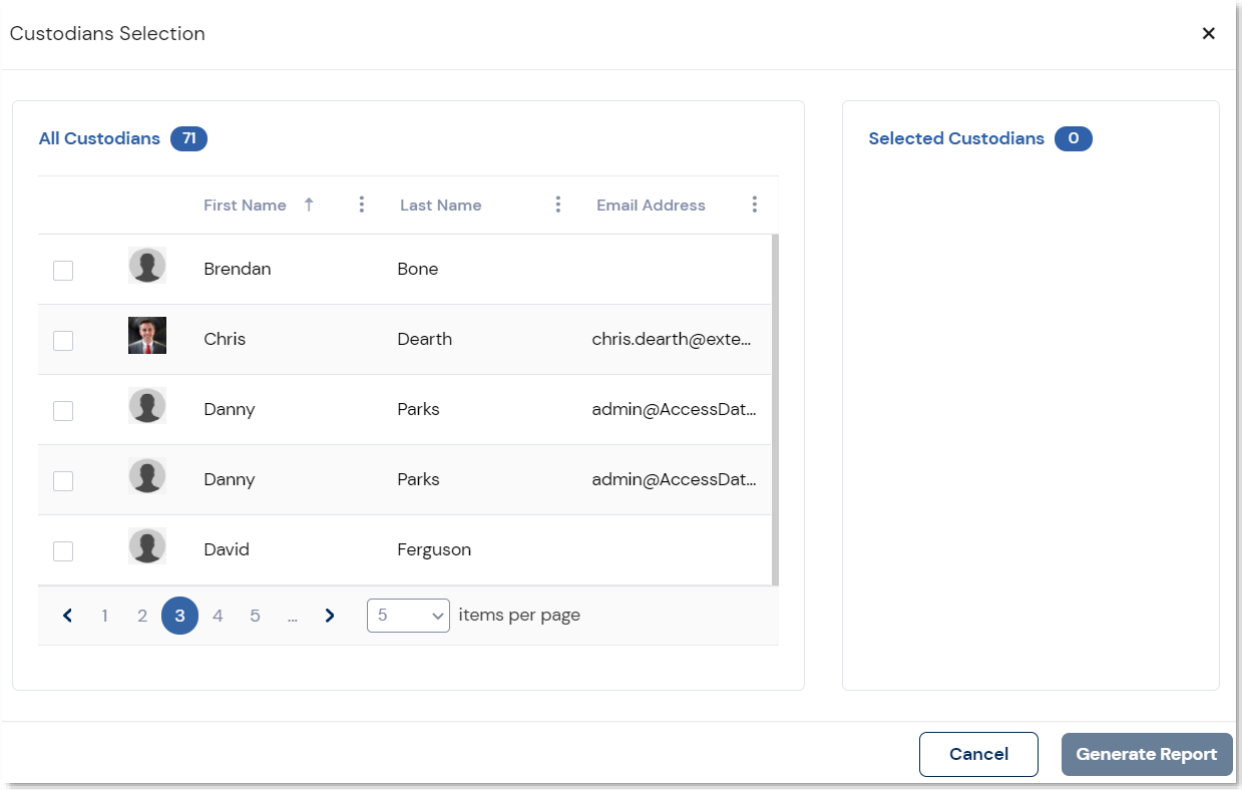
© Exterro, Inc. All rights reserved

Custodian Details report

This report provides you a detail report of the custodians in the hold such as their email address, notice dates, reminder counts, reminder dates, acceptance status, etc.

To generate custodian details report:

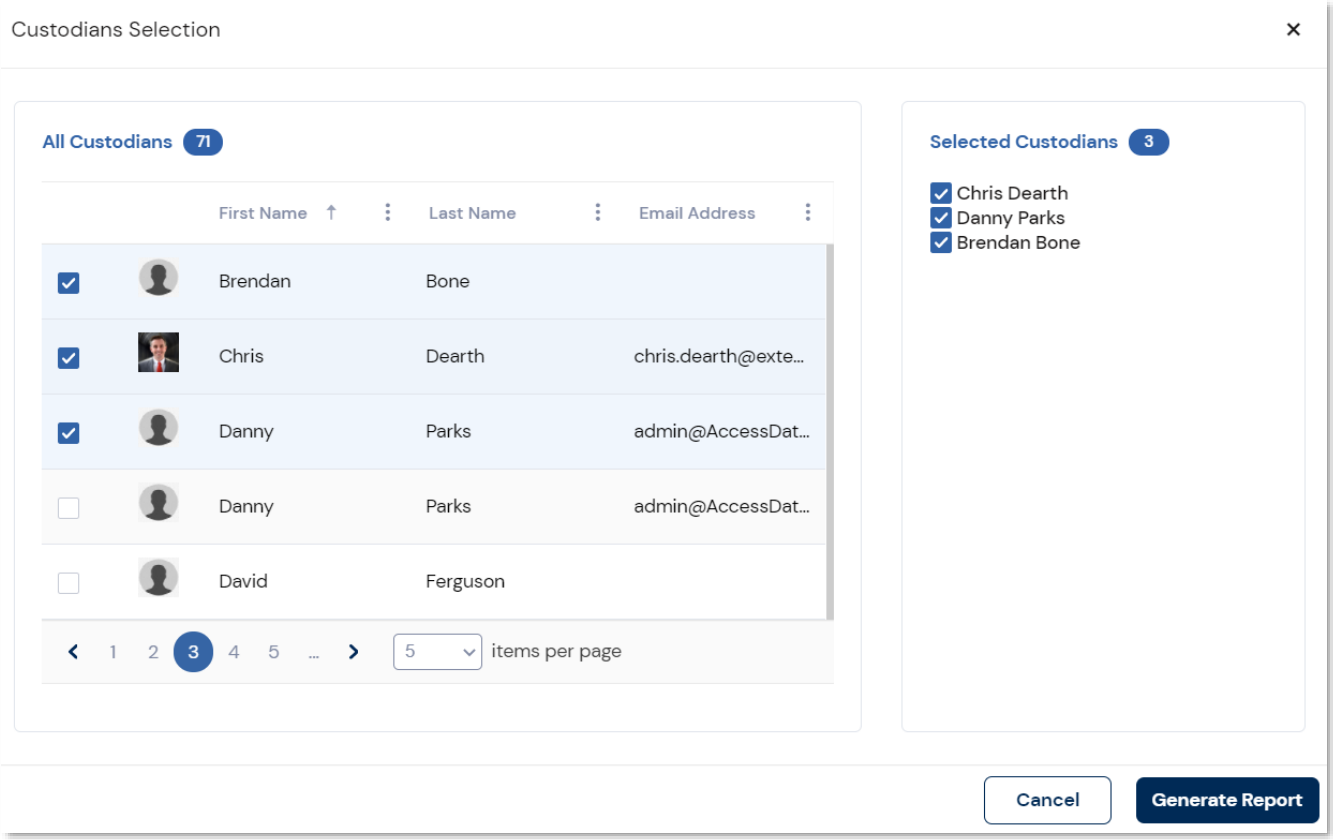
1. From the home page, click **LitHolds**.
2. Click **Generate Reports**.
3. Click **Custodian Details**.
    - The **Custodian Selection** pop-up is displayed.



4. Select the required custodians by enabling the checkbox against it.

© Exterro, Inc. All rights reserved

- The selected custodians are displayed on the right pane.



5. Click **Generate Report** to downloaded in the report in **.xlsx** format.

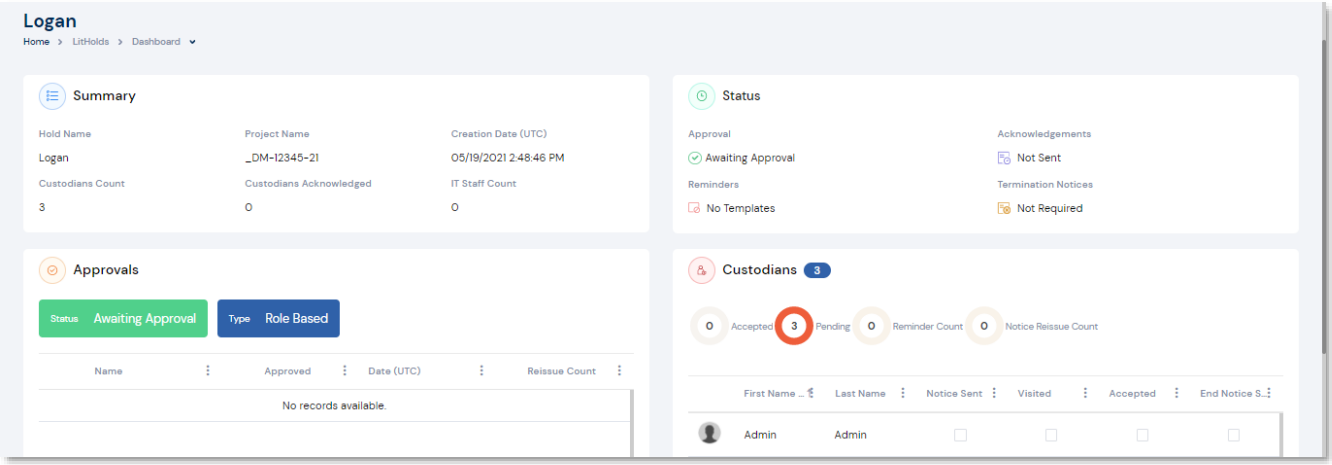
© Exterro, Inc. All rights reserved

Hold Details report

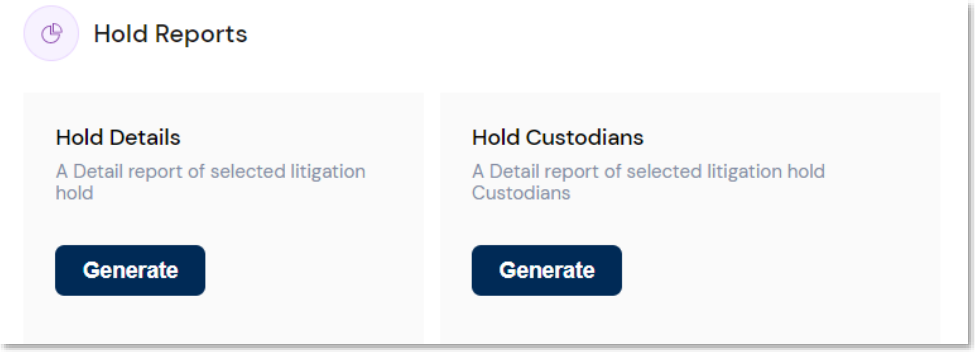
This report provides a detailed overview of a litigation hold's approvers, custodians, IT Staff, any associated document files, and interview questions. Also included are the start and end dates of the hold, the priority of the hold, and a description.

To generate hold details report:

1. From the home page, click **LitHolds**.
2. Click **View** against the hold to be viewed.
   - The **Dashboard** of the corresponding hold is displayed.



3. Navigate down to **Hold Reports** section.



4. Click **Generate** button below the **Hold Details** to downloaded in the report in **.xlsx** format.

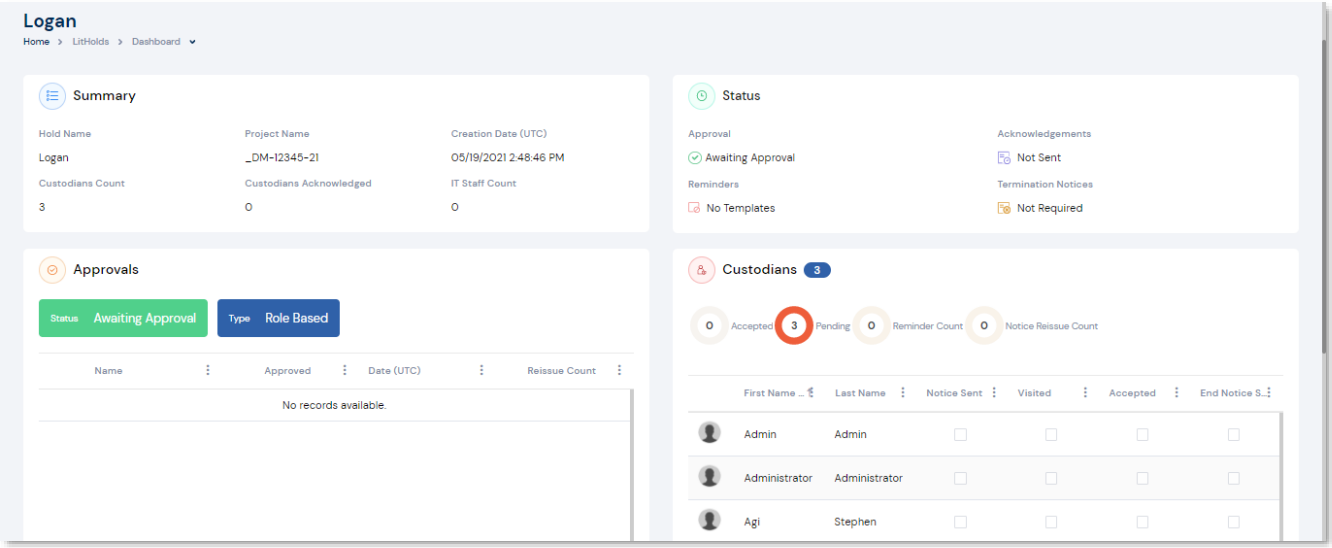
© Exterro, Inc. All rights reserved

Hold Custodians report

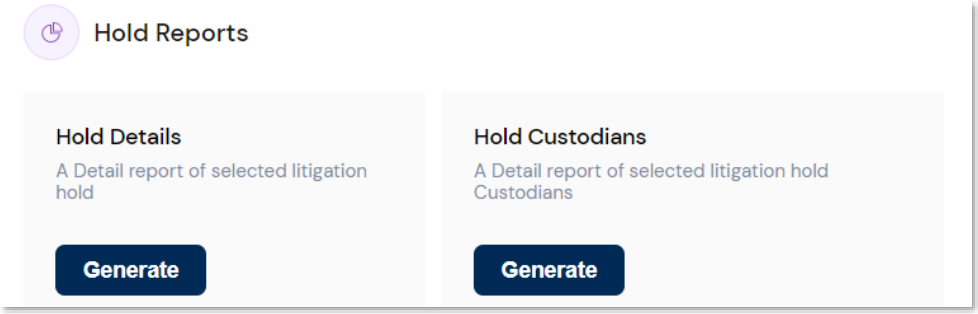
This report provides a detailed overview of the custodians associated with the corresponding litigation hold, notice details, reminder details, termination details and the count of interview questions answered.

To generate hold custodians report:

1. From the home page, click **LitHolds**.
2. Click **View** against the hold to be viewed.
   - The **Dashboard** of the corresponding hold is displayed.



3. Navigate down to **Hold Reports** section.



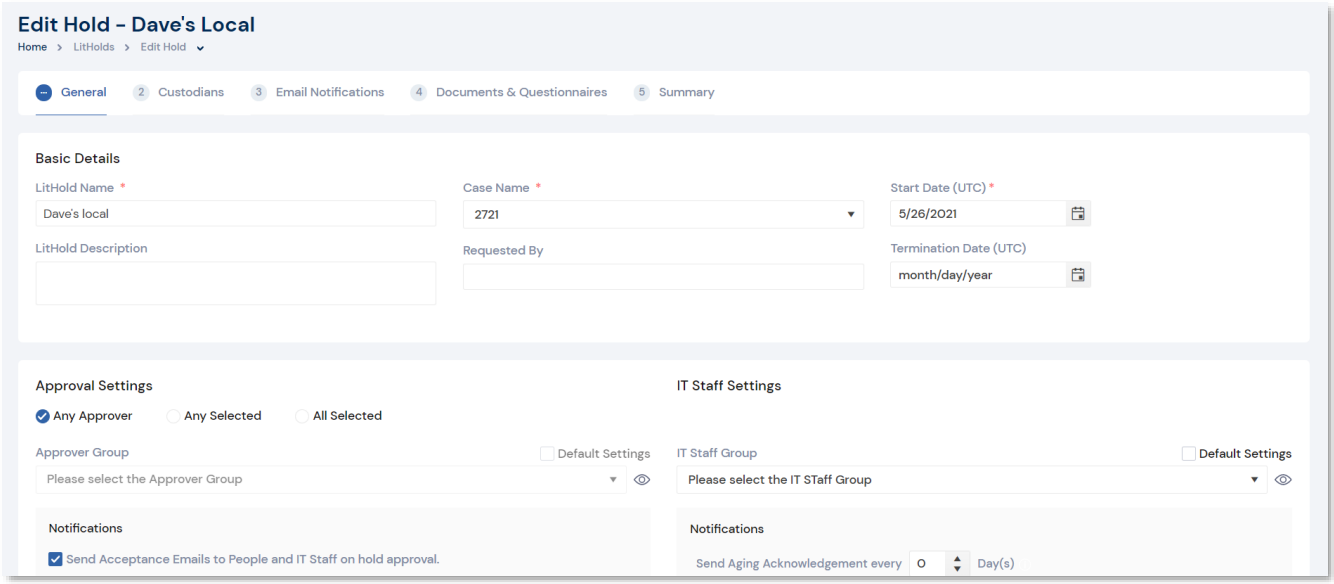
4. Click **Generate** button below the **Hold Custodians** to downloaded in the report in **.xlsx** format.

© Exterro, Inc. All rights reserved

Editing LitHolds

To edit a lithold:

1. From the home page, click **LitHolds**.
2. Click **Edit** against the hold to be edited.
   (This can be done to both active/non active litholds.)
   - The **Edit Hold** page is displayed.



3. Make the necessary changes.
4. Click **Save LitHold**.

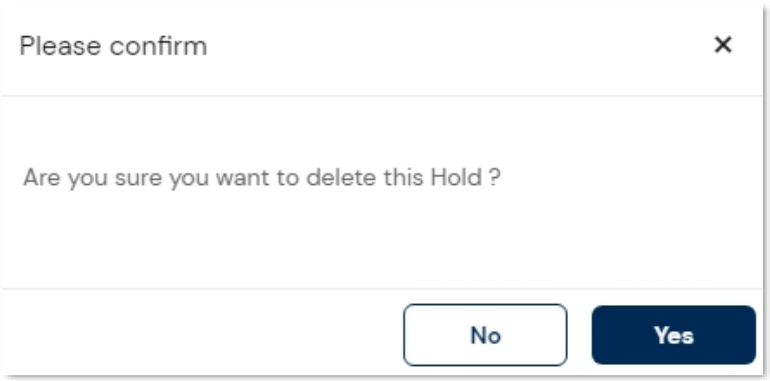
© Exterro, Inc. All rights reserved

Deleting LitHolds

You can delete a hold in any status and upon deleting it, no further email notifications are sent from it.

To delete a lithold:

1. From the home page, click **LitHolds**.
2. Click **Delete** against the hold to be deleted.
   - The **Please confirm** pop-up is displayed.



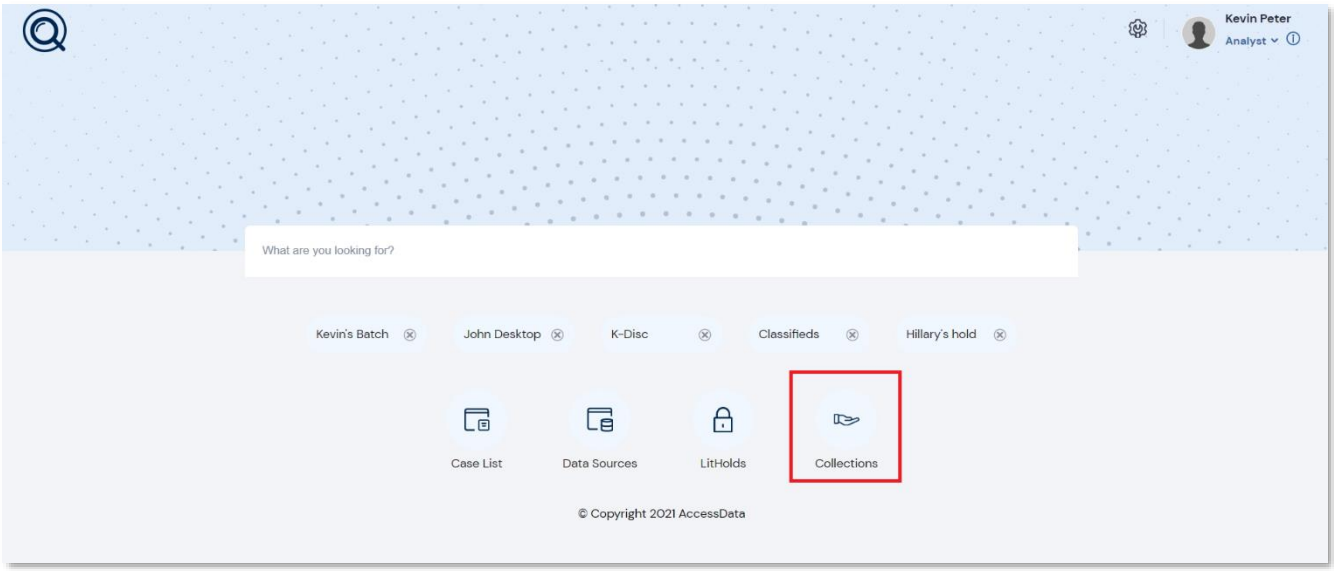
3. Click **Yes**.

Note: You can also select multiple holds from the Manage Holds page and click **Delete** to delete the selected holds at once.

© Exterro, Inc. All rights reserved

Collections

Collection is a process that gathers, filters, and archives information from a wide variety of data sources. You can create collection to collect data on a computer, network share, public data repository, email account, or all of the above within the application. The collection can be set up with filters to find only the files that are needed for the case. After collection, the data is processed and reviewed for relevance and transferred to the legal counsel.



© Exterro, Inc. All rights reserved

Elements of Collection

Managing Collections	• Creating Collections • Approving Collections • Executing Collections • Processing Collections • Cancelling Collection Process • Resubmitting Collections • Viewing Collection Details • Generating Reports for Collections • Editing Collections • Deleting Collections
Configuring data sources for collection	• Custodian (specific data sources) • Data Sources • Collection Filters for data source

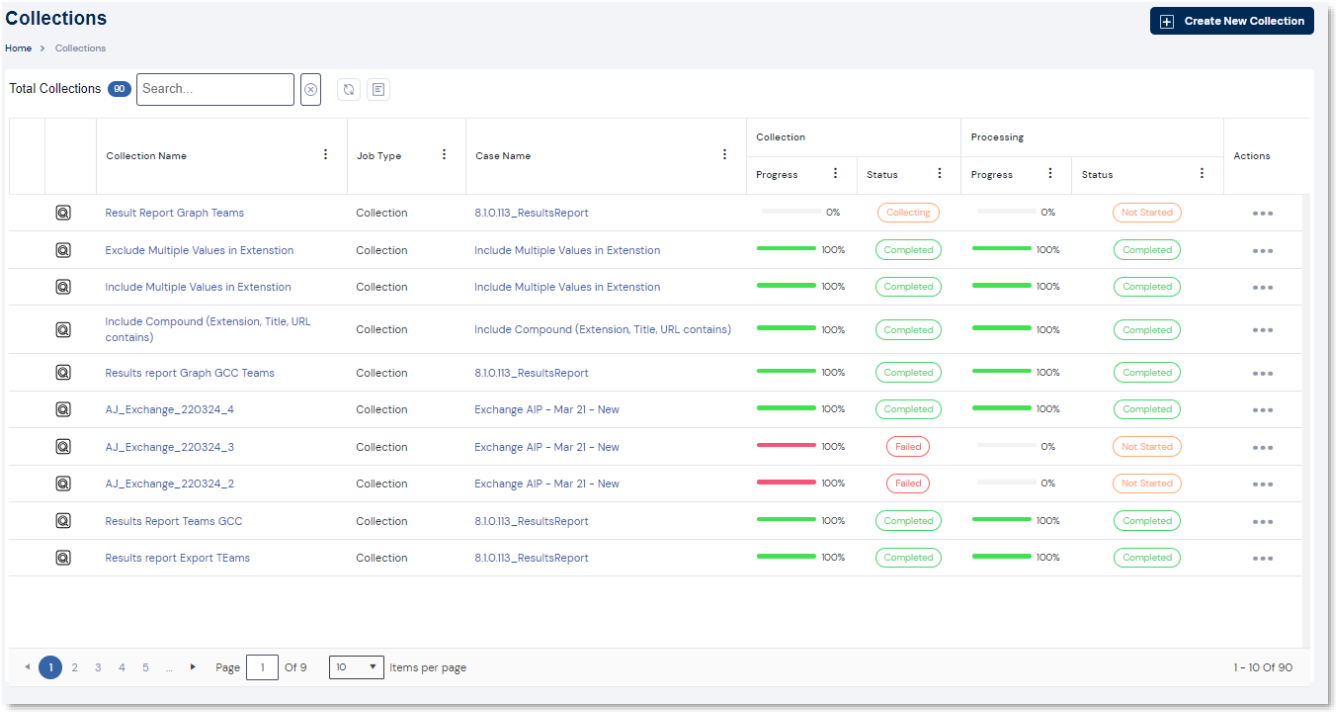
© Exterro, Inc. All rights reserved

Windows, Linux, and Other Data Sources

Creating Collections

To create a collection:

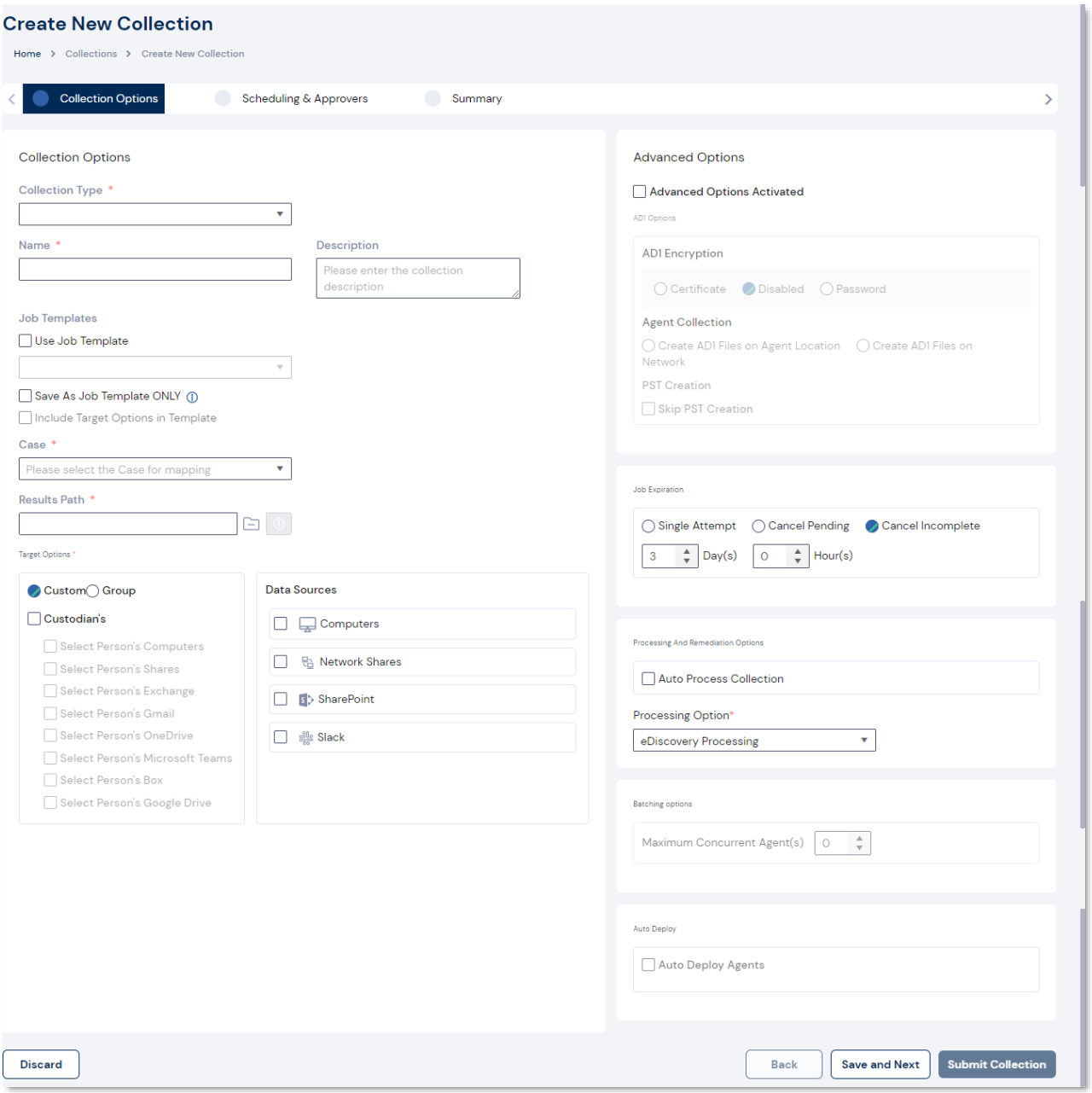
1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
   - The Manage page of Collection is displayed.



3. Click **Create New Collection**.

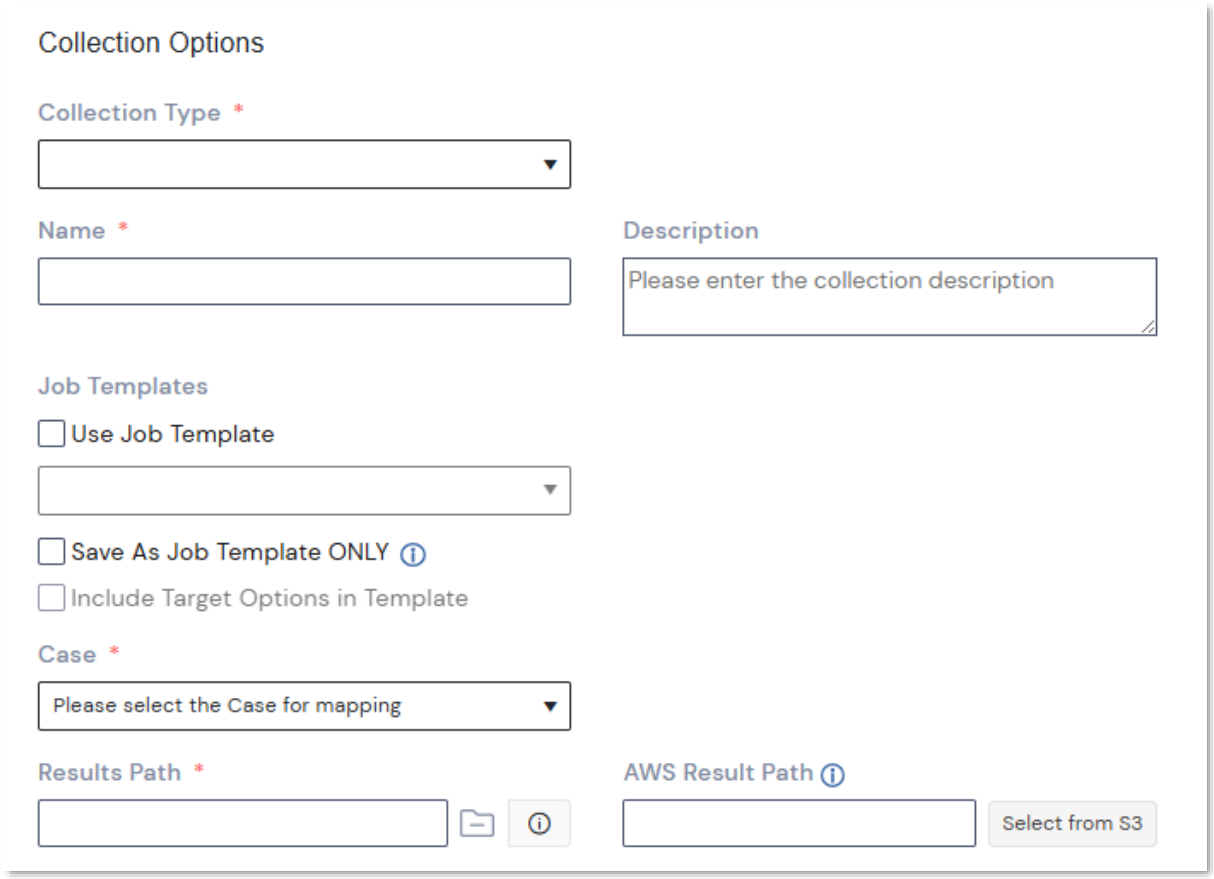
© Exterro, Inc. All rights reserved

- The collection creation page is displayed.



© Exterro, Inc. All rights reserved

Collection Options



4. Select the **Collection Type** based on the below description:
   - **File Scan** – To collect all the target files or use filters to collect specific files and folders.
   - **Agent Scan** - To run collection jobs related to RAM/Volatile analysis, Software Inventory, Agent Remediation and IOC jobs. (*Refer the Agent Scan Collections section for more details*)
   - **Report Only** – To collect a list of endpoint files. This is used primarily to help you identify the data that can be collected by giving you a report collection in the file list.

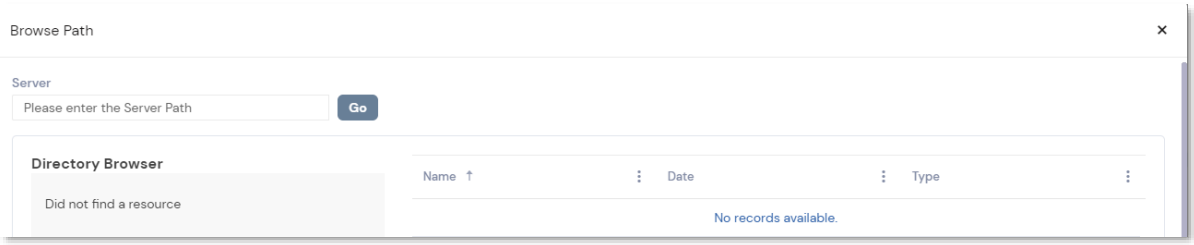
5. Provide a **Name** for the collection.
6. Provide a **Description** for the collection.
7. Select the case associated to the collection from the **Case** drop-down field.

© Exterro, Inc. All rights reserved

Note: The location for **Results Path** will be automatically populated based on the case selected in which the collected files will be stored. However, you can change the path if required. To do so,

i. Click **Folder** against the Results Path field.

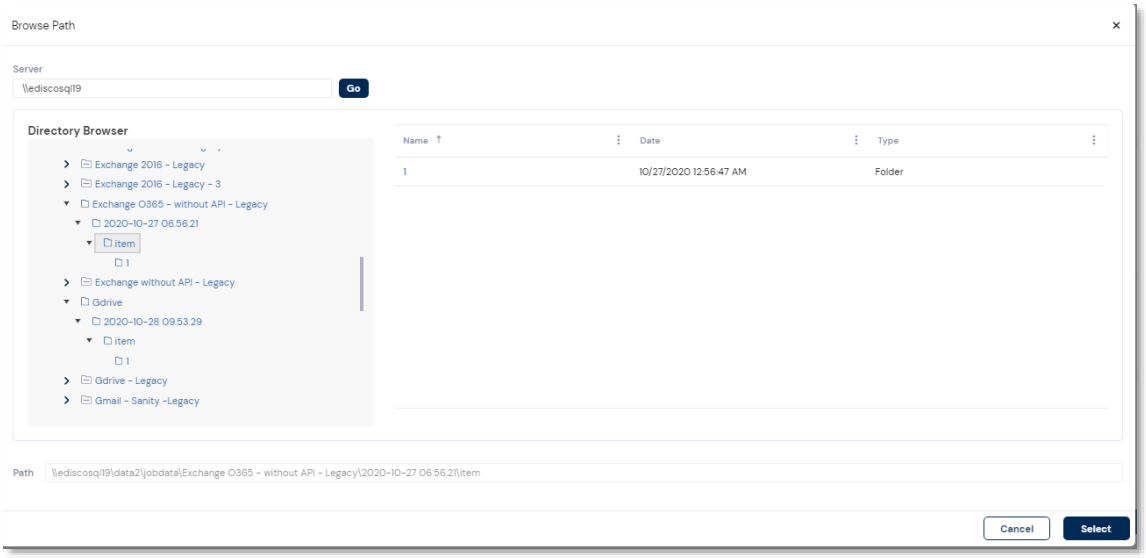
- The below page appears.



ii. Enter the **Server Path**.

iii. Click **Go** to view the directories available on the server.

iv. Select the folder to be where the results are to be saved.



v. Click **Select**.

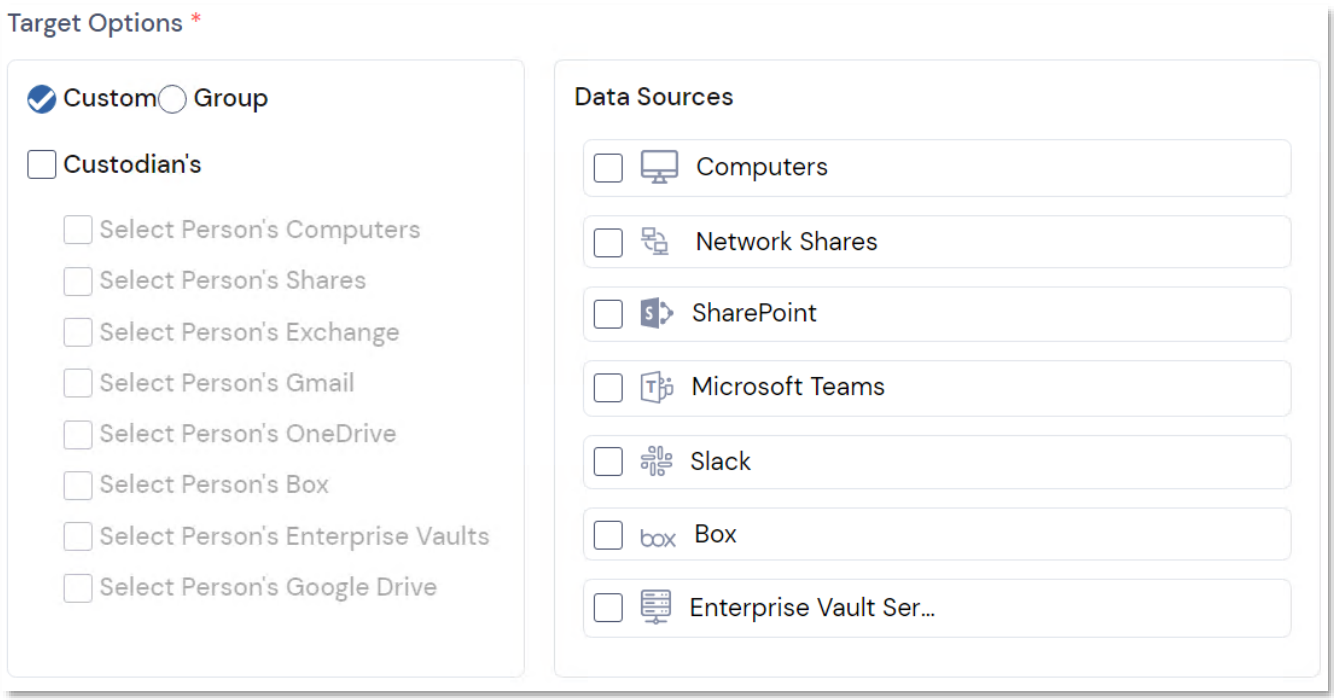
© Exterro, Inc. All rights reserved

Note: To save your collected files directly to a specific AWS S3 destination, locate the **AWS Result Path** field, click **Select from S3**, and select your desired folder location.

The **AWS Result Path** field is disabled by default. To enable it, navigate to the 'System Management' > 'Configuration' > 'Case Defaults' section, and enable the **AWS S3 Path for Collections** toggle.

© Exterro, Inc. All rights reserved

Target Options



8. Select either of the **Target Options** section as stated below:

Note: Selecting **Custodian's** with the **Custom** option will collect only the data from the data sources selected for a particular Custodian and selecting one from the **Data Sources** section will collect all the data from the particular data source, both associated and unassociated to custodians.

Alternatively, using the **Group** option will allow collection of all custodian associated data sources within an assigned group.

© Exterro, Inc. All rights reserved

a. Enable the required **Custodian's** option and select any or all of the below data sources:

- Select Custodian's Computers
- Select Custodian's Shares
- Select Custodian's Exchange
- Select Custodian's Gmail
- Select Custodian's OneDrive
- Select Custodian's Box
- Select Person's Google Drive

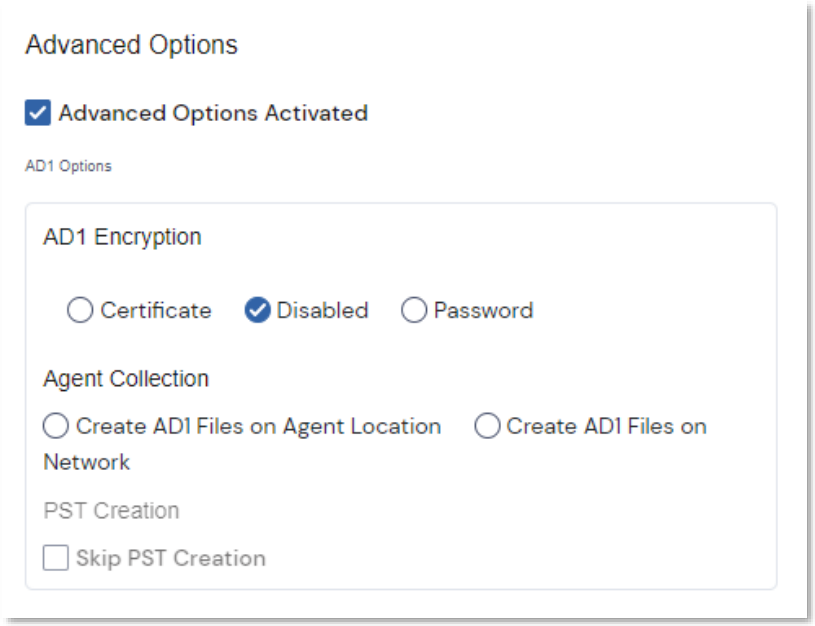
(OR)

b. Select any or all of the following **Data Sources**:

- Computers
- Network Shares
- SharePoint
- Microsoft Teams
- Slack
- Box

© Exterro, Inc. All rights reserved

Advanced Options



9. Enable the **Advanced Options Activated** checkbox to configure the following advanced collection functionalities:

   i. Select any of the following options for **AD1 Encryption** field:

   - **Disabled** – To turn off encryption of an AD1 evidence image file.
   - **Certificate** – To encrypt an AD1 evidence image file with a certificate. Certificates use public keys for encryption and corresponding private keys for decryption. You can configure the certificates that appear in the drop-down menu.
   - **Password** - To encrypt an AD1 evidence image file with a password that you specify.

   ii. Enable **Create AD1 Files on Agent** to create a AD1 image on the machine.

© Exterro, Inc. All rights reserved

iii. Enable **Create AD1 Files on Network Location** to create a AD1 image on the network share provided by the user.

Notes:

- Ensure the credentials for the network share path is configured in the **Manage Credentials** > **Redirect Acquisition** section of **System Management**.
- For **Report Only** collections, the XML reports can be generated directly at the agent location and subsequently transferred to FTK Central. This action can be performed using the **Create AD1 Files in Agent Location** option, which becomes automatically selected when you enable the **Advanced Options Activated** checkbox.

Warnings:

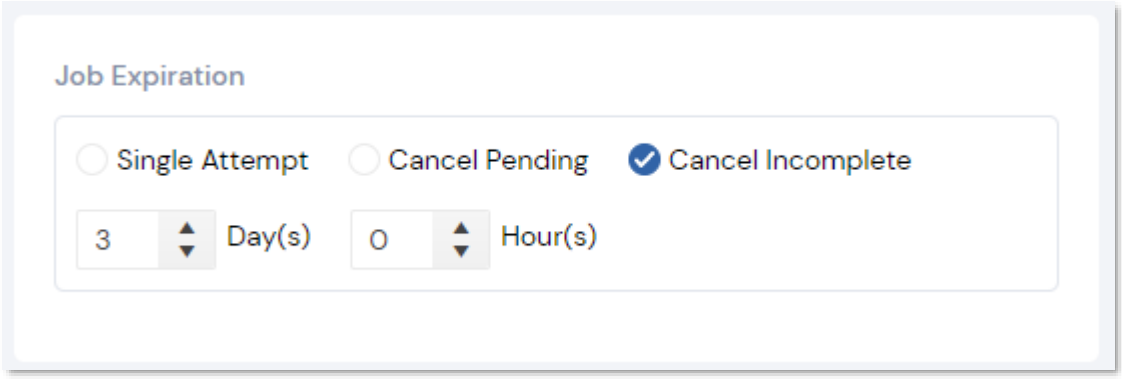
- The **Create AD1 Files on Network Location** field is applicable only when the **File Scan** option is selected as **Collection Type** and **Computers** is selected for **Data Sources**.
-

iv. Enable **Skip PST Creation** checkbox to avoid creating a PST file while collecting email files.

v. Enable **Maximum Concurrent Agent(s)** toggle to limit the amount of active agent jobs running concurrently.

© Exterro, Inc. All rights reserved

Job Expiration



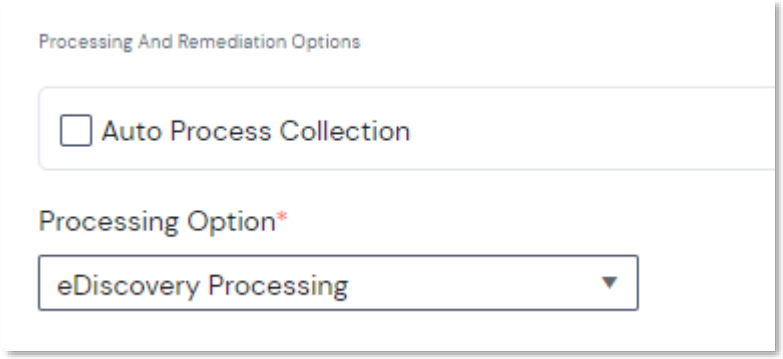
10. Select any one of the below provided options to define the time the system (site servers) should try and contact data sources within a job from the **Job Expiration** field:

- **Single Attempt** – To try only one once and terminate the unsuccessful attempt.
- **Cancel Pending** – To define the time after which a pending job should be terminated. Agents that have already contacted the server will continue to run until the task is complete regardless of the expiration date.
- **Cancel Incomplete** - To define the time after which an incomplete job should be terminated.

Warning: When cancelling a recurring job, only the job that is currently running in Site Server will cancel. The next occurrence of the job will start at its appointed time.

© Exterro, Inc. All rights reserved

Processing And Remediation Options

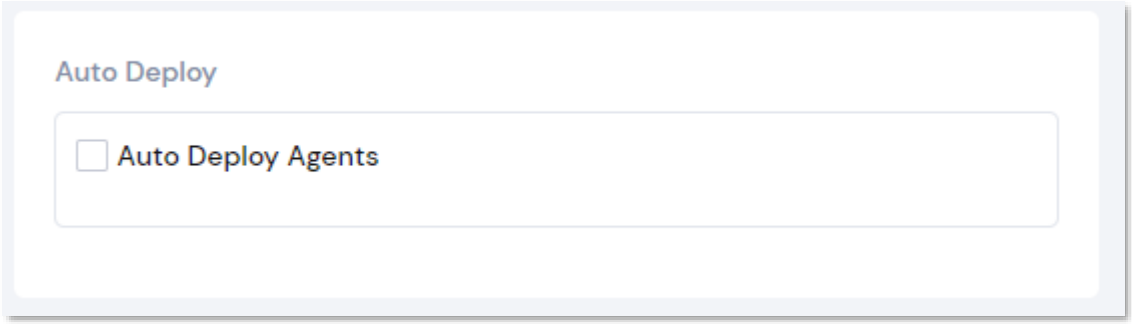


11. Enable the **Auto Process Collection** option to process the evidence automatically.

Note: If this option is disabled, you will have to manually trigger the processing.

12. Select the required processing profile from the **Processing Option** drop-down field.

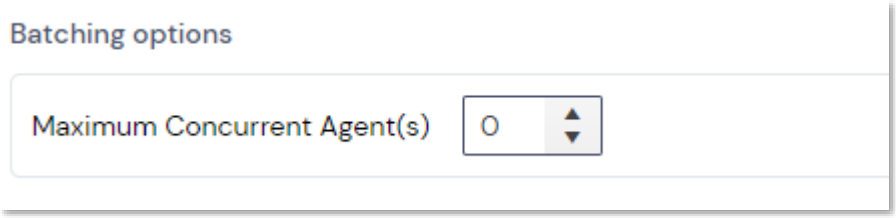
Auto Deploy



13. Enable the **Auto Deploy Agents** option if you want to deploy agents to computers included in the collection. *Refer to the Agent Credentials section.*

© Exterro, Inc. All rights reserved

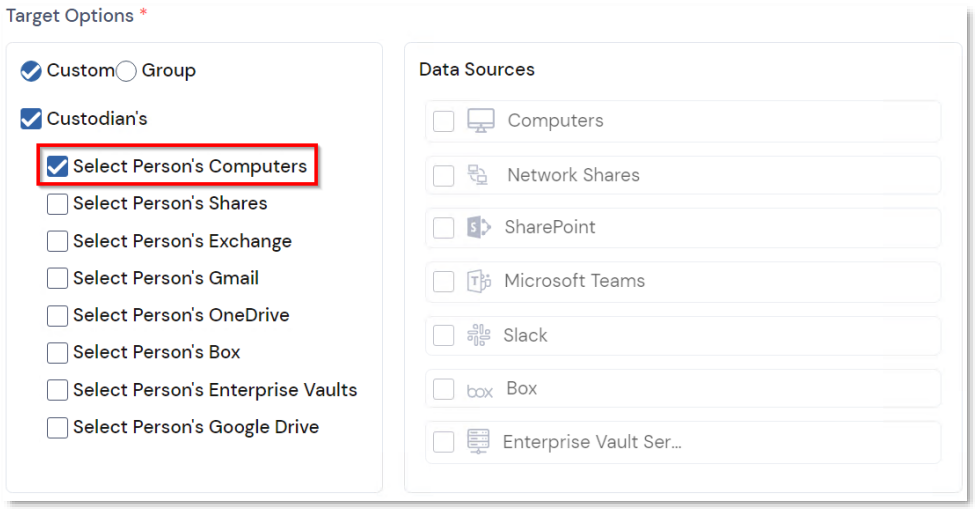
Batching Options



14. While multiple collections can run simultaneously, Batching Options allow jobs to run in groups. I.e., A selection of 3 Maximum Concurrent Agents will only allow 3 concurrent jobs to be run at once until finished, which would then allow the next batch of jobs to be started.

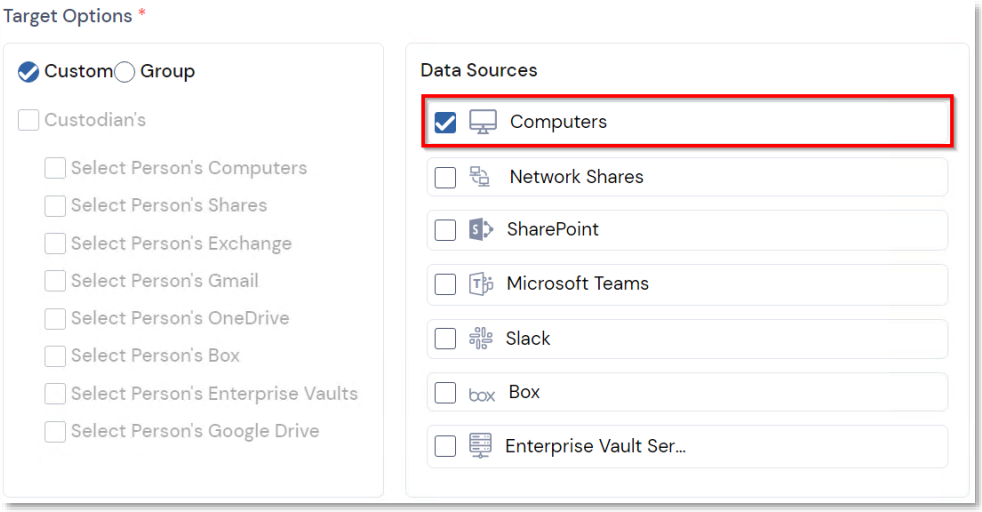
Warnings:

- The **Auto Deploy** is applicable only when the **Target Option** is selected as Computer against the Custodians or the Data Sources.
- The **Auto Deploy** option will not be applicable if multiple options are selected against the Custodians or Data Sources.



(OR)

© Exterro, Inc. All rights reserved



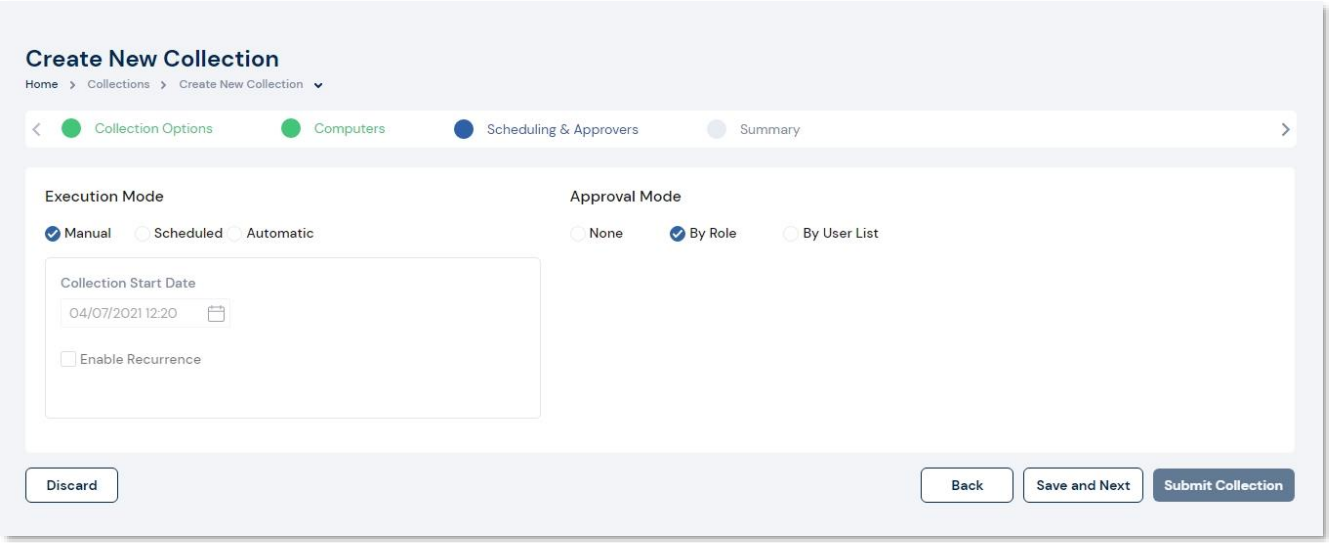
15. Click **Save and Next**.

Data Sources

Based on the data sources selected in the Target Options, the corresponding data source configuration sections will be displayed for you. Detailed steps to configure the required data source is provided in the Data Source Configuration section.

© Exterro, Inc. All rights reserved

Scheduling & Approvers

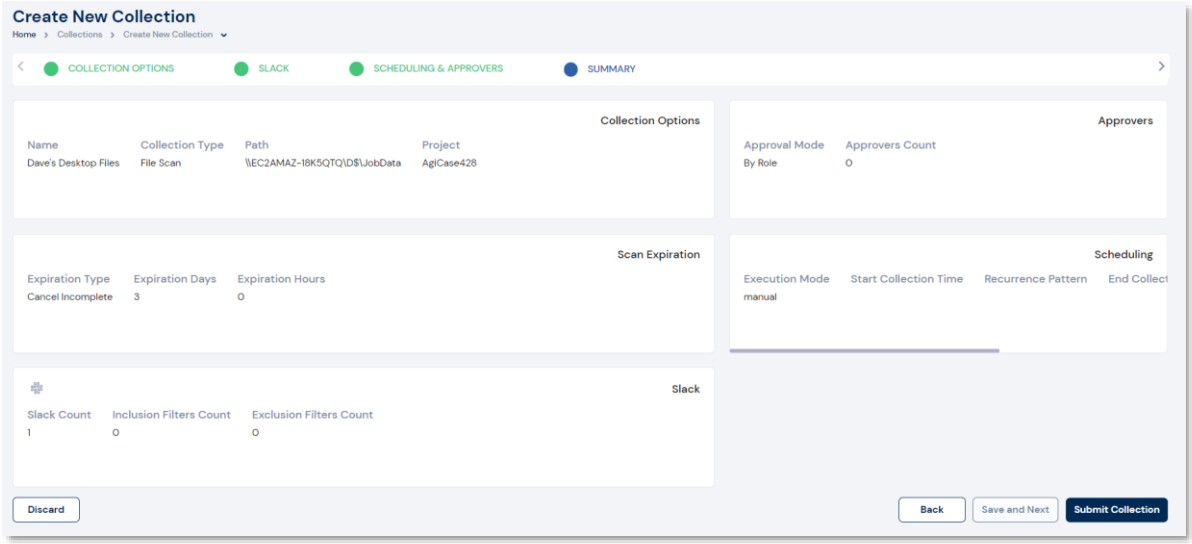


16. Select the **Execution Mode** for the Collection based as required:
    - **Manual** – You should initiate the collection process manually.
    - **Scheduled** – You can configure the **Collection Start Date** during when the collection will be initiated.
    - **Automatic** – The collection is automatically initiated based on the approval mode selected.

17. Select the **Approval Mode** based on the below description:
    - **None** – No approvals required for the collection.
    - **By Role** – Only users with selected roles assigned to them can approve this collection. After the collection is created, the job must first be approved and then it must be executed.
    - **By User List** – Only the users selected in the corresponding list can approve this collection. After the collection is created, the job must first be approved (by all the selected users) and then it must be executed.

© Exterro, Inc. All rights reserved

Summary



18. Review and ensure all the configurations made for the collection are correct.

Note: You can click **Back** to navigate back to the previous page to make any changes.

19. Click **Submit Collection**.

The collection will be created and the process will be initiated based on the selected **Execution Mode**.

© Exterro, Inc. All rights reserved

Agent Scan Collections

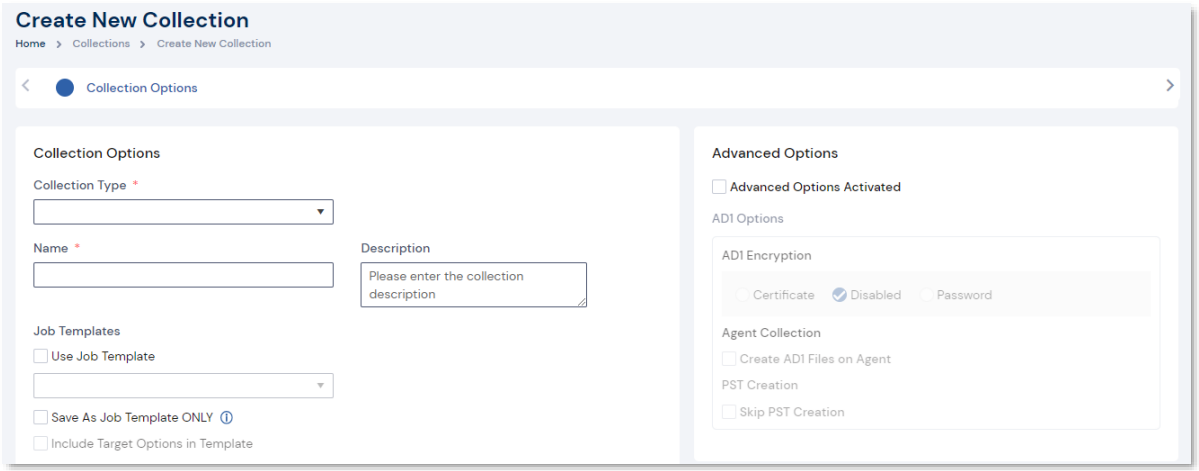
You are able to run agent jobs that range from remediation, software inventory to threat scans:

- Software Inventory
- Agent Remediation
- Volatile Job
- Threat Scan
- Memory Acquisition
- Memory Analysis

Setting up Agent Scan Jobs

To set up agent scan job:

1. From the homepage, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Click **Create New Collection**.
    - The **Create New Collection** page will be displayed.



4. Select the **Collection Type** as **Agent Scan**.
5. Provide the collection's **Name**.
6. Provide a brief description of the collection in the **Description** field.

© Exterro, Inc. All rights reserved

7. Select the case associated to the collection from the **Case** drop-down field.

Note: The location for **Results Path** will be automatically populated based on the **Case** selected in which the collected files will be stored. You can modify the path if required.

8. Select the **Computers** options from the **Data Sources** column for the **Target Options** field.

Note: Alternatively, you can enable the **Custodians** option > **Select Person's Computers**.

9. Enable the **Auto Process Collection** option to process the evidence automatically.
10. Enable the **Auto Deploy Agents** option if you want to deploy agents to computers included in the job.
11. Customize the Batching Options to run collection jobs on computers in batches.
12. Click **Save and Next**.
13. If Auto Deploy Agents was selected, you will be navigated to the **Agent Operations** section where the following information should be configured**:**
14. **Install** – Select to push an agent to the endpoint. This can cause the machine to restart without warning.
    - **Make Public Instance** - Configure the agent to check a public instance after the agent is installed.
    - **Agent Type**: Local Storage
    - **Use Site Server Default Port** – Configure the default port the site server is using.
    - **Use Custom Port** – Configure the custom port for agent usage.
    - **Service Name** – Configure the name of the agent service.
    - **Executable Name** – Configure the name of the agent executable.

    (OR)

- **Uninstall** – Select to remove an agent from the endpoint.

15. Click **Save and Next**.
16. Select the required **Computers**.
17. Select any one of the below provided **Agent Scan Type**.

© Exterro, Inc. All rights reserved

- Software Inventory
- Agent Remediation
- Volatile Job
- Threat Scan
- Memory Acquisition
- Memory Analysis

Follow the sections below to configure Agent Scan types.

Scheduling an Agent Scan Job

To schedule agent scan job:

1. From the Scheduling & Approvers section, select the Execution Mode as Scheduled.
2. Check **Enable Recurrence**.
   a. Configure the **Recurrence Pattern** based on your requirement.
   b. Configure the **End Recurrence** based on your requirement.
   c. If required, select the **Incremental Collection** option for the **Collection Options** field. This allows you to view data as soon as it becomes available rather than having to wait for the whole collection to be completed.

© Exterro, Inc. All rights reserved

Software Inventory

The Software Inventory collection job will retrieve data relating to the software installed on the machine as well as any hardware utilization data. The installedsoftware.xml associated with this collection will be stored in the job data path related to the job named during the collection.

To set up the software inventory job:

1. Select **Software Inventory** as the **Agent Scan Type**.
2. Click **Save and Next**.
3. Configure the **Scheduling & Approvers** section based on your requirements.
4. Click **Save and Next**.
5. Click **Submit Collection**.

Tip: The **System Inventory** column set in review mode can be utilized to efficiently review the system data.

© Exterro, Inc. All rights reserved

Agent Remediation

The Agent Remediation job allows processes to be stopped, scripts to be sent and executed and file deletion.

Note: When Executing or Sending Files, ensure paths provided are absolute. Additionally, ensure **they are not** UNC paths.

To setup the agent remediation:

1. Select **Agent Remediation** as the **Agent Scan Type**.
2. Click **Add New Row** in the **Agent Remediation** section.
3. Select any one of the below provided options for the **Remediation Command** field.
   - Kill process by process ID.
   - Kill all process by name.
   - Delete file.
   - Execute.
   - Send file.

Tip: Multiple options can be run by clicking **Add New Row** consecutively.

© Exterro, Inc. All rights reserved

Kill process by process ID

To kill processes by process ID on an endpoint:

4. Ensure the **Kill process by process ID** option has been selected for the **Remediation Command** field.
5. Enter the Process ID in the **Remediation Data** field.
6. Click **Save**.
7. Click **Save and Next.**
8. Configure the **Scheduling & Approvers** section based on your requirements.
9. Click **Save and Next**.
10. Click **Submit Collection**.

© Exterro, Inc. All rights reserved

Kill process by name

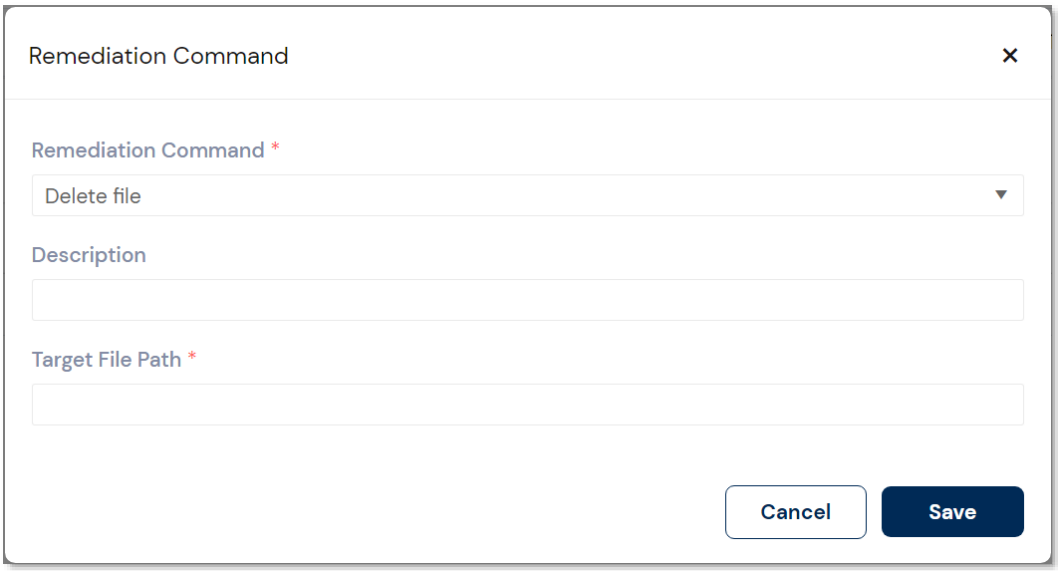
To kill processes by name on an endpoint:

11. Ensure the **Kill all process by name** option has been selected for the **Remediation Command** field.
12. Enter the process name in the **Remediation Data** field.
13. Click **Save**.
14. Click **Save and Next.**
15. Configure the **Scheduling & Approvers** section based on your requirements.
16. Click **Save and Next**.
17. Click **Submit Collection**.

© Exterro, Inc. All rights reserved

Delete File

To delete files on an endpoint:

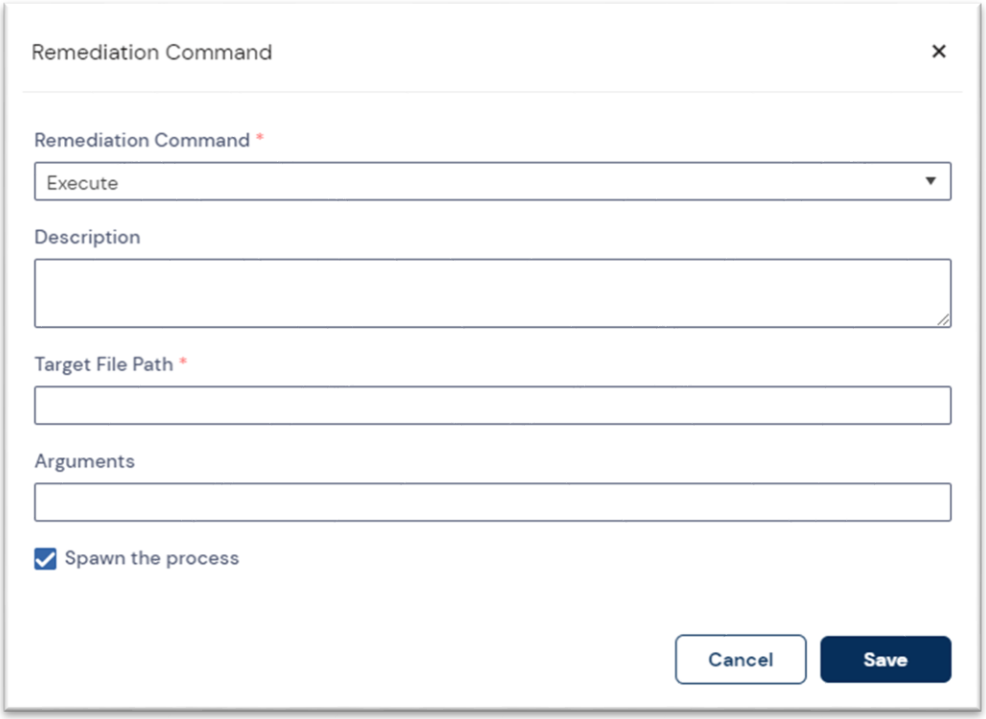


18. Ensure the **Delete file** option has been selected for the **Remediation Command** field.
19. Provide the **Description**.
20. Enter the Target File Path (for the file to be deleted).
21. Click **Save**.
22. Click **Save and Next.**
23. Configure the **Scheduling & Approvers** section based on your requirements.
24. Click **Save and Next**.
25. Click **Submit Collection**.

© Exterro, Inc. All rights reserved

Execute

To execute files on an endpoint:

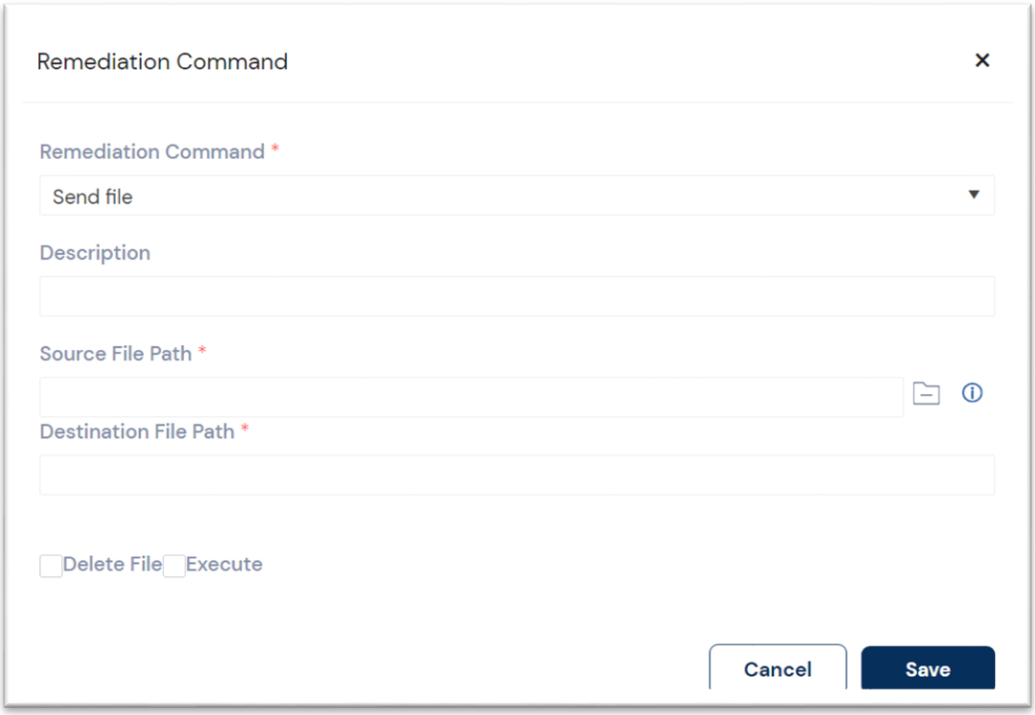


26. Ensure the **Execute** option has been selected for the **Remediation Command** field.
27. Provide a **Description**.
28. Enter the Target File Path (for the file to be executed) – this is the file located on the local machine. ***Example***: *Powershell.exe*.
29. Enter any **Command Arguments** if required.
30. Enable the **Spawn the process** option to automatically start any processes during execution.
31. Click **Save**.
32. Click **Save and Next.**
33. Configure the **Scheduling & Approvers** section based on your requirements.
34. Click **Save and Next**.
35. Click **Submit Collection**.

© Exterro, Inc. All rights reserved

Send File

To send a file to an endpoint:



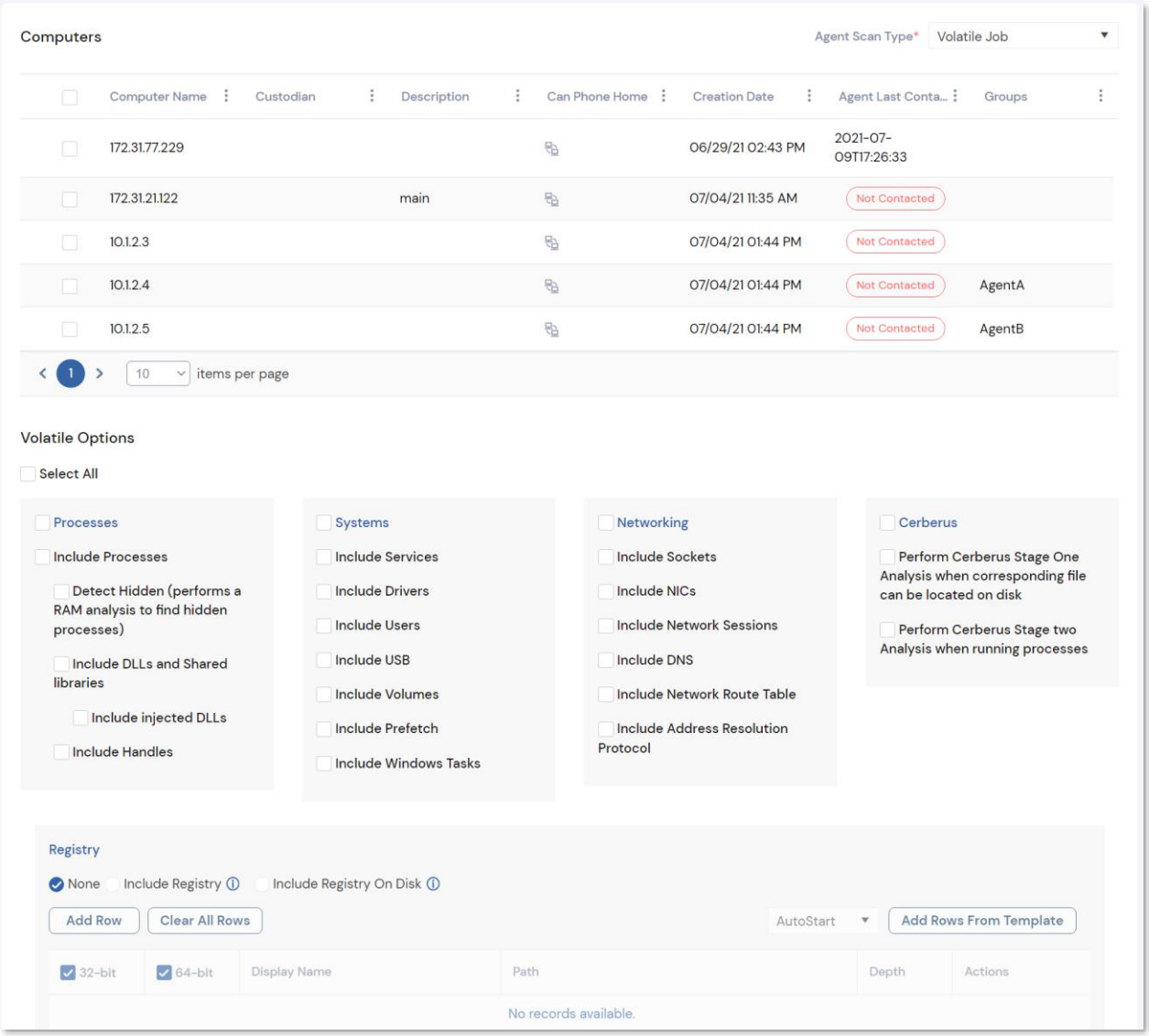
36. Ensure the Send File option has been selected for the Remediation Command field.
37. Provide a **Description**.
38. Enter or browse & select the **Source File Path** (the file being sent).
39. Enter the **Destination File Path** (where the file will be stored).
40. Select any one of the following operation commands if required:
    - **Delete File**
    - **Execute**
        - **Arguments**

41. Click **Save**.
42. Click **Save and Next.**
43. Configure the **Scheduling & Approvers** section based on your requirements.
44. Click **Save and Next**.
45. Click **Submit Collection**.

© Exterro, Inc. All rights reserved

Volatile Job

Volatile job performs an analysis of the processes, connections, services running on the operating system as well as any (customizable) registry files using Volatility. The subsequent XML files generated from Volatility can be found within the case folder. This data can be processed through Cerberus if required.



© Exterro, Inc. All rights reserved

To set up the volatile job for agent scan collections:

1. Select **Volatile Job** for the **Agent Scan Type** field.
2. Check the required **Volatile Options**.

Option Names	Descriptions
Processes	
Include Processes	To collect the processes running (at the time) in the agent
Detect Hidden (performs a RAM analysis to find hidden processes)	To collect the hidden processes running (at the time) in the agent
Include DLLs and Shared Libraries	To collect all the DLLs and Lib files in the agent
Include injected DLLs	To collect all the DLLs injected in the agent
Include Handles	To collect all the handles present in the agent
System	
Include Services	To collect the details of all services on the agent
Include Drivers	To collect the details of the drivers from System32\Drivers
Include Certificates	To collect the Imported Certificates of the agent
Include Users	To collect the user details
Include USB	To collect the USB details
Include Volumes	To collect the details of the system's physical or logical volumes
Include Prefetch	To collect the cached data
Include Windows Tasks	To collect the data of the tasks performed on the agent (Action, Task, and Triggers)
Networking	

© Exterro, Inc. All rights reserved

Option Names	Descriptions
Include Sockets	To collect the details of the Ports used to access or listen (present at the time)
Include NICs	To collect the network device details
Include Network Sessions	To collect the SMB (Server Message Block) network sessions
Include DNS	To collect the DNS (Domain Name System) present in the network
Include Network Route Table	To collect the IP routing
Include Address Resolution Protocol	To collect the ARP (Address Resolution Protocol) used in the network
Cerberus	
Perform Cerberus Stage One Analysis when corresponding file can be located on the disk	To collect the files using the YARA Rule file in ad.jam folder (present in the modules folder) of the agent
Perform Cerberus Stage Two Analysis when running processes	To collect the files using the YARA Rule file in ad.jam folder (present in the modules folder) in the agent

Note: If required, you can enable the **Select All** option to select all **Volatile Options**.

3. Select any one of the below provided **Registry** options:
   - **None**
   - **Include Registry** – To include information relating to the selected registry key.
   - **Include Registry On Disk** – To include information relating to the selected registry key as well as any hidden values.

© Exterro, Inc. All rights reserved

4. Upon selecting a **Registry** option, select any one of the below provided pre-defined templates from the drop-down and click on **Add Rows From Template**.

- AutoStart
- General
- Hardware
- UserActivity

Warning: The above field will be disabled if **None** is selected as the **Registry** option.

5. Click **Save and Next**.
6. Configure the **Scheduling & Approvers** section based on your requirements and click **Save and Next**.
7. Click **Submit Collection**.

Note: When collecting processes from a Linux endpoint, some processes may return a hash value of 0. This is correct as these particular items are forked processes, drivers or routines from a parent process.

Tip: To classify volatile jobs efficiently, the **ObjectType** and **ObjectSubType** columns can be used during review.

© Exterro, Inc. All rights reserved

Threat Scan

Threat Scan jobs are jobs that search for threats in the data. Threat Scan jobs apply filters from the IOCs and YARA rules to the data and alert you to suspicious files.

IOCs are XML documents that allow you to capture information about threats to your enterprise, including malware, registry changes, and memory artifacts. YARA rules are custom rules that you import that allow you to hunt for malware by values found in the binary or in physical memory.

Note: When creating or locating a YARA rule, make sure that the YARA rule identifier (the first line of the YARA rule) contains only alphanumeric characters and the underscore '_' character. For more information about writing YARA rules, see the YARA user manual at http://plusvic.github.io/yara/ .

© Exterro, Inc. All rights reserved

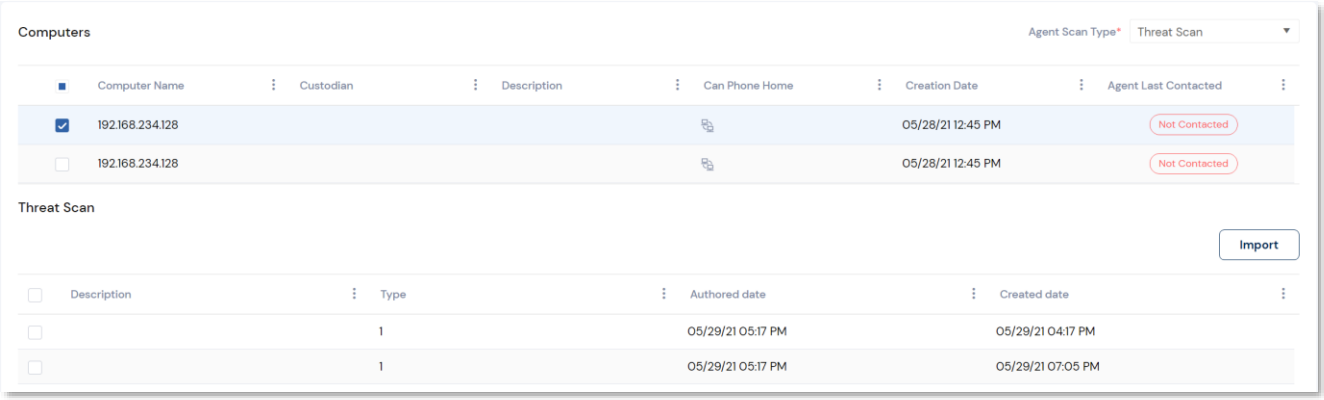
Criteria for Successful IOCs

When either creating or examining an IOC, make sure that IOC contains the following criteria:

- The focus of the IOC should be narrow. Rules specified in the IOC should focus on one particular aspect instead of casting a wide net in the data. For example, instead of an IOC rule specifying the examination of an entire system, the rule should specify a file path within the system. Or if a registry is to be examined, the IOC should examine a hive in the registry, not the full registry.

- The IOC should not consume massive system resources. Rules specified in the IOC should avoid taxing system resources. For example, if you are searching for a specific item, you should specify that the IOC examines the metadata, which can be restricted by filter. If you specify that the IOC examines the inner details, the system must open and examine every file. This consumes more system resources and taxes the system.

- An IOC with more indicator items is better than an IOC with fewer indicator items. Rules specified in the IOC should have as many indicator items as necessary. This allows the IOC to filter the data to a more manageable subset. For example, an IOC that searches for a file that is smaller than 10MB and is larger than 5MB (5<x>10) will be more successful than an IOC that only searches for a file that is smaller than 10MB (10<x).

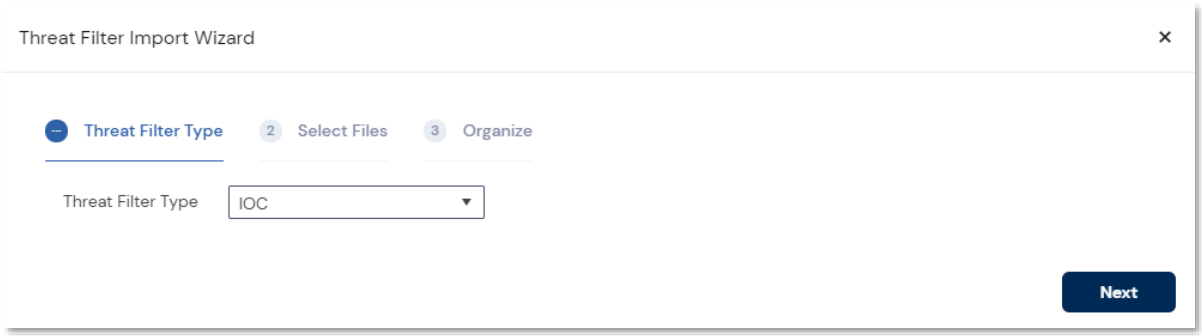


© Exterro, Inc. All rights reserved

IOC

To perform an IOC threat scan on an endpoint:

1. Select **Threat Scan** as the **Agent Scan Type**.
2. Click **Import**.
   - The **Threat Filter Import Wizard** prompt is displayed.



3. Select **IOC** for the **Threat Filter Type** field.
4. Click **Next**.
5. Click **Add Files** or **Add Folder** to browse and import the required set of rules.

Note: You can enable the **Directory processing is recursive** option in order to process the child folders and files.

6. Click **Save and Next**.
7. If required, enter a Source, Category, Tag and Group.
8. Click **Submit**.
9. Check the imported rules.
10. If required, select and configure the required **Advanced Options** provided below**:**

- Perform String Content Search
- Disable File Hashing
  - Disable only for files larger than
- Disable YARA for files larger than
- Archive Drill Down

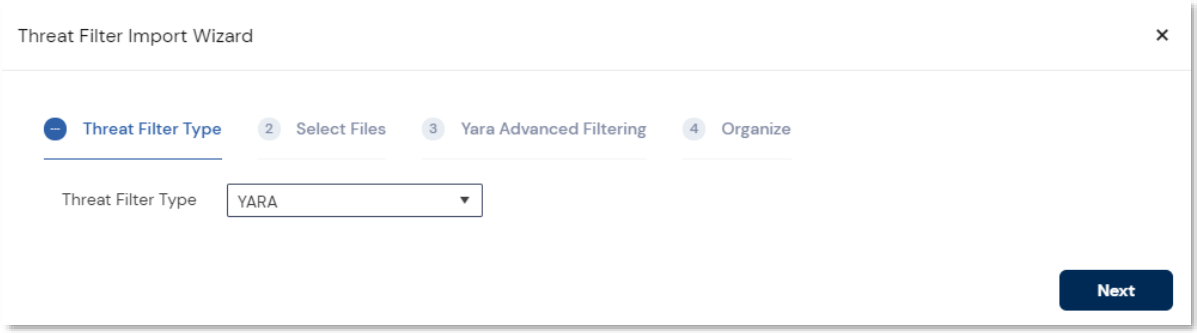
11. Click **Save and Next**.
12. Configure the **Scheduling & Approvers** section based on your requirement.
13. Click **Save and Next**.
14. Click **Submit Collection**.

© Exterro, Inc. All rights reserved

YARA

To perform YARA threat scans on an endpoint:

1. Select **Threat Scan** as the **Agent Scan Type**.
2. Click **Import**.
   - The **Threat Filter Import Wizard** prompt is displayed.



3. Select **YARA** for the **Threat Filter Type** field.
4. Click **Next**.
5. Click **Add Files** or **Add Folder** to import the required set of rules.

Note: You can enable the **Directory processing is recursive** option in order to process the child folders and files.

6. Click **Save and Next**.

© Exterro, Inc. All rights reserved

7. Select any of the below provided **Yara Advanced Filtering** options.

- **Target Process** - Allows the YARA rule to target memory and other processes.
- **Target Files** - Allows the YARA rule to target files. You can filter the files by the following:
  - **Extension** - Allows you to filter files by extension. List multiple extensions in a comma separated list. You can filter the extensions by either an equal or not equal operator. You can use a star (*) as a wildcard.
  - **Path Contains** - Allows you to filter files by the path contains. You can enter a partial path in the field as well as enter a fully qualified path.
  - **File Size (Bytes)** - Allows you to filter files by file size. You can filter file size by the following operators: any, equal, greater than, or less than. Specify the file size by bytes, kilobytes, or megabytes.
  - **File Creation Date** - Allows you to filter files by file creation date. You can filter the file creation date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.
  - **File Modified Date** - Allows you to filter files by file modification date. You can filter the file modification date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.
  - **File Last Accessed Date** - Allows you to filter files by file last accessed date. You can filter the file last accessed date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.
- **Target Both** - Allows the YARA rule to target both memory and other processes.

© Exterro, Inc. All rights reserved

8. Click **Save and Next**.
9. If required, enter the information for Source, Category, Tag and Group fields.
10. Click **Submit**.
11. Check the imported rules.
12. If required, select any of the below provided **Advanced Options**:
    - Perform String Content Search
    - Disable File Hashing
        - Disable only for files larger than
    - Disable YARA for files larger than
    - Archive Drill Down
13. Click **Save and Next**.
14. Configure the **Scheduling & Approvers** section based on your requirements.
15. Click **Save and Next**.
16. Click **Submit Collection**.

© Exterro, Inc. All rights reserved

Collecting Matched Files

When a Threat Scan is complete and has found matches on an endpoint, FTK Central will create a Threat Scan Filter which can be found in the case. The item will be listed in the review grid as **Threat Scan Filter**. While the threat scan filter will list the name of the matched files, it will further include the path, created date, modified date, accessed data, MD5 hash as well as the size.

To collect the matched files:

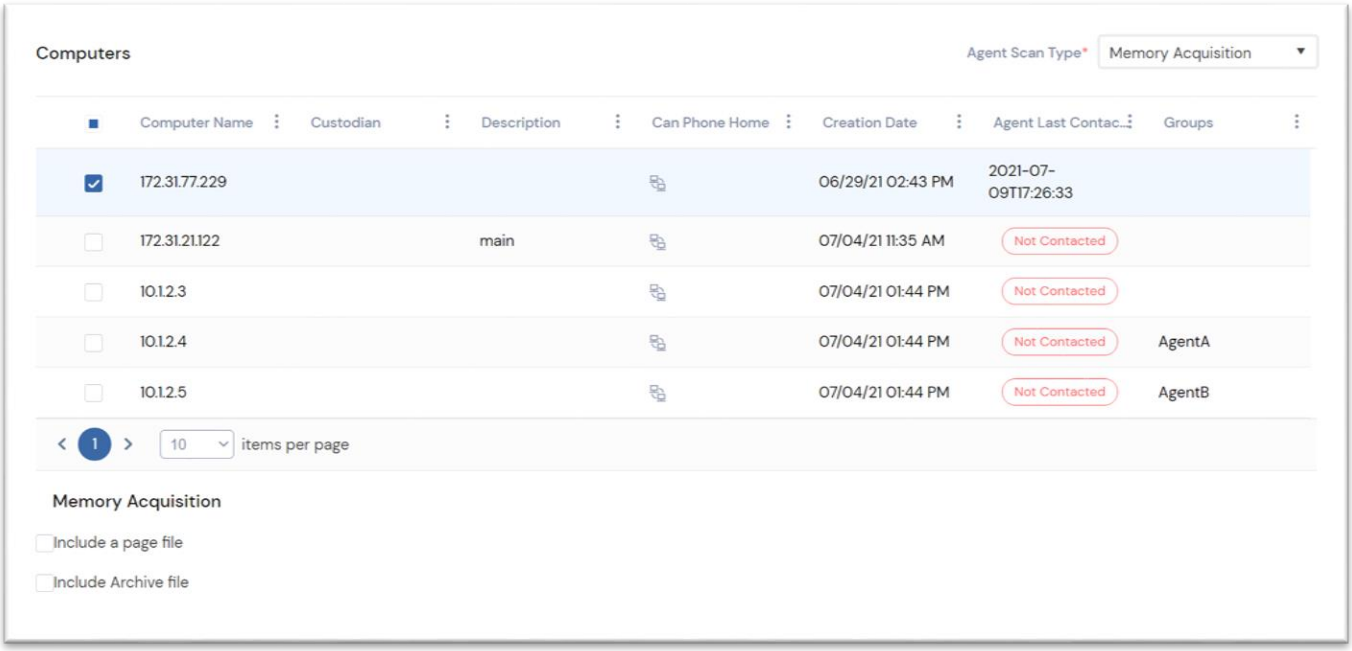
1. From the homepage, click **Case**.
2. Select a case that has had a successful threat scan job completed.
3. Click on the case name.
4. Click **Enter Review**.
5. Locate the **Threat Scan Filter** in the grid.
6. Check the required files to be collected.
7. Click **Collect Files**.

This will automatically collect the matched items and the processed files will be displayed in the case Review.

© Exterro, Inc. All rights reserved

Memory Acquisition

Executes a memory acquisition job that includes a page file and creates an archive file. The file can be found in the jobs folder associated to the case configured during collection.



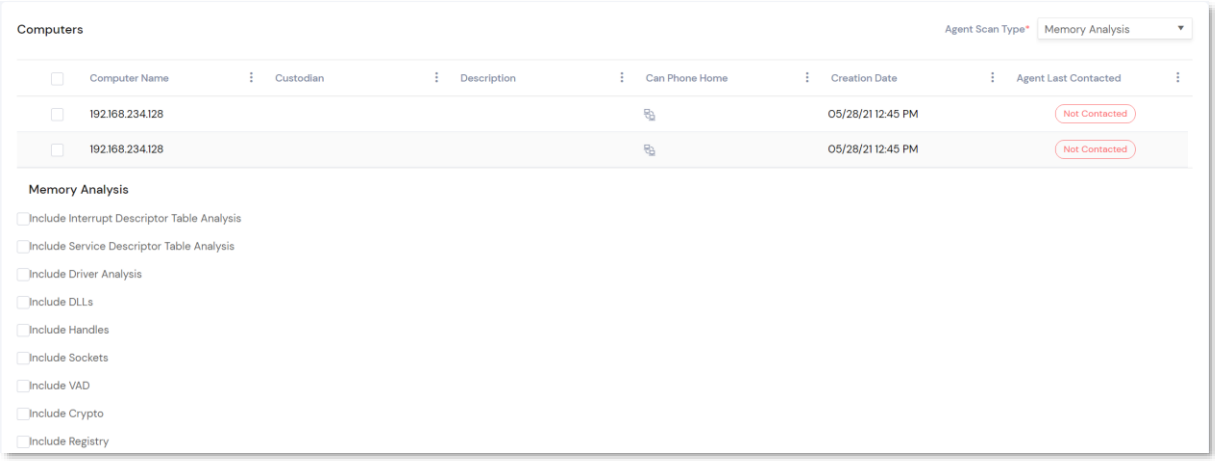
To acquire memory from an endpoint:

1. Select **Memory Acquisition** as the **Agent Scan Type**.
2. Select the required **Memory Acquisition** options.
3. Include a page file
4. Include Archive file
5. Click **Save and Next**.
6. Configure the **Scheduling & Approvers** section based on your requirement.
7. Click **Save and Next**.
8. Click **Submit Collection**.

© Exterro, Inc. All rights reserved

Memory Analysis

Executes a memory analysis job collecting DLLs, Drivers, Handles, Registry, Sockets, and VAD information.



To configure the memory analysis job:

1. Select **Memory Analysis** as the **Agent Scan Type**.
2. Select the required **Memory Analysis** options:

- Include Interrupt Descriptor Table Analysis
- Include Service Descriptor Table Analysis
- Include Driver Analysis
- Include DLLs
- Include Handles
- Include Sockets
- Include VAD
- Include Crypto
- Include Registry

3. Click **Save and Next**.
4. Configure the **Scheduling & Approvers** section based on your requirement.
5. Click **Save and Next**.
6. Click **Submit Collection**.

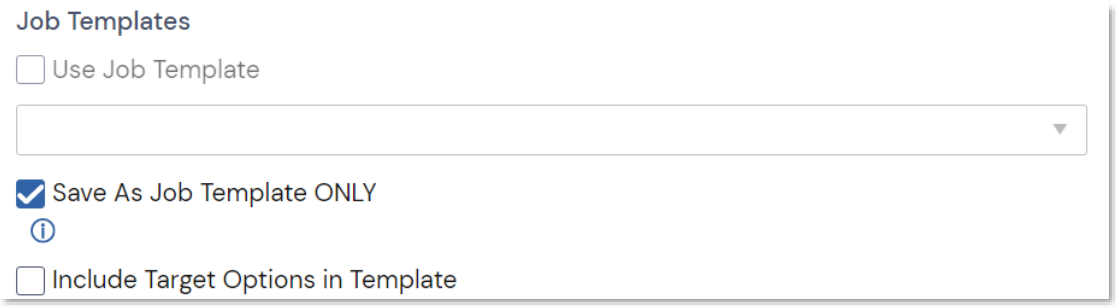
Tip: The **Memory Analysis** column set in review mode can be utilized to efficiently review memory data.

© Exterro, Inc. All rights reserved

Job Template

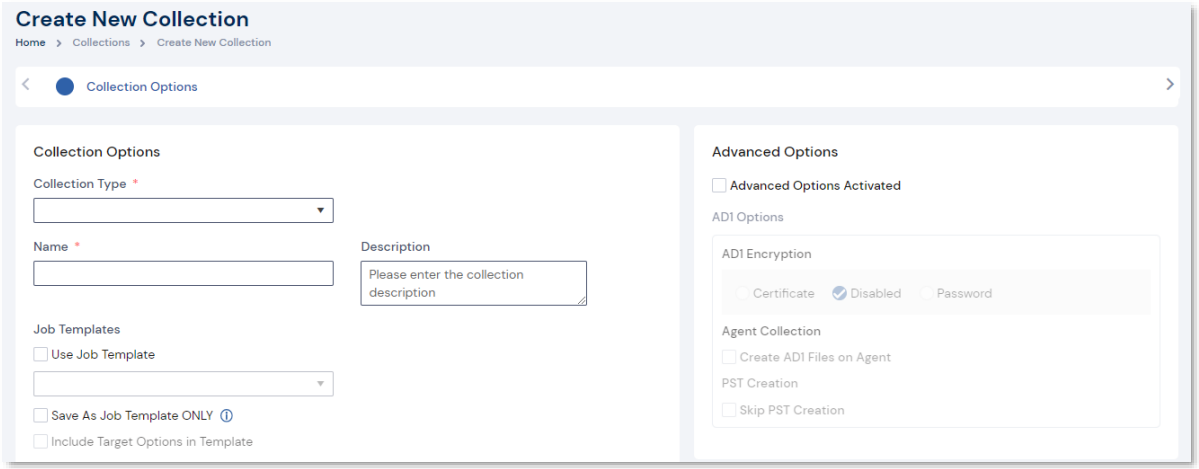
Creating a Job Template

The job templates can be utilized to create a pre-configured collection intended to assist you during collection creation. Templates can be edited during execution, if required.



To create a job template:

1. From the homepage, click **Collections**.
2. Click **Create New Collection**.
   - The **Create New Collection** page will be displayed.



3. Configure the **Collection Options**.

© Exterro, Inc. All rights reserved

4. Enable the **Save As Job Template ONLY** option in order to save the configured information as a template to be used later.

Note: You can enable the **Include Target Options in Template** option to also save the **Target Options** configuration to the template.

5. Select further collection options.

Note: These changes made to the collection plan after enabling the **Save As Job Template ONLY** option will also be saved to the template.

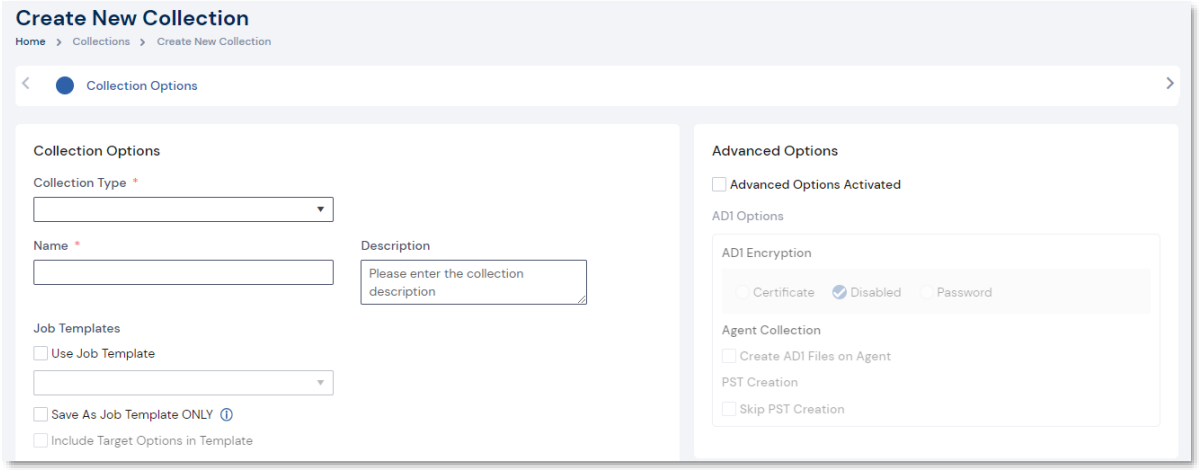
6. Click **Submit Template**.

© Exterro, Inc. All rights reserved

Selecting a Job Template

To select a job template:

1. From the homepage, click **Collections**.
2. Click **Create New Collection**.
   - The **Create New Collection** page will be displayed.

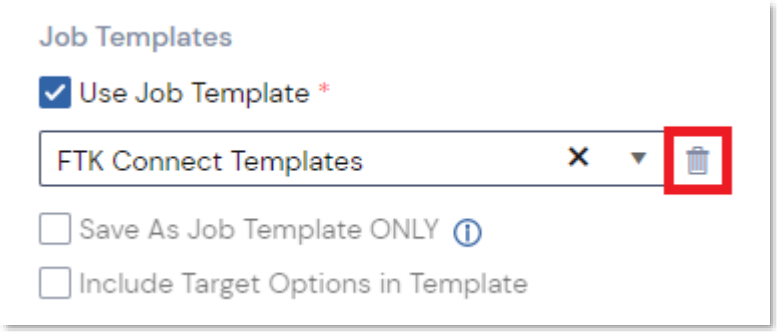


3. Configure the Collection Options.
4. Enable the Use Job Template option.
5. Select the required template from the drop-down list.
6. Upon selecting the template, corresponding information will be auto-populated to the relevant fields.

© Exterro, Inc. All rights reserved

Note:

- You can choose to delete the selected job template by clicking on the **Delete Job Template** icon displayed against the selected template.



- If the **Include Target Options in Template** option is enabled while creating a template, the corresponding targets information will also be selected during collection creation.

© Exterro, Inc. All rights reserved

Managing Collections

After creating a collection, based on the approval, execution, and processing options, you will have to manage the collection to complete it. This section helps you in managing the collection at various statuses.

Depending on the stage on which the collection is at a moment, there are 8 statuses for a collection as listed below:

Collection Status	Description
Not Started	Collection has been created but no collection data has been retrieved.
Collecting	Collection process has started and data is being collected.
Completed	Collection is completed and data has been retrieved.
Cancelled	Collection has been cancelled.
Terminated	Collection has been terminated by a user.
Failed	Collection has failed.
Completed with Errors	Collection is completed but with some errors during collection.
Pending	Collection is yet to start, pending approval.

Tip: To filter the grid efficiently, you can simply enter a keyword into the search box

located at the top of any grid and click the search button or press enter.

© Exterro, Inc. All rights reserved

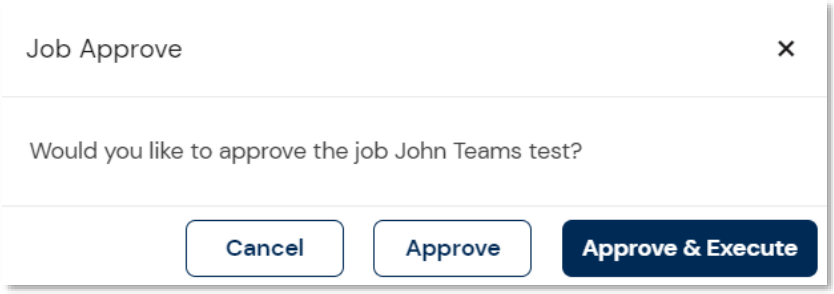
Approving Collections

Depending upon the Approval Mode selected, the collection has to be approved before it can be executed.

Warning: If multiple approvers were selected during the collection creation, all the selected users must approve the collection.

To approve a collection:

1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Click on the **Context menu** against the required collection.
4. Click on **Approve Collection**.
   - The **Job Approve** prompt is displayed.



5. Click **Approve**.

Notes:

- You can click on **Approve & Execute** to concurrently approve and execute the collection process.
- The collection will be approved for processing and the process will be initiated based on the **Execution Mode** configured for the collection.

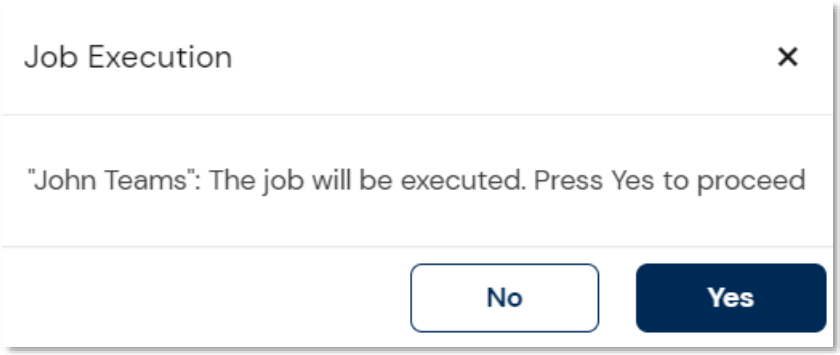
© Exterro, Inc. All rights reserved

Executing Collections

Executing a collection initiates the process of collecting the data from the target data sources. Based on the execution mode selected, you may have to manually trigger the execution for a collection. It is to be noted that you can execute a collection only after it is approved.

To execute a collection:

1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Click on the **Context menu** against the required collection.
4. Click on **Execute Collection**.
   - The **Job Execution** prompt is displayed.



5. Click **Yes**.

© Exterro, Inc. All rights reserved

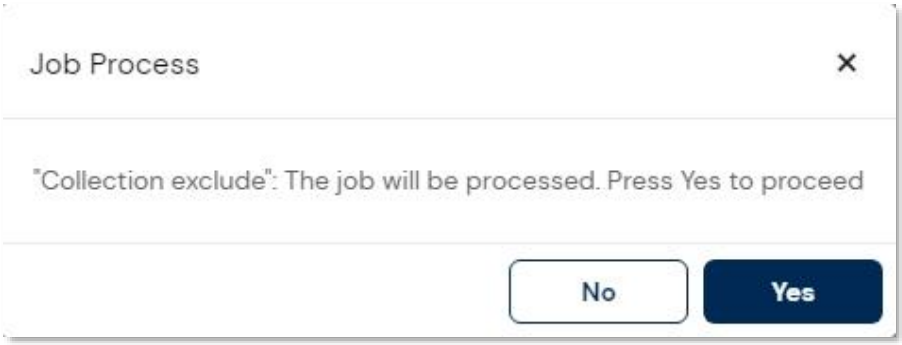
Processing Collections

If you automatically process a collection, the full collection is processed each time. For example, for the first collection, 100 files are processed. The second collection, 105 files are processed. The third collection, 145 files are processed.

During the review process you will see 350 files. If the same file occurs during all three collections, then the object names will remain identical, but the objectids will be unique.

To process a collection:

1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Click on the **Context menu** against the required collection.
4. Click on **Process Collection**.
   - The **Job Process** prompt is displayed.



5. Click **Yes**.

© Exterro, Inc. All rights reserved

Cancelling Collection Process

To cancel a collection process:

1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Click on the **Context menu** against the required collection.
4. Click on **Cancel Collection**.
   - The **Job Cancellation** prompt is displayed.

5. Click **Yes**.

© Exterro, Inc. All rights reserved

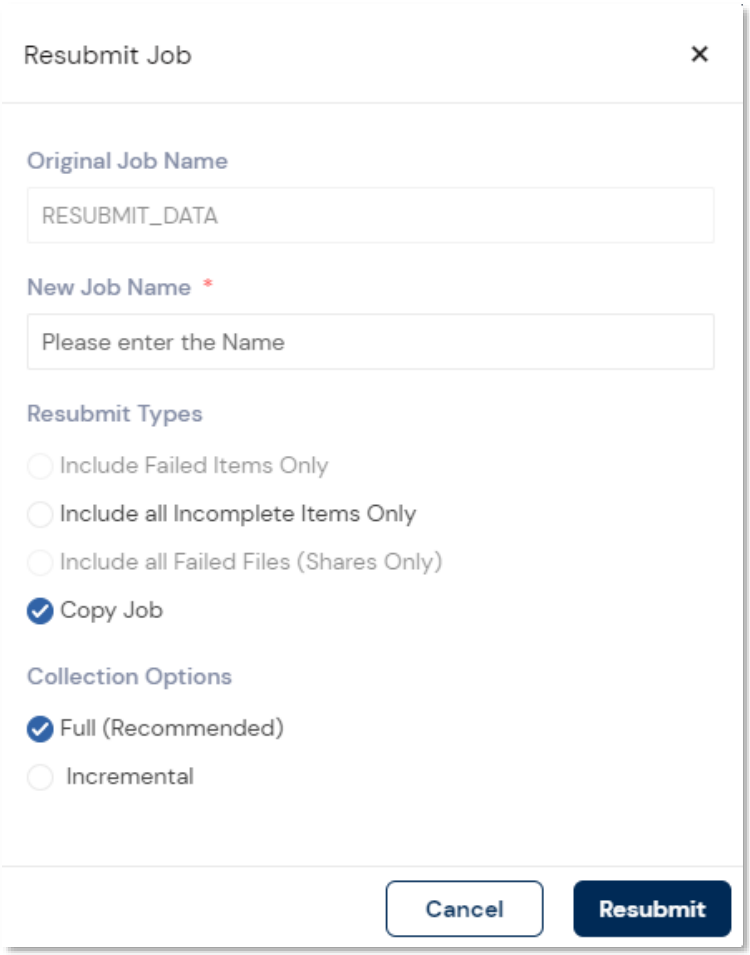
Resubmitting Collections

There may be situations where collection jobs have been stopped or failed due to your circumstances.

Resubmitting a collection will allow you to run a collection job against the target again.

To resubmit a collection job:

1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Click on the **Context menu** against the required collection.
4. Click on **Resubmit Collection**.
   - The **Resubmit Job** prompt is displayed.



5. Provide a name for the resubmitted collection in **New Job Name**.

© Exterro, Inc. All rights reserved

6. Select any one of the following **Resubmit Types** based on their descriptions:
   - **Include Failed Items Only** – To collect only the failed files.
   - **Include all Incomplete Items Only** – To collect all the files that were not collected in the previous iteration.
   - **Include all Failed Files (Shares Only)** – To collect all the files that were not collected in the previous iteration from just the Network Shares data source.
   - **Copy Job** – To duplicate the collection process and re execute the collection based on the **Collection Option**.

7. Select any one of the following **Collection Options** based on their descriptions:
   - **Full** – To collect all the files present in the data sources associated to the collection.
   - **Incremental** – To collect only the files newly added to associated data sources after completing the collection process.

8. Click **Resubmit**.

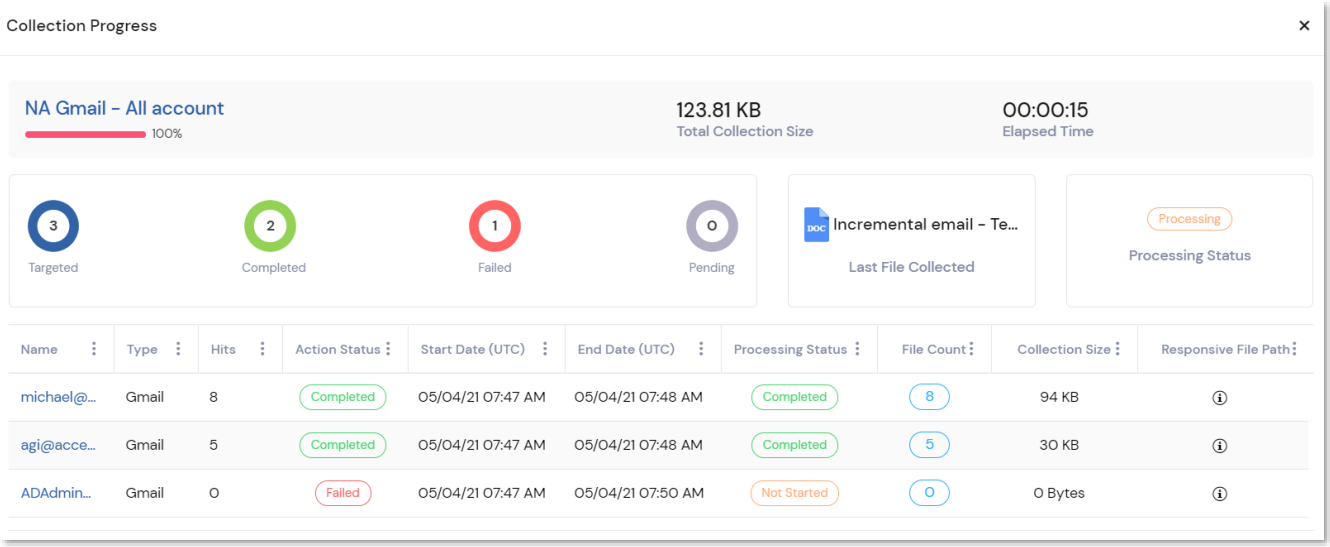
© Exterro, Inc. All rights reserved

Viewing Collection Details

You can view a snapshot of collection which includes information about the name of the collection, collection progress (in terms of percentage), total volume of files collected, time taken to collect the files, number of data sources targeted, last collected file, etc.

To view the collection details:

1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Click on the **Context menu** against the required collection.
4. Click on **Collection Details**.
   - The **Collection Progress** prompt is displayed.



Note: You can click on **Responsive File Path** button against the required data source to view the location path where the collected files are stored.

© Exterro, Inc. All rights reserved

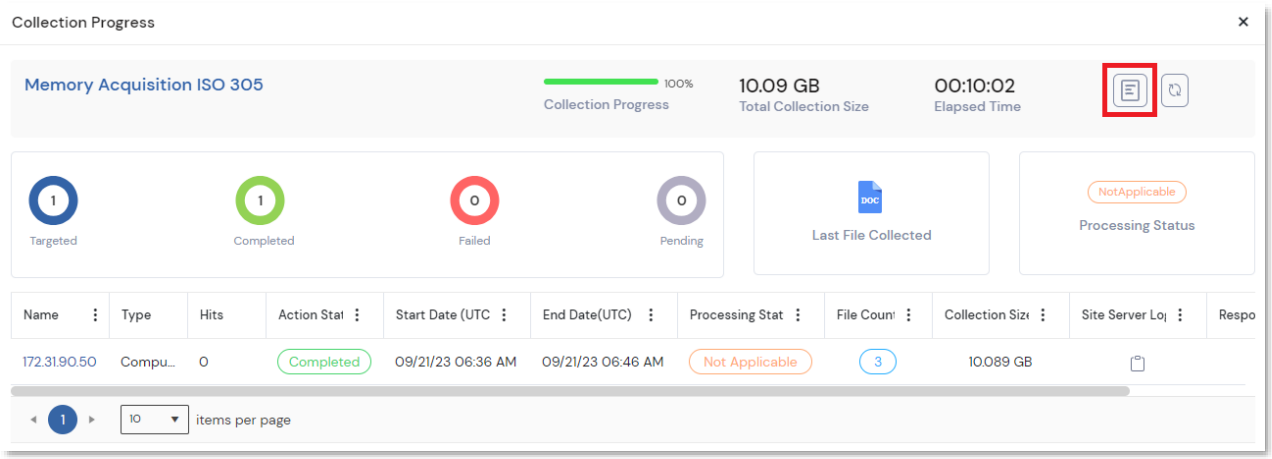
Generating Reports for Collections

You can generate detailed information reports on collected files, emails, file statistics, remediated files, etc. of a collection.

Warning: You can generate a report only after the collection is processed.

To generate the reports specific to a collection:

1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Click on the **Context menu** against the required collection.
4. Click on **Collection Details**.
5. From the Collection Progress pop-up, click on the **Download Reports** button.



6. Select any of the below mentioned reports to download it in **.xlsx** format.

Report Name	Description
Details Report	Provides a detailed snapshot of the collection which includes the Collection options, data sources, collection results (success/failure) for nodes.

© Exterro, Inc. All rights reserved

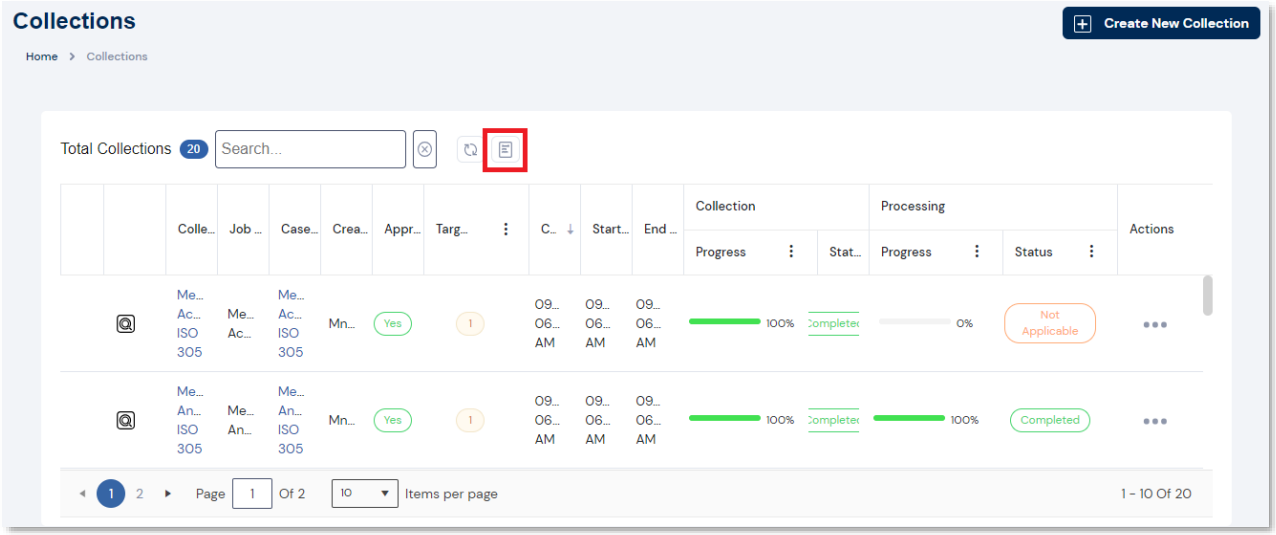
Report Name	Description
Results Report	Displays information on collection results for the job. When using a collection job to collect emails, an EmailID is generate for each email by FTK Central. This EmailID is displayed in a column in the collected email and failed email tabs of the jobs results report. ***Note:*** *The Microsoft Teams data sources collected via 'Export API' will have the following limitations:* • *The 'File Breakout' tab will be empty since the export chats are collected as message files.* • *The files attached to the messages will not be displayed under the 'Collected Files' tab.* • *The 'Subject' column under 'Collected Email' tab is empty since they are collected as email files.*
Errors Report	Displays a breakdown of failed targets and the errors associated to the collection.

Tip: The downloaded reports will also be available in the Case Folder Path.

© Exterro, Inc. All rights reserved

To generate the System Wide Collection Report:

1. From the home page, click **Collection**.
2. Click on the **Generate System Wide Collection report** button .



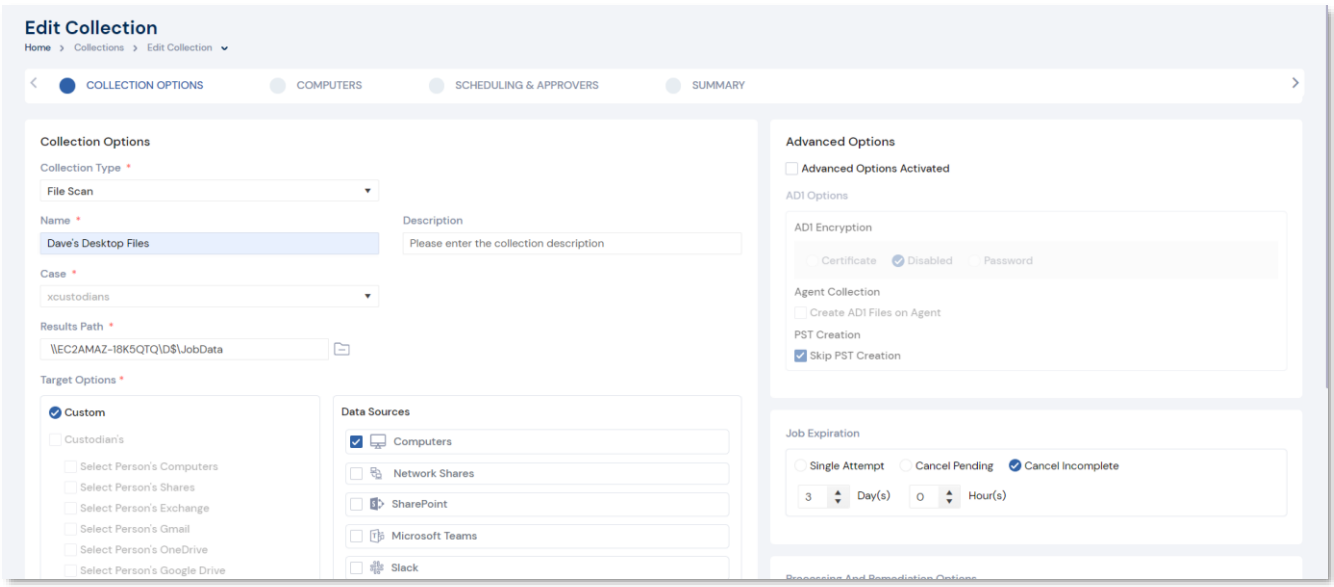
A job will be initiated to generate the System Wide Collection report. Upon job completion, you can download the report from the **Job Queue**.

© Exterro, Inc. All rights reserved

Editing Collections

To edit a collection:

1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Click on the **Context menu** against the required collection.
4. Click on **Edit Collection**.
   - The **Edit Collection** page is displayed.



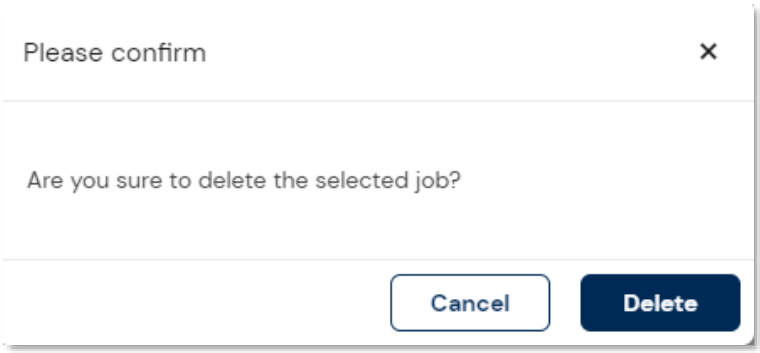
5. Make the necessary changes.
6. Click **Submit Collection**.

© Exterro, Inc. All rights reserved

Deleting Collections

To delete a collection:

1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Click on the **Context menu** against the required collection.
4. Click on **Delete Collection**.
   - The **Please confirm** prompt is displayed.



5. Click **Delete**.

© Exterro, Inc. All rights reserved

Reviewing Collections

To review a collection:

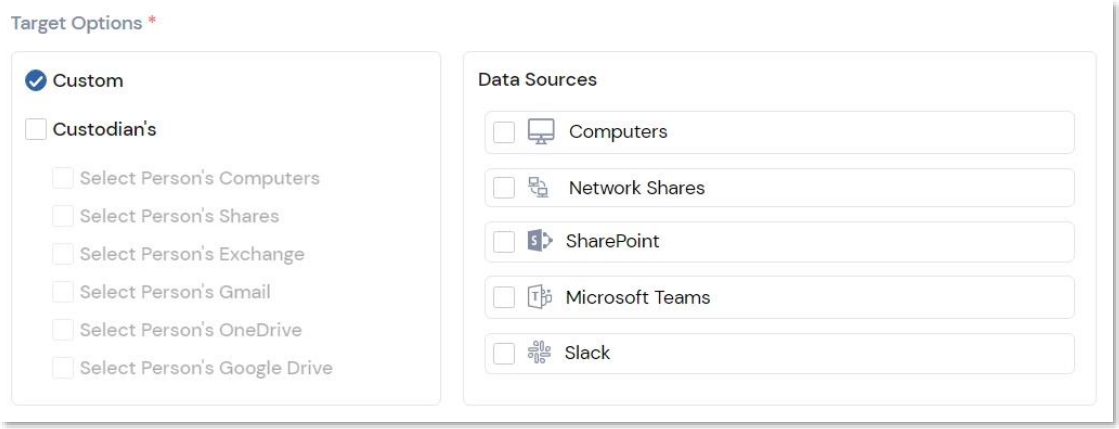
Users can access an associated case to a collection efficiently by using the review icon. This icon will navigate users to the review mode.

1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Click on the **Review** icon against the required collection.
   - The associated case will open in review mode.

© Exterro, Inc. All rights reserved

Data Source Configuration for Collection

In order to collect information from the required data sources, you should select the required options from the **Target Options** field while creating a collection. Here, the options in **Custodian's** and **Data Sources** are mutually exclusive i.e., you can select either **Custodian's** or **Data Sources**.



Notes:

- Only upon enabling the **Custodian's** checkbox, the corresponding options will be enabled.
- You can select more than one options for **Custodian's** and **Data Sources** fields.

Note: Ensure the Creating Collections Section has been reviewed before attempting a Data Source collection.

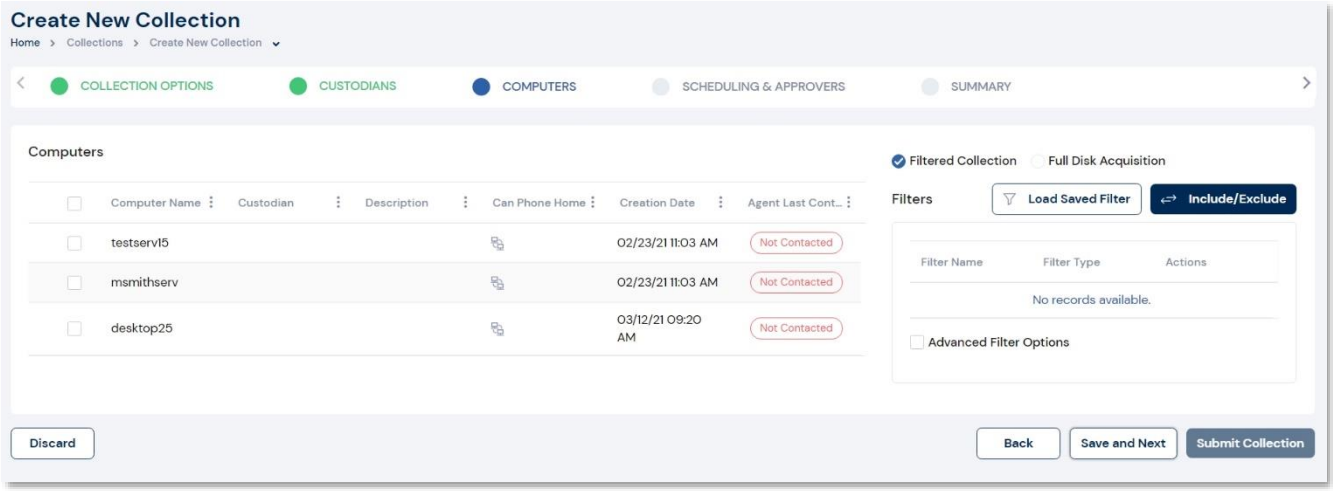
© Exterro, Inc. All rights reserved

Custodian-based Collections

To configure the custodian data source for collection:

Upon selecting the required data sources under the **Custodian's** section,

1. Select the required custodians from the list



2. Click **Save and Next**.

Based on the selected data sources, any or all of the following data sources are to be configured:

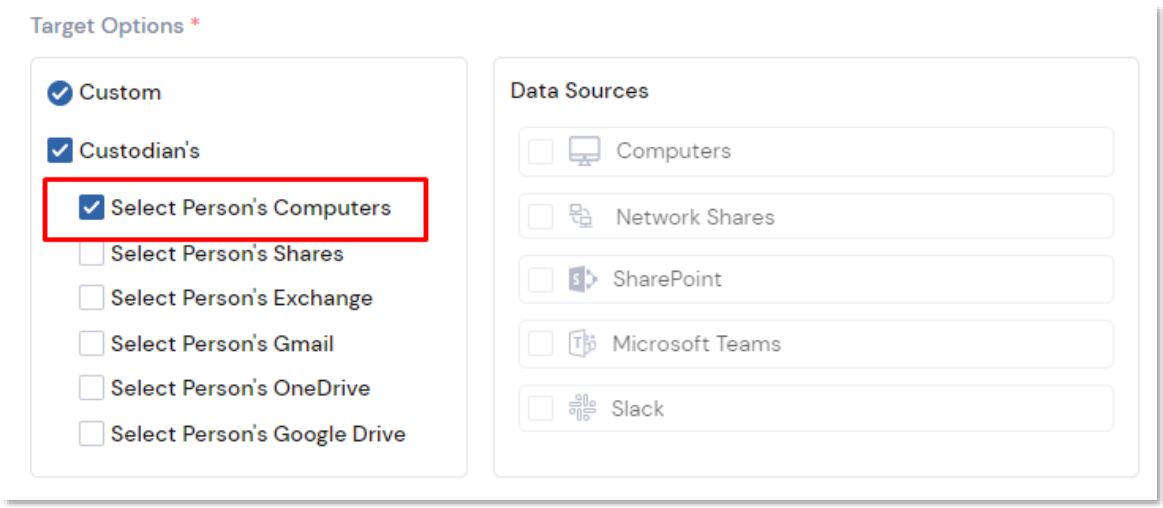
© Exterro, Inc. All rights reserved

Computers

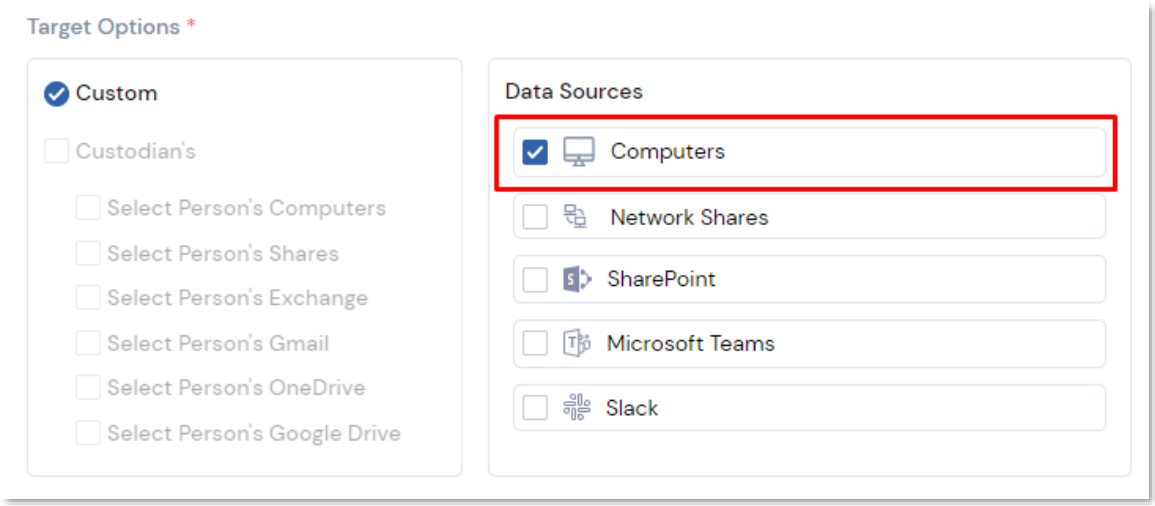
Computer-based collections allow endpoint collections with exclusive configuration options as listed below.

Auto Deploy Agents

The Auto Deploy option will be applicable only when the computer is selected in the target options, either against the Custodians or Data Sources.



(OR)

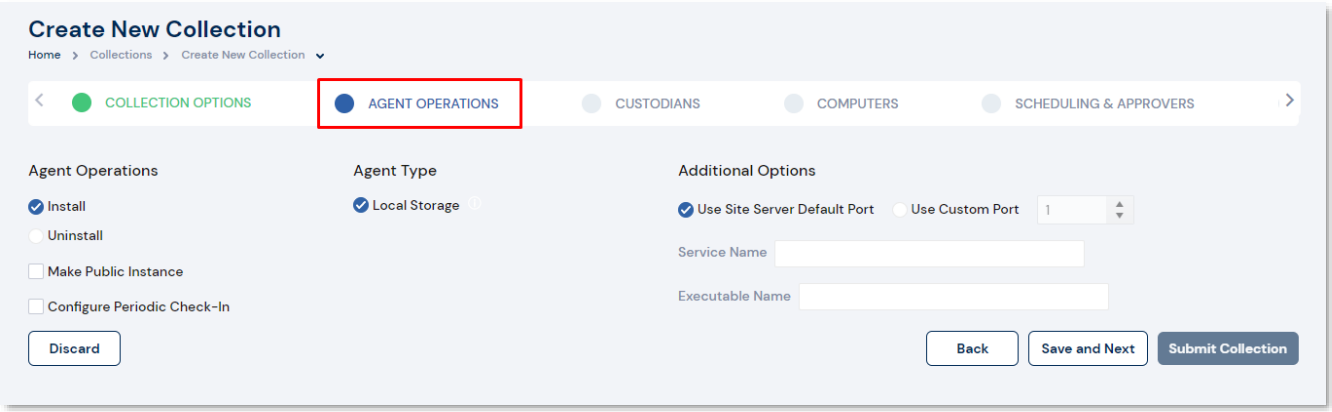


© Exterro, Inc. All rights reserved

1. Upon enabling the **Auto Deploy Agents** checkbox and clicking on **Save and Next**, the below **Agent Operations** section will be displayed.

On the Agent Operations page, select from the following options:

Option	Description
Uninstall	Select to remove the agent from the machine
Install	Select to push the agent to the machine. Remember that the agent install may cause the machine to restart without a warning.
Make Public Instance	Configure the agent to check a public instance after the agent is installed.
Configure Periodic Check-In	Configure the agent to communicate back to the server.
Agent Type – Local Storage	Agent uses local files for configuration and data. Agent is installed (persists after reboot).
Use Site Server Default Port	Enabling this will force the agent to use Port:54545
Use Custom Port	Enter the port designated to communicate with the agent.
Service Name	Enter the name that you want the agent to be displayed as.
Executable Name	Enter the name of the file that is being run.



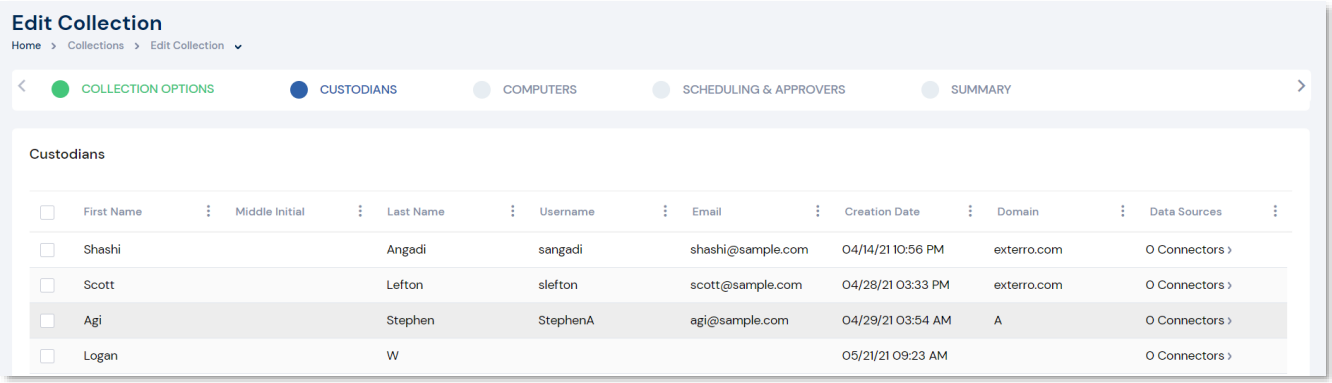
© Exterro, Inc. All rights reserved

Upon selecting the required agent operations and clicking on Save and Next, you will be navigated to the **Custodians** section.

(OR)

If the **Agent Deploy** option is not selected in the **Collection Options** section, the Agent Operations section will be skipped and you will be navigated to the **Custodians** section.

Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **Computers** section.



2. Select the required computers from the list.

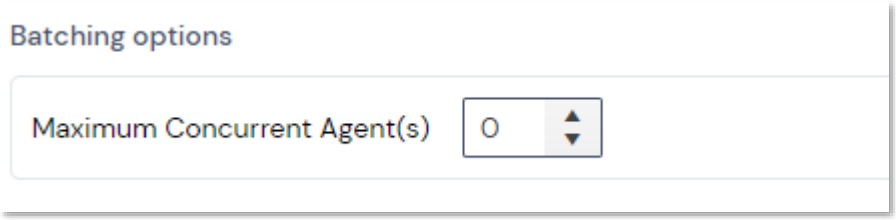
Warning: You cannot proceed to collect all the data from the computer. You must include at least one among the Extension, Size, Date, Path, Luhn, Keyword, or MD5 Hash filter properties within the Include/Exclude filters to perform a targeted collection.

3. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Batching Options

While multiple collections can run simultaneously, Batching Options allow jobs to run in groups. I.e. A selection of 3 Maximum Concurrent Agents will only allow 3 concurrent jobs to be run at once until finished, which would then allow the next batch of jobs to be started.



Advanced Filter Options

You can configure the **Advanced Filters** section in the right pane to filter and collect only the required information based on the type of Collection. The applicable filters for the collection types are listed below:

i. For Filtered Collection:

Type	Options	Description
Source Type	File System	To collect the drives from the target's file system.
	Logical Disk	To collect only the target's logical drive space.
	Physical Disk	To collect the target's entire physical drive.
Search Type	Siteserver	To search using the Site Server.
	Agent & Siteserver	To search first with the agent and then with the Site Server.
	Agent	To search files using the agent.
	Collect System Files	To search system files that are normally hidden from view. Files with "$" contain system meta data and in NTFS, the $MFT contains the file system pointers to all files.

© Exterro, Inc. All rights reserved

Type	Options	Description
	Scan Deleted Files	To scan free space of a partition for files matching the filter criteria.
	Scan Unused Disk Area	To scan unallocated disk space for files matching filter criteria.
	Archive Drill Down	If archive files exist in any of the available data sources that contain compressed files of interest, this option lets you open the archive files as part of the job and checks them against keywords supplied in the keyword filter.
	Collect Responsive Archives	Collects any archive that contains files that match filter criteria.
	Custom Drill Down Extensions	Allows you to specify the extension for the archive drill down. If you do not specify the extension, the default will be used.
	Include Deleted Files	Will scan free space of a partition for files matching filter criteria.
	Use Internal File Identification	Sees the software's file identification when checking file extensions.
	Collect Non-Extension Files	Collects all files that do not have an extension.
	Collect Unsearchable Encrypted Files	Will collect encrypted files that cannot be accessed to search for keyword filter criteria.
	Enable PreScan	Will scan the collection target before collecting. Enables accurate completion percentage, file counts, and size predictions for Real Time Status screen.

© Exterro, Inc. All rights reserved

Type	Options	Description
	Parse $130 INDX Records	Gets additional information about deleted files.
	Exclude Removable Drives/Media	Excludes removable drives that are recognized by Site Server from the collection. This option is only available for collection jobs. Not all removable drives are recognized as such so this option may not exclude ALL removable drives

ii. System Summary

This collection type will only collect files to generate a System Summary. Collected files will not be auto processed unless explicitly selected in the previous configuration page. Users must ensure that if auto processing is required, that the "Generate System Summary" Processing Option is included within the Processing Profile

Note: Only Windows Agents are supported for this job type. If a Linux Agent is selected, it will be skipped.

© Exterro, Inc. All rights reserved

iii. FTK XML Filters

The FTK XML Filter workflow allows users to import XML based filters from FTK Enterprise into FTK Central. These collection filters can be used to make the most of existing filters to collect specific artifacts at any given time.

This workflow allows users to do the following:

- Configure a specific path to store XML Filters
- Configure collections using existing FTK XML Filters
- Upload XML Filters from machines that have no direct access to the folder storing XML filters

Configuring the XML Filter Path:

The following configuration allows users to set a folder which will store all filters. This folder should be configured as required.

i. Open Windows Services and stop the FTK Central Weblab Self Host.
ii. Navigate to C:\Program Files\AccessData\Forensic Tools\x.x\bin
iii. Open ADGWeblabSelfHost.exe.config in a text editor.
iv. Locate the following configuration key:
XMLFilterPath
v. Within the value, enter a path which should be used to store any XML filters
vi. Ensure this file is saved.
vii. Restart the FTK Central Weblab Self Host

The path configured in this configuration key will be used as the storage location for any XML filters going forward. Users must ensure that any preexisting filters are copied into this directory to be available in the UI.

© Exterro, Inc. All rights reserved

Creating a Filtered Collection using an FTK XML Filter

The following steps will allow users to create a collection using an existing FTK XML Filter. It is to be noted that the filters listed will be those that have been uploaded to the configured path set in the 'Configuring the XML Filter Path' section.

i. Login to FTK Central.

ii. Navigate to **Collections**.

iii. Click **Create New Collection**.

iv. Select **File Scan**.

v. Enter the following details:

- **Name**
- **Case** - Select an existing case to store collected files
- **Data Sources** - Computers
- **Other options** can be customized at the discretion of the user

vi. Click **Save and Next**.

© Exterro, Inc. All rights reserved

What are you looking for?

Collection Options

Collection Type *
File Scan

Name *
Test Collection XML Filter

Description
Please enter the collection description

Job Templates
Use Job Template
Save As Job Template ONLY
Include Target Options in Template

Case *
001Bacani

Results Path *
\\ec2amaz-ka8r2lu\F$\JobData

Target Options *
Custom Group
Custodians
Select Person's Computers
Select Person's Shares
Select Person's Exchange
Select Person's Gmail
Select Person's OneDrive
Select Person's Microsoft Teams
Select Person's Box
Select Person's Google Drive

Data Sources
Computers
Network Shares
SharePoint
Slack

Advanced Options
Advanced Options Activated

AD1 Options
AD1 Encryption
Certificate Disabled Password
Agent Collection
Create AD1 Files on Agent Location Create AD1 Files on Network
PST Creation
Skip PST Creation

Job Expiration
Single Attempt Cancel Pending Cancel Incomplete
3 Day(s) 0 Hour(s)

Processing And Remediation Options
Auto Process Collection
Processing Option*
Forensic Processing

Batching options
Maximum Concurrent Agent(s) 0

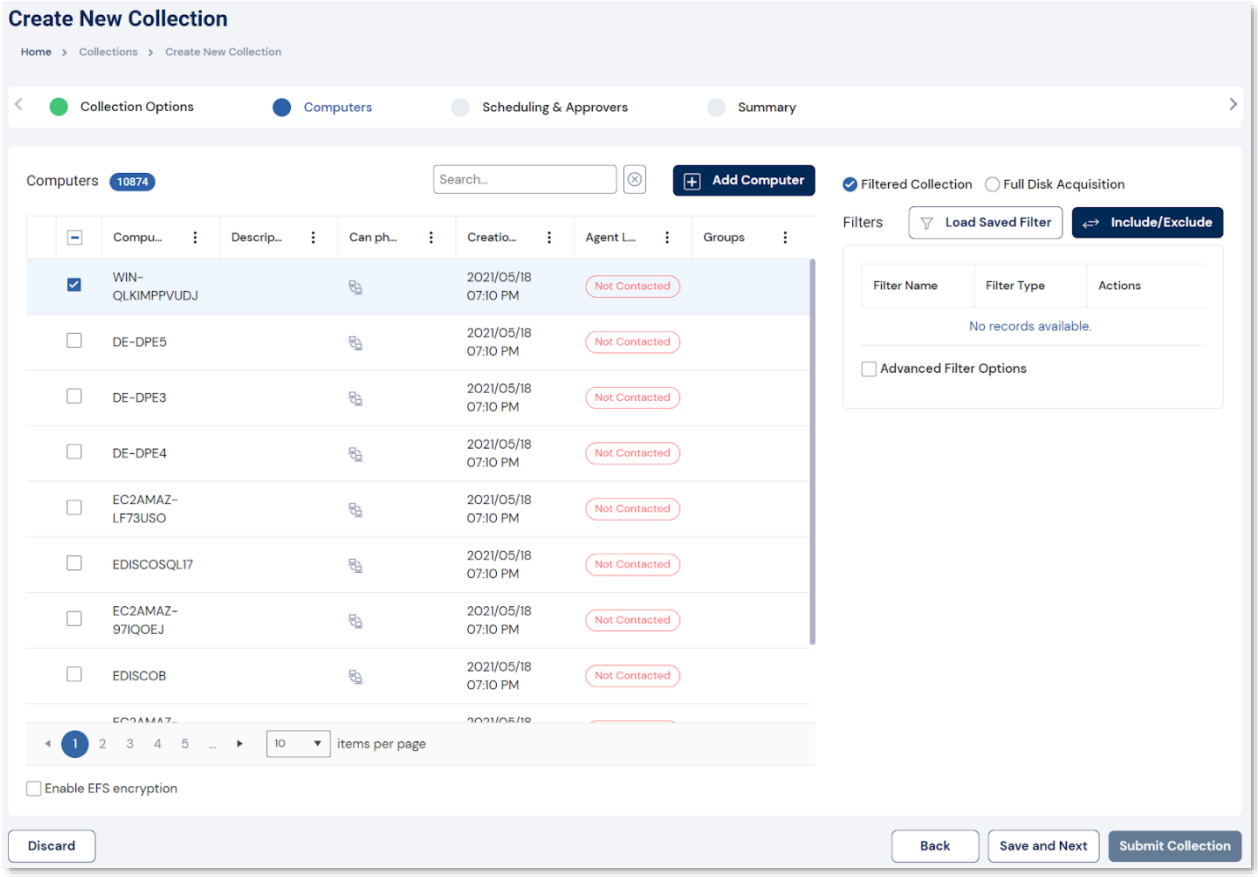
Auto Deploy
Auto Deploy Agents

Discard Back Save and Next Submit Collection

© Exterro, Inc. All rights reserved

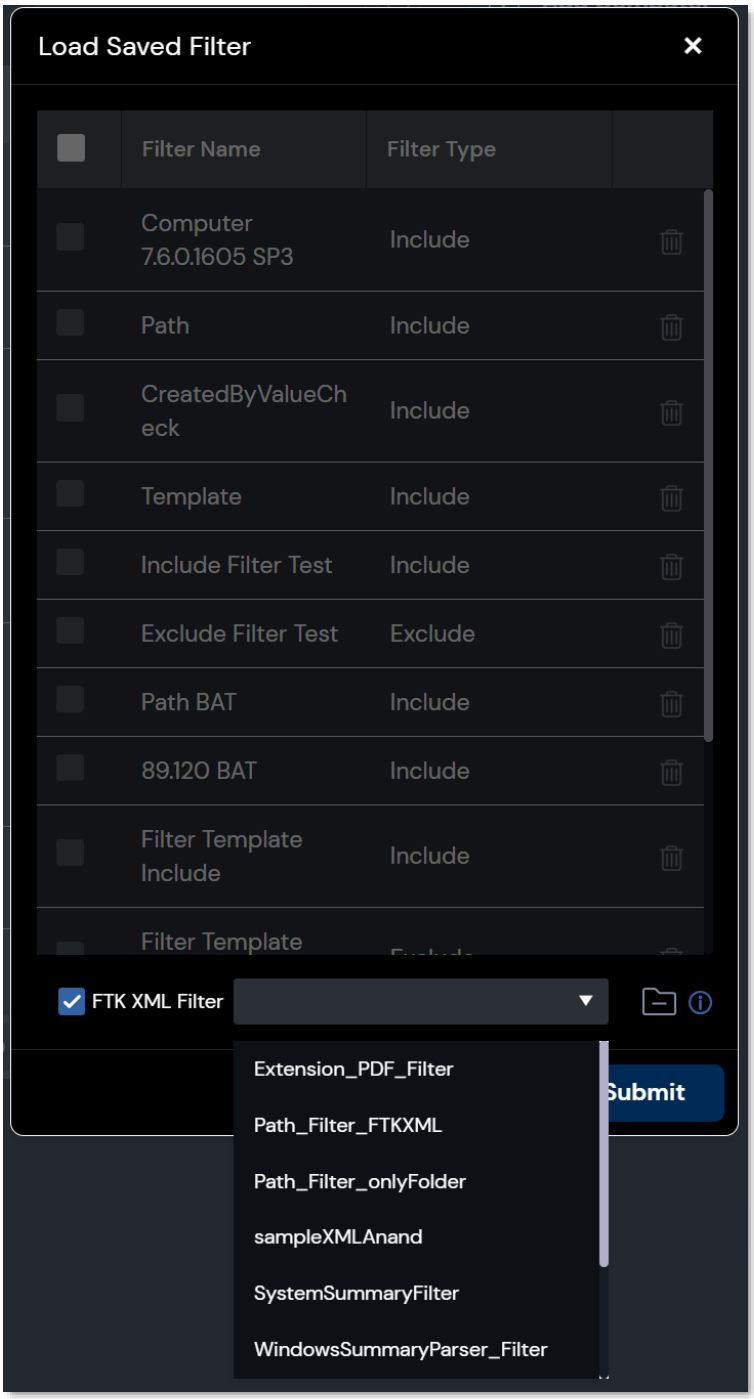
vii. Select an **Agent**.

viii. Select **Filtered Collection**.



© Exterro, Inc. All rights reserved

ix. Click on **Load Saved Filter.**



© Exterro, Inc. All rights reserved

x. Select **FTK XML Filter**.
   - Users cannot select multiple filters at the same time. If FTK XML Filter is selected, then only those filter types will be available for selection.

xi. Click the **drop-down list** to view uploaded XML Filters.
   - Alternatively, click the Folder icon to upload an XML filter into the configured path.

xii. Select a Filter and click **Submit**.

xiii. Click **Save and Next**.

xiv. At the **Scheduling & Approvers** screen, ensure this is set as **Automatic**.

xv. Click **Save and Next**.

xvi. Click **Submit Collection**.

viii. For Full Disk Acquisition

A Full Disk Acquisition job would collect the entire contents of a computer's hard drive, so the advanced options will include fewer choices as listed below:

- **Collect from Target Options**
  - **Logical Disk:** To collect only the target's logical drive space.
  - **Physical Disk:** To collect the target's entire physical drive. You can choose the sectors required.
- **Use Redirected Acquisition:** Uses the agent to push the collected data directly to the Job Data path given in the Job Options screen instead of moving it to the temporary storage location and then to the Job Data path.

© Exterro, Inc. All rights reserved

Include/Exclude Filter Options

When creating a filtered collection, Include/Exclude filters will be available. The table below lists all available options when creating a File Scan/Report Only collections.

<table>
<tr><th>Options</th><th>Descriptions</th></tr>
<tr><td>Filter Name</td><td>Allows you to name a filter when attempting to save it as a template.</td></tr>
<tr><td>Extensions</td><td>Allows you to filter files by extension. List multiple extensions in a comma separated list. You can filter the extensions by either an equal or not equal operator. You can use a star (*) as a wildcard.

Example:
<table>
<tr><th>Field</th><th>Clause</th><th>Example</th></tr>
<tr><td>Extension</td><td>Extension with full stop</td><td>.pdf</td></tr>
<tr><td>Extension</td><td>Extension with multiple spaces</td><td>.pdf, .jpg</td></tr>
<tr><td>Extension</td><td>Multiple extensions without spaces</td><td>pdf, jpg</td></tr>
<tr><td>Extension</td><td>Combination of extensions with/without full stops</td><td>.pdf, jpg</td></tr>
</table></td></tr>
</table>

© Exterro, Inc. All rights reserved

Options	Descriptions
Path	Allows you to filter files and folders by the exact (fully qualified) path provided in this field. **Example:** **Field** / **Clause** / **Example** Path / Forward slashes / //data/49ers Path / Multiple folders ***Note:*** *Supports both forward and backward slashes* / D:\Files\New test\Credit Card OR D:/Files/New test/Credit Card Path / Parent folder as a filter with multiple child filters / D:\Files\New test\ The following options will be automatically checked based on the path value entered in the field. • **Folder** – If the value provided in the field is a folder path. In this case all files in the path will be collected excluding the subfolders. ***Example:*** *C:\ProgramFiles\SampleFolder* • **Relative** – If the value provided in the field is a relative path. ***Example:*** *ProgramFiles\SampleFolder* • **Recursive** – This will be checked by default for all types of folder paths provided. In this case all files in the path will be collected

© Exterro, Inc. All rights reserved

Options	Descriptions
	including the subfolders. You can uncheck this option if you need to exclude the collection of subfolders. ***Warning:*** *If you manually uncheck all the above options after providing the path, no files will be collected from the path provided.*
File Size (bytes)	Allows you to filter files by file size. You can filter file size by the following operators: any, equal, greater than, or less than. Specify the file size by bytes, kilobytes, or megabytes. ***Note:*** *When the application collects zone.Identifier files from the Computer it also collects the files related to it. In such cases, some files that exceed the filter limit will also be collected.* ***Example:*** *When a size limit is set less than 60 KB, the system collects the zone.Identifier files that are within the limit and its related files of sizes 70 KB, 1MB, etc. that exceed the size limit.*
File Creation Date	Allows you to filter files by file creation date. You can filter the file creation date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.
File Modified Date	Allows you to filter files by file modification date. You can filter the file modification date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.
File Last Accessed	Allows you to filter files by file last accessed date. You can filter the file last accessed date by the following operators: any, range, or single. For range, you can specify either outside of the range or between the range.

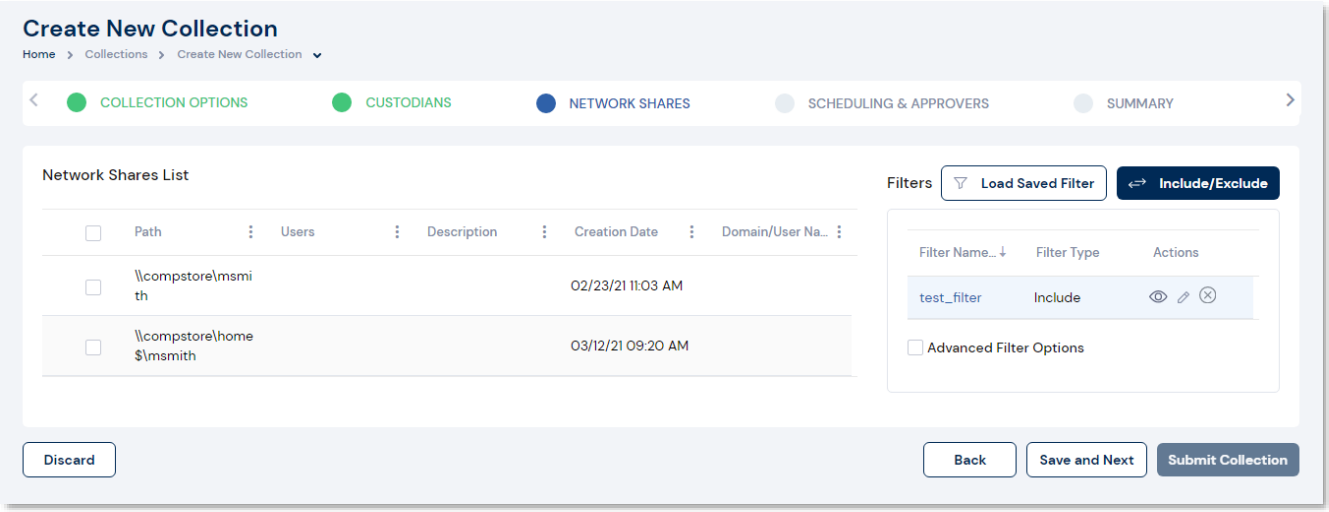
© Exterro, Inc. All rights reserved

Options	Descriptions
Keywords	Allows you to include files that match any or all regular expressions/keywords entered into the text field. When writing queries for the Keyword(s) field, use the terms AND or OR to help refine your search. For example: • Apple AND orange returns files with both terms apple and orange. • Apple OR orange returns files with either the term apple or orange. • (Apple AND orange) OR (banana) returns files with either the terms apple and orange or files with the term banana. • 'Apple and orange' OR banana returns files with either the term apple and orange or files with the term banana.
Credit Card Numbers	Used in conjunction with the Keyword option, the credit card option allows you to include credit card numbers using Luhn testing. Luhn testing distinguishes valid credit card numbers from what could be a random selection of digits.
Search File Name Only	Used in conjunction with the Keyword option, this forces the keyword search to only apply to file names.
Custom	Allows you to include a custom regex expression. To filter by regular expressions, enter the regular expression delimiters. For example: \d\d\d\d. **You are not able to use dashes when creating a custom regex expression.** For example: \d\d\d\-\d\d\-\d\d\d\d
MD5 Hash	Allows you to add specific MD5 hash values to be included in the job.

© Exterro, Inc. All rights reserved

Network Shares

Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **Network Shares** section.



1. Select the required network share locations from the list.

Note: You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Advanced Filter Options

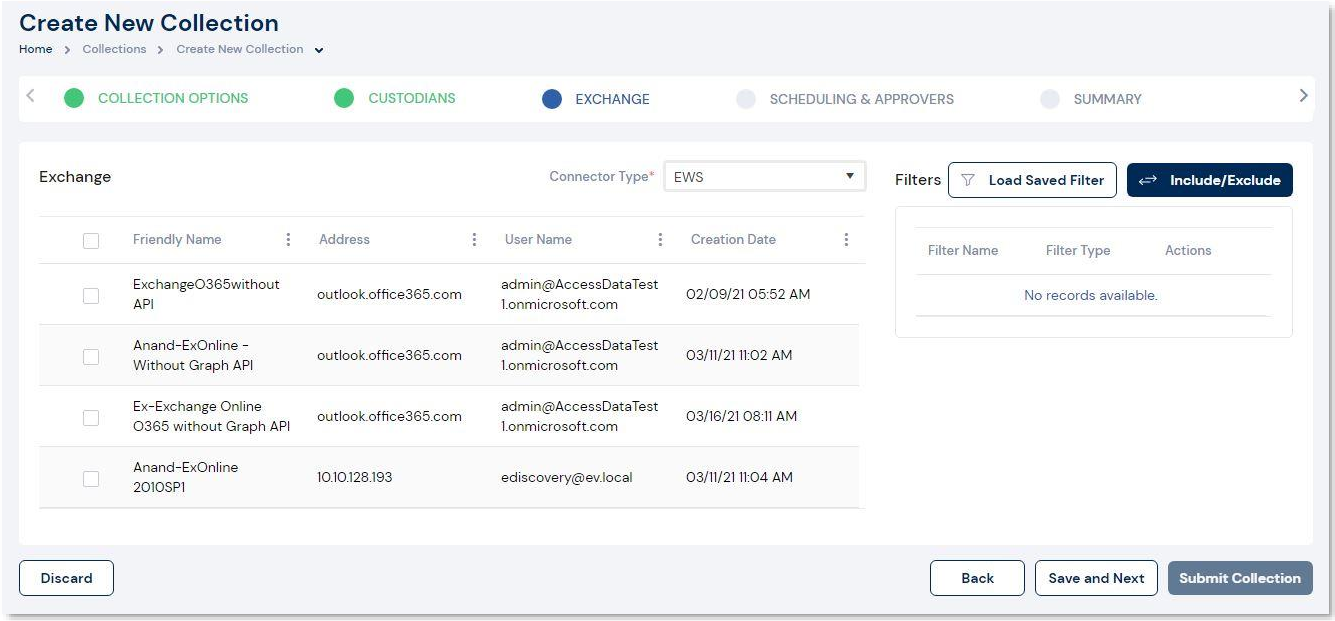
You can configure the **Advanced Filters** section in the right pane to filter and collect only the required information by using any of the filters provided below:

Filter	Description
Collect System Files	To search system files that are normally hidden from view. Files with "$" contain system meta data and in NTFS, the $MFT contains the file system pointers to all files.
Archive Drill Down	If archive files exist in any of the available data sources that contain compressed files of interest, this option allows you to open the archive files as part of the job and checks them against keywords supplied in the keyword filter.
Collect Responsive Archives	Collects the archive/container files (ZIP, RAR and so forth) of any responsive file when using the drill-down option.
Custom Drill Down Extensions	Allows you to specify the extension for the archive drill down. If you do not specify the extension, the default will be used.
Collect Non-Extension Files	Collect all files that do not have an extension.
Use Internal File Identification	Sees the software's file identification when checking file extensions.
Collect Unsearchable Encrypted Files	Collects files that cannot be accessed to search for keyword filter criteria.
Enable PreScan	Will scan the collection target before collecting. Enables accurate completion percentage, file counts, and size predictions for Real Time Status screen.

© Exterro, Inc. All rights reserved

Exchange

Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **Exchange** section.



1. Select the required Exchange mailbox connectors from the list. Ensure the Connector Type is appropriately selected. Exchange Admin Center (EAC), Exchange Web Services (EWS), Export API, and Graph API options will be listed in the drop-down list if configured.

Note: You can filter the files from the data source by using the Include/Exclude filters.

2. Select additional collection options if required. Applicable to EWS/Graph API collections only.

Collection Option	Description
Include Recoverable Deletes	Allows you to collect deletions. Deletions are enabled by default in Exchange. There's no need to specify a folder path because there is no folder structure retained for those items.
Include Recoverable Purges	Allows you to collect purges (hard deletes) of data. In order to collect purges from an Exchange server, enable purges in

© Exterro, Inc. All rights reserved

Collection Option	Description
	the Exchange server. There is no need to specify a folder path because there is no folder structure retained for those items.
Include Recoverable Versions	Allows you to collect versions of data that have been saved. In order to collect versions from an Exchange server, enable versions in the Exchange server. There is no need to specify a folder path because there is no folder structure retained for those items.
Include Archive MailBox	Allows you to collect from an archive mailbox.

3. Provide the required folder's name in the **Mailbox Folder Path(s)** field to collect the data present in the folder.

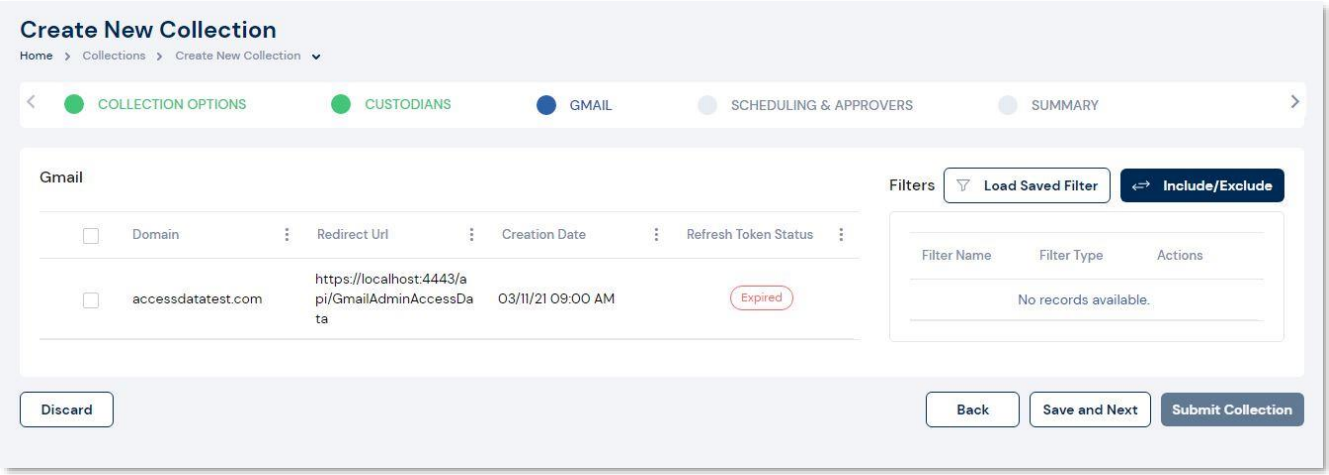
Note: You can also provide multiple folder names separated with commas (,) to collect the data present in all the specified folders.

4. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Gmail

Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **Gmail** section.



1. Select the required Gmail mailbox connectors from the list.

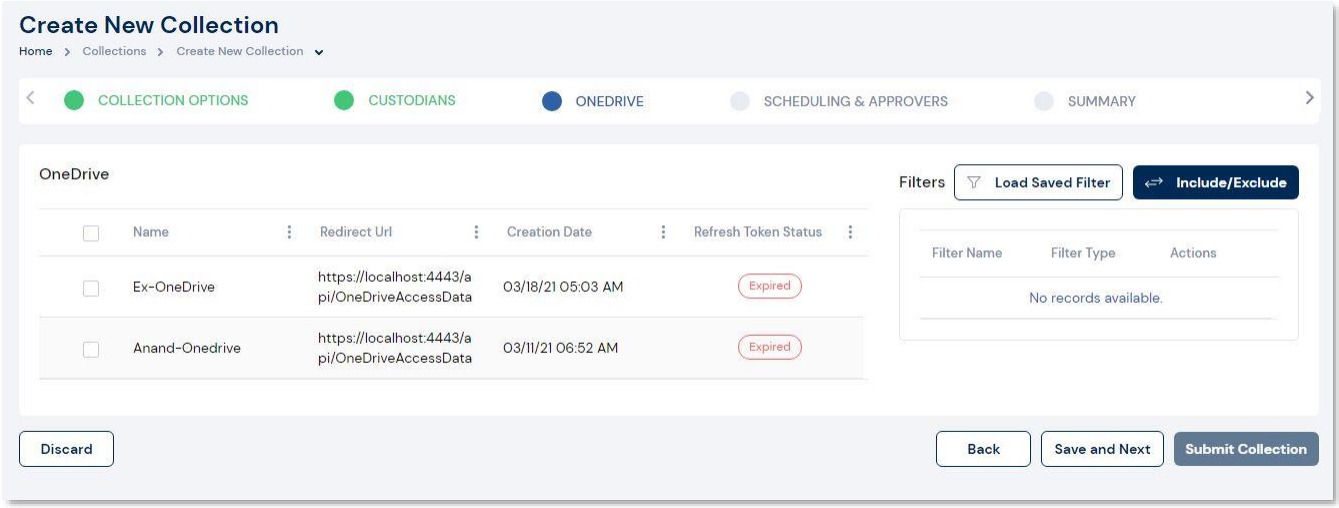
Note: You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.

© Exterro, Inc. All rights reserved

OneDrive

Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **OneDrive** section.



1. Select the required OneDrive connectors from the list.

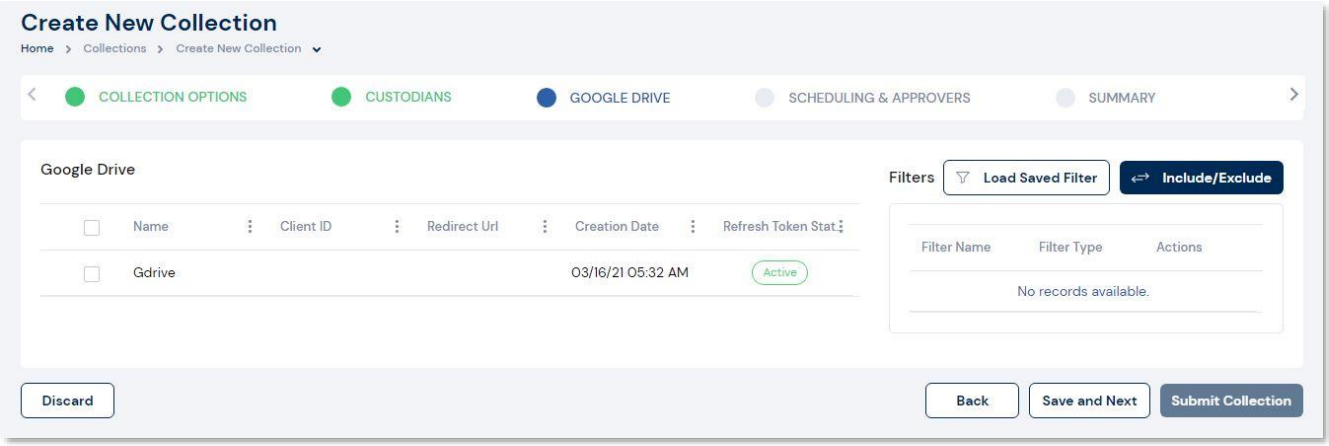
Note: You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Google Drive

Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **Google Drive** section.



1. Select the required Google Drive connectors from the list.

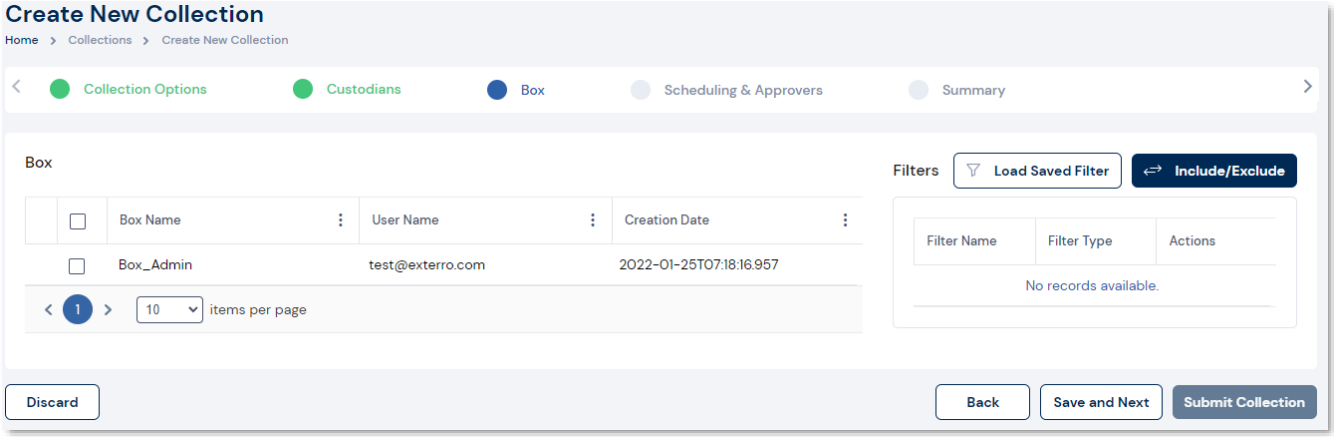
Note: You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Box

Upon selecting the required custodians and clicking on **Save and Next** from the **Custodians** section, you will be navigated to the **Box** section.



3. Select the required Box connectors from the list.

Note: You can filter the files from the data source by using the Include/Exclude filters.

4. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Data Sources

To configure the data sources for collection:

Upon selecting the required options for **Data Sources** field, any or all of the following data source are to be configured:

Note: Ensure the Creating Collections Section has been reviewed before attempting a Data Source collection.

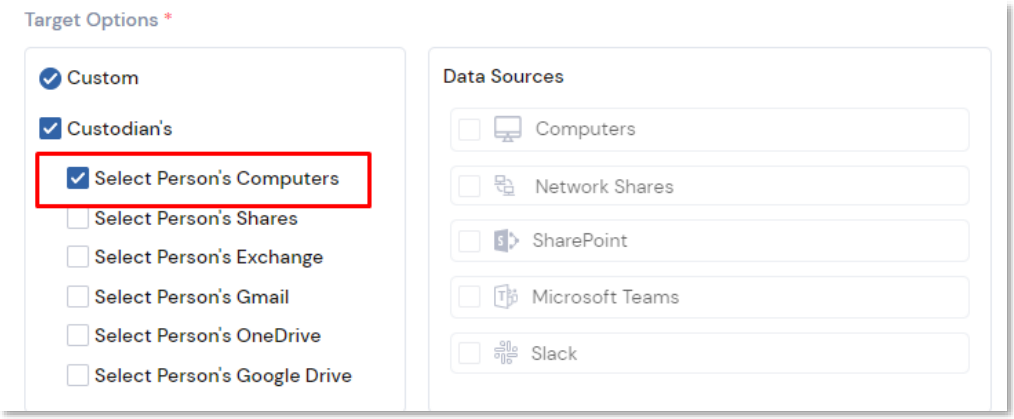
Additionally, if attempting a collection of GCC environment, refer to the Office 365 Credentials section.

© Exterro, Inc. All rights reserved

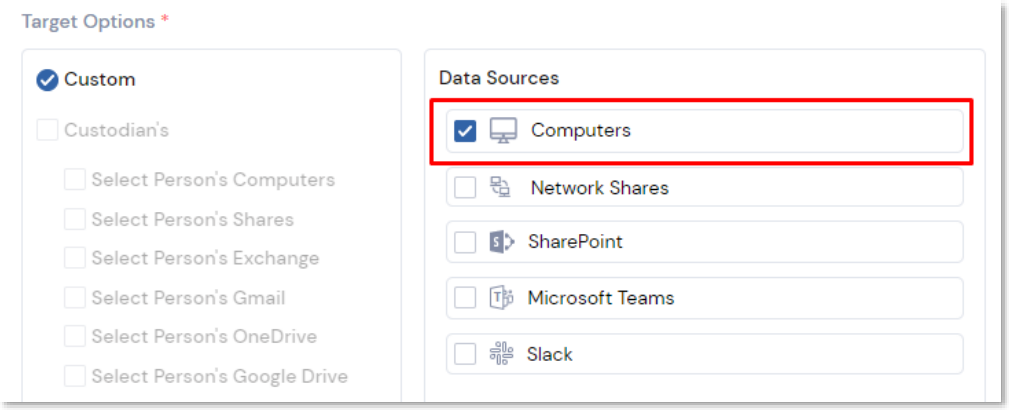
Computers

Auto Deploy Agents

The Auto Deploy option will be applicable only when the Computer is selected in the target options, either against the Custodians or Data Sources.

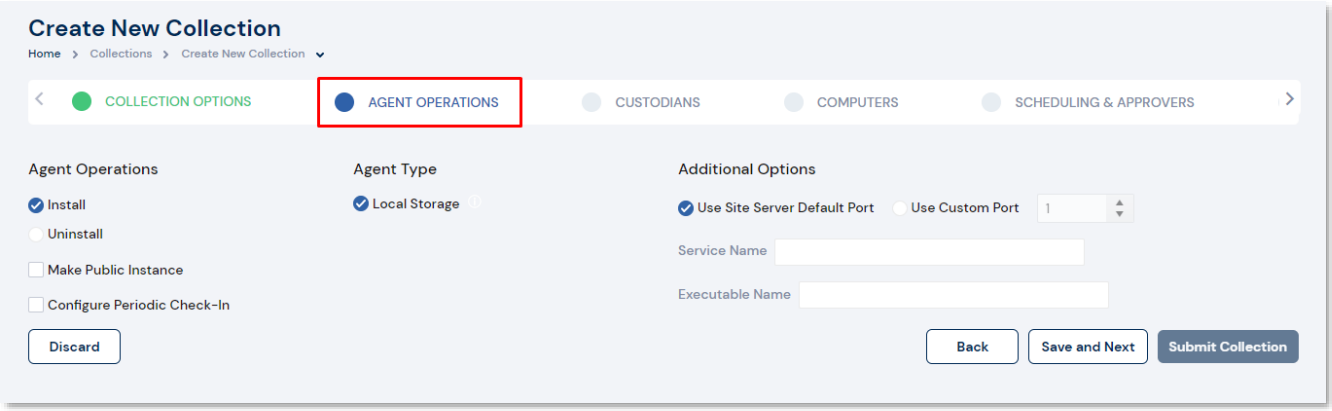


(OR)



© Exterro, Inc. All rights reserved

1. And upon enabling the **Auto Deploy Agents** checkbox and clicking on **Save and Next**, the below **Agent Operations** section will be displayed.



On the Agent Operations page, select from the following options:

Option	Description
Uninstall	Select to remove the agent from the machine
Install	Select to push the agent to the machine. Remember that the agent install may cause the machine to restart without a warning.
Make Public Instance	Configure the agent to check a public instance after the agent is installed.
Configure Periodic Check-In	Configure the agent to communicate back to the server.
Agent Type – Local Storage	Agent uses local files for configuration and data. Agent is installed (persists after reboot).
Use Site Server Default Port	Enabling this will force the agent to use Port:54545
Use Custom Port	Enter the port designated to communicate with the agent.
Service Name	Enter the name that you want the agent to be displayed as.
Executable Name	Enter the name of the file that is being run.

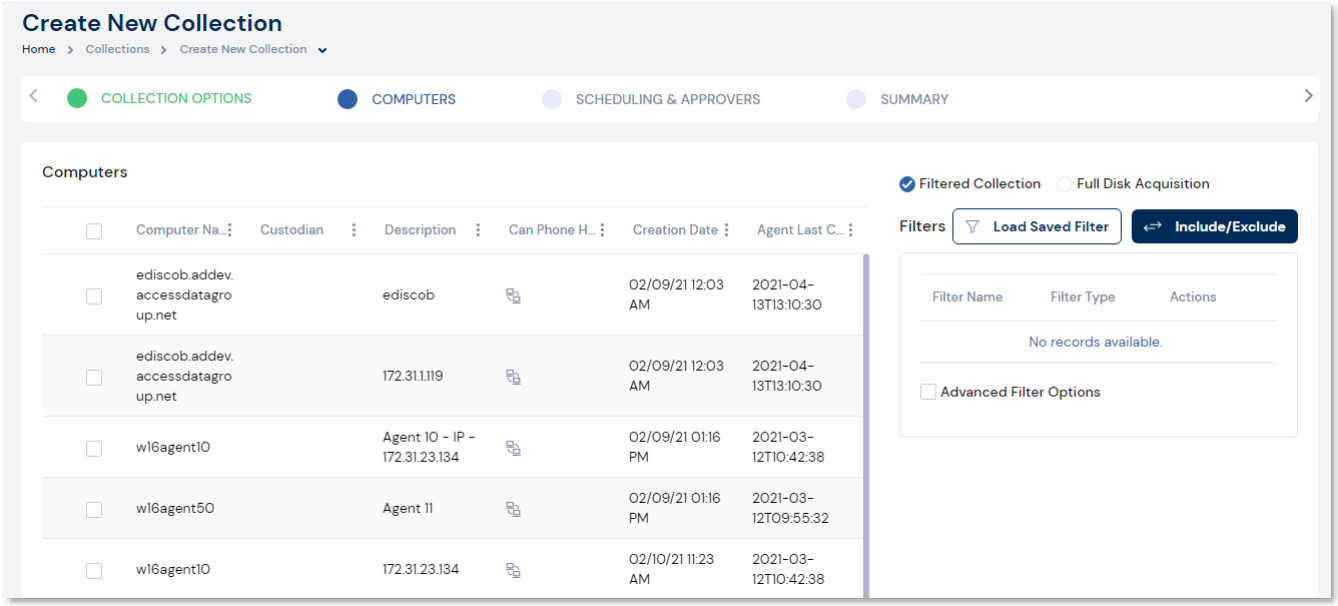
© Exterro, Inc. All rights reserved

Upon selecting the required agent operations and clicking on Save and Next, you will be navigated to the **Custodians** section.

(OR)

If the **Agent Deploy** option is not selected in the **Collection Options** section, the Agent Operations section will be skipped and you will be navigated to the **Custodians** section.

Upon selecting the required options for **Data Sources** field and clicking on **Save and Next** from the **Collection Options** section, you will be navigated to the **Computers** section.



5. Select the required computers from the list.

Warning: You cannot proceed to collect all the data from the computer. You must include at least one among the Extension, Size, Date, Path, Luhn, Keyword, or MD5 Hash filter properties within the Include/Exclude filters to perform a targeted collection.

6. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Advanced Filter Options

You can configure the **Advanced Filters** section in the right pane to filter and collect only the required information based on the type of Collection. The applicable filters for the collection types are listed below:

i. For Filtered Collection:

Type	Options	Description
Source Type	File System	To collect the drives from the target's file system.
	Logical Disk	To collect only the target's logical drive space.
	Physical Disk	To collect the target's entire physical drive.
Search Type	Siteserver	To search using the Site Server.
	Agent & Siteserver	To search first with the agent and then with the Site Server.
	Agent	To search files using the agent.
	Collect System Files	To search system files that are normally hidden from view. Files with "$" contain system meta data and in NTFS, the $MFT contains the file system pointers to all files.
	Scan Deleted Files	To scan free space of a partition for files matching the filter criteria.
	Scan Unused Disk Area	To scan unallocated disk space for files matching filter criteria.
	Archive Drill Down	If archive files exist in any of the available data sources that contain compressed files of interest, this option lets you open the archive files as part of the job and checks them against keywords supplied in the keyword filter.

© Exterro, Inc. All rights reserved

Type	Options	Description
	Collect Responsive Archives	Collects any archive that contains files that match filter criteria.
	Custom Drill Down Extensions	Allows you to specify the extension for the archive drill down. If you do not specify the extension, the default will be used.
	Include Deleted Files	To scan the free space of a partition for files matching the filter criteria.
	Use Internal File Identification	To view the software's file identification when checking file extensions
	Collect Non-Extension Files	Collects all files that do not have an extension
	Collect Unsearchable Encrypted Files	Collects files that cannot be accessed via search by keyword filter criteria.
	Enable PreScan	Will scan the collection target before collecting. Enables accurate completion percentage, file counts, and size predictions for Real Time Status screen.
	Parse $130 INDX Records	Parses $130 INDX Records. ***Note:*** *$I30 INDX records are the names given to NTFS MFT attributes containing file name indexes for directories.*
	Exclude Removable Drives/Media	Excludes removable drives that are recognized by Site Server from the collection. This option is only available for collection jobs. Not all removable drives are recognized as such so this option may not exclude ALL removable drives

© Exterro, Inc. All rights reserved

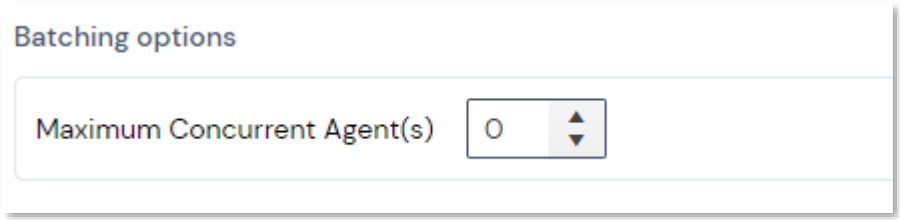
ii. For Full Disk Acquisition:

A Full Disk Acquisition job would collect the entire contents of a computer's hard drive, so the advanced options will include fewer choices as listed below:

- **Collect from Target Options**
  - **Logical Disk:** To collect only the target's logical drive space.
  - **Physical Disk:** To collect the target's entire physical drive. You can choose the sectors required.
- **Use Redirected Acquisition:** Uses the agent to push the collected data directly to the Job Data path given in the Job Options screen instead of moving it to the temporary storage location and then to the Job Data path.

Batching Options

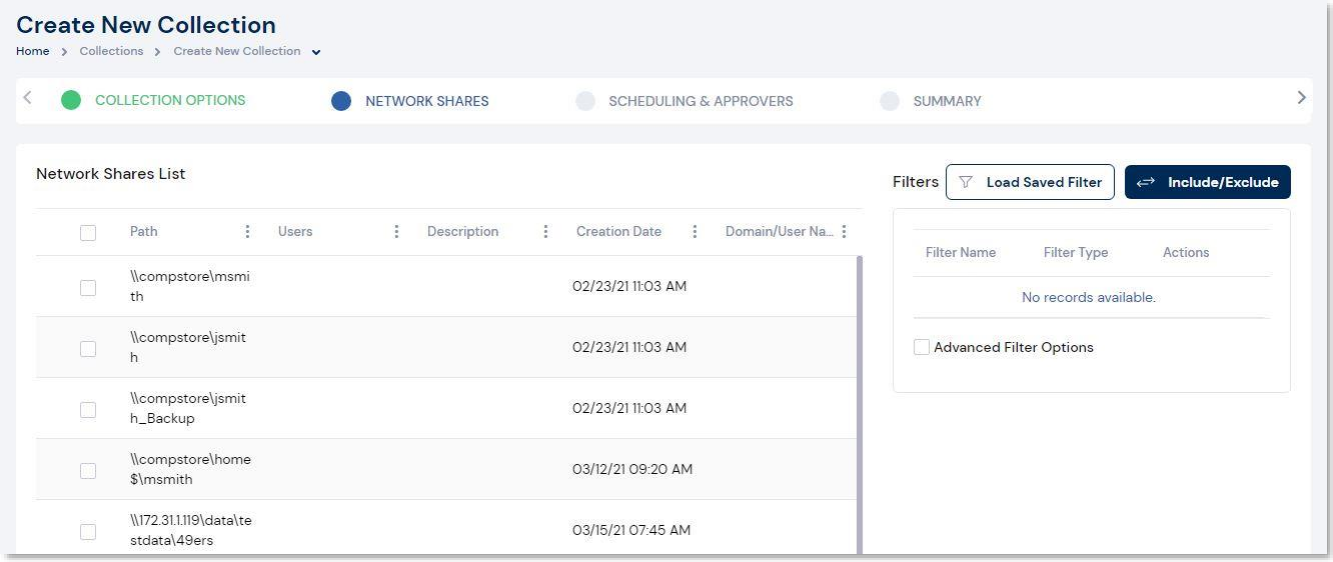
While multiple collections can run simultaneously, Batching Options allow jobs to run in groups. I.e. A selection of 3 Maximum Concurrent Agents will only allow 3 concurrent jobs to be run at once until finished, which would then allow the next batch of jobs to be started.



© Exterro, Inc. All rights reserved

Network Shares

Upon selecting the required options for **Data Sources** field and clicking on **Save and Next** from the **Collection Options** section, you will be navigated to the **Network Shares** section.



1. Select the required network share locations from the list.

Note: You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Advanced Filter Options

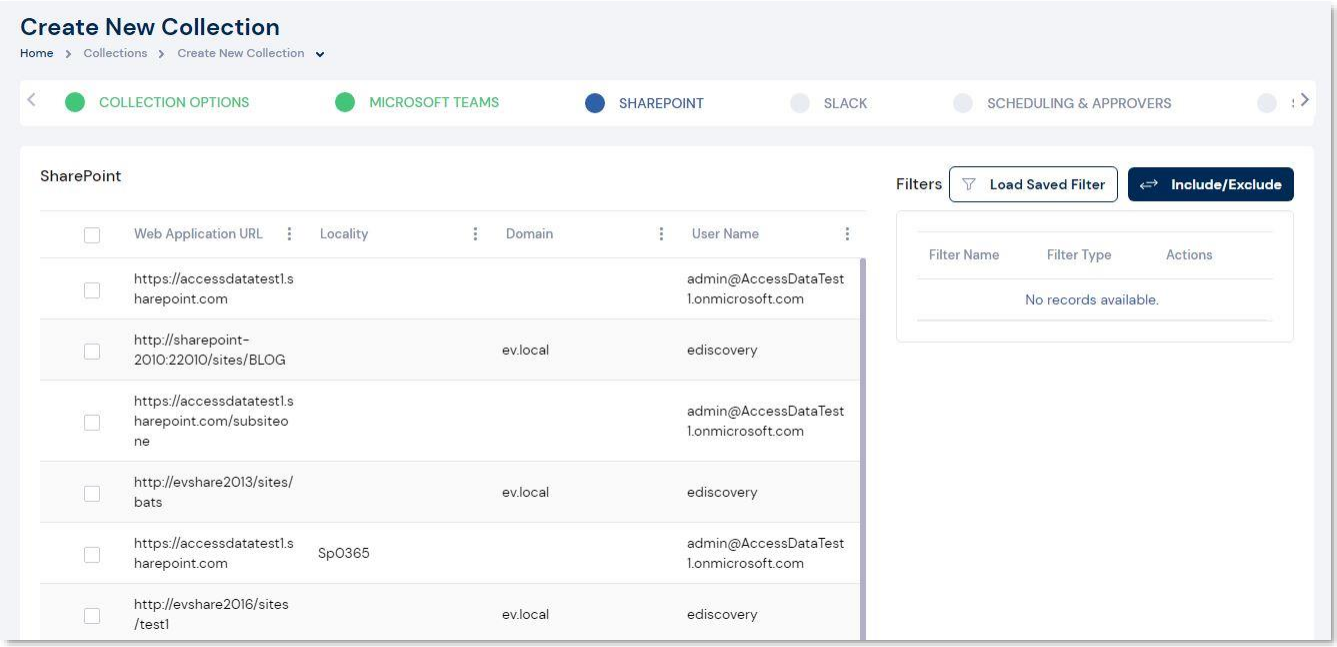
You can configure the **Advanced Filters** section in the right pane to filter and collect only the required information based on the below provided filters options:

Filter	Description
Collect System Files	To search system files that are normally hidden from view. Files with "$" contain system meta data and in NTFS, the $MFT contains the file system pointers to all files.
Archive Drill Down	If archive files exist in any of the available data sources that contain compressed files of interest, this option allows you to open the archive files as part of the job and checks them against keywords supplied in the keyword filter.
Collect Responsive Archives	Collects the archive/container files (ZIP, RAR and so forth) of any responsive file when using the drill-down option.
Custom Drill Down Extensions	Allows you to specify the extension for the archive drill down. If you do not specify the extension, the default will be used.
Collect Non-Extension Files	Collect all files that do not have an extension.
Use Internal File Identification	Sees the software's file identification when checking file extensions.
Collect Unsearchable Encrypted Files	Collects files that cannot be accessed to search for keyword filter criteria.
Enable PreScan	Will scan the collection target before collecting. Enables accurate completion percentage, file counts, and size predictions for Real Time Status screen.

© Exterro, Inc. All rights reserved

SharePoint

Upon selecting the required options for **Data Sources** field and clicking on **Save and Next** from the **Collection Options** section, you will be navigated to the **SharePoint** section.



1. Select the required SharePoint locations from the list.

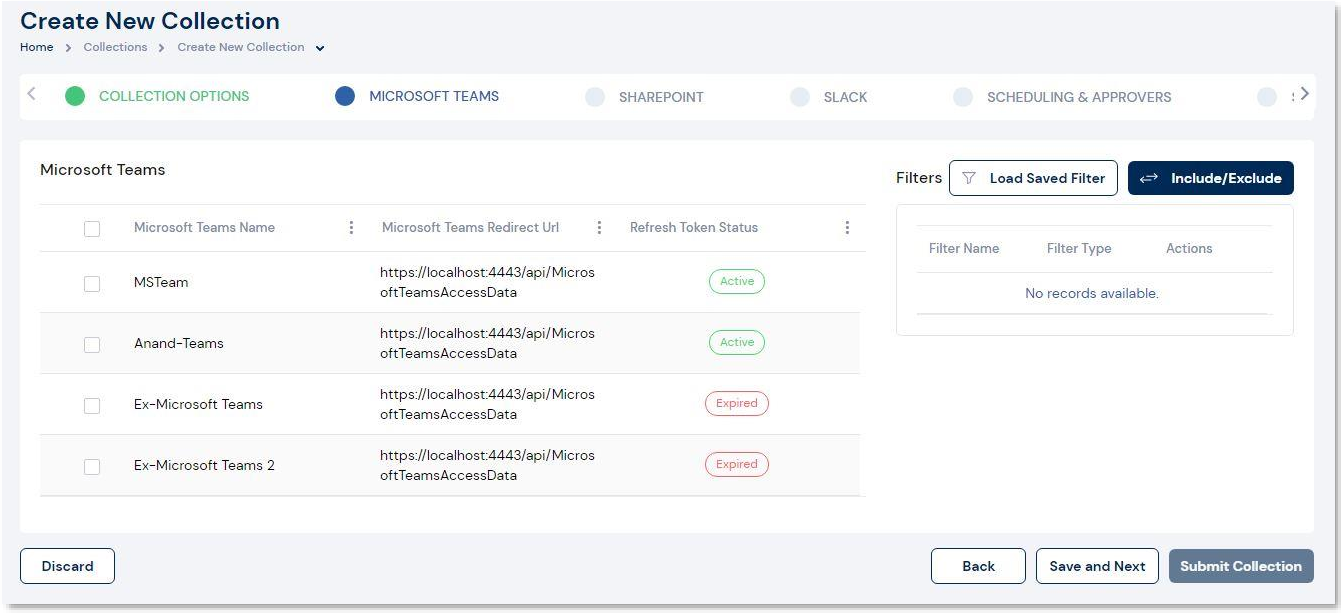
Note: You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Microsoft Teams

Upon selecting the required options for **Data Sources** field and clicking on **Save and Next** from the **Collection Options** section, you will be navigated to the **Microsoft Teams** section.



1. Select the required Microsoft Teams accounts from the list.

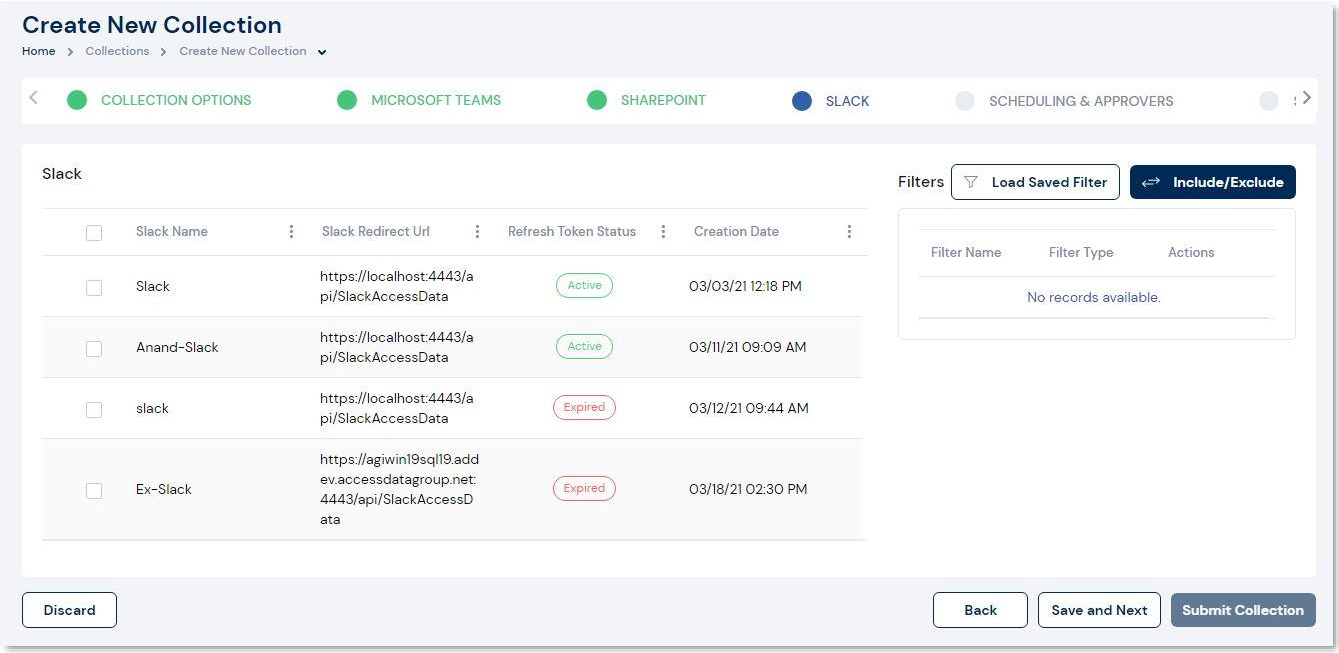
Note: You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Slack

Upon selecting the required options for **Data Sources** field and clicking on **Save and Next** from the **Collection Options** section, you will be navigated to the **Slack** section.



1. Select the required Slack accounts from the list.

Note: You can filter the files from the data source by using the Include/Exclude filters.

2. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Collection Filters for Data Sources

To configure the collection filters for data sources:

Filter behaviors

The following are the fundamentals of using filters:

- When writing queries for the Keyword(s) field, use the terms AND or OR to help refine your search. For example: "Apple AND Oranges" will return only the files with both terms "apple" and "oranges".

- In the extension field, you can use an asterisk (*) as a wildcard. For example, doc* which will include .DOC and .DOCX.

  ***Note**: You can specify multiple extensions by separating with a comma.*

- In the Path, you can include or exclude files based on folders/sub-folders in the share or on the computer. You can specify folders by doing the following:
  - Include or exclude a complete folder name. ***Example:*** *\\documents\my_Work_files*
  - Include or exclude a folder name using wildcards. e.g. *work*
  - Spaces within a folder name are allowed. e.g. shared files

  ***Note**: You can specify multiple paths by separating with a comma.*

- Multiple properties are treated with AND: When you add a filter, you can configure one or more properties within the filter and the properties are combined as an AND function. For example, if you add an inclusion filter, and in that one filter specify an extension of PDF and also a file size of greater than 2MB, the logic is "PDF" AND ">2MB". The results will include only PDF files that have a file size greater than 2 MB.
- Multiple values in same property are treated with OR: When more than one values are provided for a same property, the values are treated with OR function. As another example, if you add an inclusion filter with two extensions "DOCX, XLSX" then the results will include both DOCX and XLSX files.

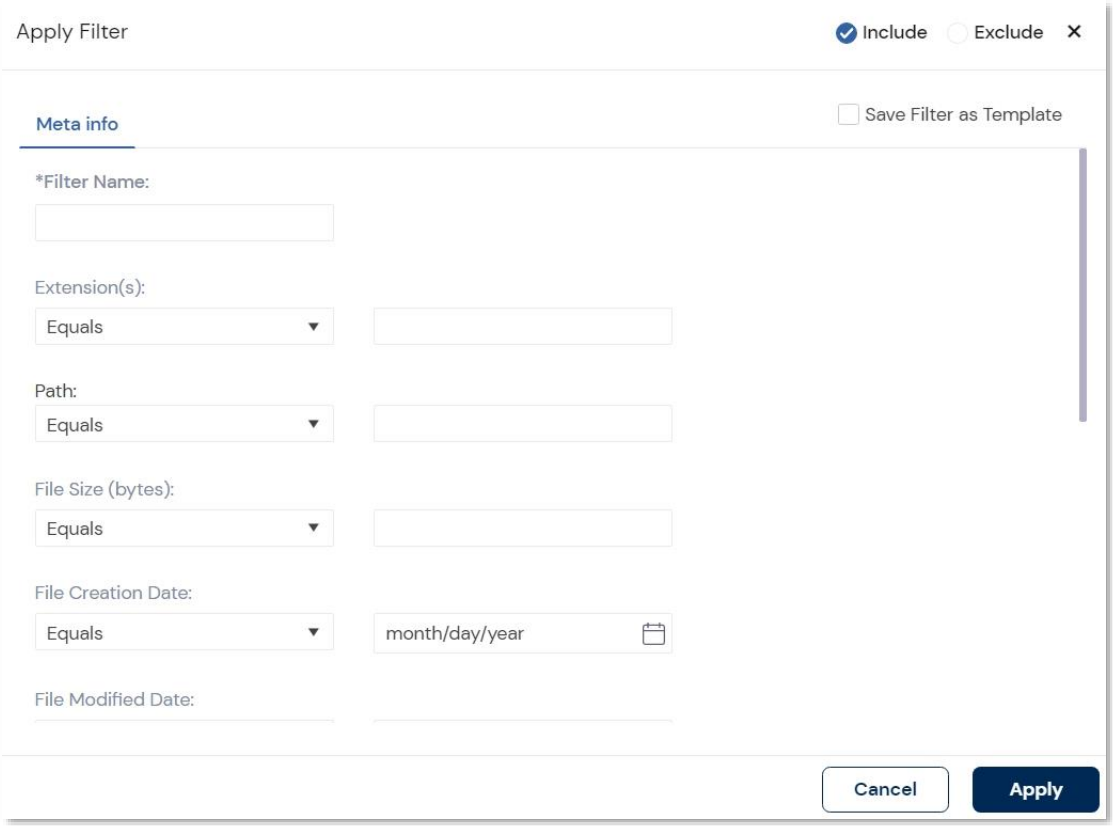
© Exterro, Inc. All rights reserved

- Path always takes precedence: If you include a path as a property in a filter, any other properties specified in the same filter will only apply to the specified path. Suppose you target a network share \\documents and you create an inclusion filter and specify the folder my_Work_files. Additionally, in the same filter you specify a file extension as PDF. In this example, only the PDF files in the my_Work_files folder is included.

- Inclusion and Exclusion filters are treated with AND: You can add both Inclusion filter and Exclusion filter to get the required data. For example, specify an Inclusion filter with extension as PDF and an Exclusion filter, file size greater than 3MB. The result will include only PDF files that are less than 3MB.

© Exterro, Inc. All rights reserved

1. From the data source section, click **Include/Exclude**.
   - The **Apply Filter** prompt is displayed.



2. Provide a name for the filter in **Filter Name**.
3. Select if you want to **Include** or **Exclude** the filtered files by enabling the required option in the top right corner of the prompt.
4. Configure the required filters as instructed in Filter Behaviors.

Note: You can enable the **Save Filter as Template** checkbox to save the configured filter as a template.

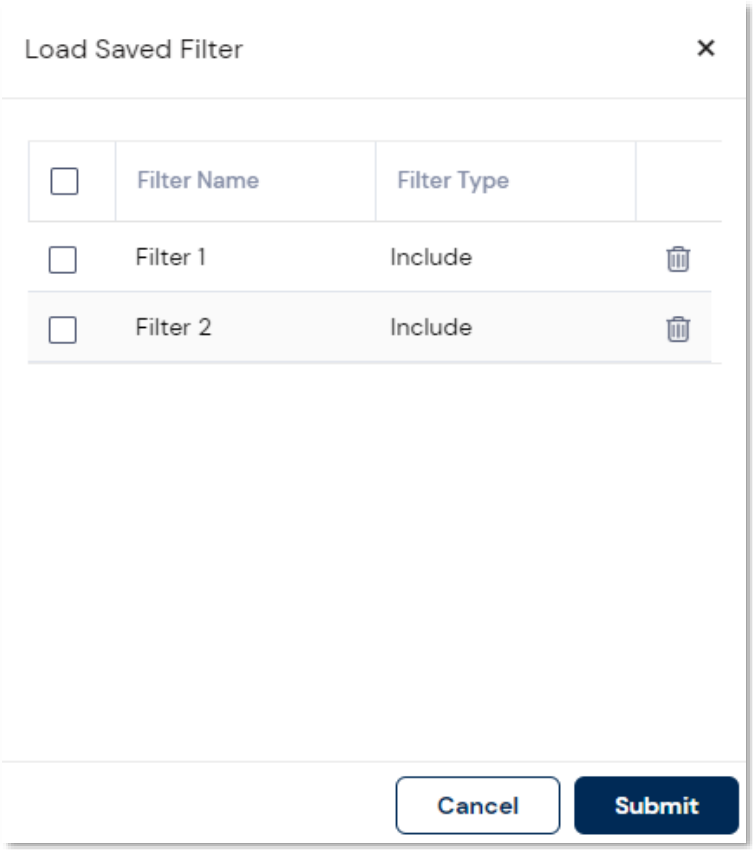
5. Click **Apply.**

© Exterro, Inc. All rights reserved

Load Saved Filters

To load a saved filter:

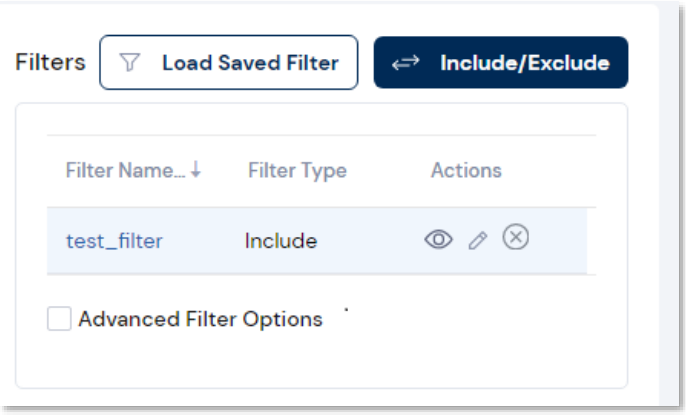
1. From the required data source section, click **Load Saved Filter**.
   - The **Load Saved Filter** prompt is displayed.



Note: You can click on **Delete** against the required filter template to delete it.

© Exterro, Inc. All rights reserved

2. Select the required filters.
3. Click **Submit**.
   - The selected filter will be applied to the data source.



Note: You can click on **View** , **Edit** , or **Delete** to view, edit, or delete the filter.

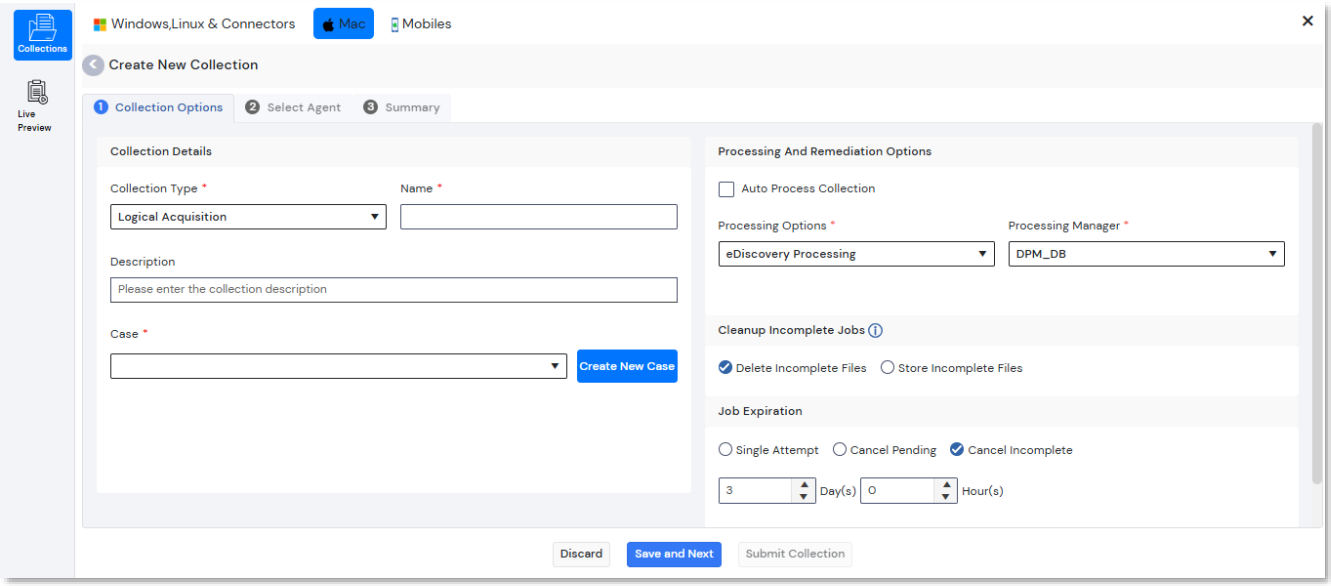
© Exterro, Inc. All rights reserved

Mac

Creating Mac Collection

To create a new collection for Mac:

1. From the home page, click on **Collections**.
2. Select the **Mac** option.
3. Click on **+ Create**.
   - The **Create New Collection** page is displayed.



Collection Options:

4. Select the required **Collection Type**.
5. Enter the Collection **Name**.
6. Provide a description of the collection.
7. Select the **Case** associated with the collection.

Note: It is recommended that a case is created prior to starting a Mac Collection. When a case is assigned to a collection, and Auto Processing is selected, the selected case will be where users will have to review data.

© Exterro, Inc. All rights reserved

8. Enable the **Auto Process Collection** option to process the evidence automatically.

Note: Auto processing will allow ingestion of collected data to a case and then be processed with a selected processing profile.

9. Select the required **Processing Options**.
10. Select the **Processing Manager**.
11. Select any one of the options below for the **Cleanup Incomplete Jobs** field:
    - **Delete Incomplete Files** – To delete partially collected files when a job fails.
    - **Store Incomplete Files** – To store partially collected files when a job fails.

12. Select the required **Job Expiration** option:

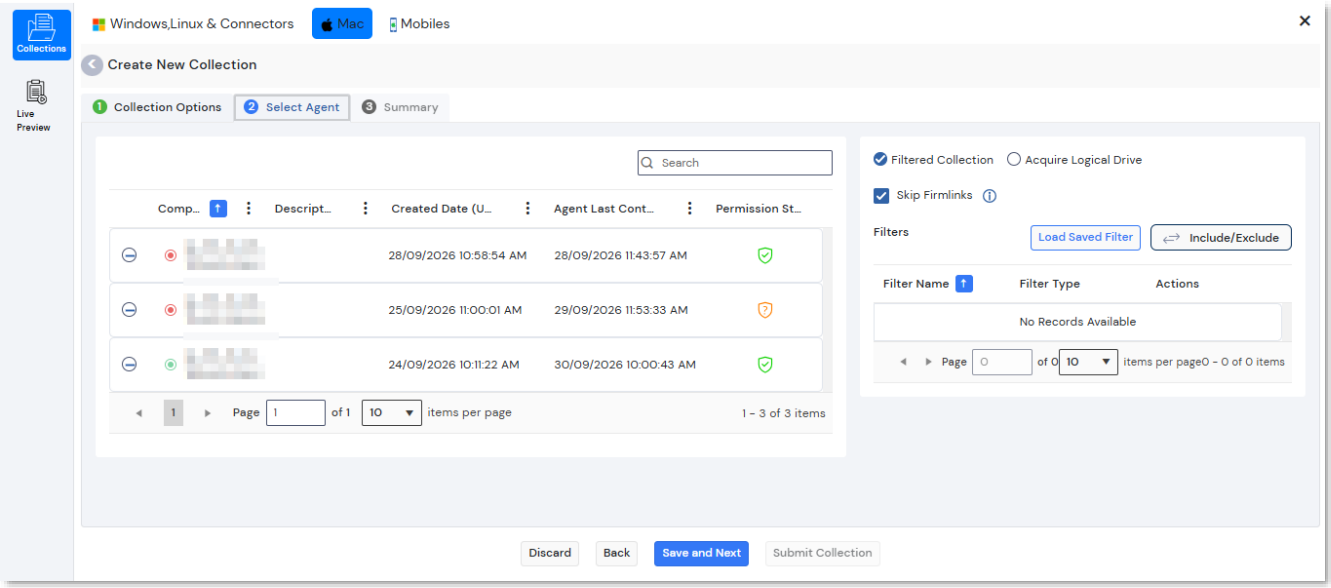
- **Single Attempt** - The collection will be cancelled if the job is not initiated within 10 minutes after the collection is created.
- **Cancel Pending** - The collection will be cancelled if the job is not initiated within the specified duration.
- **Cancel Incomplete** - The collection will be cancelled within the specified duration regardless of the job initiation status.

Note: The **Cancel Incomplete** option will be selected by default.

13. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Select Agent:



14. Select the required Mac agent from the left pane.

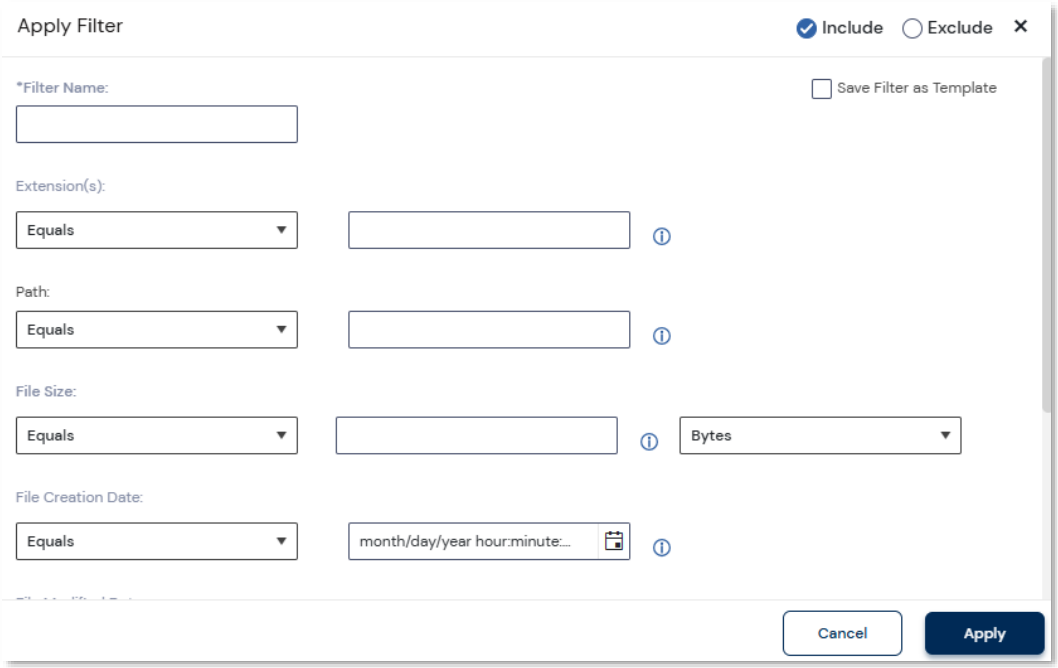
Note: The agents will be indicated with red and green colored dots to indicate the below:

- Red – The agents that have not checked-in in the last 30 minutes.
- Green – The agents that checked–in in the last 30minutes.

Note: *If Red is being shown, the agent is not necessarily unreachable, but rather it has failed to communicate within the last 30 minutes. Collections can still be initiated and when the agent has regained communication with FTK, will start the queued collection job.*

© Exterro, Inc. All rights reserved

15. Select any one of the below types of collection methods:
    - **Filtered Collection** – Enable this option to collect the filtered data from the Mac. Upon enabling this option, follow the steps below to configure the filters:



I. Select the filter type as either **Include** or **Exclude.**

II. Provide the **Filter Name**.

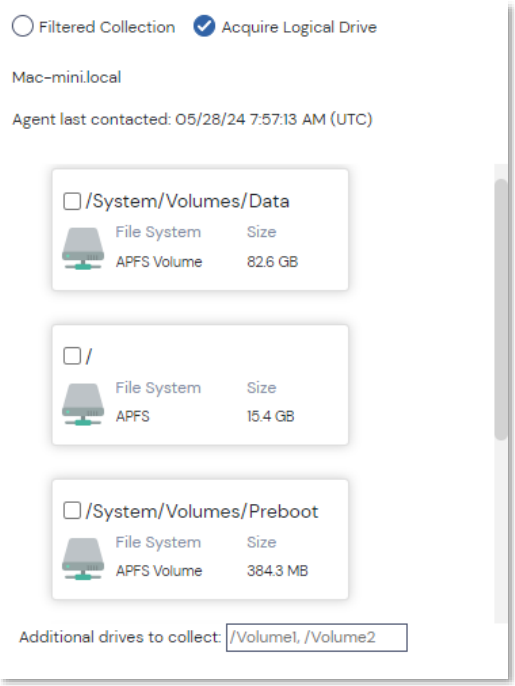
III. Configure the filters based on the Filter Behaviors.

IV. Click **Apply**.

Note: You can save the filter configurations into a template enabling the **Save Filter as Template** option before saving the filter. You can access the templates by clicking on the **Load Saved Filter** button.

© Exterro, Inc. All rights reserved

- **Acquire Logical Drive** – Enable this option to select and collect specific partitions (drives) from Mac. Upon enabling this option, select the required drives from which the data should be collected. Logical Drive information is stored for 24 hours and will refresh when connectivity is possible with the agent.



© Exterro, Inc. All rights reserved

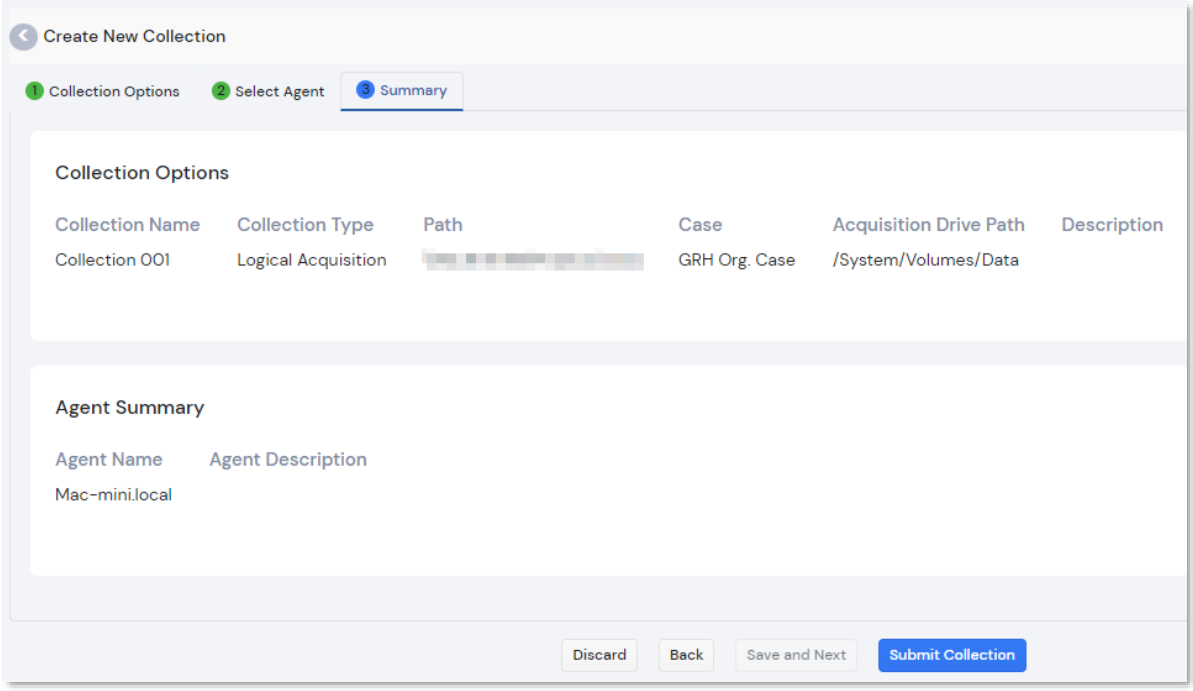
Notes:

- The size listed within this panel, indicates the amount of storage that is actively used on a listed drive and not the size of the drive itself.
- The size may be lesser than the size shown within the Collection Details. This is due to MacOS implementing transparent compression on files. Collection sizes will understandably be greater once they are made available on the Windows File System.
- You can also include additional drives for collection by providing the drive details in the **Additional drives to collect** field.

16. Enable the **Skip Firmlinks** option to prevent collecting duplicate user data across APFS firmlinks. This skips the secondary macOS data volume mount point (System/Volumes/Data).
17. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Summary:



18. From the **Summary** section, verify and ensure that all configurations made for the collection are correct.
19. Click **Submit Collection**.

The collection for Mac will be created and can be viewed in the Mac Collections Dashboard. Users can view both the collection details as well as navigate directly to the assigned case should auto-processing had been selected.

Note: The Mac collection process remains active if the system enters sleep mode automatically via a timer. However, manually putting the Mac system to sleep will cause the collection to be interrupted.

© Exterro, Inc. All rights reserved

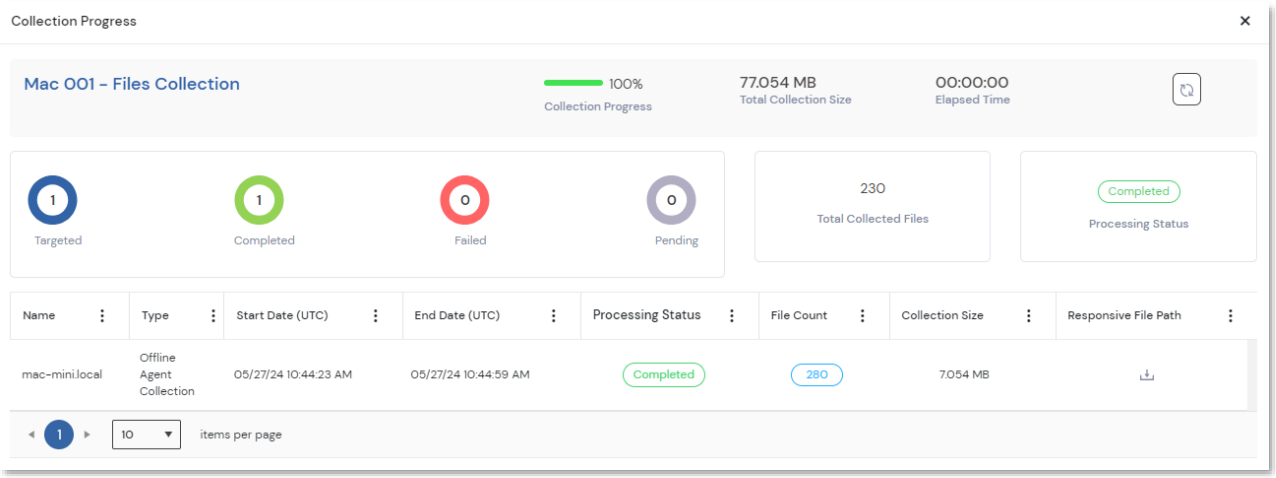
Viewing Mac Collection Details

To view the Mac Collection details:

1. From the home page, click on **Collections**.
2. Select the **Mac** option.

Note: You can click on the **Enter Review** button against the required collection view the corresponding files in the Review page.

3. Click on the **Actions Menu** button against the required collection.
4. Click on **Collection Details**.
   - The **Collection Progress** pop-up is displayed.



Notes:

- You can click on **Responsive File Path** button against the required data source to view the location path where the collected files are stored.
- The **Total Collection Size** may be greater than the size shown during Logical Drive Acquisitions. This is due to MacOS implementing transparent compression on files. Collection sizes will understandably be greater once they are made available on the Windows File System.

© Exterro, Inc. All rights reserved

- You can click on the **Refresh** button to refresh and view the updated count and processing status of the collection.

© Exterro, Inc. All rights reserved

Remote Mobile Discovery

Exterro Remote Mobile Discovery (RMD) is an advanced, efficient, and innovative solution for seamless mobile data collection in forensic investigations.

With RMD, you can:

- Remotely connects to mobile devices associated with custodians or computers.
- Collect comprehensive data or focus on specific applications as per investigative needs.
- Ensure secure and forensically sound acquisition of mobile data without physical access to the device. (a user would still be required to consent to a collection by providing their passcode during a collection).

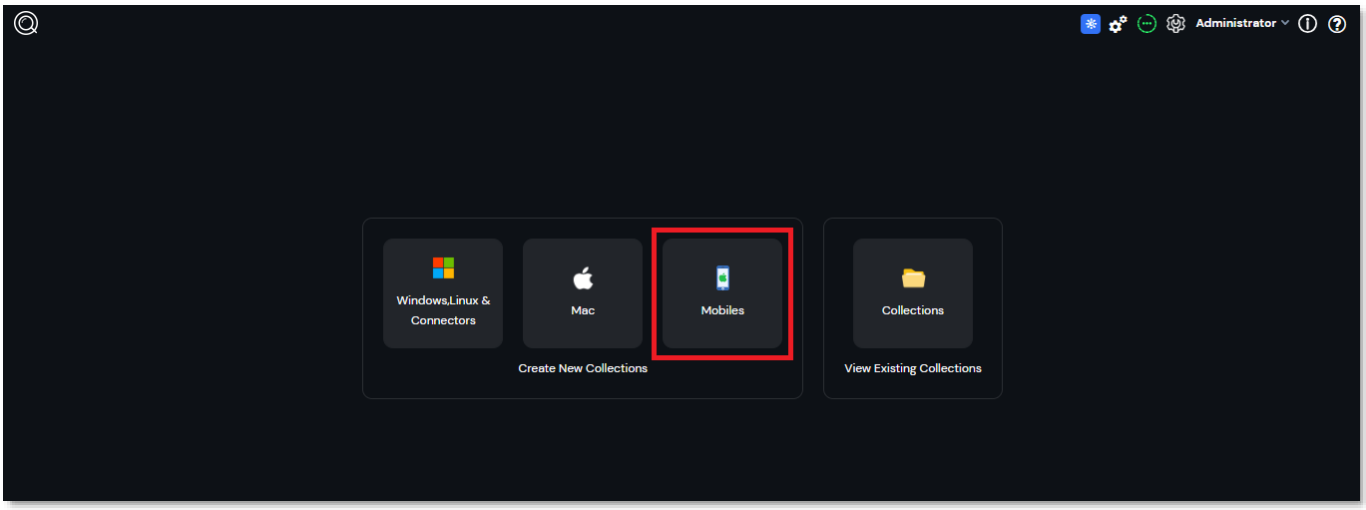
Designed for efficiency, accuracy, and compliance, RMD streamlines mobile forensic workflows, empowering investigators with fast, reliable, and remote data collection capabilities.

© Exterro, Inc. All rights reserved

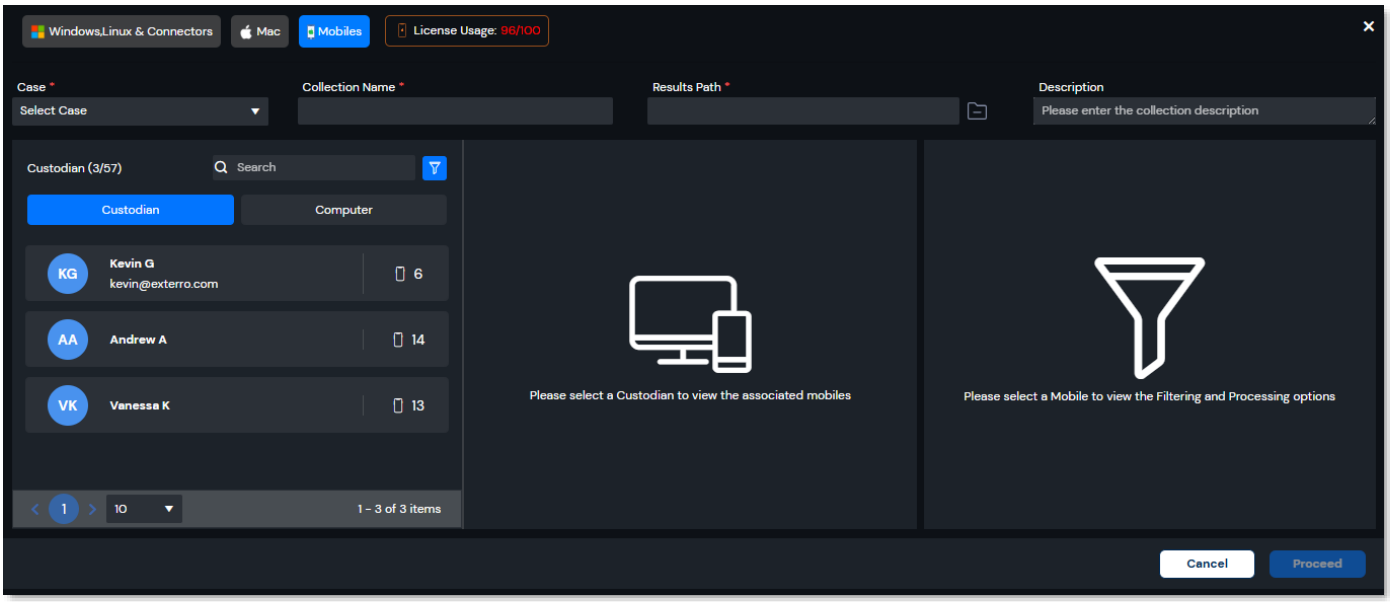
Creating Remote Mobile Collection

To create a remote mobile collection:

1. Login to the FTK Central application.
2. Select **Collections**.
3. Select **Mobiles**.

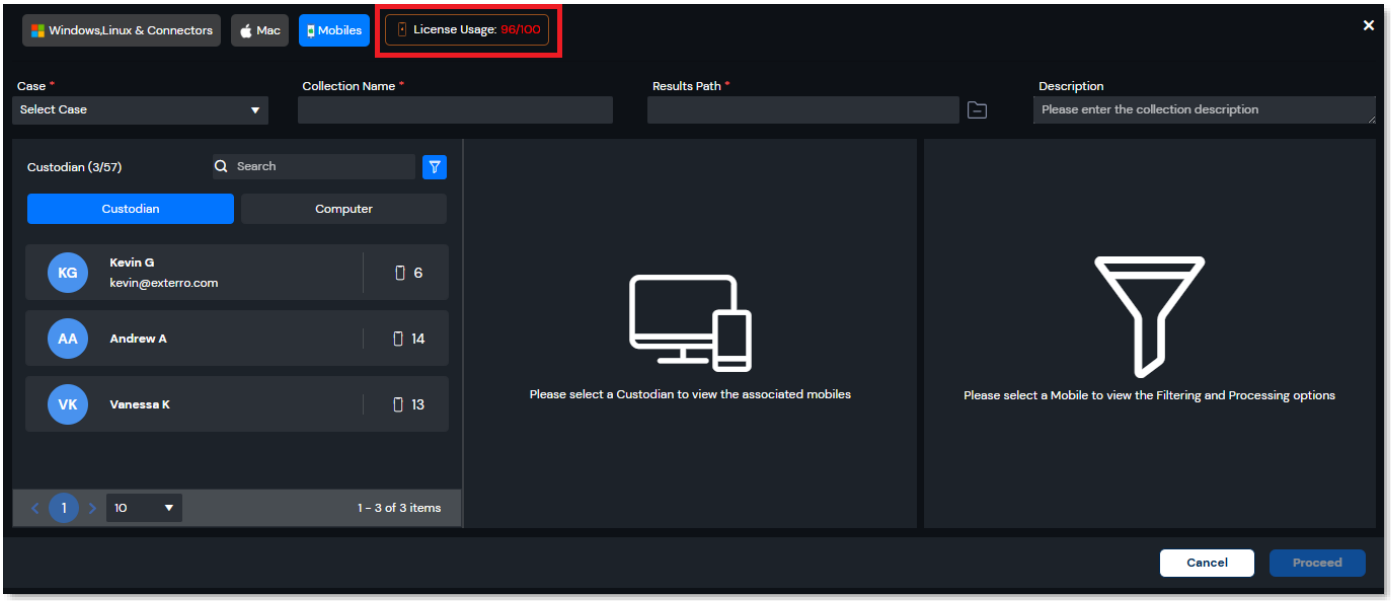


- The Mobiles Collection creation page is displayed:



© Exterro, Inc. All rights reserved

Note: The **License Usage** field in the top of the page displays the total number of unique mobile devices allowed for collection against the number of mobile devices for which the collection is in-progress or completed.

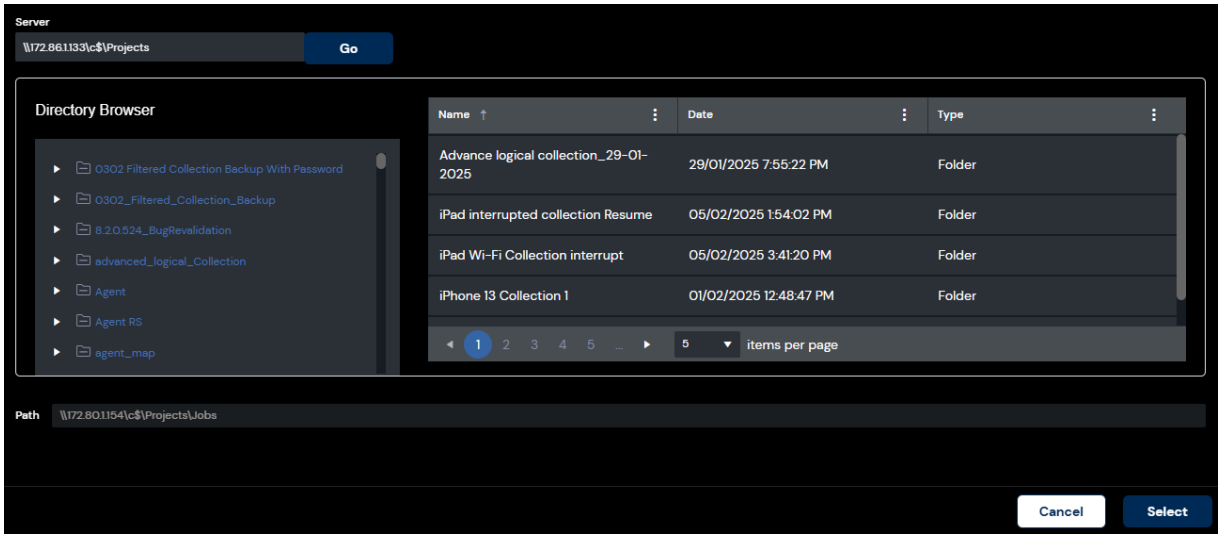


4. Provide the following details:
   - **Case** – Select the case from the drop-down.
   - **Collection Name** – Provide the collection name.

© Exterro, Inc. All rights reserved

Note: The location for **Results Path** will be automatically populated based on the case selected in which the collected files will be stored. However, you can change the path if required. To do so,

i. Click **Folder** against the Results Path field.
   - The below page is displayed.



ii. Enter the **Server Path**.

iii. Click **Go** to view the directories available on the server.

iv. Select the folder to be where the results are to be saved.

v. Click **Select**.

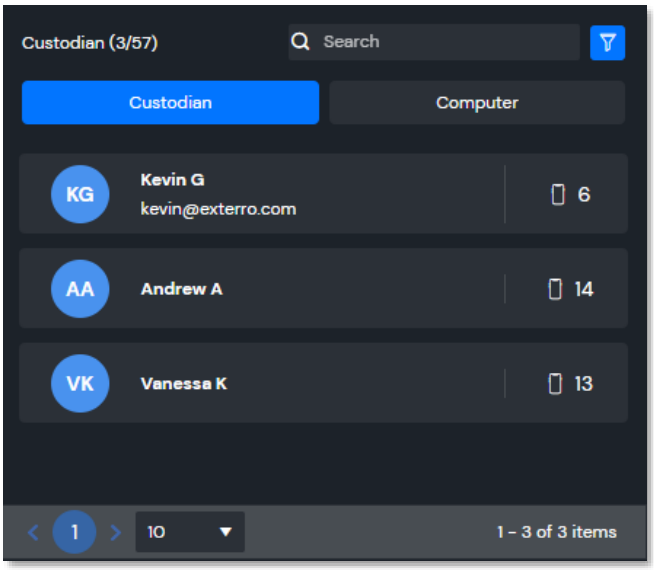
- **Description** – Provide a description of the collection that will be displayed in the details page.

© Exterro, Inc. All rights reserved

Custodian/Computer

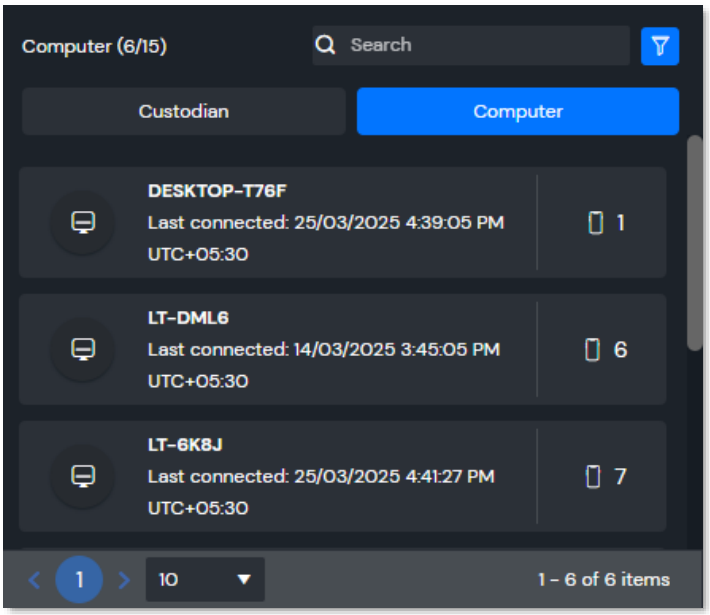
This section displays the list of custodians and computers added in the application along with the mobiles associated with it.

Custodian:

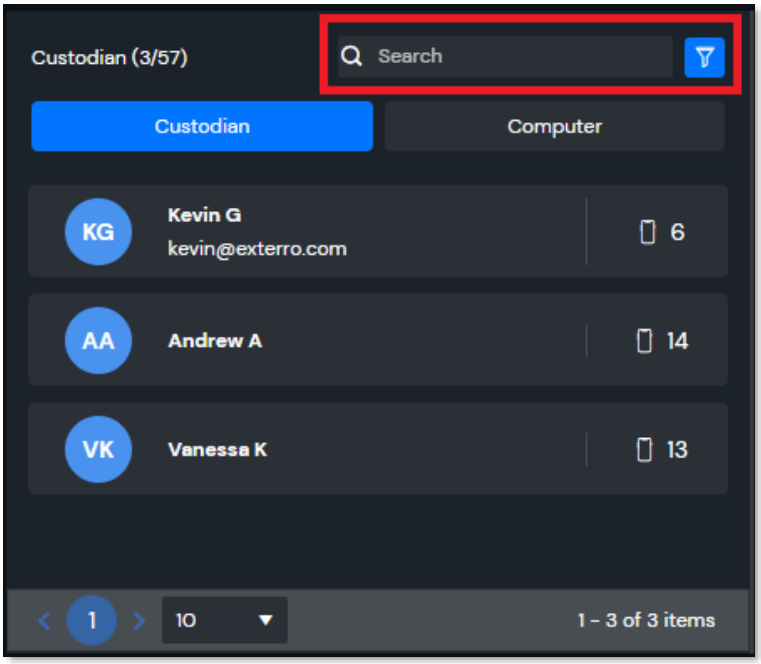


© Exterro, Inc. All rights reserved

Computer:



You can use the search bar to search for computers, custodians, or mobile device names.



© Exterro, Inc. All rights reserved

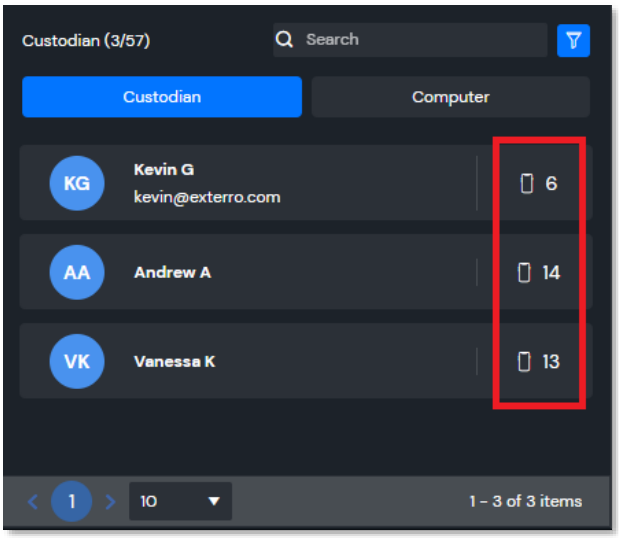
You can also click on and select any of the below options to filter the custodians and computers:

- **Recently Contacted** – Agents that have checked-in during the last auto provision.
- **Not Recently Contacted** – Agents that have not checked-in during the last auto provision.
- **Mobile Device Associated** –To filter only the custodians or computers that are associated with mobile phones.

Notes:

- Auto provision is the synchronization between site server and application databases. This synchronization is controlled based on the configuration made for the **autoprovisioninterval** property in the config file. Refer to the app config guide for more details.
- By default, the **Mobile Device Associated** filter is applied to display only the custodians and computers associated with mobile devices. However, you can disable this filter to view all the custodians and computers.

The number of mobile devices associated with the custodian or computer will be displayed against it.



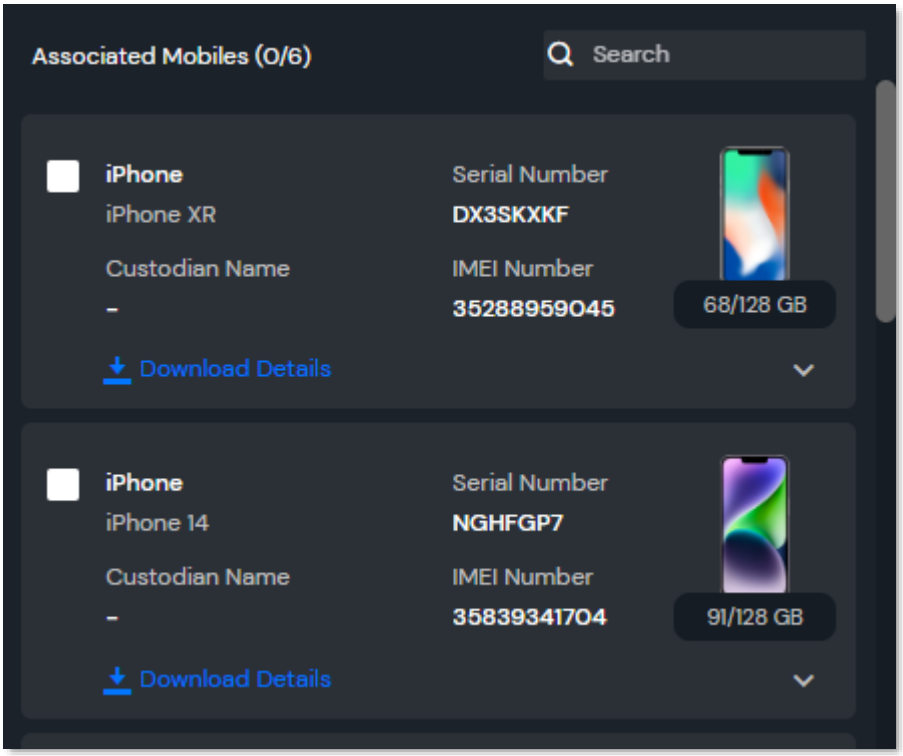
Select the **Custodian** or **Computer** section and click on the required entity to view all the associated mobiles and its details.

© Exterro, Inc. All rights reserved

Associated Mobiles

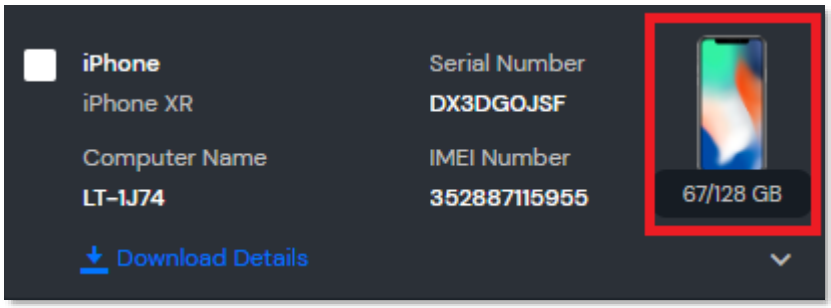
This section displays all the mobiles associated with the selected custodian or computer along with its basic details such as mobile device name, model number, serial number, etc. You can click on the expand icon to view additional information about the mobile device.

Basic details:

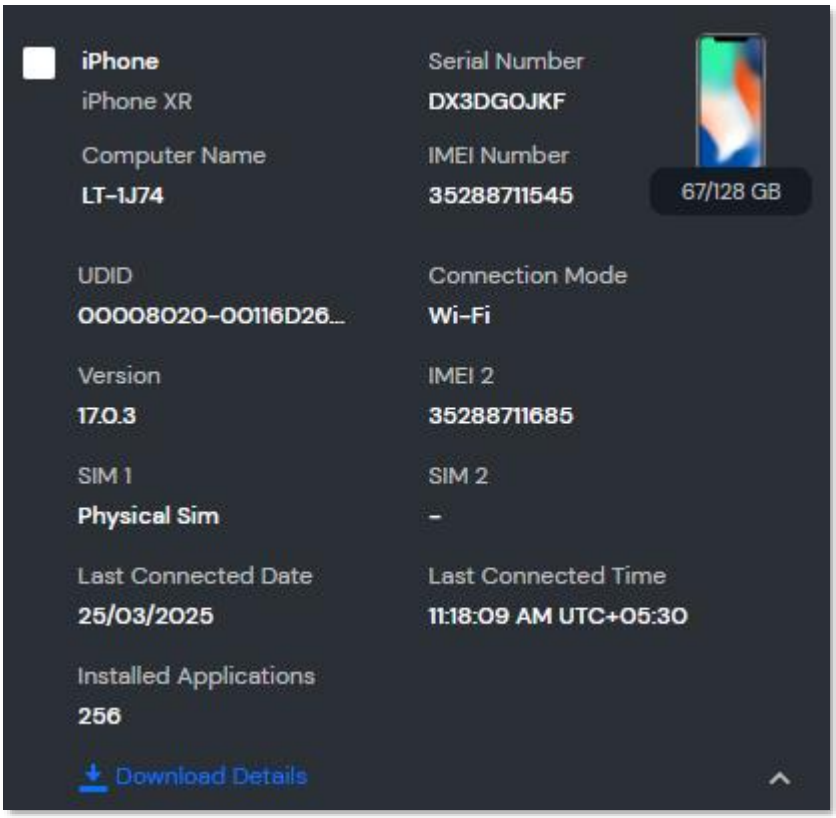


© Exterro, Inc. All rights reserved

Note: The volume displayed against the mobile device image indicates the available storage within the device's total storage.



Additional details:



© Exterro, Inc. All rights reserved

Note: You can click on the **Download Details** button to download and view the following details of the corresponding mobile device along with the list of all applications installed on the mobile device:

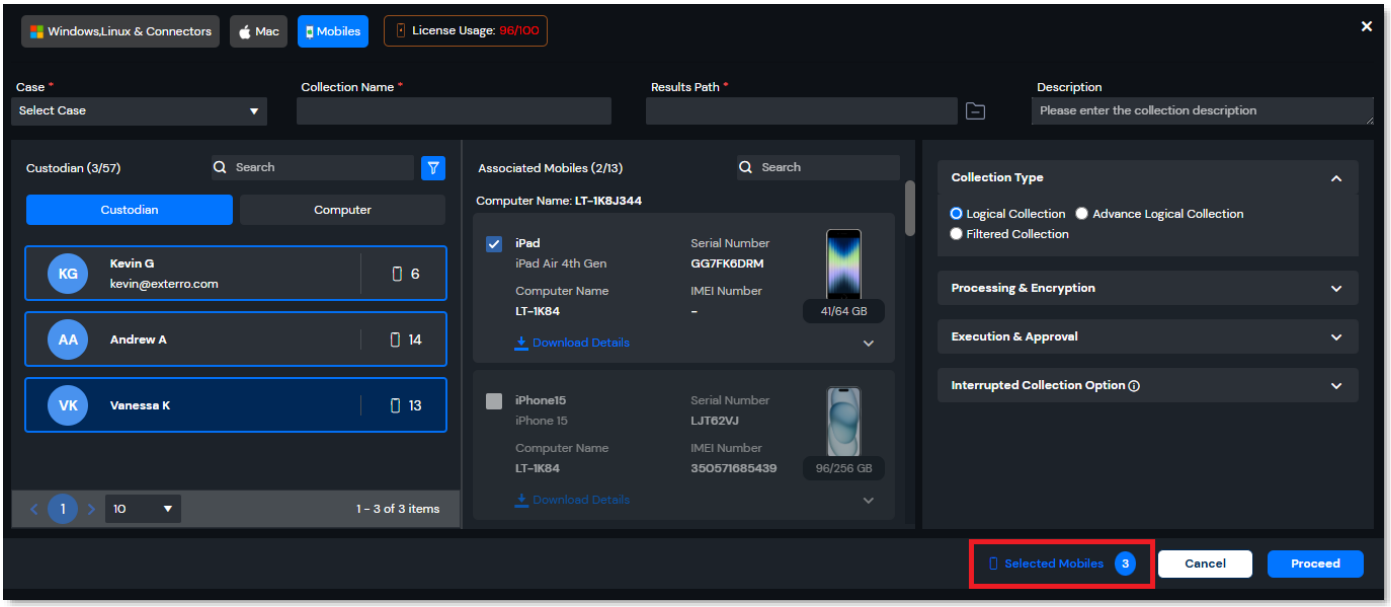
- Mobile Name
- Version
- Storage
- Serial Number
- UDID
- IMEI 1
- IMEI 2
- SIM 1
- SIM 2
- Last Connected Date & Time
- Connected Computer
- Associated Custodian
- Connection Mode
- Installed Application (Count)
- EthernetAddress
- FirmwareVersion
- HardwareModel
- TimeZone
- LastiTunesBackupDate
- BackupEncryptionEnabled

5. Check any one mobile from which the data needs to be collected.

Warning: You can select only one mobile per agent in the collection.

© Exterro, Inc. All rights reserved

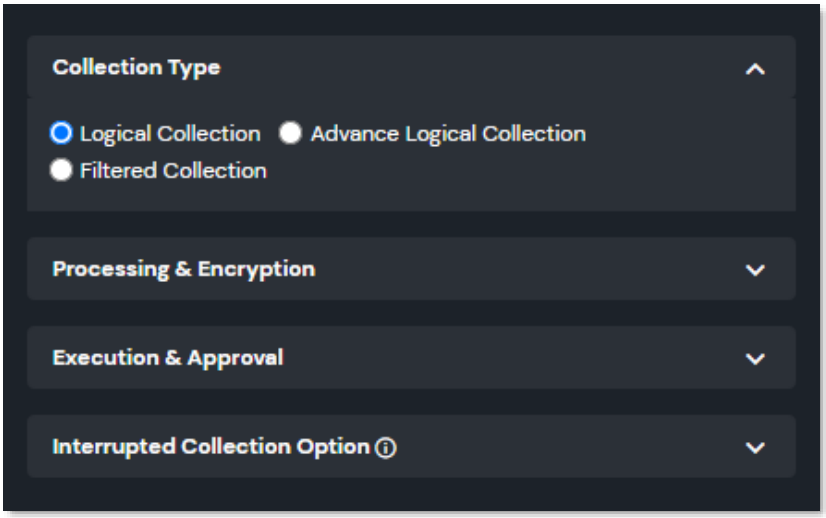
The **Selected Mobiles** option displays the total number of mobile devices selected for the collection. You can click on that count to view all the selected mobile devices and the associated custodians/computers.



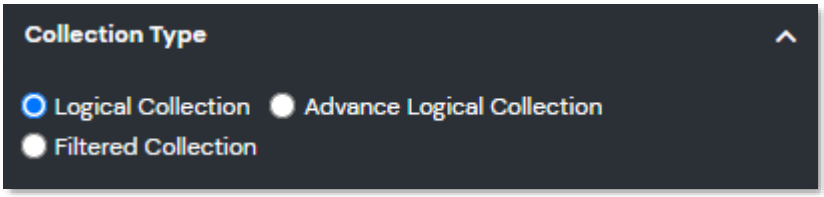
© Exterro, Inc. All rights reserved

Collection Configuration

This section displays all the configurations to filter and collect the targeted data from the mobile device.



Collection Type:

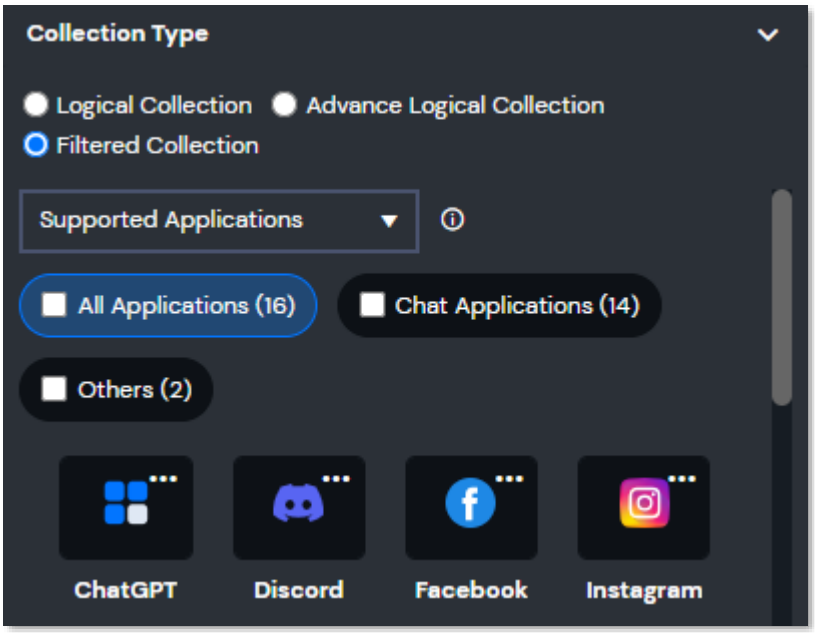


6. Select any one of the below **Collection Type** options:
   - **Logical Collection -** To collect the entire backup of the mobile device.
   - **Advance Logical Collection –** To collect the entire backup of mobile, AFC Service Data, and Lockdown Service.

© Exterro, Inc. All rights reserved

- **Filtered Collection –** To collect data specific to the selected applications. Upon selecting this option, a drop-down with the following options are displayed:
    - **Supported applications-** Displays the applications installed in the selected mobile devices that are supported by the FTK Central application, which can be selected for collection.
    - **Installed applications –** Displays all the applications that are installed in the selected mobile devices including the ones that are not supported by FTK Central. For the not supported applications, you can view them but not select them for collection.

Note: By default, the **Supported applications** option is selected for this field.



© Exterro, Inc. All rights reserved

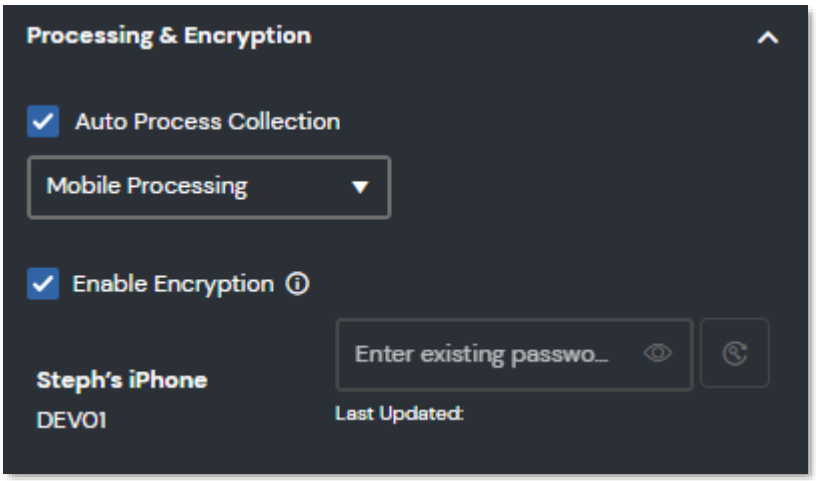
You can click on the following filtering options to filter and view the corresponding mobile applications in the device:

- All Applications
- Chat Applications
- Others

Moreover, you can click on the checkboxes against the filtering options to select the corresponding filtered applications.

You can click on the **Additional Details** ••• icon against the applications to view all the mobile devices (selected in the **Associated Mobiles** section) that have the applications installed on them.

Processing & Encryption:



7. Check the **Auto Process Collection** option and select the processing profile from the drop-down to automatically process the collected data.

© Exterro, Inc. All rights reserved

8. Check the **Enable Encryption** option and provide the iTunes backup passwords of all the selected mobile devices to create an encrypted collection.

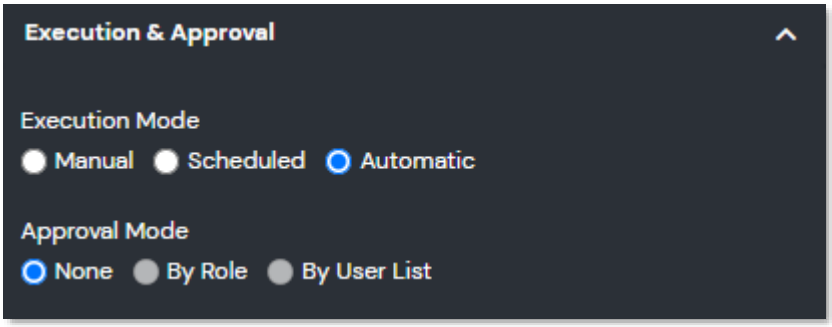
Notes:

- If an encrypted collection has already been created for the device, the password will be automatically populated. You can update the password by replacing the existing one or reset the password by clicking on the **Reset Password** icon and enter a new password.
- The time taken for the backup completion via Wi-Fi is longer when compared to wired connection.

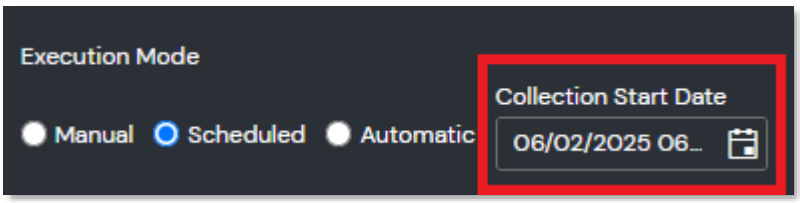
Tip: You are recommended to use encrypted backups for better security and to include additional data, such as account passwords, call history, etc.

© Exterro, Inc. All rights reserved

Execution & Approval:

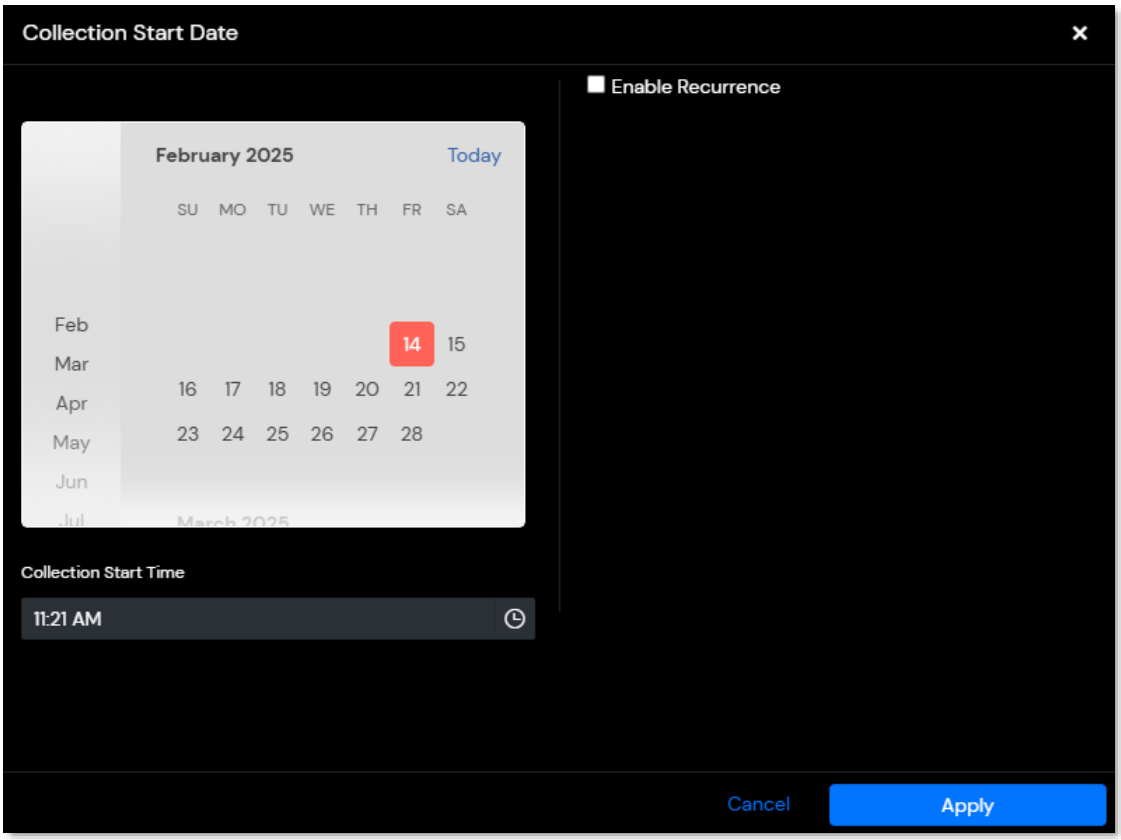


9. Select any one of the following **Execution Modes**:
   - **Manual** - To manually initiate the collection process.
   - **Scheduled** - To schedule the collection on the specified date and time. You configure it to be a recurring collection for a specified number of times using the following steps:
     i. Upon enabling the Scheduled option, the **Collection Start Date** field is displayed. Click on the icon against it.



© Exterro, Inc. All rights reserved

ii. The **Collection Start Date** pop-up is displayed.

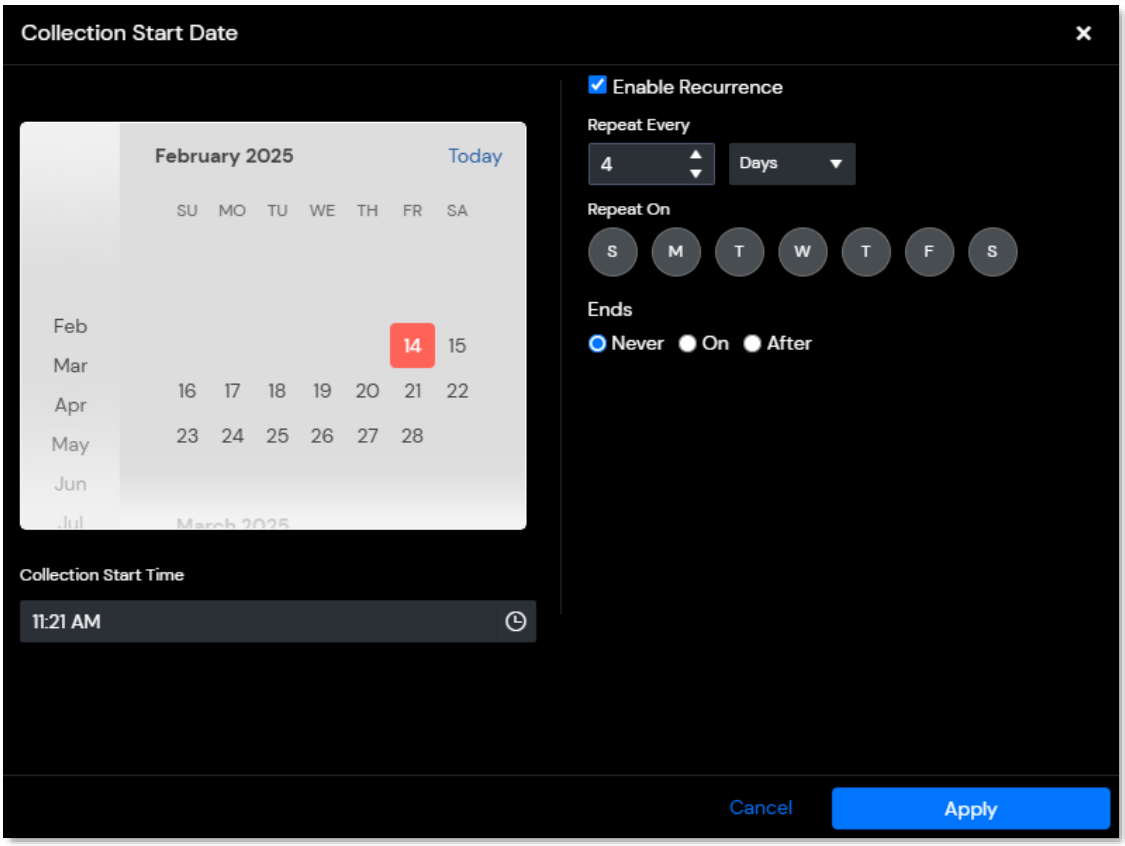


iii. Select the date from the calendar and **Collection Start Time** to schedule the collection.

Note: If you want the collection to be processed just once on the scheduled date and time, click the **Apply** button after performing the above step. If you want it to be a recurring collection that should be performed for a specified number of times, proceed to follow the below steps as well.

© Exterro, Inc. All rights reserved

iv. Check the **Enable Recurrence** option to create a recurring collection.

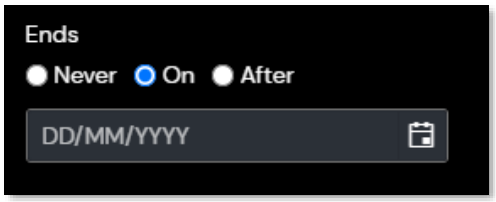


v. Select the time interval in the **Repeat Every** field during when the collection should recur.

vi. Select the days in the **Repeat On** field when the action should be repeated.

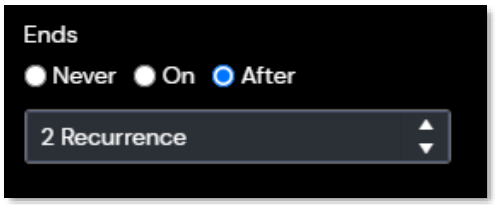
vii. Configure the Ends field to set when the recurring collection should end:

- **Never** – The recurring collection should continue indefinitely.
- **On** – Set a date when the recurring collection should end.



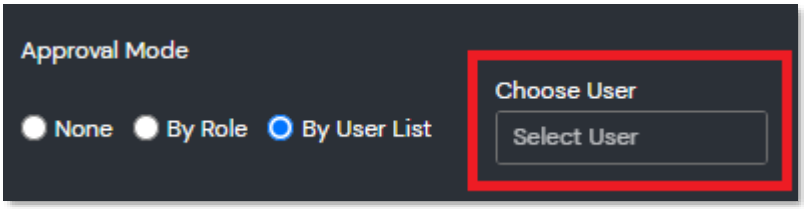
© Exterro, Inc. All rights reserved

- **After** – Set number of recurrences after which the recurring collection should end.



- **Automatic** – To automatically initiate the collection process immediately after creating it.

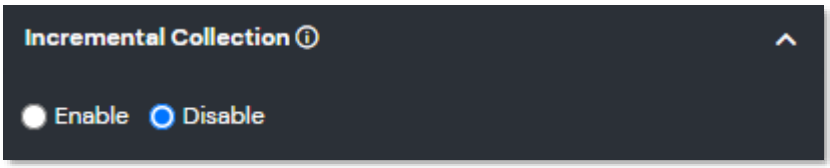
10. Select the **Approval Mode** for the collection:
    - **None** - No approvals required.
    - **By Role** - To be approved by users with specific roles.
    - **By User List** - To be approved by users selected from the **Choose User** field.



© Exterro, Inc. All rights reserved

Incremental Collection:

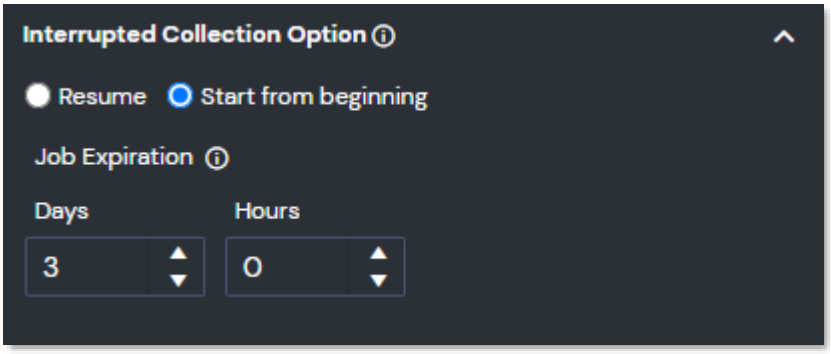
Note: This section is displayed only when the **Enable Recurrence** option is checked in the **Collection Start Date** pop-up.



11. Select any one of the following options for the **Incremental Collection** field:
    - **Enable** – The collected data will be saved in the agent's computer as a backup until the recurrence collection is concluded. If the data in the computer is deleted or moved, the collection will be initiated from the beginning.
    - **Disable** – The collected data backup will be deleted as soon as a collection's recurrence is completed.

© Exterro, Inc. All rights reserved

Interrupted Collection Option:



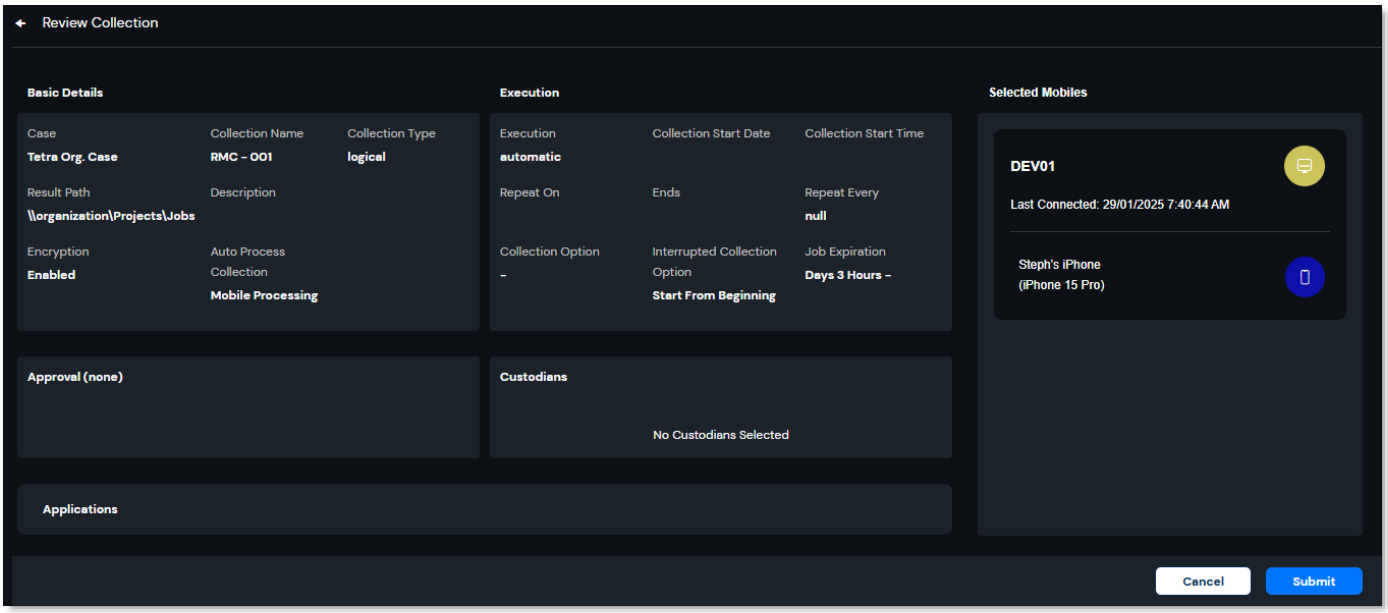
12. Select the action that should be taken in case of collection interruption:
    - **Resume** - A backup will be created and maintained till the collection is resumed to start from where it was left off.
    - **Start from beginning** - To start the collection from the beginning.

Tip: You are recommended to select the **Start from beginning** option to ensure the integrity and completeness of the data. Resuming the collection may result in missing some files which were not successfully collected prior to the interruption,

13. Set the **Job Expiration** duration.
14. Click **Proceed**.

© Exterro, Inc. All rights reserved

Review Collection



15. Review and verify the configurations made to the collection.
16. Click **Submit**.

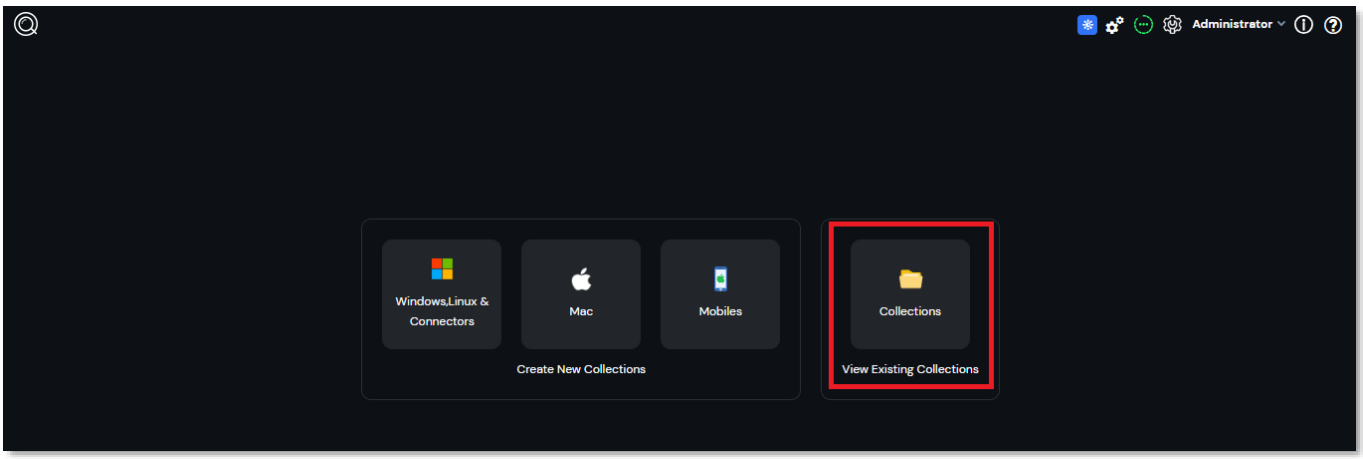
© Exterro, Inc. All rights reserved

Viewing Mobile Collection

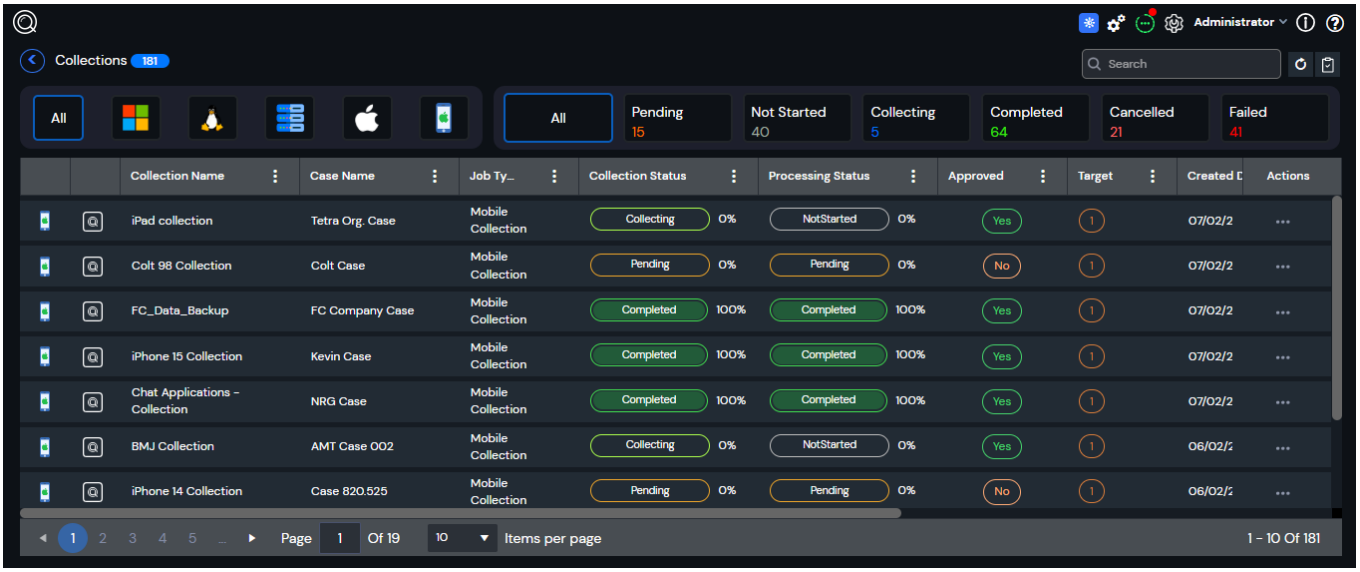
Collection Details

To view the details of a Mobile Collection:

1. Login to the FTK Central application.
2. Select **Collections**.
3. Select **View Existing Collections**.

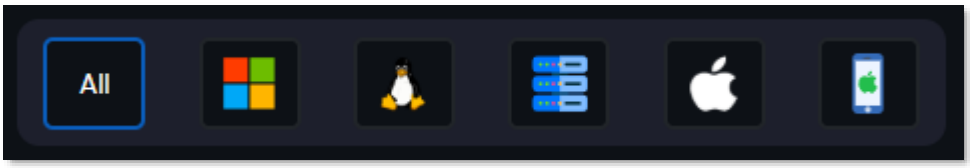


- The manage collections page is displayed.

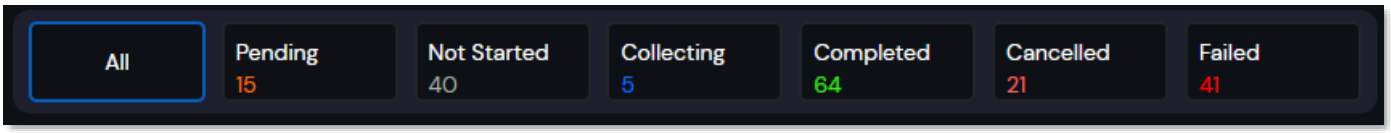


© Exterro, Inc. All rights reserved

4. You can filter the collections by clicking on any of the following filter options:
   - **Collection Type Filters:**



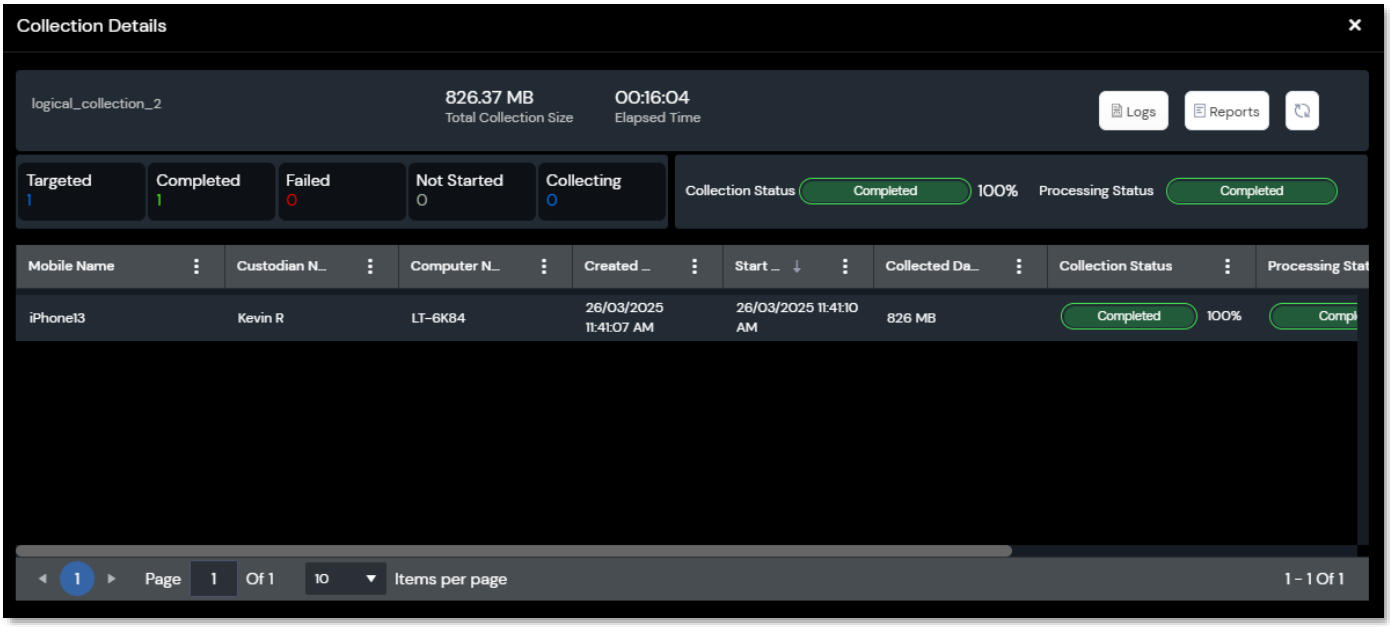
   - **Collection Status Filters:**



5. Click on the **Actions Menu** and select **Collection Details**.

© Exterro, Inc. All rights reserved

Note: Alternatively, you can click on the **Collection Status** column value against the required collection to view its details.

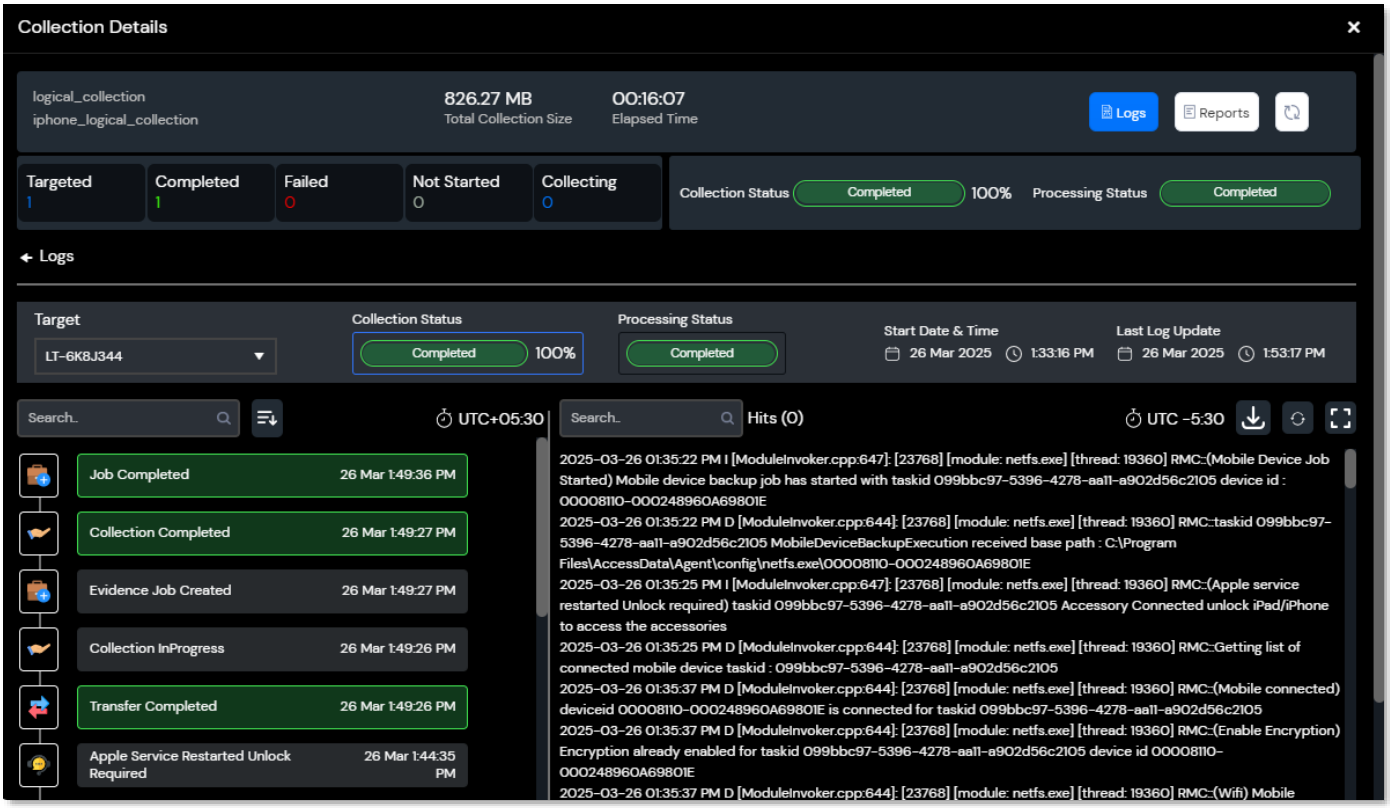


The details of the corresponding collection will be displayed.

© Exterro, Inc. All rights reserved

Collection Logs

You can click on the **Logs** button from the Collection details page to view the detailed Agent logs and comprehensive progress status of the Collection. You can select the required agent from the **Target** field to view the corresponding details.

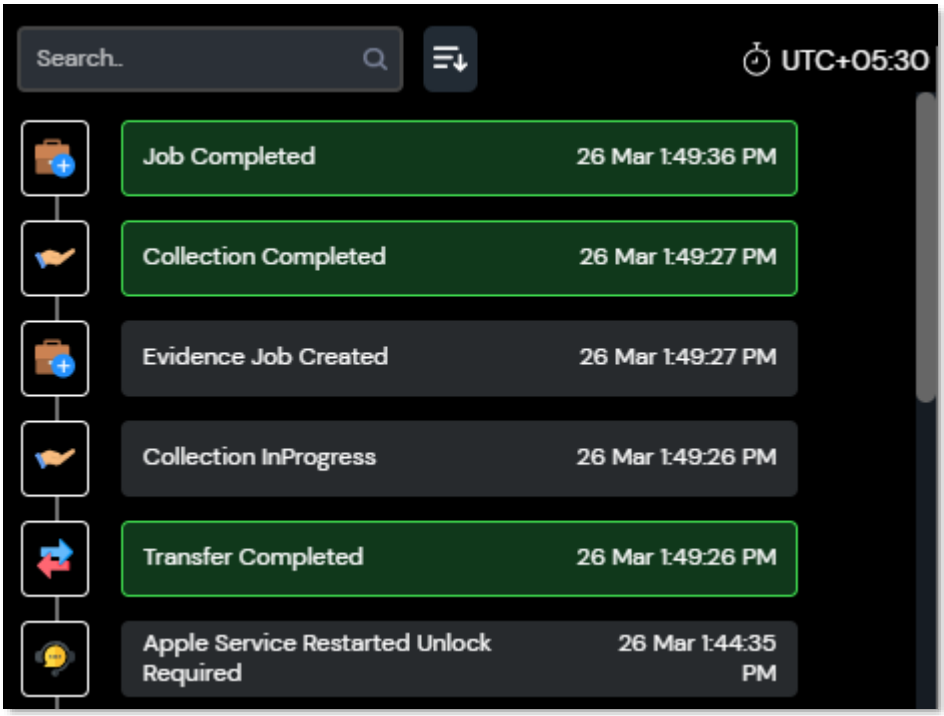


© Exterro, Inc. All rights reserved

Collection Progress:

You can view the Collection progress status from the left pane of the Logs section. You can use the search bar to search for the required status and sort the order of progress from job initiation to completion or vice versa by clicking of the **Sort** icon.

The time zone displayed here in this pane is the default time zone set in the **Case Defaults** of FTK Central Settings.



© Exterro, Inc. All rights reserved

Agent Logs:

The right pane of the **Logs** section displays the entire and detailed Agent logs. You can search for the required logs using the search bar. You can click on the following icons to perform the corresponding operations:

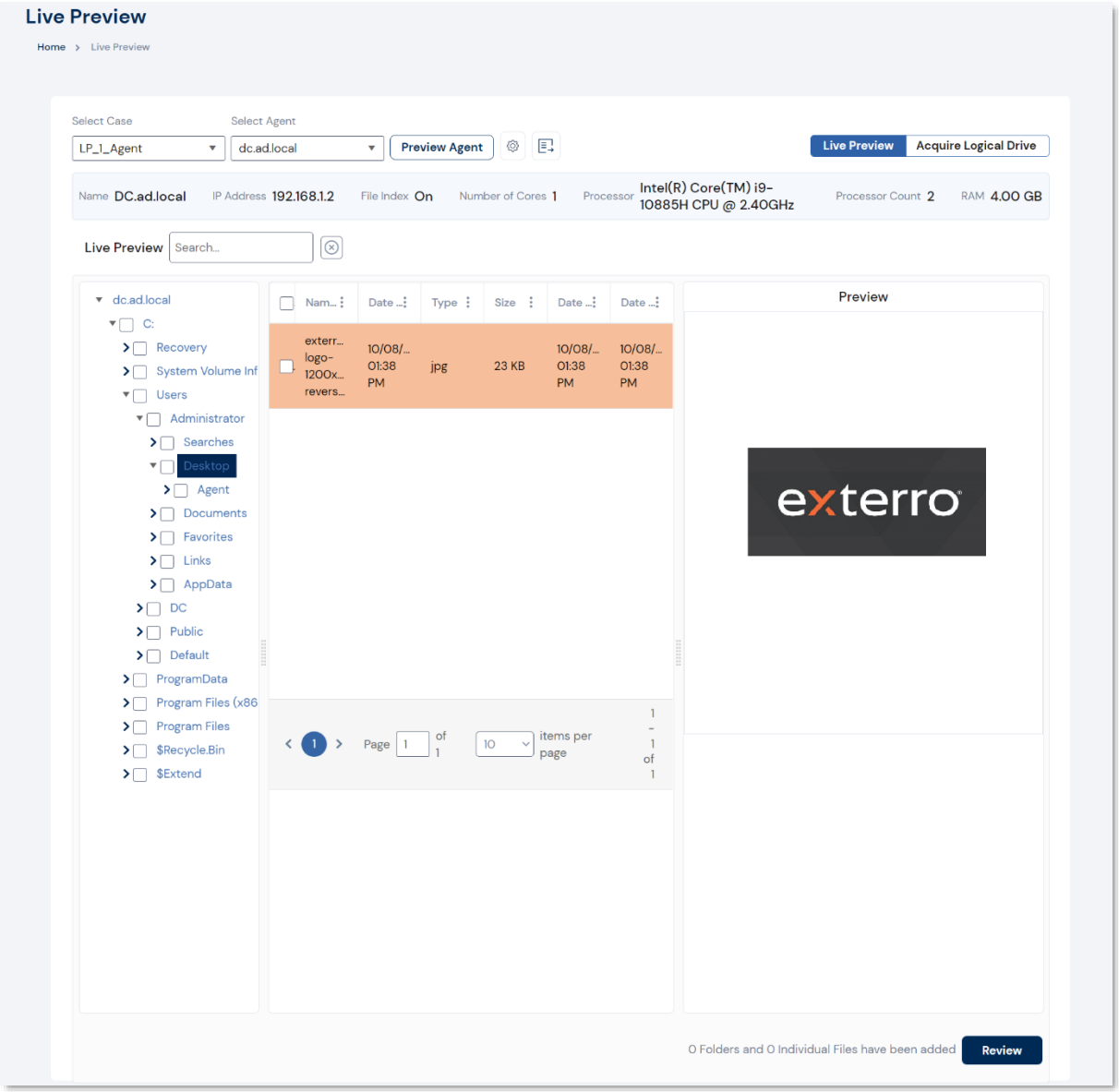
- - Download the logs
- - Refresh the logs
- - Expand the pop-up to have a better view of the logs

The time zone displayed in this section is based on the Agent selected.

© Exterro, Inc. All rights reserved

Live Preview

FTK Central users can now opt to view a Windows agent's file system prior to any collection job being initiated; this allows users to cull any data before opting to collect any files using a typical collection job. You can view the hierarchical structure of the files and folders in the system and choose to preview the files via the viewer.



© Exterro, Inc. All rights reserved

Windows, Linux, and Other Data Sources

UI Breakdown

General

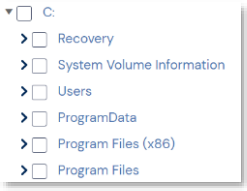
UI Element	Description
Select Case Please select	**Case Selection** – A case must be selected when attempting to utilise live preview. This list will display all available cases on a global level.
Select Agent Please select	**Agent Selection** – An agent must be selected when attempting to utilise live preview. This list will display all agents that have been added manually or via heartbeat.
Preview Agent	**Preview Agent** – Clicking this will allow an agent's file system to be shown as a live preview. • If an agent has not been recently live previewed, the button will initiate the job to collect file system information. • If an agent has been recently live previewed, the button will not initiate an additional live preview job and instead display the last file system information collected.
	Rerun Live Preview Job – Clicking this will rerun the live preview job. This will bring back the latest file system information rather than previously attained information. It is only available after a user has successfully run a live preview job for an agent in the past.

© Exterro, Inc. All rights reserved

UI Element	Description
Live Preview | Acquire Logical Drive	**Live Preview Job Selection** – Toggling this option will allow users to select a Live Preview/Acquire Logical Drive job. Each option has varying workflows.
Name DC.ad.local IP Address 192.168.1.2 File Index On Number of Cores 8 Processor Intel(R) Core(TM) i9-10885H CPU @ 2.40GHz Processor Count 16 RAM 64.00 GB	**Agent Information** – This pane will list basic network and hardware information. • **Name** – Hostname/IP of the agent selected. • **IP Address** – IP of the agent selected. • File Index – The currently toggled agent indexing status. • **Number of Cores** – Physical Cores of the agent selected. • **Processor** – Specifics about the processor. • **Processor Count**: Processor Threads of the agent selected. • **RAM** – Amount of volatile memory on the agent selected.

© Exterro, Inc. All rights reserved

Search and Culling

UI Element	Description
	Agent Indexing – Clicking this will allow Windows agent indexing to be toggled. By default, it is disabled. Additionally, users can provide specifics on what should/shouldn't be indexed on the agent system using the Include/Exclude filter options.
Live Preview Search	This field allows users to run quick searches against the Windows agents system index and accepts text strings connected by Boolean operators: AND and OR.
	**File System Tree** – When a live preview job has been completed, the file system tree will be generated. Users must check the files and folders for collection.
File Preview Viewer	This pane allows users to view files natively within the FTK Central viewer. Users must click on a single file within a directory to preview the file. **Exclusions:** • DLL • EXE • Windows Folder

© Exterro, Inc. All rights reserved

Live Previewing an Agent

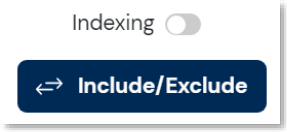
Warning: Users must ensure that an agent has been added manually using the Data Sources tab or automatically added via an active heartbeat configuration. Additionally, users must have a case available prior to attempting a live preview.

To live preview and collect files/folders from an agent:

1. From the home page, click **Collections**.
2. Select **Windows, Linux, and Other Data Sources**.
3. Select **Live Preview** from the left pane.
    - The Live Preview page is displayed.
4. Select a **Case**.
5. Select an **Agent** from the agent list.
6. Click the **Indexing** button to configure indexing on the agent (Optional).

Notes:

- You can configure an Include/Exclude filter to filter what should/shouldn't be indexed. Refer to the Indexing Filters for Live Preview.
- This configuration can be toggled prior to previewing an agent. This option must be enabled and configured before a live preview job has been initiated. Refer to the Live Preview: Windows Agent Indexing KB article.

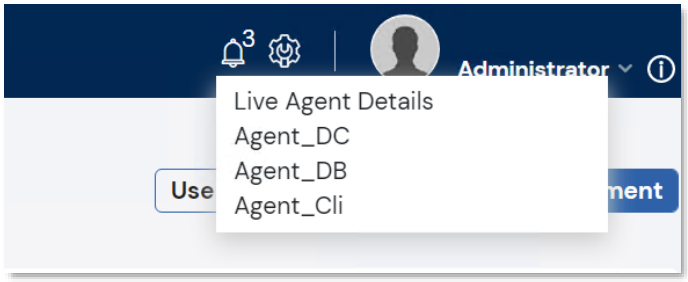


© Exterro, Inc. All rights reserved

7. Click **Preview Agent**.
   - A Live Preview job will be initiated and will begin copying file streams to generate a live preview.

Notes:

- The time it takes to complete this process is entirely dependent on the network in use.
- If an agent is offline or the site server is failing to recognize the connection with the agent, users will be prompted with a message asking if they would like to be notified (in the bell icon) when the agent regains connection with the site server. This status will be visible for 2 days or until the list of agents gets overwritten by the latest connection notifications (a list of 5 can be displayed at one time).



8. Once the job is completed, you can click **Preview Agent** again to refresh the file system tree and begin culling data.

Note: The downloaded preview files indication will be displayed globally for all cases in the **Preview Status** column.

© Exterro, Inc. All rights reserved

9. Once the file system tree has been generated, locate any folders/files of importance and check them. Alternatively use the select all checkbox to select all files and folders for collection.
    - Clicking on a single file within sub directory/file list will fetch the file and display the file in its native view.
10. Click **Review**.
    - The **Selection for Acquisition** page is displayed.
11. Check the items to finalize the collection.
12. Click **Acquire Files/Folders** to proceed with the collection.
    - The collection job will begin.

© Exterro, Inc. All rights reserved

Indexing Filters for Live Preview

The Windows agent can be configured to build a search index of the metadata and file contents of the system. The indexing is disabled by default, but for best results, you should configure the agent indexing settings to meet the requirements of your investigation.

Filter behaviors

The following are the fundamentals of using filters:

- When writing queries for the Keyword(s) field, use the terms AND or OR to help refine your search. For example: "Apple AND Oranges" will return only the files with both terms "apple" and "oranges".
- In the extension field, you can use an asterisk (*) as a wildcard. For example, doc* which will include both .doc and .docx.

  ***Note**: You can specify multiple extensions by separating with a comma.*

- In the Path, you can include or exclude files based on folders/sub-folders in the share or on the computer. You can specify folders by doing the following:
  - Include or exclude a complete folder name. ***Example:*** *\\documents\my_Work_files*
  - Include or exclude a folder name using wildcards. e.g. *work*
  - Spaces within a folder name are allowed. e.g. shared files

  ***Note**: You can specify multiple paths by separating with a comma.*

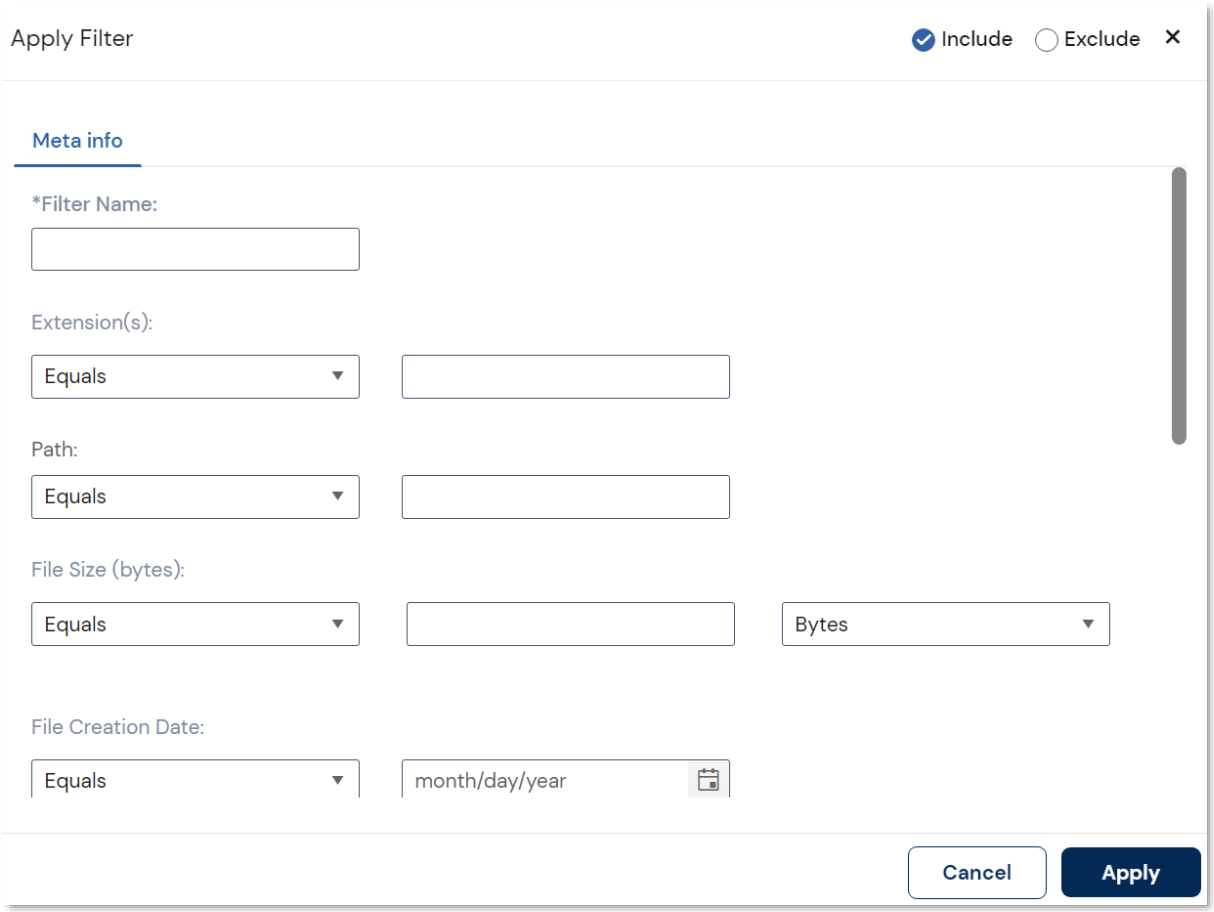
© Exterro, Inc. All rights reserved

- Multiple properties are treated with AND: When you add a filter, you can configure one or more properties within the filter and the properties are combined as an AND function. For example, if you add an inclusion filter, and an extension of PDF and also a file size of greater than 2MB, the logic is "PDF" AND ">2MB". The results will include only PDF files that have a file size greater than 2 MB.
- Multiple values in the same property are treated with OR: When more than one values are provided for a same property, the values are treated with OR function. As another example, if you add an inclusion filter with two extensions "DOCX, XLSX" then the results will include both DOCX and XLSX files.
- Path always takes precedence: If you include a path as a property in a filter, any other properties specified in the same filter will only apply to the specified path. Suppose you target a network share \\documents and you create an inclusion filter and specify the folder my_Work_files. Additionally, in the same filter you specify a file extension as PDF. In this example, only the PDF files in the my_Work_files folder is included.
- Inclusion and Exclusion filters are treated with AND: You can add both Inclusion filter and Exclusion filter to get the required data. For example, specify an Inclusion filter with extension as PDF and an Exclusion filter, file size greater than 3MB. The result will include only PDF files that are less than 3MB.

© Exterro, Inc. All rights reserved

To configure the index filter for Live Preview:

5. From the **Indexing** button, click **Include/Exclude**.
    - The **Apply Filter** prompt is displayed.



6. Provide a name for the filter in **Filter Name**.
7. Select if you want to **Include** or **Exclude** the filtered files by enabling the required option in the top right corner of the prompt.
8. Configure the required filters as instructed in Filter Behaviors.
9. Click **Apply.**

© Exterro, Inc. All rights reserved

Collection and Index related folders

Job Type	Description
• Collection • Live Preview • Acquire Logical Drive • Indexing • Index Search	Selected files/folders/logical drive will be added to an .AD1 image maintaining the existing directory structure and will be located within the case folder associated to the selected case; the folder holding the .AD1 image is named **AcquiredFiles**. **Note:** This image will not be added to a case or processed. This must be done manually.

Acquired logical drives will be added to an .AD1 image maintaining the existing directory structure and will be located within the case folder associated to the selected case; the folder holding the .AD1 image is named **AcquiredLogicalDrives**. This image will be added to a case and processed using the default processing profile configure in the administration section.

Any files that may have been previewed in the viewer will be located within the case folder associated to the selected case; the folder holding the previewed files is named **AgentLivePreview**.

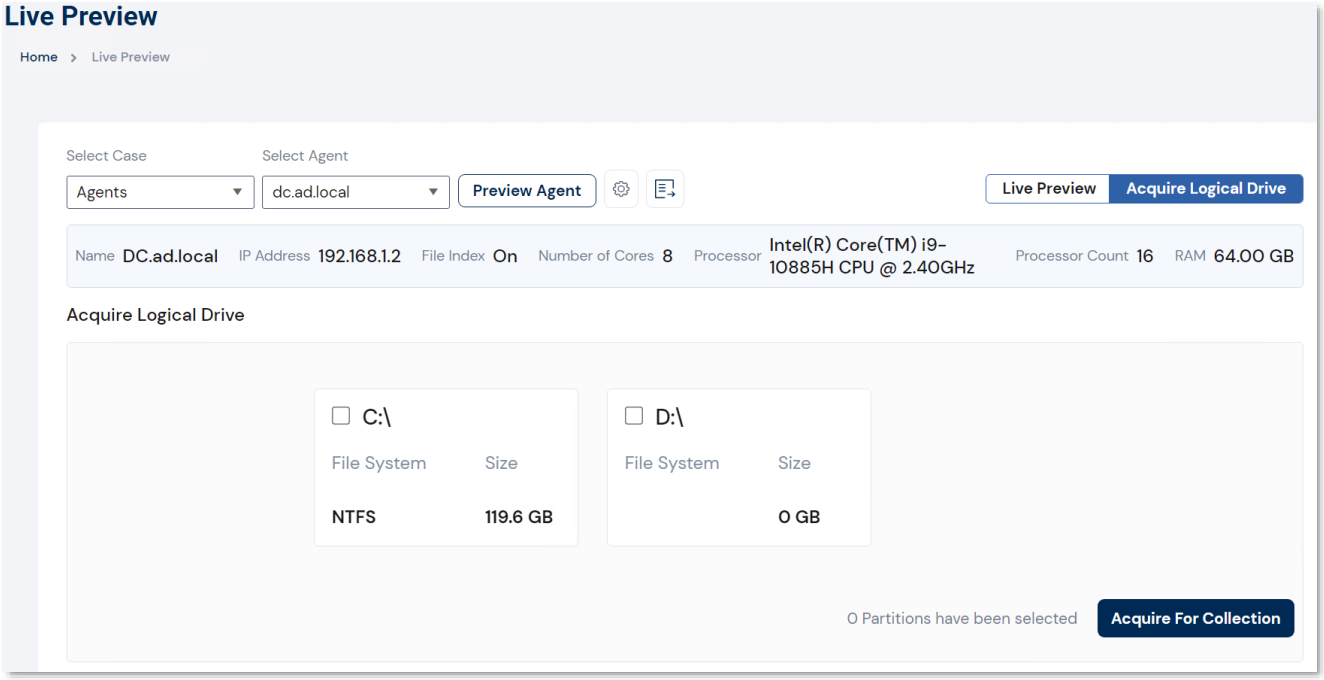
If indexing was enabled on an agent, the resulting log will be located within the case folder associated to the selected case; the folder holding the index log is named **DTSIndexJob$**.

When a search has been run again a live preview, the resulting index search report will be located within the case folder associated to the selected case; the folder holding the search report is named **DTSIndexSearch$**.

© Exterro, Inc. All rights reserved

Acquiring a Logical Drive from an Agent

Logical drive acquisitions allow users to select specific partitions for collection.



To acquire a logical drive from an agent:

1. From the home page, click **Live Preview**.
    - The Live Preview page is displayed.
2. Select **Acquire Logical Drive** in the top-right.
3. Select a **Case**.
4. Select an **Agent** from the agent list.
5. Select a drive by checking it.
6. Click **Acquire For Collection**.
    - The collection job will begin. Once complete, the image will be added and processed in the selected case.

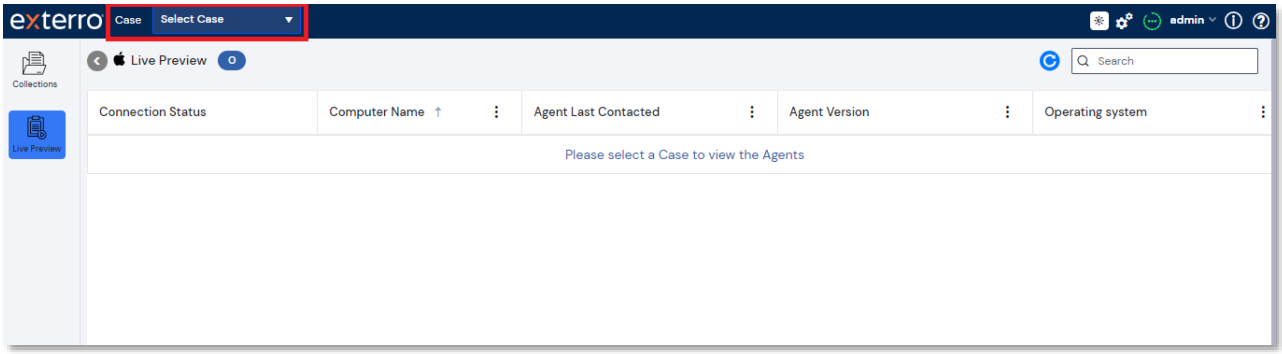
© Exterro, Inc. All rights reserved

Mac

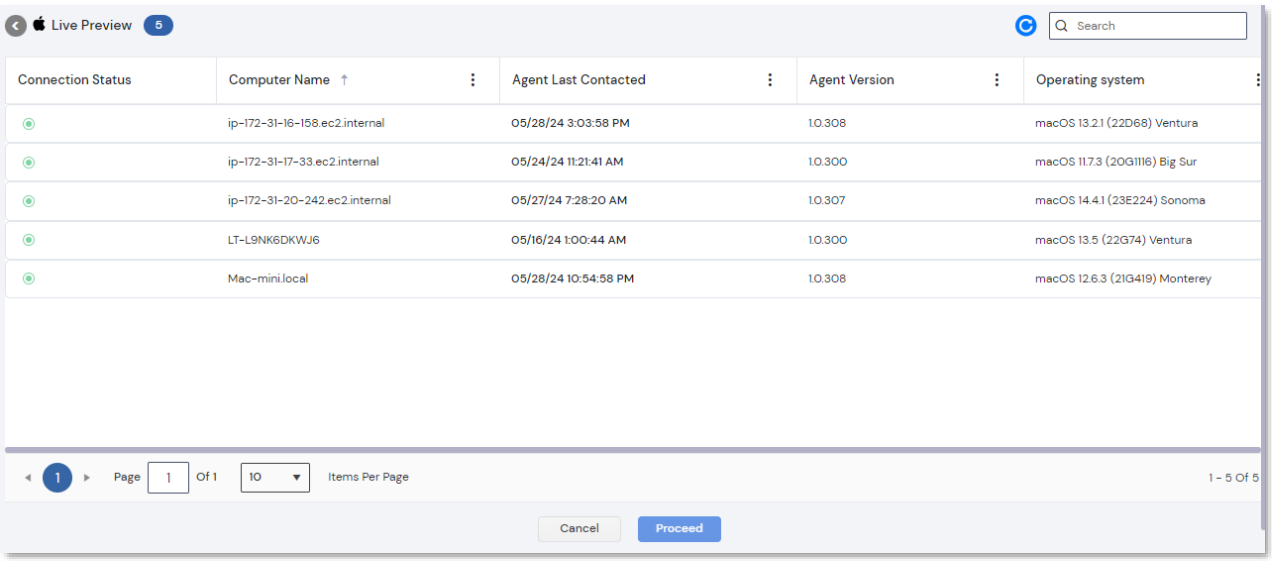
Live Previewing a Mac Agent

To live preview and collect files/folders from a Mac agent:

1. From the home page, click on **Collections**.
2. Select the **Mac** option.
3. Select **Live Preview** from the left pane.
4. Select the required **Case** from the header.

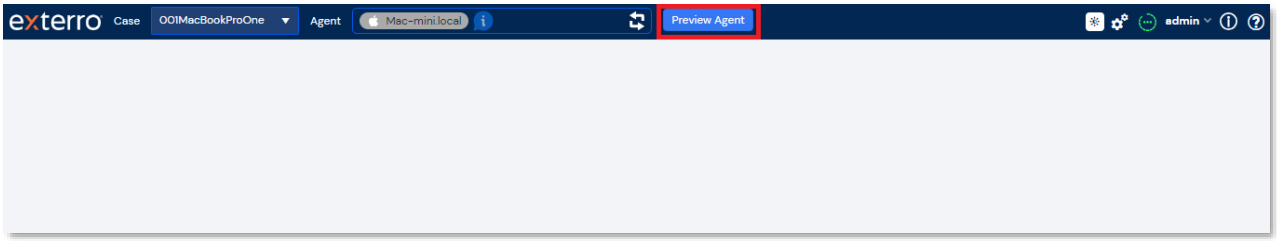


- The list of Mac agents associated with the case is displayed.



© Exterro, Inc. All rights reserved

5. Select the required Mac from the list.
6. Click **Proceed**.
7. Click **Preview Agent**.



- A Live Preview job will be initiated and will begin copying file streams to generate a live preview.

Note: The time it takes to complete this process is entirely dependent on the network in use.

Warning: Due to macOS security restrictions, certain system-protected folders are not indexed by Apple and will not appear in Advanced Search (mdfind) results during Live Preview. To view or collect files from these locations, please use the Filter Collection (rsync) operation, which scans the live disk directly.

© Exterro, Inc. All rights reserved

8. Once the file system tree has been generated, locate any folders/files of importance and check them. Alternatively use the select all checkbox to select all files and folders for collection.
   - Clicking on a single file within sub directory/file list will fetch the file and display the file in its native view.

Warning: Multimedia file types that cannot be previewed will be downloaded automatically to the system in use.

If you do not want to download such files automatically, please ensure the following options are enabled in the corresponding browser settings:

- **Microsoft Edge** – Ask me what to do with each download.
- **Google Chrome** – Ask where to save each file before downloading.

9. Click **Review**.
   - The **Acquisition** page is displayed.

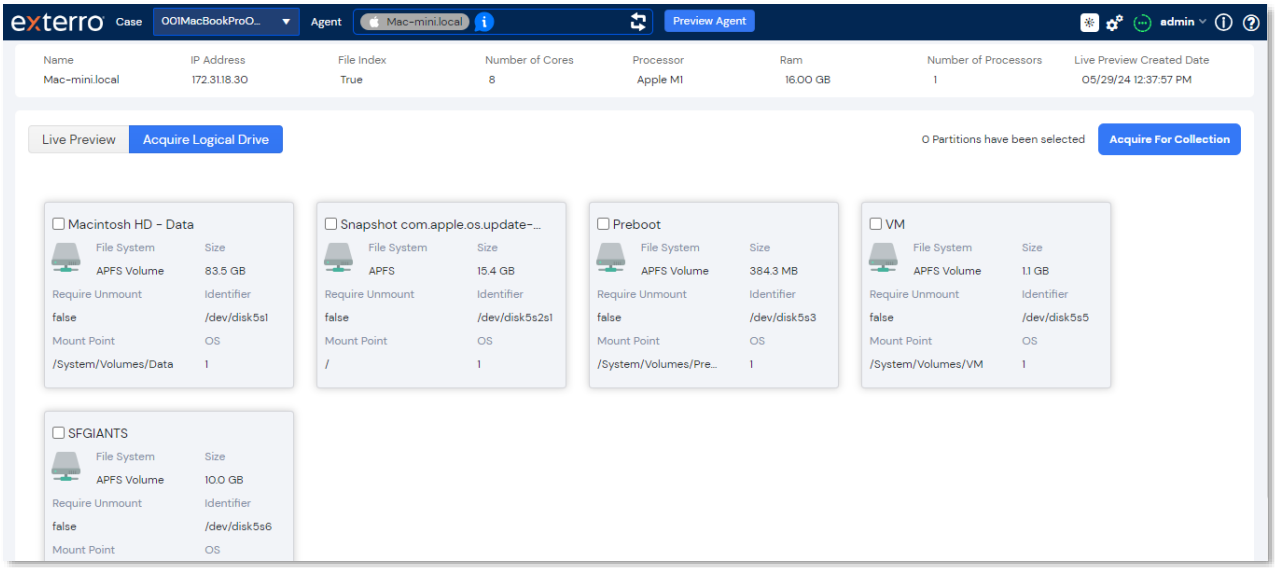
Warning: When the indexing is in-progress for an agent, incorrect search results will be displayed upon performing **Advanced Search** for the files in Live Preview.

10. Check the items to finalize the collection.
11. Click **Acquire Files/Folders** to proceed with the collection.
    - The collection job will begin.

© Exterro, Inc. All rights reserved

Acquiring a Logical Drive from a Mac Agent

Logical drive acquisitions allow users to select specific partitions for collection.



To acquire a logical drive from a Mac agent:

1. From the home page, click **Collection**.
2. Select the **Mac** option.
3. Select **Live Preview** from the left pane.
4. Select the required **Case** from the header.
5. Select the required Mac agent from the agent list.
6. Click on **Preview Agent**.
7. Select **Acquire Logical Drive**.

© Exterro, Inc. All rights reserved

8. Select the required drives by checking them.

Notes:

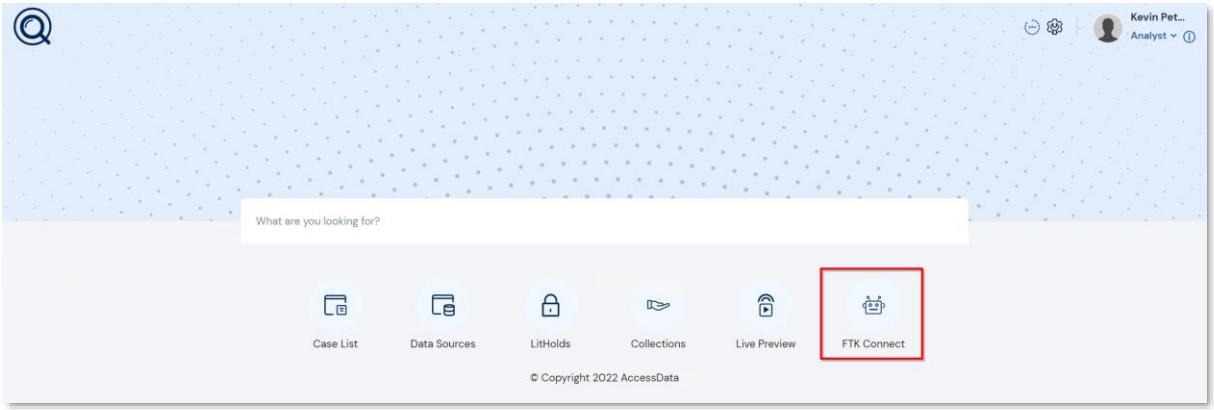
- The size listed within this panel, indicates the amount of storage that is actively used on a listed drive and not the size of the drive itself.
- The size may be lesser than the size shown in the Collection Details. This is due to MacOS implementing transparent compression on files. Collection sizes will understandably be greater once they are made available on the Windows File System.

9. Click **Acquire For Collection**.
   - The collection job will begin. Once completed, the image will be added and processed in the selected case using the default processing profile set within the Case Defaults.

© Exterro, Inc. All rights reserved

FTK Connect

FTK Connect is a robust automation add-on for FTK Central. Users can create workflows to include processes such as data ingestion, endpoint collections, exports as well as search & tagging documents. Despite the fact these options can be carried out manually by users, FTK Connect allows these workflows to be adjusted to the needs of the organization while remaining entirely automated; with manual, automated and scheduled and API Trigger execution methods.



Managing FTK Connect

Using FTK Connect, you can select and examine your data in multiple ways. You can use various panels to examine the data

Elements of Managing FTK Connect

Automation	• UI Breakdown
	• Automation Options
	  ○ Start
	  ○ Case Details
	  ○ Processing
	  ○ Search & Tag
	  ○ Collection
	  ○ Export
	• Creating an Automation
	• Job Monitors

© Exterro, Inc. All rights reserved

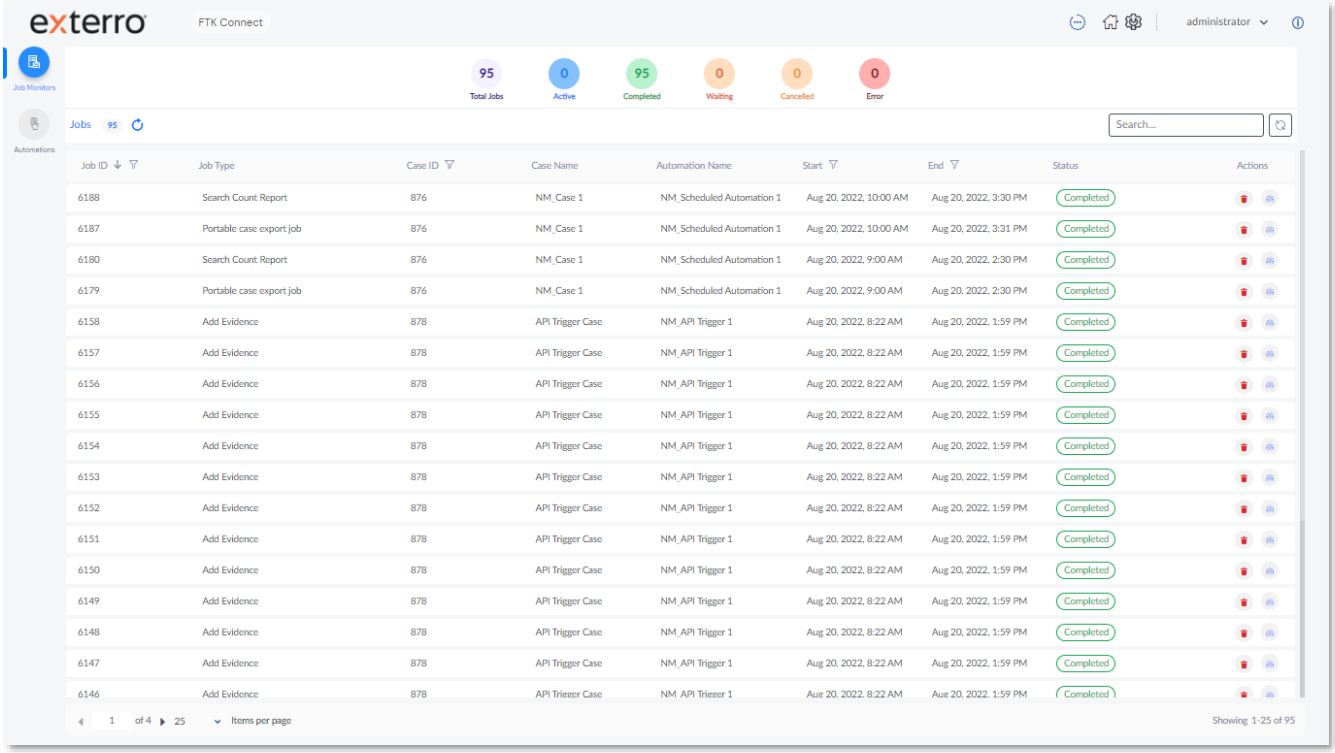
Automations

Accessing FTK Connect will open the automations homepage. This page lists all automations created so far, regardless of their current state; inactive or active. The page will also provide details of the automation such as names, description, created/modified dates, created by, active jobs and the number of times an automation has been run.

UI Breakdown

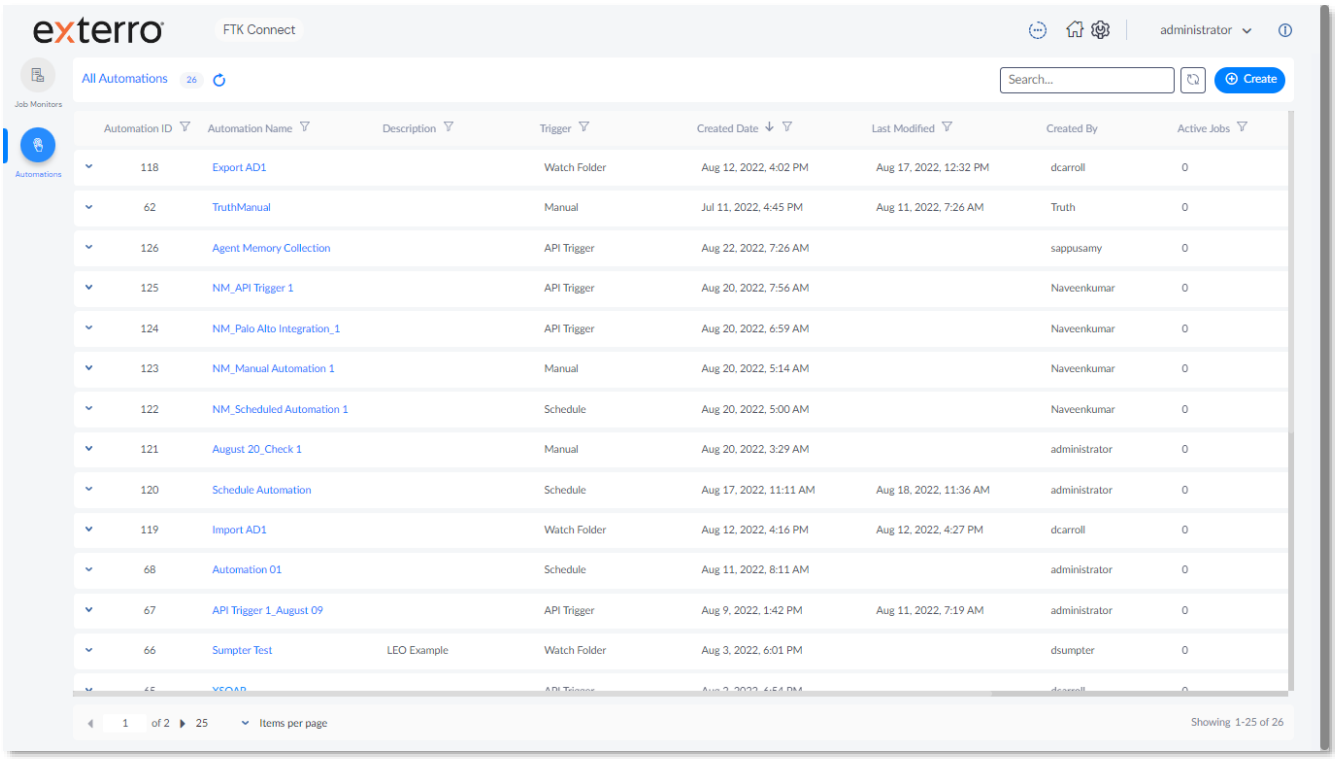
Left Pane

- **Job Monitors -** Takes you to the job monitor page where you can see automation-related job statuses.

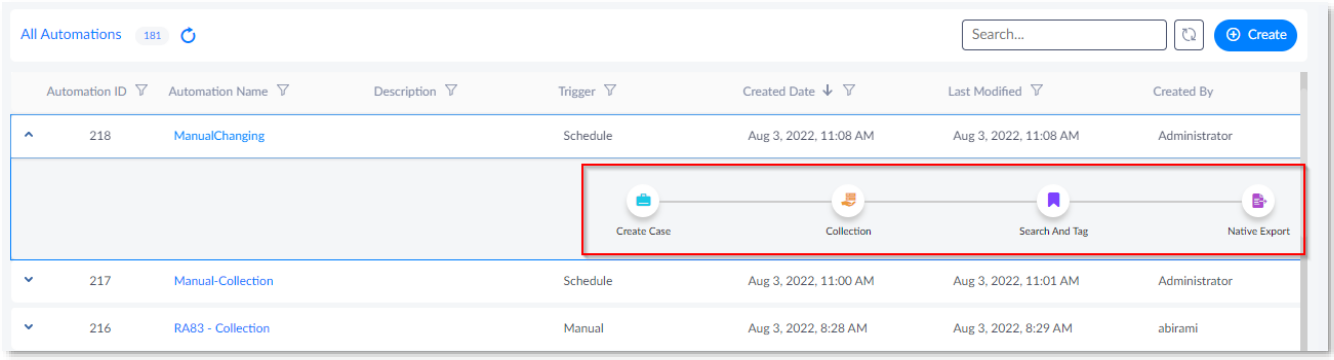


© Exterro, Inc. All rights reserved

- **Automations -** Takes you to the default home page where users can view the automations.



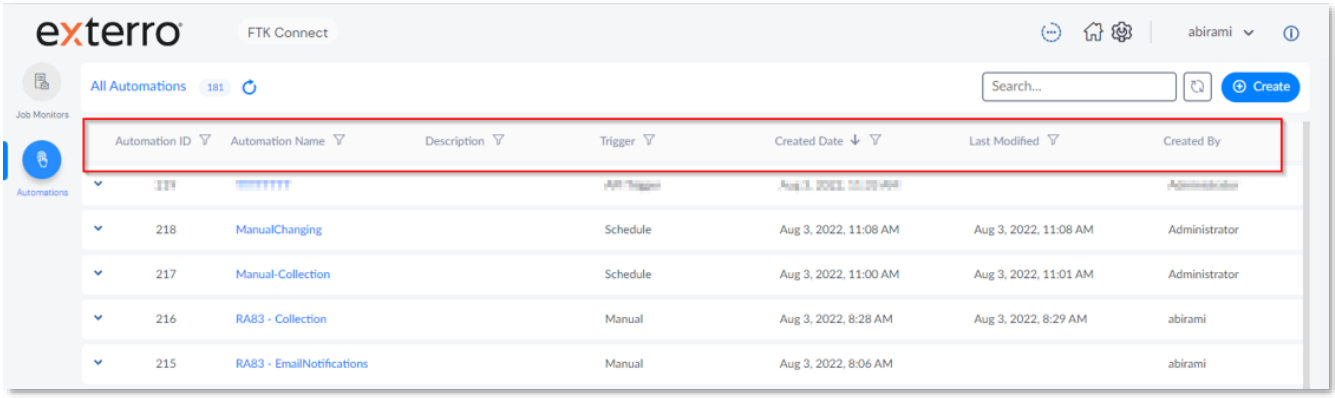
You can have a glance of the workflows in an automation by clicking on it.



© Exterro, Inc. All rights reserved

Right Pane

You can view the list of Automations available along with the following details

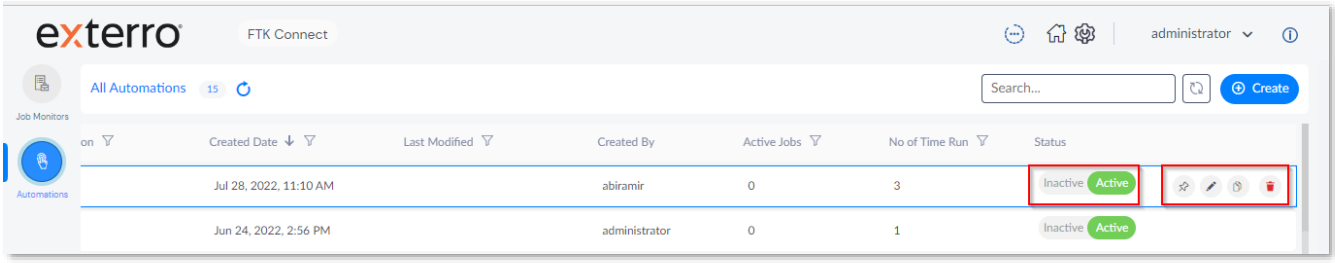


Columns	Description
Automation ID	The automation ID is assigned in incremental order.
Automation Name	The name provided for the Automation.
Description	The description provided for the Automation.
Created Date	The date when the Automation is created.
Last Modified	The latest date when the Automation was modified/edited.
Created By	The name of the user by whom the Automation was created.
Active Jobs	The jobs that are active and running at the moment.
Number of Times Run	Denotes the count of number of times the automation has been run till date.
Status	The status of the Automation whether Active/Inactive.

© Exterro, Inc. All rights reserved

Automation Options

You can also perform the following actions for the automations:



Icon	Columns	Description
	Filter	Filters the columns to view automations accordingly.
Inactive Active	Inactive/Active	Activates/Deactivates the Automation.
	Pin	Pins and keeps workflow at the top of the list.
	Trigger Automation	Executes the automation. However, this icon will be displayed only for Manual automation.
	Edit	Allows users to edit existing automations which enables to add/remove existing automation steps.
	Duplicate	Makes a copy of an existing automation.
	Delete	To delete an automation.
Create	Create	Allows users to start creating an automation.
	Administration	Navigates to administration page within FTK Central.
	Home page	Navigates to FTK Central home page.

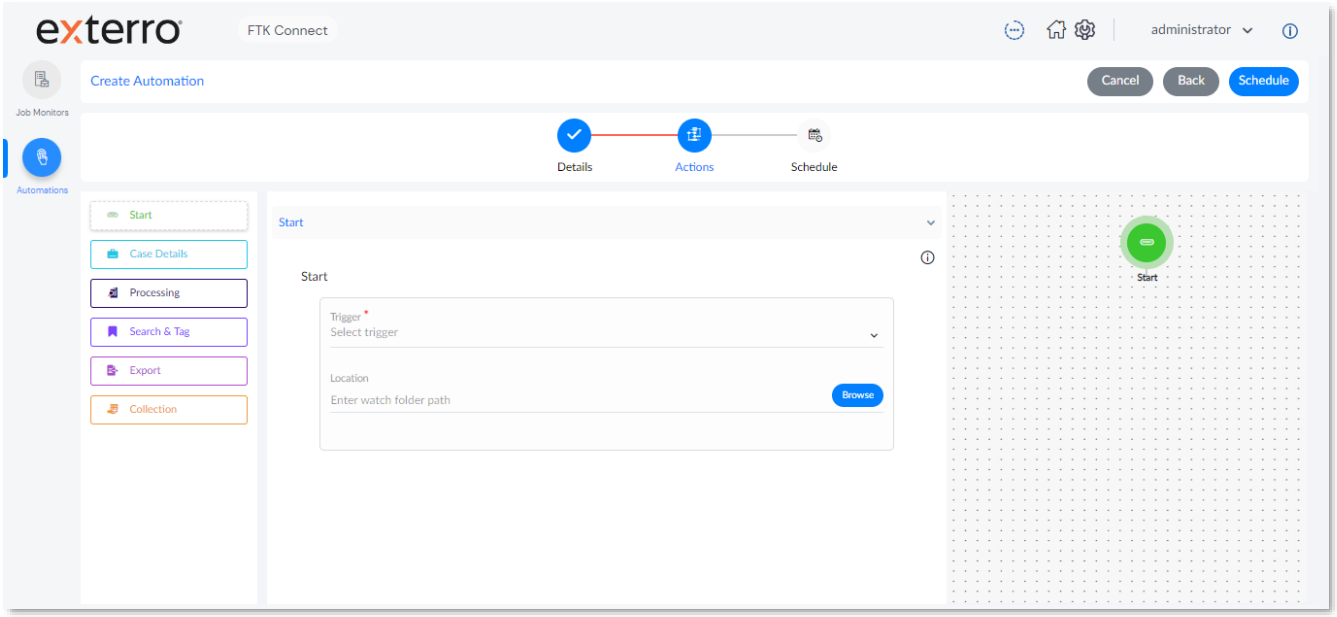
© Exterro, Inc. All rights reserved

Icon	Columns	Description
	Job queue	Shows global job statuses.

Automation Workflows

Warning: Before configuring Automation for new cases, a default path must be set within Case Defaults located in the Administration section.

There are six Workflows available out of the box in FTK Connect.

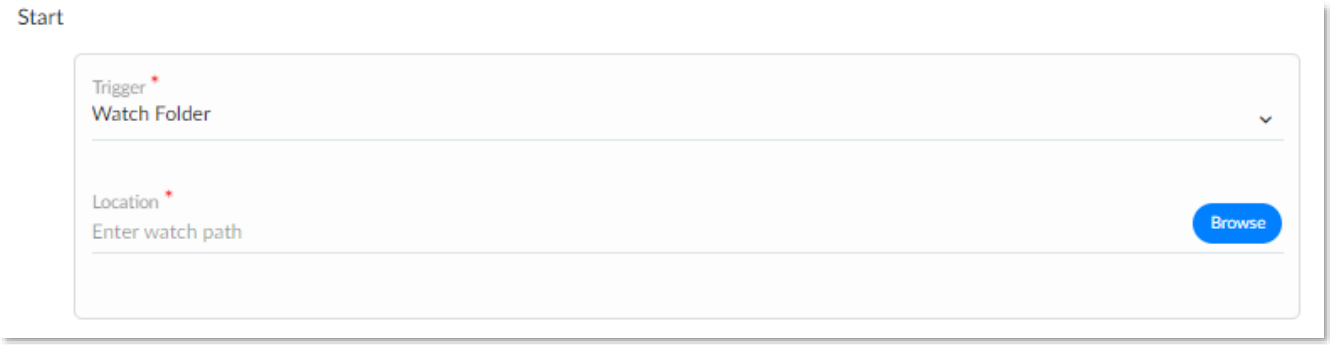


- Start
- Case Details
- Processing
- Search & Tag
- Export
- Collection

© Exterro, Inc. All rights reserved

Start

The Start option is a mandatory workflow and is to be added by default as it dictates how an automation is executed. It is important to ensure a specific trigger type is selected to ensure the automation is executed as required.



The following are the options available:

Options	Description
Watch Folder	Allows users to execute automations by listening to a watch folder location. When FTK Central is installed, it includes a listener which waits for a user-specified directory until evidence (including loose files) are fully transferred.
API Trigger	Allows users to execute workflows by calling the Automation ID using an API client.
Schedule	Allow users to schedule the execution of automations based on a time, date and optionally a recurrence.
Manual	Allows users to execute automations manually (by clicking Execute from the automations homepage).

© Exterro, Inc. All rights reserved

Watch Folder Rules

- A single Watch Folder must be associated with a workflow.
- UNC paths must be used when creating an automation workflow. This path must be accessible to the Service Account used during installation. (e.g. \\ServerName\C$\WatchFolder)
- Any Evidence (Forensic Images, loose files etc.) must be stored in a child directory within the Watch Folder. If it is not transferred within a folder, the files moved into a "Ignored" folder.
    - (e.g. \\ServerName\C$\WatchFolder\Case1_Evidence\)
- The Case name will be set based on the name of the folder storing any evidence.
    - (e.g. \\ServerName\C$\WatchFolder\Case1_Evidence\ will set the case name to Case1_Evidence)
- When a folder holding evidence is entirely transferred to a Watch Folder, it will then be moved to a folder named "Processed" within 3 minutes. This folder is used by FTK Central; processing will begin within 5 minutes.
- If an existing case requires additional evidence to be added, ensure the Watch Folder name is the same as the existing case name. (e.g. adding evidence to the Case1_Evidence case will require a child directory named Case1_Evidence within the Watch Folder).

API Trigger Rules

- API inputs will supersede the inputs from other trigger types.
- Calling the workflow ID is sufficient to execute existing automations.
- A Watch Folder is not required when using the API trigger.

Note: Refer to the API Trigger Workflow section.

© Exterro, Inc. All rights reserved

Schedule Rules

- In a manual workflow, if Processing and/or Search & Tag options are required, then a watch folder must be provided. Additional information is provided within the Start option.
- A Watch Folder is not required by default. A scenario where it may be useful to provide a watch folder path and scheduled execution is when a user may not want to ingest and process files until after hours. The scheduled date and time would be specified to execute the ingestion and processing of data using the specified parameters.

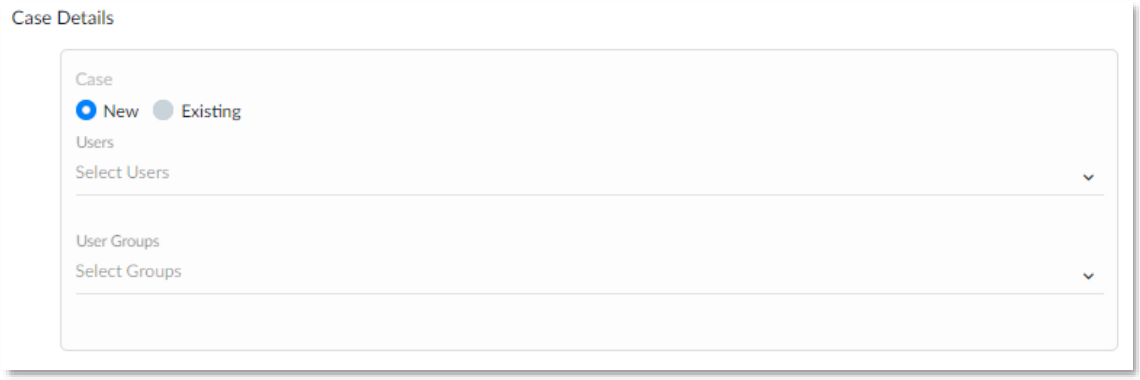
Manual Rules

- A Watch Folder is not required when using the Manual trigger.
- In a manual workflow, if Processing and/or Search & Tag options are required then a watch folder must be provided.
- Users must click "Execute" located on the automations homepage to start any manual workflows.

© Exterro, Inc. All rights reserved

Case Details

The Case Details option can be added to an automation that requires data to be ingested/processed or added via means of an agent collection to a new or existing case.



Case Detail Rules

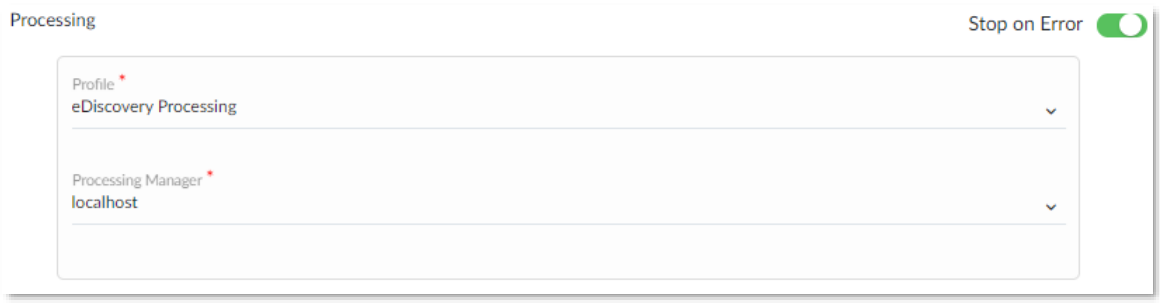
- By default, any automation created will be assigned to the user that created it.
- New cases will allow Users and/or Groups to be given access to a case.
- Multiple cases can be selected when using existing cases for an automation. Case access to existing cases will be dependent on the existing case access.
- New cases are named using the name of the Watch Folder path provided.

© Exterro, Inc. All rights reserved

Processing

The Processing option allows users to select a defined Processing Profile from a list of default out of the box options or select a custom profile which may have been created in any of the FTK product lineup. Additionally, users can select a specific Processing Manager to handle the processing jobs associated to an automation.

Note: Users can toggle the **Stop on Error** option Stop on Error to automatically stop any preceding automation options.



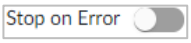
Processing Rules

- The Processing Profiles listed include default and custom profiles.
- A single Watch Folder must be associated with a processing workflow.
- A Watch Folder is not required when using the API trigger.
- The Processing option must be utilized if a new case is being created.
- The default Processing Profile will be dependent on the default configuration. These options can be found in Case Defaults within the Administration section.
- If the "Field Mode" processing profile is utilized, Search and Tag will not be functional.

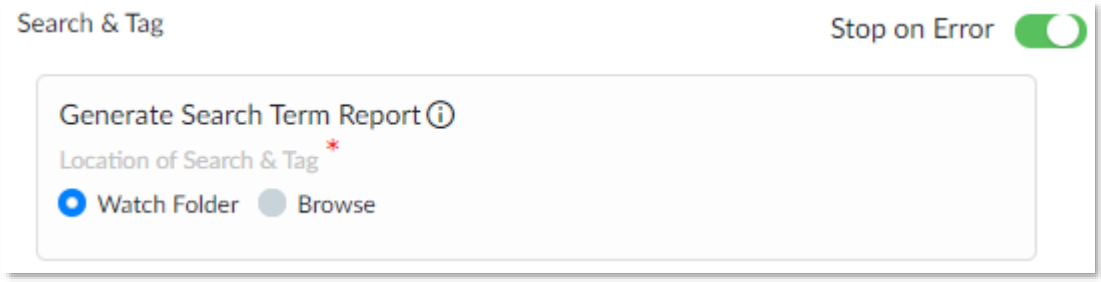
© Exterro, Inc. All rights reserved

Search & Tag

The Search & Tag option allows users to use wordlists (.txt) to automate the search and tagging of documents. Wordlists can contain specific terms followed by a label name.

Note: Users can toggle the **Stop on Error** option 

to automatically stop any preceding automation options.



Search & Tag Rules

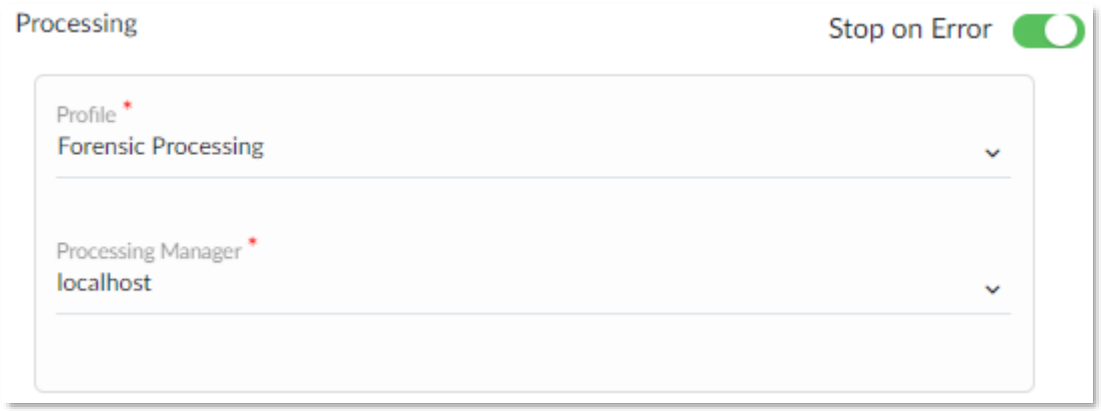
- If the Watch Folder trigger is being utilized, keyword text files must be stored in a child directory within the Watch Folder holding the evidence. It must be named "SearchAndTag"; case insensitive.
    - (e.g. \\ServerName\C$\WatchFolder\Case1_Evidence\SearchAndTag)
- If the Browse option is selected within Search & Tag options, the folder restriction above does not apply.
- If the API trigger is being utilized, a Watch Folder path is not required.
- Search terms should be provided one per line.
- Multiple search term lists can be provided.
- Search terms can be followed by a label. If a label is not provided, then the search term will be used as the name of the label.
    - (SearchTerm,Label1)
- A search term report will be created upon successful execution. This report will be stored within the case folder associated with a workflow.

© Exterro, Inc. All rights reserved

Collection

The Collection option allows users to use templated (non-scheduled) collections within an automation. These collections can be put into an existing case and processed.

Note: Users can toggle the **Stop on Error** option Stop on Error to automatically stop any preceding automation options.



Collection Rules

- A Collection workflow can only be utilized when using new cases.
- The supported collection methods are listed below:
  - Filtered Acquisition
  - Full Disk Acquisition
  - Memory Acquisition
- Collection workflows can only be utilized with the use of collection templates. Collection templates can be created within the Collection tab.
  - Target(s) must be added to a collection template.
  - Auto approval must be set within a collection template.
  - Scheduling must not be present within a collection template.

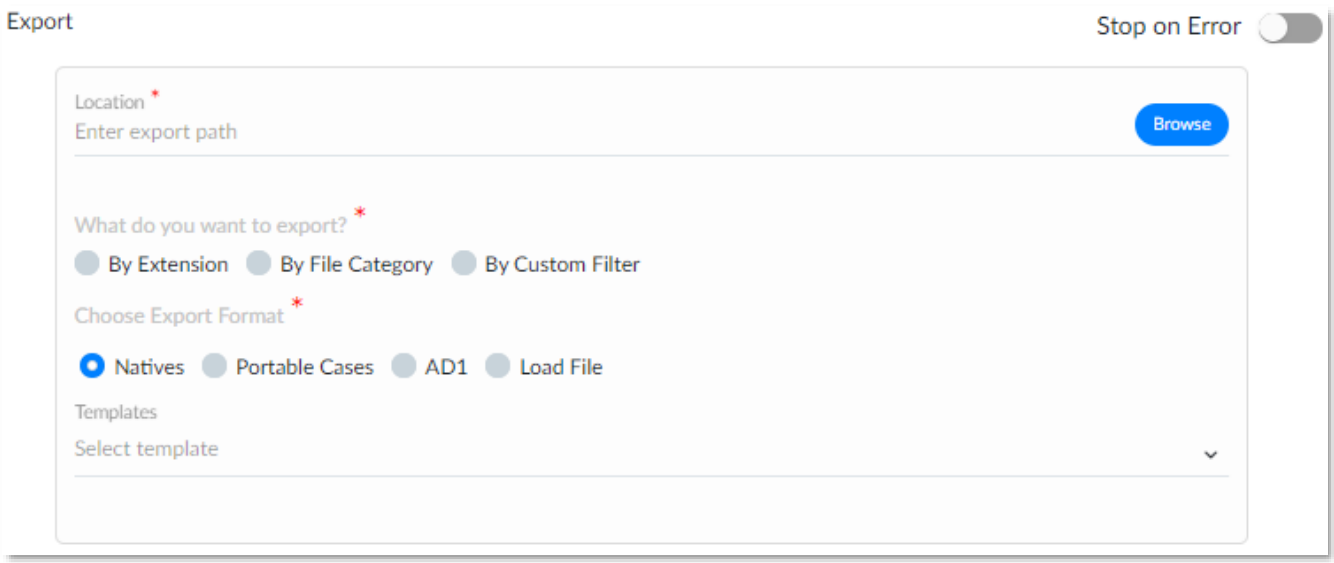
© Exterro, Inc. All rights reserved

Export

The Export option allows export of data in the specified format. This can be exported in multiple formats including natives, portable cases and AD1,

- By Extension
- By File Category
- By Custom Filter
- By Search & Tag (This option appears when search & tag automation step is used)
- By Tag (Applicable for existing cases alone. Either by Labels or by Bookmarks)

Note: Users can toggle the **Stop on Error** option Stop on Error to automatically stop any preceding automation options.



© Exterro, Inc. All rights reserved

Export Rules

By Custom Filter

- The Custom Filter drop-down will list custom filters created in FTK Lab/Enterprise.
- Default filters will not be listed.

By Search & Tag

- Search and Tag must be selected within a workflow to enable this export type.

By Tag

- An existing case must be selected within Case Details to enable this export type.
- All Labels and/or Bookmarks can be exported.

By Extension

- Multiple file extensions must be comma (,) separated.

Export Formats

Natives and AD1

- Native exports do not required a template.
- Exports without templates will be exported using (application) default settings.
- Templates can be created within the export section of a case.

Export Format Portable Case

- Template is not required for a Portable Case.

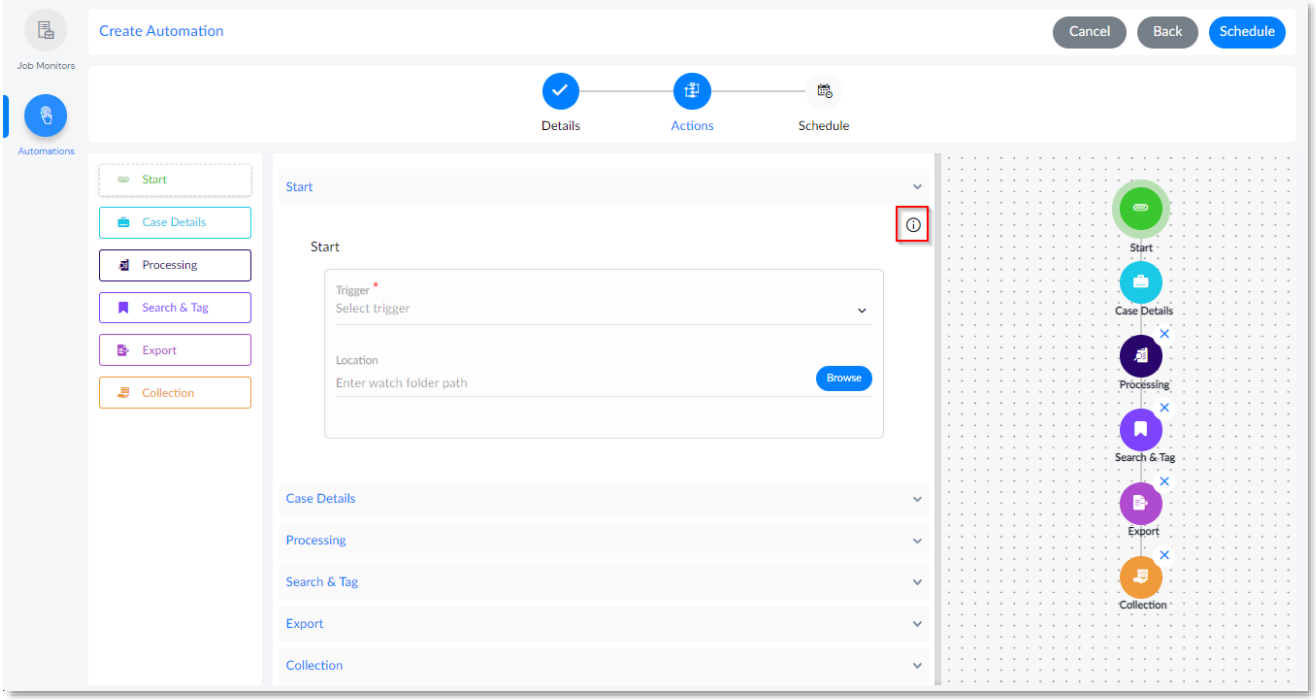
Export Format Load File

- Load File exports must include a template.
- Templates can be created within the export section of a case.

© Exterro, Inc. All rights reserved

Creating an automation

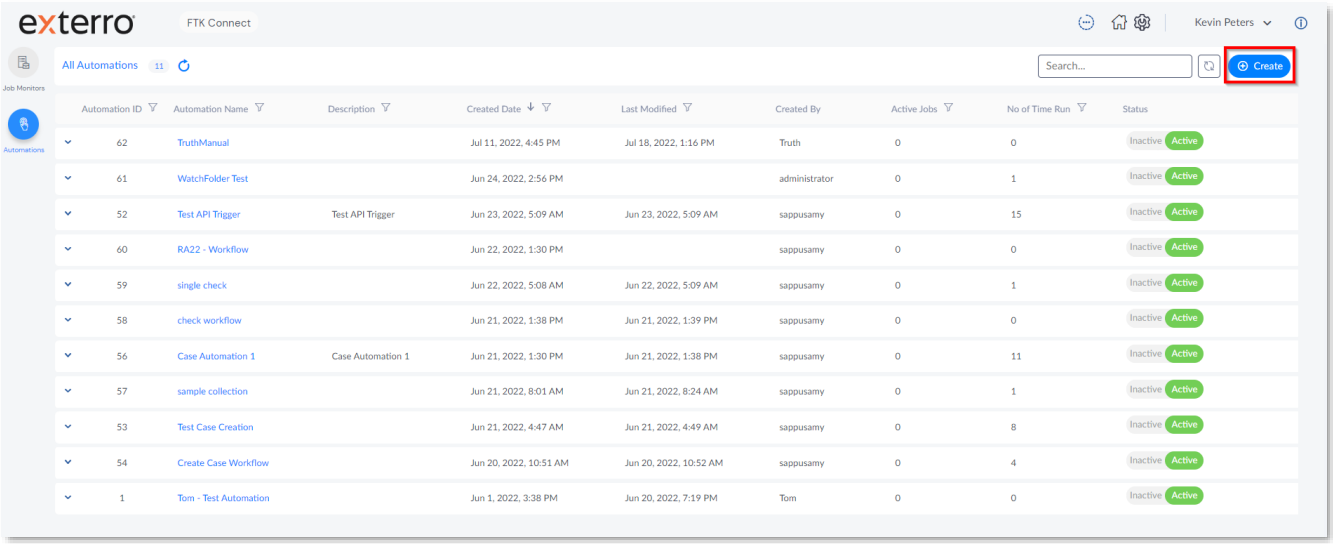
You can create Automations with either all of the available automations or with the required ones.



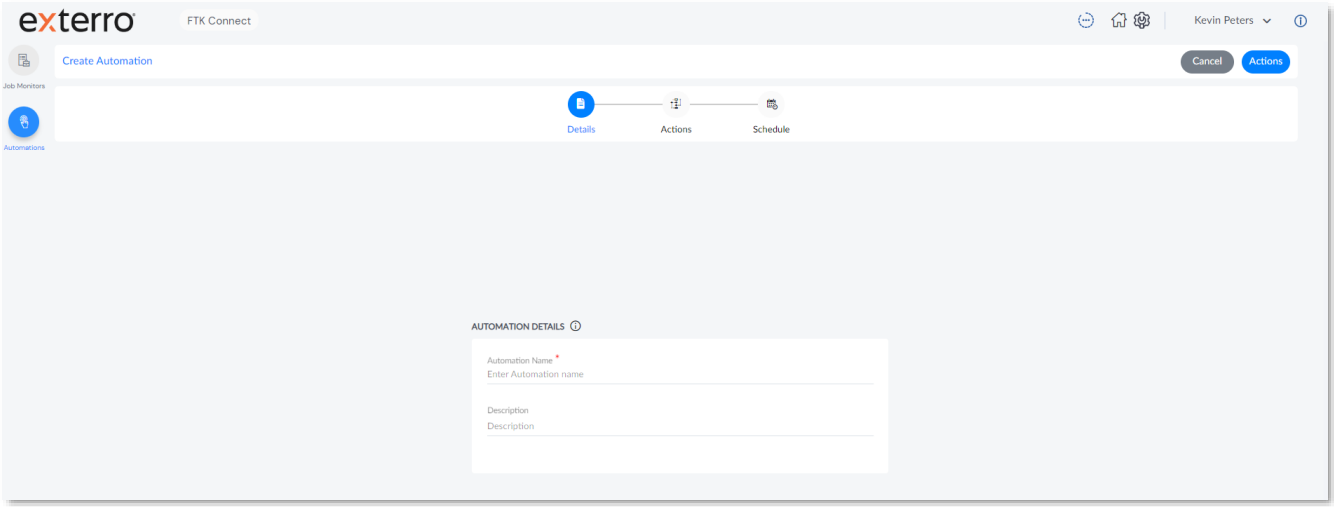
Note: You can click on the ⓘ (**Rules Section**), to list the rules which shall be considered while configuring each section of the Automation.

© Exterro, Inc. All rights reserved

8. From the Home Page of FTK Central, click **FTK Connect**.
    - The Manage Page of Automation is displayed.



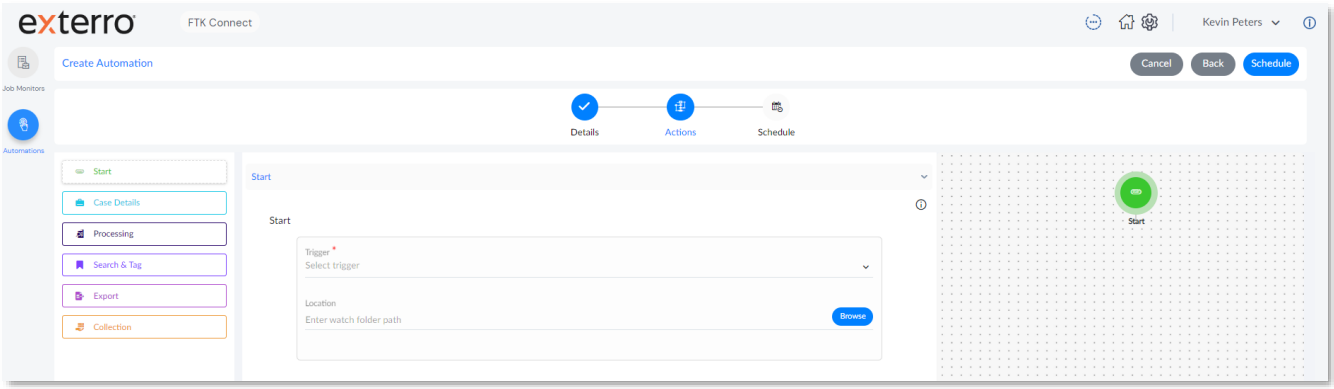
9. Click **Create**.
10. Enter an **Automation Name**.
11. Enter an **Automation Description**.



12. Click **Actions**.

© Exterro, Inc. All rights reserved

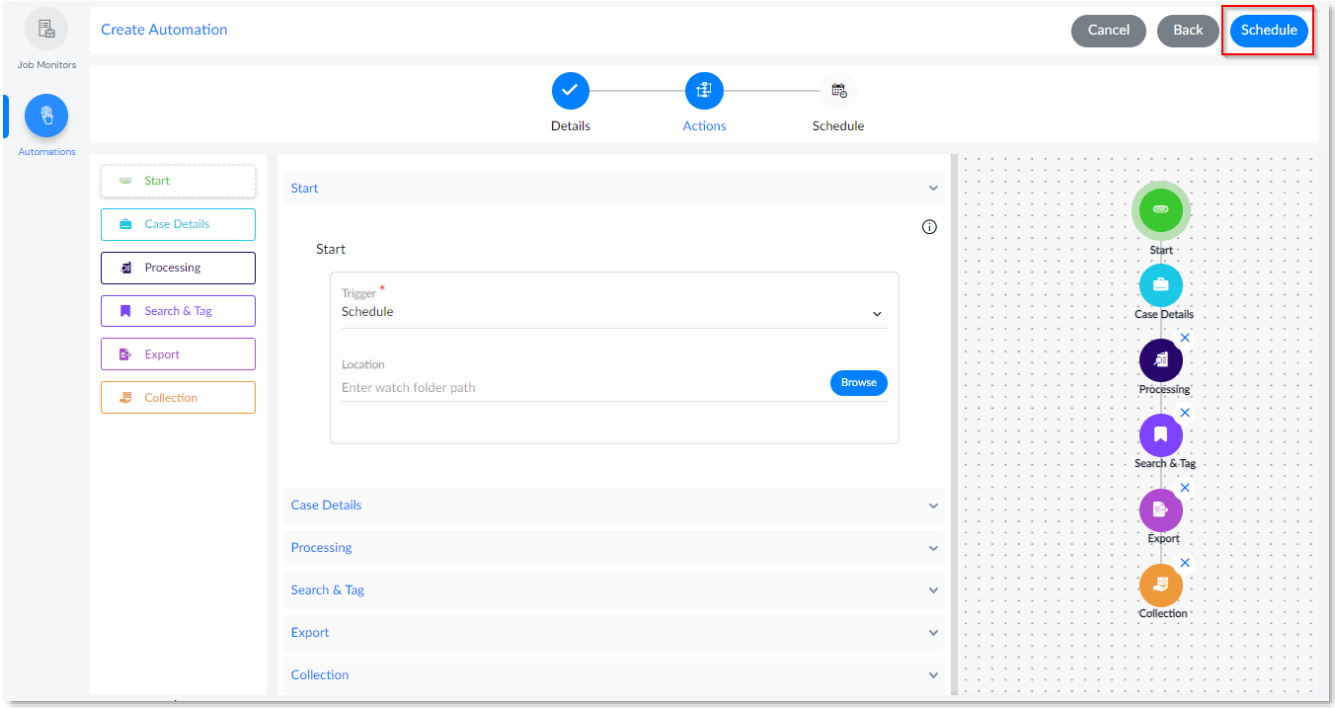
- The Automation Workflows section is displayed.



13. Fill in the required details for the Automation Workflows.

Note: It is mandatory to configure the **Start** and **Case Details** Automation Workflows. Also, you can refer to the **Automation Workflows** section for detailed rules.

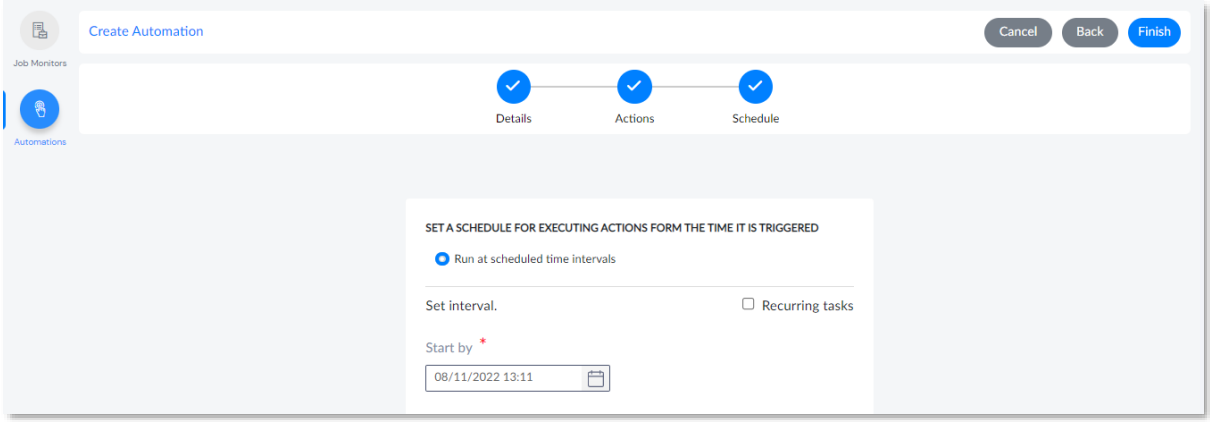
14. Once the Automation Workflows are configured, click **Schedule**.



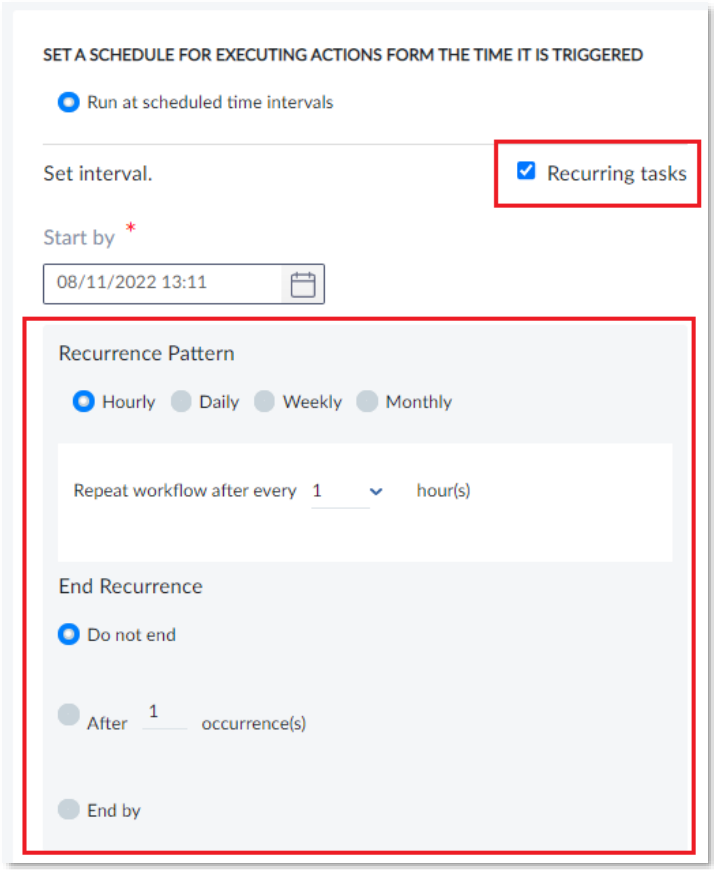
© Exterro, Inc. All rights reserved

15. Set the time intervals, (Date and Time) for the Schedule to be triggered.

Note: The user will be prompted to specify the time interval only for the **Schedule** trigger type. This step can be skipped for rest of the Trigger types (Watch Folder, API Trigger and Manual).

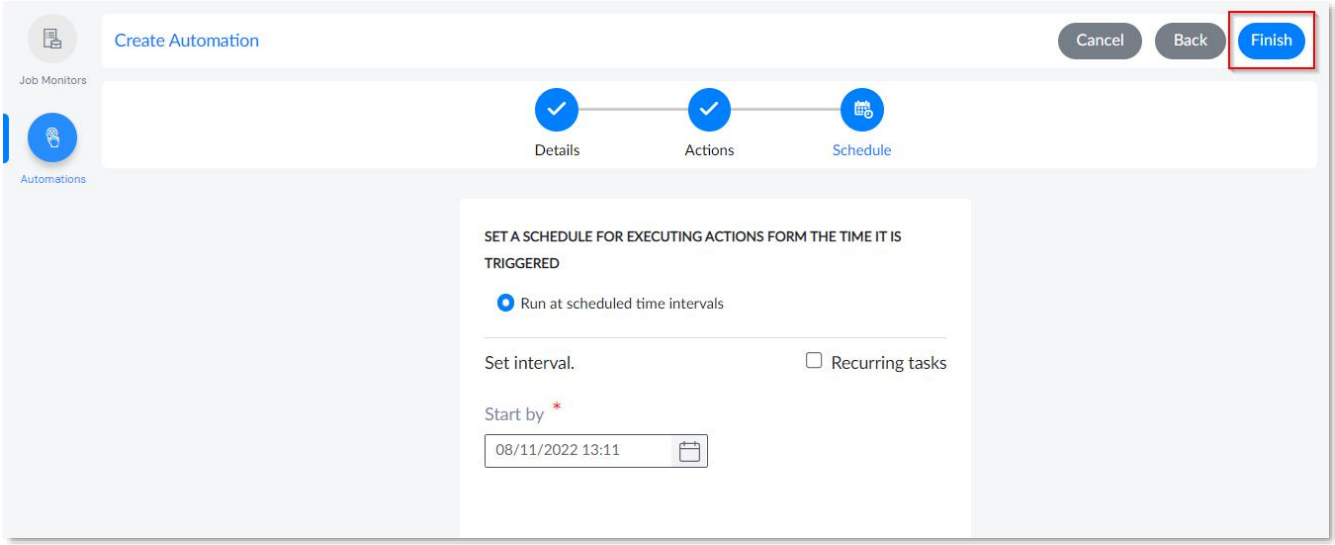


Note: You can also set the Recurring tasks for the Schedule.



© Exterro, Inc. All rights reserved

16. Click **Finish**.



The Automation will be created successfully and listed on the Manage page of Automation.

Note: By default, once the automation is created, it will be in Active status.

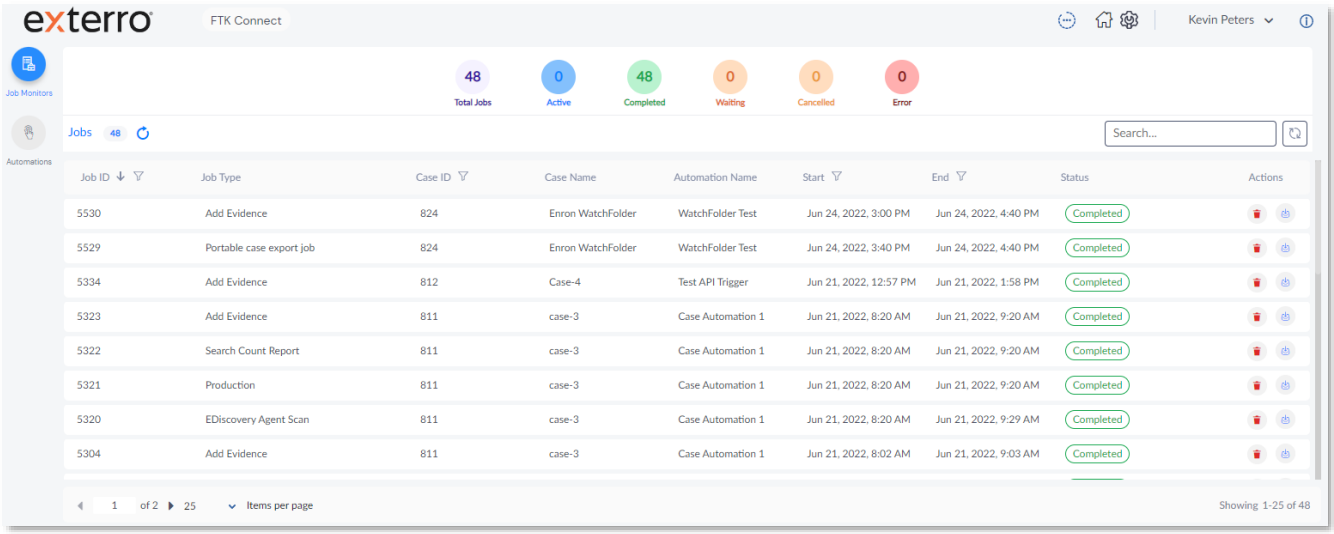
© Exterro, Inc. All rights reserved

Job Monitors

The Job Monitor displays all jobs related to the created automations. You can Delete jobs as well as access automation-specific job logs.

Tip: To filter the automation job list efficiently, you can simply enter a keyword into the search box

located at the top of the automations page and click the search button or press enter.



The Job Monitors page displays the following information:

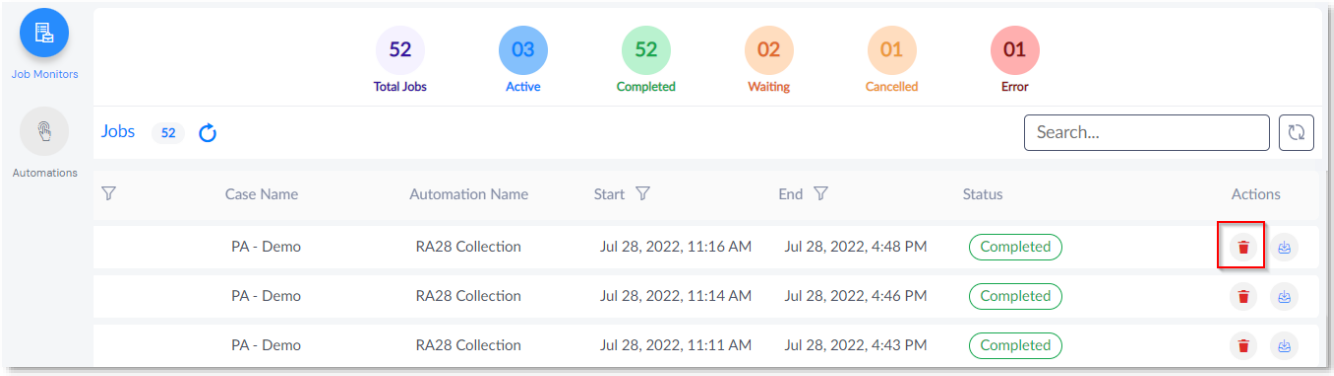
- Live count of Active, completed, waiting, canceled and error jobs are displayed.
- List of any automation-related jobs that are active, waiting, or completed.

© Exterro, Inc. All rights reserved

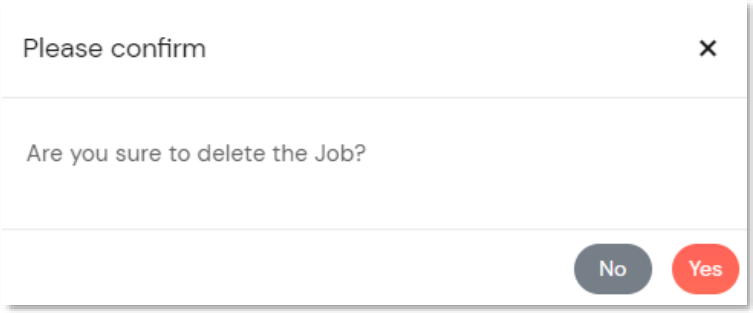
Job log will only retrieve logs related to a specific workflow. It will not list every job across the application.

To delete a Job:

17. Click **Delete** against the job to be deleted.



- A confirmation pop-up is displayed.

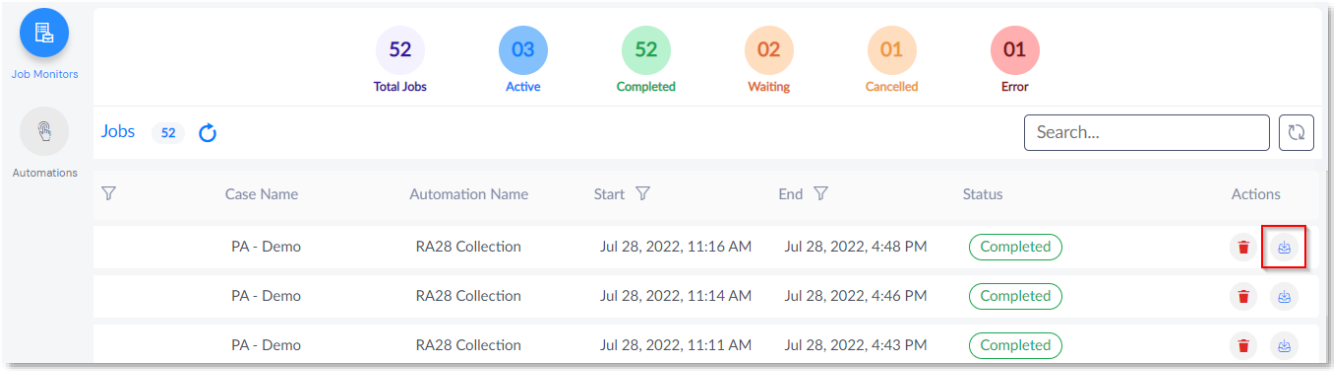


18. Click **Yes**.

© Exterro, Inc. All rights reserved

To download a Job log:

19. Click **Download** against the job.



Limitations/Known Bugs

1 **Watch Folder** - Evidence would be processed only if they are available within 1 sub-folder level. If the evidence is present inside multiple sub-folders, it would not be processed.

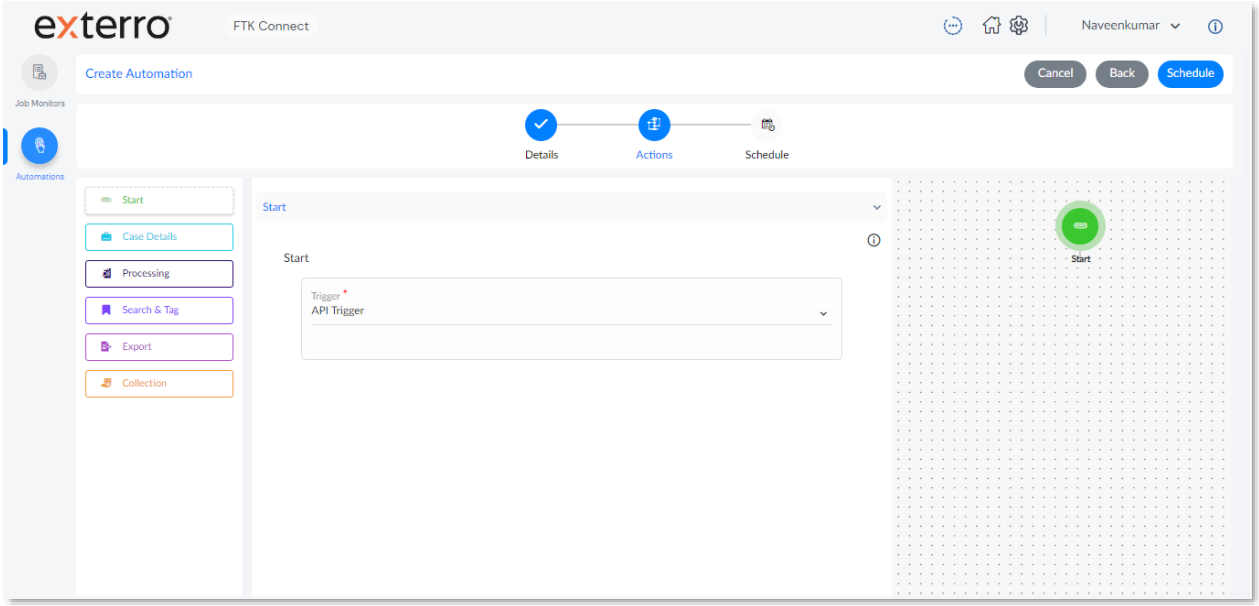
2 **Schedule** - If we create automation based on Schedule trigger option and set the automation to 'Inactive' then still automation would be triggered at the specified time frame unless the automation is deleted.

© Exterro, Inc. All rights reserved

API Trigger Workflow

API Trigger workflow:

1. From the **Create Automation** page,
2. Choose **API Trigger** from the 'Trigger' drop-down (in the Start step and create the automation with the desired steps).



The following sections demonstrate how to trigger the automation with Postman API client tool.

Generating User ID

Send a POST request from the Postman API client to the below URL to generate the User ID

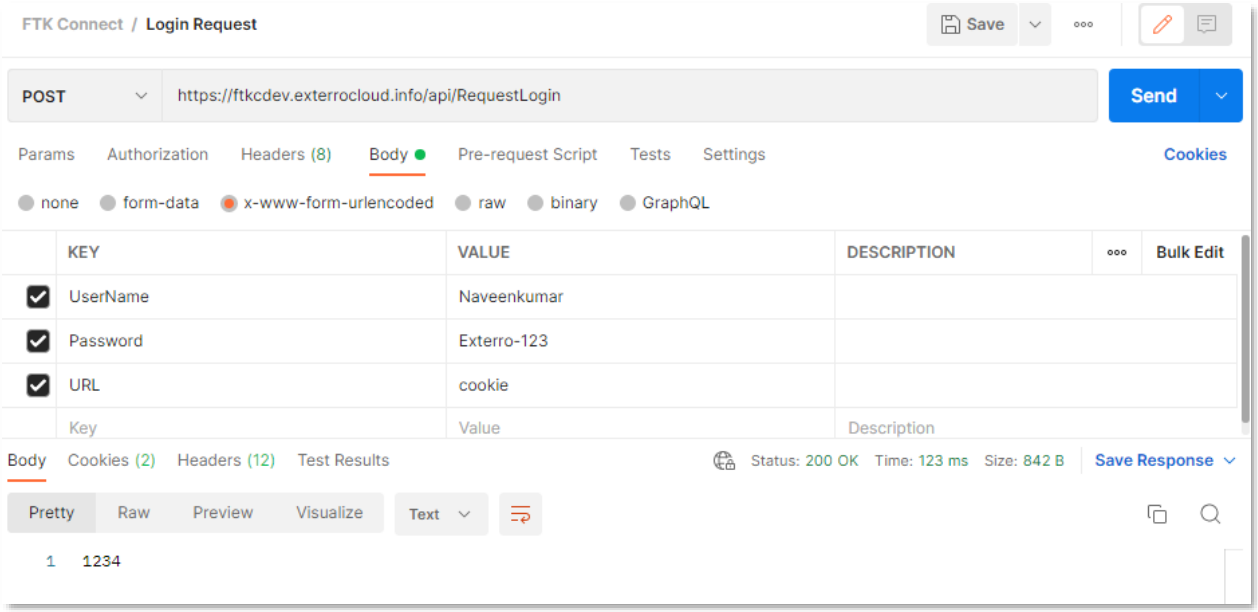
https://<ftkcapp>/api/RequestLogin

The body of the POST request should have the following key value pairs:

Key	Value
UserName	The FTK Central email address of the user for whom the User ID is to be generated.

© Exterro, Inc. All rights reserved

Password	The FTK Central password of the user for whom the User ID is to be generated.
URL	Set the value of URL to “cookie”.



The POST request would fetch the User ID for the provided FTK Central/Connect user in its response body.

Generating Enterprise API Key

The EnterpriseApiKey should be generated using the below URL

```
<ftkcapp>/api/security/<user_id>/getenterpriseapiguid
```

The value of the “user_id” provided here is the value generated from the Generating User ID section.

Sending API Trigger Request

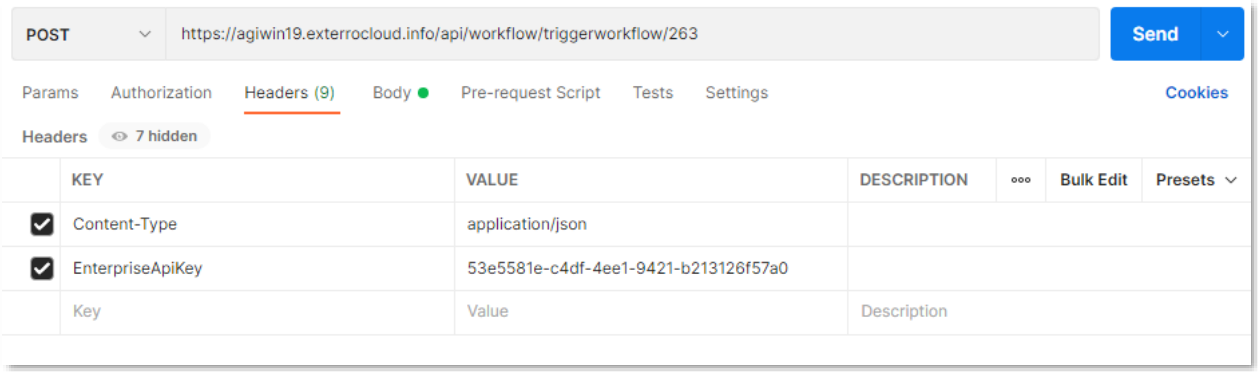
Send a POST request from the Postman API client to the below URL to trigger the automation.

```
https://<ftkcapp>/api/workflow/triggerworkflow/<automation_id>
```

© Exterro, Inc. All rights reserved

The Headers of the request should contain the following key value pairs:

Key	Value
Content-Type	Set the value of Content-Type to “application/json”.
EnterpriseApiKey	Provide the generated EnterpriseApiKey from the Generating Enterprise API Key section.



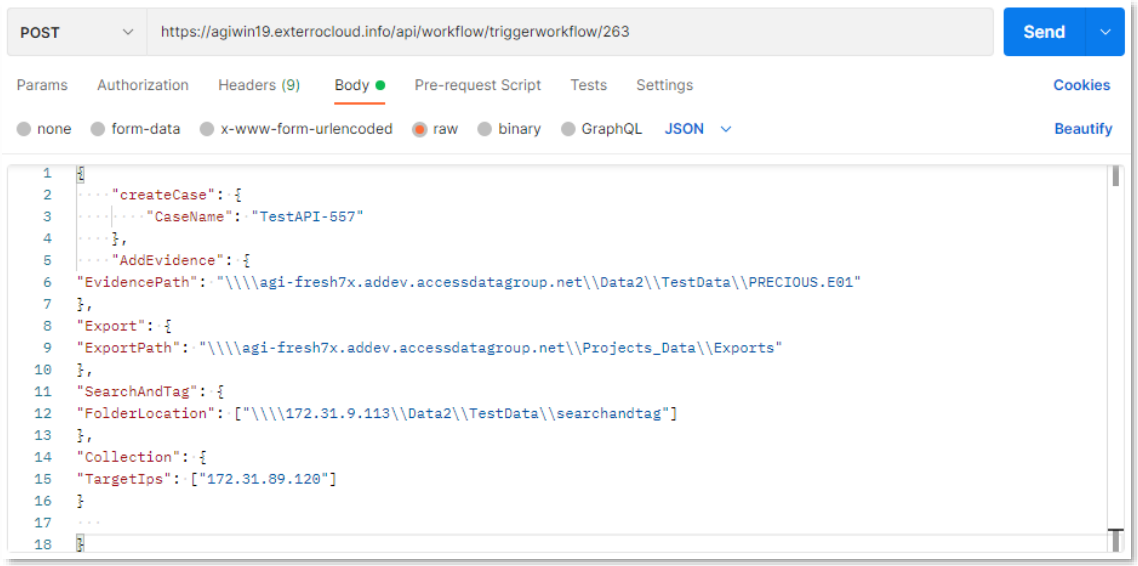
Provide the body of the request in the below format:

```
{

"createCase": {"CaseName": "TestAPI-557"},

"AddEvidence": {"EvidencePath": "\\\\agi-fresh7x.addev.
accessdatagroup.net\\Data2\\TestData\\PRECIOUS.E01"},

"Export": {"ExportPath": "\\\\agi-fresh7x.addev. accessdatagroup.net\\Projects_Data\\Exports"},

"SearchAndTag": {"FolderLocation": ["\\\\172.31.9.113\\Data2\\TestData\\searchandtag"]},

"Collection": {"TargetIps": ["172.31.89.120"]}

}
```

Request	Description
createCase	Applicable for new case creation step.

© Exterro, Inc. All rights reserved

AddEvidence	Applicable for Processing step where the evidence path should be provided.
Export	Applicable for Export step where the export path should be provided.
SearchAndTag	Applicable for Search & Tag step where the location of the search & tag files should be provided.
Collection	Applicable for Collection step where the target IP for collection should be provided.



A successful request would fetch true in its response body and the automation would be triggered.

Sending API Trigger Request without Login Request

If the EnterpriseApiKey for the user is already available and the user is logged into the FTK Connect application, the POST request to the below URL can be directly sent to trigger the automation from the Postman API client with the appropriate headers and body as mentioned in the Sending API Trigger Request section.

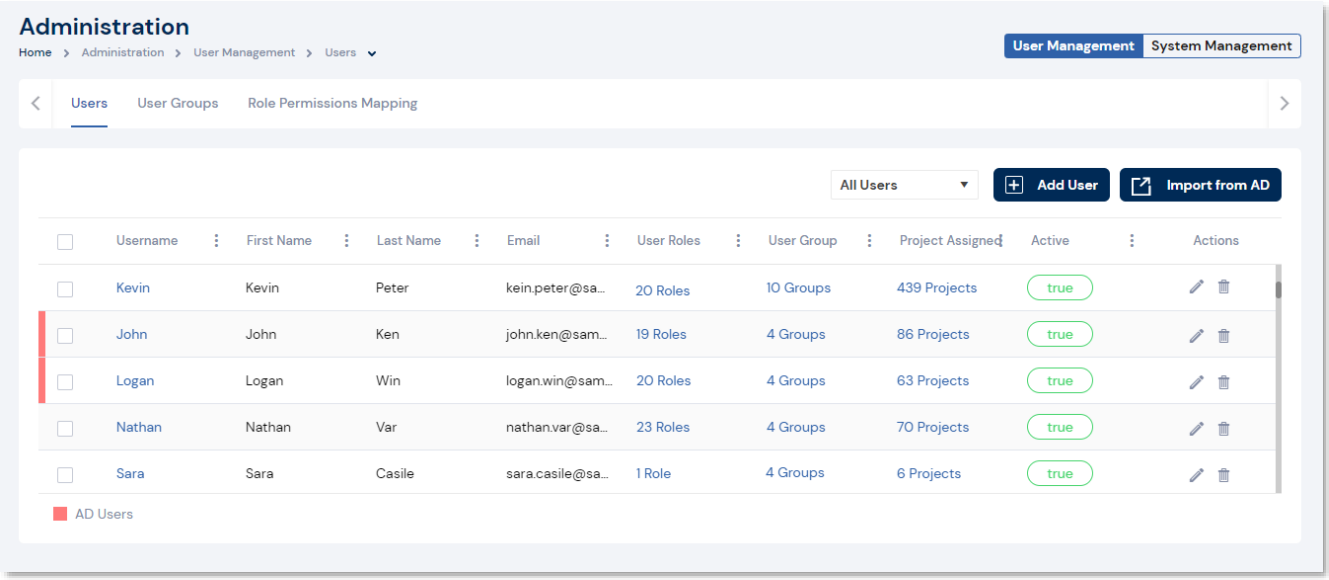
https://<ftkcapp>/api/v2/enterpriseapi/workflow/triggerworkflow/<automation_id>

© Exterro, Inc. All rights reserved

Administrating FTK Central

Administration Portal

Administration Portal allows you to manage Users, User Groups, Permissions and Roles. Additionally, you can configure the System Settings such as the Site Server, agents, mail servers, certificates, and also monitor application health metrics.



Tip: To filter the grid efficiently, you can simply enter a keyword into the search box

located at the top of any grid and click the search button or press enter.

© Exterro, Inc. All rights reserved

User Management

Every user using FTK Central must log in with a user account. Each account has a username and password. Administrators create this user accounts for users and provide appropriate permissions. You can manage users and their groups, permissions, monitor their activity on the application from this page.

Elements of User Management

Users	• Adding Users to application • Importing Users from Active Directory • Activating/Deactivating Users • Editing Users • Deleting Users
User Groups	• Creating User Groups • Editing User Groups • Deleting User Groups
Assigning Roles	• Creating Roles • Assigning Users/User Groups • Editing Roles • Deleting Roles
Case-Level Permission	• Viewing and Assigning Case-Level Permissions

© Exterro, Inc. All rights reserved

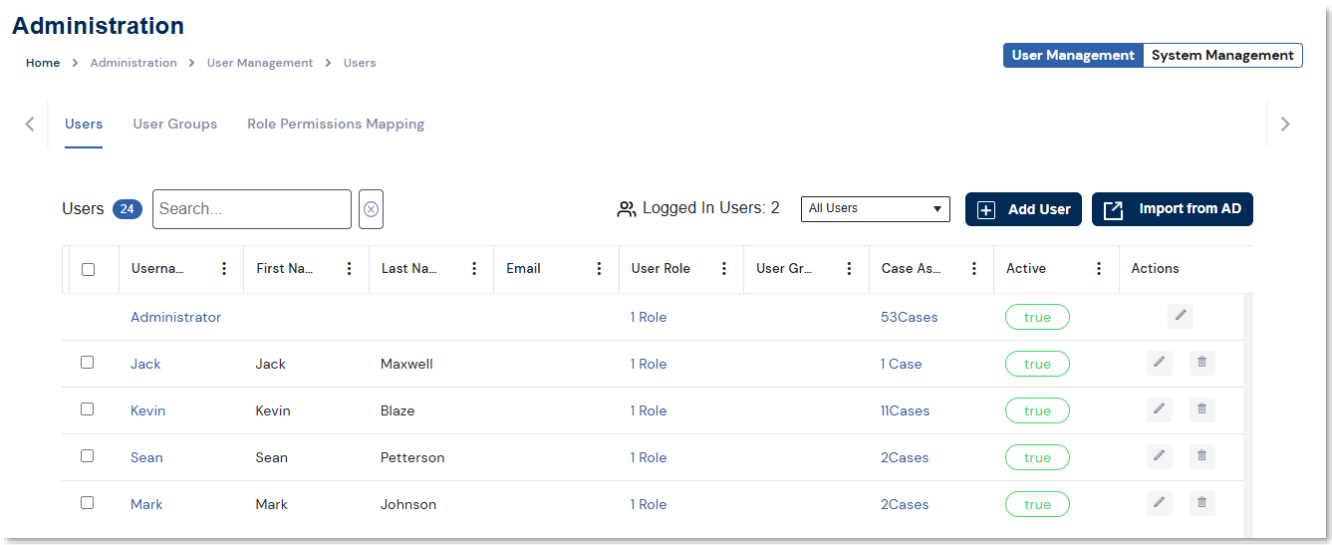
Users

A user is any person who logs in and performs tasks in the FTK Central. You can assign users different with permissions based on the tasks that you want them to perform. The permissions that a user has affects the items that they see and the tasks that they can perform in the application. You assign permissions to a user by configuring roles and then associating users, or groups of users, to those roles.

Adding Users

To add a user:

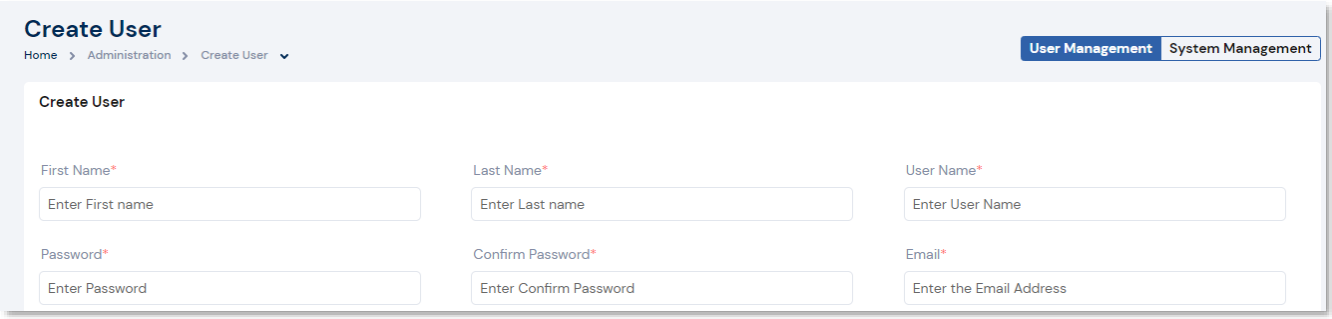
1. From the home page, click **Settings** from the top-right corner.
   - The **Administration** page is displayed.



2. Click **Add User**.

© Exterro, Inc. All rights reserved

- The **Create User** page is displayed.



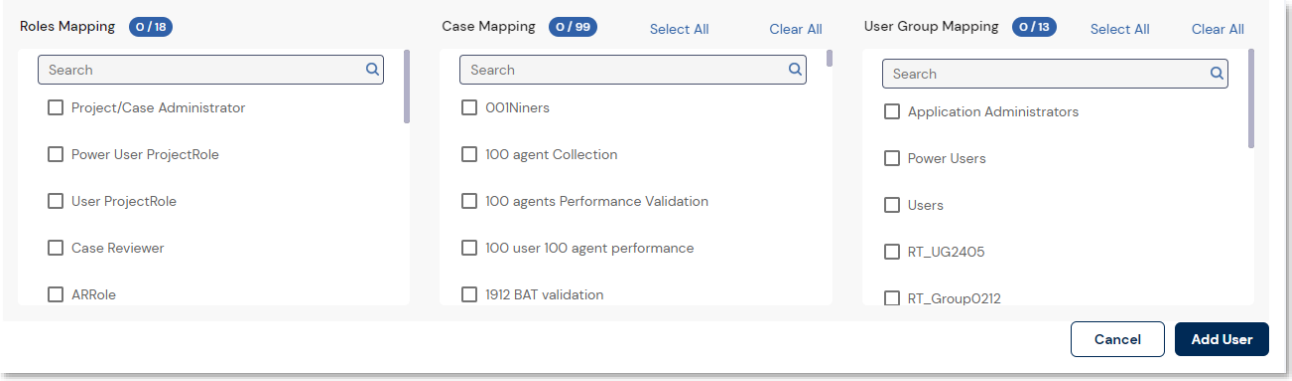
3. Enter the **First Name** of the user.
4. Enter the **Last Name** of the user.
5. Provide a **User Name**.
6. Provide a **Password**.

Warning: The below provided are the **Password** complexity requirements:

- Should contain at least 8 characters.
- Should contain at least 1 uppercase letter.
- Should contain at least 1 number.
- Should contain at least 1 special character.

© Exterro, Inc. All rights reserved

7. Repeat the same in **Confirm Password**.
8. Enter the **Email** address of the user.



9. Select the roles to be associated for the user from **Role Mapping**.
10. Select the cases to be associated for the user from **Case Mapping**.
11. Select the groups for the user to which the user has to be associated from the **Users Group Mapping**.
12. Click **Add User**.

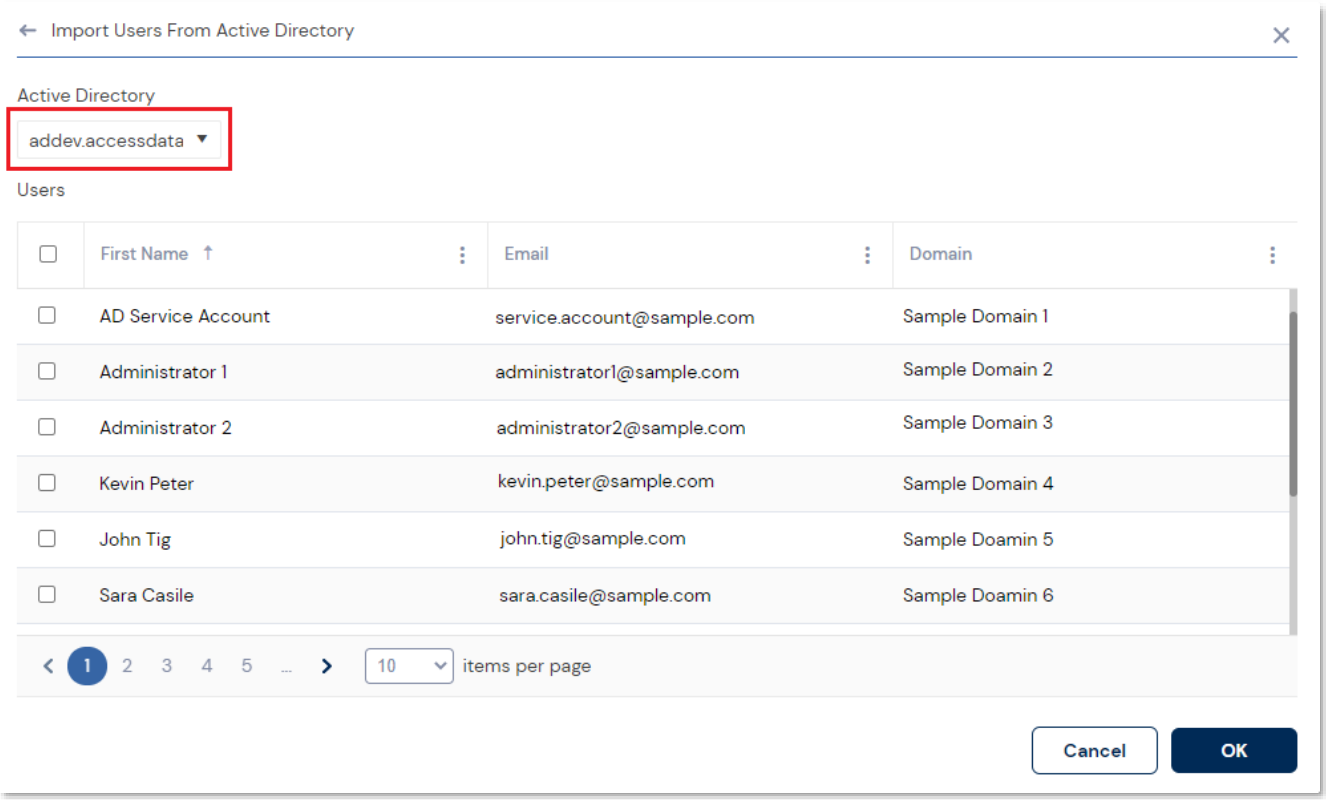
© Exterro, Inc. All rights reserved

Importing Users from Active Directory

Warning: You have to configure Active Directory before proceeding to this section.

To import users from an Active Directory:

1. From the home page, click **Settings** from the top-right corner.
2. Click **Import from AD**.
   - The **Import Users From Active Directory** page is displayed.

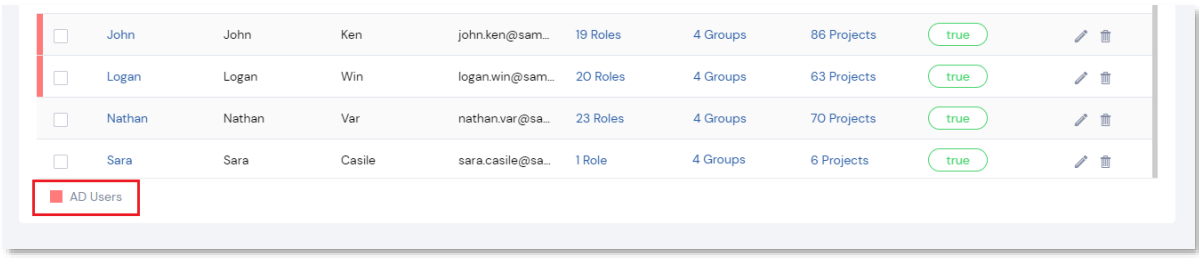


© Exterro, Inc. All rights reserved

3. Select the required **Active Directory** from the drop-down.
4. Enable the checkbox against the users to be imported.
5. Click **OK**.

Notes:

- The imported users from Active Directory will be indicated with **AD Users** against it on the Manage Users page.



- When Active Directory users are deleted, FTK Central will deactivate the corresponding users' account in the application upon resynchronization.

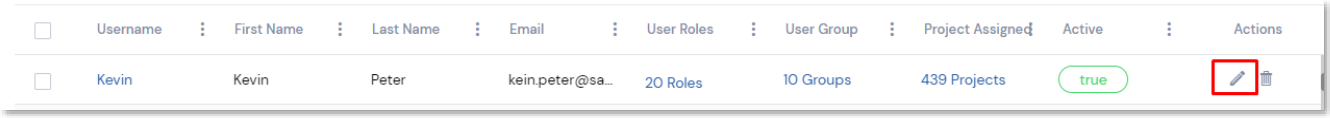
© Exterro, Inc. All rights reserved

Activating/Deactivating Users

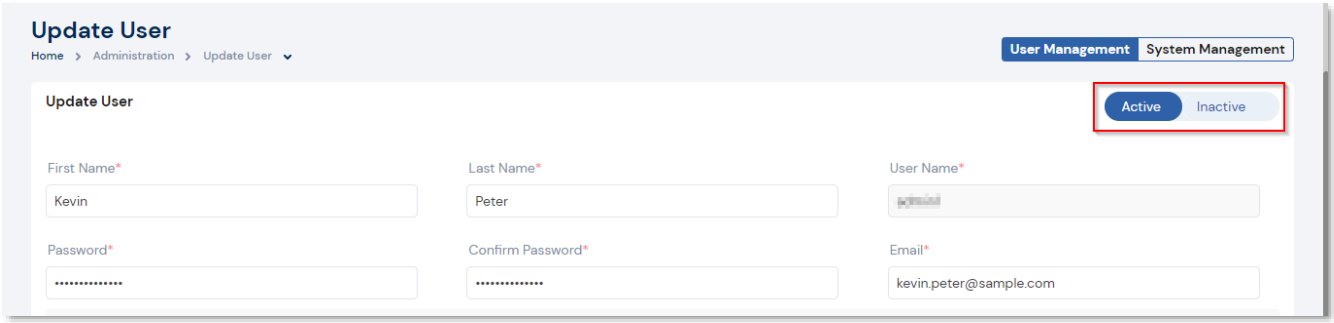
FTK Central allows you to change the status of users to Inactive thereby making them unable to use the application. By default, all users are created in Active status, however you can change the status to Active or Inactive whenever required.

To activate/deactivate a user:

1. From the home page, click **Settings** from the top-right corner.
2. Click **Edit** against the user to be edited.



- The **Update User** page is displayed.



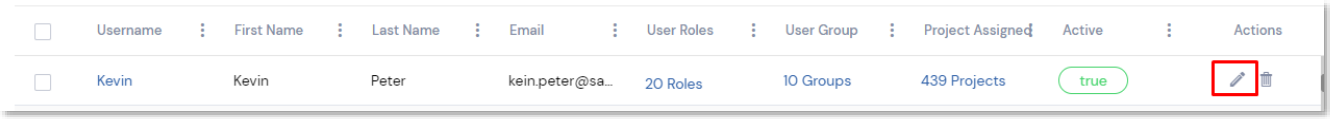
3. Toggle to set the user as **Active** or **Inactive**.
4. Click **Update.**

© Exterro, Inc. All rights reserved

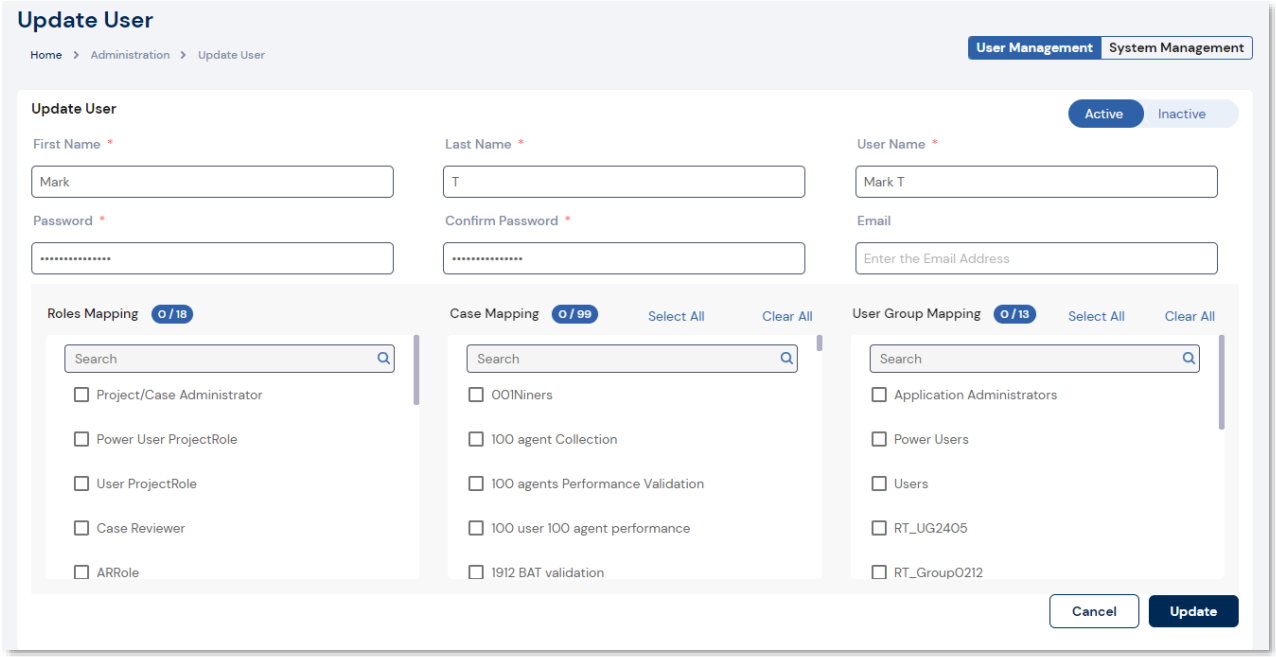
Editing Users

To edit a user:

1. From the home page, click **Settings** from the top-right corner.
2. Click **Edit** against the user to be edited.



- The **Update User** page is displayed.



3. Make the necessary changes.

Warning: You can edit the Username only for the non-admin users and cannot be edited for the admin users.

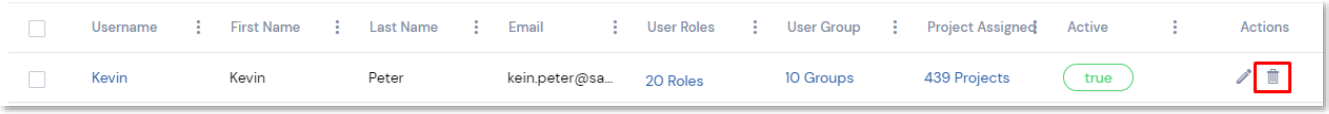
4. Click **Update.**

© Exterro, Inc. All rights reserved

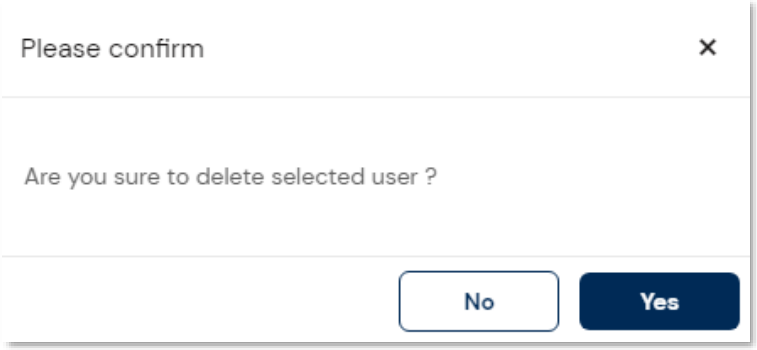
Deleting Users

To delete a user:

1. From the home page, click **Settings** from the top-right corner.
2. Click **Delete** against the user to be deleted.



- The **Please confirm** pop-up is displayed.



3. Click **Yes**.

© Exterro, Inc. All rights reserved

User Groups Management

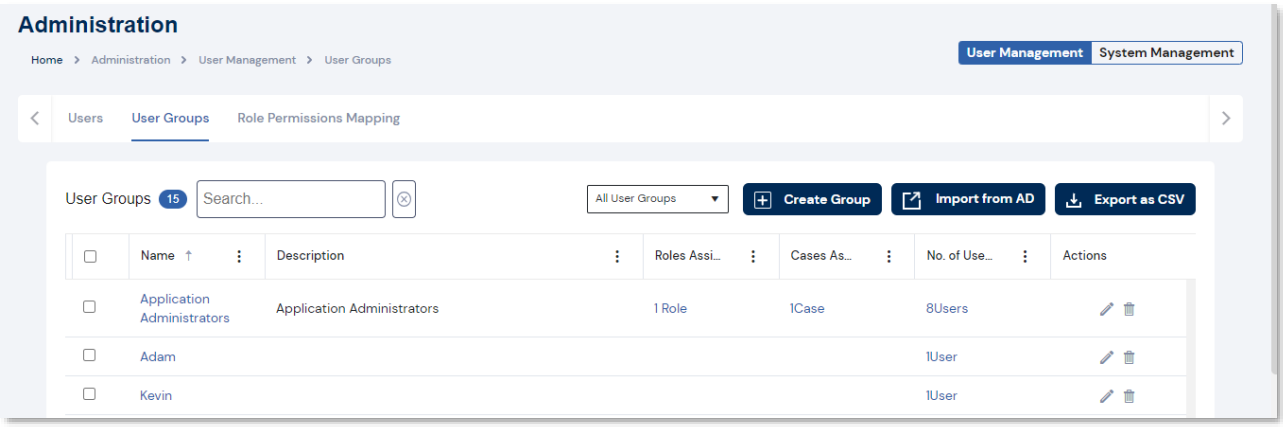
User Groups allow you to consolidate the set of users who perform the same tasks. Categorizing users into groups makes it easier to assign and manage case permissions for users. Grouping helps you assign permissions to a set of users reviewing the same case at once. You can group users of different roles into one User Group.

Note: You can export the list of user groups from this page by clicking on the **Export As CSV** button.

Creating User Groups

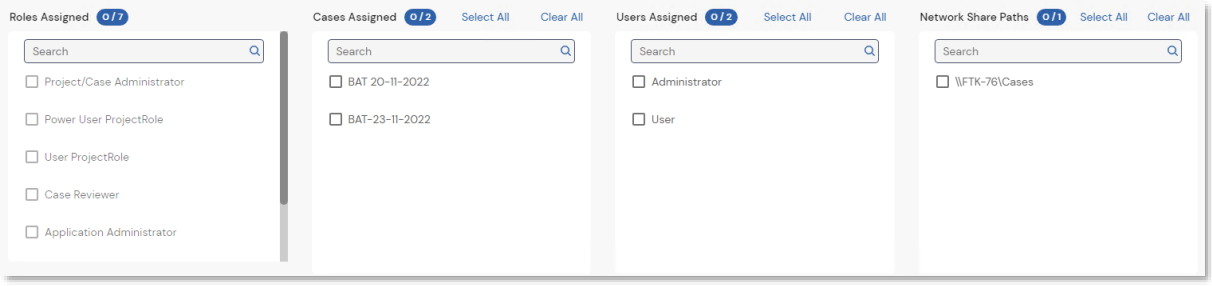
To create a user group:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **User Groups** tab.



© Exterro, Inc. All rights reserved

3. Click **Create Group**.
   - The **Create Group** page is displayed.



4. Provide a name for the group in **Group Name**.
5. Provide a **Description** for the group.

6. Select the roles required for the group from **Roles Assigned**.

Note: You can read what is a Role and how is it helpful from the Roles section, later in the document.

7. Select the users required for the group from **Users Assigned**.
8. Select the network share paths for the group from **Network Share Paths**.

Warning: Non-Administrator users are only allowed to access the **Network Share Paths** assigned to them.

9. Select the cases (case) to be associated for the group from **Cases Assigned**.

Warning: Assigning a user to specific cases will prevent the user accessing other cases.

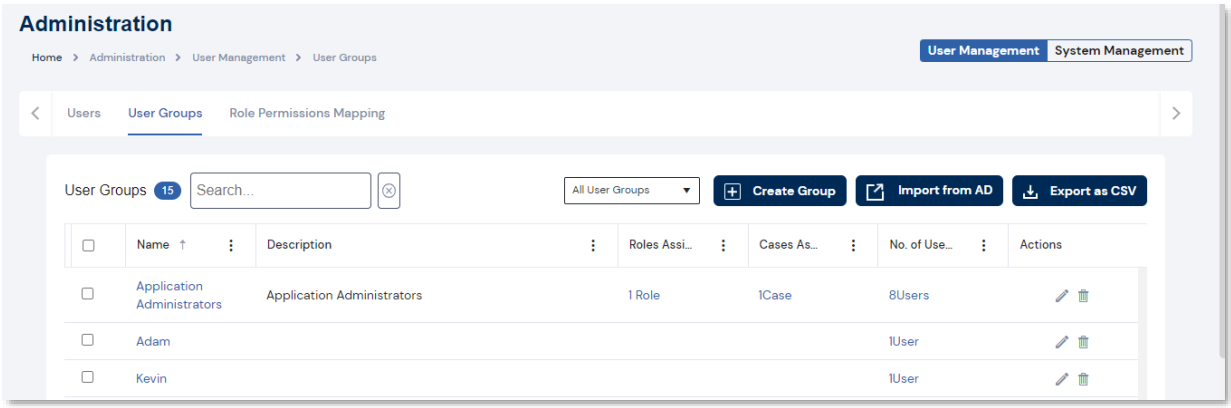
10. Click **Create Group**.

© Exterro, Inc. All rights reserved

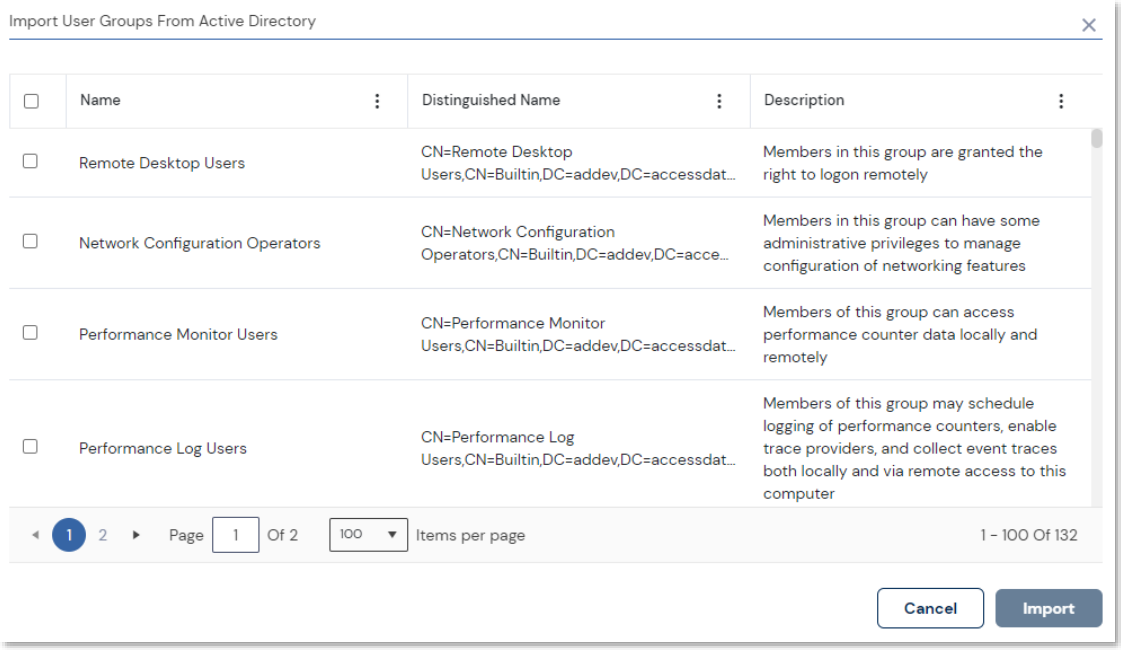
Importing User Groups from Active Directory

To import user groups from active directory:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **User Groups** tab.



3. Click on the **Import from AD** button.
   - The **Import User Groups From Active Directory** pop-up is displayed.



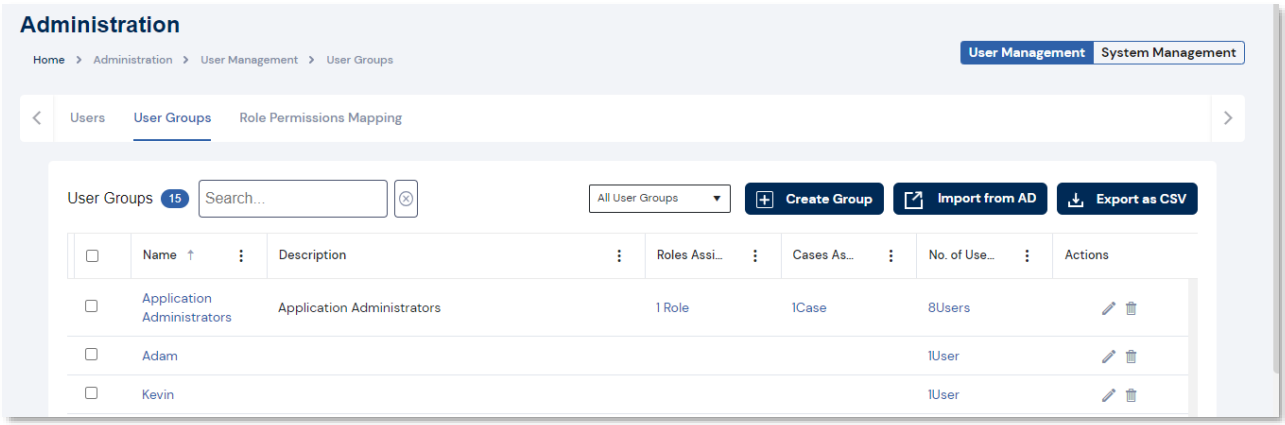
4. Select the required active directories from the pop-up and click **Import**.

© Exterro, Inc. All rights reserved

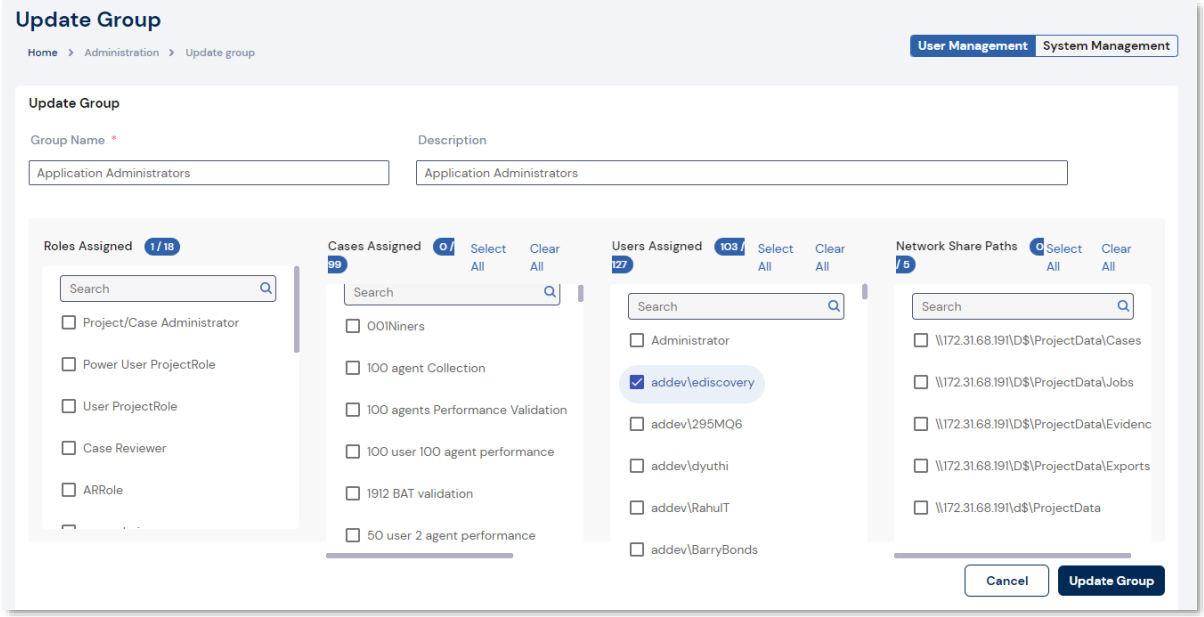
Editing User Groups

To edit a user group:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **User Groups** tab.



3. Click on the user group to be edited.
4. Click **Edit**.



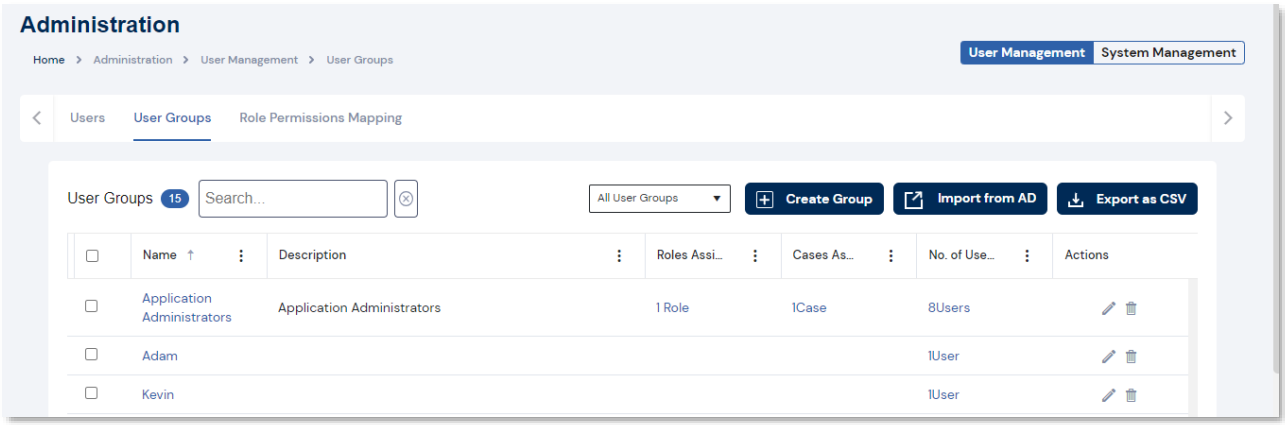
5. Make the necessary changes.
6. Click **Update Group**.

© Exterro, Inc. All rights reserved

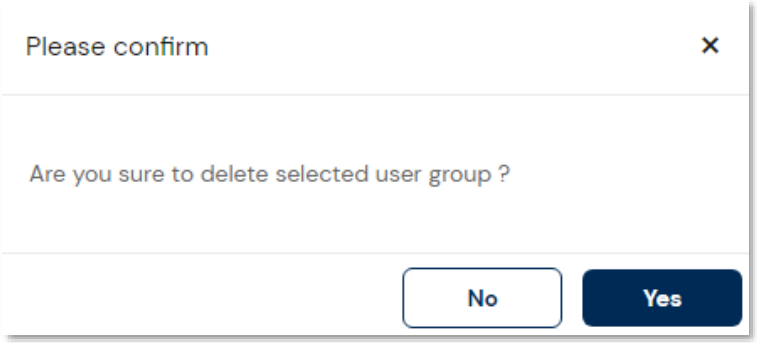
Deleting User Groups

To delete a user group:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **User Groups** tab.



3. Click **Delete** against the user group to be deleted.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

© Exterro, Inc. All rights reserved

Assigning Roles

A Role is a combination of various permissions required for a user to perform the actions intended. You can assign different permissions to different roles, based on the tasks that you want them to perform. The permissions determine what a user sees and the actions the user performs on the application. Moreover, the cases and options that the users of a particular role see on the application is determined by the permissions enabled for the user/user group.

FTK Central provides the following three default Roles:

- Administrator - To manage the whole application. Users in this role will be provided with all the permissions to manage the application.
- Power User - To aid in managing the application. Users in this role will be provided with permissions to create, edit, manage users, and user groups.
- Users - To only reviews files in a case. This role grants the user permissions for create/edit cases and files in it.

Note: Only the users with 'System Management' permission will be able to access the System Management Settings.

However, you can create any number of additional role types with combination of the any of the following permissions as required by your organization:

Permission Group	Definition
General Management	
User Management	Create, delete and edit users.
Create Custodians	Create custodians.
Delete Custodians	Delete custodians
Manage Data Sources	Create, delete and edit data sources.

© Exterro, Inc. All rights reserved

Permission Group	Definition
Activity Log Access	View activity log within FTK Central.
Manage Templates	Edit role templates.
Assign Users to a Case	Required with User Management permission and vice versa to assign users to a case.
Database Management	Add additional databases.
Edit Case Auditing	To access the **Case Auditing** feature in the Case Summary page
Case/Project Admin	
Case/Project Admin	Full rights to all functionality on a case-level basis.
Case	
Create/Edit Case	Create and edit cases.
Delete Case	Delete cases.
View Case Jobs	View case jobs in the job status menu.
Manage Case Custodians	Add and remove custodians within Case Summary.
Add/Edit Evidence	Add or edit the evidence of a case.
Delete Evidence	Delete the evidence of a case.
Backup/Restore Cases	Backup cases from the case list context menu.
Restore Cases from Backup/Restore	Restore cases from the case list context menu.
Create Case Dashboards	Create and edit case dashboards.
Assign Users to a Case	Assign users to a case during case creation.
Re-Index Case	Re-indexing the files of a case.

© Exterro, Inc. All rights reserved

Permission Group	Definition
Exports	
Create Export	Create exports using the export wizard.
Delete Export	Delete created exports.
Export Item Grid	Export records within the grid.
Search & Review	
View Files List	View the review grid.
View Natives	View files in the viewer in native format.
View Text	View files in the viewer as text.
View Coding Panel	View coding panel within review.
Edit Documents	Edit documents within review.
Manage Tags	Create and rename tags within the Tags menu.
Delete Tags	Delete tags within the Tags menu.
Manage Tag Permissions	Assign permissions for tag values.
View Tags	View tags within the Tags menu.
Assign Tags	Assign tags to a document.
View Privileged Documents	View flagged privileged documents.
View Ignored Documents	View flagged ignored documents.
Flag Document as Privileged	Flag documents as privileged within the context menu.
Flag Document as Ignored	Flag documents as ignorable within the context menu.

© Exterro, Inc. All rights reserved

Permission Group	Definition
Manage Review Sets	Create and edit review sets within Batch Administration.
Delete Review Sets	Delete batches within review sets within Batch Administration.
View Review Sets	View review sets and batches within Batch Administration.
Run Searches	Run searches in review mode.
Save Searches	Save searches that a user assigned with this permission makes.
Bulk Imaging	Bulk image documents using the context menu.
Download Files	Download files within review mode.
View Annotations	View annotations in native, image and text view within review mode.
Add Annotations	Add annotations within review mode but cannot view them unless assigned view permissions.
Delete Annotations	Delete annotations within review mode.
View Document History	View document history in the object attributes menu within review mode.
Manage Profiles	Create and edit profiles.
View Save global search	Configuring the Case Permission for a Saved Search (whether to display the search for all cases or just one case).
Litigation Hold	
Approve Lit Holds	Approve configured litigation holds.
Manage Lit Holds	Manage litigation holds, including creating, viewing and deleting Litigation Holds.
View Lit Holds	View Litigation Holds.
Reports	

© Exterro, Inc. All rights reserved

Permission Group	Definition
View Data Report	View and create Processing Report types in the Reports wizard.
View Audit Report	View and create Event Report types in the Reports wizard.
Evidence Collection	
Approve Collection Jobs	Approve collection jobs form the collections tab.
Create Collection Jobs	Create collection jobs from the Collections tab.
Delete Collection Jobs	Delete collections from the Collections tab.
Execute Collection Jobs	Execute collection jobs from the Collections tab.
Initiate Processing	Process files form a collection job.
FTK Connect	
Add/Edit Automations	Create and edit automations in FTK Connect.
Delete Automations	Delete any automation created in FTK Connect.
DPM DPE	
View DPM DPE	To view the DPM and DPE details in the Monitor DPM DPE section and DPM DPE Configuration section of System Management.
Edit DPM DPE	To activate/deactivate and delete the DPE in the DPM DPE Configuration section of System Management
AWS S3 Management	
Manage S3 Buckets	To create and manage the AWS S3 bucket (via AWS S3 Management section)
Upload Files/Folders	Upload files and folders into the AWS S3 bucket (via AWS S3 Management section)
Delete Files/Folders	Delete files and folders from the AWS S3 bucket (via AWS S3 Management section)

© Exterro, Inc. All rights reserved

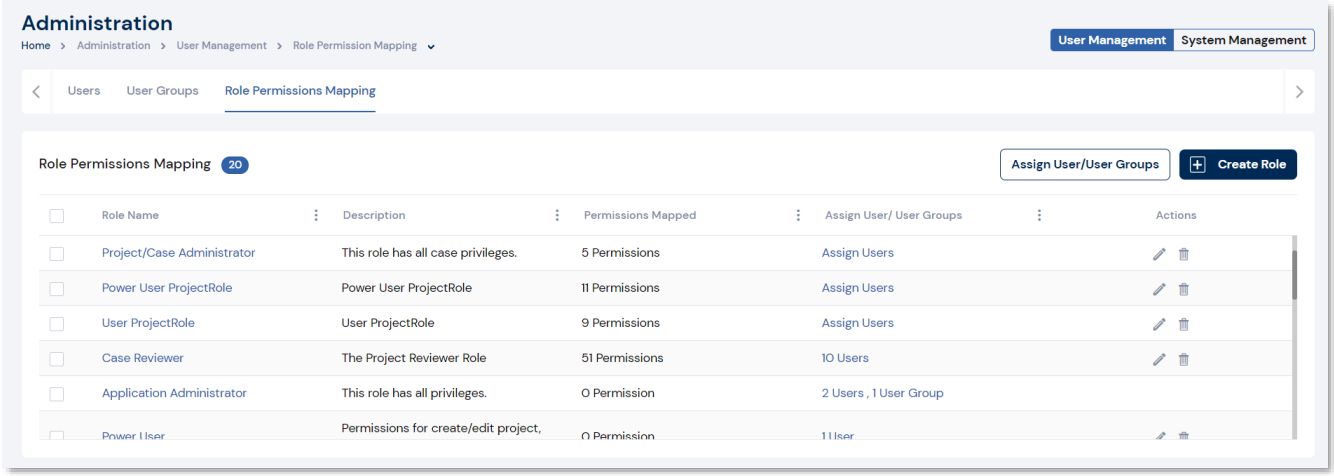
Permission Group	Definition
Download Files/Folders	Download files and folders from the AWS S3 bucket (via AWS S3 Management section)

© Exterro, Inc. All rights reserved

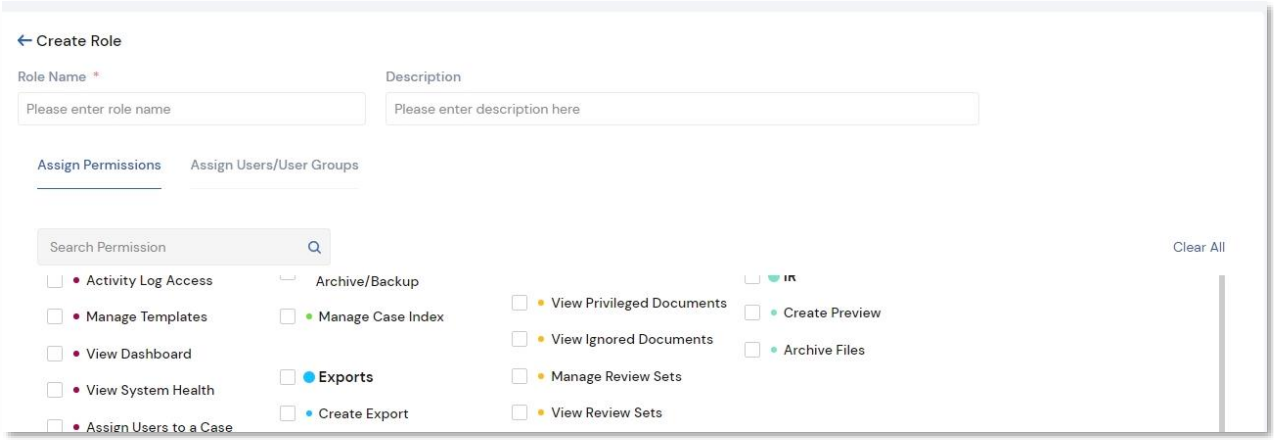
Creating Roles

To create a role:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **Roles Permissions Mapping** tab.



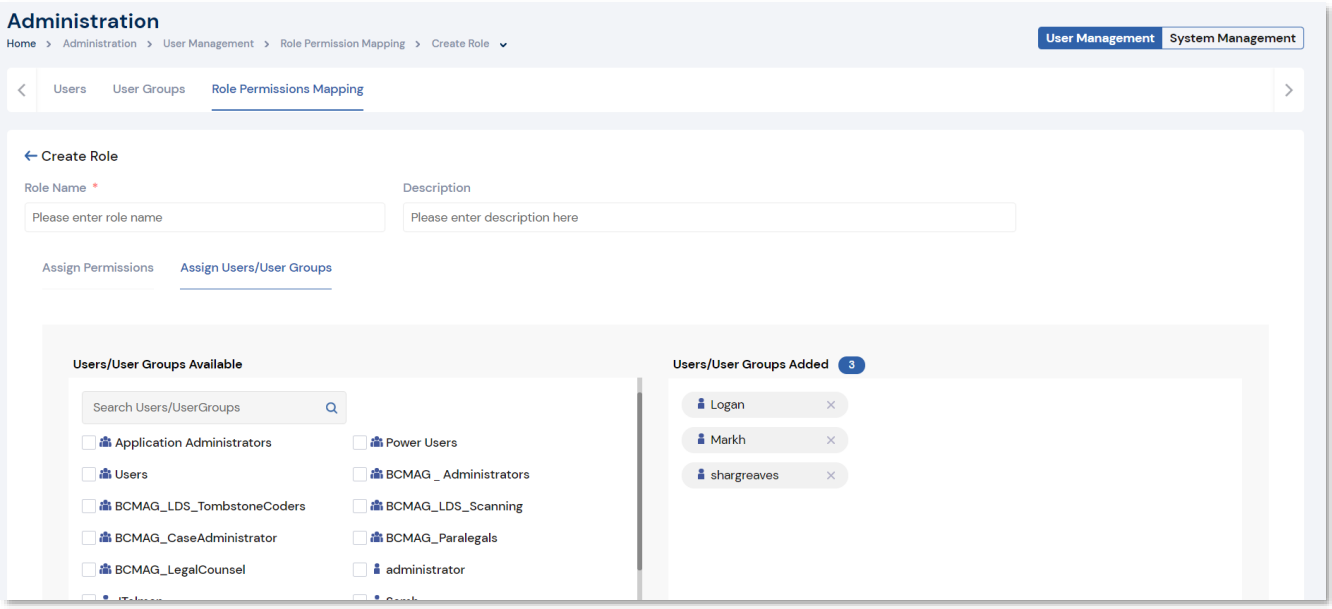
3. Click **Create Role**.
   - The **Create Role** page is displayed.



4. Provide a name for the role in **Role Name**.
5. Provide a **Description** for the role.
6. Enable the required permissions.
7. Navigate to **Assign Users/User Groups**.

© Exterro, Inc. All rights reserved

8. Select the required Users and User groups.
   - The selected users and user groups will be displayed in the right-pane.



9. Click **Create Role**.

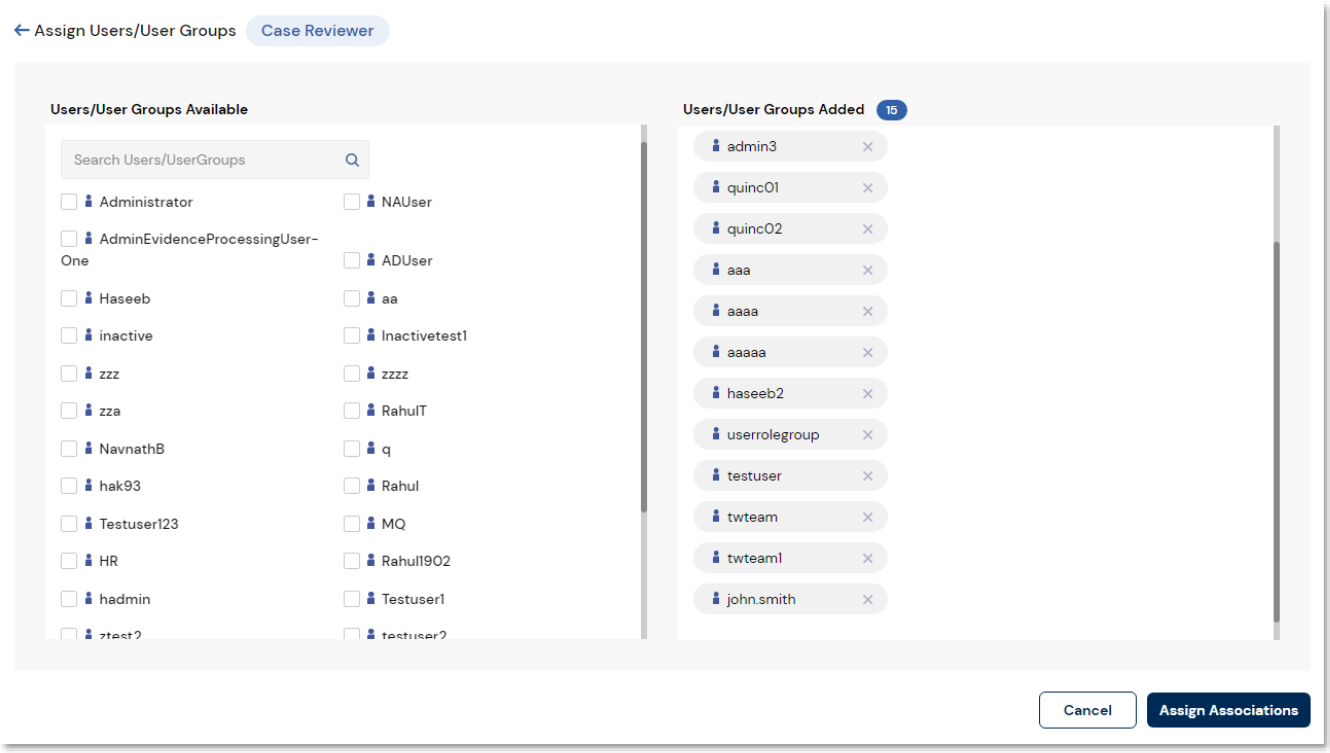
© Exterro, Inc. All rights reserved

Assigning Users/Users Groups

You can assign a role to multiple users and user groups at once using this option.

To assign roles for users and user groups:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **Roles Permissions Mapping** tab.
3. Select the required roles for which the users or user groups is to be assigned.
4. Click **Assign User/User Groups**.
    - The **Assign Users/User Groups** page is displayed.



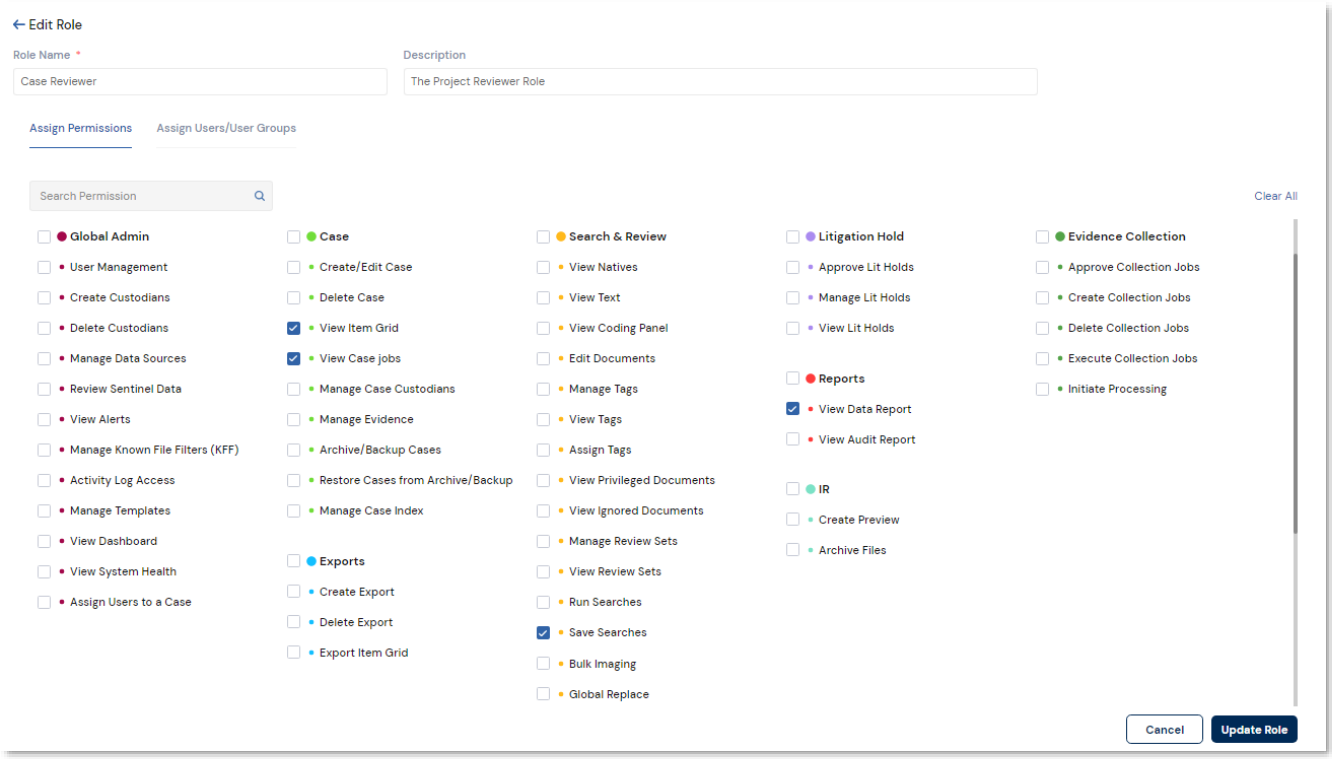
5. Select the required users or user groups.
6. Click **Assign Associations**.

© Exterro, Inc. All rights reserved

Editing Roles

To edit a role:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **Roles Permissions Mapping** tab.
3. Click **Edit** against the role name to be edited.
   - The **Assign Permissions** tab of the **Edit Role** page is displayed.



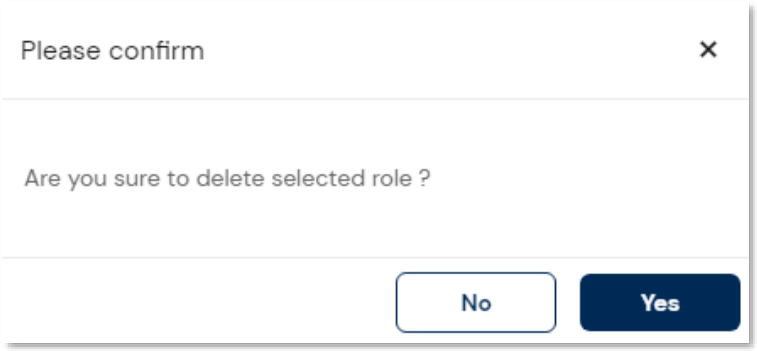
4. Make the necessary changes.
5. Click **Update Role**.

© Exterro, Inc. All rights reserved

Deleting Roles

To delete a role:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **Roles Permissions Mapping** tab.
3. Click **Delete** against the role to be deleted.
   - The **Please confirm** pop-up is displayed.



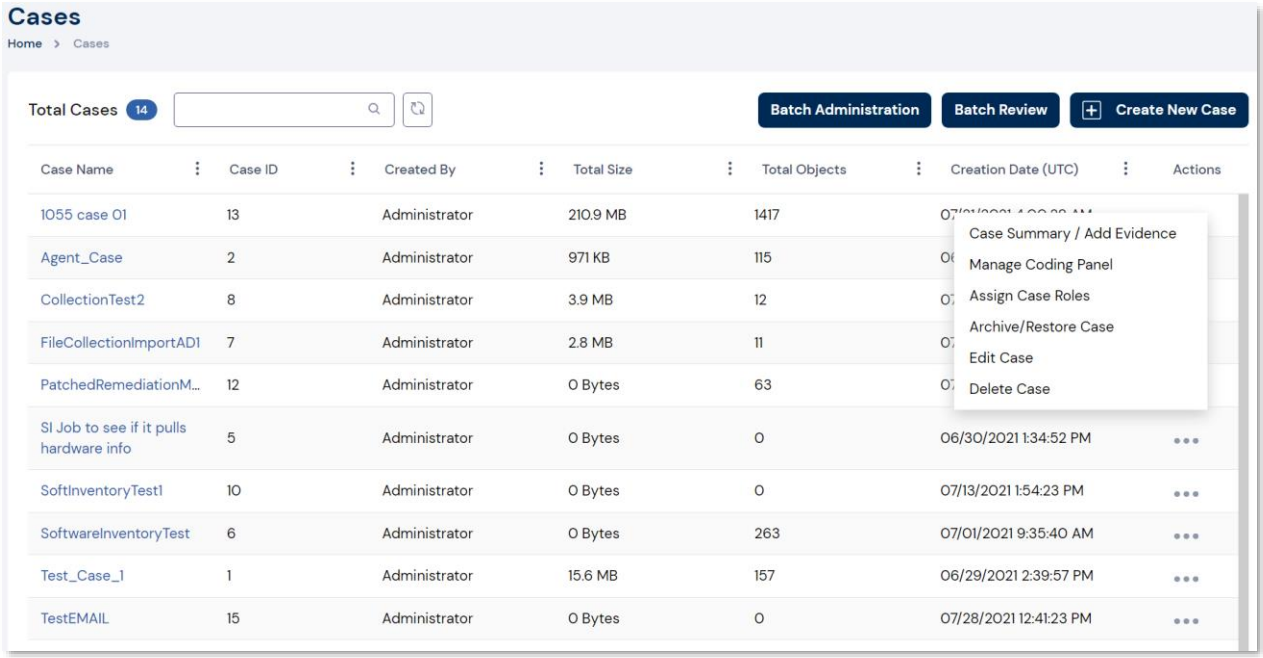
4. Click **Yes**.

© Exterro, Inc. All rights reserved

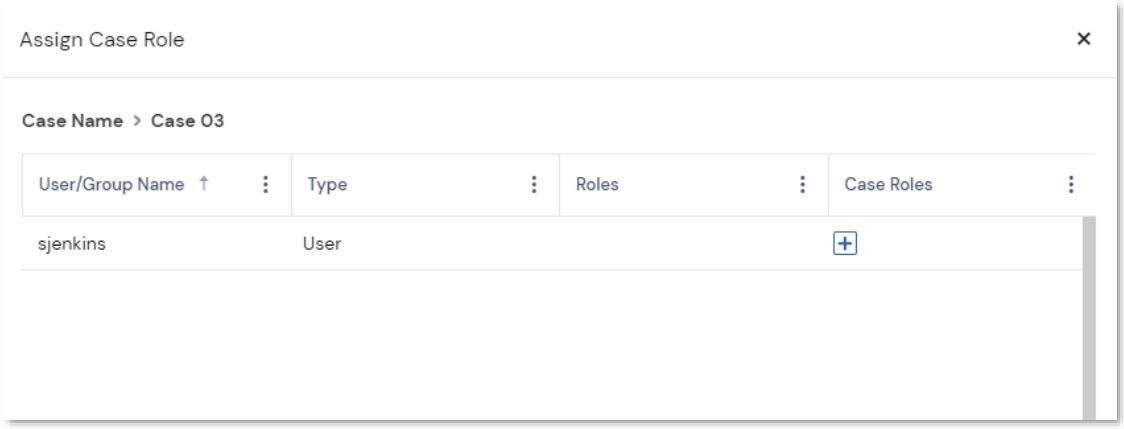
Viewing and Assigning Case-Level Permissions

To view the case-level permission (context menu) and assign roles:

1. From the home page, click **Case List**.

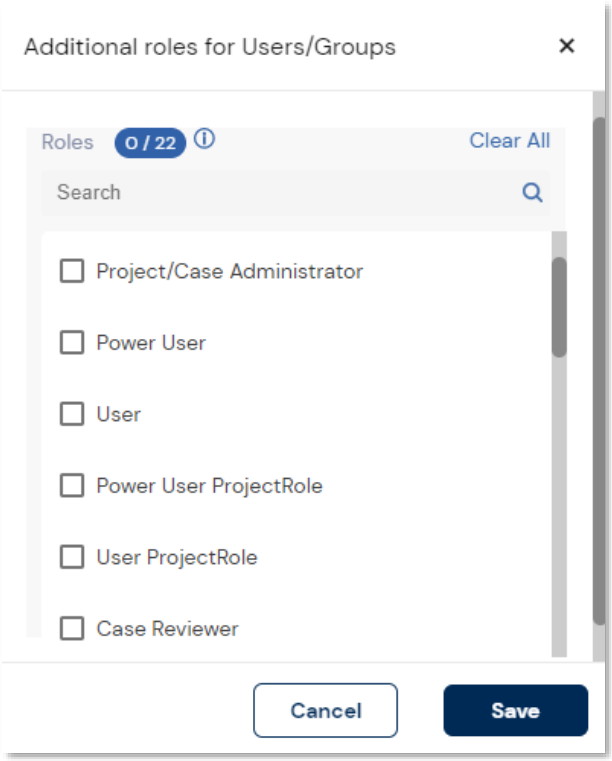


2. Click the **Context menu** against the required case.
3. Click **Assign Case Roles**.
   - The **Assign Case Role** prompt is displayed.



© Exterro, Inc. All rights reserved

4. Click on the **Assign Case Roles** button against the required user/group name.
   - The **Additional roles for User/Groups** prompt is displayed.



5. Check the applicable roles and click **Save**.

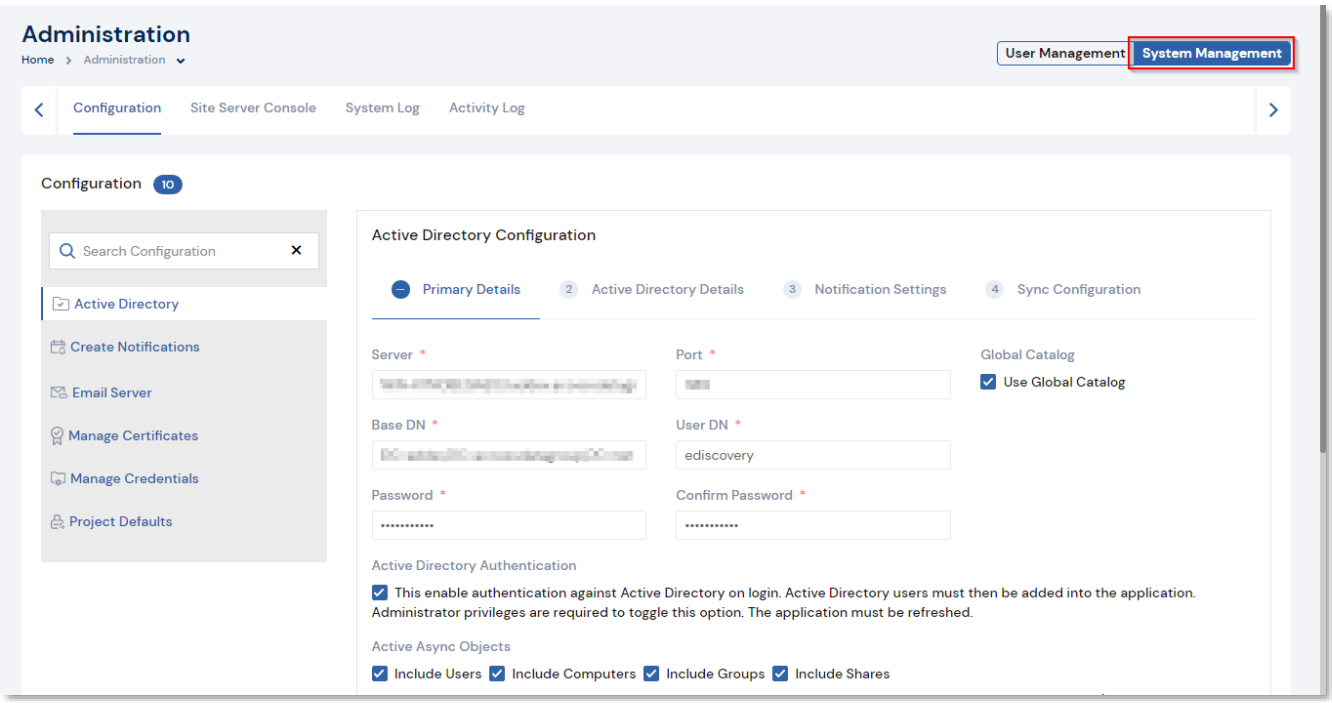
Note: Roles that are disabled for selection are already assigned to a user at a global-level.

© Exterro, Inc. All rights reserved

System Management

System management within the Administration Portal allows you to configure numerous options ranging from general application configuration, Site Server Console, email servers, agents, certificates, credentials, default options, health metrics, etc. These are global settings that affect the entire system.

Note: Only the users with 'System Management' permission will be able to access the System Management Settings.



© Exterro, Inc. All rights reserved

Elements of System Management

Configurations	• Active Directory Configuration • Notifications • Email Server
Manage Certificates	• EFS Certificates • Notes Certificates • AD1 Certificates
Manage Credentials	• Redirected Acquisition • Share Credentials • Agent Credentials
Case Defaults	• Case Defaults • Creating Redaction Reasons • Creating Custom Columns
Site Server Console	• Status • Configuration • Phone Home Settings • Agent Installer • Health Metrics • Jobs
System Log	• Viewing System Log
Activity Log	• Viewing Activity Log
Job Management	• To Map Jobs to a specific server

© Exterro, Inc. All rights reserved

Configurations

Active Directory Configuration

This section allows you to configure Active Directory to synchronize and import users. After performing an initial sync, you can sync on a recurring schedule. You can also select to import one or more types of objects, such as Users and Groups. When the Active Directory is synchronized, users are imported and synchronization only occurs from Active directory to the application. It is to be noted that the changes are not synced only from the active directory to the application and not vice versa.

You can also configure the system to send an email notification when a value in Active Directory is changed and synced. This can be helpful when you have a custodian in a Litigation Hold and the status of that user changes. For example, they may move locations or may no longer be employed. You configure the email notifications as part of the Active Directory sync setting. The notification email contains a time stamp, the name of the user that the change occurred for, the properties that changed, and the old and new values of the changed properties

When a user is deleted in active directory, the person is not deleted in FTK Central. Instead, the person is flagged as Deleted from Active Directory and still appears as a custodian. Data that is associated with the custodian is not impacted in any way.

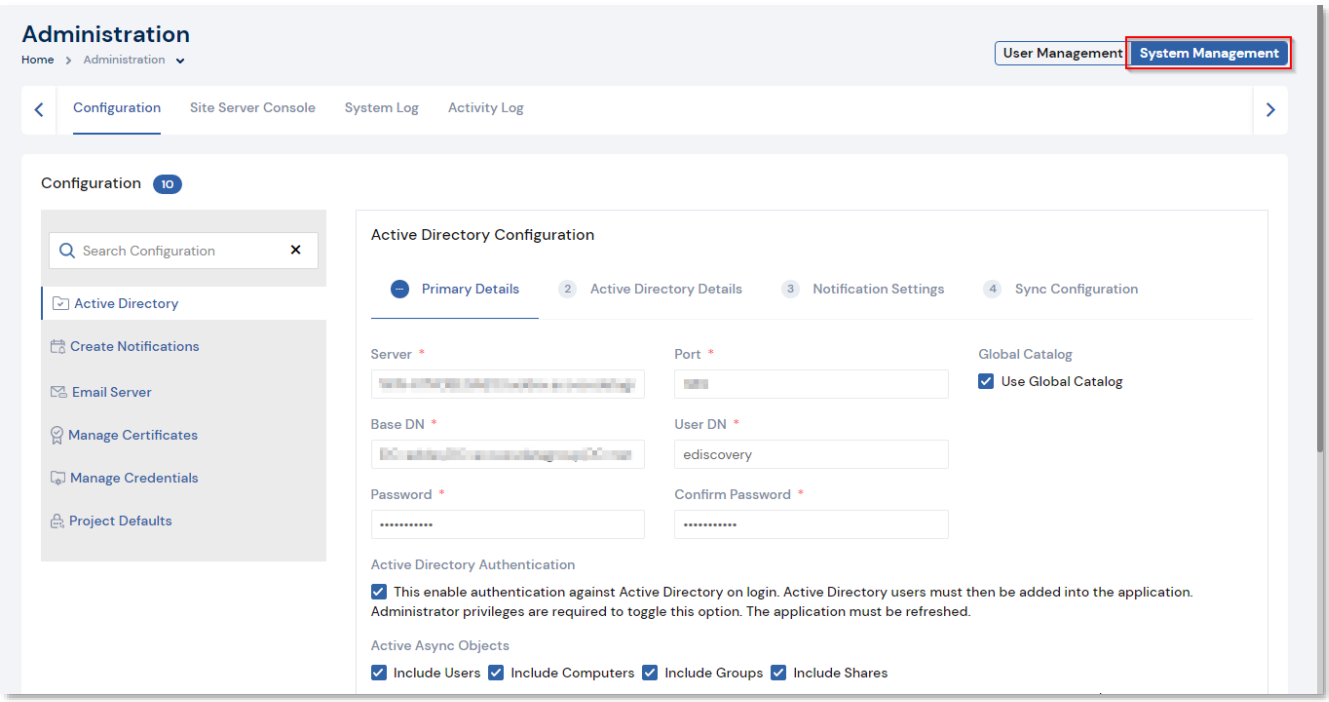
Supported Methods:

- **Forms (Active Directory authentication)** - Presents a login screen for users to provide their Active Directory credentials. Active Directory username should be in the format "domain\user".
- **IWA (Active Directory authentication)** - Passes the credentials that the browser is running with (typically the credentials used to log into the machine).

© Exterro, Inc. All rights reserved

To configure an active directory:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
   - The **Active Directory Configuration** page is displayed.



3. Provide the required details

Notes:

- When importing **Groups**, users within these groups will inherit any permissions associated to the imported group. However, these can be overridden by assigning a role or permission directly to a user.
- The **Global Catalog** option should be disabled while importing groups.

© Exterro, Inc. All rights reserved

Primary Details

Fields	Description
Server	Enter the server name of a domain controller in the enterprise.
Use Global Catalog	Select to use the global catalog.
Port	Enter the connection port number used by Active Directory. ***Note**: The default port number is 389.* If you want to support synch with an entire Active Directory forest, set the port as 3268. Otherwise, the synch only collects information from one domain instead of the entire forest. ***Note**: The default ports for communicating with Active Directory are:* • *LDAP: 389* • *Secure LDAP(SSL): 636* • *Global Catalog: 3268* • *Secure Global Catalog(SSL): 3269*
Base DN	Enter the starting point in the Active Directory hierarchy at which the search for users and groups begins. The Base DN (Distinguished Name) describes where to load users and groups. For example, in the following base DN *dc=domain,dc=com* you would replace domain and com with the appropriate domain name to search for objects such as users, computers, contacts, groups, and file volumes.
User DN	Enter the distinguished name of the user that connects to the directory server. For example, *tjones or <domain>\tjones*
Password	Enter the password that corresponds to the User DN account. This is the same password used when connecting to the directory server.

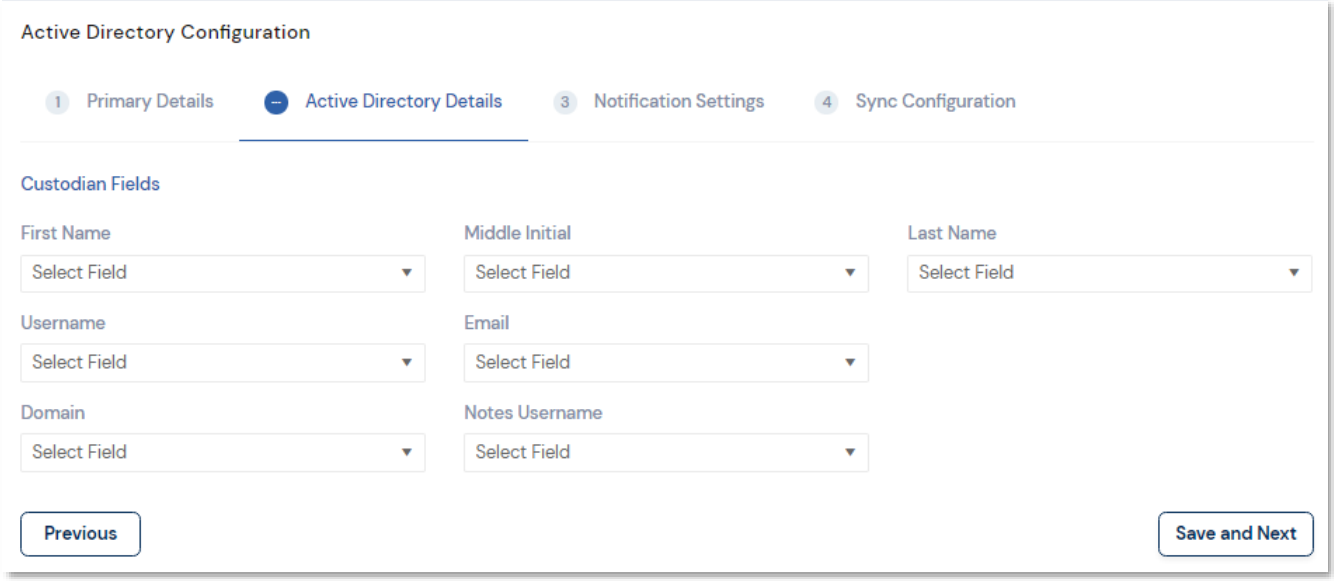
© Exterro, Inc. All rights reserved

Fields	Description
Active Directory Authentication	Select to enable authentication against Active Directory on login.
AD Sync Objects	You can select which types of objects to include or not include: Users, Groups, Computers, or Shares. All objects are selected by default. If you want to exclude objects from being synced, de-select those objects. This can be helpful to easily add new users only.
AD Sync Recurrence	Configure a daily recurrence by selecting or entering the time of day to start the sync. If a sync is in progress when the interval occurs, the interval is skipped to allow the current sync to complete.
Test Configuration	Click to test the current configuration to ensure proper communication exists with the Active Directory server.
AD Synchronization	Set to inactive by default.

4. Click **Save and Next**.

© Exterro, Inc. All rights reserved

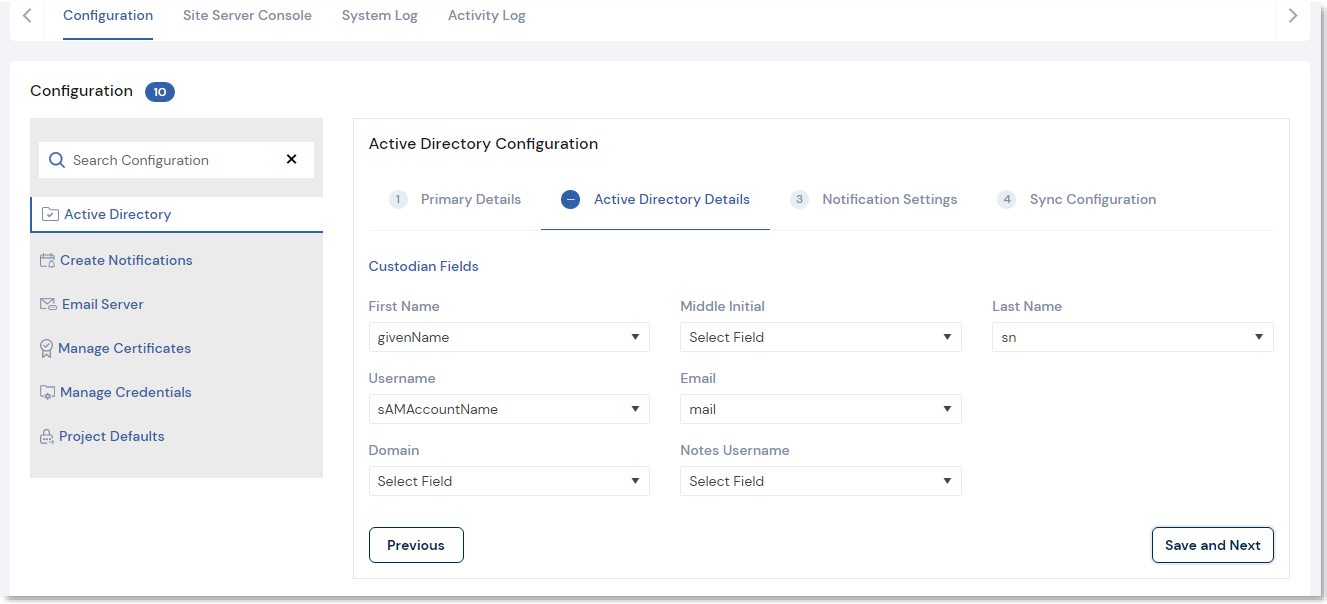
Active Directory Details



5. Select the Custodian Fields to be mapped from the fields on the active directory.

Fields	Description
First Name	The first name of the person.
Middle Name	The middle initial of the person
Last Name	The last name of the person.
Username	The computer username of the person.
Email	The email address of the person. This will be retrieved from the Active Directory.
Domain	The network domain to which the person belongs.
Notes Username	The username of the person as it appears in their Lotus Notes Directory. A Lotus Notes username is typically formatted as Firstname Lastname/Organization as in the following example: • Pat Ng/ICM

© Exterro, Inc. All rights reserved

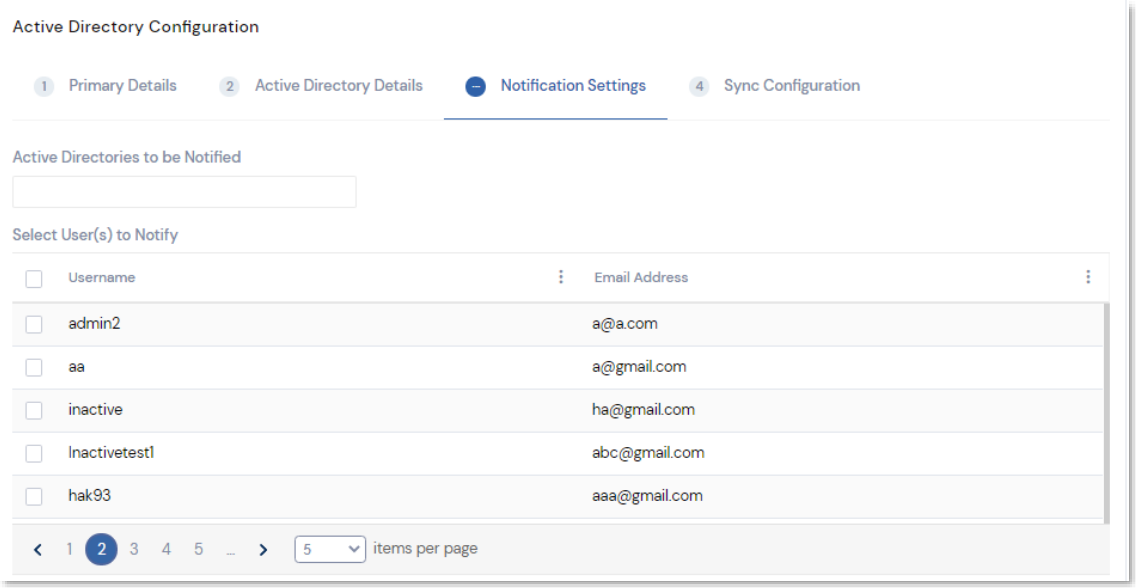


6. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Notification Settings

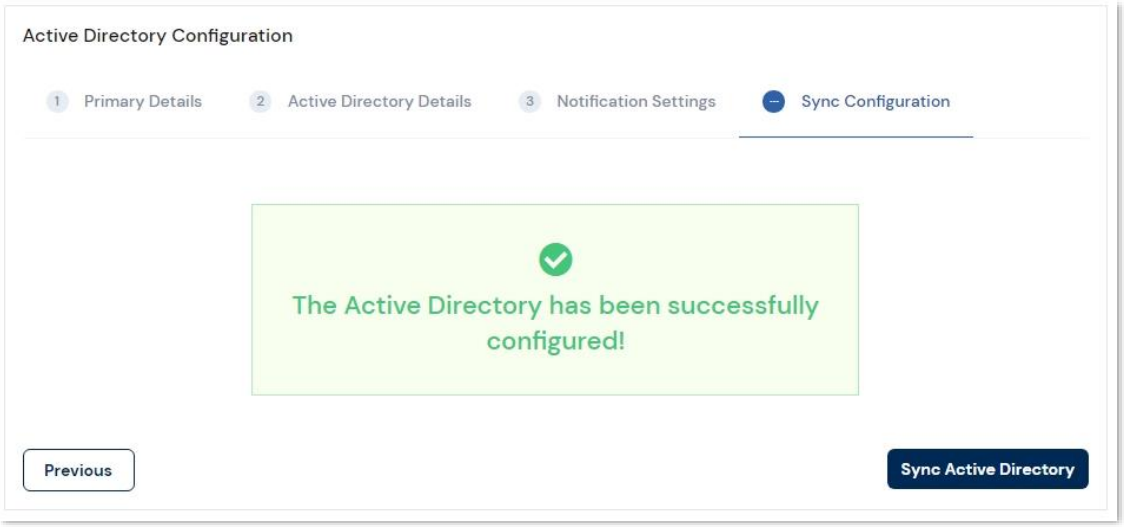
You can select which Active Directory fields you want to be notified about when changes occur and which application users to send an email to. The notification email contains a time stamp, the name of the user that the change occurred for, the properties that changed, and the old and new values of the changed properties.



7. Select the **Active Directories to be Notified**.
8. Select the users to be notified.
9. Click **Save and Next**.

© Exterro, Inc. All rights reserved

Sync Configuration



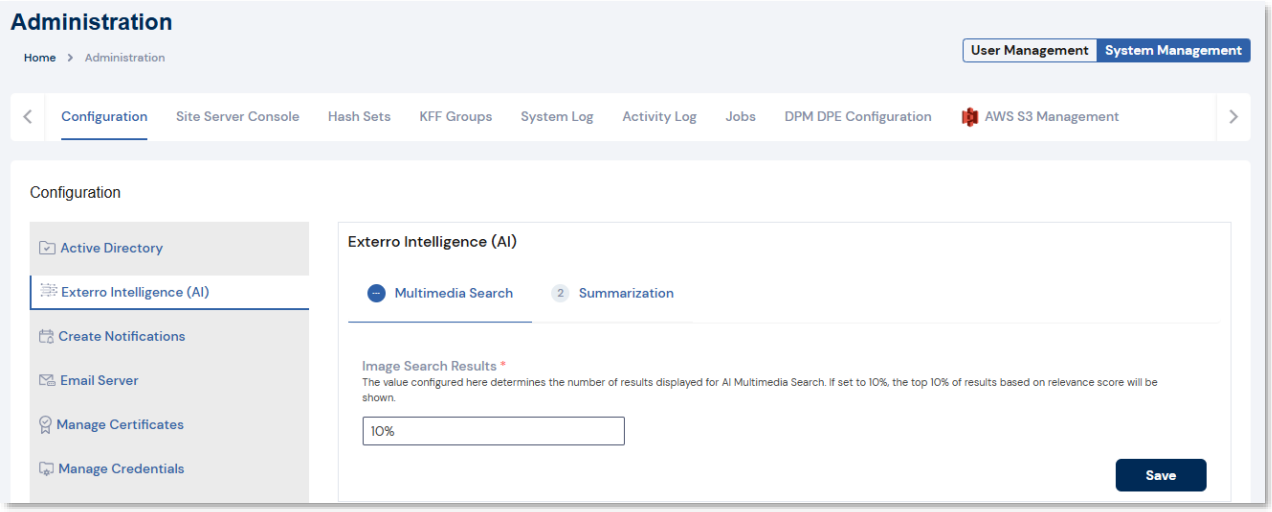
10. Click **Sync Active Directory**.

© Exterro, Inc. All rights reserved

Exterro Intelligence (AI)

This section allows you to make the necessary configurations related to the following AI features:

- Multimedia Search
- Summarization



© Exterro, Inc. All rights reserved

Multimedia Search

The percentage configured in the **Image Search Results** field will determine whether to display the entire search results or just a fraction of the most relevant results.

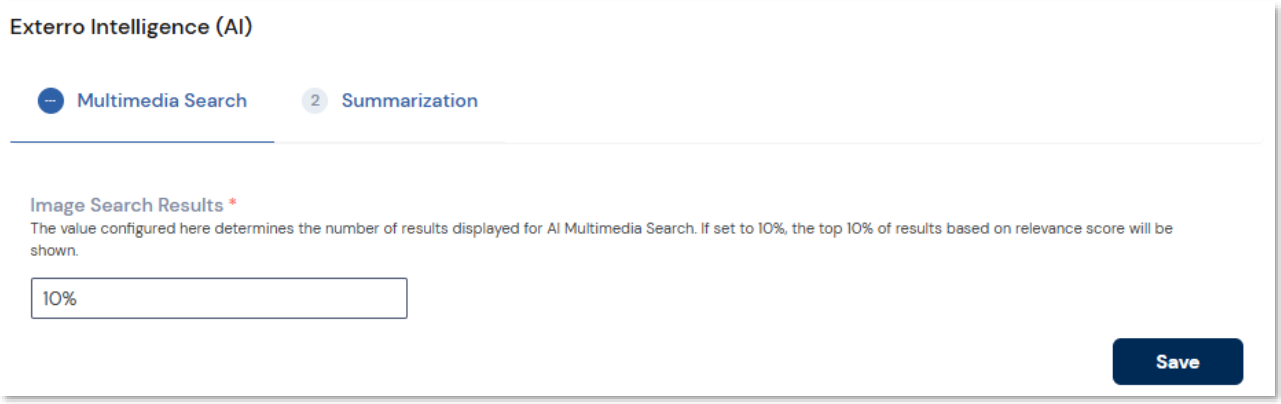
Example:

Image Search Results *- 20%*

Search keyword *- Knife*

The total number of images containing knife *– 100*

Results displayed in Thumbnail View *– 20 (with the highest relevancy score)*

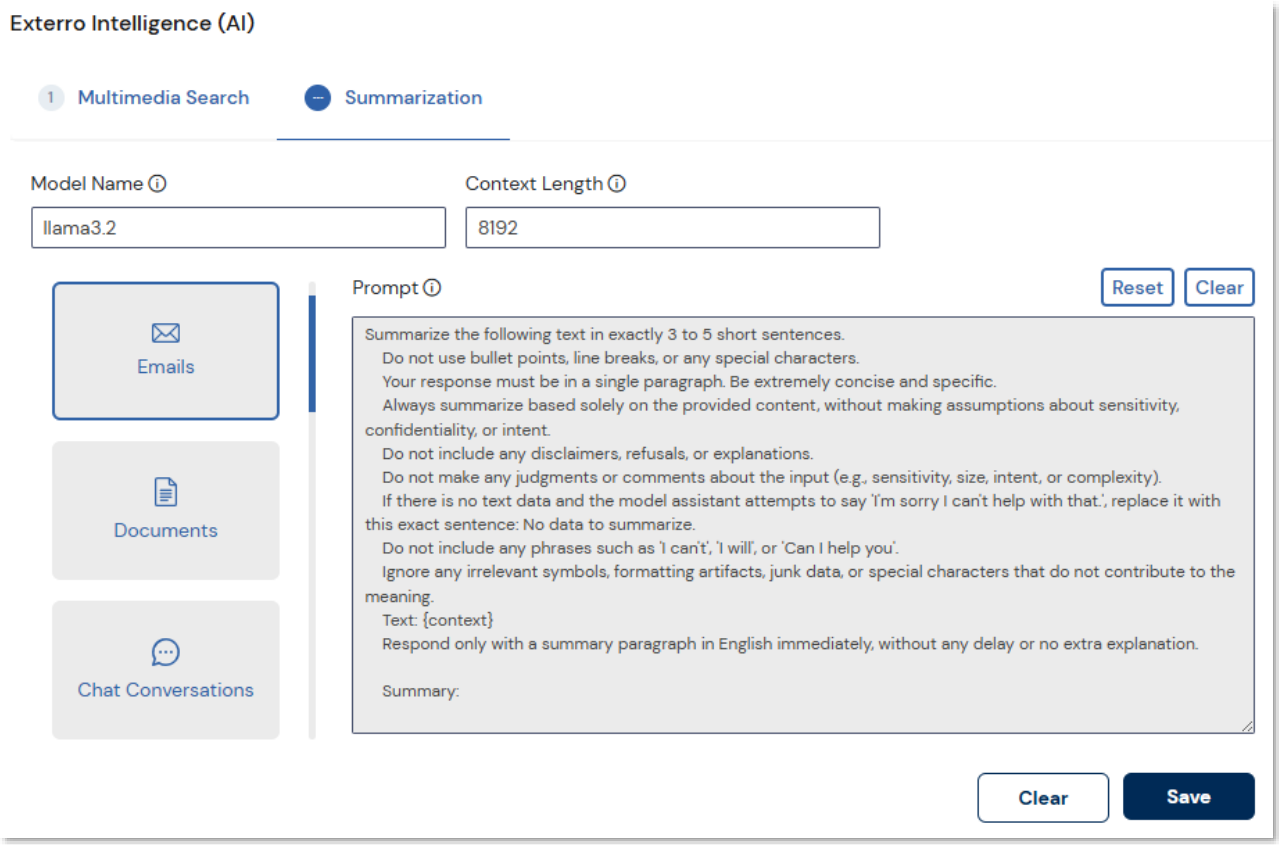


Note: The value set in the **Image Search Results** field will be set as default for all the applicable cases. However, you can change it based on your preference (using the **Result** field) while performing the search in the **Thumbnail View.**

© Exterro, Inc. All rights reserved

Summarization

You can configure the below fields to determine how the overall summarization process should be performed for the Email, Chat, and Documents:



- **Model Name** – The AI model intended to perform the summarization.

Note: You are recommended to use the default AI models present in the FTK Central application.

© Exterro, Inc. All rights reserved

- **Context Length** – The maximum number of characters that can be utilized while generating the summary.
- **Prompt** – You can meticulously describe and instruct the application on how the summarization should be performed (such as, what all information is expected in the summary, how the summary should be presented, etc.)

  You can set up different **Prompt** instruction sets for each file type by choosing the required file type from the left pane.

Note: Ensure the prompts you provide are not contradictory to avoid incorrect or inaccurate results

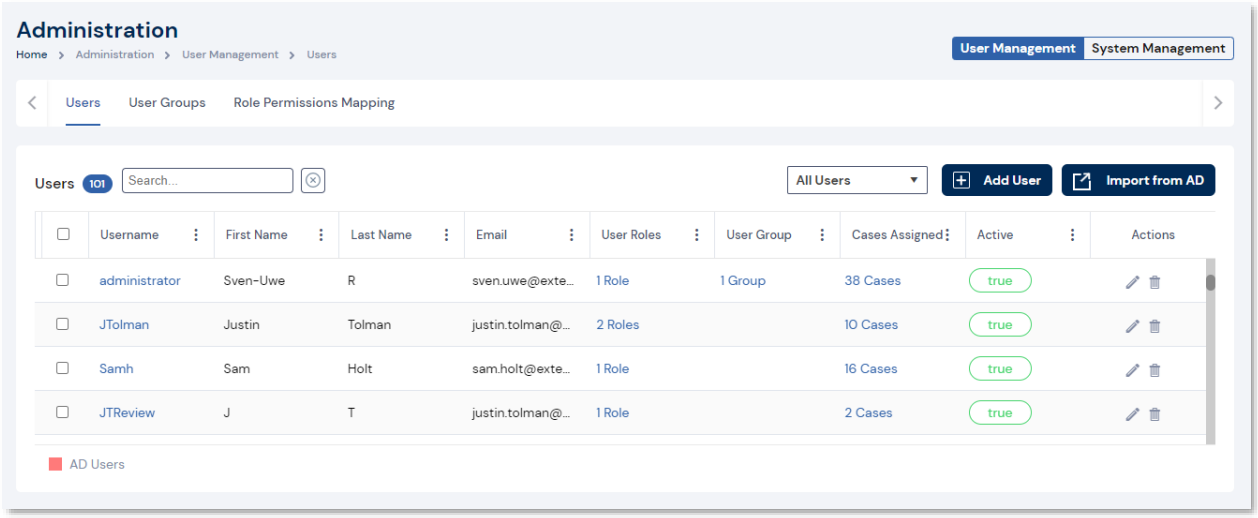
© Exterro, Inc. All rights reserved

Create Notifications

You can configure event notifications for certain system events. You select which type of event for which you want a notification and the users to whom the notification is sent.

To create a job notification:

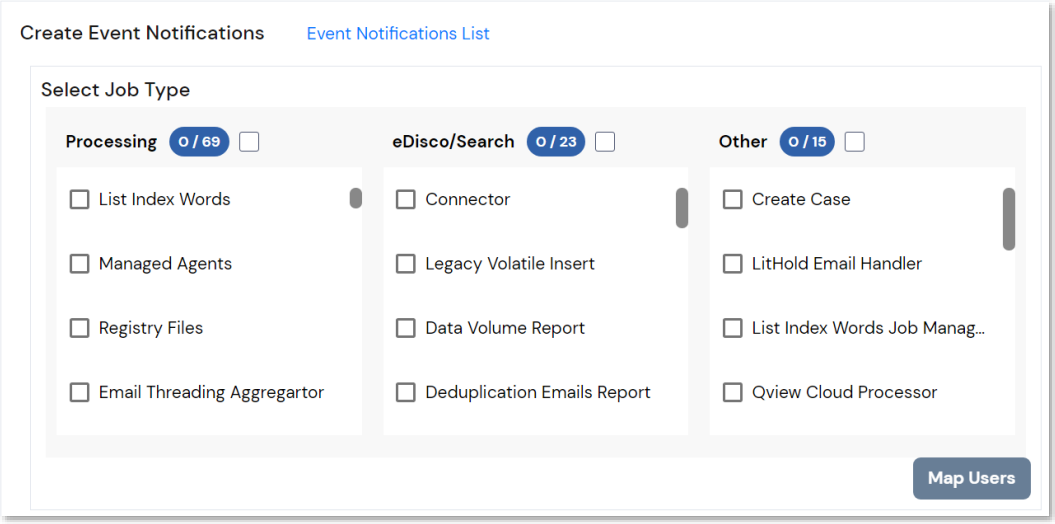
1. From the home page, click **Settings** button from the top-right corner.
   - The **Administration** page is displayed.



2. Navigate to the **System Management** tab.
3. Click **Create Notifications** from the left pane of **Configuration** section.

© Exterro, Inc. All rights reserved

4. Select **Create Event Notifications**.



5. Check the required job types.
6. Click **Map Users**.
7. Select the required users whose actions within the application should be notified.

Note: You can click on **Add More Email IDs** to assign email addresses that may not pertain to a user account. These email addresses will be notified when a user event has taken place.

8. Click **Save**.

Note: You can click on the **Edit** or **Delete** icon to edit or delete the event notifications respectively.

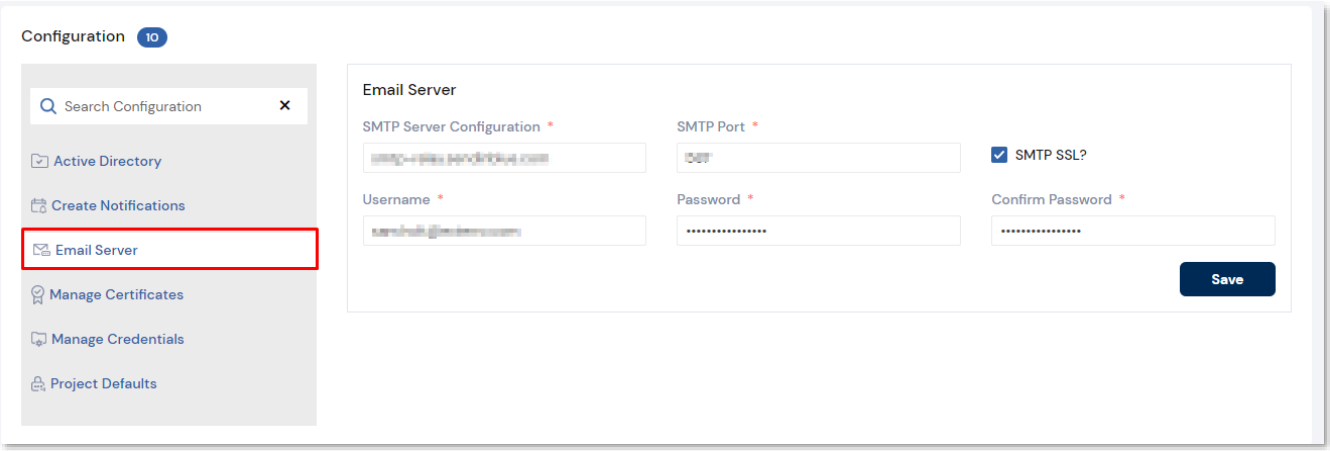
© Exterro, Inc. All rights reserved

Email Server

You can configure the Email Notification Server so that you create and send notification emails.

To create an email server:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to **System Management** tab.
3. Click **Email Server**.
   - The **Email Server** page is displayed.



4. Enter the **SMTP Server Configuration**, i.e., the address of the SMTP mail server (for example, smtpserver.domain.com or server1) on which you have a valid account.

Warning: You must have an SMTP-compliant email system, such as a POP3 mail server to receive notification messages from the application.

5. Enter the **SMTP Port** number.

Note: Port 25 is the standard non-SSL SMTP port. However, if a connection is not established with default port 25, contact the email server administrator to get the correct port number.

6. Enable the **SMTP SSL** checkbox to encrypt the communication.
7. Provide the **Username,** i.e., the email address of the sender account.
8. Provide the **Password** of the sender account
9. Enter the same in the **Confirm Password** field.
10. Click **Save**.

© Exterro, Inc. All rights reserved

Manage Certificates

Management of certificates can be done within the configuration page. These certificates will encrypt the data.

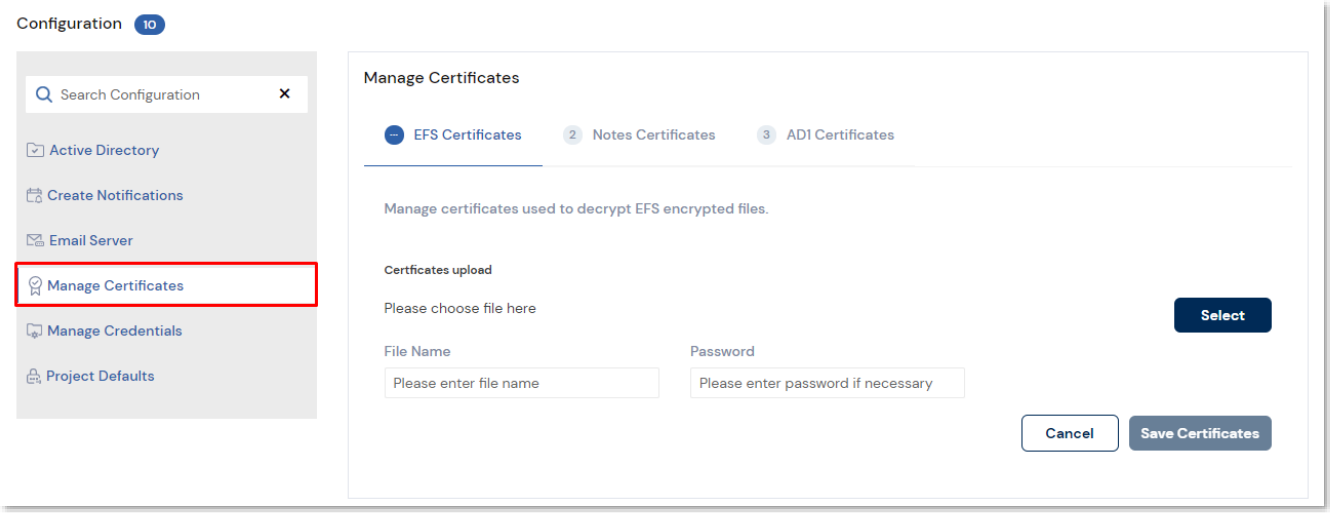
EFS Certificates

EFS is a file system driver that provides file system-level encryption in most Microsoft Windows operating systems. Files are transparently encrypted on NTFS file systems to protect confidential data from attackers with physical access to the computer. To decrypt the EFS files so that the system can process them, you will need to configure an EFS certificate.

© Exterro, Inc. All rights reserved

To manage EFS certificate:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Manage Certificates**.
    - The **Manage Certificates** page is displayed.



4. Click **Select** and upload the .pfx certificate file.
5. Provide a name for the certificate in **File Name**.
6. Enter the password that is necessary to access the .pfx file in **Password**.
7. Click **Save Certificates**.

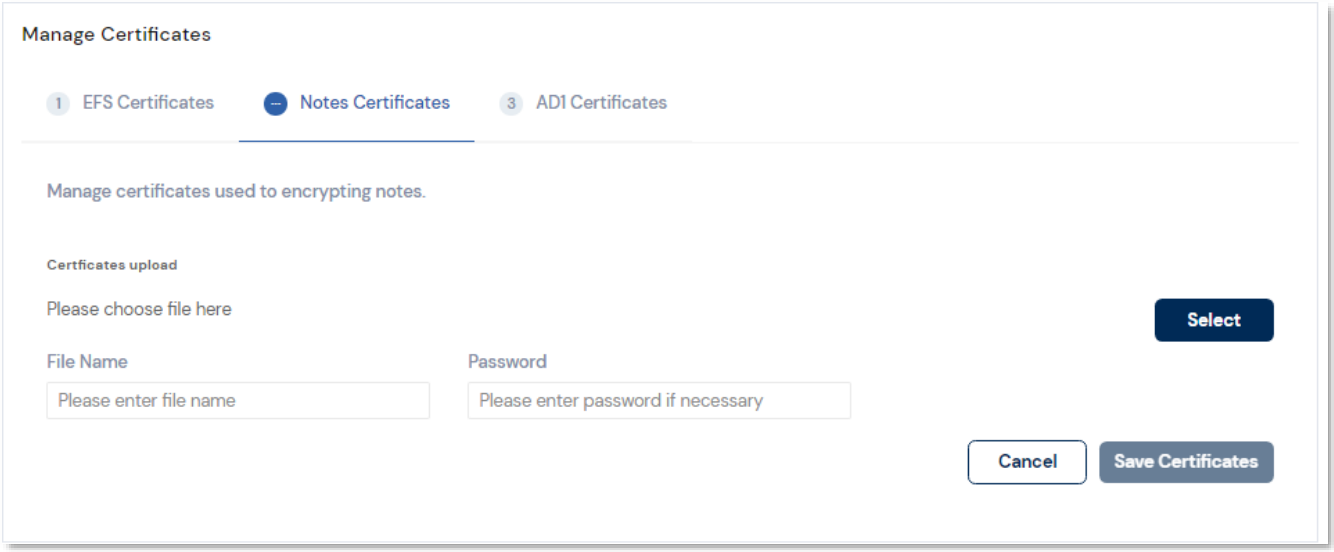
© Exterro, Inc. All rights reserved

Notes Certificates

This allows you to manage certificates used for encrypting Lotus Notes files.

To manage Lotus Notes certificate:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Manage Certificates**.
4. Navigate to **Notes Certificates**.



5. Click **Select** and upload the file.
6. Provide a name for the certificate in **File Name**.
7. Enter the certificate **Password,** if applicable.
8. Click **Save Certificates**.

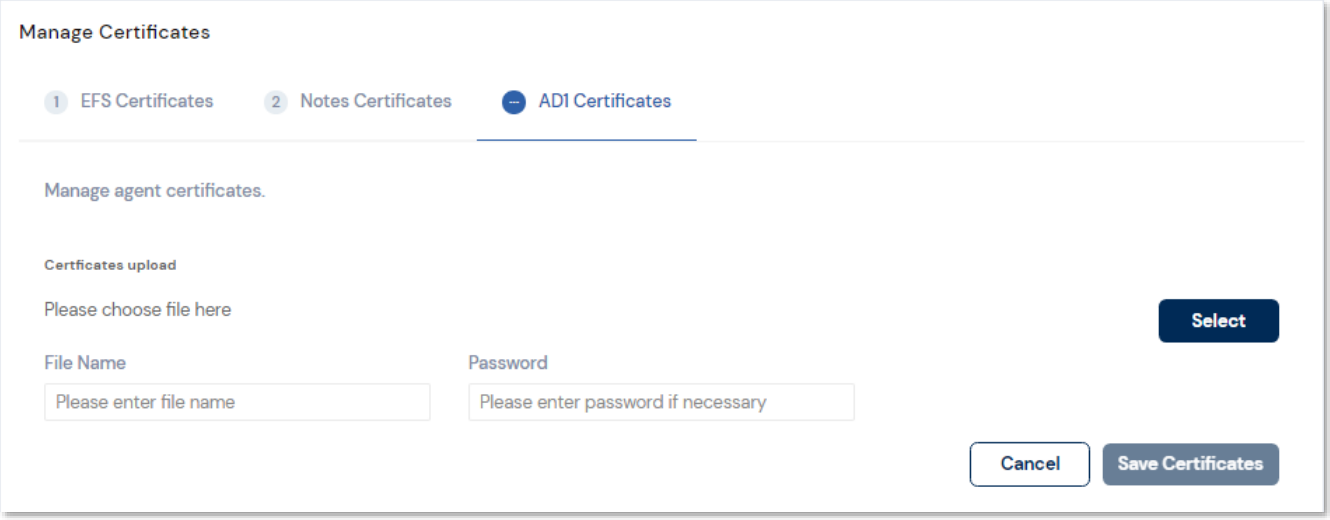
© Exterro, Inc. All rights reserved

AD1 Certificates

Allows you to manage certificates used for encrypting AD1 files.

To manage AD1 certificate:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Manage Certificates**.
4. Navigate to **AD1 Certificates**.



5. Click **Select** and upload the file.
6. Provide a name for the certificate in **File Name**.
7. Enter the certificate **Password,** if applicable.
8. Click **Save Certificates**.

© Exterro, Inc. All rights reserved

Manage Credentials

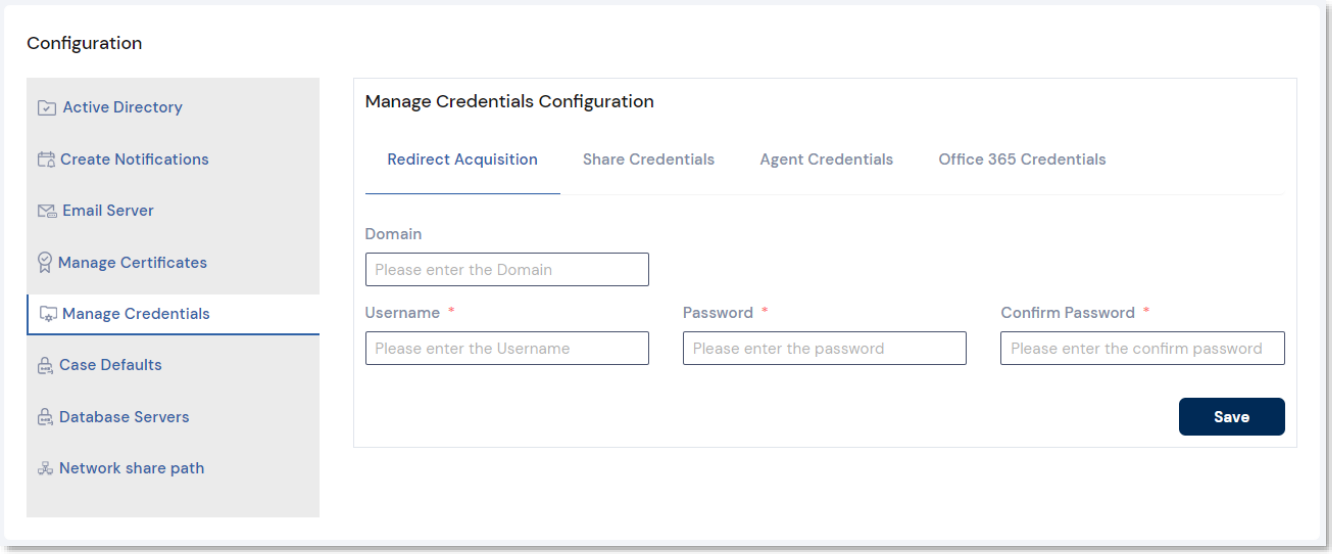
You can define the credentials used by the system to install the Agent on a target computer, as well as configuring share credentials and redirected acquisitions.

Redirected Acquisition

You can use Redirected Acquisition to direct the results of a full disk (logical or physical) collection from an agent(s) to the configured collection data path.

To manage the redirected acquisition credentials:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Manage Credentials**.
    - The **Manage Credentials Configuration** page is displayed.



4. Enter the **Domain** name.
5. Provide the **Username**.
6. Provide the **Password**.
7. Enter the same in **Confirm Password** field.
8. Click **Save**.

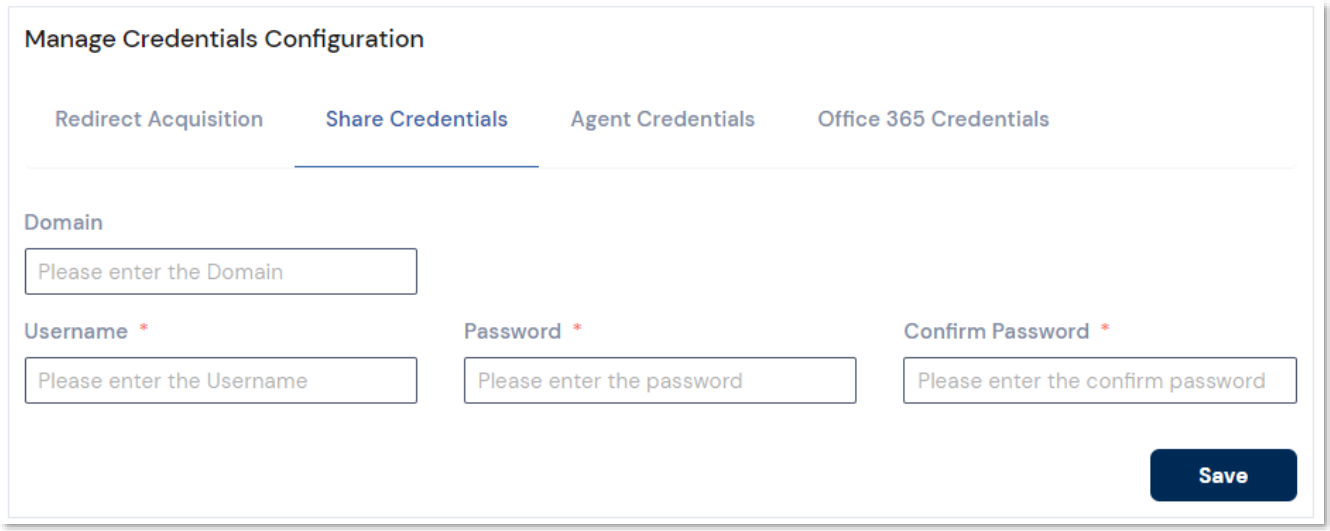
© Exterro, Inc. All rights reserved

Share Credentials

You can define the credentials used by the system to access network shares that are configured as Data Sources.

To define share credentials:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Manage Credentials**.
4. Navigate to **Share Credentials**.



5. Enter the **Domain** name.
6. Provide the **Username**.
7. Provide the **Password**.
8. Enter the same in **Confirm Password** field.
9. Click **Save**.

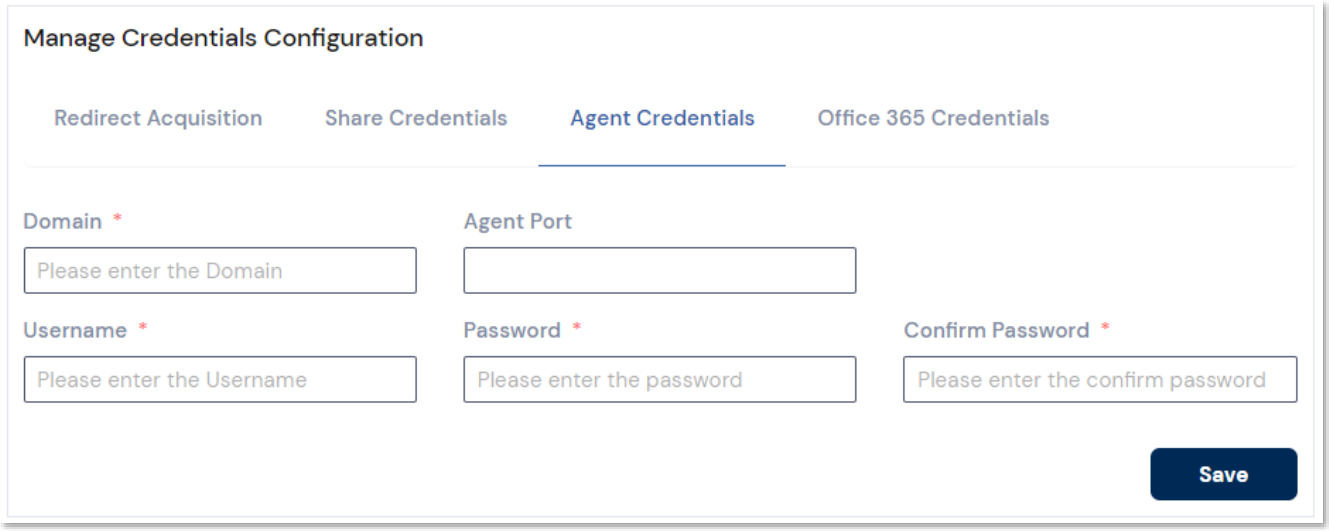
© Exterro, Inc. All rights reserved

Agent Credentials

You can define the credentials used by the system to install the Agent on a target computer. These credentials must be populated for agent deployments via FTK Central.

To define agent credentials:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Manage Credentials**.
4. Navigate to **Agent Credentials**.



5. Enter the **Domain** name.
6. Enter the **Agent Port**.
7. Provide the **Username**.
8. Provide the **Password**.
9. Enter the same in **Confirm Password** field.
10. Click **Save**.

© Exterro, Inc. All rights reserved

Office 365 Credentials

You can define the URLs to allow collections from Office 365 GCC environments such as Exchange, OneDrive, Teams and SharePoint. You can also choose the API method to be Graph API or Export API.

> **Note:** When the required URLs are configured, they will only allow GCC high collections. Users must remove GCC URLs and replace them with non-GCC URLs to allow collections from non-GCC environments.

GCC URLs

Azure AD Authentication URL: https://login.microsoftonline.us

Microsoft Graph URL: https://graph.microsoft.us

Non-GCC URLs

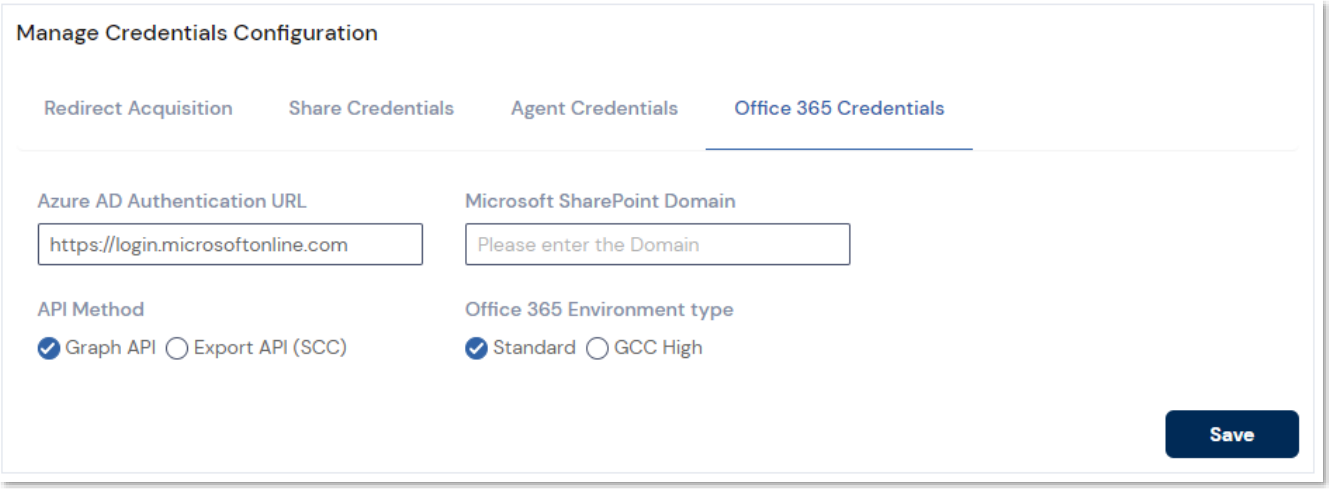
Azure AD Authentication URL: https://login.microsoftonline.com

Microsoft Graph URL: https://graph.microsoft.com

© Exterro, Inc. All rights reserved

To define Office 365 credentials:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Manage Credentials**.
4. Navigate to **Office 365 Credentials**.
5. Enter the **Azure AD Authentication URL**.



6. Enter the **Microsoft Sharepoint Domain**.
7. Choose the **API Method**.
   e) Graph API - Selecting this will collect data using the Graph API method.

© Exterro, Inc. All rights reserved

f) Export API (SCC) – Selecting this will collect data using the PowerShell script.

API Method
○ Graph API ● Export API (SCC)

Office 365 Environment type
● Standard ○ GCC High

Refresh Token
Please enter the Refresh Token

Admin User Account
Please enter the Admin User Accou

Microsoft Teams Redirect Url
Please enter the Microsoft Teams R

Microsoft Client ID (Teams & OneDrive)
Please enter the Client ID

Microsoft Client secret (Teams & OneDrive)
Please enter the Client secret

Microsoft Sharepoint Username
Please enter the Username

Microsoft Sharepoint Password
Please enter the Password

Tenant Active Directory Name
Please enter Tenant Active Director

O365 Export Scope ○ Indexed only ○ Unindexed only ● Both Indexed and Unindexed

i. Enter the **Refresh Token**.
ii. Enter the **Admin User Account**.
iii. Enter the **Microsoft Teams Redirect URL**.
iv. Enter the **Microsoft Client ID (Teams & OneDrive)**.
v. Enter the **Microsoft Client Secret (Teams & OneDrive)**.
vi. Enter the **Microsoft Sharepoint Username**.
vii. Enter the **Microsoft Sharepoint Password**.
viii. Enter the **Tenant Active Directory Name**.

© Exterro, Inc. All rights reserved

ix. Choose the **O365 Export Scope**.

a. Indexed Only - All items, excluding the one that have unrecognized format are encrypted, or not indexed for other reasons.

b. Unindexed only - Only the items that have an unrecognized format are encrypted, or not indexed for other reasons.

c. Both Indexed and Unindexed - All the items, including the one that have unrecognized format are encrypted, or not indexed for other reasons.

8. Select the **Office 365 Environment type**.

a) Standard - Select this to collect data for Standard Method where the URL of O365 will end with **.com**.

b) GCC High - Select this to Collect data specific to GCC where the URL ends with **.us**.

9. Click **Save**.

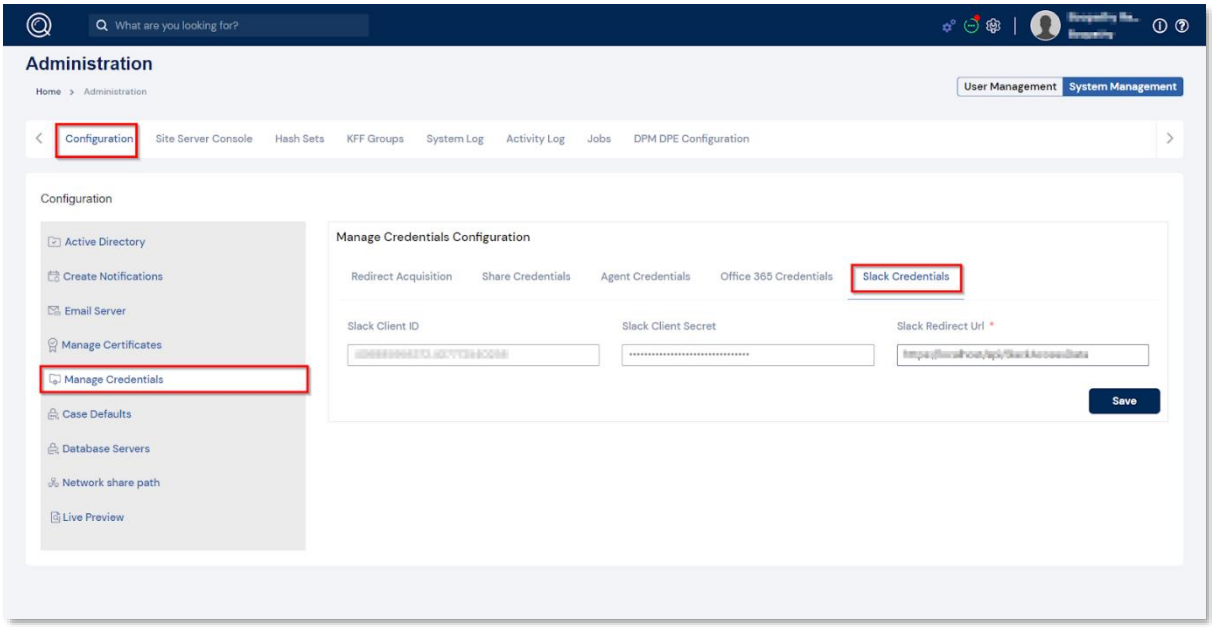
© Exterro, Inc. All rights reserved

Slack Credentials

To define Slack credentials:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Manage Credentials**.
4. Navigate to **Slack Credentials**.

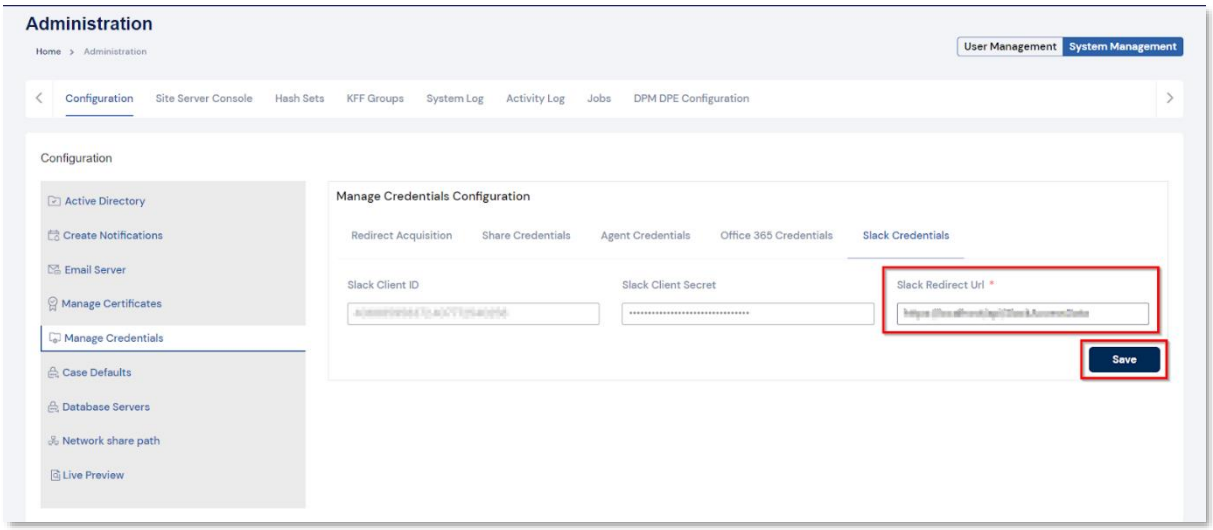
Note: The Slack Client ID and Slack Client Secret values will be pre-populated.



© Exterro, Inc. All rights reserved

5. Enter Exterro's FTK Central URL in the **Slack Redirect URL** field.

Example: *https://<testsite.exterro.net>/api/SlackAccessData*



6. Click **Save**.

Note: If your organization has enabled Block Files Download, you must create a Slack app using the https://api.slack.com URL and register it accordingly. You are recommend reaching out to the Exterro Support team for assistance in configuring the application.

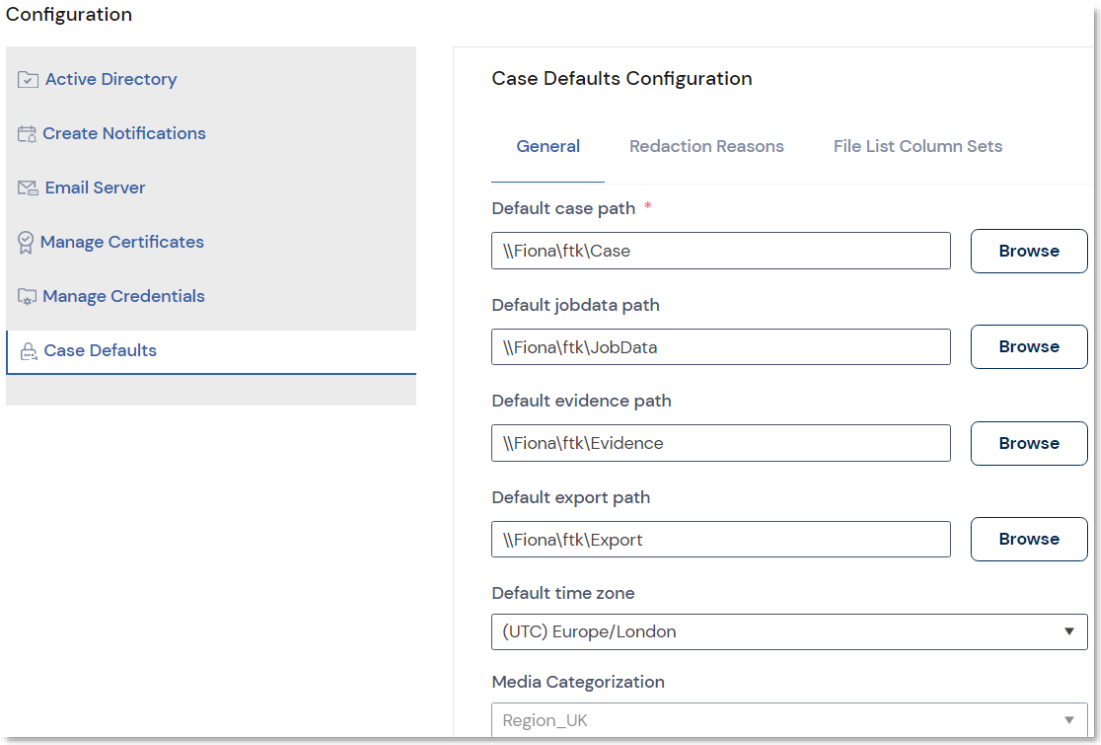
© Exterro, Inc. All rights reserved

Case Defaults

Configuring Case Defaults allows you to enter default directories for case, job data, evidence and export paths as well as other significant options.

General

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to **System Management** tab.
3. Click **Case Defaults**.



© Exterro, Inc. All rights reserved

4. Click **Browse** and choose the path/setting for the following fields.
   - **Default Case Path** – The selected path will appear during case creation. This directory will be pre-defined whenever creating a new case. If no default path is configured, the user creating the case must provide this information.
   - **Default Job Data Path** – The selected path will appear during case creation. The selected path will appear during case creation. This directory will be pre-defined whenever creating a new case. If no default path is configured, the user creating the case must provide this information.
   - **Default Evidence Path** – The selected path will appear during case creation. The selected path will appear during case creation. This directory will be pre-defined whenever creating a new case. If no default path is configured, the user creating the case must provide this information.
   - **Default Export Path** – The selected path will appear during case creation. The selected path will appear during case creation. This directory will be pre-defined whenever creating a new case. If no default path is configured, the user creating the case must provide this information.
   - **Default Processing Profile** – The selected processing profile will appear during case creation. This can be changed during case creation if required.
   - **Default Load File Path** – The selected load file path will be applicable during case creation, where the load file import option is selected.
   - **System Time Zone** – The selected time zone will appear as a default during case creation.
   - **Default date format** – The selected date format will be used to display the dates in the application.
   - **Media Categorization** – The selected media category will be set as the default region when categorizing data using VIC/CAID. This list will not be populated unless a KFF server is present and a case has objects which match the KFF alerts.

5. Click **Save**.

© Exterro, Inc. All rights reserved

Creating Redaction Reasons

Redaction Reasons can be used by organizations/teams to clearly identify content of importance without revealing the specifics. These redaction reasons appear when you redact areas of a document.

Refer the Using the Image Panel section for more details.

Creating a redaction reason:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click Case Defaults > Redaction Reasons.
4. Click Add Redaction Reason.
5. Enter a Column Set Name.
6. **Assign Case** using the drop-down list.

Note: By default, if a case is not assigned, it will be assigned to all cases.

7. Click **Submit**.

Note: You can edit or delete a saved redaction reason by clicking on the **Edit** button or **Delete** button respectively.

© Exterro, Inc. All rights reserved

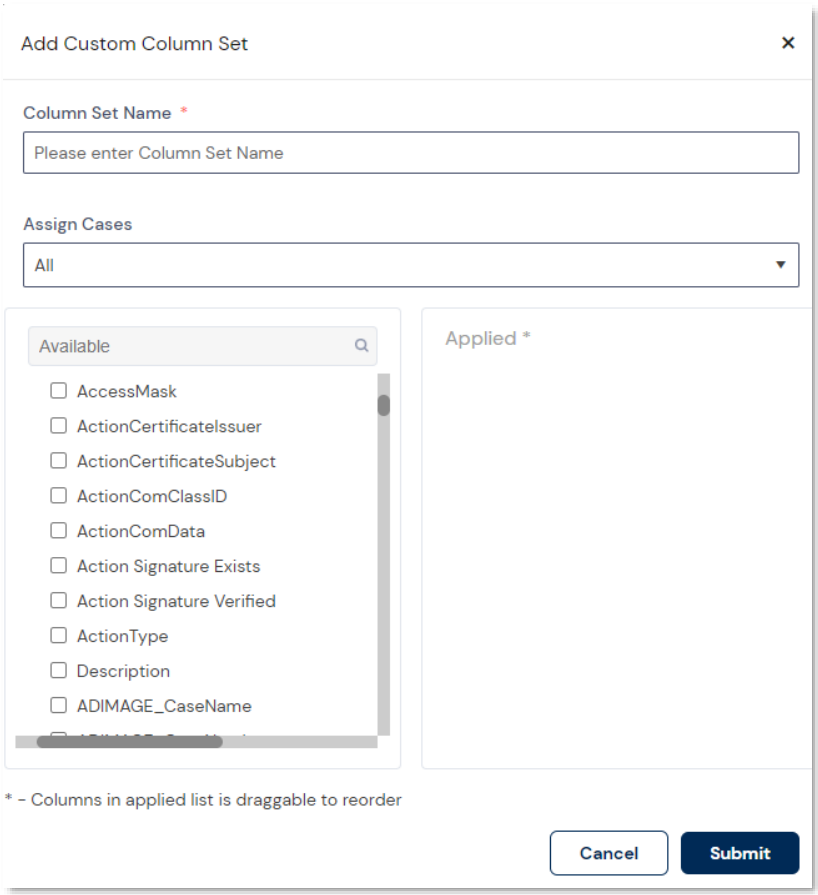
Creating Custom Column Sets

Custom columns are global columns. In other words, once a custom column is created, it is available for use in all Cases and can be edited in the Administration section on a case-by-case basis. The newly created column is automatically displayed in the Case List with the other default columns.

If a custom column is deleted, it is removed from any previously created case(s) that may have populated the column with data.

To create a custom column set:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click Case Defaults > Custom Column Sets.
4. Click Add Column Set.
    - The **Add Custom Column Set** prompt is displayed.



© Exterro, Inc. All rights reserved

5. Enter a Column Set Name.
6. Select the required case from the **Assign Case** drop-down field.
7. Select the required columns from the **Available** panel.

Tip: You can click and drag the required columns to rearrange them.

8. Click **Submit**.

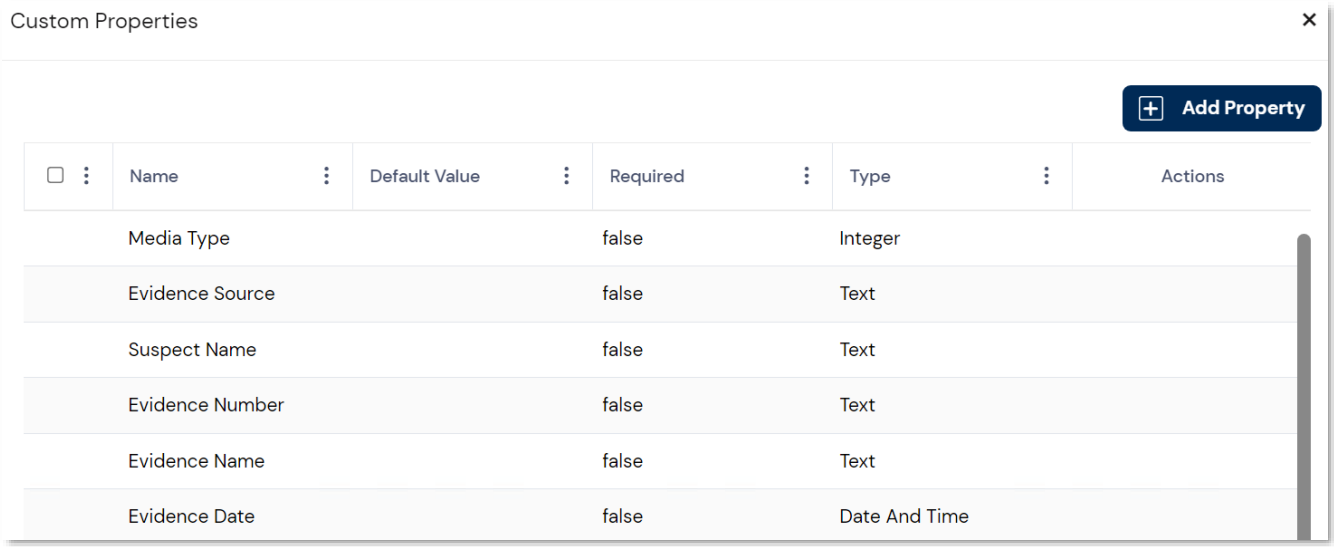
Tip: You can select the created custom column set by navigating to **Case > Enter Review > List View** > click the **Columns** drop-down list**.**

Note: You can edit or delete a saved custom column set by click on the **Edit** or **Delete** button respectively.

© Exterro, Inc. All rights reserved

Creating Custom Case Properties

Case properties relate to the fields that appear for each evidence item being ingested. These fields can be customized for specific requirements.

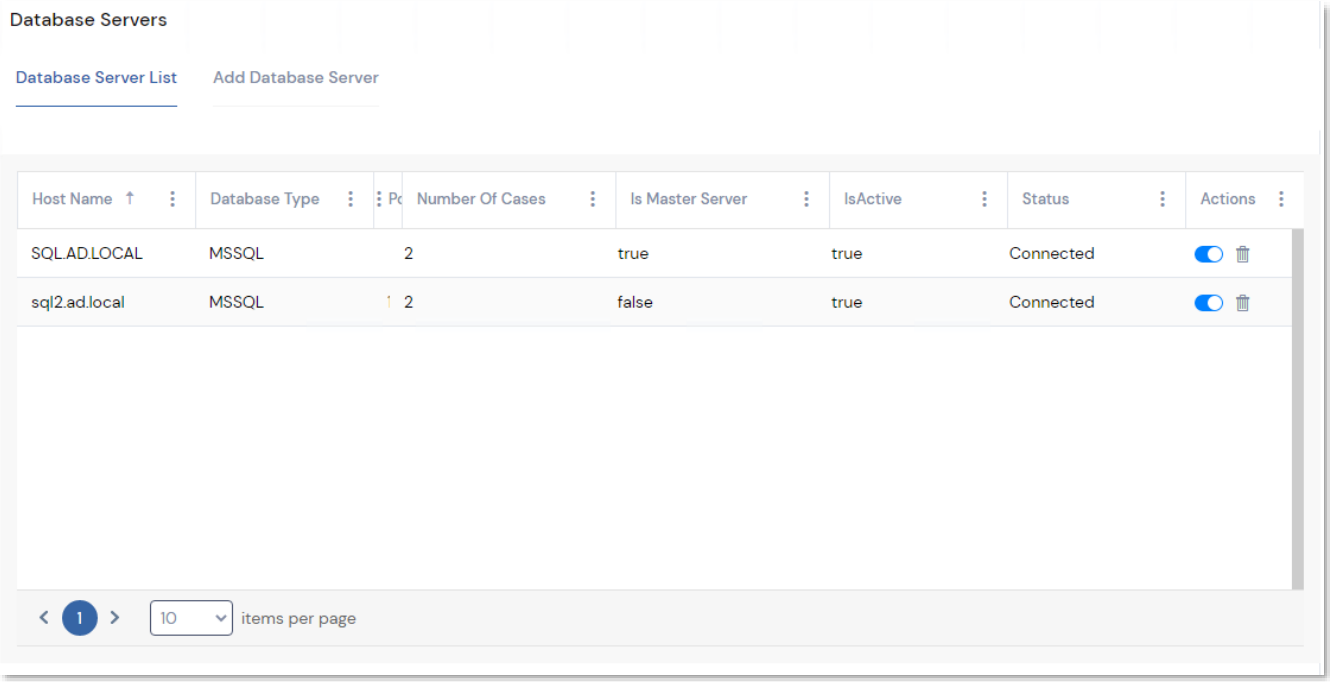


1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Case Defaults** > **Custom Case Properties**.
4. Upon checking the Process Evidence option, you will be navigated to a new section.
5. Click **Custom Case Properties**.
6. Click **Add Property**.
7. Enter a **Name** and **Description**.
8. Check the **Required** box to ensure this field is filled in during ingesting of evidence. If a value is not selected for a pick list, a choice will be selected automatically.
9. Select the **Type**.
    - **Date**
    - **Pick List** – Items should be listed one per line.
    - **Text**
10. Click **Create**.

© Exterro, Inc. All rights reserved

Database Servers

Configuring additional database servers allows for cases to be evenly distributed (round robin). Users must have one database configured as a master server in order for this functionality to operate.



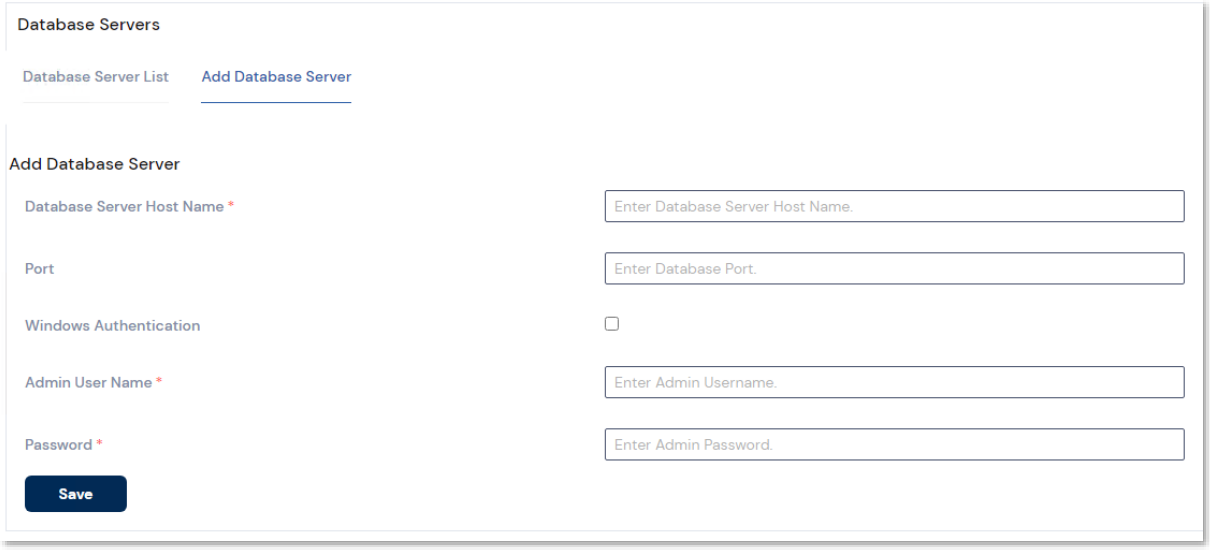
Note: Please ensure you have followed the Multi-Database Setup KB article before attempting the steps below.

© Exterro, Inc. All rights reserved

Adding Database Server

Adding a database server:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click Database Servers.
4. Navigate to the **Add Database Server** section.



5. Enter the **Database Server Host Name** or IP address.
6. Enter the **Port** (Default: 1433).

7. Enter the Admin (sa) Credentials or click Windows Authentication.

Note: If you are using the **Windows Authentication** option, the user must be a domain-level service account with local administrator permissions to all servers.

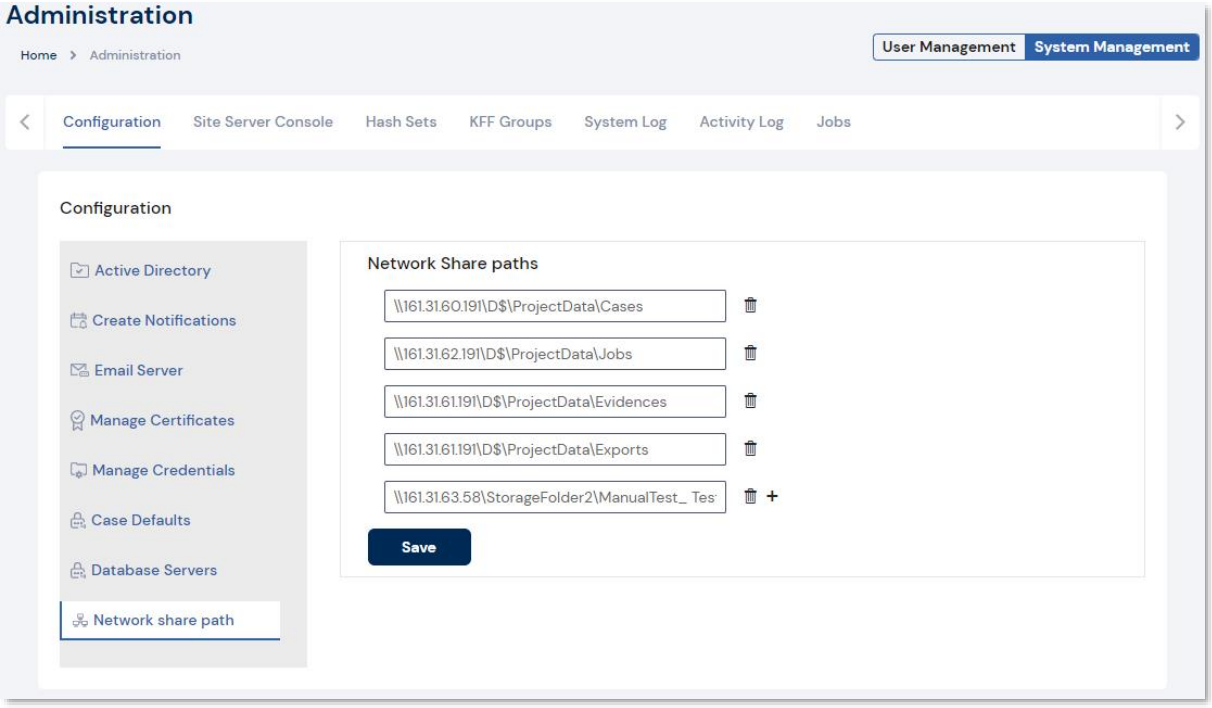
8. Click **Save**.

Tip: To stop cases being assigned to a specific database, users can simply click the toggle icon in the **Actions** column. This will not stop access to the cases stored on this database, it will only remove it from the active database pool for new cases.

© Exterro, Inc. All rights reserved

Network Share Paths

Configuring Network Share paths allows you to enter paths which users should have access to. This can include areas such as evidence stores, export paths and other resource stores. When configured administrators can associate a network share path to a user within the User Management section; edit User Groups. Application administrators will have access to all network shares whereas standard users will not have access to any directories unless specified within User Management.



© Exterro, Inc. All rights reserved

Paths to Consider:

The paths listed below should be considered when assigning Network Share Paths to users.

Module	Tab/Page	Path
Case List	Primary Details	Case Folder Path
		Job Data Path
	Load Files	File Path, Image Path
	Process Evidence	Evidence Path
Data Sources	Network Shares	Path
Collection	Collection Options	Results Path
System Management	Configuration	Default Case Path
		Default Job Data Path
		Default Evidence Path
		Default Export Path
		Default Load File Path
FTK Connect	Create - Workflow Steps	Watch Folder- Location
		Export - Location
		Search and Tag - Location
Case List - Enter Review	Export	Path
	Additional Analysis	Registry Reports Path
	Export-Media-Categories	Export Path
	Export-Semantics21	Export Path

© Exterro, Inc. All rights reserved

Module	Tab/Page	Path
	Create Report - Audit log	Report Path
Cases	Backup	Case Backup Directory
	Restore case	Restore Directory
Collection	Agent Remediation → send file	Source File Path
	Agent Remediation → Execute, Delete	Target File Path
	Threat Scan	Select Files, Folders

Adding Network Share Paths

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Click **Network Share Path**.
4. Click the **+** button to create a new network share path field.
5. Enter a **UNC** path to a desired destination.
    - An example of share paths that can be added are:
        - Case Folder
        - Job Data Folder
        - Evidence Folder
        - Export Folder
6. Click **Save**.

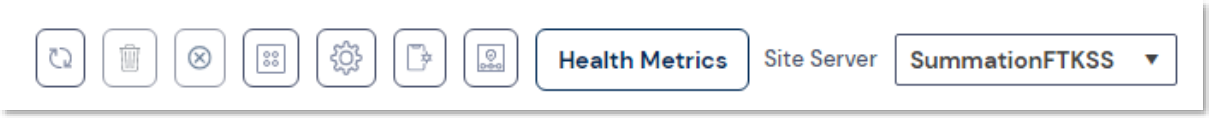
Note: To delete an existing/new Network Share path, click the **delete** button.

© Exterro, Inc. All rights reserved

Site Server Console

The Site Server Console lets you monitor all active site servers, monitor the jobs they are running along with the status of the servers. Moreover, you will be able to control throttling on Agents or Site Servers using Network Traffic Controls and set Phone Home Settings.

Note: The Site Server requires PostgreSQL to be installed.



Button:	Description
	Refresh job list.
	Delete job.
	Cancel job.
	View site server status.
	View site server configuration.
	View phone home settings.
	Replace agent installers.
Health Metrics	View site server health metrics.
SummationFTKSS	Site server toggle.

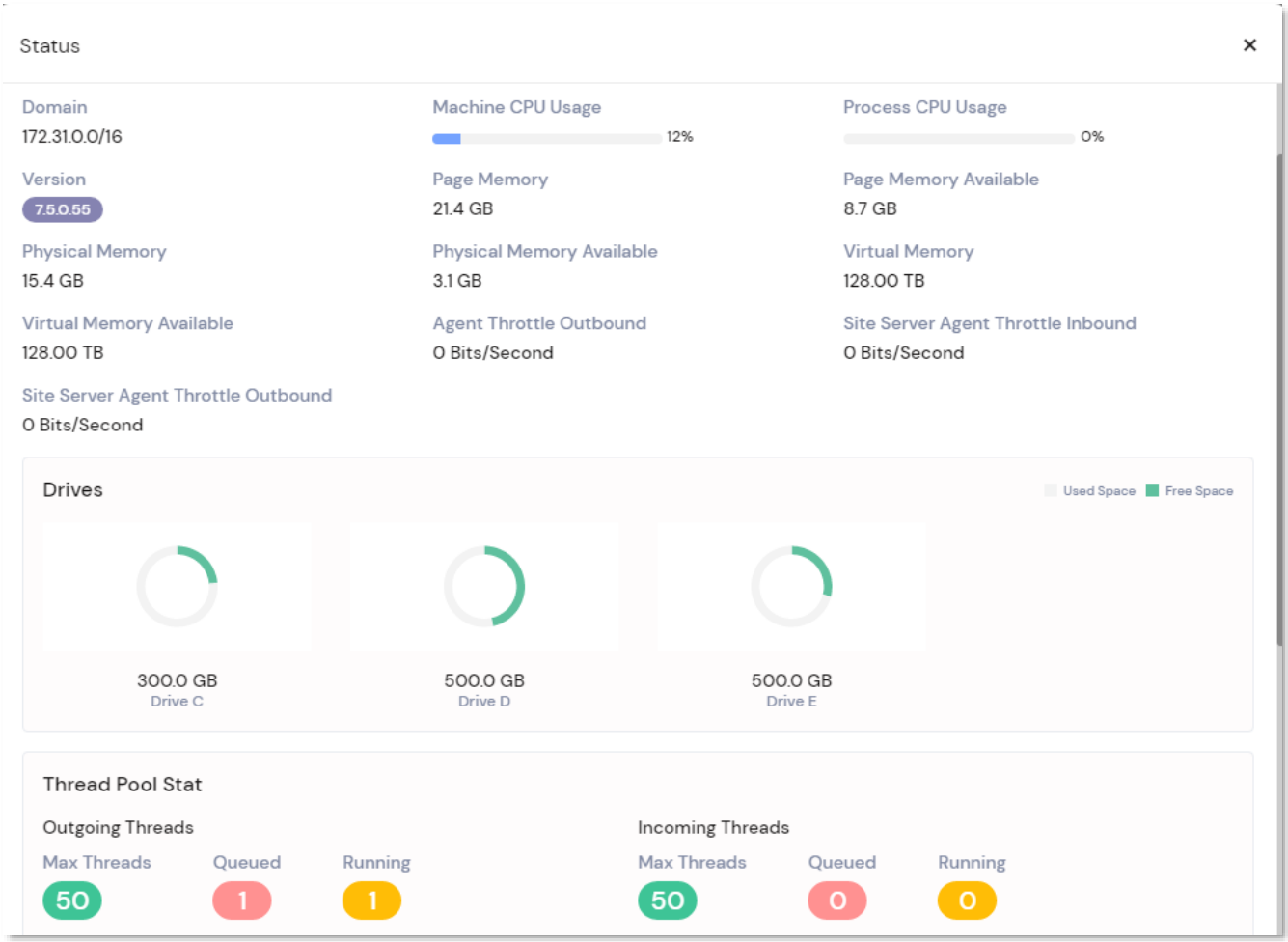
© Exterro, Inc. All rights reserved

Status

You can view statistics about your Site Servers using the Status tab of the Site Server Console.

To view the status of the site servers:

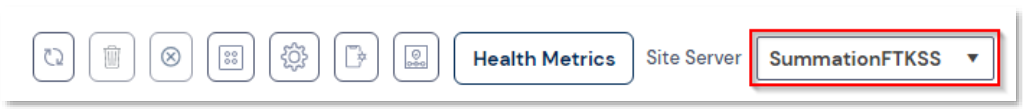
1. From the home page, click on **Settings** from the top-right corner.
2. Navigate to **System Management** tab from right pane.
3. Navigate to **Site Server Console** tab.
4. Click on the **Status** button .
   - The **Status** details page is displayed.



© Exterro, Inc. All rights reserved

Status	Description
Name	Friendly name of the site server.
Site Server Type	Root, Public, Private, Private Protected.
Site Server Status	Online/Offline.
Domain	Where the site server resides.
Machine CPU Usage	Current CPU usage on site server.
Process CPU Usage	Current CPU usage by the site server.
Version	Version of the site server.
Page Memory	Page memory amount.
Page Memory Available	Currently available page memory.
Physical Memory	Physical memory amount.
Physical Memory Available	Currently available physical memory.
Virtual Memory	Virtual memory amount.
Virtual Memory Available	Currently available virtual memory.
Agent Throttle Inbound/Outbound	Agent Throttling.
Site Server Agent Throttle Inbound/Outbound	Site Server to Agent throttling.
Drives	Drives available on the site server.
Thread Pool Stat	Overview of incoming/outgoing threads.
Interface	Hostname and port of the site server.
Replication Stat	If there is a parent site server present.

Note: You can choose the required site server from the drop-down.

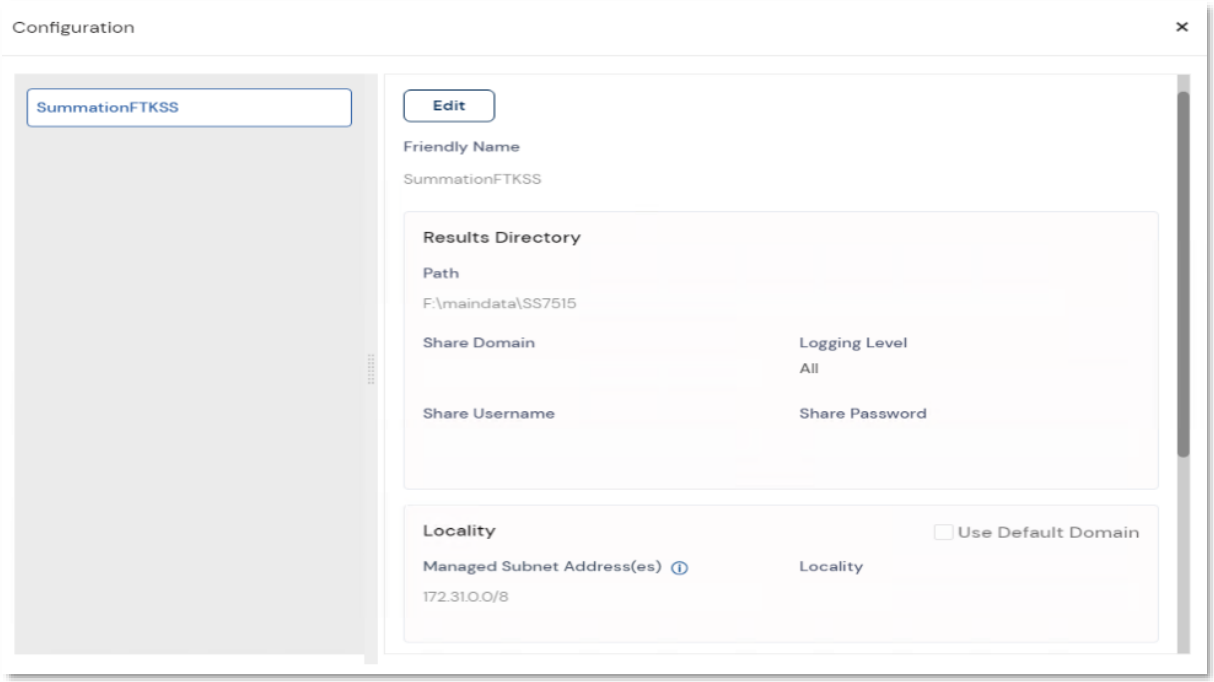


© Exterro, Inc. All rights reserved

Configuration

To configure the site servers:

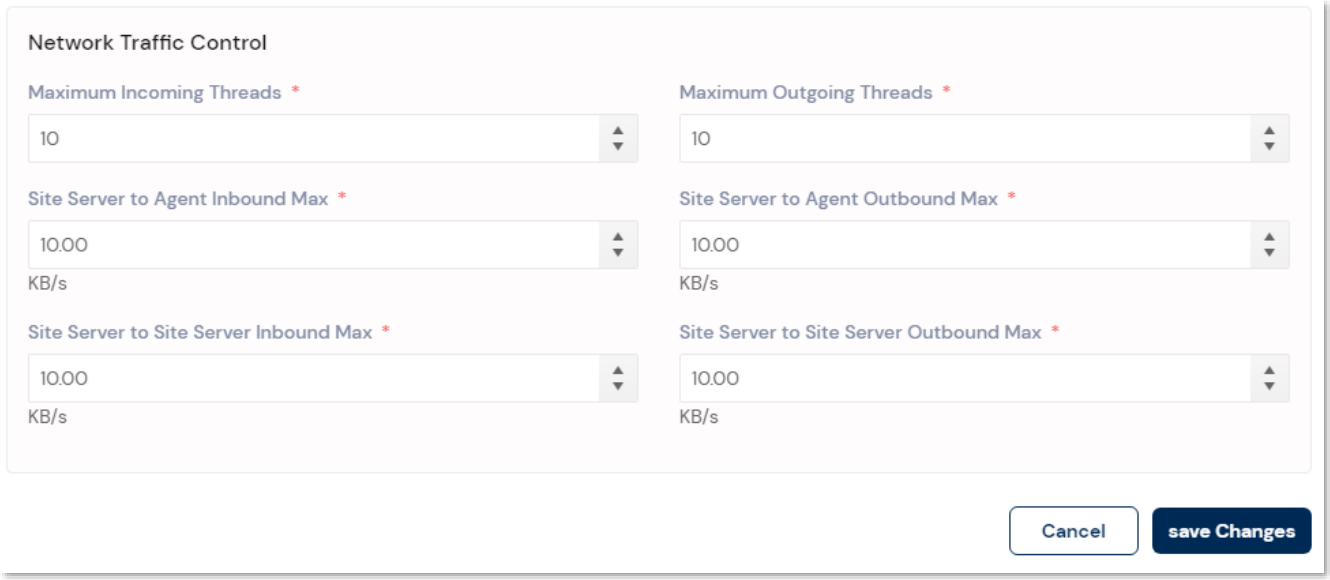
1. From the home page, click on Settings from the top-right corner.
2. Navigate to **System Management** tab from right pane.
3. Navigate to **Site Server Console** tab.
4. Click on the **Configuration** button .
   - The **Configuration** prompt is displayed.



5. Click **Edit**.

© Exterro, Inc. All rights reserved

6. Set the inbound and outbound limits for the agent's connection.



7. Make the necessary changes.
8. Click **Save Changes**.

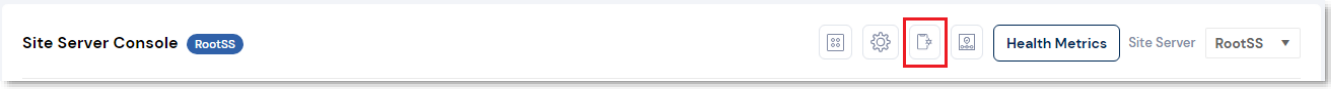
© Exterro, Inc. All rights reserved

Phone Home Settings

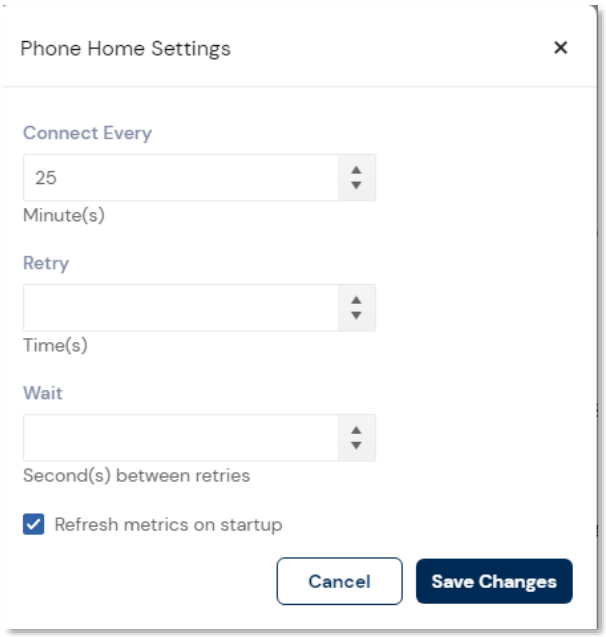
Phone Home allows you to configure interval checking between the agent and site server.

To configure home phoning settings:

1. From the home page, click on **Settings** from the top-right corner.
2. Navigate to **System Management** tab from right pane.
3. Navigate to **Site Server Console** tab.
4. Click on the **Phone Home Settings** button .



- The **Phone Home Settings** page is displayed.



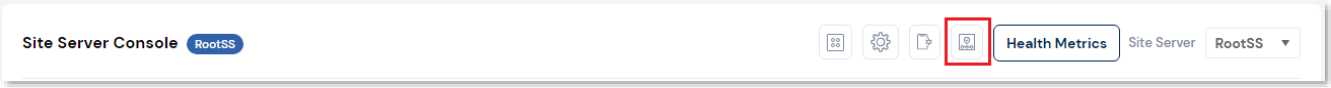
5. Select the minutes for **Connect Every** field.
6. Select the time to **Retry**.
7. Select the time in seconds to **Wait** between retries.
8. Enable the **Refresh metrics on startup** checkbox to refresh any endpoint metrics during App startup.
9. Click **Save Changes**.

© Exterro, Inc. All rights reserved

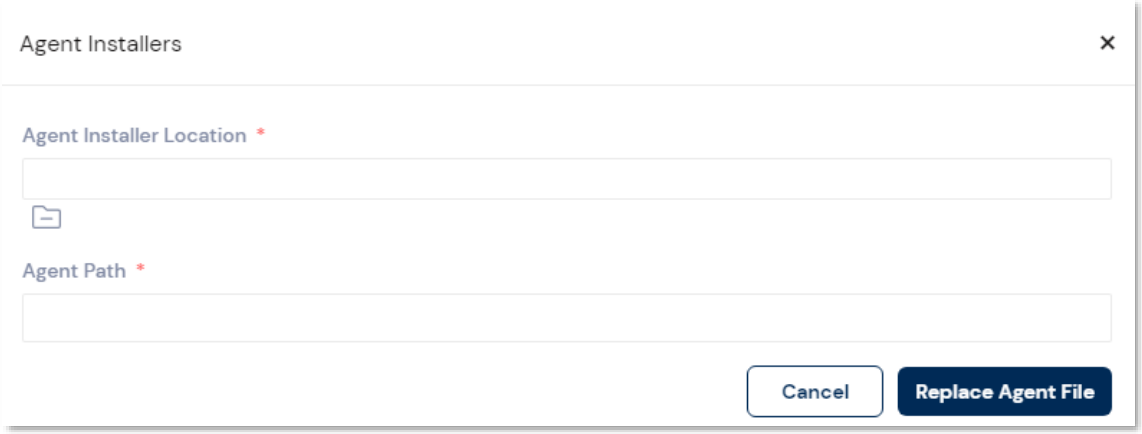
Agent Installer

To select the agent installer location:

1. From the home page, click on **Settings** from the top-right corner.
2. Navigate to **System Management** tab from right pane.
3. Navigate to **Site Server Console** tab.
4. Click on the **Agent Installers** button .



- The **Agent Installers** page is displayed.



5. Choose the **Agent Installer Location**.
6. Provide the **Agent Path**.
7. This can be within the "Agent" folder in the site server results directory.

   32-Bit installer location \x32\ AccessData Agent.msi
   64-Bit installer location \x64\ AccessData Agent (64-bit).msi

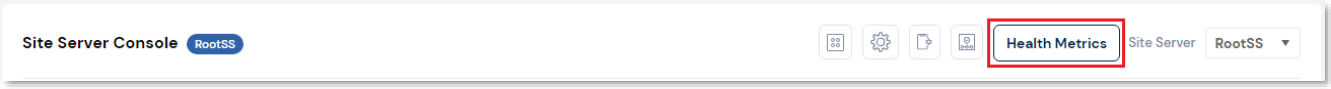
8. Click **Replace Agent File.**

© Exterro, Inc. All rights reserved

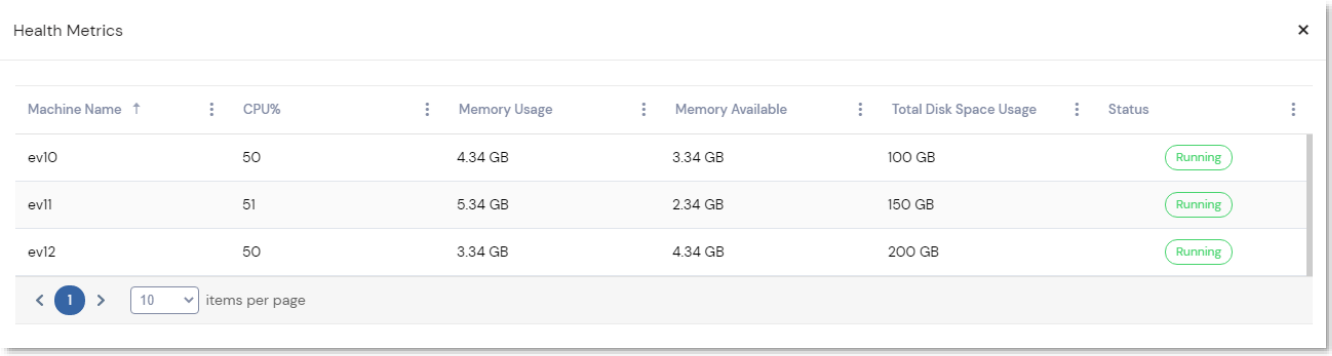
Health Metrics

To view the health metrics:

1. From the home page, click on **Settings** from the top-right corner.
2. Navigate to **System Management** tab from right pane.
3. Navigate to **Site Server Console** tab.
4. Click **Health Metrics**.



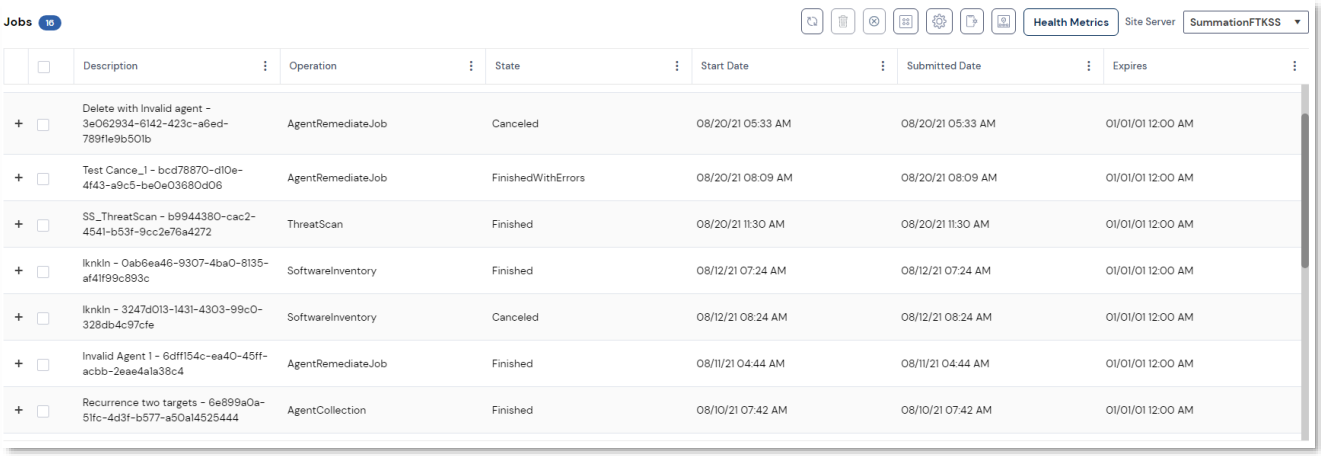
- The **Health Metrics** page is displayed.



© Exterro, Inc. All rights reserved

Jobs

To view jobs:



1. From the home page, click on **Settings** from the top-right corner.
2. Navigate to **System Management** tab from right pane.
3. Navigate to **Site Server Console** tab.
4. All jobs (All States) will be listed in the **Jobs Grid**.

Tip: Clicking the **Plus** + beside a job will expand the tasks to show which Site Server has sent the job as well as the targeted endpoint.

© Exterro, Inc. All rights reserved

System Log

Almost all major internal events occurring in the system are recorded in the System Log. This can be used in conjunction with the activity log to monitor the work and status of your system.

The following are examples of the types of events that are recorded:

- Completion of evidence processing for an individual case
- Exports started and finished
- Starting of internal services
- Job failures
- System errors
- Errors accessing computers and shares

You can filter the log information that is displayed based on the following different types of criteria:

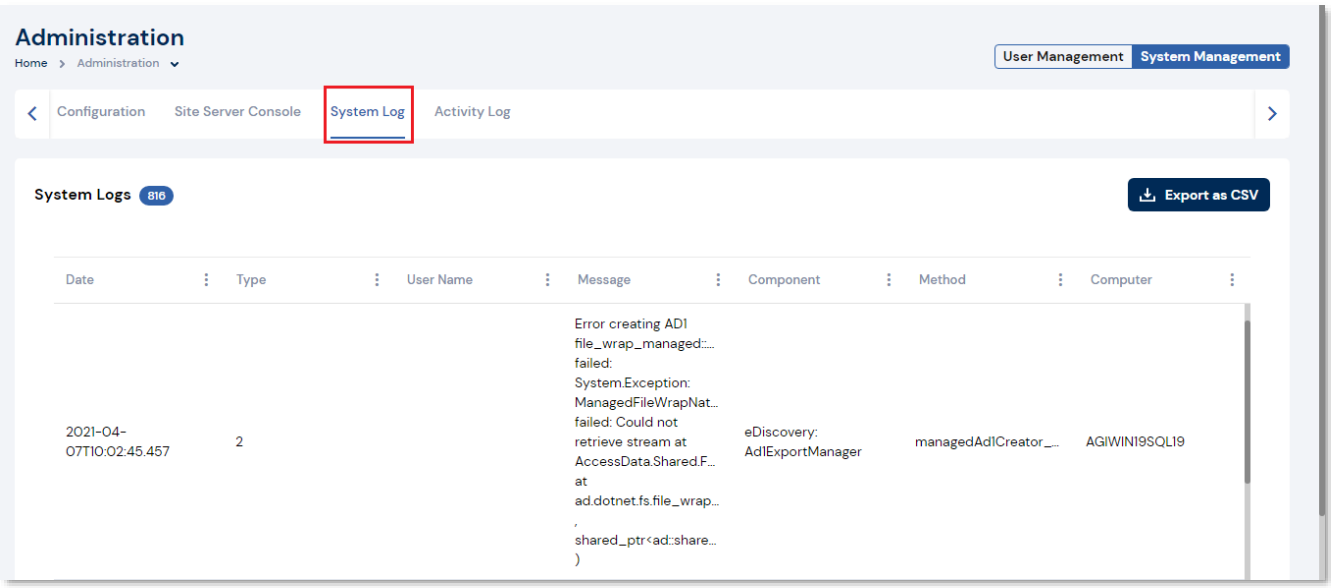
- Date and time of the log message
- Log type such as an error, information, or warning
- Log message contents
- Which component caused the log entry
- Which method caused the log entry
- Username
- Computer name

© Exterro, Inc. All rights reserved

Viewing System Log

To view the system logs:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to **System Management** tab from right pane.
3. Navigate to **System Log** tab.



Note: You can click **Export as CSV** and download the log in .csv format.

© Exterro, Inc. All rights reserved

Activity Log

When certain internal activities occur in the system, it is recorded in the Activity log. The Activity Log can help you detect and investigate attempted and successful unauthorized activity in the application and to troubleshoot problems. This can be used in conjunction with the System Log to monitor the work and status of your system.

The following are examples of the types of activities that are recorded:

- A user logged out
- A user is forced to log out due to inactivity
- Processing started on the case
- A case is opened

You can filter the log information that is displayed based on the following different types of criteria:

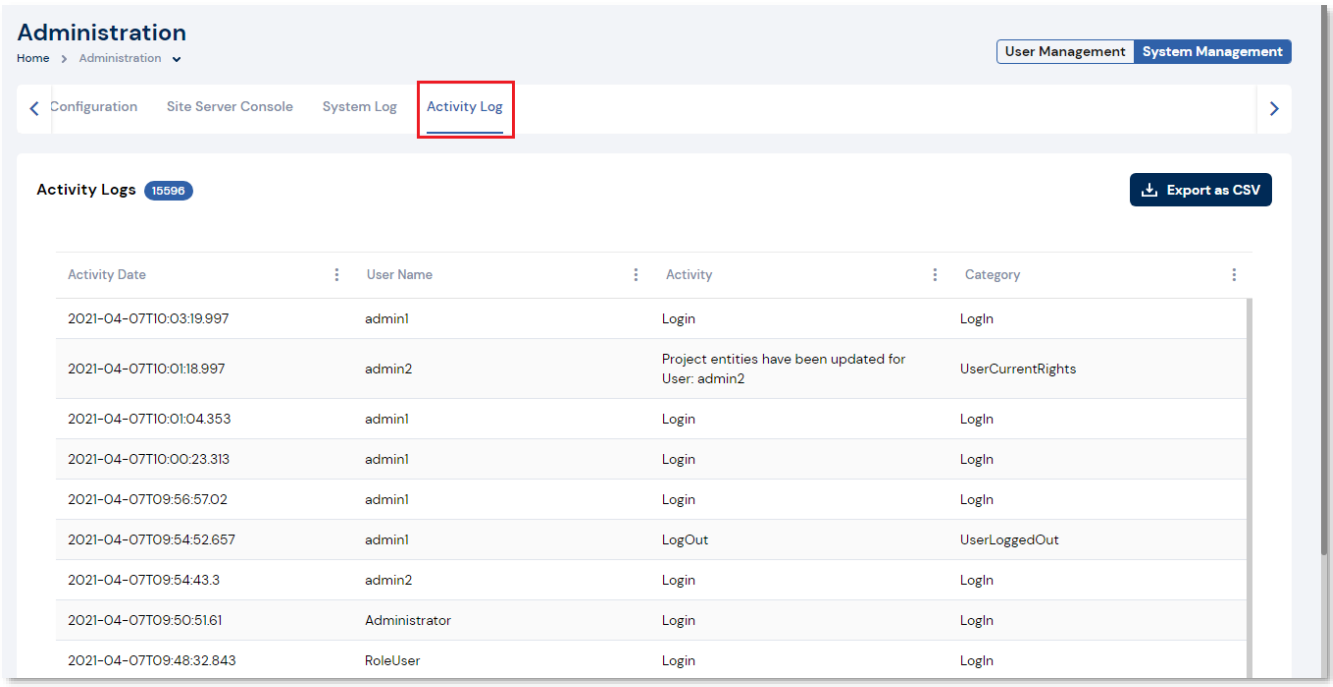
- Category
- Activity Date
- Activity
- Username

© Exterro, Inc. All rights reserved

Viewing Activity Log

To view the activity logs:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to **System Management** tab from right pane.
3. Navigate to **Activity Log** tab.



Note: You can click **Export as CSV** and download the log in .csv format.

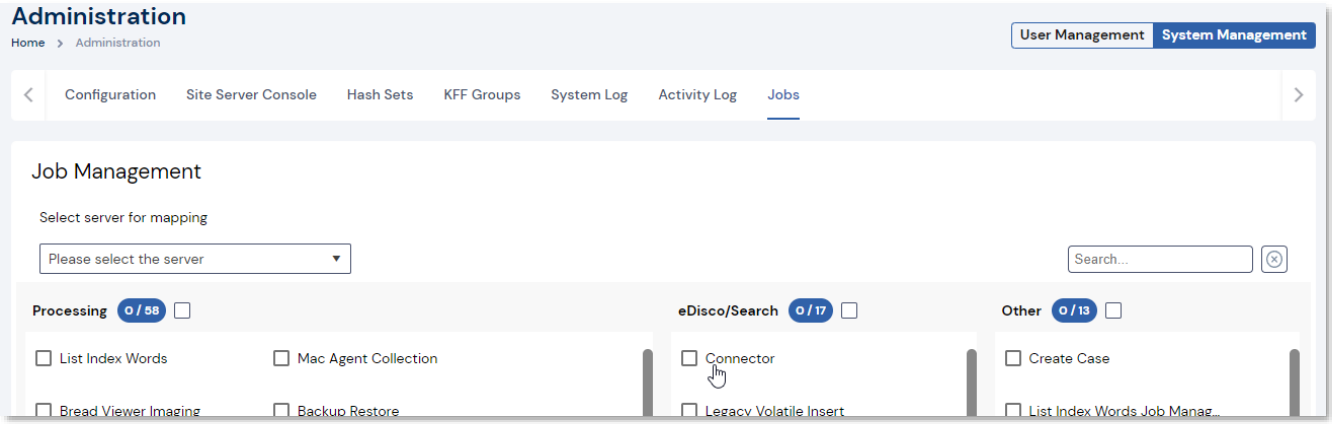
© Exterro, Inc. All rights reserved

Job Management

To map the jobs to a specific server:

Note: To use Job Management, you must have followed the steps in this KB article.

1. From the home page, click on the **Settings** button from the top-right corner.
   - The **Administration** page is displayed.



2. Navigate to the **System Management** tab.
3. Select the **Jobs** section.
4. Select a server from the drop-down list.
5. Check the required job categories from the following sections:
   - **Processing**
   - **eDisco/Search**
   - **Other**

Warning: If no job types are selected, all the jobs will be assigned by to a server.

6. Click **Associate Job(s) to server**.

© Exterro, Inc. All rights reserved

DPM DPE Configuration

Uploading and processing of evidence files in the FTK Central application is now greatly enhanced using the Distributed Processing Manager (DPM) and Distributed Processing Engine (DPE).

With this feature, you can create processing managers (DPM) each configured with multiple processing engines (DPE). You can use these engines to store huge volumes of data and process all the corresponding jobs at a faster rate, thereby increasing the efficiency.

Notes: You can check the status of the DPM DPE and the corresponding processing jobs from the Monitoring DPM and DPE section.

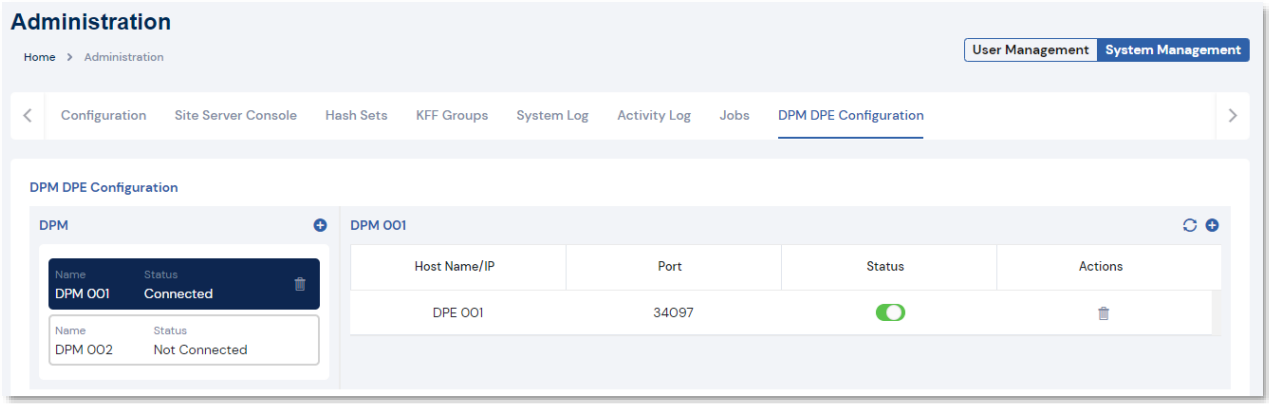
© Exterro, Inc. All rights reserved

Configuring the DPM DPE

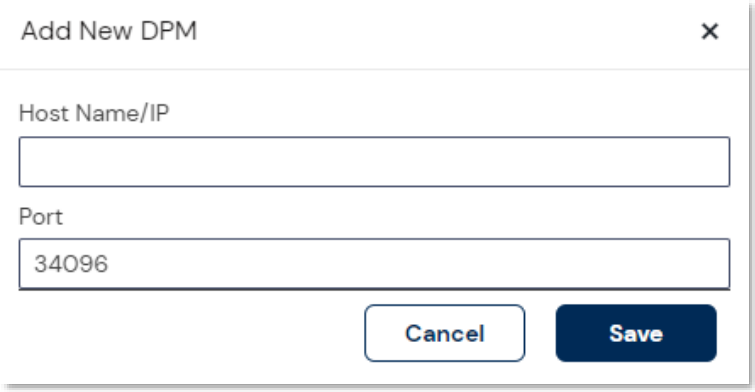
To configure the DPM and DPE:

1. From the home page, click on the **Settings** button from the top-right corner.
   - The **Administration** page is displayed.

2. Navigate to the **System Management** tab.
3. Select the **DPM DPE Configuration** section.



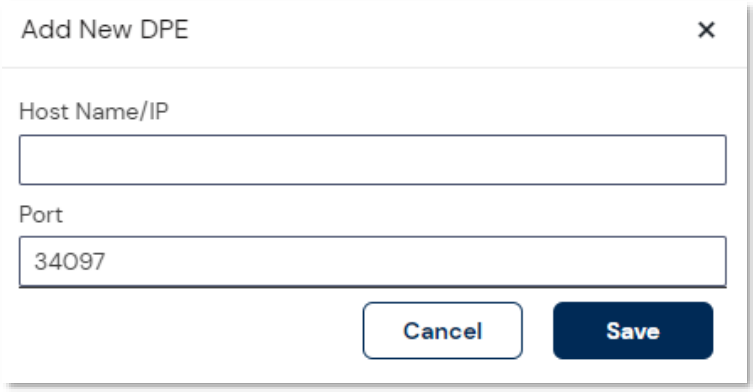
4. Click on the button against the **DPM** section.
   - The **Add New DPM** pop-up is displayed.



5. Enter the **Host Name/IP**.
6. Provide the **Port** number.
7. Click **Save**.

© Exterro, Inc. All rights reserved

8. Click on the button against the **DPE** section.
   - The **Add New DPE** pop-up is displayed.



9. Enter the **Host Name/IP**.
10. Provide the **Port** number.
11. Click **Save**.

Notes:

- You can click on the **Delete** button against the required DPM or DPE to delete it.
- You can click on the button against the **DPE** section to refresh the list of processing engines created.

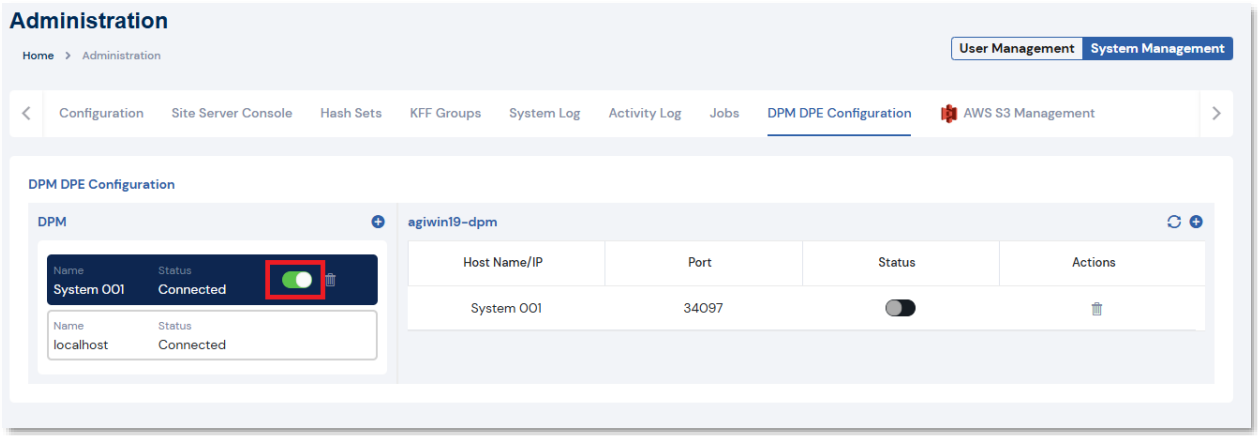
© Exterro, Inc. All rights reserved

Enabling/Disable the DPM

To enable/disable the DPM:

1. From the home page, click on the **Settings** button from the top-right corner.
   - The **Administration** page is displayed.

2. Navigate to the **System Management** tab.
3. Select the **DPM DPE Configuration** section.
4. Enable or disable the toggle against the required DPM to enable or disable the processing machine.



Notes: This option is not applicable for localhost DPM since it is the system's default processing manager and must always remain active.

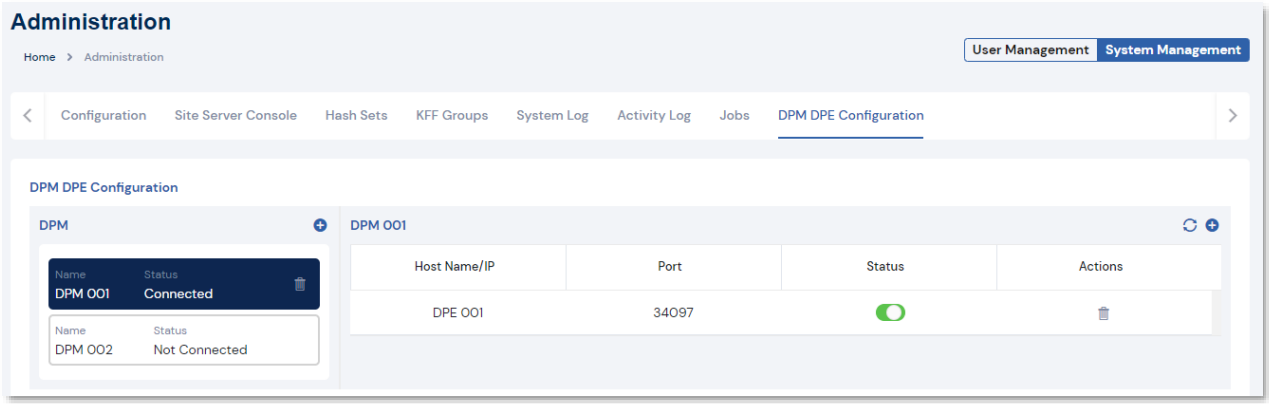
© Exterro, Inc. All rights reserved

Enabling/Disable the DPE

To enable/disable the DPE:

5. From the home page, click on the **Settings** button from the top-right corner.
   - The **Administration** page is displayed.

6. Navigate to the **System Management** tab.
7. Select the **DPM DPE Configuration** section.



8. Enable or disable the **Status** toggle against the required DPE to enable or disable the processing jobs associated with the corresponding DPE.

© Exterro, Inc. All rights reserved

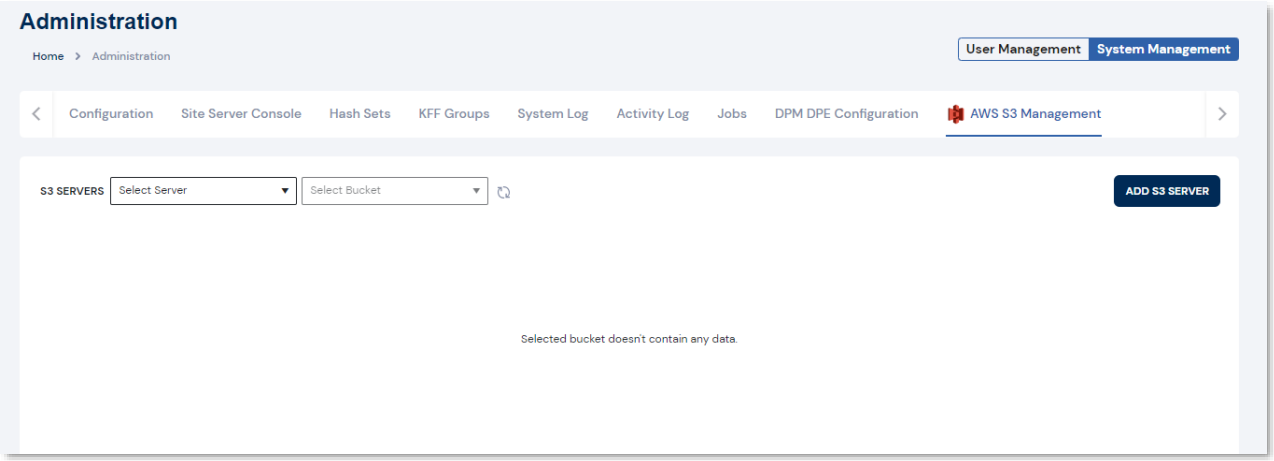
AWS S3 Management

You can now effectively store and manage all your files and folders in the Amazon Web Services (AWS) S3 buckets directly within the FTK Central application using the **AWS S3 Management** section. From this section you can directly upload, download, and delete files/folders in the AWS S3 bucket.

To view the files in AWS S3 buckets:

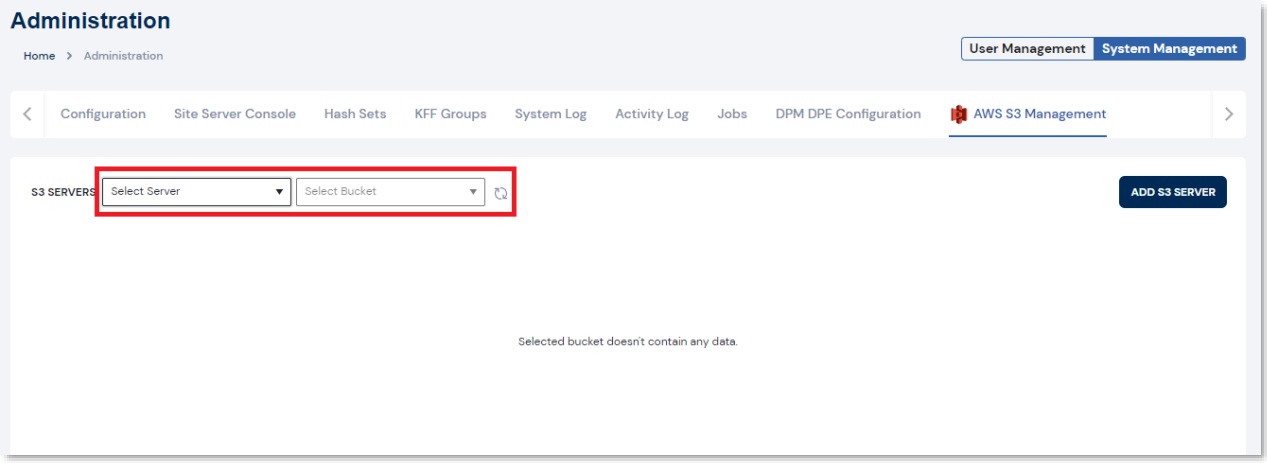
1. From the home page, click on the **Settings** button from the top-right corner.
   - The **Administration** page is displayed.

2. Navigate to the **System Management** tab.
3. Select the **AWS S3 Management** section.

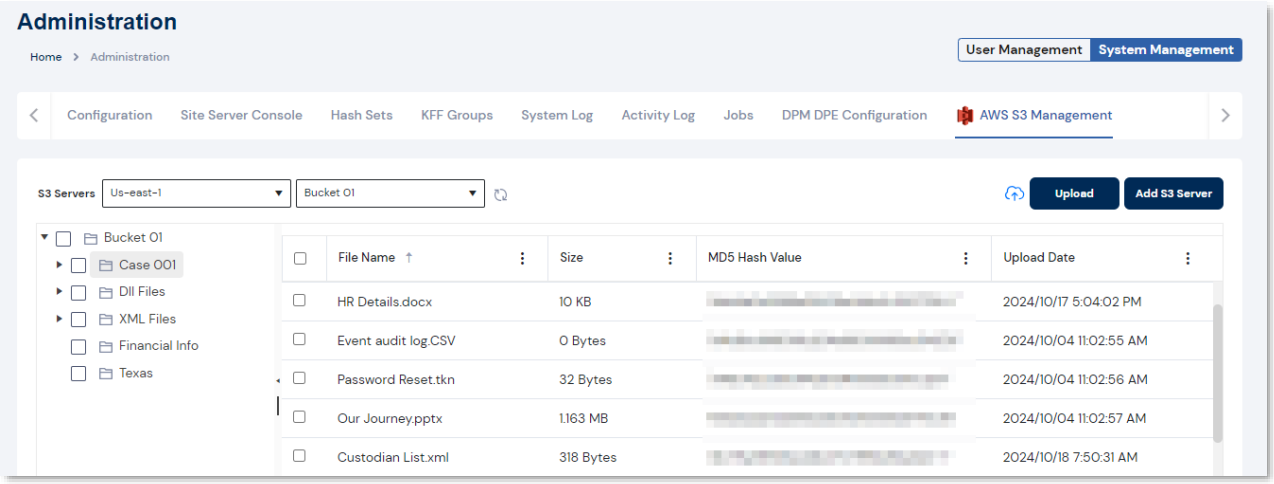


© Exterro, Inc. All rights reserved

4. Select the S3 Server and bucket from the **S3 Servers** drop-down.



- All the files and folders present in the selected bucket will be displayed.

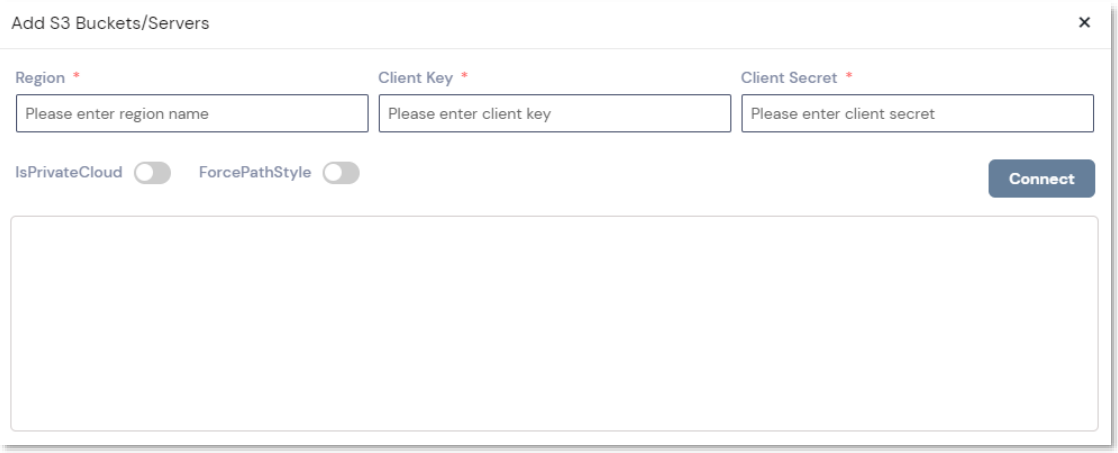


© Exterro, Inc. All rights reserved

Adding S3 Servers

To add the S3 servers:

1. From the **AWS S3 Management** section, click on the **Add S3 Server** button.
   - The **Add S3 Buckets/Servers** pop-up is displayed.



2. Provide the AWS **Region**.

Region Name	Technical ID (Input this as your 'Region')
US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Canada (Central)	ca-central-1
Canada West (Calgary)	ca-west-1
Mexico (Central)	mx-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europe (Paris)	eu-west-3
Europe (Frankfurt)	eu-central-1
Europe (Zurich)	eu-central-2
Europe (Stockholm)	eu-north-1
Europe (Milan)	eu-south-1
Europe (Spain)	eu-south-2
Asia Pacific (Tokyo)	ap-northeast-1

© Exterro, Inc. All rights reserved

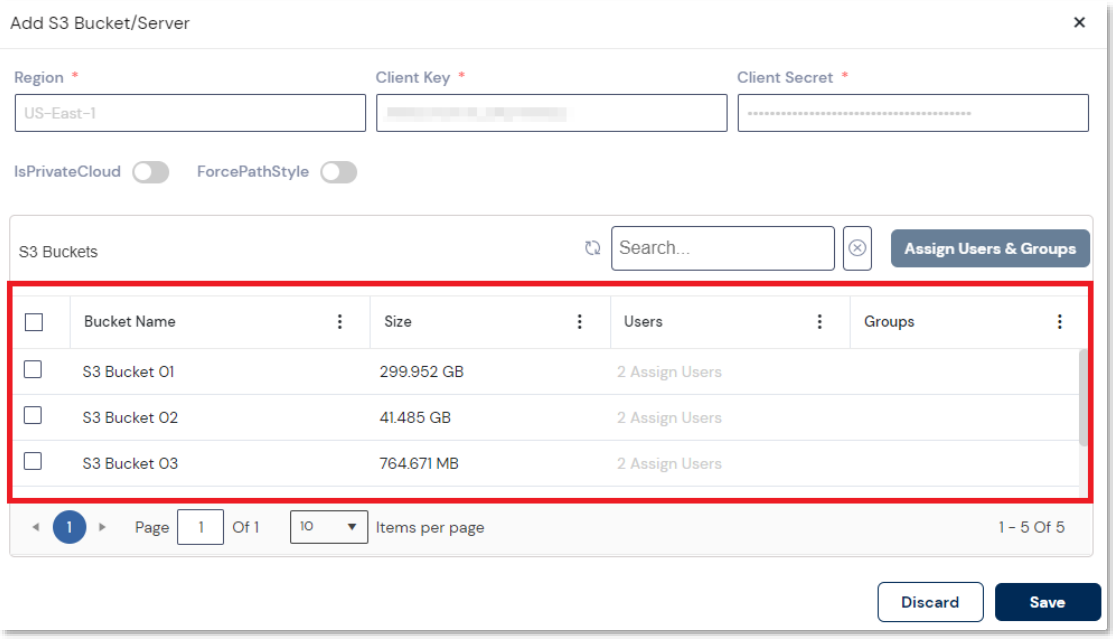
Region Name	Technical ID (Input this as your 'Region')
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Osaka)	ap-northeast-3
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Hyderabad)	ap-south-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Jakarta)	ap-southeast-3
Asia Pacific (Melbourne)	ap-southeast-4
Asia Pacific (Malaysia)	ap-southeast-5
Asia Pacific (New Zealand)	ap-southeast-6
Asia Pacific (Thailand)	ap-southeast-7
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Taipei)	ap-east-2
Middle East (Bahrain)	me-south-1
Middle East (UAE)	me-central-1
Middle East (Saudi Arabia)	me-south-2
Israel (Tel Aviv)	il-central-1
Africa (Cape Town)	af-south-1
South America (São Paulo)	sa-east-1
AWS GovCloud (US-East)	us-gov-east-1
AWS GovCloud (US-West)	us-gov-west-1
China (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1

3. Provide the **Client Key.**
4. Provide the **Client Secret**.
5. Enable the below options if required:
   - **Is Private Cloud** – Should be enabled if the bucket/server is hosted in a private cloud.
   - **Force Path Style** – This field is accessible only when the **Is Private Cloud** option is enabled.

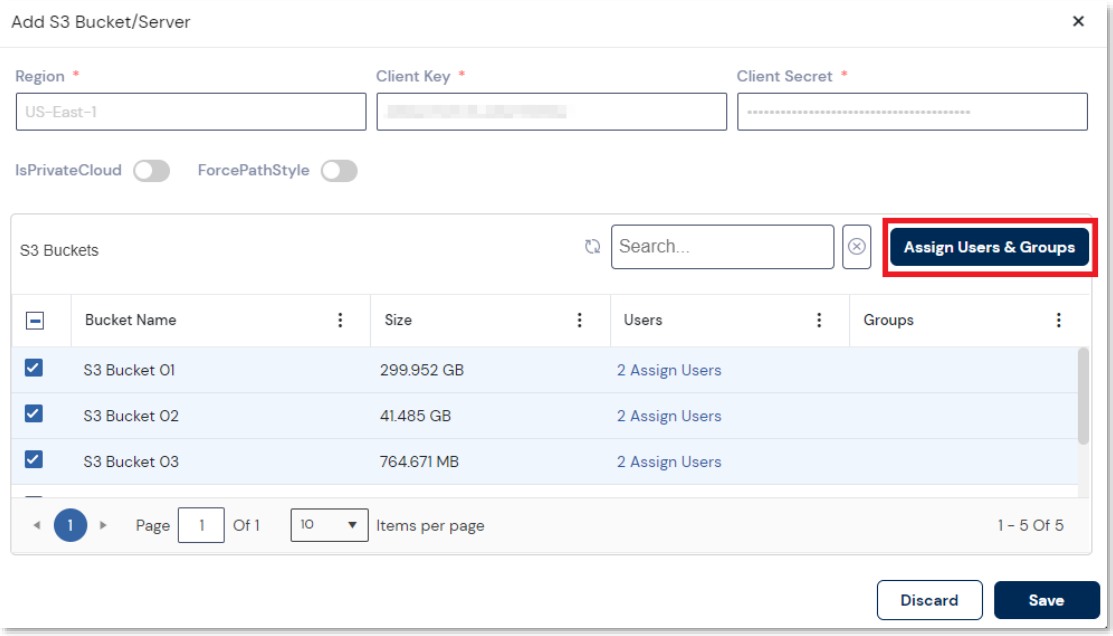
6. Click on **Connect**.

© Exterro, Inc. All rights reserved

- Upon clicking on **Connect**, the AWS S3 buckets available for the provided region and credentials will be displayed.

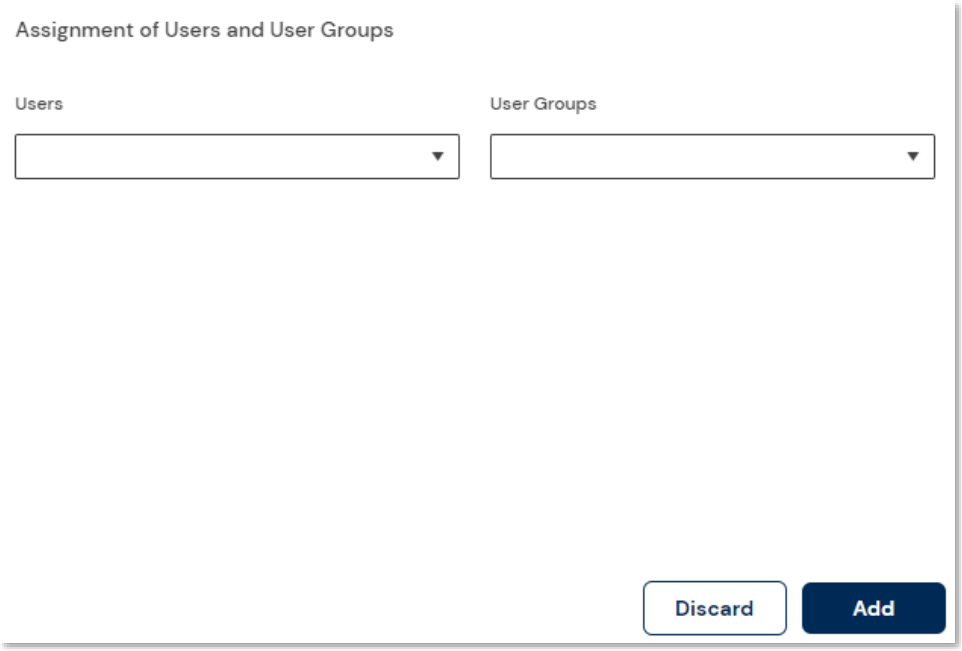


7. Select the required S3 buckets and click on **Assign Users & Groups**.



© Exterro, Inc. All rights reserved

- The **Assignment of Users and User Groups** pop-up is displayed.



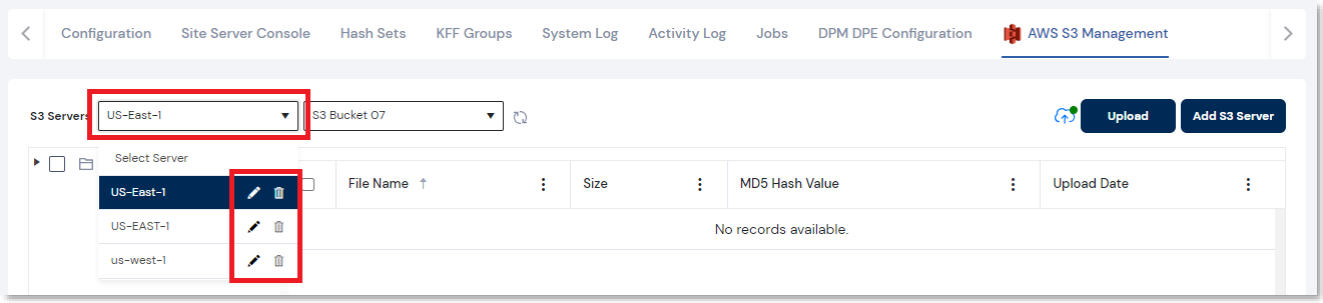
8. Select the required **Users** and **User Groups** from the corresponding dropdowns and click **Add**.
   - The users and groups will be assigned to the selected S3 buckets.

9. Click **Save**.

The buckets will be saved and displayed in the **AWS S3 Management** section.

© Exterro, Inc. All rights reserved

Note: You can edit or delete the S3 buckets by clicking on the **Edit** or **Delete** icon displayed against the servers in the **S3 Server** drop-down.

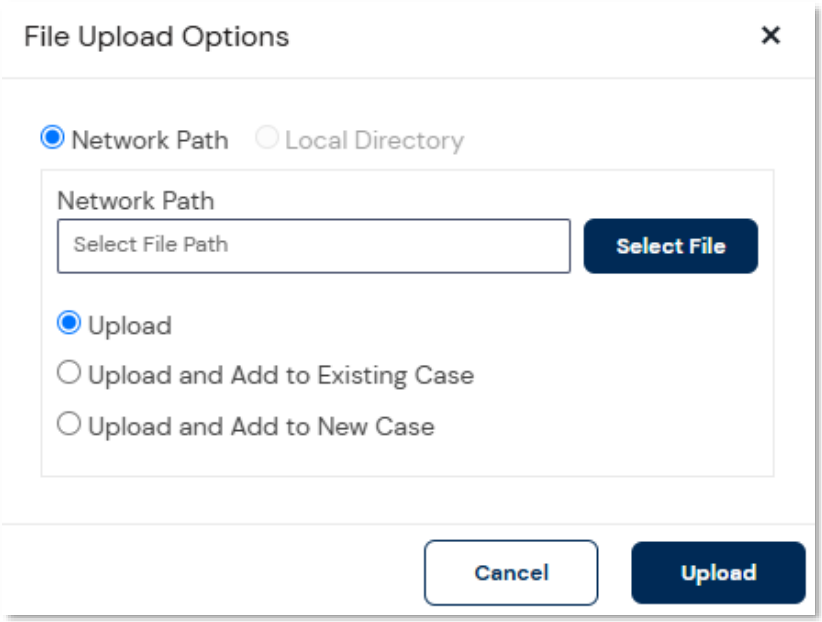


© Exterro, Inc. All rights reserved

Uploading Files into S3 Servers

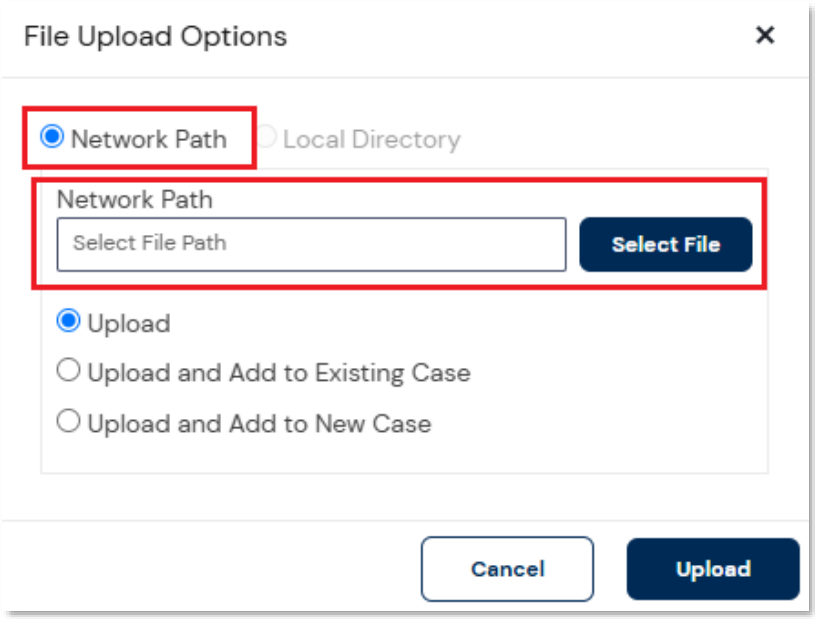
To upload files into the S3 server:

1. From the **AWS S3 Management** section, click on the **Upload** button.
   - The **File Upload Options** pop-up is displayed.

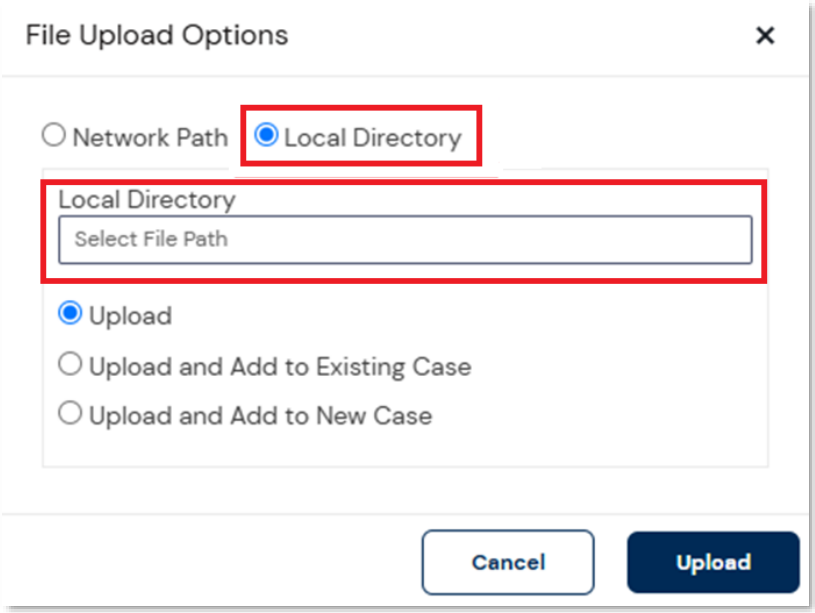


© Exterro, Inc. All rights reserved

2. Select any one of the below options:
   - **Network Path** – To upload files and folders present in the network path.



   - **Local Directory** – To upload files and folders from your local machine.

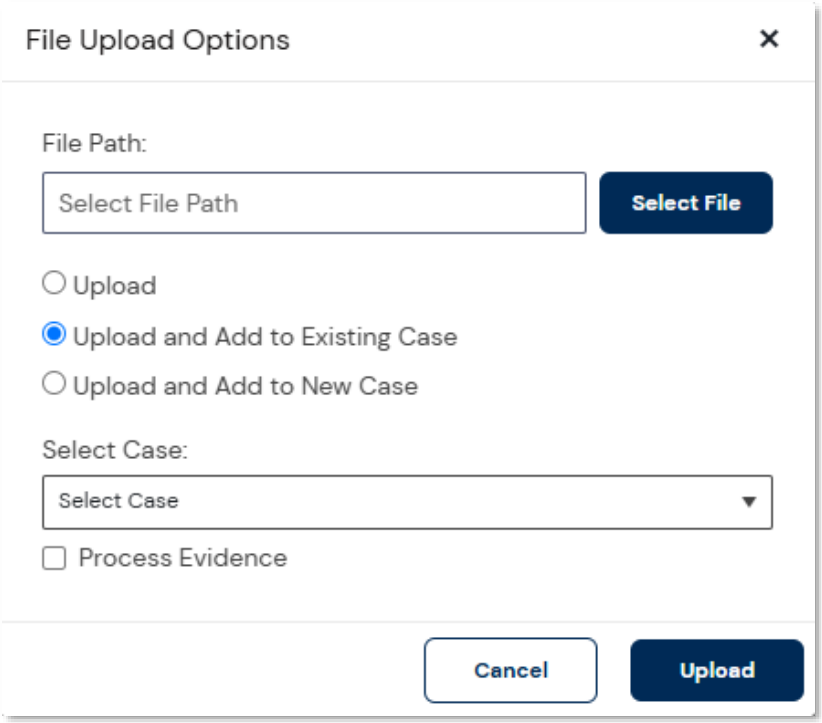


© Exterro, Inc. All rights reserved

Notes:

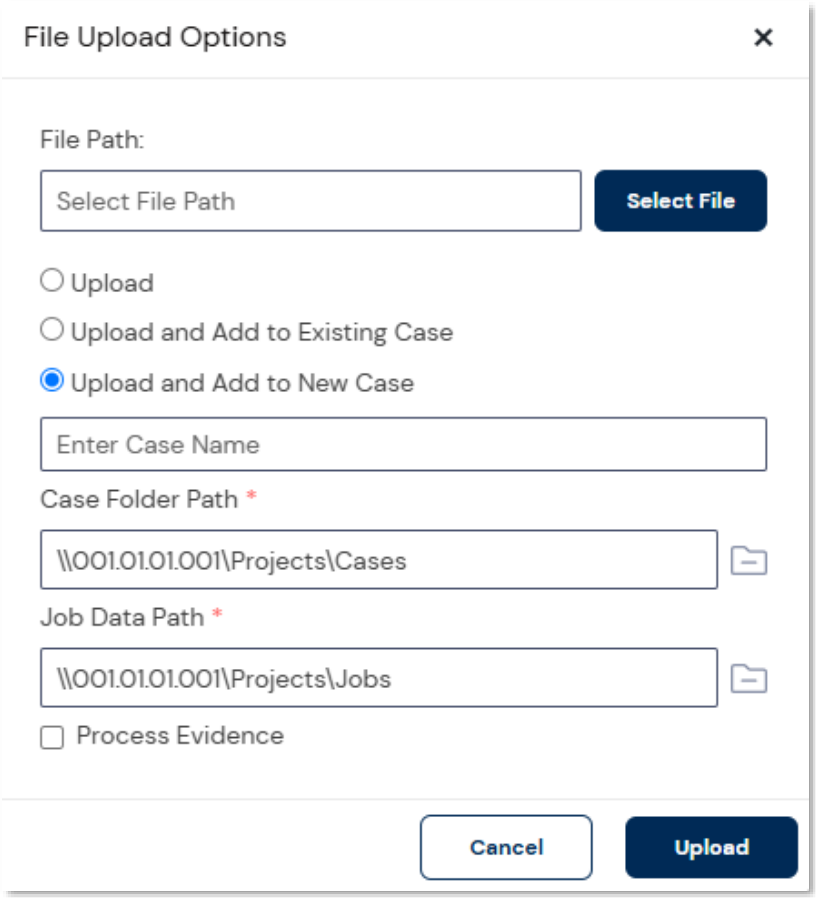
- The **Local Directory** option will be enabled only when the **Exterro AWS Service** is installed in your machine. Refer to the **FTK 8.2 SP1 Installation Guide** for more details
- The files/folders will be uploaded into the selected folder of the bucket. If the bucket itself is selected, the files/folders will be uploaded in the bucket's root.

3. Select any one of the upload options:
   - **Upload** – To upload the files into the AWS S3 bucket.
   - **Upload and Add to Existing Case** – To upload the files into the AWS S3 bucket and add them to case present in the FTK Central application. When this option is selected, a case should be selected from the **Select Case** drop-down.



© Exterro, Inc. All rights reserved

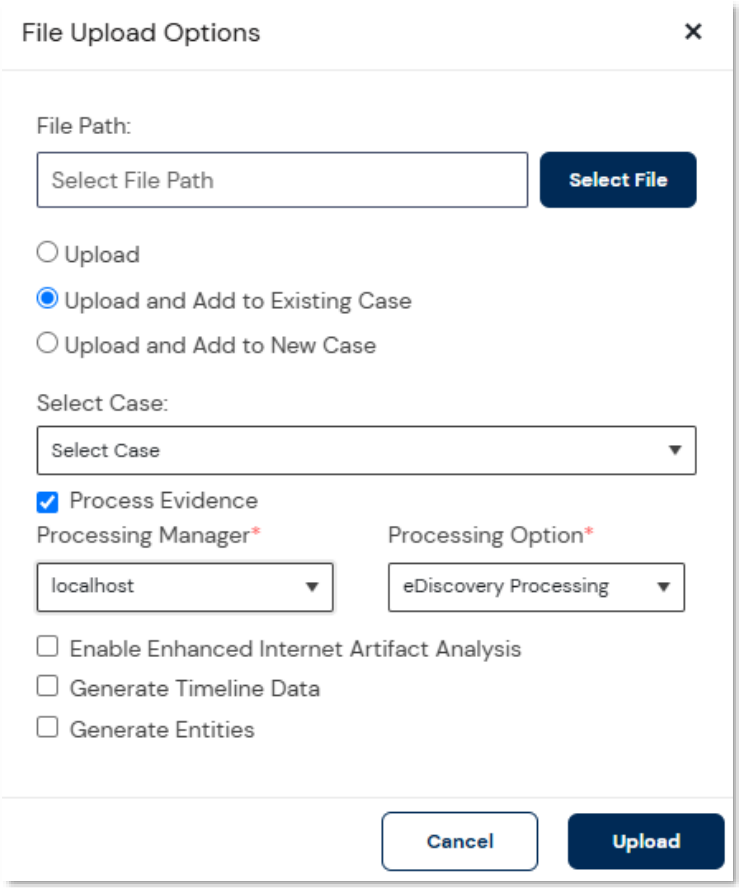
- **Upload and Add to New Case** – To upload the files into the AWS S3 bucket, create a new case, and add the uploaded files to the case. When this option is selected, you should provide the **Case Name**, **Case Folder Path**, and **Job Data Path** to create the case.



© Exterro, Inc. All rights reserved

4. Enable the **Process Evidence** option to initiate the evidence processing operation for the files being added to the case. Upon enabling this option, the following fields will be displayed to configure the corresponding information:

- **Processing Manager** – Select the server in which the processing should be performed.
- **Processing Option** – Select the type of file processing option.
- **Generate Timeline Data** - To automatically generate the timeline data in the **Timeline View** of Review page.
- **Enable Enhanced Internet Artifact Analysis** – To categorize and display the information collected from browsers. The categorization will be displayed under the **Web Page Category** section of **Internet and Browser** filter.
- **Generate Entities** – To automatically identify and categorize entities from the case files including details such as phone numbers, email addresses, and social media profiles. This information can be viewed from the **Entity Management Dashboard** in the Review page.



© Exterro, Inc. All rights reserved

Note: When the **Process Evidence** option is enabled, the files being added to the case (existing or new) will be directly stored in both the AWS S3 location and the corresponding case's evidence location.

When the option is disabled, the files will be stored in only in the AWS S3 location. These files will be moved to the evidence location only after initiating the evidence processing from the corresponding case.

5. Click **Upload**.

Notes:

- If encrypted evidence is uploaded from the **Network Share** and added to a new or existing case, an additional pop-up intended for decryption will be displayed. Refer to the Evidence Decryption section for more details.
- If encrypted evidence is uploaded from the **Local Directory** and added to a new or existing case, the evidence will be listed in the **Encrypt Evidence List** pop-up (can be accessed by clicking on the icon present across the application).

  You can click on the icon against the required evidence to decrypt it. Refer to the Evidence Decryption section for more details.

The selected files will be uploaded into the corresponding AWS S3 bucket.

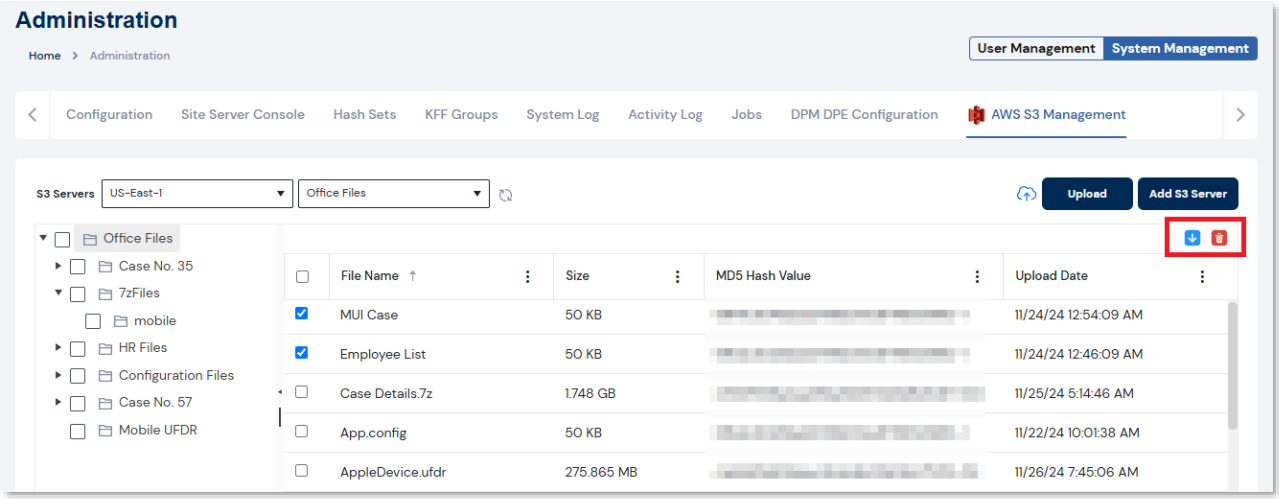
© Exterro, Inc. All rights reserved

Downloading files/folders from the S3 Servers

To download the files/folders from the S3 Servers:

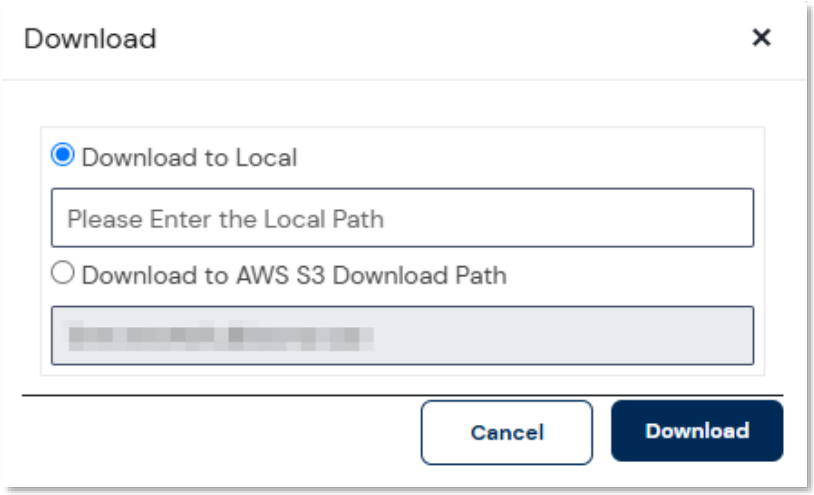
1. Select the required files and folders.

   - The **Download** button will be displayed only upon selecting the files/folders.



2. Click on the **Download** button.

   - The **Download** pop-up is displayed.



© Exterro, Inc. All rights reserved

3. Select any one of the below provided download options:
   - **Download to Local** – To download the selected files or folders into your local machine.
   - **Download to AWS S3 Download Path** – To download the selected files or folders into the preconfigured network path.

Notes: The **Download to Local** option will be enabled only when the **Exterro AWS Service** is installed in your machine. Refer to the **FTK 8.2 SP1 Installation Guide** for more details.

4. Click on **Download** to perform the action.

The selected files or folders will be downloaded into the selected location.

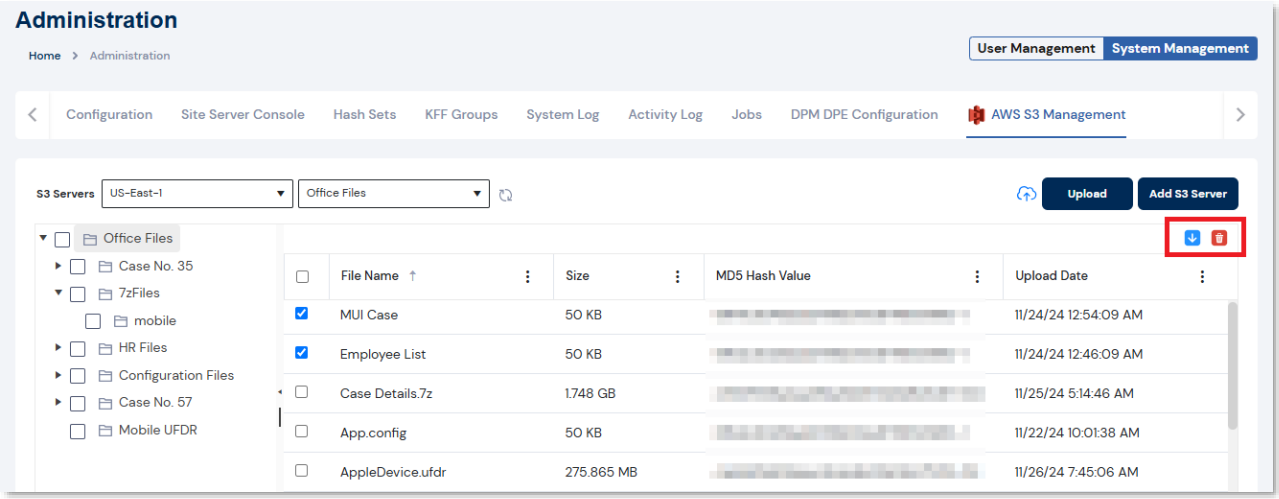
© Exterro, Inc. All rights reserved

Deleting files/folders from the S3 Servers

To delete the files/folders from the S3 Servers:

1. Select the required files and folders.

   - The **Delete** button will be displayed only upon selecting the files/folders.



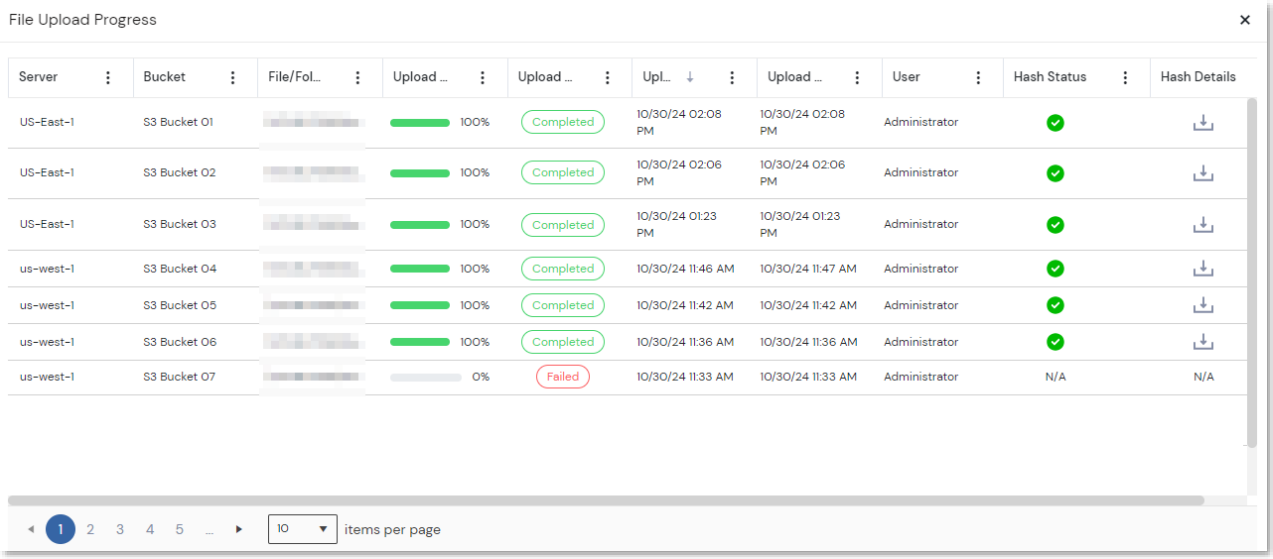
2. Click on the **Delete** button to delete the selected files and folders.

© Exterro, Inc. All rights reserved

Upload Progress and Hash Verification

File Upload Progress:

You can click on the **File Upload Progress** button from the AWS S3 Management section to view the progress of all the files and folders being uploaded to the corresponding AWS S3 buckets.



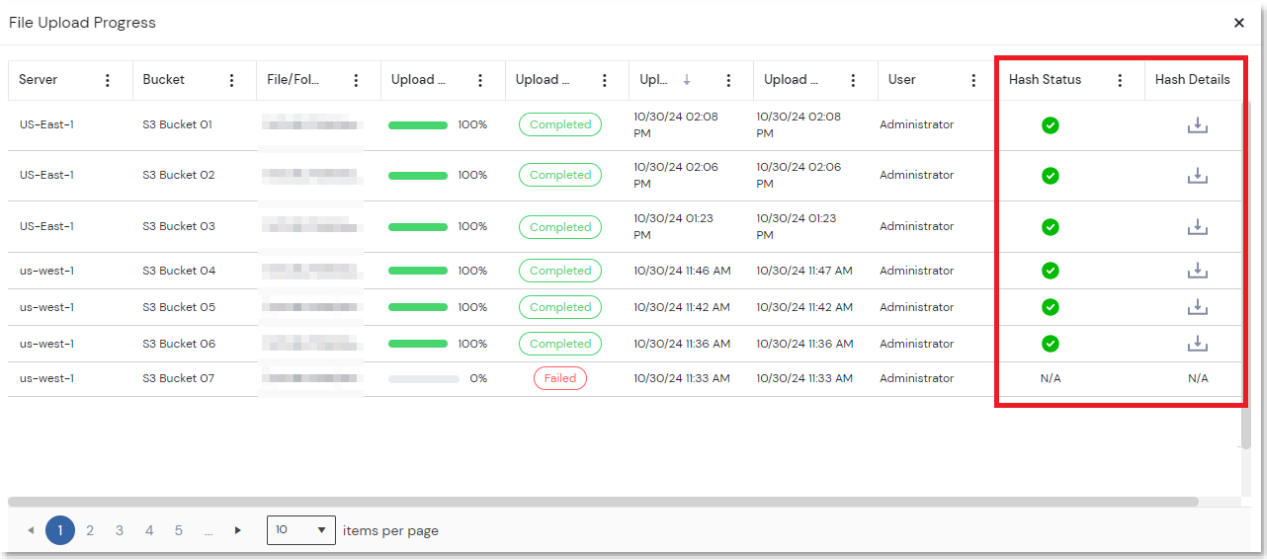
Note: This section also displays the status of cases backed up on AWS S3 location. For such cases, the **Files/Folders Name** column will display the temporary location when the upload is in-progress. However, upon completing the upload process, the original file name will be displayed in the **Files/Folders Name** column.

© Exterro, Inc. All rights reserved

Hash Verification:

The Hash verification is used to ensure the integrity of the files and folders being uploaded into the AWS S3 bucket. You can verify the hashes of the uploaded files and folders using the following columns displayed in the **File Upload Progress** pop-up.

- **Hash Status** – Indicate whether the hash verification of the files/folders uploaded to the corresponding S3 bucket was successful or not.
- **Hash Details** – To download and view the CSV file consisting of the hash values of the uploaded files/folders.



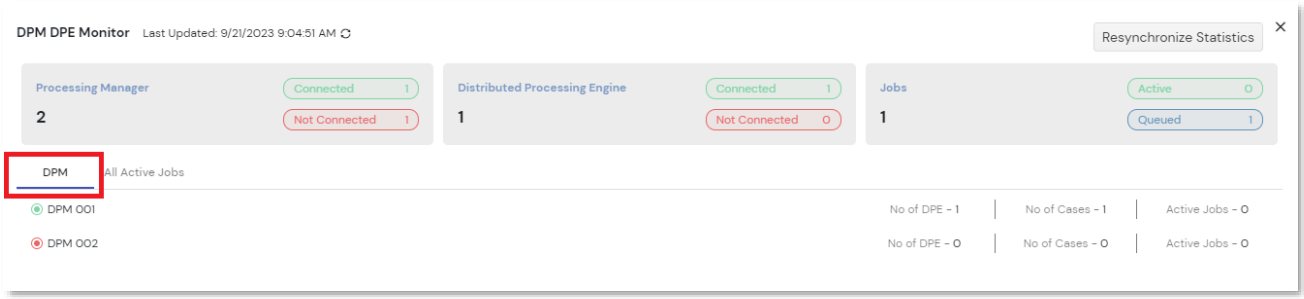
© Exterro, Inc. All rights reserved

Monitoring DPM and DPE

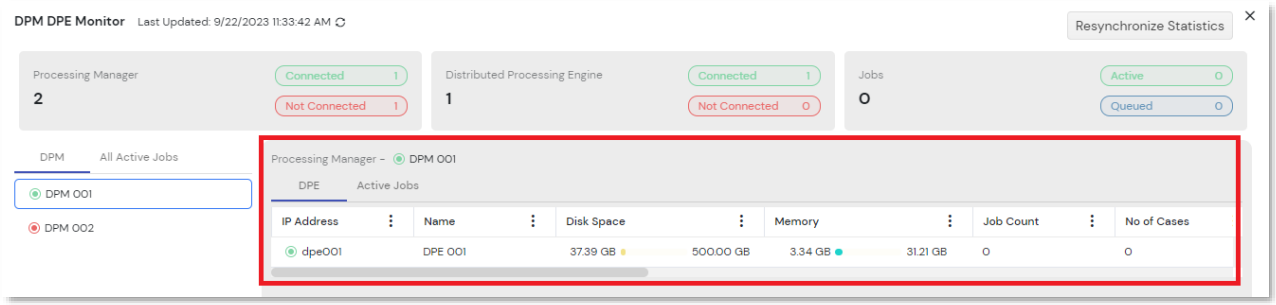
This section provides you with the total number of DPM and DPE present in the application along with the corresponding associated job statuses.

To monitor the DPM and DPE:

1. From the home page, click **Case List**.
2. Click the **DPM DPE Monitor** button from the top-right corner.
   - The **DPM DPE Monitor** pop-up is displayed which lists the DPM configured in the application (under **DPM** tab).



3. Click on the required DPM to view the associated DPE.



Notes:

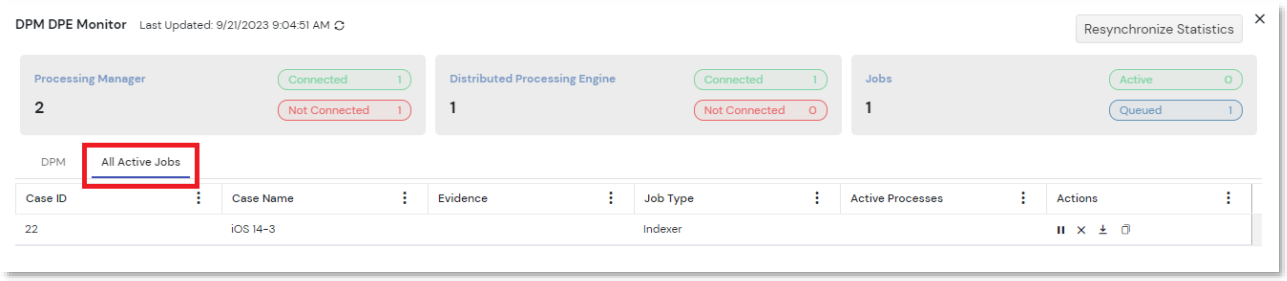
- You can click on to refresh the DPM details.
- You can click on Resynchronize Statistics to refresh the DPM associated job details.

© Exterro, Inc. All rights reserved

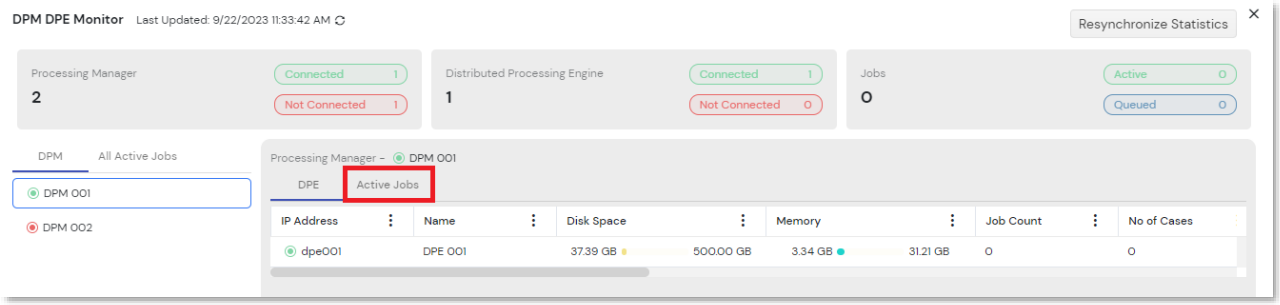
DPM DPE Associated Jobs

To view the jobs associated with DPM DPE:

1. From the home page, click **Case List**.
2. Click the **DPM DPE Monitor** button from the top-right corner.
   - The **DPM DPE Monitor** pop-up is displayed.
3. For DPM, click on **All Active Jobs** tab against the **DPM** tab to view the status of all the jobs associated with the DPM.



4. For DPE, click on the **Active Jobs** tab from the **Processing Manager** section to view the jobs associated with the DPE.



Note: When DPM or DPE service is turned down, restarted, or the machine is shut down and restarted, the job will be marked as **Failed** until the service or machine is restored.

© Exterro, Inc. All rights reserved

Note: You can click on the following icons against the required job to perform the corresponding operations:

- - To pause the job.
- - To cancel the job.
- - To download the job's log.
- - To copy the job path.

© Exterro, Inc. All rights reserved

Monitoring Processing Jobs

This section allows you to view and monitor the jobs performed on a case. You can view the list of jobs available for a case and also delete the jobs from this page.

Viewing Jobs

Tip: To filter the grid efficiently, you can simply enter a keyword into the search box

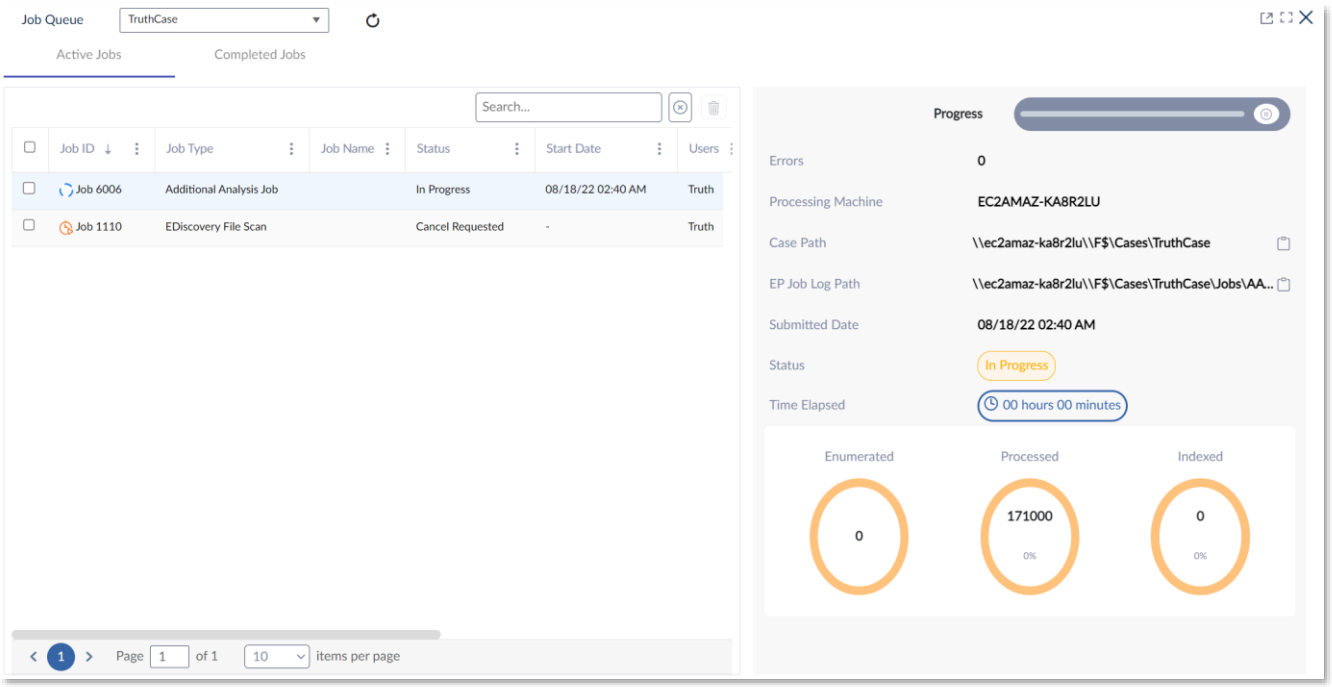
located at the top of any grid and click the search button or press enter.

© Exterro, Inc. All rights reserved

Active Jobs

To view the active job:

1. From the home page, click **Case List**.
2. Click the button from the top-right corner.
   - The **Job Queue** pop-up is displayed with the list of active jobs globally.



3. Select the required case from the drop-down box against **Job Queue**.
   - The active jobs of the selected case are displayed.

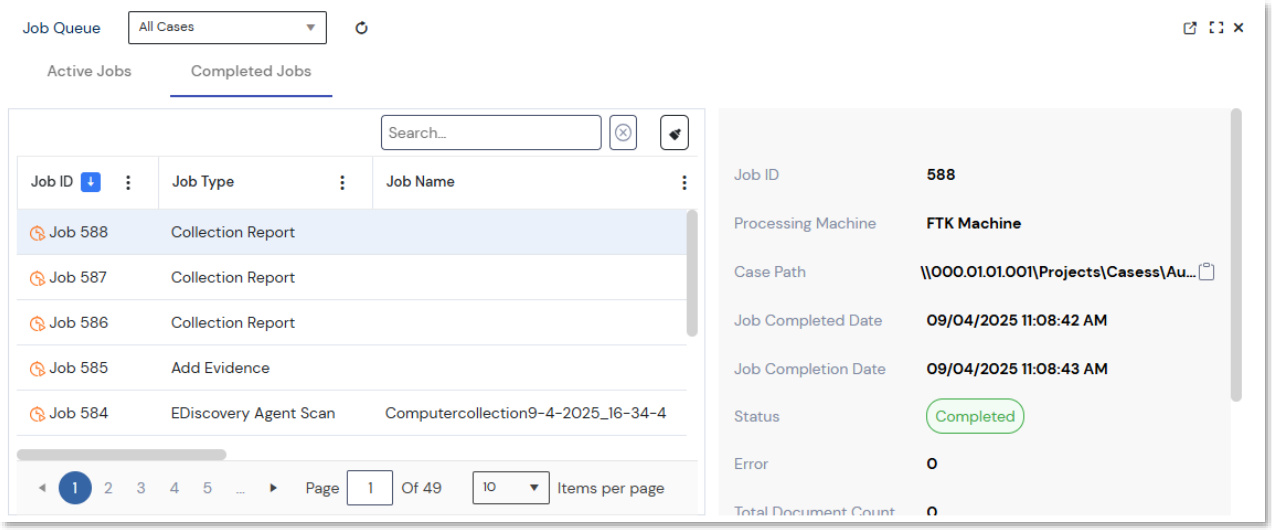
© Exterro, Inc. All rights reserved

Completed Jobs

Completed jobs will any jobs that are completed across the application. Additionally, any errors relating to a job will be indicated, with the number of errors within a job being listed. Users can toggle to view additional columns within Review mode to view errors related to a specific file using the **HasProcessingError** and **ProcessErrorDescription** columns.

To view the completed jobs:

1. From the home page, click **Case List**.
2. Click the button from the top-right corner.
3. Click **Completed Jobs**.
    - The list of completed jobs is displayed.



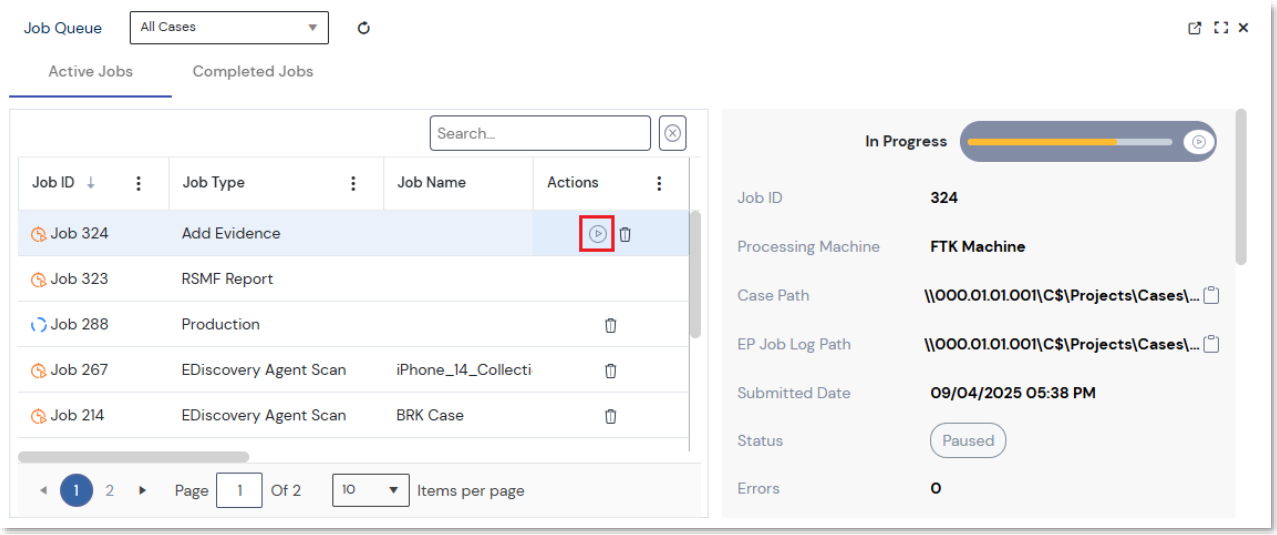
4. Select the required case from the drop-down box against **Job Queue**.
5. Click the required job.
    - The corresponding status details of the job is displayed in the right pane.

© Exterro, Inc. All rights reserved

Pausing/Resuming Jobs

To pause or resume the active job:

1. From the home page, click **Case List**.
2. Click the button from the top-right corner.
   - The **Job Queue** pop-up is displayed with the list of active jobs.
3. Click on the **Pause** or **Resume** button displayed against the required job (in the **Actions** column) to perform the corresponding action.

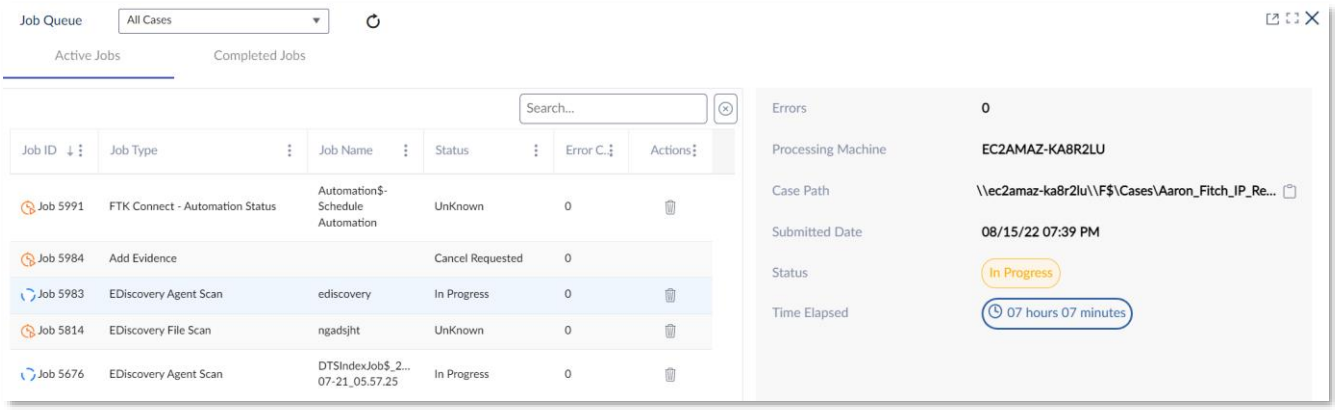


© Exterro, Inc. All rights reserved

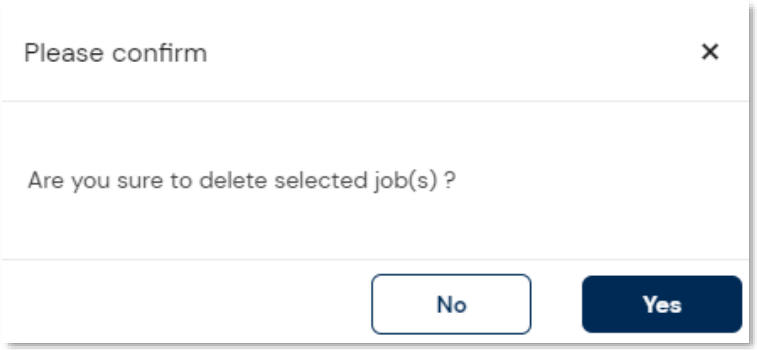
Deleting Jobs

To delete the active job:

1. From the home page, click **Case List**.
2. Click the button from the top-right corner.
   - The **Job Queue** pop-up is displayed with the list of active jobs.



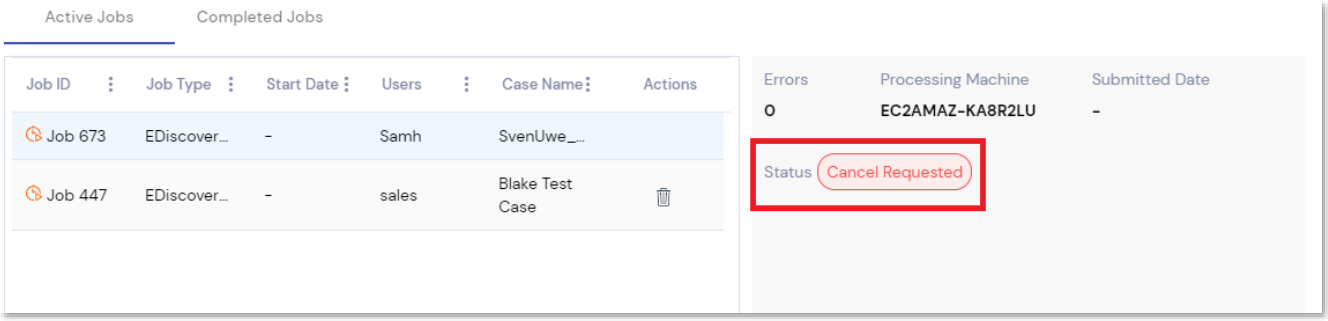
3. Click on the **Delete** button.
   - The **Please confirm** pop-up is displayed.



4. Click **Yes**.

© Exterro, Inc. All rights reserved

- The job will be stopped and the status of the job will be updated as **Cancel Requested**.



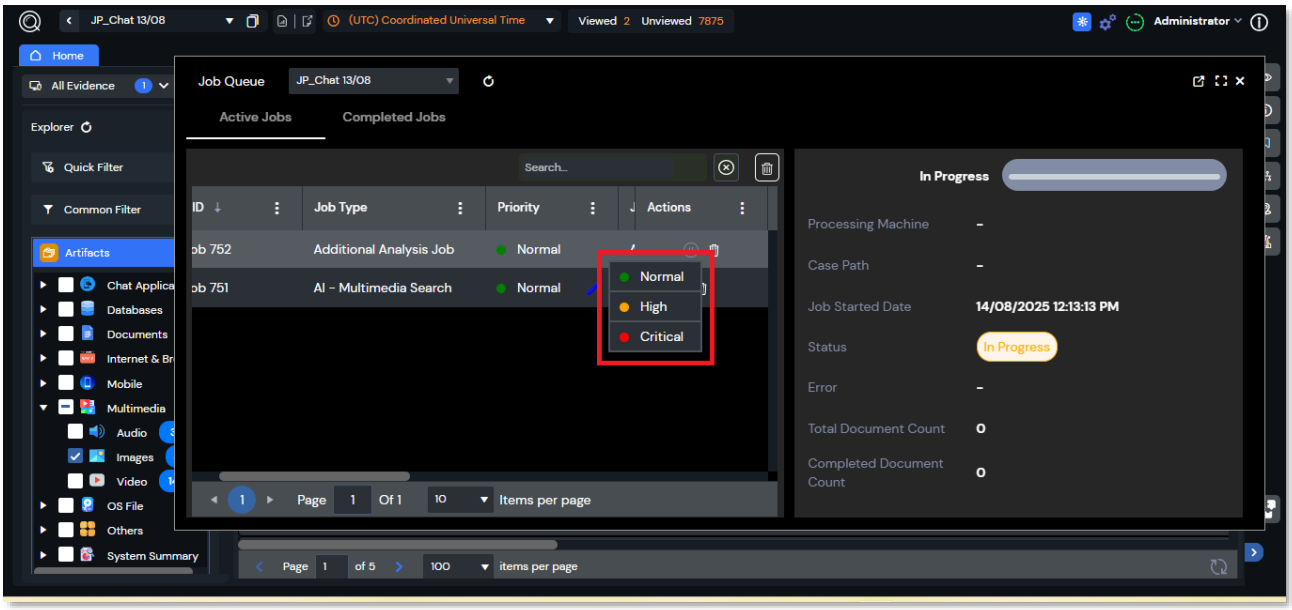
© Exterro, Inc. All rights reserved

Editing an AI Job's Priority

Upon initiating the multimedia search or summarization process, the corresponding job will be created in the Job Queue of FTK Central to monitor its status. Moreover, you can set the priority for all the AI jobs (before it is completed) to define the precedence.

To edit an AI job's priority:

1. Click on from the FTK Central application
2. Click on the **Edit** icon in the **Priority** column against the required job.
3. Select any one of the following priority options based on the corresponding description:
   - **Critical:** The highest priority and should have precedence over all other AI jobs.
   - **High:** High priority and will be executed after the **Critical** jobs are done. These jobs have precedence over the **Normal** AI jobs.
   - **Normal:** The default priority and will be processed after all the **Critical** and **High** priority jobs are completed.



© Exterro, Inc. All rights reserved

Notes:

- All the AI jobs will be processed sequentially in the above-mentioned order.
- Initially, all the jobs will be assigned with the **Normal** priority.
- Only users with all case-level permissions can change the AI jobs' priority
- When two jobs are set with the same priority, they will be processed sequentially based on their Job IDs
- For AI jobs initiated from the FTK Enterprise application, the priority cannot be set in the FTK Central job queue.

© Exterro, Inc. All rights reserved

Configuring Project Vic/CAID

Project VIC is a global partnership that uses advanced technology to fight child sexual exploitation and trafficking. In order to use this feature, you must have an account set up with Project VIC. Project VIC has compiled information about known online child abuse images. Known image or video files have unique identifier known as a "hash value."

When you process your evidence data, it is compared to the known hash values. If a match is found, the file in your evidence is flagged. You can easily see flagged files in review mode. You can also provide information to Project VIC about images that were previously unknown.

Initializing Project Vic/CAID

To initialize the Project Vic/CAID:

1. From the home page, click **Settings** from the top-right corner.
2. Navigate to the **System Management** tab.
3. Select **Project Defaults** from the left pane of **Configuration**.
4. Click on **Media Categorization**.
5. Select a relevant category for your region.
   - VIC_Canada
   - VIC_US
   - CAID_UK
6. Click **Save**.

Warning: Once a **Media Categorization** region has been selected, it cannot be changed. This list will not be populated unless a KFF server is present and a case has objects which match the KFF alerts.

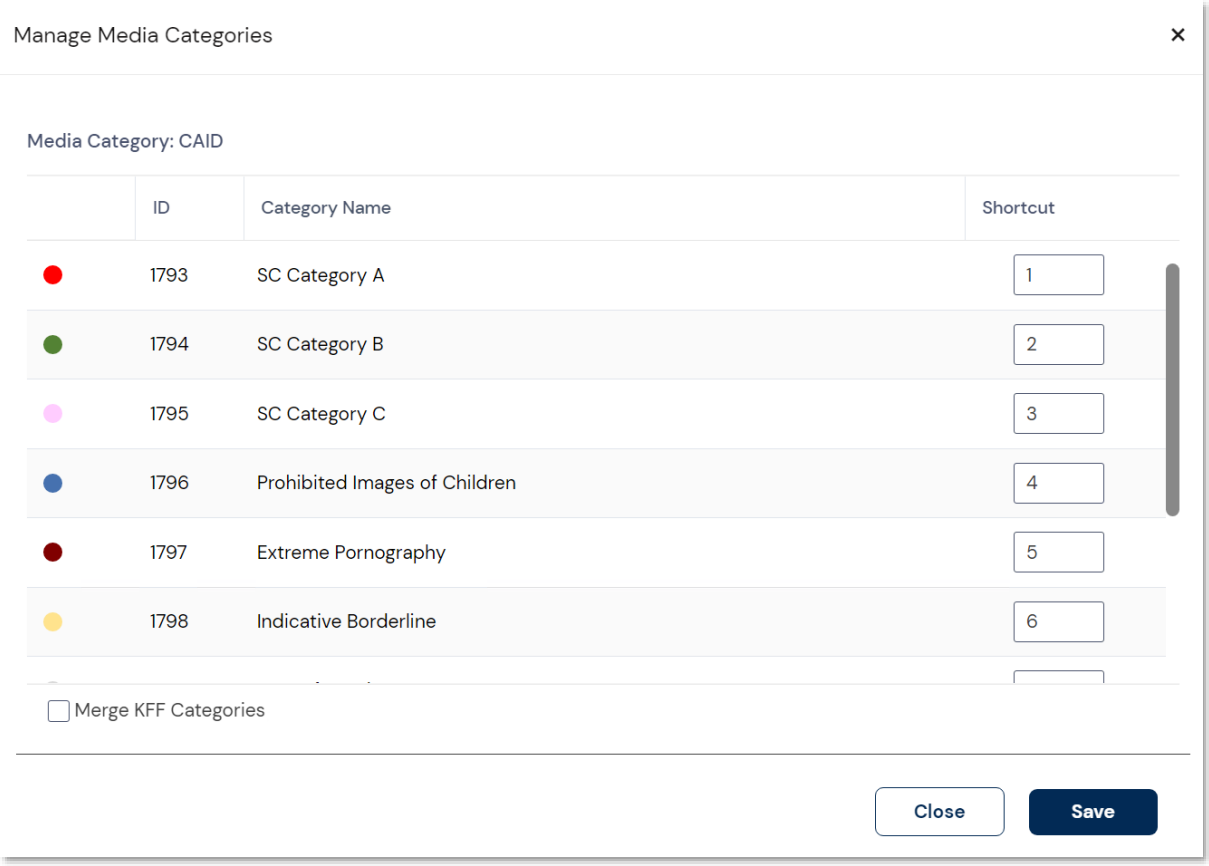
© Exterro, Inc. All rights reserved

Initializing Project Vic/CAID on a Case Level

To initialize Project Vic/CAID on a case-level:

Note: Each case will require Project Vic/CAID to be initialized.

1. From the home page, click **Case List**.
2. Click the **Context menu** (in the **Actions** column) against the required case.
3. Click **Initiate Media Categories**.
   - The **Manage Media Categories** prompt is displayed.



Note: The categories displayed in this section are retrieved directly from Project Vic/CAID.

© Exterro, Inc. All rights reserved

4. Define a keyboard shortcut using the **Shortcut** fields.

Note: The shortcuts can be numeric characters. These hotkeys use **SHIFT** in combination with the assigned numerical character.

5. Enter the investigator details.
   - **Project Vic Case Number**
   - **Contact Name**
   - **Contact Title**
   - **Contact Phone**
   - **Contact Email**
   - **Contact Organization**

6. Enable the **Merge KFF Categories** option if pre/post categorized data is required to be used during categorization. Selecting this option will auto assign the categories flagged by KFF, a bookmark value. Post categorized data goes to the same bookmarks and users will be able to look at pre and post categorized data together.

7. Click **Save**.

Tip: Administrators can initialize media categorization on new cases (not including any existing cases) by setting the "EnableMediaCategorizationOnAllCases" parameter as "TRUE" in the adg.WeblabSelfHost.exe.config file.

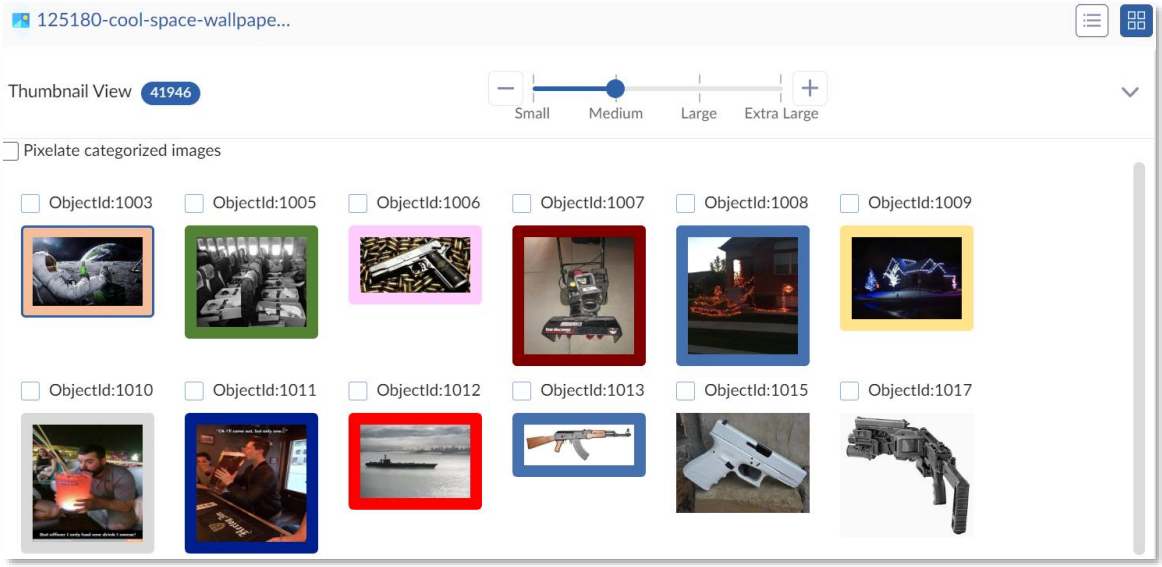
© Exterro, Inc. All rights reserved

Categorizing documents in Review Mode

To categorize documents in review mode:

1. From the home page, click **Case List**.
2. Click on a **Case Name**.
3. Click **Enter Review**.
4. Click on the **Tags** tab.
5. Select **Bookmarks**.
6. Open the **Shared** bookmarks folder.
7. In the Grid, check or highlight the records requiring categorization.
8. Check the required bookmark.
9. The images in thumbnail view and in the viewer, will display a colored border associated to the CAID categorization.

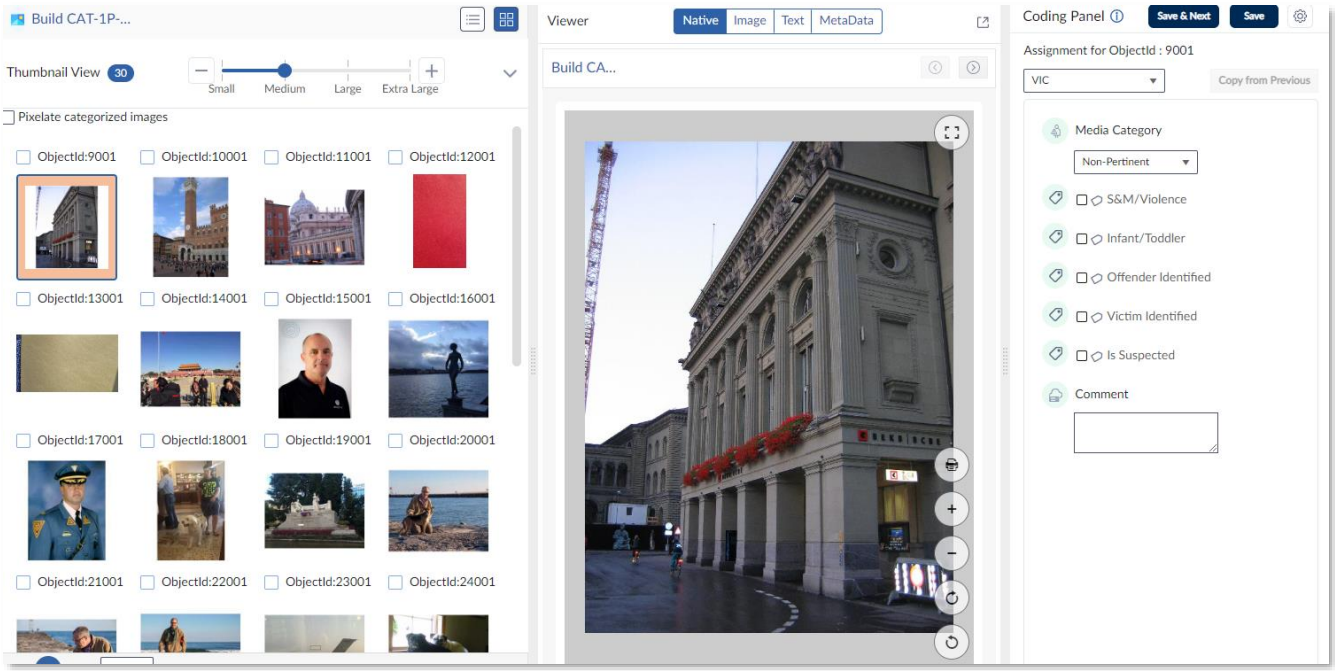
Tip: Alternatively, you can use **Thumbnails** view and press the hotkey assigned to a specific category to apply the bookmarks to a file. E.g., SHIFT + 1.



© Exterro, Inc. All rights reserved

Using the Coding Panel to Categorize Images

The Coding Panel can be used in addition to the Tags functionality to categorize images. If a case has been initialized for media categorization, the coding panel will allow users to select their chosen media categorization regions custom coding panel for grading.



To categorize documents in review mode:

1. From the home page, click **Case List**.
2. Click on a **Case Name**.
3. Click **Enter Review**.
4. Click on the **Coding Panel** tab.
5. Select the applicable region from the drop-down list.
6. Use the options provided to begin categorization.

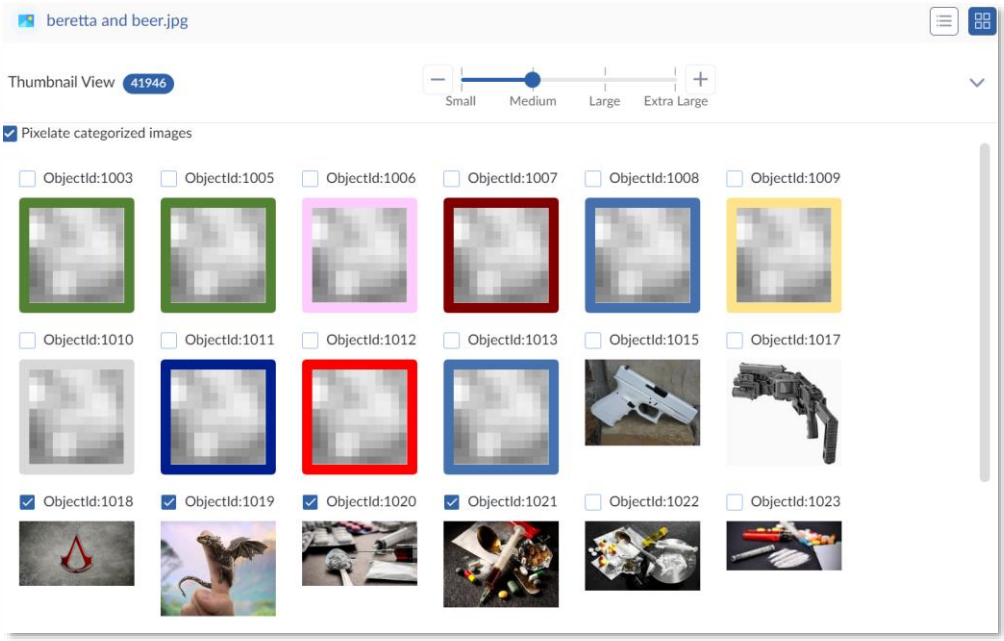
Note: Users can click **Save & Next** to apply any coding panel values and move onto the next file.

© Exterro, Inc. All rights reserved

Pixelating Categorized Images

When images have been categorized using CAID/VIC, users can pixelate these images automatically.

Clicking **Pixelate Categorized Images** will enable this option.

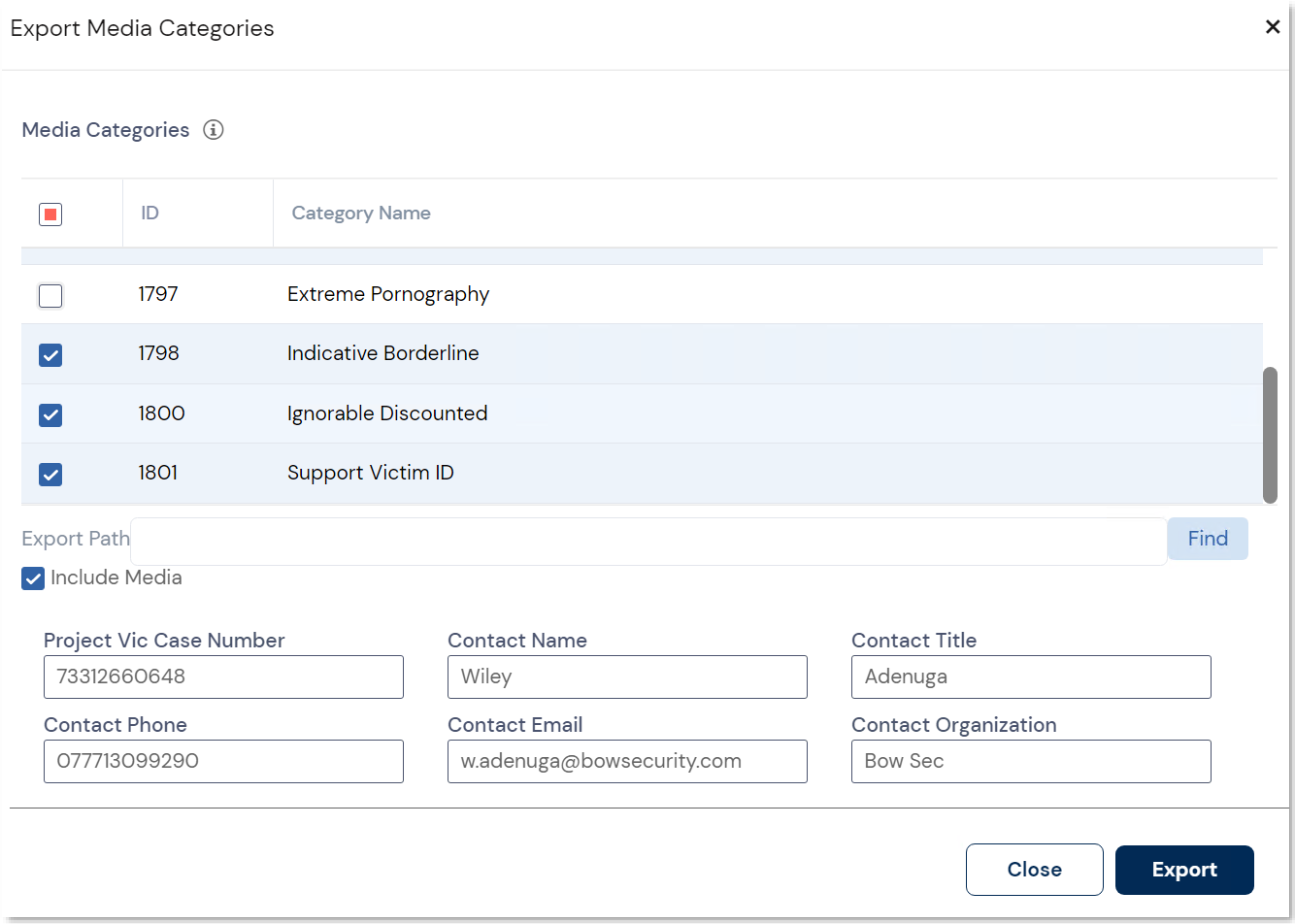


© Exterro, Inc. All rights reserved

Exporting Media Categories

To export media categories:

1. From the home page, click **Case List**.
2. Click on a **Case Name**.
3. Click **Enter Review**.
4. Select the required files.
5. Right-click on a selected file.
6. Select **Export media categories**.
   - The **Media Categories** prompt is displayed.



© Exterro, Inc. All rights reserved

7. Check the categories requiring export.

Note: The selected categories will be exported in JSON format.

8. Select an **Export Path**.
9. Enable the **Include Media** option if the categorized data is required to be exported. This will not export all media categories due to export rules set by CAID.

Note: The exported files will be stored in categorized folders within the export destination.

© Exterro, Inc. All rights reserved

Filtering Categorized Data

To filter categorized data in review mode:

1. From the home page, click **Case List**.
2. Click on a **Case Name**.
3. Click **Enter Review**.
4. Click on the **Filter** tab.
5. Expand **Tags > Bookmarks > Shared > Media Category**.
6. Check the required media category to filter and view categorized data.

© Exterro, Inc. All rights reserved

Managing Security Devices and Licenses

This appendix includes information Exterro product licenses, Virtual CodeMeter activation, Network License Server, and API Key configurations.

Installing and Managing Security Devices

Exterro products require a licensing security device that communicates with the program to verify the existence of a current license.

You must install the security device software and drivers before you can manage licenses with License Manager.

This section explains installing and using the CodeMeter Runtime software and the License Manager.

Installing the Security Device

Exterro products require a licensing security device that communicates with the program to verify the existence of a current license. The device is a WIBU-SYSTEMS (Wibu) CodeMeter (CmStick). This USB device requires specific software to be installed prior to connecting the devices and running your Exterro products.

You will need the WIBU-SYSTEMS CodeMeter Runtime software with a WIBU-SYSTEMS CodeMeter (CmStick), either the physical USB device, or the Virtual device.

Store the CmStick or dongle in a secure location when it is not in use.

© Exterro, Inc. All rights reserved

Installing the CodeMeter Runtime Software

When you purchase a product, Exterro provides a USB CmStick with the product package. To use the CmStick, you must first install the CodeMeter Runtime software, either from the shipping disc or from the setup file downloaded from the Exterro website.

Note: The CodeMeter software is automatically installed as part of the FTK suite.

To download the CodeMeter installer from the Exterro website:

1. Go to the Exterro download page at: http://www.Exterro.com/product-download.
2. On the download page, click **CodeMeter**.
3. Click Download Page.
4. Click **Download Now**.
5. Save the installation file to your download directory or other temporary directory on your drive.

To install CodeMeter:

1. Launch the installer from the download by doing the following:
   - Navigate to the CodeMeter installation folder ("\{F5F91CCC-5315-49F7-8849-AE1673C65222}"), and double-click the installation file.

2. Wait for the *Preparing to Install* processes to complete.
3. In the Welcome dialog, click **Next**.
4. Read and accept the License Agreement
5. Enter User Information.
6. Click **Next**.
7. Select the features you want to install.
8. Click Next > Install > Finish.
9. Click **OK**.

© Exterro, Inc. All rights reserved

CodeMeter Error

If you are not using NLS for your security device configuration, after clicking **No**, you will see the following additional message.

- *Security Device Not Found*

To remedy, click **OK**, then install the correct CodeMeter Runtime software, and connect the CmStick or run License Manager to generate your Virtual CmStick. Then, restart FTK.

Installing License Manager

License Manager lets you manage product and license subscriptions using a security device or device packet file.

You can access the License Manager installer from the Web or from the FTK installer.

To download the License Manager installer from the Exterro website:

1. Go to the Exterro download page at: http://www.Exterro.com/product-download.
2. On the download page, click **License Manager**.
3. Click Download Page.
4. Click Download Now.
5. Save the installation file to your download directory or other temporary directory on your drive.

© Exterro, Inc. All rights reserved

To install License Manager:

1. Navigate to the License Manager installation folder ("\{6F8C49D6-8EDC-4F06-9348-2E6EC0798963}"), and double-click the installation file.
2. Wait for the *Preparing to Install* processes to complete.
3. Click **Next** on the Welcome screen
4. Read and accept the License Agreement.
5. Click **Next**.
6. Accept the default destination folder, or select a different one.
7. Click **Next**.
8. In the Ready to Install the Program dialog, click **Back** to review or change any of the installation settings. When you are ready to continue, click **Install**.
9. Wait while the installation completes.
10. If you want to launch License Manager after completing the installation, mark the **Launch AccessData License Manager** check box.
11. Select the **Launch AccessData License Manager** check box to run the program upon finishing the setup. The next section describes how to run License Manager later.
12. Click **Finish** to finalize the installation and close the wizard.

© Exterro, Inc. All rights reserved

Starting License Manager

To launch License Manager:

1. Launch License Manager by clicking the **License Manager** icon on your desktop.

When starting, License Manager reads licensing and subscription information from the installed and connected WIBU-SYSTEMS CodeMeter Stick, or Keylok dongle.

Note: If using a Keylok dongle, and License Manager either does not open or displays the message, "Device Not Found"

2. Verify the correct dongle driver is installed on your computer.
3. With the dongle connected, check in Windows Device Manager to make sure the device is recognized. If it has an error indicator, right click on the device and choose Uninstall.
4. Remove the dongle after the device has been uninstalled.
5. Reboot your computer.
6. After the reboot is complete, and all startup processes have finished running, connect the dongle.
7. Wait for Windows to run the Add New Hardware wizard. If you already have the right dongle drivers installed, do not browse the internet, choose, "No, not this time."
8. Click **Next** to continue.
9. On the next options screen, choose, "Install the software automatically (Recommended)
10. Click **Next** to continue.
11. When the installation of the dongle device is complete, click Finish to close the wizard.
12. You still need the CodeMeter software installed, but will not need a CodeMeter Stick to run License Manager.

Note: If using a CodeMeter Stick, and License Manager either does not open or displays the message, "Device Not Found".

© Exterro, Inc. All rights reserved

13. Make sure the CodeMeter Runtime 4.20b software is installed. It is available at www.Exterro.com/support.
    - Click Downloads and browse to the product.
    - Click on the download link. You can Run the product from the Website, or Save the file locally and run it from your PC.
    - Once the CodeMeter Runtime software is installed and running, you will see a gray icon in your system tray.
14. Make sure the CodeMeter Stick is connected to the USB port.

If the CodeMeter Stick is not connected, License Manager still lets you to manage licenses using a security device packet file if you have exported and saved the file previously.

To open License Manager without a CodeMeter Stick installed:

1. Click Tools > License Manager.
   License Manager displays the message, "Device not Found".

2. Click **OK**, then browse for a security device packet file to open.

Note: Although you can run License Manager using a packet file, Exterro products will not run with a packet file alone. You must have the CmStick or dongle connected to the computer to run Exterro products that require a license.

© Exterro, Inc. All rights reserved

Using License Manager

License Manager provides the tools necessary for managing Exterro product licenses on a WIBU-

SYSTEMS CodeMeter Stick security device, a Keylok dongle, a Virtual Dongle, or in a security device packet file.

License Manager displays license information, allows you to add licenses to or remove existing licenses from a dongle or CmStick. License Manager, and can also be used to export a security device packet file. Packet files can be saved and reloaded into License Manager, or sent via email to Exterro support.

In addition, you can use License Manager to check for product updates and in some cases download the latest product versions.

License Manager displays CodeMeter Stick information (including packet version and serial number) and licensing information for all Exterro products. The Purchase Licenses button connects directly to the Exterro website and allows you to browse the site for information about products you may wish to purchase. Contact Exterro by phone to speak with a Sales Representative for answers to product questions, and to purchase products and renew licenses and subscriptions.

The License Manager Interface

The License Manager interface consists of the following two tabs that organize the options in the License Manager window

- Installed Components
- Licenses

© Exterro, Inc. All rights reserved

Installed Components Tab

The Installed Components tab lists the Exterro programs installed on the machine. The Installed Components tab is displayed in the following figure.

The following information is displayed on the Installed Components tab:

- License Manager Installed Components Tab Features

Item	Description
Program	Lists all Exterro products installed on the host.
Installed Version	Displays the version of each Exterro product installed on the host.
Newest Version	Displays the latest version available of each Exterro product installed on the host. Click Newest to refresh this list.
Product Notes	Displays notes and information about the product selected in the program list.
Exterro Link	Links to the Exterro product page where you can learn more about Exterro products.

The following buttons provide additional functionality from the Installed Components tab:

- License Manager Installed Components Buttons

Button	Function
Help	Opens the License Manager Help web page.

© Exterro, Inc. All rights reserved

- License Manager Installed Components Buttons (Continued)

Button	Function
Install Newest	Installs the newest version of the programs checked in the product window, if that program is available for download. You can also get the latest versions from our website using your Internet browser.
Newest	Updates the latest version information for your installed products.
About	Displays the About License Manager screen. Provides version, copyright, and trademark information for License Manager.
Done	Closes License Manager.

Use the Installed Components tab to manage your Exterro products and stay up to date on new releases.

© Exterro, Inc. All rights reserved

Licenses Tab

The Licenses tab displays CodeMeter Stick information for the current security device packet file and licensing information for Exterro products available to the owner of the CodeMeter Stick, as displayed in the following figure.

The Licenses tab provides the following information:

License Manager Licenses Tab Features:

Column	Description
Program	Shows the owned licenses for Exterro products.
Expiration Date	Shows the date on which your current license expires.
Status	Shows this status of that product's license: None: the product license is not currently owned Days Left: displays when less than 31 days remain on the license. Never: the license is permanently owned. This generally applies to Hash Tables and Portable Office Rainbow Tables.
Name	Shows the name of additional parameters or information a product requires for its license.
Value	Shows the values of additional parameters or information a product contained in or required for its license.
Show Unlicensed	When checked, the License window displays all products, whether licensed or not.

© Exterro, Inc. All rights reserved

License Management Options:

The following license management actions can be performed using buttons found on the License tab:

Button	Function
Remove License	Removes a selected license from the Licenses window and from the CodeMeter Stick or dongle. Opens the Exterro License Server web page to confirm success.
Refresh Device	Connects to the Exterro License Server. Downloads and overwrites the info on the CodeMeter Stick or dongle with the latest information on the server.
Reload from Device	Begins or restarts the service to read the licenses stored on the CodeMeter Stick or dongle.
Release Device	Click to stop the program reading the dongle attached to your machine, much like Windows' Safely Remove Hardware feature. Click this button before removing a dongle. This option is disabled for the CodeMeter Stick.
Open Packet File	Opens Windows Explorer, allowing you to navigate to a .PKT file containing your license information.
Save to File	Opens Windows Explorer, allowing you to save a .PKT file containing your license information. The default location is My Documents.
Finalize Removal	Finishes the removal of licenses in the unbound state. Licenses must be unbound from the CmStick or dongle before this button takes effect.
View Registration Info	Displays an HTML page with your CodeMeter Stick number and other license information.
Add Existing License	Allows you to bind an existing unbound license to your CodeMeter Stick, through an internet connection to the Exterro License Server.
Purchase License	Brings up the Exterro product page from which you can learn more about Exterro products.
About	Displays the About License Manager screen. Provides version, copyright, and trademark information for License Manager.
Done	Closes License Manager.

© Exterro, Inc. All rights reserved

Opening and Saving Dongle Packet Files

You can open or save dongle packet files using License Manager. When started, License Manager attempts to read licensing and subscription information from the dongle. If you do not have a dongle installed, License Manager lets you browse to open a dongle packet file. You must have already created and saved a dongle packet file to be able to browse to and open it.

To save a security device packet file:

1. Click the **Licenses** tab, then under License Packets, click **Save to File**.
2. Browse to the desired folder and accept the default name of the .PKT file; then click **Save**.

To open a security device packet file:

1. Select the **Licenses** tab.
2. Under License Packets, click **Open Packet File**.
3. Browse for a dongle packet file to open. Select the file and click **Open**.

Adding and Removing Product Licenses

On a computer with an Internet connection, License Manager lets you add available product licenses to, or remove them from, a dongle.

To move a product license from one dongle to another dongle, first remove the product license from the first dongle. You must release that dongle, and connect the second dongle before continuing. When the second dongle is connected and recognized by Windows and License Manager, click on the Licenses tab to add the product license to the second dongle.

© Exterro, Inc. All rights reserved

Removing a License

To remove (unassociate or unbind) a product license:

1. From the Licenses tab, mark the program license to remove.
   - This action activates the Remove License button below the Program list box.

2. Click **Remove License** to connect your machine to the Exterro License Server through the internet.
3. When you are prompted to confirm the removal of the selected licenses from the device, click **Yes** to continue, or **No** to cancel.
4. Several screens appear indicating the connection and activity on the License Server, and when the license removal is complete, the following screen appears.
5. Click **OK** to close the message box.

Note: Another internet browser screen appears from License Manager with a message that says, "The removal of your licenses from Security Device was successful!" You may close this box at any time.

© Exterro, Inc. All rights reserved

Adding a License

To add a new or released license:

1. From the Licenses tab, under Browser Options, click **Add AccessData License.**

The AccessData License Manager Web page opens, listing the licenses currently bound to the connected security device, and below that list, you will see the licenses that currently are not bound to any security device. Mark the box in the Bind column for the product you wish to add to the connected device, then click **Submit**.

2. An AccessData License Manager Web page will open, displaying the following message, "The Exterro products that you selected has been bound to the record for Security Device <*ID number*> within the Security Device Database.
3. "Please run License Manager's "**Refresh Device**" feature in order to complete the process of binding these product licenses to this Security Device." You may close this window at any time.
4. Click **Yes** if License Manager prompts, "Were you able to associate a new product with this device?"
5. Click **Refresh Device** in the Licenses tab of License Manager. Click **Yes** when prompted.

You will see the newly added license in the License Options list.

© Exterro, Inc. All rights reserved

Adding and Removing Product Licenses Remotely

While License Manager requires an Internet connection to use some features, you can add or remove licenses from a dongle packet file for a dongle that resides on a computer, such as a forensic lab computer, that does not have an Internet connection.

If you cannot connect to the Internet, the easiest way to move licenses from one dongle to another is to physically move the dongle to a computer with an Internet connection, add or remove product licenses as necessary using License Manager, and then physically move the dongle back to the original computer. However, if you cannot move the dongle—due to organization policies or a need for forensic soundness—then transfer the packet files and update files remotely.

Adding a License Remotely

To remotely add (associate or bind) a product license:

1. On the computer where the security device resides:
   i. Run License Manager.
   ii. From the Licenses tab, click Reload from Device to read the dongle license information.
   iii. Click **Save to File** to save the dongle packet file to the local machine.

2. Copy the dongle packet file to a computer with an Internet connection.
3. On the computer with an Internet connection:
   i. Remove any attached security device.
   ii. Launch License Manager. You will see a notification, "No security device found".
   iii. Click **OK**.
   iv. An "Open" dialog box will display. Highlight the .PKT file, and click Open.
   v. Click on the **Licenses tab**.
   vi. Click **Add Existing License**.
   vii. Complete the process to add a product license on the Website page.
   viii. Click **Yes** when the License Manager prompts, "Were you able to associate a new product with this dongle?"

© Exterro, Inc. All rights reserved

ix. When License Manager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted to save the update file, [serial#].wibuCmRaU.

x. Save the update file to the local machine.

4. After the update file is downloaded, copy the update file to the computer where the dongle resides:

5. On the computer where the dongle resides:

i. Run the update file by double-clicking it. ([serial#].wibuCmRaU is an executable file.)

ii. After an update file downloads and installs, click **OK**.

iii. Run **License Manager**.

iv. From the **Licenses tab**, click **Reload from Device** to verify the product license has been added to the dongle.

© Exterro, Inc. All rights reserved

Removing a License Remotely

To remotely remove (unassociated, or unbind) a product license:

1. On the computer where the dongle resides:
   i. Run **License Manager**.
   ii. From the **Licenses tab**, click **Reload from Device** to read the dongle license information.
   iii. Click **Save to File** to save the dongle packet file to the local machine.

2. Copy the file to a computer with an Internet connection.
3. On the computer with an Internet connection:
   i. Launch License Manager. You will see a notification, "No security device found".
   ii. Click **OK**.
   iii. An "Open" dialog box will display. Highlight the .PKT file, and click **Open**.
   iv. Click on the **Licenses tab**.
   v. **Mark the box for the product license you want to unassociate**; then click **Remove License**.
   vi. When prompted to confirm the removal of the selected license from the dongle, click **Yes**.
   vii. When License Manager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted save the update file.
   viii. Click **Yes** to save the update file to the local computer.
   ix. The Step 1 of 2 dialog details how to use the dongle packet file to remove the license from a dongle on another computer.
   x. **Save** the update file to the local machine.

4. After the update file is downloaded, copy the update file to the computer where the dongle resides.

© Exterro, Inc. All rights reserved

5. On the computer where the dongle resides:
   i. Run the update file by double-clicking it. This runs the executable update file and copies the new information to the security device.

   ii. Run License Manager
   iii. On the **Licenses tab**, click **Reload** from Device in License Manager to read the security device and allow you to verify the product license is removed from the dongle.

   iv. Click **Save** to File to save the updated dongle packet file to the local machine.

6. **Copy** the file to a computer with an Internet connection.

Sending a Dongle Packet File to Support

Send a security device packet file only when specifically directed to do so by Exterro support.

To create a dongle packet file:

1. Run License Manager
2. Click on the **Licenses tab**.
3. Click Load from Device.
4. Click **Refresh Device** if you need to get the latest info from AD's license server.
5. Click **Save to File**, and note or specify the location for the saved file.
6. Attach the dongle packet file to an e-mail and send it to support@exterro.com

© Exterro, Inc. All rights reserved

Virtual CodeMeter Activation Guide

Introduction

A Virtual CodeMeter (VCM) allows the user to run licensed Exterro products without a physical CodeMeter device. A VCM can be created using AccessData License Manager, but requires the user to enter a Confirmation Code during the creation process.

Preparation

- Contact your Exterro sales rep to order a VCM confirmation code.
- Install the CodeMeter Runtime 7.30 or newer verision. (available on the Wibu download page)
- Install the latest release of License Manager (available on the Exterro download page).
- The following steps are to be run on the system where you want to permanently attach the VCM.

Note: Once created, the VCM cannot be moved to any other system.

© Exterro, Inc. All rights reserved

Setup for Online Systems

To setup a virtual CodeMeter:

1. Unplug any Exterro dongles you currently have connected.
2. Launch License Manager.
3. Select Create A Local Virtual CMStick.
4. Click **OK.**
5. In the **Confirmation Code Required** dialog, enter your confirmation code.
6. Click **OK**.

   AccessData License Manager will automatically synchronize with the License Server over the Internet.

7. Click **OK** when the update completes.

   Upon performing the above step, License Manager will create the VCM on the system.

Once all the steps are performed, AccessData License Manager displays a serial number for the VCM on the Licenses tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

© Exterro, Inc. All rights reserved

Setting up VCM for Offline Systems

You can setup a Virtual CodeMeter on a system that is not connected to the internet (offline). You must also have one machine that connects to the internet to perform certain steps. This section details what to do on which machine.

To perform these steps on the offline system:

1. Unplug any Exterro dongles you currently have connected.
2. Launch License Manager.
3. Select Create Empty Virtual CMStick (offline).
4. Click **OK.**
5. The resulting dialog prompts you to save the *.wibucmrau file. Enter a name and path for the file, then click Save.
6. **Transfer** the *.wibucmrau to the Online system.

To perform these steps on the online system:

1. Unplug any Exterro dongles you currently have connected.
2. Launch License Manager.
3. Select Create Activation File (online).
4. Click **OK**.
5. In the **Confirmation Code Required** dialog, enter your confirmation code and click **OK**.

   AccessData License Manager will automatically synchronize with the License Server over the internet.

6. Data synchronized from the server will be written to the *.wibucmrau file. Click **OK** when the update completes.
7. **Transfer** *.wibucmrau back to the offline system.

© Exterro, Inc. All rights reserved

To perform these steps on the offline system:

1. Unplug any Exterro dongles you currently have connected.
2. Launch License Manager.
3. Select Create Activate Virtual CMStick (offline).
4. Click **OK**.
5. The resulting dialog prompts you to browse to the location of the newly updated *.wibucmrau file. Locate the file, then click Open. License Manager creates the VCM on your system.
6. At this point, AccessData License Manager should now display a serial number for the VCM on the "Licenses" tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

© Exterro, Inc. All rights reserved

Virtual CodeMeter FAQs

Q: **How do I get a Virtual CodeMeter (VCM)?**

A: Contact your Exterro product sales representative. They will provide you with a VCM confirmation code.

Q: **How do VCMs work?**

A: A VCM operates in almost exactly the same way as a hardware CodeMeter device, except that they exist as a file stored on the hard disk. During activation, the VCM file (named with a WBB extension) is tied to the hardware of the system using unique hardware identifiers. Those unique identifiers make VCMs non-portable. When AccessData License Manager is launched, it will automatically load the VCM and display its license information. From there, you can refresh, remove, add existing licenses, etc just the same you would with a hardware security device.

Q: **Are VCMs supported on virtual machines (VM)?**

A: No. Due to the fact that virtual machines are portable and VCMs are not, VCMs are not supported on virtual machines. Currently it is recommended to use Exterro Network License Service (NLS) to license systems running as virtual machines.

© Exterro, Inc. All rights reserved

Q: **How can I "unplug" a VCM?**

A: If you want to prevent License Manager from automatically loading the VCM you can "unplug" it by stopping the CodeMeter Runtime Service server and then moving (cut and paste) the WBB file to a new location (renaming the file does not suffice). By default the WBB file is located at:

32 bit systems:

C:\Program Files\CodeMeter\CmAct\

64 bit systems:

C:\Program Files (x86)\CodeMeter\CmAct\

Q: **I have activated a VCM on my system, but now I need to activate it on a different system. What should I do?**

A: Since a VCM is uniquely tied to the system on which it is activated, it cannot be moved to any other system. If you need to activate a VCM on a different system, you need to contact your Exterro Sales Representative.

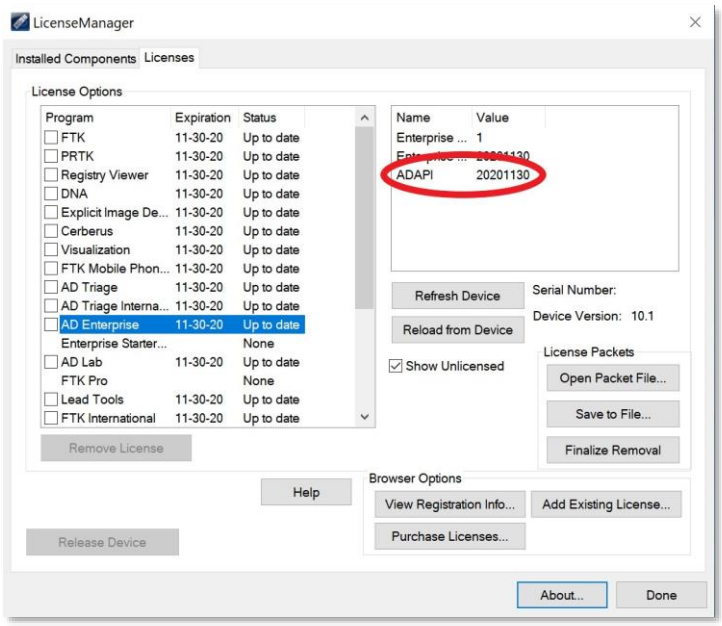
Q: **What if I need to reinstall Windows, format my drive, change my system's hardware, or back up my VCM in case of a disaster? Will the VCM still work?**

A: The VCM can be backed up by simply copying the WBB file to a safe location. It can be restored by copying the WBB file to the CmAct folder. The VCM cannot be restored without a WBB file. If you do not have a backup of your WBB file, you will need to get a new confirmation code from your Exterro Sales Representative.

© Exterro, Inc. All rights reserved

About API Key Generation

To generate an API authentication key, your CodeMeter License dongle must have the ADAPI sub-license (with current expiration date) applied as a license attribute of your AD FTK / Lab / Enterprise license. As long as this dongle is plugged into the machine when you launch the FTK.exe program, you will be able to generate API keys through the application. Typically, you will want to bind this key to the application administrator account so that the API key has access to all of the REST API calls.



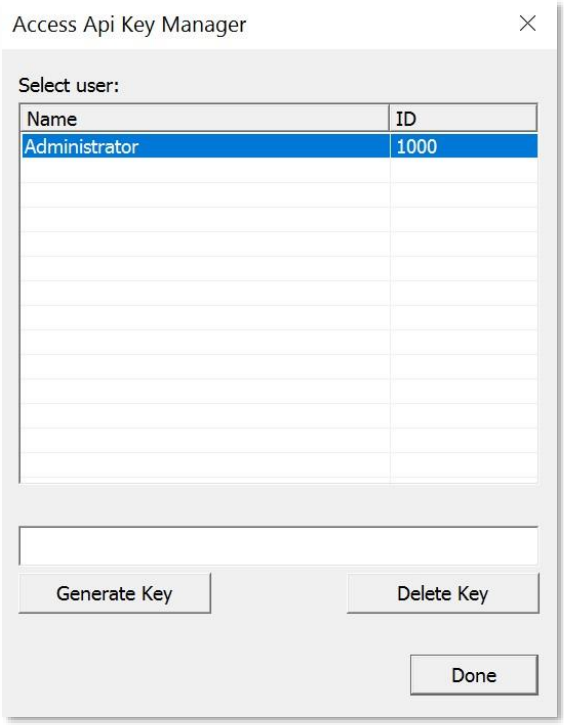
© Exterro, Inc. All rights reserved

How to generate an API key:

1. Insert the CodeMeter licensed for ADAPI to the Examiner system.
2. Launch FTK/Lab/Enterprise/QView

Note: QView requires users to obtain an API key using the Administration tab.

3. In the Case Management interface, select the Access API Key option from the Tools menu.
4. In the Access API Key Manager window, select the user account for whom you wish to generate an API key.



Note: Appropriate API related permissions will be granted to the selected user account once the API key is generated.

5. Click the **Generate Key** button.
6. The generated API key will populate in the key field.

© Exterro, Inc. All rights reserved

To generate API key via FTK Central:

1. Navigate to FTK Central.
2. Follow the notation below, to access your API key.

   <FTKCentralURL>/api/security/{userid}/getenterpriseapiguid

Note: The (userid) in the above URL is to be replaced with your User ID in FTK Central. For example, 1000 would be administrator.

© Exterro, Inc. All rights reserved

Agent Installations

Manually Installing The Windows Agent

This chapter covers the manual installation of the agent in a Windows environment.

Agent Certificate Requirements

The certificates used by agent and site server can use either the **SHA-1 or SHA-256** hashing algorithm. These do not require any "Key Usage" or other special fields.

Manual Installations

Perform the following steps to manually install the **Agent in Windows**:

- Specific Instructions for eDiscovery
- Specific Instructions for Forensics Products
- Manually Installing the Agent
- Configuring Execname and Servicename Values

© Exterro, Inc. All rights reserved

Manually Installing the Agent

To manually install the Agent

1. Run **AccessDataAgent.msi** or **AccessDataAgent(64bit) using msiexec**.

Note: These .msi files are located in the Program:

Files\AccessData\Forensic Toolkit\5.1\Bin\Agent\<x32 or x64>folder after installation.

There are several command line parameters available to use with this **.msi** as documented below.

Here is an example command line that will install with the defaults:

If AccessDataAgent.msi resides in the folder *C:\enterprise and ManagementServer.crt* resides in:

- [Drive]:\certificates, type the following command line to install the agent with defaults:
- msiexec /i [Drive]:\enterprise\AccessDataAgent.msi

  CER=[Drive]:\certificates\ManagementServer.crt.

© Exterro, Inc. All rights reserved

Command Line Options:

The following table lists the command line options available for use with this **AccessDataAgent.msi**:

Option	Action
/i (i or x required)	Specifies install.
/x (i or x required)	Specifies un-install.
/qn (optional)	Allows you to install in quiet mode with no user interaction.
<path and msi file name> (required)	If running from the folder where the .msi is located you do not have to include path, only the filename.
CER=<path and certificate file name> (required)	Specifies the certificate the agent uses. Always include the path, regardless of location.
ALLUSERS=<n>	Configures the installer to be available to all users. The default option varies per operating system. The options are: • allusers=1 configures the installer to be available to all users. • allusers=0 configures the installer to be available to only the user who is installing the agent.
INSTALLDIR=<custom install path> (optional)	Allows you to change the install location from the default folder: (C:\Program Files\AccessData\Agent).
PORT=<xxxx> (optional)	Allows you to change the port from the default port (3999).
LIFETIME=<d> (optional)	Allows you to configure the life cycle of the agent. The "d" value equals the Time To Live (TTL) measured in days. Adding a number preceded by a dash measures the TTL in minutes. For example: <-d >.
CONNECTIONS=<n>	Allows you to configure the number of maximum connections for the agent.
STORESIZE=<n>	Allows you to configure the size of the data store.

© Exterro, Inc. All rights reserved

Option	Action
TRANSIENT=1	Allows you to configure the agent as a Transient Agent. Transient Agents have no protected storage and remove themselves when the agent machine is restarted.
SERVICELESS=1	Allows you to configure the agent to install with no protected storage and no installed service. The agent removes itself when the agent machine restarts or when the lifetime option expires, whichever comes first.

Install command for Agent Jobs

```
msiexec /i "C:\AgentInstall\AccessData Agent (64-bit).msi" cer="C:\AgentInstall\AccessData E1.crt"
SSLIST="publicssDNS,publicssNLB,192.192.192.192" HTTPSPORT=443 TCPPORT=54545
```

User if needed to install for RMD (Mobile) collection

```
msiexec /i "C:\AgentInstall\AccessData Agent (64-bit).msi" cer="C:\AgentInstall\AccessData E1.crt"
SSLIST="publicssDNS,publicssNLB,192.192.192.192" HTTPSPORT=443 TCPPORT=54545
INSTALL_RMD=1
```

© Exterro, Inc. All rights reserved

Configuring Execname and Servicename Values

The Execname and Servicename values change the names of the agent executable and agent service respectively. These values are added to the MSI using an MSI editor (such as ORCA.exe a free MSI editor).

Changing the Execname Value

To make changes to the execname value

1. Run **Orca.EXE**.
2. Click **File > Open**.
3. Browse to the folder containing the **AccessData Agent.msi** or **AccessData Agent (64-bit).msi** file and open the file and the default path is:

   [Drive]:\Program Files\AccessData\Forensic Toolkit\3.2\Bin\Agent\x32 (or x64)
4. In the **Tables** list, select File.
5. In the **FileName** column, double-click "u4jwdc7h.exe|agentcore.exe".
   i. Enter the filename to use for the agent core executable.

   Note: Replace the entire string with the filename.
6. Press **Enter**.
7. Click **File > Save**.

   Note: Do not close Orca.EXE if you are also changing the service name.

© Exterro, Inc. All rights reserved

Changing the Servicename Value

To make changes to the Servicename value

1. Run **Orca.EXE**.
2. Click **File > Open**.
3. Browse to the folder containing the **AccessData Agent.msi** or **AccessData Agent (64-bit).msi** file and open the file. The default path is:

   [Drive]:\Program Files\AccessData\Forensic Toolkit\3.2\Bin\Agent\x32 (or x64)

4. In the **Tables** list, select "ServiceControl".
5. In the **Name** column, double-click "AgentService".
   i. Enter the name to use for the AgentService and press Enter.

   Note: Use the same value in steps 5, 7 and 8.

6. In the **Tables** list, select "ServiceInstall".
7. In the **Name** column, double-click "AgentService".
   i. Enter the name to use for the **AgentService** (use the same value entered in step 5) and press **Enter**.
8. In the **DisplayName** column, double-click "AgentService".
   i. Enter the name to use for the AgentService (use the same value entered in steps 5a and 7a) and press **Enter**.
9. Click **File > Save**.
10. Click **File > Close**.

© Exterro, Inc. All rights reserved

To add a throttling registry key

You can edit a registry key that allows you to control what percentage of the CPU is used for the agent. This gives you the ability to throttle the CPU and insure that the agent does not consume all of the CPU available.

Important Information

The following information is important to know about installing and executing an agent:

- In version 7.2 and newer, agent modules are automatically deployed to the agent as part of the Windows agent installation process.
- The ADMON module does not run on low resource priority. The ADMON module must run on Normal priority or higher in order to maintain connection to the system drivers.

© Exterro, Inc. All rights reserved

Installing The Linux Agent

This chapter discusses the **Linux Agent Installer**.

Installing The Enterprise Agent on Linux

The AccessData Agent is available for Unix-, Linux-, and Mac-based operating systems as well as for Windows. This chapter discusses the specific installation files to use for supported Linux platforms. The following chapter discusses installing the Mac Agent.

Supported Platforms

Linux Agent Supported Platforms

The **Linux Agent Installer** supports the following platforms:

Installer	OS
agent-linux32.sh agent-linux64.sh	• Amazon Linux v1 • Amazon Linux v2 • Red Hat Linux 7.x • CentOS_5.11_x64 • CentOS 7.x • CentOS 8.x • Ubuntu 14 and newer • Debian 8.7 and newer • Fedora 33 The 6.2 or newer Linux Agent requires GLIBC 2.17. Collection from a system running an older GLIBC version can be attempted using the 6.1 version of the Agent, which can be obtained by contacting AccessData Support. A system's GLIBC version can be determined by running the following command: ldd - version.

© Exterro, Inc. All rights reserved

Installer	OS
agent-rh5.sh agent-rh5x64.sh (older 6.1 agent; available on request)	• CentOS Enterprise 5 (32- & 64-bit) • CentOS 7.1 64-bit • Debian 8.7 64-bit • RedHat 5 (32- & 64-bit) • Red Hat Enterprise Linux 7.1 64-bit • Red Hat Enterprise Linux 7.3 64-bit • SLED 11 (Suse Linux Enterprise Desktop) (32- & 64-bit) • Ubuntu 9 (and newer) (64-bit)
agent-rh3.sh or agent-rh3x64.sh (older 6.1 agent; available on request)	RedHat 3 (32- & 64-bit) Novell Linux Desktop (NLD) 9 (32-bit) SLED 10 (Suse Linux Enterprise Desktop) (32- & 64-bit)
Be sure to use the correct installer file for your 32- or 64-bit architecture/OS)	

To install the Linux Agent:

Execute the following command as root, and provide the appropriate information:

```
./agent-linux<bits>.sh <certpath> [-i <installpath>]
```

where <bits> is 32 or 64 depending on the operating system agent that is being used, and where <certpath> is the location of the public certificate to be used for identification, and where [-i <installpath>] indicates the directory to install the agent in. This defaults to:

```
/usr/AccessData/agent
```

© Exterro, Inc. All rights reserved

To install the Linux Agent on Fedora Based OS's:

Execute the following commands as root/sudo:

1. Open **Terminal** within the agent location path.
2. Enter the following command to give executable rights:

```
chmod +x agent-linux64.sh
```

3. Follow the installation steps in the *To Install Linux Agent section* above.
   - If the agent service fails to start, the steps below must be followed.
4. Enter the following command to set the security contet of the Agent Core daemon:

```
sudo /sbin/restorecon -v /etc/rc.d/init.d/agentcored
```

5. Enter the following command to search the Audit log and then update the **allow/dontaudit** policy for the **Agent Core** daemon:

```
sudo ausearch -c '(entcored)' --raw | audit2allow -M my-entcored
```

6. Enter the following command to update the SELinux policy module:

```
sudo semodule -X 300 -i my-entcored.pp
```

7. Enter the following commands to restart the agent:

```
sudo /etc/init.d/agentcored stop
sudo /etc/init.d/agentcored start
```

8. Enter the following command to check the status of the agent:

```
sudo /etc/init.d/agentcored status
```

© Exterro, Inc. All rights reserved

Enterprise Linux Agent Install Parameters and Options:

Option	Result
-installpath, -i <installpath>	The destination path for installing the agent. **Default:** */usr/ AccessData/agent/.*
-lifetime, -l <lifetime>	The lifetime of the agent. **Default:** 0. If <lifetime> ==0, it will never uninstall itself. If <lifetime> >0 it is days before uninstall. If <lifetime> <0 it is in minutes before uninstall.
-port, -p <port>	The port the agent listens on. **Default:** 3999.
-connections, -c <connections>	The maximum number of concurrent connections allowed by the agent. **Default**:10.
-size, -s <storagesize>	The protected storage area size. **Default** is 16777216 (16 MB)

Uninstallation

To uninstall the Linux Agent, execute the following command as root:

```
# ./agent-linux64.sh -rf
```

Starting/Stopping the Service

The Linux Agent service is started automatically on system startup, but can be stopped, started, and restarted anytime manually by executing commands such as the following (as root)

```
/etc/init.d/agentcored stop

/etc/init.d/agentcored start

/etc/init.d/agentcored restart
```

© Exterro, Inc. All rights reserved

Installing The Mac Agent

This chapter discusses the Agent Installer for Apple Macintosh.

Comparing the Mac OS X Agent to the macOS Agent

In keeping up with architecture and security enhancements in macOS (macOS 15 Sequoia, macOS Sonoma 14.0, macOS Ventura 13.0, macOS Monterey 12.0, macOS Big Sur 11.0, macOS Catalina 10.15). Any mentions of macOS agent only apply to the managed agent that supports macOS Catalina 10.15 and the newer versions of macOS.

Apple Macintosh OS Agent Reference:

Version	Code Name	AccessData Agent Type	Agent Installer Package
macOS 10.15	Catalina	AccessData Managed Agent	AccessDataAgent-macos-installer-x64-1.X.XX.pkg
macOS 11.0	Big Sur	AccessData Managed Agent	AccessDataAgent-macos-installer-x64-1.X.XX.pkg
macOS 12.0	Monterey	AccessData Managed Agent	AccessDataAgent-macos-installer-x64-1.X.XX.pkg
macOS 13.0	Ventura	AccessData Managed Agent	AccessDataAgent-macos-installer-x64-1.X.XX.pkg
macOS 14.0	Sonoma	AccessData Managed Agent	AccessDataAgent-macos-installer-x64-1.X.XX.pkg
macOS 15.0	Sequoia	AccessData Managed Agent	AccessDataAgent-macos-installer-x64-1.X.XX.pkg

© Exterro, Inc. All rights reserved

Installing the macOS Managed Agent

Supported macOS Versions

- Big Sur (macOS 11)
- Monterey (macOS 12)
- Ventura (macOS 13)
- Sonoma (macOS 14)
- Sequoia (macOS 15)

Backwards Compatibility

FTK Site Server is enhanced with Backward compatibility, the process of ensuring the older versions (before 8.2 SP2) of Agents (along with the latest) will work without any issues with the latest version of Site Server. The Backward Compatibility process is supported for the 8.1 SP3 (Agent version - 1.0.502) and 8.2 SP1 (Agent version - 1.0.402) versions.

Prerequisites

The prerequisites outlined below are specific to macOS Agents only.

- Port Requirements
- Certificate Requirements
- Site Server Installation
- Temporary Location for Agent Data

There are two different types of deployment methods used for macOS agent which are provided below:

- **Deployment Type 1** - For macOS Agents that operate in an isolated network environment and lack direct network visibility and connectivity to the application server.
- **Deployment Type 2** - For macOS Agents that **do not** operate in an isolated environment and has direct network visibility and connectivity to the application server.

© Exterro, Inc. All rights reserved

Deployment Type 1

Deployment Type 1 is designed for macOS Agents located outside the organization's internal network, such as remote employee devices or systems in field locations. These agents rely on a reverse proxy (Integrated with the Site Server Managed API) to establish secure and reliable communication with the FTK Web Service over the internet.

Key Features:

- **Flexibility and Reach:** Agents enable FTK to manage endpoints regardless of physical location, supporting remote and distributed workforces.
- **Reverse Proxy Support:** To facilitate communication, a reverse proxy acts as an intermediary, providing a secure path for check-ins and data transfer from devices to the central server.
- **Secure External Connectivity:** With properly configured certificates and HTTPS, these agents ensure encrypted data exchange, maintaining high security standards.
- **Dynamic Configuration:** Designed to adapt to varied and unpredictable network conditions common in remote environments.
- **Use Case:** Essential for organizations with a hybrid workforce or devices operating in remote, external, or untrusted networks.

Considerations:

- Configuration of the reverse proxy is necessary.
- Performance may depend on the quality of the endpoint's internet connection.
- Live Preview is not supported for macOS Agents (Deployment Type 1).

© Exterro, Inc. All rights reserved

Deployment Type 2

Deployment Type 2 is designed to operate within the same local or enterprise network as the FTK Web Service. These agents directly communicate with the FTK Web Service without the need for additional intermediaries (Reverse Proxy via Site Server), making their deployment straightforward and highly efficient for centralized environments.

Key Features:

- **Direct Communication:** On-network agents establish a seamless and direct connection to the FTK Web Service over internal network protocols.
- **High Performance:** They typically experience minimal latency, ensuring faster data transfers and real-time operations like Live Previews and Data Collection.
- **Simplicity of Configuration:** With no need for complex routing or proxy setups, deploying on-network agents is quick and easy.
- **Security Within Controlled Environment:** Communication occurs within a trusted internal network, leveraging existing security policies and firewalls for protection.
- **Use Case:** Ideal for organizations where endpoints and servers reside on the same internal infrastructure, such as within a corporate office or data center.
- **Live Preview:** Allows Live Preview of MacOS Agents within the application.

Considerations:

- Limited to environments where agents can maintain a consistent connection to the internal network.
- Not suitable for endpoints operating outside the corporate infrastructure on remote, external, or untrusted networks.

© Exterro, Inc. All rights reserved

Ports

The following ports ensure secure and controlled connectivity between macOS Agents and the FTK application. Users must ensure their firewall and network settings allow outbound traffic to these ports to establish a successful connection.

Functionality	Port	Deployment Type
Agent Check-In	443 Can be customized when configuring the Site Server.	Deployment Type 1
Agent Jobs	4446 Can be customized when configuring the FTK Web Service.	Deployment Type 1 and Deployment Type 2
Agent Live Preview	3999 Cannot be customized.	Deployment Type 2

Certificates

Purpose

The FTK Web Service certificate is essential for establishing secure, encrypted communication between the application server and macOS Agents during collections and Agent check-ins. The certificate is presented to macOS agents configured to communicate with the FTK Web Service directly (Deployment Type 2) as well as any macOS Agents communicating through the Reverse Proxy - Site Server (Deployment Type 1).

© Exterro, Inc. All rights reserved

A default certificate is provided, however if a custom certificate is required, ensure the following is reviewed:

Configuration File Location:

The certificate configuration parameters are found in ADG.WeblabSelfHost.exe.config. This file is found in the FTK application installation directory.

Location: *C:\Program Files\AccessData\Forensic Tools\<Version>\bin\ADG.WeblabSelfHost.exe.config*

Configuration Properties:

Private Certificate	
Configuration Properties	**Description**
certificateFileName	Specifies the full path to the PFX certificate file used by the FTK Web Service.
certificatePassword	The password relating to the certificate provided for certificateFileName. This password will be automatically encrypted after restarting the FTK Web Service.
certificateThumbprint	An optional configuration. Instead of specifying a certificate file, you can reference a certificate from the system store using its unique thumbprint.

Certificate Properties

- A PFX certificate must be configured to enable secure HTTPS connections.
- Common Name (CN): Ensure this matches the FQDN or alias of the FTK Web Service host.
- Certificate Authority (CA): Ensure it is signed by a trusted CA to ensure validity.
- Must be trusted by all FTK Web UI clients (Deployment Type 2).

Validation Settings

- validateCertificate configuration key can be found in the agentinstall.config during macOS Agent installations.
- This is set to false by default. If set to true, a custom certificate must be provided.

© Exterro, Inc. All rights reserved

macOS Agent Validation Certificates

Purpose:

These certificates enable secure communication between the FTK Web Service and macOS agents. The FTK Web Service presents the private certificate (agentCertificateFileName) to macOS Agents for authentication. A public certificate (clientCertificatePath), derived from this (agentCertificateFileName) certificate, must be distributed to macOS Agents for authentication.

The macOS agent hosts its local API over HTTPS, ensuring only the FTK Web Service and it's related UI are the only clients that can access the Agent API.

A default certificate is provided, however if a custom certificate is required, ensure the following is reviewed:

Private Certificate

Configuration File Location:

The certificate configuration parameters are found in ADG.WeblabSelfHost.exe.config. This file is found in the FTK application installation directory.

Location: *C:\Program Files\AccessData\Forensic Tools\<Version>\bin\ADG.WeblabSelfHost.exe.config*

© Exterro, Inc. All rights reserved

Configuration Properties:

Private Certificate	
Configuration Properties	**Description**
agentCertificateFileName	Specifies the full path to the PFX certificate file used by the FTK Web Service.
agentCertificatePassword	The password relating to the certificate provided for agentCertificateFileName. This password will be automatically encrypted after restarting the FTK Web Service.
agentCertificateThumbprint	An optional configuration. Instead of specifying a certificate file, you can reference a certificate from the system store using its unique thumbprint.
Certificate Properties	

- A PFX certificate must be configured to enable secure HTTPS connections.
- Common Name (CN): Ensure this matches the FQDN of the FTK Web Service host.
- A public certificate should be derived from this PFX in .CER (DER) format, and explicitly mentioned in the **agentinstall.config** > clientCertificatePath during macOS Agent installation in addition to setting the **validateCertificate** configuration to true.

© Exterro, Inc. All rights reserved

Public Certificate

Configuration File Location

The certificate configuration parameters are found in the agentinstall.config. This file is located in the root directory of the unzipped agent installer packages and should be copied along with the agent installer during installation.

Location: *C:\Program Files\AccessData\Forensic Tools\<version>\bin\Agent\MAC*

Configuration Properties:

Private Certificate	
Configuration Properties	**Description**
clientCertificatePath	Specifies the full path to the public certificate used by the macOS Agent.
Certificate Properties	

- A CER certificate must be configured to enable secure HTTPS connections.
- Common Name (CN): Ensure this matches the FQDN of the agent.

Certificate File Placement:

During installation the public key file (.cer) is copied to the following macOS Agent location automatically:

- **Default Location:** /Library/ExterroEnterpriseMacAgent/<Agent Version>

The macOS Agent will check both locations for a certificate, if either is empty, it will check the other before proceeding.

© Exterro, Inc. All rights reserved

Site Server Managed API Certificate (Deployment Type 1)

Purpose:

Site Servers act as a reverse proxy for agent check-ins using the Managed API. The PFX certificate secures the HTTPS connection between the macOS Agent and the Site Server. The FTK Site Server presents this private certificate to macOS Agents for authentication. macOS Agents will validate the presence of a CA-signed certificate during Check-Ins.

Private Certificate	
Configuration Properties within Site Server UI	**Description**
Certificate Path	Specifies the full path to the PFX certificate file used by the Site Server Managed API.
Certificate Password	The password relating to the certificate provided in the Certificate Path. This password will be automatically encrypted after restarting the Site Server.
HTTPS Port	The port which will be used by the Site Server Managed API to listen on for any macOS Agent communication. By default this port is 443.
Reverse Proxy (Mac Agents Only)	This option will enable/disable the reverse proxy for agents to communicate to. Exterro advises Deployment Type 1 to keep this option selected.
FTKC FQDN/IP	The FTK Web Service URL followed by the MangedAgentApiPort used for macOS Agents. This field is activated upon checking the Reverse Proxy (Mac Agents Only) option. *<FTK Central application URL>:<managed API Port>*

© Exterro, Inc. All rights reserved

Certificate Properties

- A **PFX certificate** must be configured to enable secure HTTPS connections.
- **Common Name (CN):** Ensure this matches the FQDN of the Site Server host.
- **Certificate Authority (CA):** Ensure it is signed by a trusted CA to ensure validity.
- This certificate must be trusted by all macOS Agents (Deployment Type 1).

Validation Settings

- validateCertificate configuration key can be found in the agentinstall.config during macOS Agent installations.
- This is set to false by default. If set to true, this certificate must be trusted by the macOS Agent.

Configuration Location

The certificate parameters should be configured in the **Agent Check-In Settings** tab within the Site Server Configuration pop-up. Refer to the Site Server Configuration section.

© Exterro, Inc. All rights reserved

Summary of Certificates

Certificate	Type	Purpose	Configuration Location	Server/ Client
FTK Web Service Certificate - certificateFileName	PFX - PKCS#12	Secures communication between the server, clients accessing the FTK Web UI, macOS agents connecting to the service, and Site Servers acting as Reverse Proxies for macOS Agent collections.	ADG.WeblabSelfHost.exe.config file on the FTK Web Service host. Public certificate (.CER - DER) should be derived from this PFX and added to all macOS Agent Keychains if a reverse proxy is not in use and validateCertificate is set to true	Server
Agent Validation Certificate - agentCertificateFileName	PFX - PKCS#12	Authenticates and secures communication between the FTK Web Service and macOS Agents.	ADG.WeblabSelfHost.exe.config file on the FTK Web Service host	Server
Agent Validation Certificate - ClientCertificatePath	CER - X.509 DER		agentinstall.config file on macOS Agents	Client
Site Server Managed API Certificate (Deployment Type 1)	PFX - PKCS#12	Secures HTTPS communication between macOS Agents and the Site Servers Managed API.	Agent Check-In configuration tab within the Site Server Config UI. Public certificate (.CER - DER) should be derived from this PFX and added to all macOS Agent Keychains if a reverse proxy is in use and validateCertificate is set to true.	Server

© Exterro, Inc. All rights reserved

Host Entries (Deployment Type 2 Only)

For Deployment Type 2, the below provided steps should be performed to establish a connection between Mac Agent and FTK Central application:

In Mac agent:

1. Open the Terminal.
2. Execute the below command

```
sudo nano/etc/hosts
```

3. Provide the Agent IP, in case of off network pass public IP and URL

```
<FTKC application IP address><space><URL>
```

In FTK Central server:

1. Navigate to the below location:

```
C:\Windows\System32\drivers\etc\hosts
```

2. Provide the mac agent IP address and URL in the below format:

```
<MAC IP address><Tab><hostname of the MAC machine>
```

© Exterro, Inc. All rights reserved

macOS Agent Location

The following location stores macOS Agent installers for both ARM/Intel processors:

```
C:\Program Files\AccessData\Forensic Tools\<Version>\bin\Agent\MAC
```

- **For Mac with an Apple Silicon processor** - ARM version of the agent installer
  - **Installer name:** ExterroEnterpriseMacAgent-installer-arm64-(Agent_version)
- **For Mac with an Intel processor** - X64 version of the agent installer
  - **Installer name:** ExterroEnterpriseMacAgent-installer-x64-(Agent_version)

Temporary Location

The following path is required on the server hosting the FTK Web Service. This folder will serve as the upload location for any data transferred by a given macOS Agent. This is the default path required for macOS Agent collections; **however, this can be customized based on an organization's requirements.**

```
C:\temp\managed_agent_uploads
```

- This folder should be accessible by the Service Account used during installation of FTK and its related components.
  - The Service Account should have full read/write permissions available.

© Exterro, Inc. All rights reserved

Site Server (Deployment Type 1 Only)

Site Server

To enable communication between macOS Agents and the FTK Web Service, a Site Server must be deployed. This server acts as an intermediary, ensuring that direct communication between external agents and the FTK Web Service is avoided.

While this deployment deviates from traditional site server configurations, it leverages the Managed Site Server API specifically for check-ins and reverse proxy functionality. This solution is designed to operate seamlessly with minimal setup required, providing an efficient and secure communication pathway.

The FQDN/IP of the system should be added as the value for the **ServerBaseUris** configuration in the macOS Agent configuration file (agentinstall.config).

Note: The Site Server Managed API will run and start automatically regardless of the Site Server type being used.

© Exterro, Inc. All rights reserved

Site Server Installation

The following steps should be followed if an environment does not have an existing site server available for use with the macOS Agent:

1. Download the latest Site Server available here.
2. Extract the Site Server ZIP file.
3. Open and run the **Exterro_Site_Server.exe** file as an Administrator.
4. Click **Next** on the Welcome page.
5. Read and **Accept** the License Agreement.
6. Click **Next**.
7. Select the Installation Location and click **Next**.

   Default: *C:\Program Files\AccessData*

8. Select the **Specific User Account** and enter the **User Credentials** used for installing all FTK Components.
   - The credentials required are typically those of the Service Account used during the installation of FTK and its associated components. This account must be a member of the local administrators' group to ensure proper permissions. Use of the "Local System" account is recommended only if all components, including case and evidence storage, are hosted on a single machine.
9. Click **Next**.
10. Click **Install**.
11. Once the installation has completed, perform the following steps:
    a. Check Open Site Server Config.
    b. Click Finish once the installation is complete.
    c. Follow the steps in the Site Server Configuration section.

© Exterro, Inc. All rights reserved

Configuring FTK Web Service Settings

The following steps should be followed once the prerequisites are completed:

1. Open the Windows Services and stop the Exterro Self Host Service.
2. Open the below provided file in a text editor *(**Example:** Notepad++):*

```
C:\Program Files\AccessData\ForensicTools\8.1\bin\ADG.WeblabSelfHost.exe.config
```

3. Change the value of the certificateFileName setting to the full file path of the PFX file.

   Example:

```
<add key="certificateFileName" value="C:\Program
Files\AccessData\Certificates\myCertificateui.pfx" />
```

Note: The certificateFileName (.PFX) must be in the same directory as **ADG.WebLabSelfhost.exe** otherwise a full path must be provided.

4. Change the value of the certificatePassword setting to the password entered when creating the PFX certificate.

   Example:

```
<add key="certificatePassword" value="myPassword" />
```

Note: The password string should be provided in clear text, it will then be encrypted when the Exterro Self Host Service is restarted.

5. (Optional) Change the value of the **ManagedAgentApiPort** setting to the port for use with Mac agents; the FTK Web Service presents the (certificateFileName) certificate on the specified port.

Component	Inbound Port Required
FTK Web Server	4446

© Exterro, Inc. All rights reserved

6. (Optional) Change the value of the **agentCertificateFileName** setting to the full file path of the PFX file if a custom certificate is required in a deployment.

Note: A default certificate is provided and configured for both the FTK Web Service and macOS Agent. Should a custom certificate be provided in the agentCertificateFileName configuration; the agentinstall.config > ClientCertificateFileName must have a path to a public certificate explicitly mentioned (derived from the agentCertificateFileName).

Example:

```
<add key="certificateFileName" value="C:\Program
Files\AccessData\Certificates\myCertificateui.pfx" />
```

Note: The agentCertificateFileName (.PFX) must be in the same directory as **ADG.WebLabSelfhost.exe** otherwise a full path must be provided.

7. (Optional) Change the value of the **agentCertificatePassword** setting to the password entered when creating the PFX certificate.

Example:

```
<add key="agentCertificatePassword" value="myPassword" />
```

Note: The password string should be provided in clear text, it will then be encrypted when the **Exterro Self Host Service** is restarted.

© Exterro, Inc. All rights reserved

8. Change the value of the **ManagedAgentUploadFolder** setting to the location where you would like the agent to store temporary upload files during collections.

Notes:

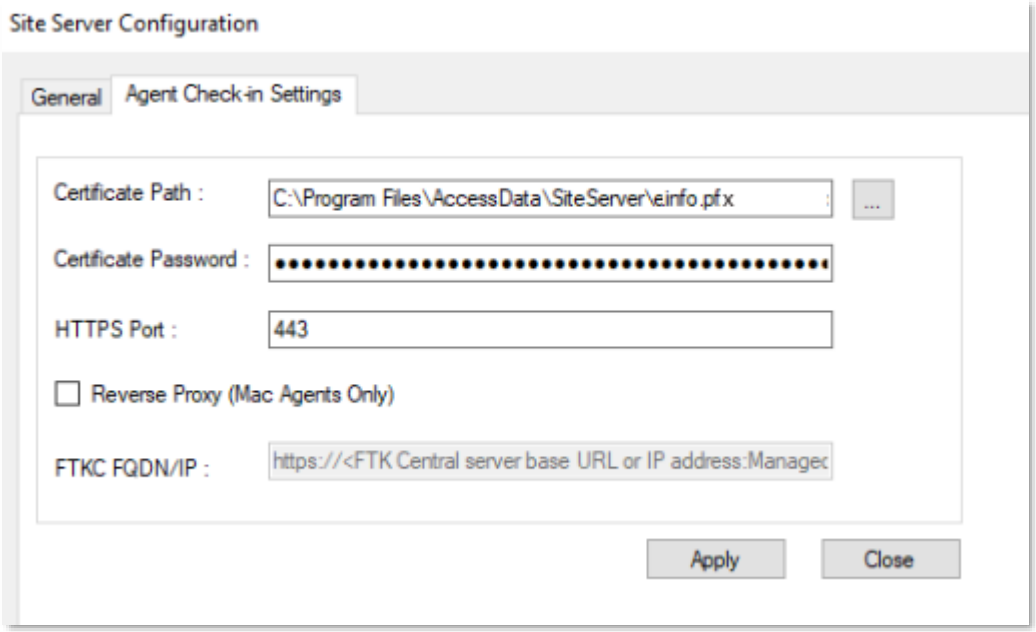
- Ensure the directory specified in the **ManagedAgentUploadFolder** setting exists in the temp folder. The upload directory can be a file share or drive path.
- The default value for this configuration is **C:\temp\managed_agent_uploads**.

9. Restart the **Exterro Self Host Service.**

© Exterro, Inc. All rights reserved

Configuring FTK Site Server Settings (Deployment Type 1 Only)

The following steps should be followed once a Site Server has been successfully installed. The following steps will ensure minimal configurations are made to enable macOS Agent connectivity.



1. Open the **Configure Site Server** application as an Administrator.
2. Select the **Agent Check-in Settings** tab.
3. Browser and select a Certificate within the **Certificate Path**.
4. Provide the **Certificate Password.**

Note: Passwords must be provided in plain text and will be encrypted automatically when the Managed Site Server service restarts.

5. Provide the value for HTTPS Port.
   - 443 is the default port used; however, users can customize this as required.

© Exterro, Inc. All rights reserved

- This port determines where agents can check-in through.

6. Check the **Reverse Proxy (Mac Agents Only)** option.
7. Provide the value in the below syntax for the **FTKC FQDN/IP** field:

```
<FTK Central application URL>:<managed API Port>
```

Note: The FTKC FQDN/IP field will be enabled only upon checking the **Reverse Proxy (Mac Agents Only)** field. The Managed Agent API Port relates to the FTK Web Service Configuration key: **ManagedAgentApiPort.** By default, this port is set to 4446.

8. Click **Apply** to save the configurations made in the **Agent Check-in Settings** section.
   - Upon clicking Apply, the Exterro Site Server Managed API will be restarted.

© Exterro, Inc. All rights reserved

Installing the macOS Agent

Locating the Agent Installer

To locate the agent installer:

1. Navigate to the below location in the FTK Central server:

   C:\Program Files\AccessData\Forensic Tools\<Version>\bin\Agent\MAC

2. Copy any one of the following agent installers into the Mac machine (based on the Mac machine in which the installation should be performed):
   - **For Mac with an Apple Silicon processor** - ARM version of the agent installer
     - **Installer name:** ExterroEnterpriseMacAgent-installer-arm64-(Agent_version)
   - **For Mac with an Intel processor** - X64 version of the agent installer
     - **Installer name:** ExterroEnterpriseMacAgent-installer-x64-(Agent_version)

3. (Optional) Copy the custom public .CER certificate which will be used for the Mac Agent into the Mac machine (based on the Mac machine in which the installation should be performed).

   Note: This public certificate should be derived from the custom .PFX certificate configured in the ADG.weblabselfhost.exe.config > agentCertificateFileName configuration. If these certificates do not match, macOS Agents will have communication issues.

   Warning: During installation ensure both the .CER certificate and agent installer are stored in the same location of the Mac machine.

4. Locate the **ExterroEnterpriseMacAgent.zip.**
5. Move the required ZIP file (x64 or arm64) into the agent.
6. Extract the zip file in the agent to obtain the **agentinstall.config** and **ExterroEnterpriseMacAgent**(x64/arm64.pkg)

© Exterro, Inc. All rights reserved

Configuring the Agent Installation Parameters

Note: Ensure the **Exterro Site Server Managed API** service is running in your machine before performing the below steps**.**

To configure the agent installation parameters:

1. Open the **agentinstall.config** in a text editor.
2. Update the **ServerBaseUris** value to the server and port of your server separated with a colon (:).

Syntax for Single Server:

```
<servername_or_public_ip>:<port number>
```

Example:

ServerBaseUris=ftkc.example.com:443

Syntax for Multiple Servers:

```
<servername_or_public_ip>:<port number>,<servername_or_public_ip>:<port number>
```

Example:

ServerBaseUris=ftkc.example.com:443,172.31.15.195:4446

© Exterro, Inc. All rights reserved

Note: The **<servername_or_public_ip>** should be replaced with the value of:

- The fully qualified domain name (FQDN) or IP of the Site Server (Deployment Type 1)
- The fully qualified domain name (FQDN) or IP of the FTK Web Service (Deployment Type 2)

The **<port number>** should be replaced with the value of:

- HTTPS Port configuration present in the Site Server (Deployment Type 1)
- ManagedAgentApiPort configuration present in the ADG.WeblabSelfHost.exe.config (Deployment Type 2)

3. (Optional) Update the ClientCertificatePath value to the public certificate derived from the PFX configured for the agentCertificateFileName if a custom certificate has been configured.

© Exterro, Inc. All rights reserved

Agentinstall.config - Common Configurations - Reference

Warning: The configuration file contains many configurations, some of which are not recommended to be edited. The following configurations listed are common configurations.

Configuration	Default Value	Description
ServerPollIntervalSeconds	1800	Time interval for agent check-in. This value should be provided in seconds. ***Example:*** *1800 = 30 Minutes* ***Note:*** *The minimum value recommended to set for this configuration is 300.*
ServerBaseUris	FTKC dns/Server name	Server to which the agent has to be connected with, followed by the port. **Example Deployment Type 1:** exampleserver.com:[HTTPS PORT - Site Server] **Example Deployment Type 2:** exampleserver.com:[ManagedAgentApiPort - FTK Web Service] ***Note:*** *You can add multiple URLs (belonging to the same server) separated with commas (,).* **Example:**

© Exterro, Inc. All rights reserved

Configuration	Default Value	Description
		ServerBaseUris=ftkc.example.com:443,172.31.15.195:4446 In this case, the first address is publicly accessible, and the IP address is internal only. This allows users to use an agent in hybrid environments, where they are roaming across public/private networks.
validateCertificate	false	Set to false by default. The certificate presented by the FTK Web Service (Deployment Type 2) or Site Server (Deployment Type 1) will not be validated by the macOS Agent. If validateCertificate is set to true, the agent would expect a trusted certificate to be presented to the macOS Agent during collections and check-ins.
ClientCertificatePath	-	Client certificate path is the public certificate used to initiate trust with the FTK Web Service, allowing Live Preview. A certificate should be explicitly mentioned if a custom certificate has been provided for the agentCertificateFileName configuration in the ADG.weblabselfhost.exe.config file.
CollectionFailedFileCount	0	The maximum number of failed files allowed during the collection process. If the number of files exceeds this value, the collection will fail.

© Exterro, Inc. All rights reserved

Note: The configurations above can be accessed and updated after the installation from the following appsettings.json file in the below location:

```
/Library/ExterroEnterprise/(agent version)/appsettings.json
```

After making the changes/updates to the file, the Agent should be restarted by executing the below command in the terminal:

```
sudo adagent restart
```

© Exterro, Inc. All rights reserved

Installing the agent

Prerequisites:

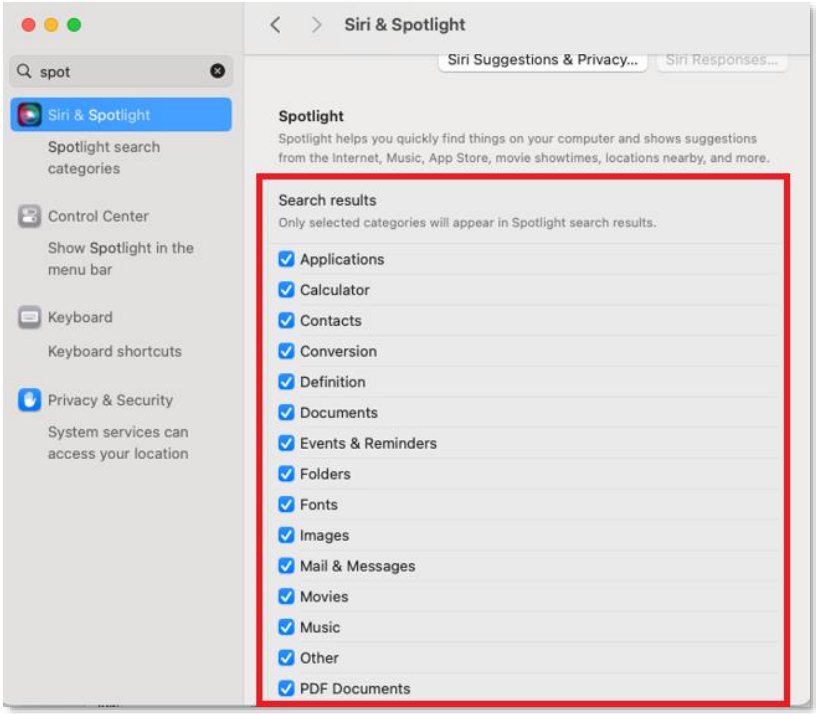
Spotlight Indexing must be enabled to perform Searching/Filtered Collections on MacOS Agents. Failure to enable Spotlight indexing will result in 0 search result hits.

Note: *The Spotlight indexing is enabled by default. However, you are recommended to check and ensure if the option is enabled.*

You can follow the below steps to enable Spotlight Indexing if it is disabled:

To enable spotlight indexing:

1. Navigate to the System Settings in your machine.
2. Search for 'Spotlight'.
3. Select all the Spotlight categories displayed in the right pane.



© Exterro, Inc. All rights reserved

To install the agent:

Warnings:

- During installation ensure both the .CER certificate and agent installer are present in the same location of the Mac machine if using custom certificates.
- If you want to use custom certificates instead of the default ones, you should change the value of 'validateCertificate property' to 'True' in the agentinstall.config file.

1. Double click on the package installer file to install the agent.

Installer file name:

ExterroEnterpriseMacAgent-installer-arm64-(Agent_version)/ExterroEnterpriseMacAgent-installer-x64-(Agent_version)

Note: During the installation, you will be prompted multiple times (may vary on differing macOS version) to allow permission intended to perform the following actions:

- To access the agentinstall.config file
- To access the client certificate file
- To move the Mac agent package to the trash

You are recommended to click on **Allow** for all prompts, they are mandatory for the installation process.

© Exterro, Inc. All rights reserved

Ensuring Full Disk Access for the agent

To ensure Full Disk access for the agent:

1. Navigate to the System Preferences > Privacy and Security in the Mac.
2. Select Full Disk Access from the list of settings.
3. Ensure that the following options have been granted with the full disk access:

Application	Purpose
/Library/ExterroEnterpriseMacAgent>/ADG.ManagedAgentSvc	Required for full disk collections. ***Note:*** *This application's permissions should be enabled upon upgrading the Mac Agent version for the FTK 8.2 SP1 and lower versions.*

© Exterro, Inc. All rights reserved

macOS Agent Log Locations

System	Logs Location
Agent	~/Library/ExterroEnterpriseMacAgent/Logs
FTK Web Server	%PUBLIC%\Documents\AccessData\AccessDataLogs\adgselfhost.txt
Site Server (Site Server Managed API)	C:\Users\Public\Documents\AccessData\AccessDataLogs\SiteServerManagedHostLog.txt
Site Server (Reverse Proxy)	C:\Users\Public\Documents\AccessData\AccessDataLogs\MacReverseProxyHostLog.txt

Uninstalling the macOS Agent

Agents can be uninstalled using the command below:

```
sudo bash /Library/ExterroEnterpriseMacAgent/uninstall.sh
```

Note: *While upgrading the Agents of FTK 8.2 SP2 and later versions, the older versions of the Agents will be automatically uninstalled.*

© Exterro, Inc. All rights reserved

Stop/Restart the macOS Agent

Agents can be started/restarted using the command below:

```
sudo adagent restart
```

Agents can be stopped using the command below:

```
sudo adagent stop
```

Pushing the macOS Agent

The macOS agent can be pushed to Mac systems using **jamf PRO** based on configured **Jamf policies**. Once a macOS device has been enrolled to jamf and the agent has been pushed, enrolled devices will check in with jamf PRO every 5 minutes by default to pull down any updated policies. For this documentation, it is assumed that your organization's jamf PRO installation meets the following prerequisites.

Jamf PRO Prerequisites

- The targeted machines should be enrolled in **JAMF** with the ability to manage **Policies** and **Configuration Profiles**.
- A Mac with a manually installed **Agent** is required to obtain baseline information.

***Note**: You can refer to the **Exterro FTK 8.2 SP2 Mac Agent - Deployment Guide (via JAMF Pro)** for more information.*

© Exterro, Inc. All rights reserved

Installing the Legacy Mac Agent

The following sections relate only to the legacy Mac agent (Sierra 10.12 and older).

This section covers the following tasks:

- Installing the macOS Managed Agent.
- Building the Mac OS X Agent Package.
- Configuring the Mac OS X Agent's Network Port.
- Installing the Mac OS X Agent.
- Uninstalling the Mac OS X Agent.

Configuring the AccessData Mac OS X Agent Install Package

The AccessData Agent requires an X.509 certificate in order to establish a secure network connection to the server or for FTK Enterprise, the computer running Examiner. The package installer has been provided to aid in the distribution efforts of these certificates by allowing an Administrator to modify the AccessDataAgent package installer prior to installation of AccessData Agent software for Apple Macintosh. In addition to certificate distribution, the port used by the Agent can be configured.

The following instructions allow an Administrator to configure the AccessData Agent package installer.

© Exterro, Inc. All rights reserved

Building the Mac OS X Agent Package

The **AccessData Mac** Agent installer requires that a certificate (or certificate tree) is bundled with the installer. The following is the sequence of steps that must be followed to bundle a certificate file into the installer.

1. Make a copy of your **AccessData Enterprise** agent public certificate available to your system.
2. Locate the **Mac Agent installer MPKG** file.

Note: Agent packages are found under *\Enterprise\Agents* folder on the FTK Enterprise installation media.

3. Using a package manager (or right-click **Show Package Contents** on a Mac system), open the **MPKG** to display the package contents.
4. Within the **MPKG**, create a new folder, called **Configure**.
5. Copy the public certificate file to the **Configure** folder.
6. Rename the public certificate file to **adagent.cert**.
7. **(Optional)**: If you wish to change the default port that the agent listens on, create a new text file within the **Configure** folder containing nothing but the desired port number, and name the file **adagent.port**. The Mac agent package is now ready for deployment to target systems.

© Exterro, Inc. All rights reserved

Configuring the Mac OS X Agent's Network Port

The **AccessDataAgent** installer allows an Administrator to (optionally) configure the port the Agent will use to communicate with an Examiner when installed. This is done by adding a file containing the port number to the AccessDataAgent package installer. The following is a set of instructions an Administrator will use to configure the AccessData Agent package installer. To do so, complete Steps 1-5 under Bundling a Certificate, then continue with Step 1 here. If you do not need to do a custom configuration of the port, skip to Step 6 below.

8. Create a text file named **adagent.port** that contains the port number the Agent is to use; this file is to be distributed to each installation of the Agent.
9. Place the **adagent.port** file into the Configure folder (previously created to contain the X.509 certificate).
10. Right-click the **AccessDataAgent** package installer file.
11. Select **Show Package Contents** popup menu item.
12. Ensure that the **Configure** folder is located in the same folder opened in Step 4 (alongside the Contents folder).
13. Close the window.

Note: The installer will not run successfully if all of the above steps are not already completed. The folder and file names must be exactly as documented.

© Exterro, Inc. All rights reserved

Mac OS X Agent Additional Configuration Options

The **Mac installer** supports the same settings as the **Linux installer**. Each setting should be added as a file inside a Configure directory inside the **mpkg** folder.

Enterprise Mac Agent Configuration Options:

Option (filename)	Result
adagent.cert	Specifies the certificate file used for communication
adagent.port	Specifies the port the agent will listen on. The setting should contain nothing more than a number. The default port number is 4999
adagent.lifetime	Specifies the amount of time before the agent dissolves. Again the file should contain nothing more than a number. Same rules as for the Linux agent about sign and value. The default is 0.
adagent.connections	Sets the maximum number of concurrent connections allowed by the agent. The file should contain only a number. The default is 10.
adagent.size	Sets the protected storage area size. The file should contain only the number. The default is 16777216. (16 MB).

Installing the Mac OS X Agent

When the certificate is bundled and the port configuration file is complete and saved, distribute the AccessDataAgent package installer to each target computer and run it locally.

1. Copy the **MPKG** to the root of the drive / authenticating if prompted.
2. Double-click the **MPKG** file to install the **Enterprise Agent**.

© Exterro, Inc. All rights reserved

Uninstalling the Mac OS X Agent

The **AccessData Mac Agent** can be uninstalled via the provided utility.

1. Log in to the Mac system as a system administrator account.
2. Browse to the following directory:

   /Library/Application Support/AccessData

3. Double-click the uninstall utility.
4. Enter the current user password.

Note: If the system administrator account does not have a password associated to it, a password must be assigned in order to run the uninstall utility.

© Exterro, Inc. All rights reserved

References

This section provides you example workflows within FTK Central. However, it is not mandatory for you to follow the same workflow as your usage may vary.

FTK Central Workflow

Step	Tasks
1.	Configure and setup FTK Central and the users before collecting evidence.
2.	Add Custodian, Network shares, computers, and groups whose data you want to collect.
3.	Create a Case.
4.	Create a litigation hold. (Optional)
5.	Collect evidence from the people, network shares, computers, and groups that you added.
6.	Approve, execute, and then process a collection.
7.	Review data. After you process a collection, you open the resulting case from the Case List into Review. From Review, you filter, search, and apply labels on the processed data until you have a dataset that contains only relevant files for the case.
8.	Export the dataset to a load file.

© Exterro, Inc. All rights reserved

Administrators Workflow

Step	Tasks
1.	Active Directory Configuration.
2.	Manage users, groups, and roles.
3.	Configure default case settings.

Case Managers Workflow

Step	Tasks
1.	Create a Case.
2.	Configure the user/group permissions for a Case.
3.	Loading Data.
4.	Manage evidence and custodians.
5.	Configure the review tools to be used in case review.
6.	View details about the case.
7.	Monitor the processing jobs.
8.	Manage Document Groups.
9.	Create Production Sets.
10.	Export the selected evidence.
11.	Run reports.

Data Sources Workflow

Step	Tasks
1.	Configure the application to collect from a public data source.
2.	Run a collection job.

© Exterro, Inc. All rights reserved

Supported File Systems And Drive Image Formats

This appendix lists the file systems and image formats that are analyzed.

File Systems

The following list describes the file systems identified and analyzed by FTK Central:

Identified and Analyzed File Systems

- APFS
- AFF4
  - HFS, HFS+
- CDFS
  - JFS
- EFS
  - NTFS
- exFAT
  - ReiserFS 3
- Ext2FS
  - UFS1, UFS2
- Ext3FS
  - VxFS (Veritas File System)
- Ext4FS
  - Windows 8 and Server 2012 ReFS
- FAT 12, FAT 16, FAT 32
  - XFS
- Android
  - Physical Images, File System Images, Android Backups (.adb) encrypted/unencrypted, UFD.
- iOS
  - Full File System Images.

© Exterro, Inc. All rights reserved

Recognized and Analyzed Whole Disk Encryption Formats

The following table lists identified and analyzed Whole Disk Encryption (WDE) decryption products (these all require the investigator to enter the password, FTK products don't "crack" these):

- APFS Encrypted
    - McAfee Drive Encryption
- Apple FileVault
    - Microsoft Windows Bitlocker
- Apple FileVault 2
    - PGPDisk®
- Checkpoint / PointSec R73 7.4.5
    - SecureDoc WinMagic AES
- Checkpoint 7.6.150 with token challenge
    - Symantec Endpoint Encryption (formerly Guardian Edge)
- Dell Encryption
    - Symantec Drive Encryption (PGP WDE) 10.0 (only)
- Guardian Edge
    - Utimaco Safeguard Easy
- McAfee Endpoint Encryption (Safeboot 5.x / 6.0
    - Utimaco SafeGuard Enterprise

© Exterro, Inc. All rights reserved

Hard Disk Image Formats

The following table lists identified and analyzed hard disk image formats:

Supported Hard Disk Image Formats

- AccessData Logical Image (AD1)
  - Lx0, Lx01
- AFF (Advanced Forensic Format)
  - LVM, LVM2
- Apple Disk Image Files (*.dmg)
  - LVM2
- CTR (X-Ways)
  - MSVHD (MS Virtual Hard Disk)
- Encase E01, including 'incomplete' Tableau- created files
  - Nero Image Files (*.nrg)
- Encase EX01
  - Raw (*.001,*.1,*.bin,*.dd,*.gho,*.raw,*.img)
- Encase L01 Logical Image
  - Safeback 2.0 and under
- Expert Witness
  - SMART Image Files (*.s01)
- Ghost (forensic images only)
  - SnapBack
- ICS
  - Virtual Box Images (*.vdi)
- Image Files *.img *.ima
  - VMWare (*.vmdk)
- Linux DD
  - YAFFS Images (*.yaffs1,*.yaffs2)
  - Virtual Hard Disk (*.vhd, *.vhdx)

© Exterro, Inc. All rights reserved

Supported CD and DVD Formats

The following table lists identified and analyzed CD and DVD image formats:

- Alcohol (*.mds)
    - PlexTools (*.pxi)
- BDAV
    - Roxio (*.cif)
- CloneCD (*.ccd)
    - SACD
- ISO
    - SVCD
- IsoBuster CUE
    - VCD
- Nero (*.nrg)
    - Virtual CD (*.vc4)
- Pinnacle (*.pdi)
    - Virtual CD (*.vc4)

© Exterro, Inc. All rights reserved

exterro
Data Risk Management

We'd love to hear from you

Our team will be happy to help you on any questions. Write to us!

support@exterro.com

Copyright © 2024 Exterro, Inc.