exterro®
Data Risk Management

KNOWN FILE FILTER (KFF) INSTALLATION GUIDE

JULY 2026

Table of Contents

About Exterro

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

1 What is 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 filename 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.

How KFF Works

The Known File Filter (KFF) is a body of MD5 and SHA1 hash values computed from electronic files. Some predefined data is gathered and cataloged by several US federal government agencies or you can configure your own. KFF is used to locate files residing within case evidence that have been previously encountered by other investigators or archivists. Identifying previously cataloged (known) files within a case can expedite its investigation.

When evidence is processed with the MD5 Hash (and/or SHA-1 Hash) and KFF options, a hash value for each file item within the evidence is computed, and that newly computed hash value is searched for within the KFF data. Every file item whose hash value is found in the KFF is considered to be a known file.

Notes:

- If two hash sets in the same group have the same MD5 hash value, they must have the same metadata.
- If you change the metadata of one hash set, all hash sets in the group with the same MD5 hash file will be updated to the same metadata.

The KFF data is organized into Groups and stored in the KFF Server. The KFF Server service performs lookup functions.

2 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.
- **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 into 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.

KFF Components

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 contain 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 Group or 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 predefined collection of hashes that you can import into the KFF Server. You can use the following predefined libraries: • NSRL • NDIC HashKeeper (End of life) • DHS • For law enforcement users, you can also use Case VIC/CAID libraries.

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 filename or extension.

You can also import hashes into the KFF Server that are contained in .tsv, .csv .hke, .hdi, .hdb, .hash, .nsrl, .db or .kff file formats. You can also manually add hashes.

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

Hash Sets must be organized into KFF Groups before they can be utilized in a case.

3 Installing & Upgrading the KFF

Determining where to install the KFF

For FTK Lab/Enterprise and FTK Central, the KFF Server can be installed on a different system if required. **However, it can be installed on the same computer that runs FTK Lab/Enterprise and FTK Central.**

For FTK and FTK Pro applications, the KFF Server must be installed on the same computer that runs the FTK Examiner application.

Installing the KFF

Prerequisites:

- Python 2.7 (x64)
  - This will be installed during the installation of Cassandra.
- Java 8u241 (x64) or newer
  - This must be downloaded and installed prior to the installation of the KFF –Download Here.
- Microsoft Visual C++ 2010 (x64)
  - This must be downloaded and installed prior to the installation of KFF/Cassandra - Download Here.

Steps to Install:

1. Mount the KFF .ISO.
2. Navigate to ("<Drive>:**autorun.exe**").
3. Run the **autorun** executable as an **administrator**.
4. Click **Cassandra 64 bit**.
5. Review and accept the License Agreement and click **Next**.
6. Verify or change the **Destination Folder** and click **Next**.
7. If utilizing a multi-box setup, check and configure **Enable Remote Access**.

Warning: This will be required if you decide to use a remote KFF server. If installing on the same system, then you do not need to check this.

   i. In the **RPC_Address** field, enter the **IP Address or DNS Name** of the computer you are installing on. For example, KFFServer.local.

ii. In the **Port to use** field, leave the default 9042.

iii. Click **Next**.

8. If **Remote Access** was enabled, set the User Credentials for the service and click **Next**.

> **Warning:** This account should be a member of the local administrator's group and be a domain-level account in a multi-box environment.

9. Click **Install** to perform the installation.
10. Click **Finish**.
11. Restart FTK/Lab/Enterprise/Central if they were already open.

Upgrading Cassandra 3.11.2.4 to 3.11.11.9

Prerequisites:

- Java 8u241 or newer (x64)
  - This must be downloaded and installed prior to the installation of the KFF –Download Here.
- Uninstall the existing Cassandra version.
  - Previously imported hash sets and groups will not be removed. Users will still have access to these without the need to re-import them.
- Microsoft Visual C++ 2010 (x64)
  - This must be downloaded and installed prior to the installation of KFF/Cassandra - Download Here.

Steps to Upgrade:

1. Mount the KFF .ISO.
2. Navigate to ("<Drive>:\Cassandra**AccessData_Cassandra_Installer.exe**").
3. Run the **AccessData_Cassandra_Installer** executable as an **administrator**.
4. Click **Next**.
5. Review and accept the License Agreement and click **Next**.
6. Change the **Destination Folder** to the path used by the previous Cassandra installation and click **Next.**
7. If utilizing a multi-box setup, check and configure **Enable Remote Access**.

> **Warning:** This will be required if you decide to use a remote KFF server. If installing on the same system, then you do not need to check this.

i. In the **RPC_Address** field, enter the IP Address or DNS Name of the computer you are installing on. For example, KFFServer.local.
ii. In the **Port to use** field, leave the default 9042.
iii. Click **Next**.

8. If **Remote Access** was enabled, set the User Credentials for the service and click **Next**.

> **Warning:** This account should be a member of the local administrator's group and be a domain-level account in a multi-box environment.

9. Click **Install** to perform the installation.
10. Click **Finish**.
11. Restart FTK/Lab/Enterprise/Central if they were already open.

Configuring the KFF Server Location on FTK/Lab/Enterprise

> **Warning:** To configure KFF within FTK/Lab/Enterprise/Central, you must be logged in with a user account with admin privileges.

Steps to Configure:

1. In the **Case Manager**, click **Tools > Preferences > Configure KFF**.
2. You can set or view the address of the KFF Server.
   - If you installed the KFF Server as local on the same computer as the application, this value must remain as **localhost**.
   - If you installed the KFF Server as a remote instance.
3. Click **Test Server**.
4. Click **Save**.
5. Click **OK**.

Configuring the KFF Server Location on FTK Central and FTK Plus

Steps to Configure:

1. Navigate to ("<Drive>:**Program Files\AccessData\Forensic Tools\<Version>\bin**").

2. Open **ADG.WeblabSelfHost.exe.config** in a text editor.
3. Locate the **KFFServerURL** configuration key.
4. Modify the configuration key value to match KFF Server IP/Hostname and port.

```
<add key="KFFServerURL" value="KFFServer:9042" />
```

5. Save the changes made to the configuration file.
6. Restart the **Exterro Self Host Service**.

4 Importing KFF Data

About KFF Import Utility

Due to the large size of some KFF data, a stand-alone KFF Import utility is available to use to import the data. This KFF Import utility can import large amounts of data faster than using the import feature in the application as well as allowing users to actively use FTK while imports are occurring.

It is required that you install and use the KFF Import utility to import pre-configured libraries such as NIST NSRL.

Installing the KFF Import Utility

Steps to Install:

1. Mount the KFF .ISO.
2. Navigate to ("<Drive>:**autorun.exe**").
3. Run the **autorun** executable as an **administrator**.
4. Click **Install KFF Import Utility 64 bit**.
   - Support for SQLite hash sets have been added to the latest Import Utility available here.
5. Click **Next**.
6. Review and accept the License Agreement and click **Next**.
7. Verify or change the **Destination Folder** and click **Next**.
8. Click **Install**.

Importing a CSV Using the KFF Import Utility

Steps to Import:

1. Open the **KFF Import Utility** as an **Administrator**.
2. Click **Browse** and locate the CSV that you would like to import.
3. Click **Open**.
4. (Optional) – Enter **Default Set** details.
5. If a remote KFF Server was installed, in the **Server Address** field, you must enter the IP address of the computer that has the KFF Server installed to it. **Otherwise leave this as localhost.**
6. Click **Import**.
7. Click **OK**.

Importing the NIST NSRL Library (Legacy Format)

Steps to Import:

1. Open and extract the **nsrlsource_2.54** ZIP folder to a folder located on the KFF Server.
   - For example, create a folder named **NSRL**.
2. Extract **NSRLFile.txt**.
   - This file will be in excess of 20GB.
3. Open the **KFF Import Utility** as an **Administrator**.
4. Click **Browse** and locate the NSRLFile.txt file you would like to import.
5. Click **Open**.
6. Enter **Default Set** details *(This step is optional)*.
7. If a remote KFF Server was installed, in the **Server Address** field, you must enter the IP address of the computer that has the KFF Server installed to it. **Otherwise leave this as localhost.**
8. Click **Import**.
9. Click **OK**.

Warning: This import process can take several hours. Users can monitor the progress using the progress bar located at the bottom of the KFF Import Utility. When the import is complete, a prompt will appear notifying that the import process has completed.

Importing the NIST NSRL Library (Latest RDSv3 - SQL Format)

Prerequisites: Please refer to the **Installing the KFF Import Utility** **section and ensure the latest Import Utility is downloaded.**

Steps to Import:

1. On the KFF Server, run the 7.6 or later version of the KFF Import Utility **as an Administrator**.

   ***Note**: Failure to run the application as an Administrator may result in ingestion failures.*

2. In the File to Import field, browse to and select the **.DB** file (if using the latest RDSv3 format - this is only compatible with version 7.6+ of the KFF Import Utility).
   a. It is imperative that the FULL RDS set is ingested first before attempting to import any other Delta sets.
3. If a remote KFF Server was installed, in the **Server Address** field, you must enter the IP address of the computer that has the KFF Server installed to it. **Otherwise leave this as localhost.**
4. Click **Import**.
5. Click **OK**.

Warning: This import process can take several hours. Users can monitor the progress using the progress bar located at the bottom of the KFF Import Utility. When the import is complete, a prompt will appear notifying that the import process has completed.

5 RocksDB KFF Configuration

Overview

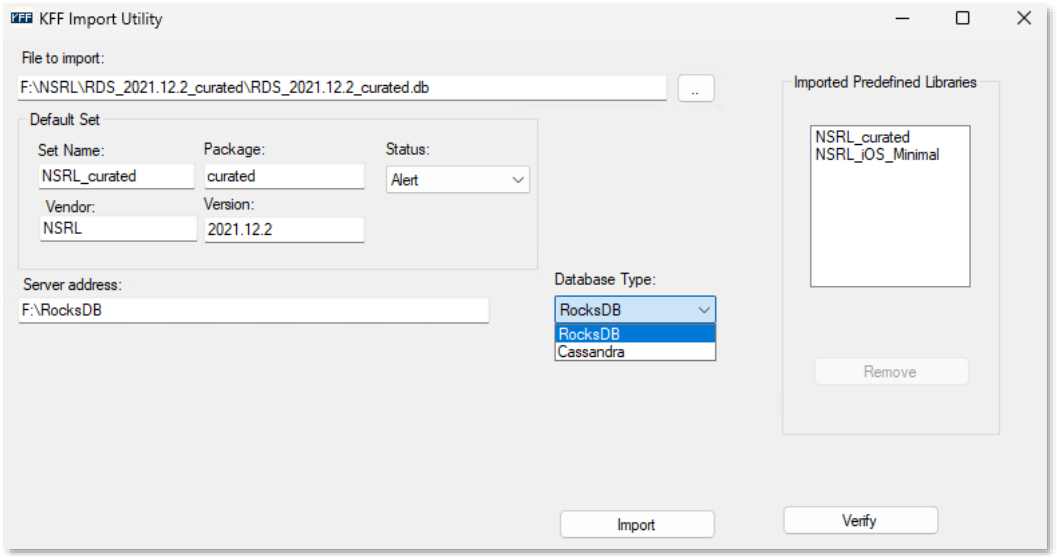
RocksDB is an advanced high-performance database integrated to support Known File Filter (KFF) cross-hash matching. It replaces Apache Cassandra to deliver faster retrieval times and increased processing efficiency.

KFF Import Utility Setup

When importing hash sets using the **KFF Import Utility**, users can select between **Cassandra** and **RocksDB**.

Configuration Steps

1. Open the **KFF Import Utility**.
2. Select the **Database Type**:
    - **Cassandra:** Uses standard legacy configuration parameters.
    - **RocksDB:** Requires a target directory path.
3. In the **Server address** field, specify the full local folder path where the RocksDB database should be created (or where an existing RocksDB database resides, e.g., **F:\RocksDB**).
    - *If an existing RocksDB path is specified, the utility automatically populates all existing dataset information.*
4. Configure dataset details (**Set Name**, **Package**, **Vendor**, **Version**) as needed, then click **Import**.

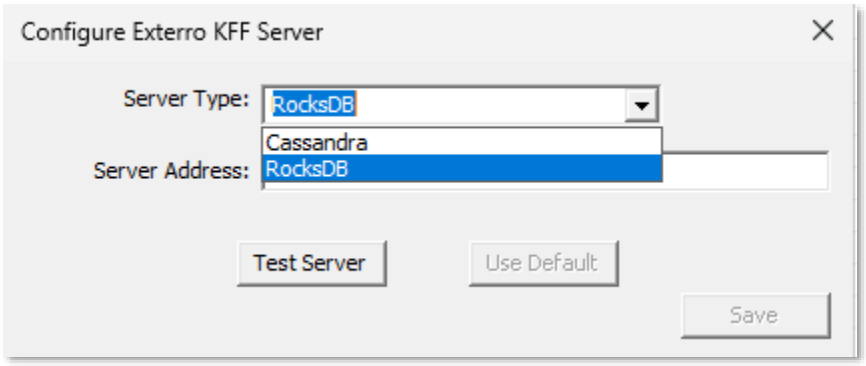


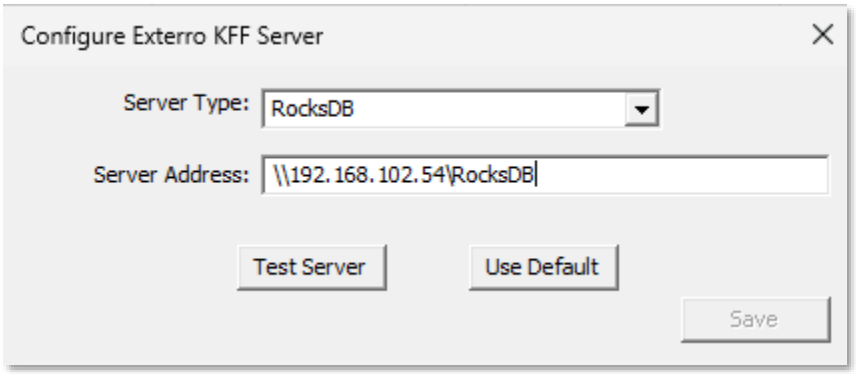
Note: Always import KFF data locally. *To prevent database corruption, data loss, or network dropouts, import datasets directly on the local machine hosting the RocksDB directory. Do not perform data imports over remote network shares. Remote share paths should only be used during evidence processing/read operations.*

Server Configuration

FTK (Desktop) Setup

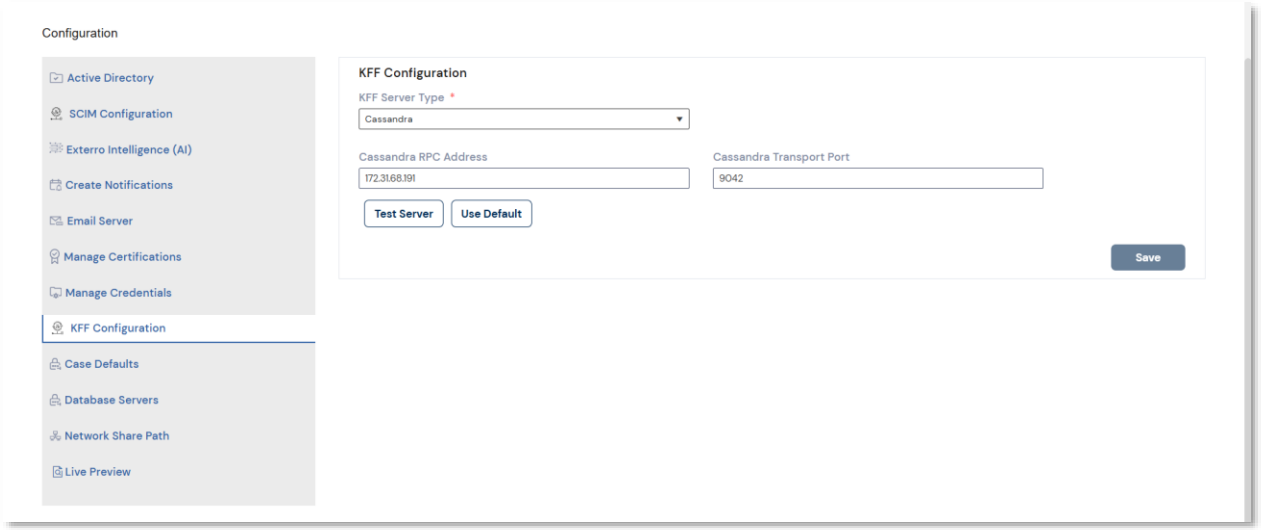
1. Navigate to the **Configure Exterro KFF Server** menu.
2. Set **Server Type** to **RocksDB**.
3. In the **Server Address** field, enter the directory path:
    - **Local Path:** e.g., **F:\RocksDB**
    - **Remote UNC Path:** e.g., **\\192.168.102.54\RocksDB**
4. Click **Test Server** to verify connection and directory access.
5. Click **Save** to confirm settings.





FTK Central (Web) Setup

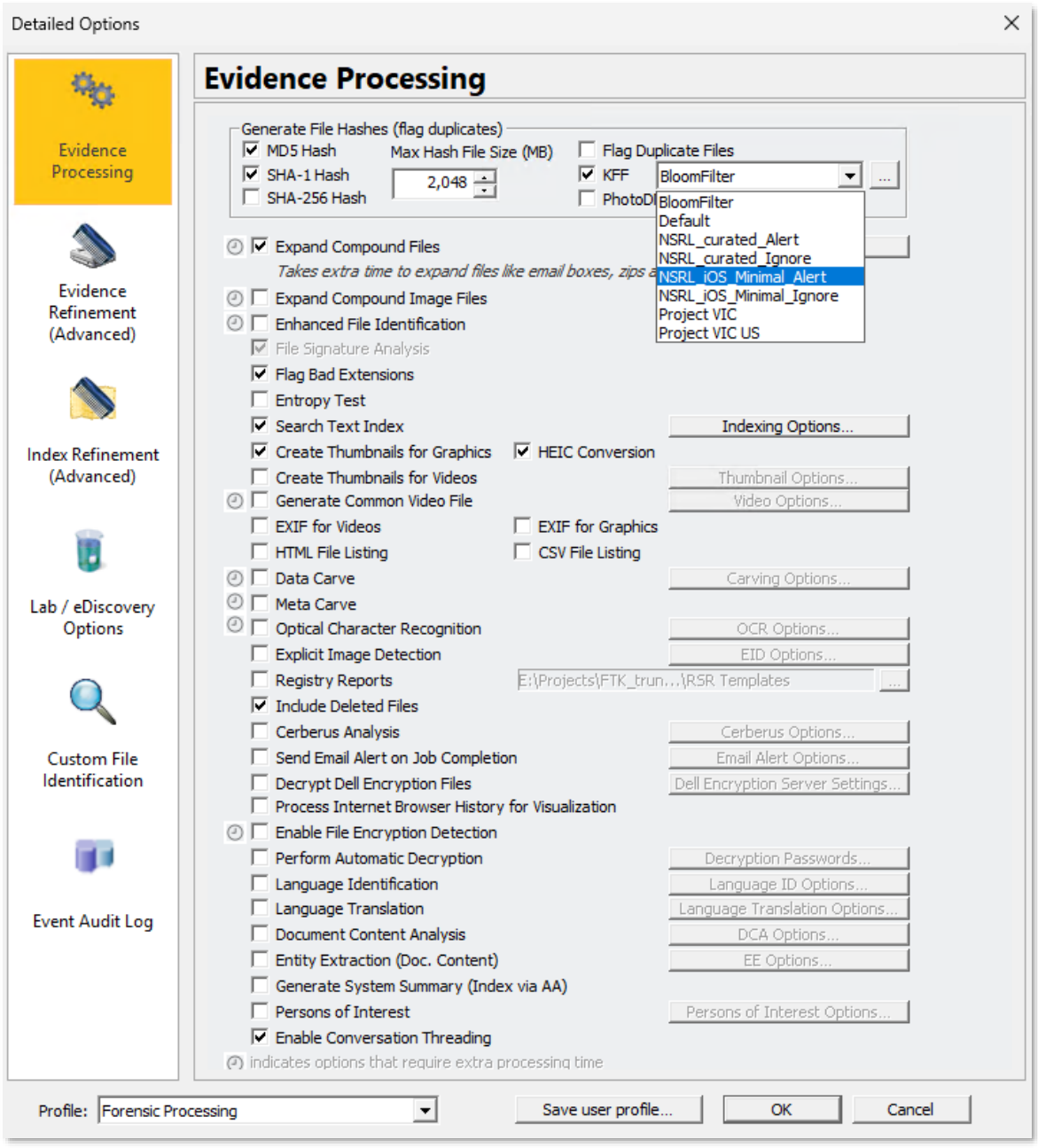
1. Open **Settings** and navigate to **KFF Configuration**.
2. Select **RocksDB** from the **KFF Server Type** dropdown.
3. Enter the target folder path in the **Server Address** field.
4. Click **Test Server** to validate connectivity.



5. Click **Save** upon successful validation.

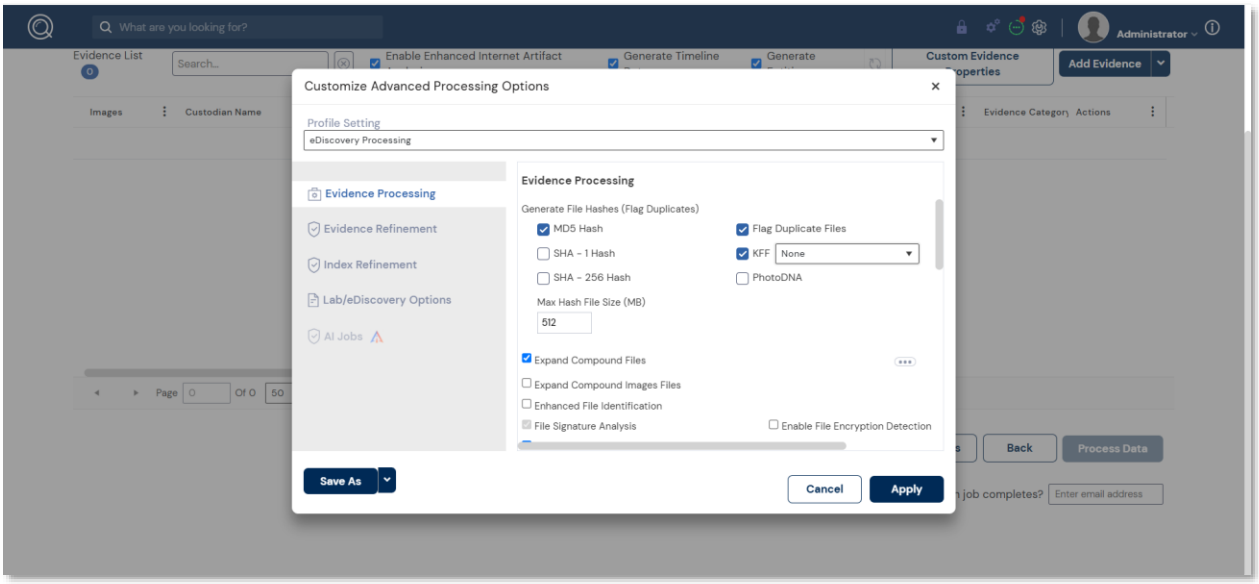
Evidence Processing & Hash Matching

Once RocksDB is configured and saved, available KFF groups and sets automatically populate within processing options.



Processing Steps:

1. Initiate **New Case Processing** or navigate to **Evidence Refinement / Custom Processing Options**.
2. Under **Evidence Processing Options**, locate **Generate File Hashes (Flag Duplicates)**.
3. Check the **KFF** checkbox and select the desired KFF set or profile (e.g., *NSRL_iOS_Minimal_Alert*) from the dropdown menu.
4. Complete additional processing settings and click **Process Data**. FTK will automatically route hash queries through the configured RocksDB instance.



Contact Exterro

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

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

Contact:

Exterro, Inc.

2175 NW Raleigh St., Suite 110

Portland, OR 97210.

Telephone: 503-501-5100

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

Fax: 1-866-408-7310

General E-mail:info@exterro.com

Website: www.exterro.com