

FTK STANDALONE 8.3 INSTALLATION GUIDE

JULY 2026

Table of Contents

- About Exterro 3
- Prerequisites 3
 - Fresh Installations 3
 - Upgrades 3
- 1 Exterro FTK Standalone 8.3 Installer 4
 - 1.1 Installing FTK Standalone 8.3..... 4
 - 1.2 Database: Fresh Installations and Upgrades 16
 - 1.2.1 Fresh Installations 17
 - 1.2.2 Existing Installations (Upgrades) 22
- Contact Exterro 26

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.

Prerequisites

The following prerequisites must be adhered to before attempting to install or upgrade FTK.

Fresh Installations

- Windows updates have been installed.
- Disable any antivirus/malware scanning software.
- Login credentials for an account that is a member of the local administrator's group. A local system account should only be used if all components as well as case and evidence storage will be on a single machine.

Upgrades

- The currently installed version of FTK must be 8.0 or 8.0 service pack (SP1, SP2) or 8.1 / 8.2, 8.1 / 8.2 service pack (SP1, SP2).
 - Attempts to upgrade from FTK 7.6 or earlier are not supported.
- Windows updates have been installed.
- Disable any antivirus/malware scanning software.
- Login credentials for an account that is a member of the local administrator's group. A local system account should only be used if all components as well as case and evidence storage will be on a single machine.



Warning: If User Account Control (UAC) is enabled, all prompts must be agreed to by clicking on **Yes**.

1 Exterro FTK Standalone 8.3 Installer

1.1 Installing FTK Standalone 8.3

Before beginning, extract your downloaded installation package to a local directory. Ensure that all standard prerequisite folders and binaries are present in your extraction folder:

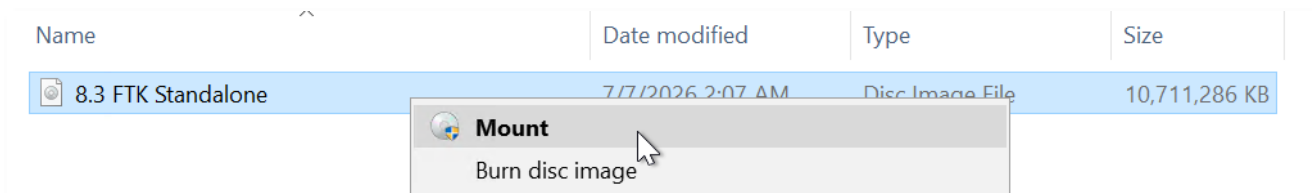
- CodeMeterRuntime_8.20
- Exterro Evidence Processing Engine
- Exterro Forensic Tools
- Exterro License Manager
- Exterro PostgreSQL
- Prerequisite-Microsoft DotNET Framework 4.8
- Prerequisite-Microsoft Visual C++ 2015-2022 Redistributable
- Prerequisite-Python 3.13.2

Note: You can view the installation logs by navigating to either of the following file paths:

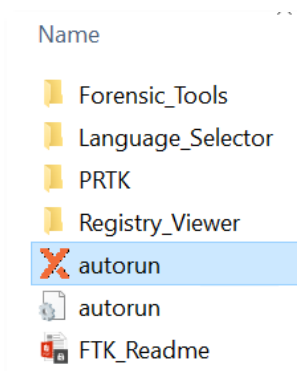
- %temp%\exterro-installer.log
- %LOCALAPPDATA%\Exterro\exterro-installer.log

Steps:

1. Download the Latest ISO Disc Image file (**8.3 FTK Standalone**) from the Exterro Product Downloads page.
2. Right-click on the downloaded file and select **Mount**.

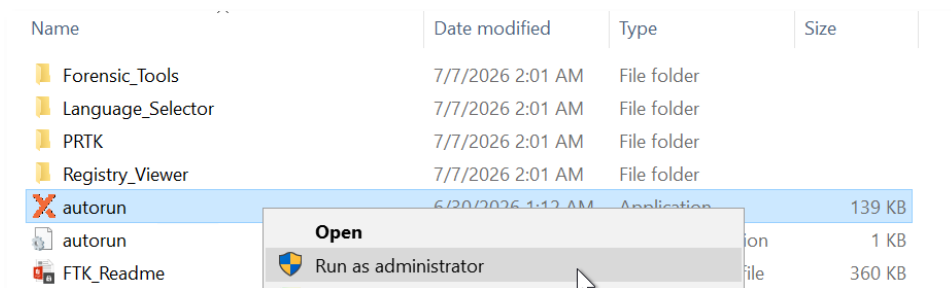


- The following components will be listed:

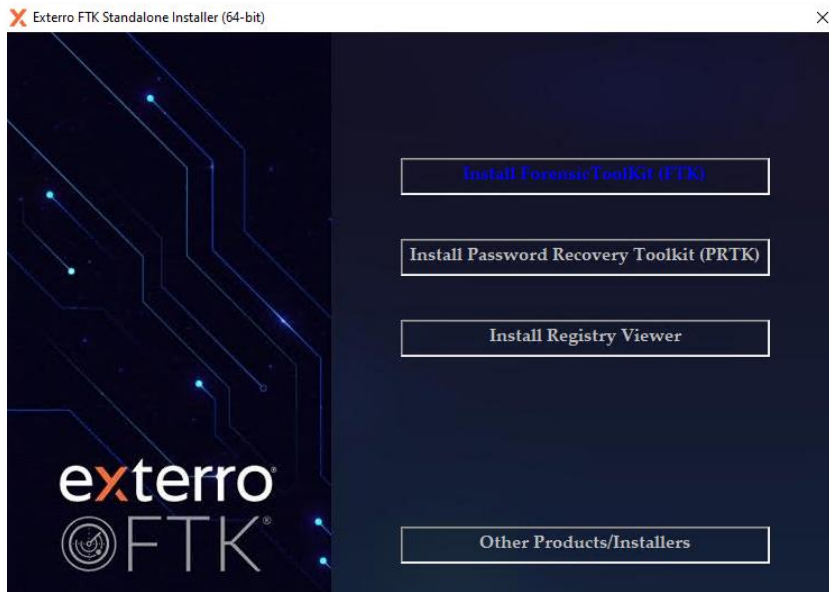


3. Do one of the following to start with the installation:

- A. Right-click on the **autorun** file and select **Run as administrator**.



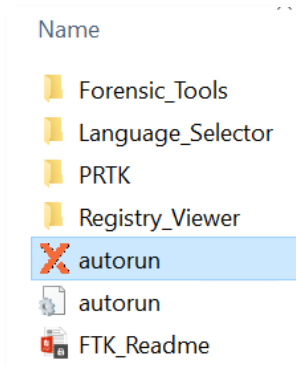
- The following **Forensics Tools Installer** page will be displayed.



- i. Click on the **Install Forensics Tools 64-bit** option to start the installation process.

(or)

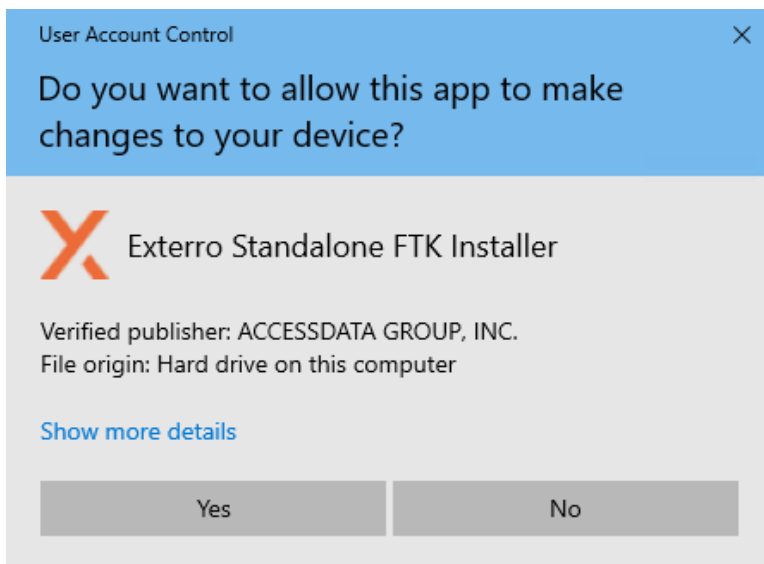
- B. Navigate to the **Forensic_Tools** folder.



- The following components will be listed:

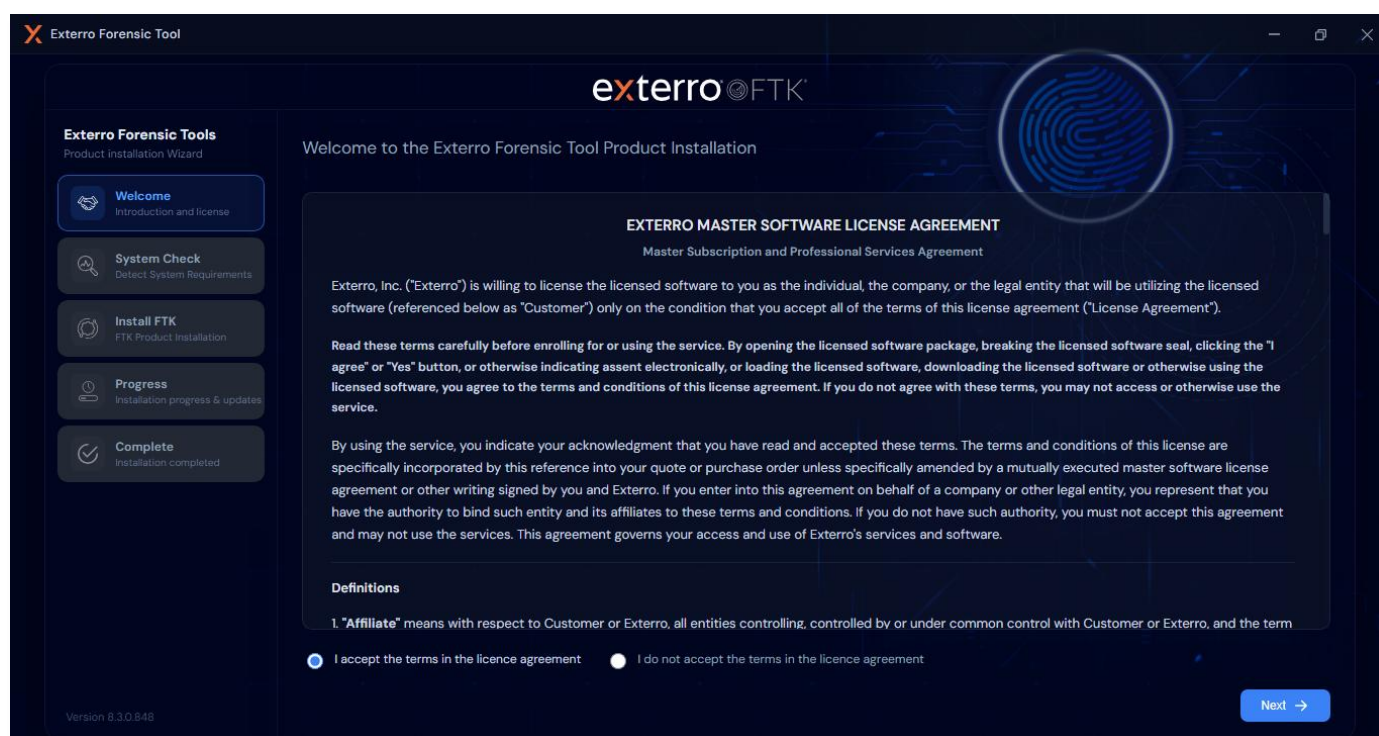
Name	Date modified	Type	Size
 CodeMeterRuntime_8.20	6/18/2026 6:40 AM	File folder	
 Exterro Evidence Processing Engine	6/18/2026 6:40 AM	File folder	
 Exterro Forensic Tools	6/18/2026 6:42 AM	File folder	
 Exterro License Manager	6/18/2026 6:42 AM	File folder	
 Exterro PostgreSQL	6/18/2026 6:42 AM	File folder	
 Prerequisite-Microsoft DotNET Framework 4.8	6/18/2026 6:42 AM	File folder	
 Prerequisite-Microsoft Visual C++ 2015-2022 Redistributable	6/18/2026 6:43 AM	File folder	
 Prerequisite-Python 3.13.2	6/18/2026 6:43 AM	File folder	
 Exterro Standalone FTK Installer	6/18/2026 6:43 AM	Application	80,100 KB

- Right-click on the **Exterro Standalone FTK Installer** file and select **Run as Administrator** to grant the elevated system privileges necessary for installation.
- A Windows User Account Control prompt will appear on your desktop asking: *"Do you want to allow this app to make changes to your device?"*



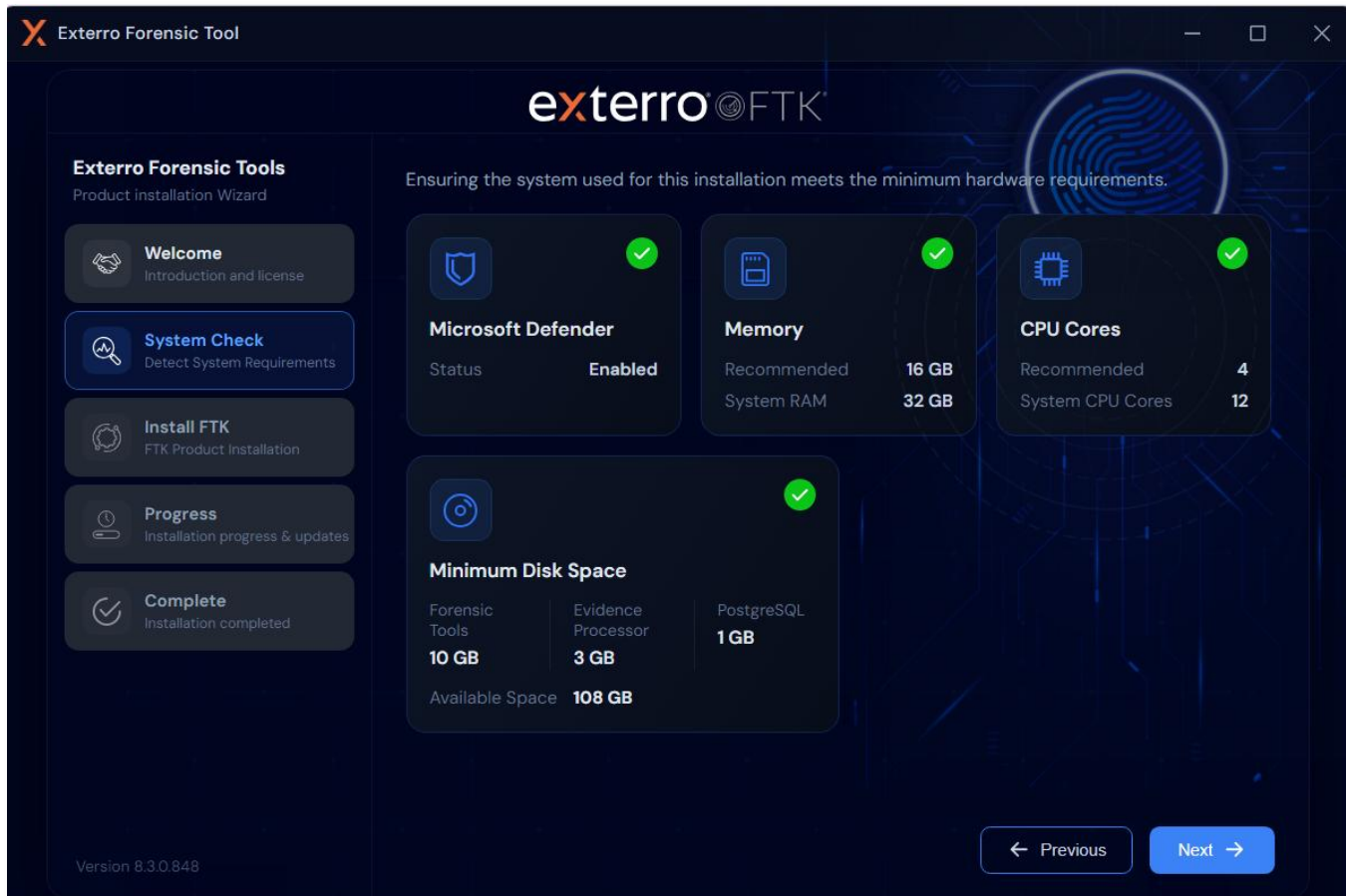
- Click **Yes** to bypass the security check and launch the main installation wizard.

- The **Exterro Forensic Tool Product Installation Wizard** screen will be displayed.



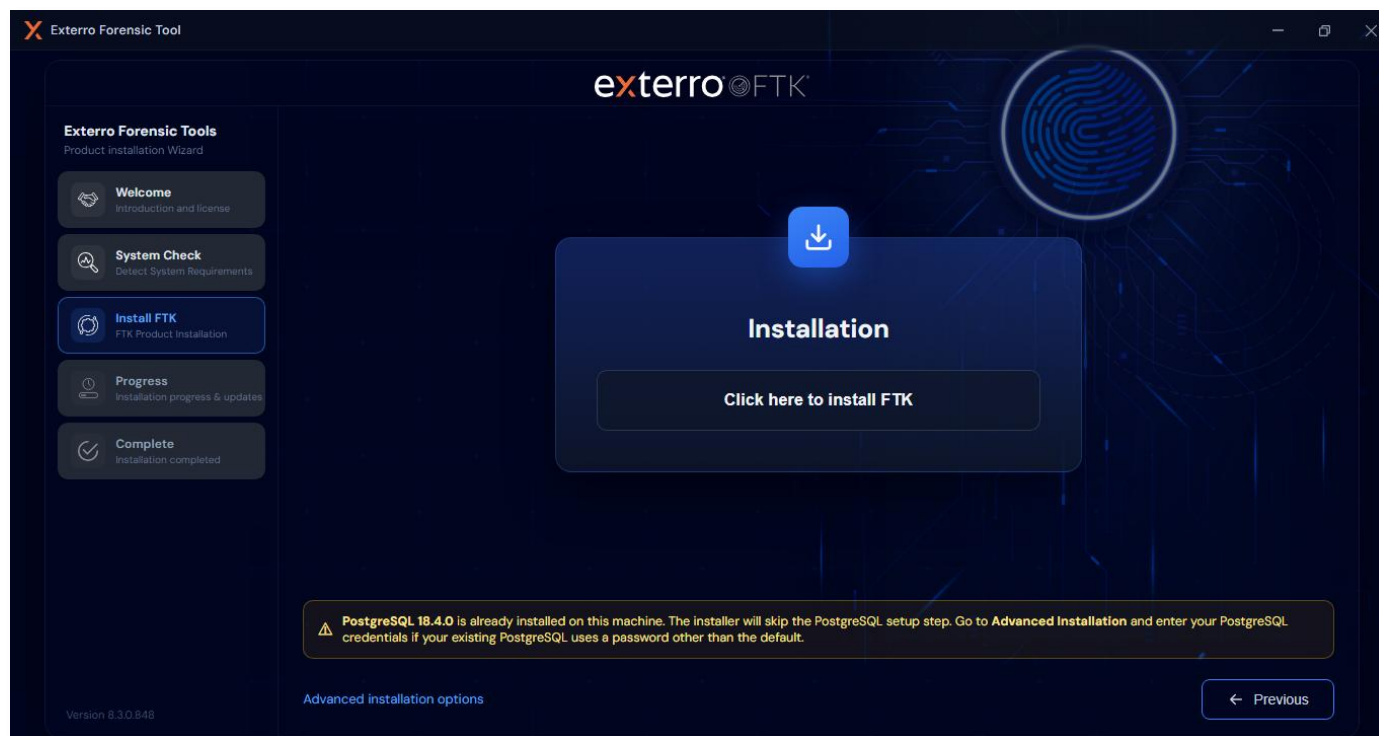
5. Read through the provided *Exterro Master Software License Agreement*.
6. Select the radio button labeled **I accept the terms in the license agreement**.
7. Click the **Next** button located at the bottom right corner of the window.

- The installer will automatically perform an environmental check on your machine's hardware and dependent software packages.

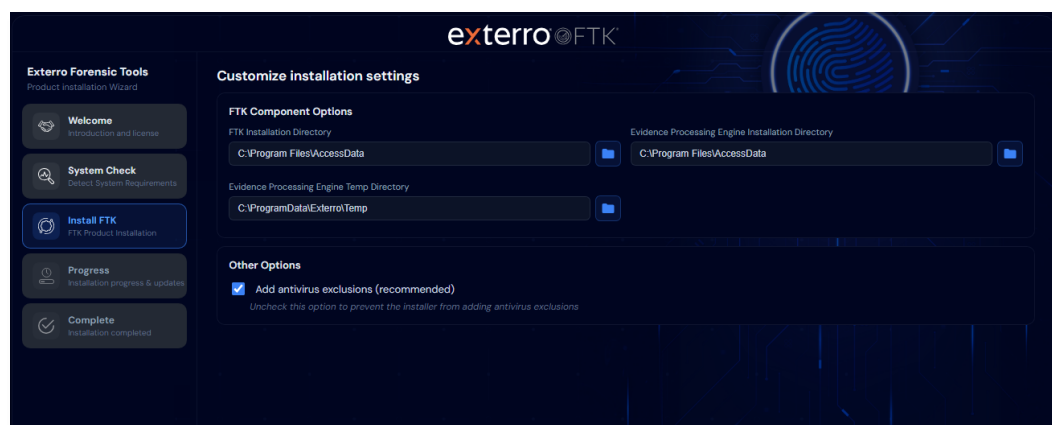


8. Review the diagnostic status checklist carefully:
 - **Microsoft Defender Integration:** Confirms active state.
 - **System Memory (RAM):** Ideally 16 GB minimum. If your system flags a warning (e.g., 15 GB detected), note that it will not block installation but may limit processing speeds.
 - **CPU Cores:** Recommended 4 System CPU Cores.
 - **Available Disk Space:** Validates allocation for Forensic Tools (10 GB), Evidence Processor (3 GB), and PostgreSQL (1 GB).
9. Once you confirm your hardware complies, click **Next**.

- The setup wizard detects existing environments. If an existing PostgreSQL backend is found, an optimization recommendation banner will appear.



10. Click on the text link labeled **Advanced installation options** at the lower-left corner of the screen.



Note: Case defaults configured here will be reflected on the 'Case Defaults' page in the FTK Central UI. If the changes are not visible immediately, you are recommended to restart the 'Exterro WebLabSelfHost' service for the updates to take effect.

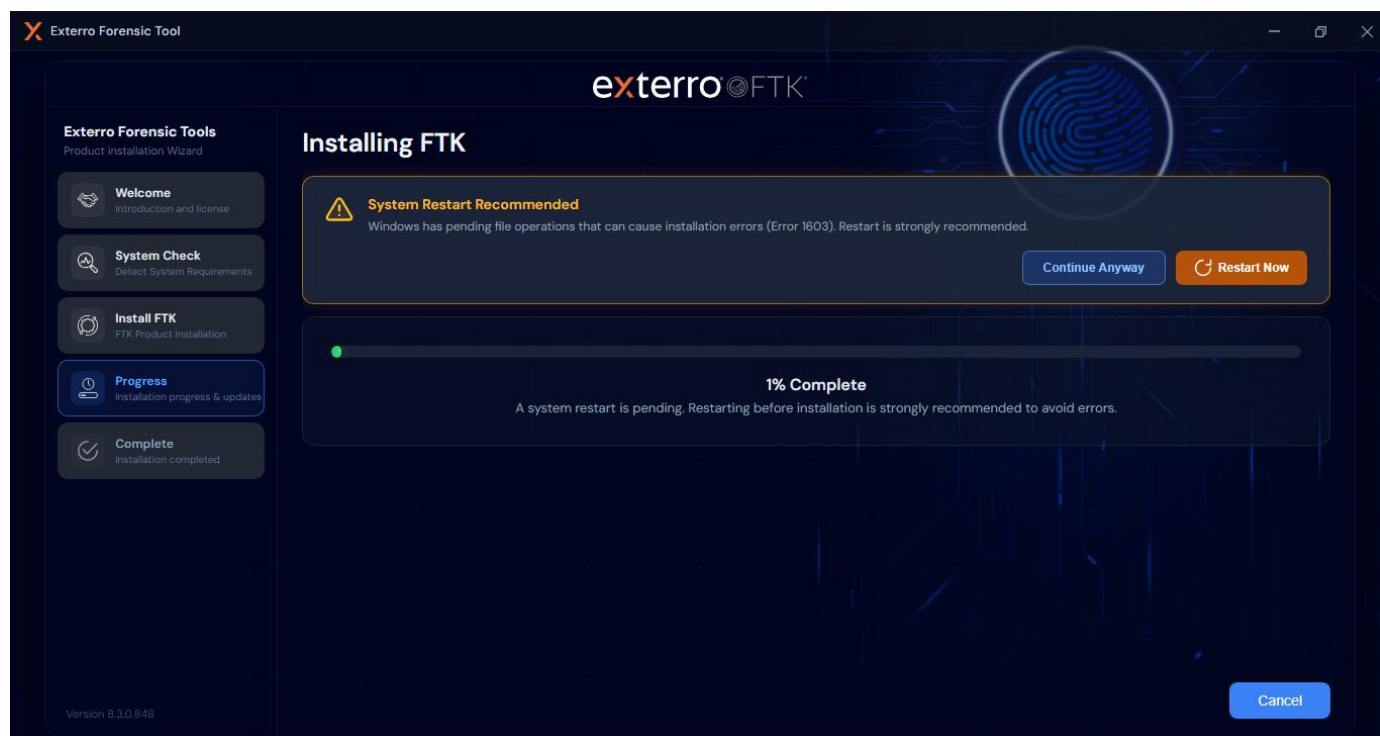
11. Configure your target environment parameters:

- **Target Directories:** Review and alter default paths for the *FTK Application*, *Evidence Processing Engine*, and *Evidence Processing Engine Temp* scratchpad folder.
- **Antivirus Exclusions:** Ensure that the option **Add antivirus exclusions (recommended)** is checked to stop real-time scanners from locking critical analytical tables.

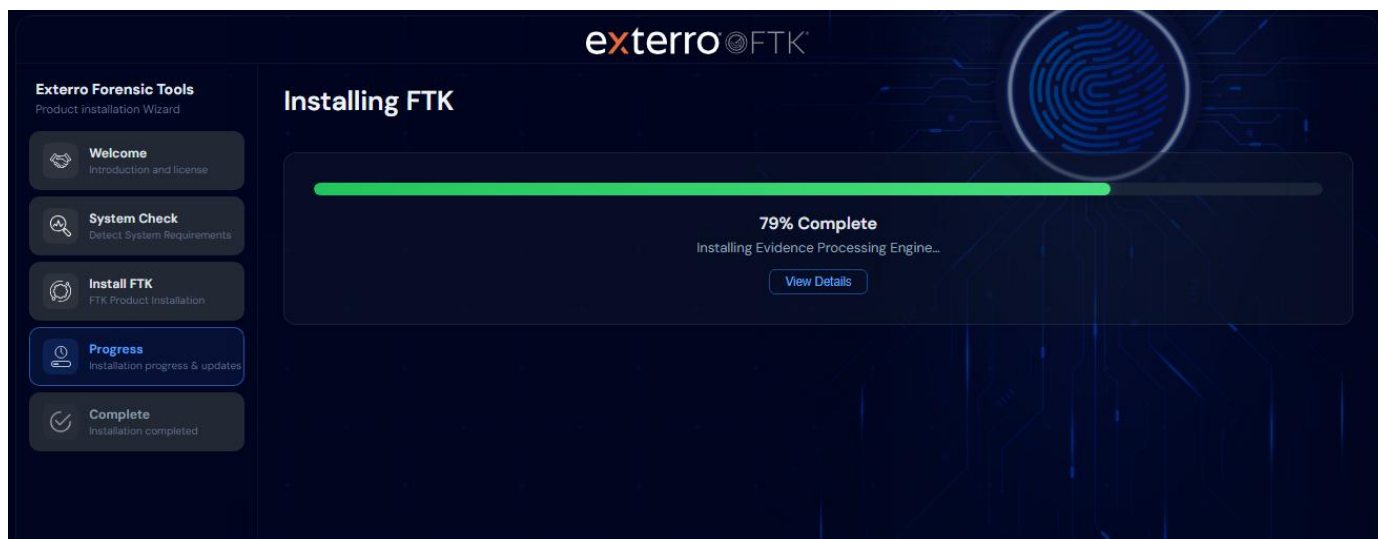
12. Click **Install** to start processing the binaries.

Note: If your operating system has pending file actions from background installations, a yellow alert dialog box may interrupt the deployment sequence.

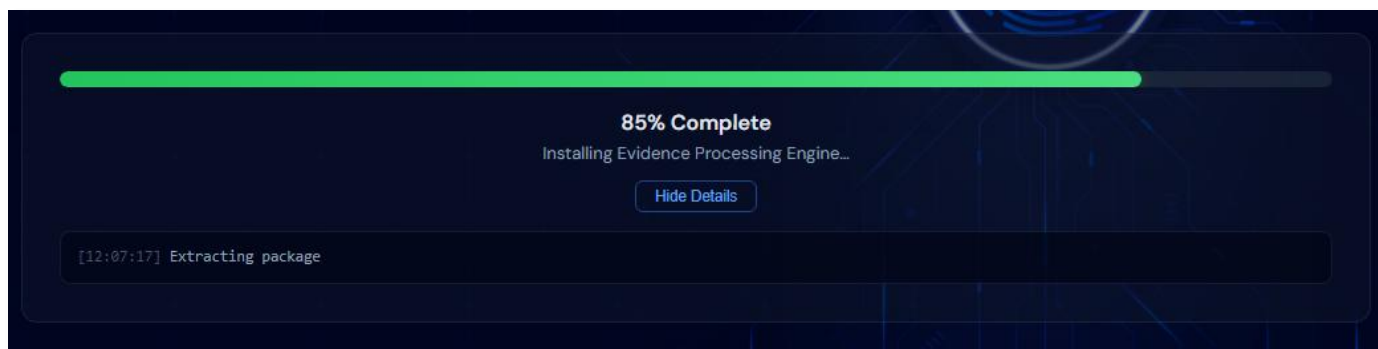
- The warning will note that pending actions can lead to standard MSI errors (such as Error 1603). Restart is strongly recommended.
- Click **Restart Now** if you wish to apply updates safely, or click **Continue Anyway** to bypass the prompt and proceed directly with the setup loop.



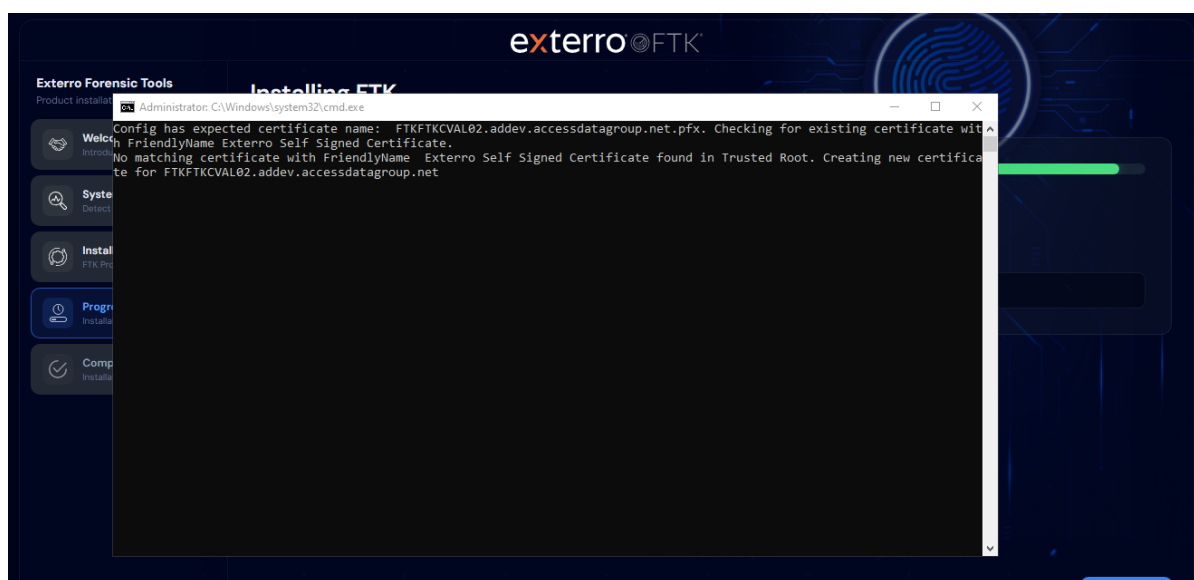
- The installation wizard will now cycle through copying configurations and registry keys. Monitor the primary status indicators as they move through various completion stages (e.g., *Installing Evidence Processing Engine*, *Installing PostgreSQL*).



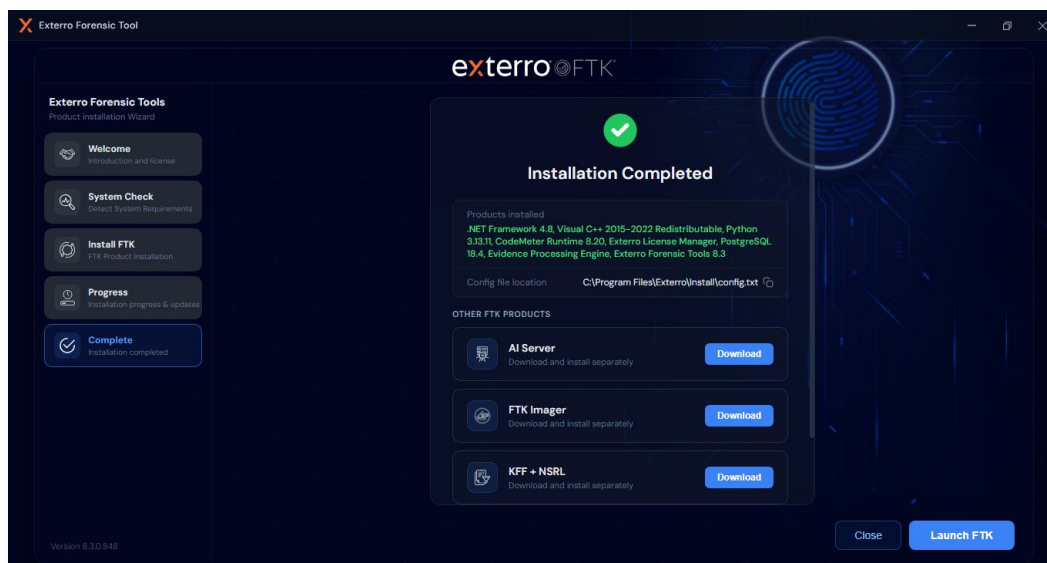
13. To see granular background operations, click on the **View Details** toggle switch.



Important Note regarding Command Prompt windows: During network security or database token generation, an administrative Command Prompt (cmd.exe) console window will open multiple times. **Do not close, alter, or press any keys within this console.** Allow it to execute and terminate automatically.

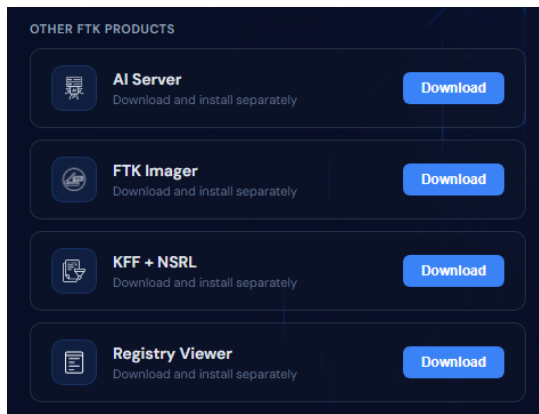


- Once all modules have been successfully copied, the installer's final screen will be displayed.



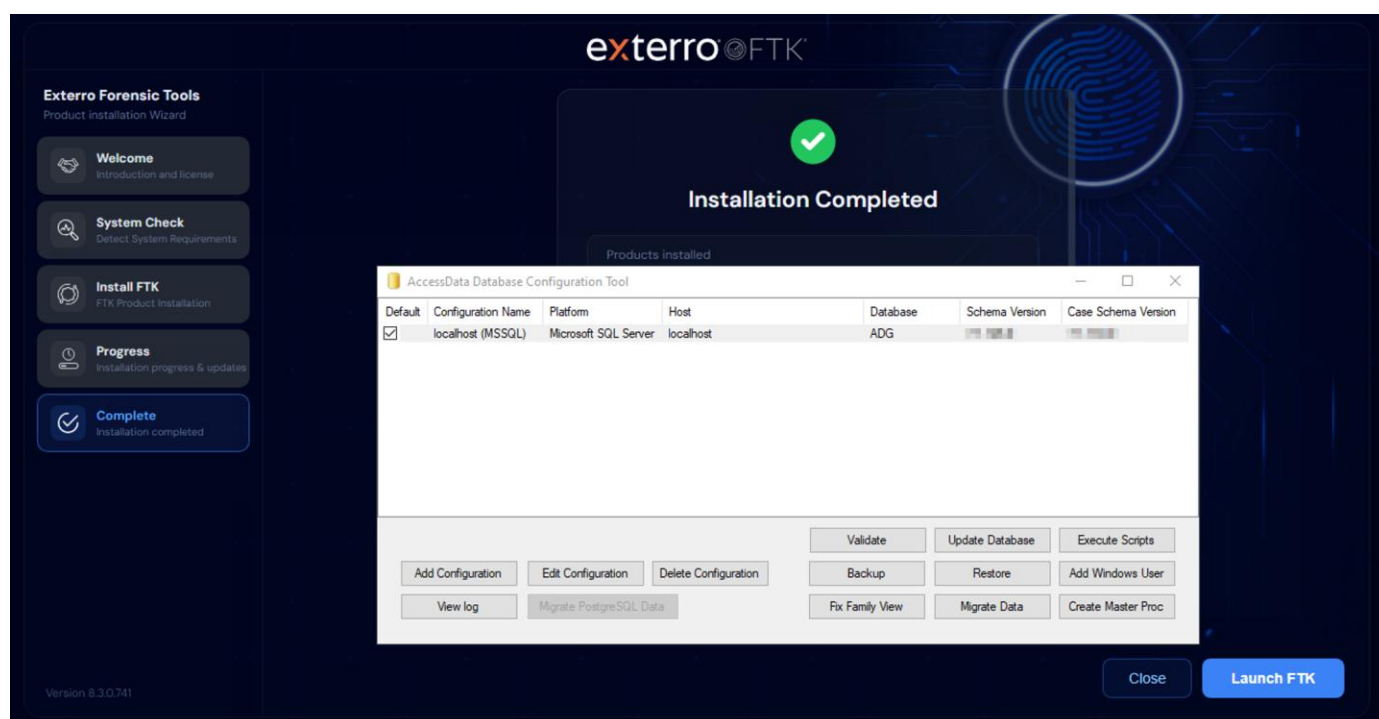
14. Review the structural summaries, which show your assigned default database routing ports (e.g., Username: **postgres**, Port: **5433**).

***Note:** If you require supplementary toolkits from the suite, select the **Download** buttons alongside the listed components.*



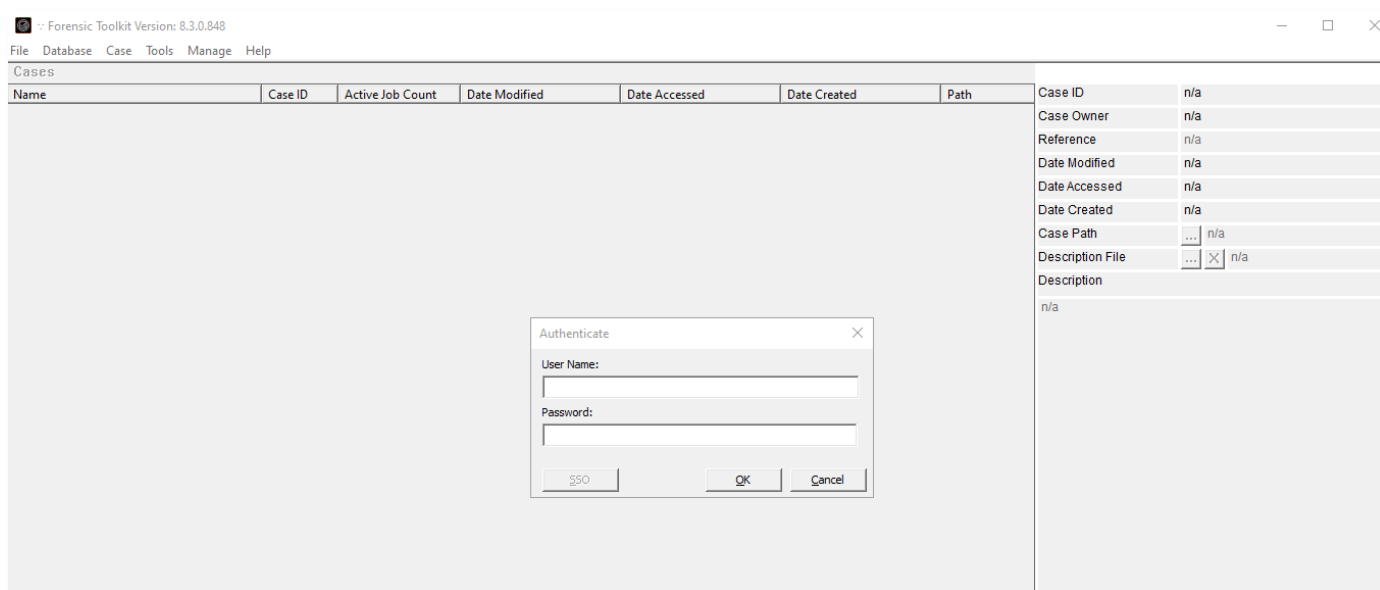
Note: The application will route you through the integrated setup modules:

- **Fresh Installation:** Fill in your database parameters in the [Fresh Installation](#) section if you are mapping out a completely new instance.
- **Upgrades:** If migrating from older environments, follow the migration prompts to apply your database updates via the AccessData Database Configuration Tool. Refer to the [Existing Installation \(upgrades\)](#) section.



15. Click the **Launch FTK** button. The initial startup processes may take up to 60 seconds to prepare.

- Once connection paths are validated and authenticated by the configuration utility, your secure **Forensic Toolkit Login Screen** will display. Enter your credentials to begin standard forensic workflows.



1.2 Database: Fresh Installations and Upgrades

For all installations and upgrades, a database must be created or updated for FTK.

- If this is a fresh installation of FTK without any database present, please follow the [Fresh Installations](#) section.*
- If this is an upgrade for an existing installation of FTK, please follow the [Existing Installations \(Upgrades\)](#) section.*

1.2.1 Fresh Installations

Method 1 – Using FTK to add a new database

Steps:

1. Navigate to the **Windows Desktop**.
2. Open **FTK.exe**.



- Once FTK has loaded, an **Add Database** dialog will be displayed.

The image is a screenshot of the "Add Database" dialog box. It has a title bar with "Add Database" and a close button (X). The dialog contains the following fields and options:

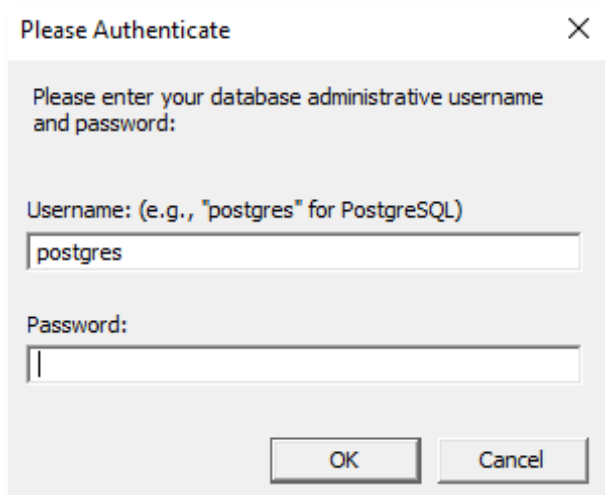
- RDBMS**: A dropdown menu with "PostgreSQL" selected.
- Host (IP or DNS name)**: A text field with "localhost" entered. To its right is a "Discover" button.
- Display name (optional)**: An empty text field.
- Postgres dbname**: A text field with "ADG" entered.
- Port number**: A section with a checkbox "Use Default Port" which is checked. To the right of this section is a checkbox "Cloud Based" which is unchecked.
- Below the port number section are two more unchecked checkboxes: "Use Integrated Security" and "Set as default database".
- At the bottom right are "OK" and "Cancel" buttons.

3. Enter the following details:

- **RDBMS:** MSSQL or Postgres (This should be set as Postgres if you did a Default installation.)
- **Host (IP or DNS name):** Database location, this should be localhost if a Default installation was completed.
- **Display Name:** This is an optional field and simply names an instance within FTK database connection configuration files.
- **Postgres/MSSQL dbname:** If a default installation was completed, this should be set as 'ADG'.
- **Port Number:** If a default installation was completed, this should be set as 'Use Default Port'. If a custom port was selected, this must be entered now.

4. Click **OK**.

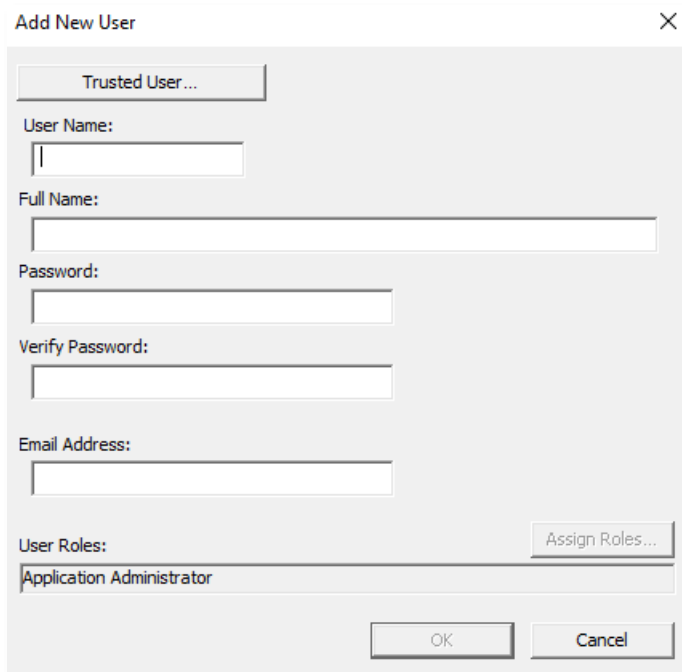
- The **Please Authenticate** dialog will be displayed.

A screenshot of a 'Please Authenticate' dialog box. The dialog has a title bar with a close button (X). The main text says 'Please enter your database administrative username and password:'. Below this, there are two input fields. The first is labeled 'Username: (e.g., "postgres" for PostgreSQL)' and contains the text 'postgres'. The second is labeled 'Password:' and is empty. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

5. Enter the database administrator credentials and click **OK**.

- If a default installation was completed, the credentials would be:
 - **Username:** postgres
 - **Password:** AD@Password

- The **Add New User** dialog will be displayed.



The screenshot shows the 'Add New User' dialog box. It contains the following elements:

- Trusted User...** button
- User Name:** input field
- Full Name:** input field
- Password:** input field
- Verify Password:** input field
- Email Address:** input field
- User Roles:** dropdown menu (currently showing 'Application Administrator')
- Assign Roles...** button
- OK** and **Cancel** buttons at the bottom.

6. Enter the following details:

- **User Name**
- **Full Name**
- **Password**
- **Verify Password**
- **Email Address (Optional)**

7. Click **OK**.

Method 2 – Using DBConfig to add a new database

Note: Before attempting any database setups, it is important to ensure the Exterro Self-host Service has been stopped. This can be done using Windows Services. Once complete, users can start the service again.

Steps:

1. Navigate to the Forensic Tools “bin” folder.

<Drive:>\Program Files\AccessData\Forensic Tools\8.3\bin

2. Open **DBConfig.exe** as an Administrator.
3. Click **Add Configuration**.
4. Enter the following details:
 - **Database Type:** MSSQL or Postgres (This should be Postgres if you did a Default installation.)
 - **Server Name:Port:** Database location in the format host:port (Port is only needed when using a non-default port. This should be localhost if a Default installation was completed.)
 - **Create Database:** True

Database Information

Configuration Name: Default

Database Type: Postgres

Server Name : Port: localhost

Database Name / SID: ADG

Database Schema: ADG7x1

Authentication Mode: AccessData Default Password

☒ Create Database

Authentication Mode: Database Authentication

System User: postgres

System Password:

☒ Install WordNet ☐ Cloud Install

Application Admin: Administrator

Admin Password:

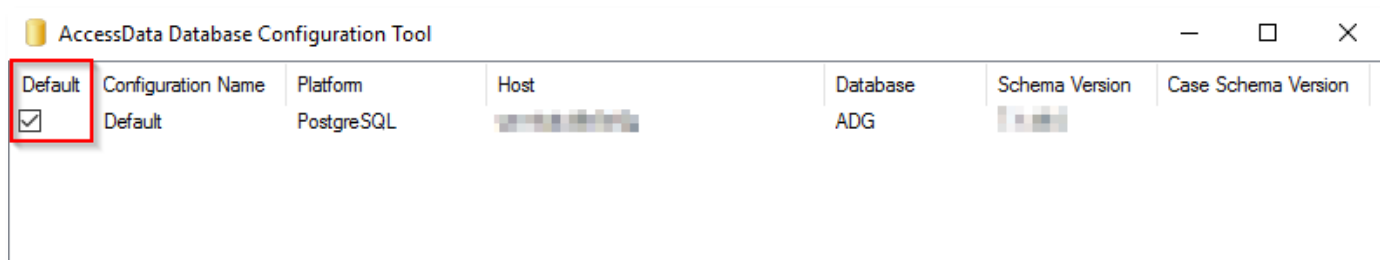
Confirm Password:

Transfer From...

Version: AccessData Database 7.1

Create Cancel

- **Authentication Mode:** Mode to authenticate to your database (This should be Database Authentication if a Default installation was completed.)
 - **System User:** When using Database Authentication, this is the database user to use when authenticating (This should be postgres if a Default installation was completed.)
 - **System Password:** When using Database Authentication, this is the database password to use when authenticating (This should be AD@Password if a Default installation was completed.)
 - **Application Admin:** The desired username for your first FTK administrator.
 - **Admin Password:** The desired password for your first FTK administrator.
5. Click **Create** and the database creation will begin.
6. Once the database is created, confirm the **Default** box is checked against the newly created database.



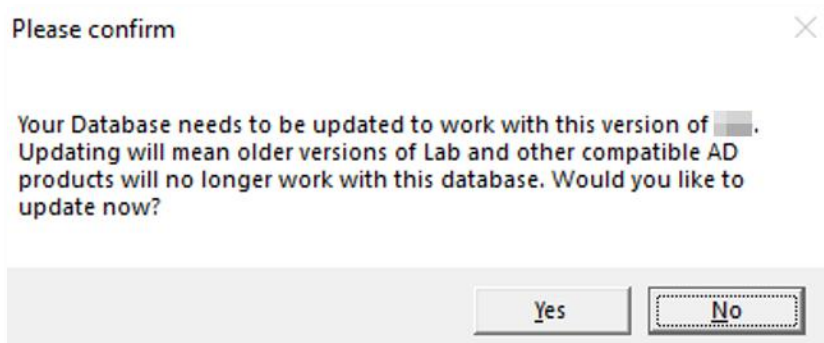
1.2.2 Existing Installations (Upgrades)

Users upgrading from an existing installation of FTK have two methods when upgrading their database. Both methods are documented below and users can opt to choose any method they feel comfortable executing.

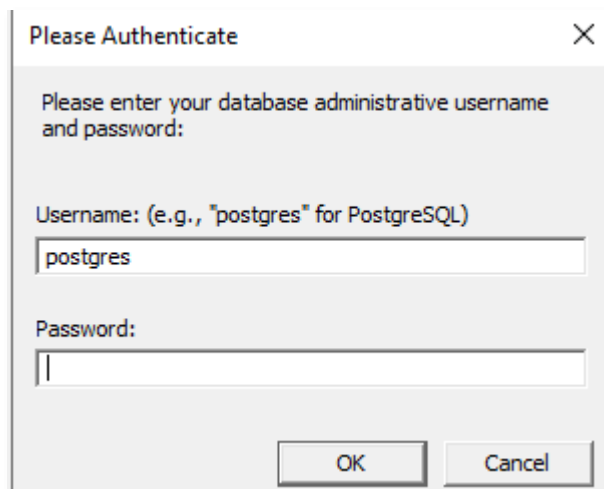
Method 1 – Using FTK to upgrade an existing database

Steps:

1. Click 'Launch FTK' on the installation page.
2. Enter the Application Administrator credentials when prompted.
 - Successful logins will be prompt with a 'Please Confirm' database upgrade dialog.



3. Click **Yes**.
 - The **Please Authenticate** dialog will appear.



Note: If there are any cases previously created, it is required to follow the below steps to update the case schema database.

- i. Navigate to the Forensic Tools “bin” folder.

```
<Drive:>\Program Files\AccessData\Forensic Tools\8.3\bin
```

- ii. Open **DBConfig.exe** as an Administrator.
- iii. Refer to the below '[Method 2 – Using DBConfig to upgrade an existing database](#)' section for further information.

4. Enter the Database Administrator credentials when prompted and click **OK**.

- If a default installation was completed in the past, the credentials would be:
 - **Username:** postgres
 - **Password:** AD@Password

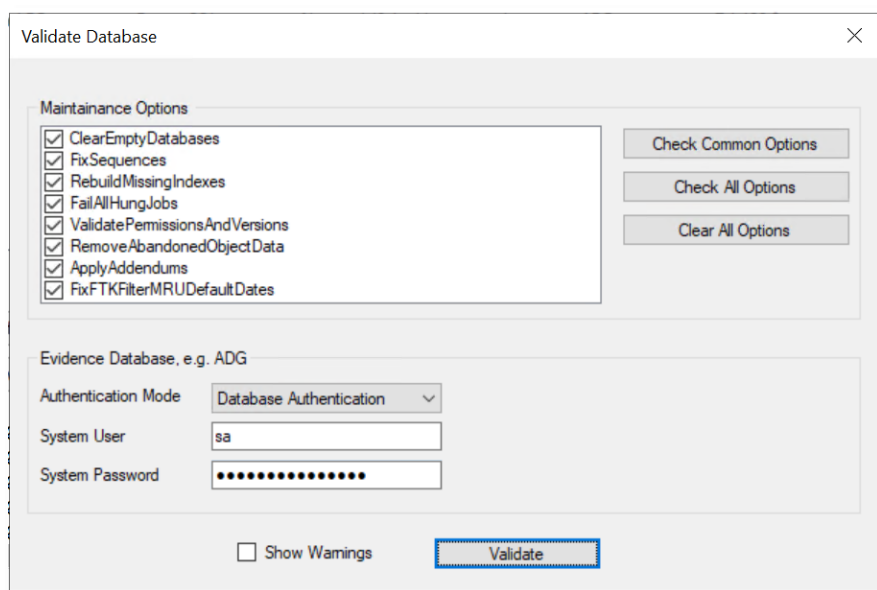
5. Click **OK**.

- The database upgrade process will begin. Once completed, the case list will be refreshed, and the application toolbar will display the name of the connected database instance.

Method 2 – Using DBConfig to upgrade an existing database**Steps:**

Note: Ensure all FTK-related applications and background processes are completely closed before proceeding.

1. The DB Config tool will open automatically upon successful installation:
2. Select the existing database and click **Validate**.
3. Select an **Authentication Mode**.
4. Click **Check Common Options**.



5. Click **Validate**.



Warning: Database Validate Successful should appear. Do not proceed if this does not, please send any messages that accompany an unsuccessful validation to support@exterro.com.

6. Click **OK** once successfully validated.
7. Highlight the desired database and click **Update Database**.
8. Select a **Backup Path**.
9. Select an **Authentication Mode**.

Validating app db connection information

Update Shared schema from 7.1.120.0 to 7.1.120.0
Update Case schemas from 7.1.120.0 to 7.1.120.0

Backup path ☒ No Backup Path (Not recommended)

The database server must have write access to the backup path

Evidence Database, e.g. ADG

Authentication Mode

System User

System Password

10. Click **Update**.
11. Once the database is created, confirm the **Default** box is checked against the upgraded database.

	Configuration Name	Platform	Host	Database	Schema Version	Case Schema Version
☒	Default	PostgreSQL		ADG		

Contact Exterro

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

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

Contact:**Exterro, Inc.**

2175 NW Raleigh St., Suite 110

Portland, OR 97210.

Telephone: 503-501-5100

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

Fax: 1-866-408-7310

General E-mail: info@exterro.com

Website: www.exterro.com

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

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

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

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