# Table of Contents

Overview......................................................................................................................................................................... 3
Purpose of the document............................................................................................................................................... 3
FTK 7.6 - Patching Process .............................................................................................................................................. 3
  Which Components should this Patch be applied to? ................................................................................................ 3
Prerequisites ............................................................................................................................................................... 4
Patch Installation......................................................................................................................................................... 4
Database Schema Upgrade ......................................................................................................................................... 7
  Database Validation ...................................................................................................................................................... 8
Upgrading Database Schema Manually (FTK Central & FTK Enterprise) ......................................................... 9
Upgrading Database Schema Automatically (FTK and FTK Lab). ........................................................................... 12
Windows Agent Module Update ............................................................................................................................... 13
  Updating Site Server Modules ............................................................................................................................... 13
  Updating The Disk Preview Module On Deployed Agents ............................................................................. 14
New Installation Verification ..................................................................................................................................... 15
Contact Exterro............................................................................................................................................................. 16
Overview

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 Legal GRC 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.

Purpose of the document

The purpose of this document is to provide users with step-by-step instructions required to initiate the automated installation of the FTK 7.6 SP1 patch.

FTK 7.6 - Patching Process

Which Components should this Patch be applied to?

- Forensic Tools 7.6
- Distributed Processing Manager
- Processing Engine

⚠️ **Warning:** The patch must be applied to all components within an environment. Failure to adhere to these requirements may result in unexpected and critical errors.
Prerequisites

The following prerequisites should be ensured to complete the patching process in a seamless manner:

- FTK 7.6 has been installed.
- The latest Windows updates must be installed prior to any patch.
- The patches must be executed as an Administrator.
- Processing jobs must not be active during patching.
- The Exterro Self Host Service must be stopped prior to patching.

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

Patch Installation

**Note:** Ensure this patch is applied to all machines in an environment. This includes machines with FTK, FTK Lab, FTK Enterprise, FTK Plus or FTK Central as well as any machine being used as a Distributed Processing Manager or Distributed Processing Engine.

Users are advised to install the patch on all processing engines before any distributed processing managers to avoid any connection issues.

Steps:

1. Navigate to AccessData Forensic Tools 7.6 Patch.exe.
2. Right click on the file and select **Run as Administrator**.
   - The prompt below will be displayed and the executable will begin to extract its contents ready for the patching process to begin.
3. Click **Apply Patch**.

4. Review and accept the **EULA**. Click **Continue**.
   - A patch confirmation prompt will appear.

5. Click **OK** to begin the patching process.
   - The **patching process** will begin.
   - It is imperative to observe the patch installer, as patch confirmation prompts will appear for each component it needs to patch. **E.g.** if a server has the FTK application and a evidence processor installed, a patch confirmation prompt will appear more than once requiring users to select **OK** or **Cancel**.
6. When the patching process is complete, the installer will automatically be closed.

**Note:** During this process, the patcher will check for dependencies and other components that require patching. This validation is performed for the components such as AccessData Evidence Processing Engine, Exterro Forensic Tools, FTK Plus, etc. Users must ensure this patch installer is run on distributed machines.

*It is recommended to restart the system once the patching process is completed.*
Database Schema Upgrade

Once the 7.6 SP1 patch has been installed on all related components, users are required to update the schema of their existing application database.

Database schema upgrades will be completed automatically for users running FTK and FTK Lab once the application has been opened post patch installation.

**Note:** Before attempting any validations and upgrades, it is important to ensure the Exterro Self Host Service has been stopped. This can be done using Windows Services. Once validations and the upgrade have completed, users can start the service again.

Users of FTK Central or FTK Enterprise are advised to refer to the [Upgrading Database Schema Manually section (FTK Central and FTK Enterprise)](#).

Users of FTK or FTK Lab are advised to refer to the [Upgrading Database Schema Automatically section (FTK and FTK Lab)](#).
Database Validation

**Steps:**

1. On the application server, navigate to the Forensic Tools "bin" folder.
   - `<Drive:>\Program Files\AccessData\Forensic Tools\7.6\bin`
2. Open **DBConfig.exe** as an Administrator.
3. Locate and click on the existing database that is being used.
4. Click **Validate**.
5. Click **Check Common Options**.
6. Select an **Authentication Mode**.
7. Click **Validate**.
   - 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**.
Upgrading Database Schema Manually (FTK Central & FTK Enterprise)

Steps:

1. If the **AccessData Database Configuration Tool** window isn’t already open, open **DBConfig.exe** as Administrator.
   - `<Drive:\Program Files\AccessData\Forensic Tools\7.6\bin`

2. If a desired database is not already listed, click **Add Configuration**.

3. Complete the following, then click **Connect**:
   - **Database Type**: MSSQL or Postgres
   - **Server Name**: Port: Database location in the format host:port (Port is only needed when using a non-default port).
4. Highlight a desired database, and click **Update Database**.

5. Select a backup path, set an authentication mode, and click **Update**.
6. After the update completes, confirm the **Default** box is checked next to the entry for a desired database.

7. Close the **AccessData Database Configuration Tool** window and reboot the computer.
Upgrading Database Schema Automatically (FTK and FTK Lab)

Users that do not follow the manual process of upgrading the database schema using DBConfig can follow the steps below.

Steps:
1. Open FTK, FTK Lab or FTK Enterprise.
2. Enter administrator login credentials.
   - A database schema upgrade prompt will appear.
3. Click Yes.
4. Enter the database administrator login credentials and click OK.
   - The database schema upgrade will begin. The application may look like it has crashed but it is currently waiting for the database schema upgrade to complete.
5. When the database schema has been upgraded, the application will responsive and available to use.
Windows Agent Module Update

The patching process will not update the existing modules within the Site Server installation location and as a result users may face issues with Disk Previews.

Updating Site Server Modules

These steps must be followed on all machines running Site Server 7.6.0.216.

Steps:

1. On the Application server, navigate to the “modules” folder.
   - <Drive:>\Program Files\AccessData\Forensic Tools\7.6\bin\Agent\modules\Windows\x64
2. Copy the DiskPreview.PKG agent module to the Site Server Installation directory and replace the existing version.
   - <Drive:>\Program Files\AccessData\SiteServer\modules\Windows\x64
3. Delete the existing Site Server Results folder.
   - This can be found within the Site Server Configuration application.
4. Open the Site Server Configuration application as an administrator.
5. Modify the Site Server Results path, either adding or removing a trailing slash.
6. Click Apply.
   - The Site Server Results folder will be rebuilt with the updated module.
7. Click Close.
Updating The Disk Preview Module On Deployed Agents

These steps must be followed on all machines running Forensic Tools 7.6.0.618.

**Steps:**

1. Ensure the FTK 7.6 SP1 patch has been installed.
2. Open **FTK Enterprise** and log in.
3. Create a new case or open an existing one.
4. Click **Tools > Configure Agent Push**.
5. Ensure the Path to trusted modules certificate is correct
   - `<Drive>:\Program Files\AccessData\Forensic Tools\7.6\bin\Agent\modules\adata.p7b`
6. Ensure the Path to agent modules is correct.
   - `<Drive>:\Program Files\AccessData\Forensic Tools\7.6\bin\Agent\modules`
7. Click **OK**.
   - **Steps beyond this point are only required on a single machine running FTK Enterprise/Central.**
8. Click **Evidence > Add Remote Data**.
9. Select an **Agent(s)** within the **Node list**.
10. Select (Optional) **Physical Drive (Preview/Acquire)**.
    - Other agent jobs can be used in this process to update agent modules.
11. Select **Install or Update Agent Modules** and **Modules only**.
12. Click **OK**.
13. In the **Select Drives** pane, select a drive.
14. Select **Preview Information Only**.
15. Click **OK** to begin the agent job and the module update.
New Installation Verification

Once the installation is completed, users can confirm the new version installation by viewing the new version number on the title bar of the application window (as highlighted in the image shown below).

Additionally, please ensure the **Schema Version** has been updated to 7.1.104.0 within DBConfig.
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.
4145 SW Watson Ave., Suite 400
Beaverton, OR 97005.
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