

FTK SUITE 8.2 SP3 - INSTALLATION GUIDE

OCTOBER 2026

Table of Contents

About Exterro.....	3
Purpose of the Document.....	3
1 Prerequisites.....	3
2 Before You Begin	4
2.1 Stop All Active Jobs	4
2.2 Restart All Affected Systems.....	4
2.3 Close All Exterro Applications	4
3 Installation Steps - FTK Enterprise/Lab/Central	5
4 Site Server Upgrade Steps	13
4.1 Site Server Upgrade / Fresh Installation.....	13
4.2 Site Server Configuration - Agent Check-in Settings	21
Contact Exterro	24

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.

Purpose of the Document

This guide provides clear step-by-step instructions for upgrading the **Exterro FTK (Forensic Toolkit)** application to version **8.2 SP3**.

1 Prerequisites

Before beginning the upgrade, verify that all related Exterro applications are running the required minimum versions listed below.

To check currently installed versions, navigate to:

Start > Control Panel > Programs > Programs and Features

Application	Minimum Required Version
Exterro Forensics Tools 8.2	8.2 / 8.2 SP1/SP2
Exterro Forensics Tools Suite 8.2	
Exterro FTK Plus	
Exterro Desktop Viewer	
Exterro Evidence Processing Engine 10.29	10.29 SP1/SP2
Exterro Distributed Processing Manager 10.29	

2 Before You Begin

Complete the following steps on every machine in your environment before starting the installation.

2.1 Stop All Active Jobs

- Ensure that **no active jobs** are currently running under the **WeblabSelfHost** service.
- Wait for all in-progress jobs to complete, or safely pause/cancel them before continuing.

2.2 Restart All Affected Systems

Important: *In a distributed environment, the restart must be performed on every machine running any of the services listed below. Failing to do so may result in patch conflicts or installation failures due to locked files (DLLs, EXEs, or configuration files).*

Restart machines running any of the following services:

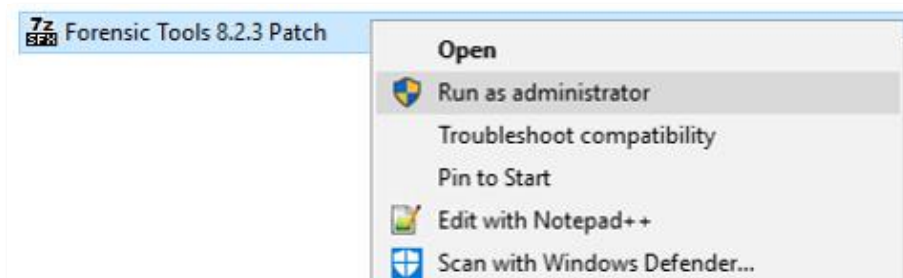
- Exterro Distributed Processing Manager
- Exterro Evidence Processing Engine
- Exterro Forensic Tools
- Exterro Site Server
- Exterro FTK Plus/Desktop Viewer

2.3 Close All Exterro Applications

- Close FTK, DPM, and any other Exterro applications before proceeding.
- Ensure no Exterro background processes are running in Task Manager.

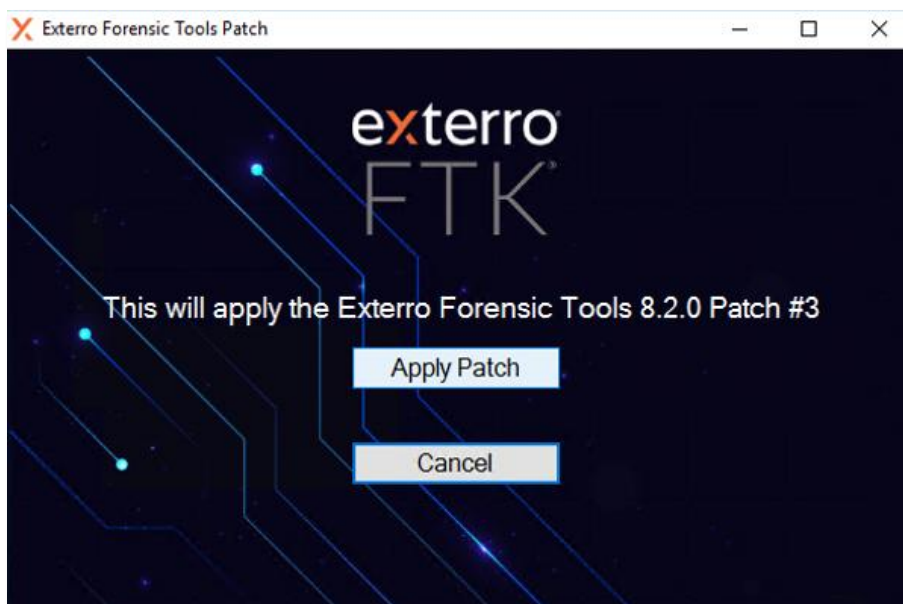
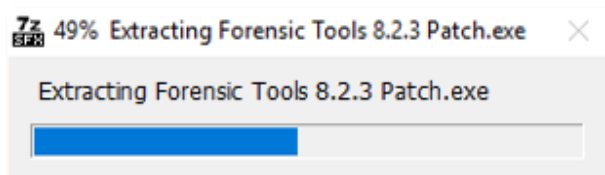
3 Installation Steps - FTK Enterprise/Lab/Central

1. Download the Latest patch installer (FTK 8.2 SP3) from the [Exterro Product Downloads page](#).
2. Right-click on the downloaded file, **Forensic Tools 8.2.3 Patch.exe** and select **Run as administrator**.

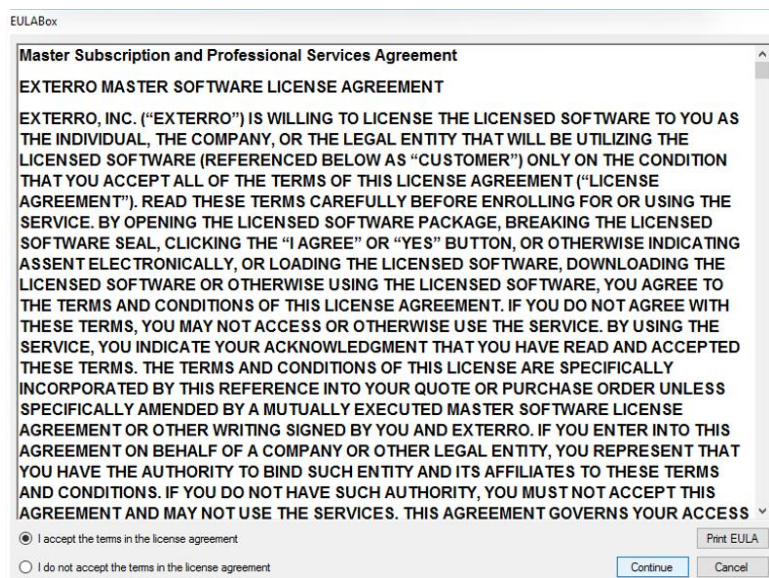


Note: If prompted by **User Account Control**, click **Yes** to allow the application to make changes to your device.

3. The extraction process will begin, and it may take 2 to 3 minutes. Once completed, click **Apply Patch**.

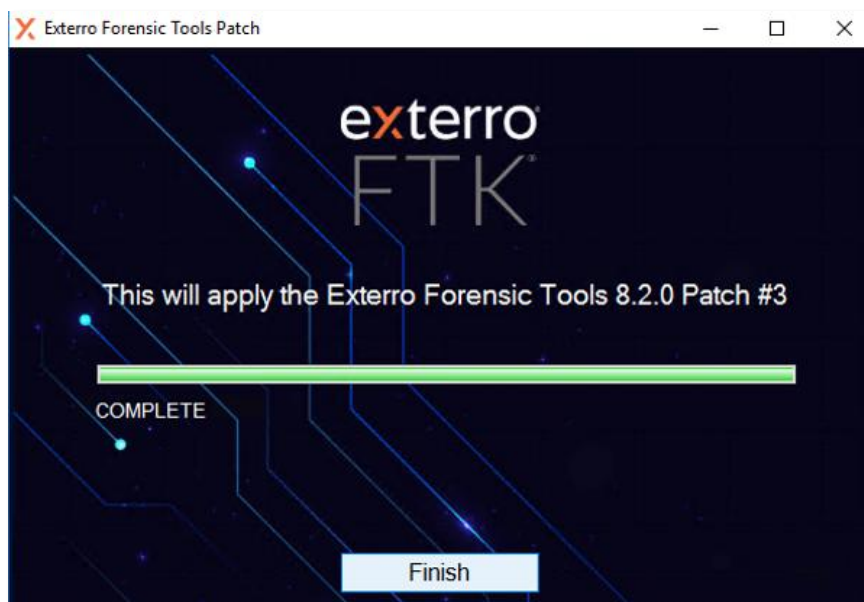


4. Read and accept the terms and conditions of the License Agreement and click **Continue**.

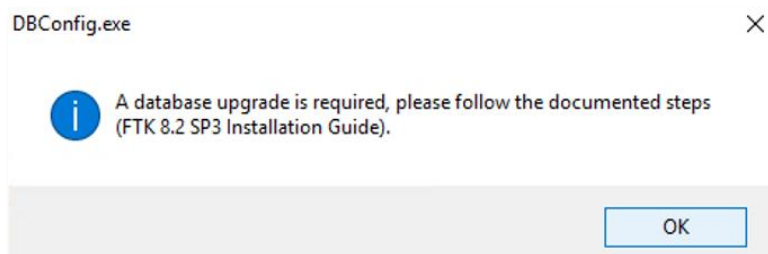


5. The upgrade will proceed with the following components applied sequentially:
 - i. **FTK Plus Patch**
 - ii. **Desktop Viewer Patch**
 - iii. **EP/DPE Patch Application with Black Ice Printer Driver**
 - iv. **DPM Patch Application**
 - v. **FTK Patch**

6. After all the above patches have been applied, click **Finish** to start with the Database update.



- The following DB Config pop-up is displayed:



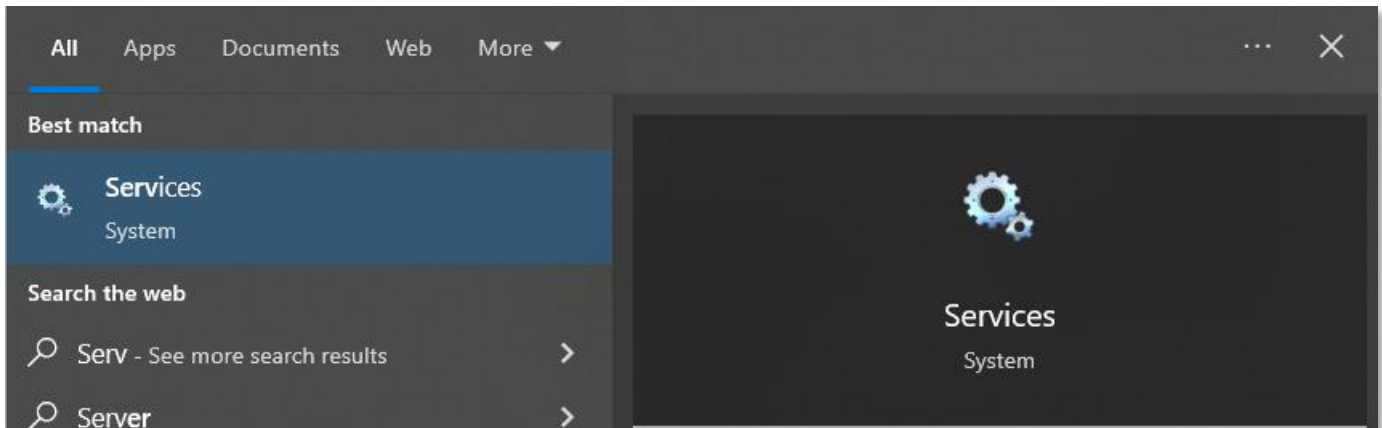
7. Click **Ok**. The DB Config tool will open.

Note: Perform the following steps (from Step 8 – Step 14) if you are upgrading from version 8.2 or 8.2 SP1; these steps can be ignored if you are upgrading from version 8.2 SP2.

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.

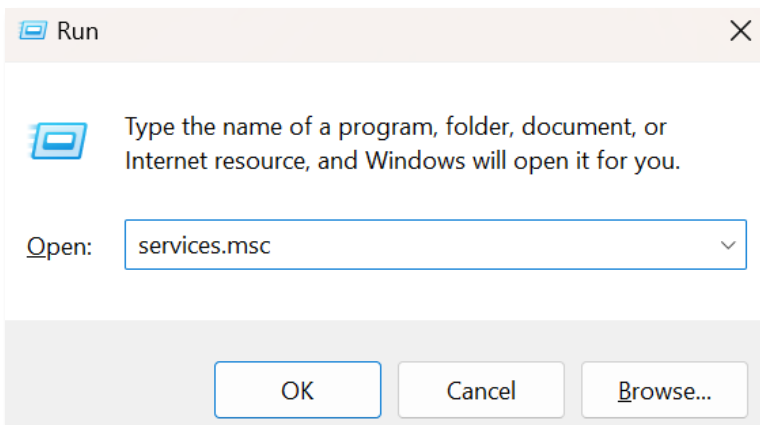
8. To update the database, begin by stopping the **Exterro Self-Host Service**.

- i. Open the **Start** menu, search for **Services**, and click on it to launch the **Windows Services** window.
- ii. In the Services window, locate the required service, right-click on it, and select **Stop**.

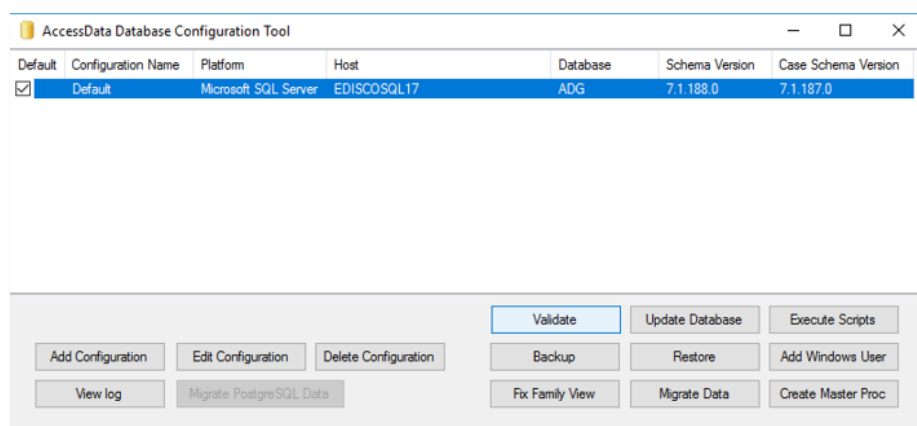


Alternative method:

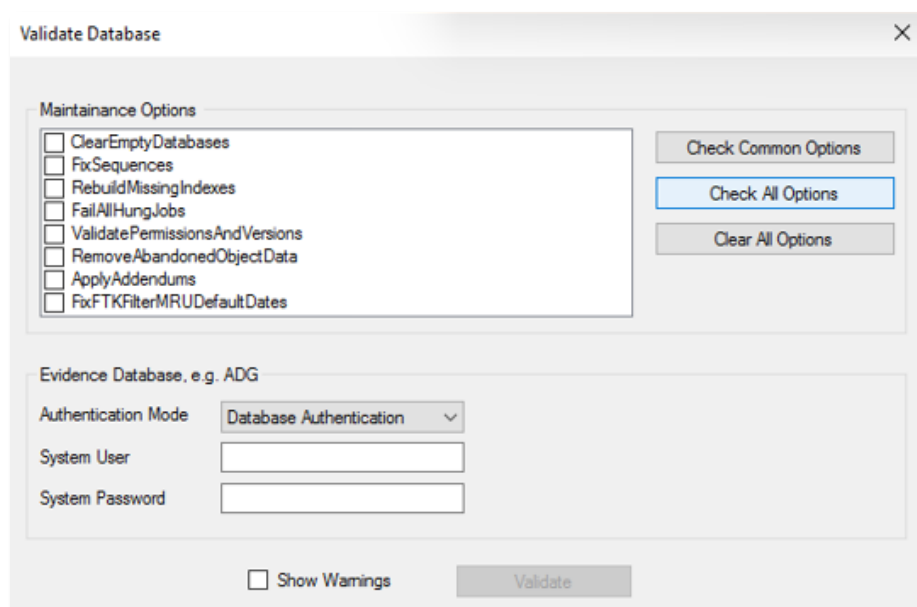
- i. Press **Windows + R** to open the **Run** dialog box. Type **services.msc**, click **OK**, then find and stop the necessary service.



9. From the **Database Configuration Tool**, select the existing applicable database and click **Validate**.



- The **Validate Database** page is displayed.



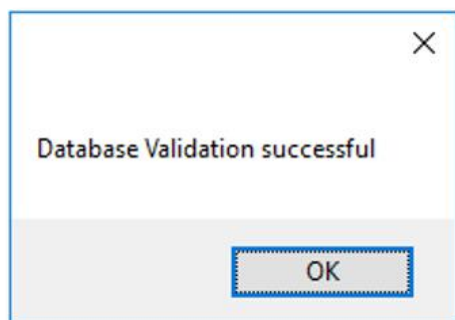
10. Select an **Authentication Mode** (Windows or Database Authentication).

Note: If Database Authentication is used, enter the **Service Account (sa) credentials** to proceed.

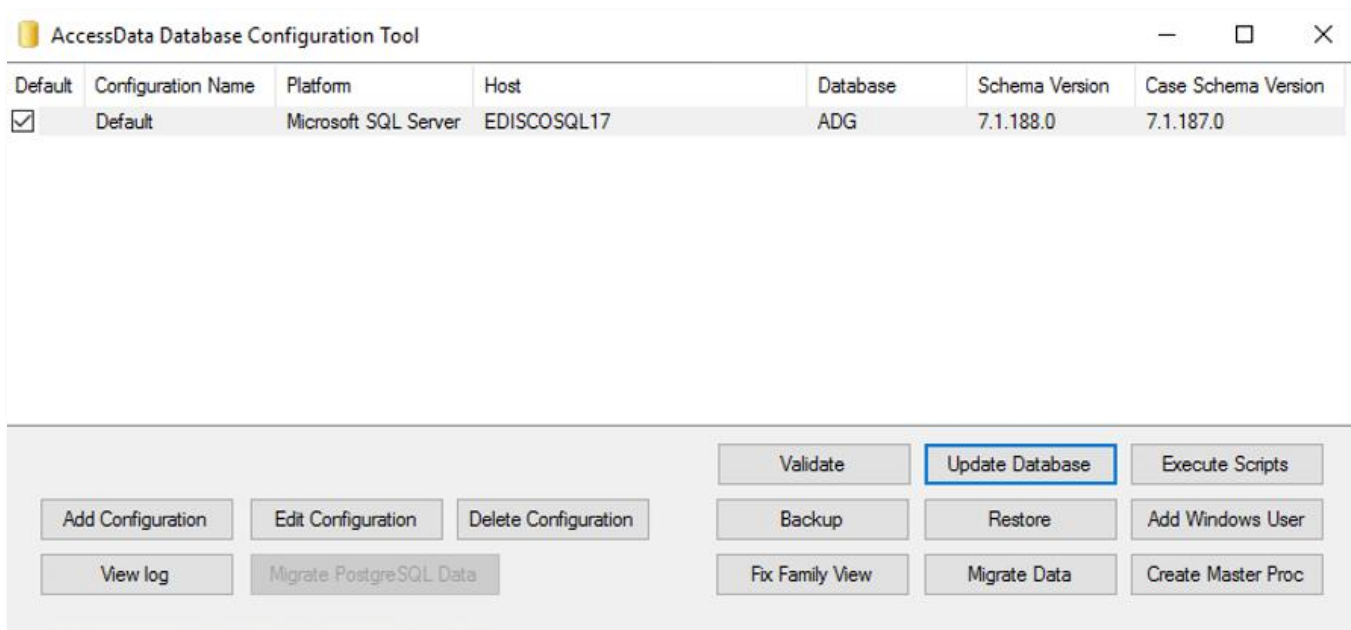
11. Click **Check All Options**. And click **Validate**.

Warning: Proceed with the next steps only when your **Database validation is successful** pop-up message is displayed. If this message does not appear, do not continue with the process and forward any error messages or details from the failed validation to support@exterro.com.

12. Once the validation is successful, click **Ok**.

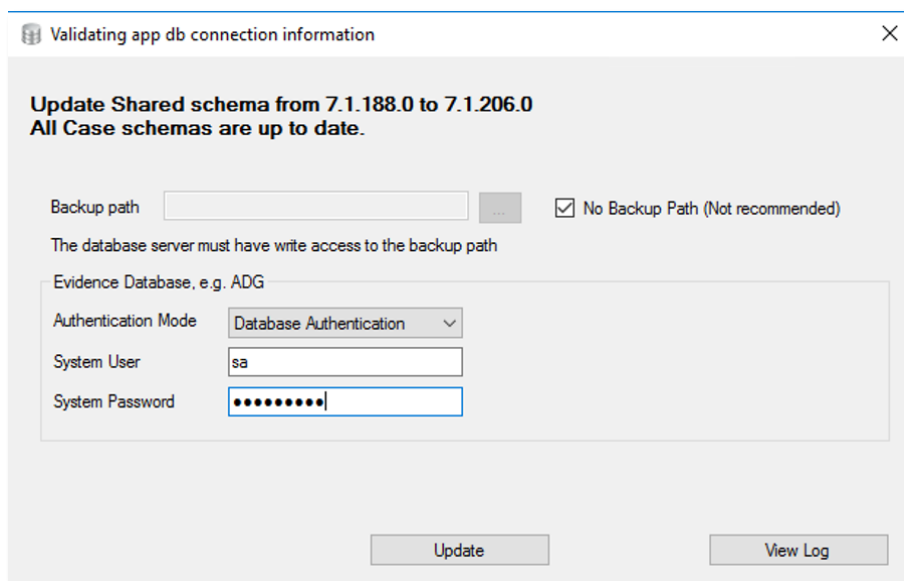


13. From the **Database Configuration Tool**, select the required database and click **Update Database**.



14. Select the required database and click **Update Database**.

- The following page is displayed.



15. Select a **Backup Path**.

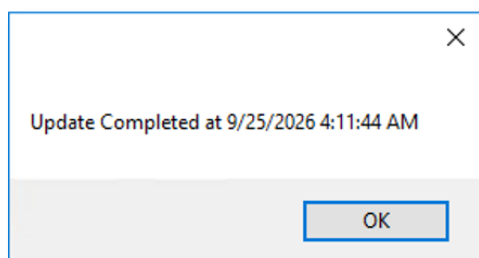
Note: The **Backup Path** specified must be accessible from the Database Server by the service account in use. The **No Backup Path** option should **only** be selected if the user has already backed up their database through another method.

16. Select an **Authentication Mode**.

Note: If Database Authentication is used, enter the Service Account (sa) credentials to proceed.

17. Click **Update**.

- You will be indicated with an update completed pop-up.



18. Click **Ok**.

Note: Once the database is updated, confirm the **Default** box is checked against the newly created database. You are recommended to contact the Exterro Support Team in case any errors are displayed.



Note: After the installation is completed, verify that all applications have been upgraded to their corresponding version by navigating to **Start > Control Panel > Programs > Programs and Features**.

Applications	Version
Exterro Forensic Tools 8.2	8.2 SP3
Exterro Forensics Tools Suite 8.2	
Exterro FTK Plus	
Exterro Desktop Viewer	
Exterro Distributed Processing Manager 10.29	10.29 SP3
Exterro Evidence Processing Engine 10.29	

Important Note: The Desktop Viewer reserves the ports from 9000 to 9010 to support multiple concurrent sessions via HTTPS for secure communication. To ensure this, you are recommended to uninstall the older version and install the latest (8.2 SP3) version of Desktop Viewer on your machine.

4 Site Server Upgrade Steps

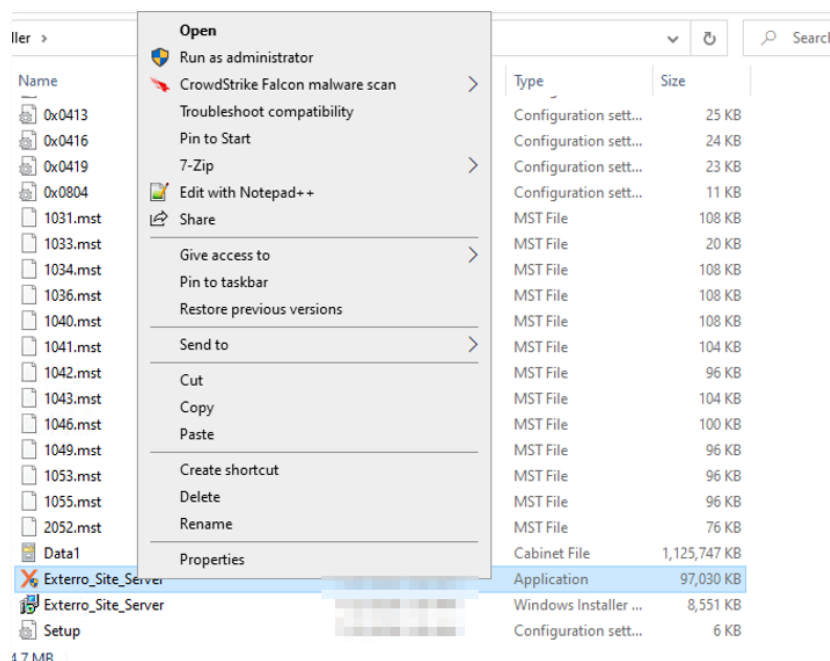
Prerequisite: Install or upgrade to **PostgreSQL 14.x** before installing the Site Server. Refer to the **Exterro FTK Site Server - PostgreSQL 14.x Upgrade Guide** for detailed PostgreSQL installation and upgrade steps.

4.1 Site Server Upgrade / Fresh Installation

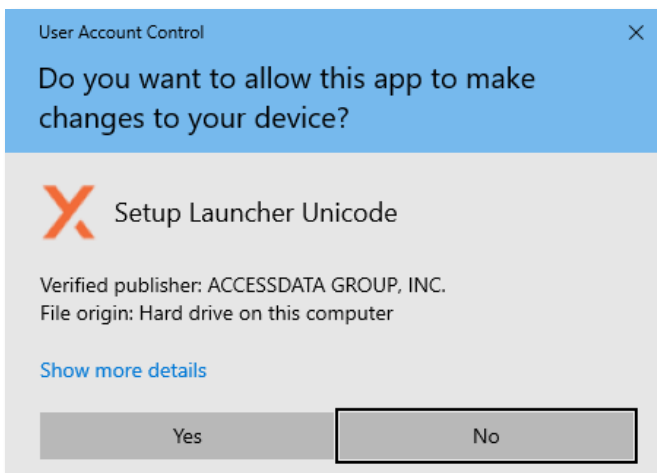
To install or upgrade Site Server, follow these steps:

Note: Site Server can be upgraded from versions 8.2 or 8.2 SP1/SP2 to 8.2 SP3. Ensure that a local instance of AccessData/Exterro managed PostgreSQL is installed and running. After installation or upgrade, perform a clean start or restart the instance to apply changes.

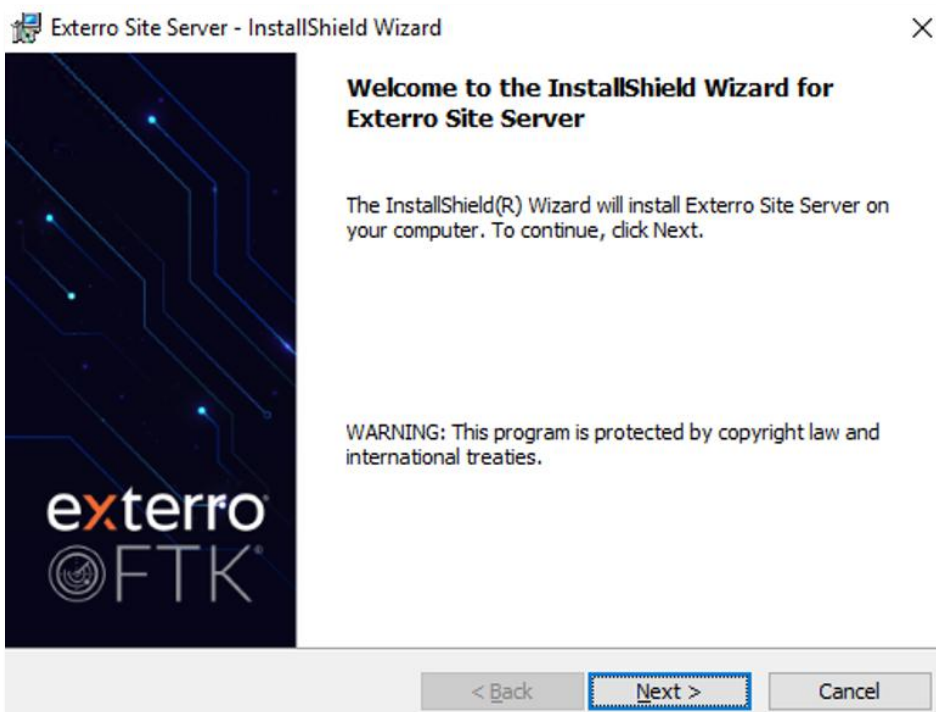
- Download the Site Server installer using the following method:
 - Method:** (Product Downloads page): Download the latest Site Server installer directly from the [Exterro Product Downloads page](#).
- A ZIP file will be downloaded. Extract the folder, and right-click on the **SiteServer.exe** file and select **Run as Administrator**.



- When prompted by **User Account Control**, click **Yes**.

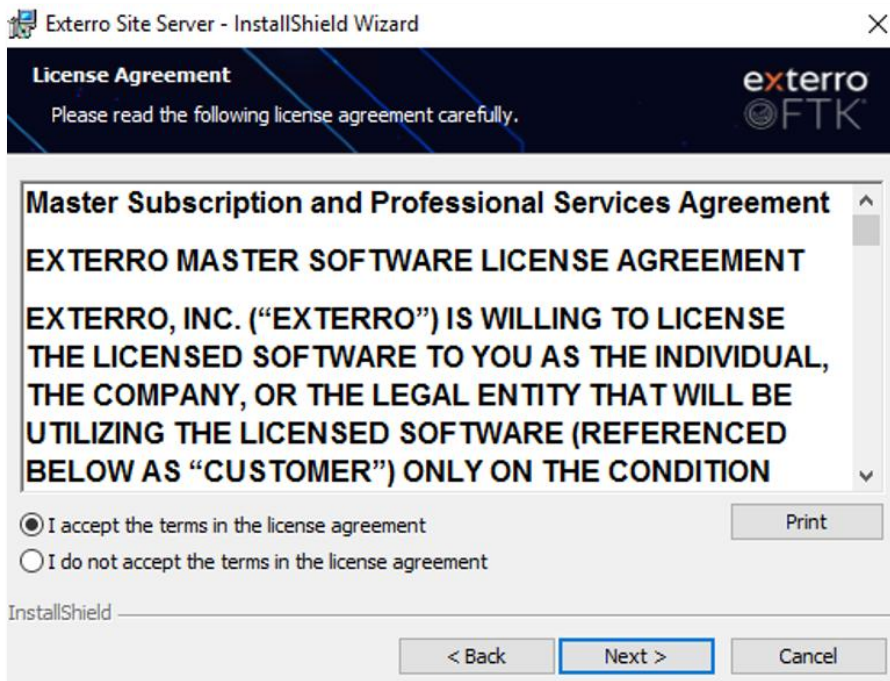


- The following page will be displayed.



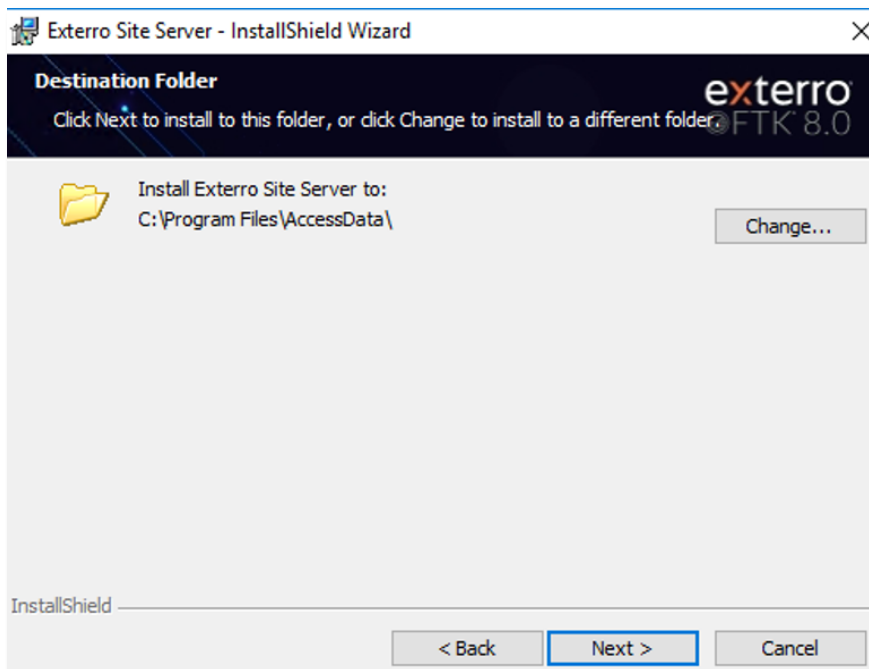
- Click **Next**.

- The **License Agreement** page is displayed.



5. Review and accept the terms and click **Next**.

- The **Destination Folder** page is displayed.



6. Select the folder location and click **Next**.

- The **User Credentials** page is displayed.

Exterro Site Server - InstallShield Wizard

User Credentials
Set the Credentials of the Exterro Site Server Services

☒ Local System Account ☐ Specific User Account

If you are installing a child site server, you can configure the service to use credentials that give the service access to the eDiscovery server's responsive path without having to communicate through the parent site server. In order to do this, you must specify the credentials of an account name that exists on both the site server and the eDiscovery server. Use the Specific User Account option to set the credentials.

User name:
[Text Box]

Domain (Leave BLANK if user account is a local non-domain account):
[Text Box]

Password:
[Text Box]

InstallShield

< Back Next > Cancel

7. Provide the user credentials and click **Next**.

- The Ready for installation page is displayed.

Exterro Site Server - InstallShield Wizard

Ready to Install the Program
The wizard is ready to begin installation.

Click Install to begin the installation.

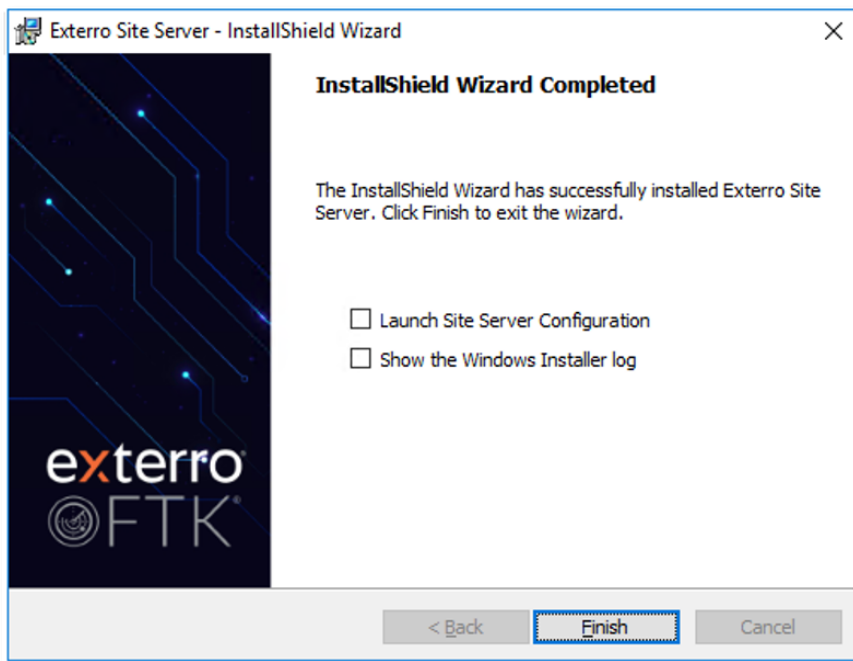
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

InstallShield

< Back Install Cancel

8. Click **Install** to begin installation.

- The following page will be displayed.



9. When installation is completed, enable the **Launch Site Server Configuration** checkbox (to open **SSConfig.exe**).
10. Click **Finish**.

- The **Site server Configuration** page will be displayed.

Site Server Configuration - General Settings:

Site Server Configuration

General Agent Check-in Settings

Type: Root Friendly Name:

Secure Communications

Private Certificate: D:\Certs\QA\SelfSignedCert.p12 ...

Public Certificate: D:\Certs\QA\SelfSignedCert.crt ...

Agent Private Certificate: D:\Certs\QA\SelfSignedCert.p12 ...

Database

System Password: Database Port: 5432

Collection

☒ Linux Collection ☐ Windows Collection ☒ Network Collection

IP Configuration

Internal Addresses/FQDN:

External Addresses/FQDN:

☒ Use Secure Client

TCP Port: 54545 Heartbeat Port: 54555 Client Port: 54321 SS to SS Port: 54548

Results

Results Directory or unc path: C:\SS_8.2SP2HF7 ...

Results share domain:

Results share username:

Results share password:

Site Server System

Parent Instance: parent

Children Instances: ...

Site Server Instances: ...

Locality

☐ Default Domain

Managed Subnet Address(es): ...

Locality (optional):

Configuration

Max Client Connections: 40 Replication Threads: 5

Max Agent Threads: 50 Retry Count: 5

Max Job Threads: 50 Retry Delay (ms): 100

Max SS Incoming Threads: 50 Max Event Threads: 50

Bandwidth Control

☐ 0 KB/second in from SiteServer

☐ 0 KB/second out to SiteServer

☐ 0 KB/second in from Agent

☐ 0 KB/second out to Agent

Logging Level: ALL

Agent Port: 3999 ☐ Agent Checkin Log

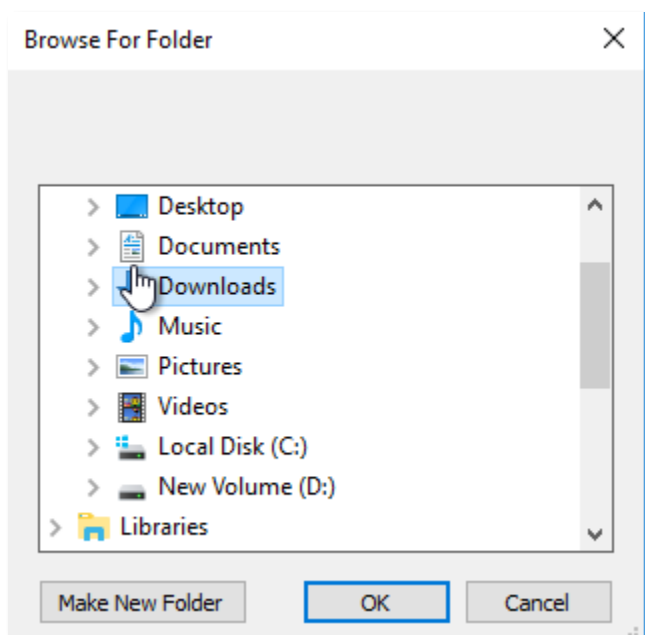
CatchAll Delay(s): 0

Apply Close

Notes:

- For **Fresh Installation**, configure all required fields manually.
- For **upgrade**, existing configurations from the previous version are retained automatically.
- For the Root site server, only the **System Password** and **Results Directory** needs to be configured.

11. Enter the **PostgreSQL System Password** in the 'System Password' field.
12. You can click on the **Browse (...)** option to select an existing folder or click **Make New Folder** to create and choose a new folder.



Note: If this path was previously selected, ensure that a trailing backslash is included, or remove it to rebuild the results folder with the latest agent modules and installers.

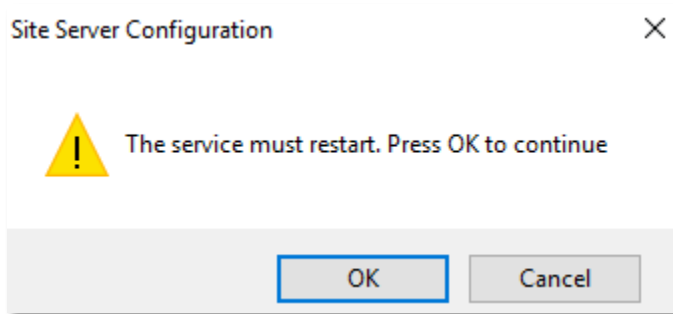
For example:

- With a backslash: **C:\Program Files\AgentModules**
- Without a backslash: **C:\Program Files\AgentModules**

13. Click on **Apply** to save the configurations made in the **General Settings** section.

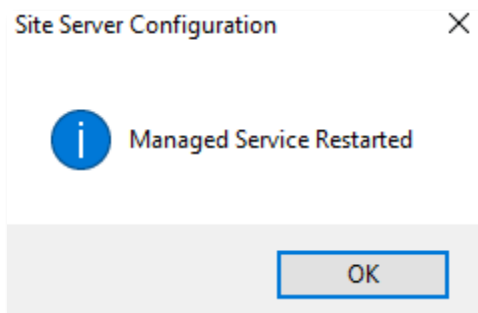
Note: For more configuration details, refer to the [Configuring Site Server \(KB article\)](#).

- A (Warning) **Site Server Configuration** pop-up is displayed.



14. Click **OK**.

- A pop-up will appear prompting you to restart the service. The service must be restarted, and any ongoing jobs may need to be restarted.



15. Click **OK**.

4.2 Site Server Configuration - Agent Check-in Settings

The **Agent Check-in Settings** section applies only to public site servers and is not applicable for users trying to configure it for root.

Important: The following fields should be configured for the corresponding Agents:

Agent Type	Fields to be configured
Off-Network Windows Agent	• Certificate Path • Certificate Password • HTTPS Port
Off-Network Mac Agent	• Certificate Path • Certificate Password • HTTPS Port • Reverse Proxy (Mac Agents Only) • FTKC FQDN/IP
Both Off-Network Windows and Off-Network Mac Agents	• Certificate Path • Certificate Password • HTTPS Port • Reverse Proxy (Mac Agents Only) • FTKC FQDN/IP

Steps:

1. From the **Site Server Configuration** pop-up, select the **Agent Check-In Settings** section.

The screenshot shows the 'Site Server Configuration' dialog box with the 'Agent Check-in Settings' tab selected. The fields and options are as follows:

- Certificate Path :** C:/Program Files/AccessData/SiteServer/publicss8-1-01.add (with a browse button '...')
- Certificate Password :** (empty text field)
- HTTPS Port :** 443
- ☒ **Reverse Proxy (Mac Agents Only)** ☐ **Save Agent Logs During Checkin**
- FTKC FQDN/IP :** (empty text field)
- Buttons:** Apply, Close

2. Browse and select the required PFX certificate from the **Certificate Path** field.
3. Provide the **Certificate Password**.

Note: Passwords must be provided in plain text and will be encrypted automatically when the Site Server service is restarted.

4. The value for **HTTPS Port** is updated as **443** by default. However, you can change it based on your preference.

Note: The value in **HTTPS Port** determines the managed site server service's running port.

5. Check the **Reverse Proxy (Mac Agents Only)** option for reverse proxy mac agents.
6. Provide the value in below syntax for the **FTKC FQDN/IP** field:

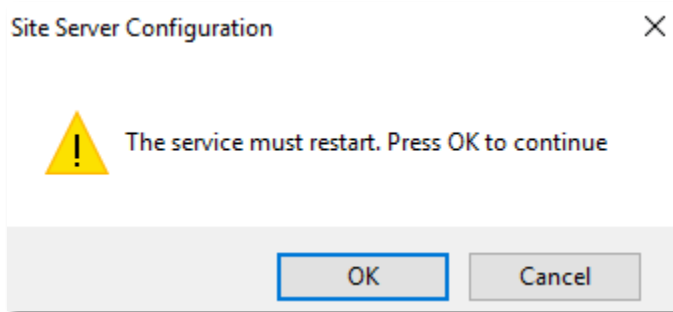
<FTK Central application URL>:<managed API Port>

Note: The **FTKC FQDN/IP** field will be enabled only upon checking the **Reverse Proxy (Mac Agents Only)** field.

7. Click on **Apply** to save the configurations made in the **Agent Check-in Settings** section.

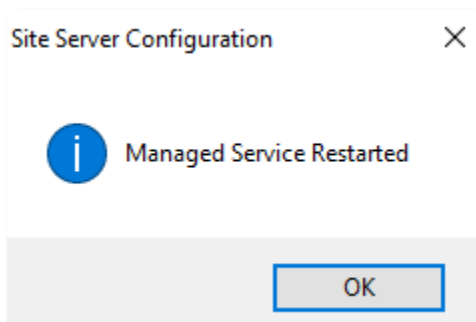
Note: Upon clicking on **Apply**, the Exterro Site Server Managed API will be restarted.

- A (Warning) **Site Server Configuration** pop-up is displayed.



8. Click **OK**.

- A pop-up will appear prompting you to restart the service.



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.