exterro®
Data Risk Management

FTK 8.3 - OPENSSL MIGRATION GUIDE

JULY 2026

Table of Contents

© Exterro, Inc. All rights reserved.

© Exterro, Inc. All rights reserved.

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 Introduction

FTK 8.3 brings a major cryptographic modernization, moving the product onto a supported, long-term-support OpenSSL release. It is delivered as a single coordinated upgrade that refreshes agents to the 8.3 build. This advisory explains what's new, why the server and agents are upgraded together, and how to roll 8.3 out smoothly across your environment.

Note: *Do not upgrade your server-side FTK components to 8.3 until you are able to redeploy the agent across your entire environment. Plan the server upgrade and the fleet-wide agent refresh as a single coordinated change.*

This guide is intended to assist with planning the FTK 8.3 upgrade. Information regarding OpenSSL versions, support lifecycle, and resolved vulnerabilities is based on the OpenSSL Project's published release notes and security advisories. For product-specific deployment guidance, refer to the FTK 8.3 documentation or contact Exterro team.

© Exterro, Inc. All rights reserved.

2 Executive Summary

FTK 8.3 introduces a comprehensive cryptographic modernization, upgrading the secure communication infrastructure that connects FTK server components to enterprise agents. This essential release transitions FTK to OpenSSL 3.5 LTS a long-term-supported library maintained through April 8, 2030. The upgrade aligns FTK's secure channels with modern industry cryptographic standards, strengthens resilience against emerging threats, and establishes a streamlined framework for future security patching.

Because pre-8.3 agents and 8.3 server-side components operate on fundamentally different cryptographic foundations, communication between legacy agents and modernized servers cannot be established natively. Consequently, FTK 8.3 requires a single, coordinated rollout spanning both server-side infrastructure and the endpoint agent fleet.

> ***Note:*** *Do not upgrade server-side FTK components to 8.3 until your deployment teams are fully prepared to redeploy the 8.3 agent across all enterprise endpoints. Server upgrades and fleet-wide agent redeployment must be executed as a unified, synchronized change to ensure uninterrupted endpoint connectivity.*

To accommodate complex operational environments requiring staged administrative approvals, FTK 8.3 HF1 will be released shortly following the primary release. FTK 8.3 HF1 will introduce an optional, off-by-default Compatibility Mode as well as throttled Out-of-Band deployment controls. However, full fleet migration to the 8.3 agent remains the standard and recommended target architecture. For customers who cannot move to 8.3 immediately, Exterro will continue to provide support during the transition, as it has over the past year.

© Exterro, Inc. All rights reserved.

3 Scope of Affected Systems

This modernization directly impacts all secure agent-to-server channels. Any deployment utilizing FTK enterprise agents falls within the scope of this advisory, regardless of the underlying host operating system:

Component	Action	Operational Impact & Details
FTK Server Infrastructure *(Central / Processing / Site Servers)*	Upgrade Server	Transitions to **OpenSSL 3.5**. Restores agent communication upon completion of **fleet-wide 8.3 agent deployment**.
FTK Agent - Windows	Redeploy Fleet	Requires **8.3 build** to negotiate the updated secure channel. Supports enhanced **Out-of-Band (OOB) updates**
FTK Agent - Linux *(x86-64)*	Redeploy Fleet	Requires **8.3 build** to negotiate the updated secure channel.
FTK Agent - Linux *(ARM64 / AWS Graviton)*	Newl supported	Native support enabled by the **OpenSSL 3.5 architecture**. (see Key Technical Enhancements in FTK 8.3 section).

***Note**: If you deploy agents, both your server and agents must be upgraded to version 8.3 together. Running mismatched server and agent versions is not supported.*

Example - Unsupported Configurations:

- *Version 8.3 server managing pre-8.3 agents*
- *Pre-8.3 server managing version 8.3 agents*

© Exterro, Inc. All rights reserved.

4 Strategic Rationale & Technical Necessity

FTK 8.3 upgrades its cryptographic foundation to a current, long-term supported (LTS) version of OpenSSL. This ensures stronger long-term security, easier maintenance, and ongoing compliance.

4.1 Long-Term Cryptographic Support Architecture

FTK 8.3 adopts OpenSSL 3.5 LTS supported through April 8, 2030 providing a modern, actively maintained cryptographic foundation that resolves known vulnerabilities. Crucially, this upgrade allows Exterro to seamlessly integrate future OpenSSL security patches, keeping your deployments secure with minimal effort over the long term.

4.2 Release Governance and Minimizing Disruption

Upgrading a major OpenSSL version requires refreshing all deployed agents. To prevent unnecessary disruption, Exterro intentionally deferred this upgrade during routine service packs and hotfixes, avoiding forced fleet-wide redeployments for routine updates.

A cryptographic shift of this magnitude belongs in a major release where teams can properly plan for it. FTK 8.3 is that release. Rather than making incremental, disruptive changes, we consolidated the OpenSSL upgrade to deliver it deliberately and all at once.

Note: *Service packs and hotfixes preserve agent compatibility so routine updates apply without re-touching endpoints. A major architectural upgrade like this belongs in a major release which is why it arrives in FTK 8.3 via a single, coordinated agent refresh.*

© Exterro, Inc. All rights reserved.

5 Key Technical Enhancements in FTK 8.3

Beyond moving to a supported cryptographic library, the 8.3 change unlocks new platform support and improves how future agent updates are delivered.

5.1 OpenSSL 1.0.2j to 3.5 LTS (3.5.5) Integration

FTK 8.3 incorporates OpenSSL 3.5.5 LTS, replacing the legacy 1.0.2j library. This update introduces forward-looking security features, including post-quantum cryptographic algorithm implementations (ML-KEM, ML-DSA, and SLH-DSA), native QUIC protocol support, and substantial cryptographic throughput optimizations over earlier OpenSSL 3.0 releases.

5.2 Native AWS Graviton (ARM64) Linux Agent Support

The OpenSSL 3.5 architectural transition unlocks native support for Linux running on ARM64 and AWS Graviton processors. Previously constrained by legacy library limitations, enterprise cloud workloads hosted on modern ARM architectures can now be fully monitored and integrated into FTK environments.

5.3 Out-of-Band (OOB) Update Enhancements - Windows Agents

FTK 8.3 resolves numerous reported issues with Out-of-Band updates, the mechanism that allows Windows agents to fetch updates dynamically from your site servers. With these fixes in place, future updates to Windows agents can be delivered in place from the site server, without IT or deployment teams performing a manual redeployment. Out-of-Band updates are a Windows-agent capability today. A follow-on release, FTK 8.3 HF1, will add the ability to control how many Out-of-Band updates occur within a 24-hour period, so a rollout can be tested at small scale before opening it up further - see Preview: FTK 8.3 HF1 Features section.

© Exterro, Inc. All rights reserved.

Why this matters for the upgrade ahead:

The 8.3 upgrade is a one-time, coordinated agent refresh. For the supported life of the OpenSSL 3.5 LTS branch - through April 2030 - updates stay within that branch and preserve agent compatibility, so they will not require another coordinated, fleet-wide redeployment. For Windows agents, Out-of-Band updates can additionally deliver those updates dynamically from your site servers.

Change in 8.3	What it gives you
OpenSSL 3.5 LTS	Supported, maintained crypto through 2030; PQC algorithms; QUIC; performance gains.
Graviton / ARM64 Linux agents	Coverage for modern ARM64 hosts, including AWS Graviton - previously unsupported.
Out-of-Band update fixes (Windows)	Dynamic, site-server-driven updates for Windows agents; removes manual redeployment from future Windows updates.

© Exterro, Inc. All rights reserved.

6 Coordinated Upgrade Strategy

The way 8.3 is rolled out follows directly from moving across an OpenSSL major version: the server and the agents are modernized together, in one coordinated step.

6.1 Connection Negotiation Modernization

OpenSSL 3.x is a new major version, and it brings the secure channel up to a current standard. Several of those changes affect how a connection is negotiated:

- **Protocol Deprecation:** Retirement of legacy protocols (such as SSLv3) and restrictive cipher selection.
- **Elevated Security Baselines:** Enforcement of higher default security thresholds, disqualifying weak keys, deprecated ciphers, and outdated signature algorithms.
- **Architecture Modernization:** Transition away from legacy ENGINE mechanisms toward modern OpenSSL providers.

6.2 Operational Alignment

FTK 8.3 components are built on OpenSSL 3.5 LTS, while agents running versions prior to 8.3 use OpenSSL 1.0.2j. Because these versions are based on different cryptographic foundations, they cannot establish secure communications using the same security policies. Upgrading both the FTK server and enterprise agents to version 8.3 ensures they operate on the same modern cryptographic foundation, enabling secure communication and consistent security behavior.

> ***Note: Plan the upgrade as a single coordinated change.*** *The FTK server and all enterprise agents should be upgraded together as part of the same maintenance activity. If the server is upgraded while agents remain on a pre-8.3 version, those agents will be unable to reconnect until they are also upgraded to FTK 8.3.*

6.3 Why This Change Is Introduced in a Major Release

Service packs and hotfixes are intended to maintain compatibility with existing enterprise agents, allowing updates to be applied without requiring changes across every endpoint. A cryptographic modernization of this scale affects the security foundation shared by the FTK server and its enterprise agents, making a coordinated upgrade necessary. For this reason, the change is delivered as part of the FTK 8.3 major release, where upgrading both the server and enterprise agents together can be planned and executed as a single, coordinated activity. The one-time enterprise agent refresh is therefore an expected part of the 8.3 upgrade.

© Exterro, Inc. All rights reserved.

7 Required Upgrade Sequence

Upgrade to FTK 8.3 as a single, coordinated change across the FTK server and the entire enterprise agent fleet. The recommended deployment sequence ensures all components transition to the new cryptographic foundation together, minimizing disruption and restoring secure communications promptly.

Note: *Verify deployment readiness before starting. Confirm that the FTK 8.3 enterprise agent can be deployed to all managed endpoints before upgrading any server-side component. If part of the agent fleet cannot yet be updated, postpone the upgrade until all endpoints are ready.*

8 Deployment Considerations

8.1 Mixed Operating System and Architecture Environments

FTK 8.3 enterprise agents support Windows, Linux (x86-64), and, beginning with version 8.3, Linux on ARM64 (AWS Graviton). Plan the enterprise agent upgrade across all supported platforms using your existing deployment processes.

Windows enterprise agents can be updated using Out-of-Band (OOB) updates, allowing them to retrieve the new version dynamically from site servers. Linux x86-64 and Linux ARM64 enterprise agents should be upgraded using your standard software deployment mechanisms. Ensure newly supported ARM64 (AWS Graviton) systems are included in your deployment inventory so they are upgraded alongside the rest of the environment.

8.2 Air-Gapped and Offline Collection Nodes

For endpoints that do not have connectivity to a site server, distribute the FTK 8.3 enterprise agent using your existing offline deployment process during the same coordinated upgrade window. Because these systems cannot receive dynamic updates, they must be explicitly identified and included in the deployment plan to ensure the entire enterprise agent fleet is upgraded consistently.

© Exterro, Inc. All rights reserved.

9 Security Posture & Ongoing Maintenance

FTK 8.3 adopts OpenSSL 3.5 LTS, providing a supported, long-term-maintained cryptographic foundation that significantly simplifies future security maintenance.

OpenSSL 3.5 LTS is supported through 8 April 2030 and continues to receive security patches and maintenance updates. Upgrading to this release resolves the known OpenSSL issues addressed upstream and establishes a modern cryptographic foundation for FTK.

Going forward, this enables faster and more efficient delivery of future security updates, making it easier to keep deployments current with less operational effort. This long-term maintainability and simplified security lifecycle is one of the primary security benefits of FTK 8.3.

© Exterro, Inc. All rights reserved.

10 Support & Timeline

10.1 Continued Support During the Transition

Exterro recognizes that redeploying enterprise agents across large environments may require additional planning and time. Customers who are unable to upgrade to FTK 8.3 immediately will continue to receive support while they prepare and execute their migration, as has been the case throughout the transition period.

For Windows enterprise agents, the Out-of-Band (OOB) update enhancements introduced in FTK 8.3 simplify the delivery of future enterprise agent updates, reducing the operational effort required for subsequent deployments.

10.2 Version Timeline

Item	Status	Notes
OpenSSL 3.5 (shipped in 8.3)	LTS	Supported through 8 April 2030.

10.3 Getting Help

For assistance with migration planning, pilot deployments, upgrade validation, or enterprise agent rollout, contact your Exterro Account Manager or Exterro Technical Support.

10.4 Preview: FTK 8.3 HF1 Features

Following the release of **FTK 8.3**, **FTK 8.3 HF1** will introduce two new **SSConfig** options for both **Windows** and **Linux enterprise agents**:

- **Compatibility Mode** (disabled by default) enables pre-8.3 enterprise agents to continue communicating with FTK 8.3 components without requiring immediate redeployment. This option is intended as a temporary transition mechanism for customers who need additional time to complete their enterprise agent rollout. It is not a replacement for the coordinated upgrade strategy described in Required Upgrade Sequence section.
- **Controlled Out-of-Band (OOB) Rollout** allows administrators to limit the number of Out-of-Band enterprise agent updates within a 24-hour period. This enables organizations to validate updates in a small scale before expanding deployment across the broader enterprise agent fleet.

Note: *Additional information about both configuration options will be provided in the* ***FTK 8.3 HF1 Release Notes****.*

© Exterro, Inc. All rights reserved.

11 Version & Capability Comparison

Attribute	Before 8.3 (OpenSSL 1.0.2j)	FTK 8.3 (OpenSSL 3.5.5 LTS)
OpenSSL branch	1.0.2	3.5 LTS
Support horizon	Previous release	Supported till April 2030
Future security updates	Tied to major releases	Delivered easily within the LTS branch
Post-quantum algorithms	No	ML-KEM, ML-DSA, SLH-DSA
QUIC support	No	Yes
Default security policy	Permissive (legacy)	Higher default security level
Upgrade model	In-place service packs	Coordinated server + agent refresh
Linux ARM64 / Graviton agents	Not supported	Supported
Out-of-Band agent updates	Known issues	Numerous fixes (Windows)

12 OpenSSL Vulnerability Reference

Migrating to OpenSSL 3.5 LTS addresses the known OpenSSL vulnerabilities resolved in the upstream release, including high-impact denial-of-service (DoS) and memory safety issues. The upgrade also places FTK 8.3 on a modern, long-term-supported cryptographic foundation that continues to receive security patches and maintenance updates.

© Exterro, Inc. All rights reserved.

13 Frequently Asked Questions (FAQ)

1. **Can we run an 8.3 server with our existing agents for a while?**

   Not on 8.3 itself. With the OpenSSL upgrade, 8.3 components and pre-8.3 agents start from different cryptographic foundations, so pre-8.3 agents reconnect only once they are refreshed to 8.3. Plan the server and agents as one coordinated upgrade. Shortly after 8.3 ships, FTK 8.3 HF1 will introduce an off-by-default Compatibility Mode for customers who need more time to secure approvals for a full redeployment - see the next question.

2. **What is Compatibility Mode in FTK 8.3 HF1?**

   Compatibility Mode is an off-by-default option, configured in SSConfig and available for both Windows and Linux agents, that allows older agents to keep communicating with 8.3 components without being redeployed. It is intended for customers who need a little more time to secure approvals for a full-scale redeployment, not as a substitute for it - redeploying the fleet to 8.3 remains the outcome to plan for.

3. **Do we really have to touch every endpoint?**

   For this upgrade, yes - every agent moves to the 8.3 build as part of the coordinated refresh. Afterwards, updates within the 3.5 LTS branch preserve agent compatibility and will not require repeating this; for Windows agents, Out-of-Band updates can deliver them dynamically from your site servers. A comparable upgrade would next be expected around 2030, when the 3.5 branch reaches the end of its supported life.

4. **We cannot upgrade right now - are we cut off?**

   No. Exterro will continue to support customers who cannot move to 8.3 immediately while they plan their migration, as it has over the past year.

5. **What do we gain by moving to OpenSSL 3.5?**

   A long-term-supported cryptographic foundation, maintained through 2030; resolution of known OpenSSL issues; new platform support such as AWS Graviton; and - going forward - a far simpler path for Exterro to deliver security patches, keeping your deployment current with less effort.

6. **Can we control the pace of Out-of-Band updates?**

   From FTK 8.3 HF1, yes. A new SSConfig option lets you set how many Out-of-Band updates can occur within a 24-hour period, so you can test a rollout at small scale before opening it up to a larger volume of updates.

© Exterro, Inc. All rights reserved.

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.