MixMasters, Inc.

FTPS Security Overview

Private File Transfer Infrastructure

Document Version: 1.1

Last Updated: March 2026

Prepared By: MixMasters, Inc.

1. Introduction

This document provides a technical overview of the FTPS (FTP over TLS) security model used by MixMasters, Inc. for encrypted file transfer operations. The FTPS environment is designed to ensure confidentiality, integrity, and controlled access for customer file exchanges.

FTPS services operate independently from the mmcld.site web domain and are hosted on a secure server managed by our hosting provider. All file transfers occur over encrypted channels and require authenticated access.

2. FTPS Protocol & Encryption

MixMasters uses FTPS Explicit Mode (FTPES), which provides TLS encryption for both control and data channels.

Key Characteristics:

- Protocol: FTPS Explicit (FTPES)
- Encryption: TLS 1.2 or higher
- Plain FTP: Disabled
- Data Channel Encryption: Enabled
- Passive Mode: Supported and recommended

This ensures all credentials and file contents are encrypted end-to-end.

3. Server Identity & Certificate Validation

FTPS connections are made to the following hostname:

gator4269.hostgator.com

The FTPS server presents a trusted SSL certificate issued by a major certificate authority (CA). Customers may validate:

- Certificate issuer (Sectigo/Comodo or equivalent)
- Certificate expiration date
- Hostname match (gator4269.hostgator.com)
- Full certificate chain

The certificate is automatically renewed by the hosting provider.

4. Authentication & Access Control

All FTPS access requires authenticated login. MixMasters enforces:

- No anonymous FTP access
- Unique credentials per customer
- No shared accounts
- Strong password requirements
- Encrypted credential transmission via TLS

Credentials are issued directly to authorized customer IT personnel.

5. Directory Isolation & Permissions

Each customer is isolated within their own directory using chroot (jail) enforcement.

Protections include:

- No access to parent directories
- No visibility into other customer folders
- No cross-account file access
- Write permissions limited to assigned directories

This prevents accidental or unauthorized access to other customers' data.

6. Logging & Monitoring

The FTPS server maintains logs for:

- Successful logins
- Failed login attempts
- File uploads and downloads
- IP addresses
- Timestamps
- Session commands

Logs are retained by the hosting provider for security and audit purposes.

7. Directory & File Access Controls

The FTPS environment enforces strict directory access rules:

- Directory listing disabled
- Sensitive file types blocked
- No access to system-level configuration files
- Only customer-specific directories are accessible

7.1 Directory Structure (Conceptual Model)

Each customer is isolated within their own FTPS directory under the MixMasters FTPS root. A simplified conceptual structure is:

```
public_ftp/
  mmcloud/
    CustomerA/
    CustomerB/
    CustomerC/
    ...
```

Key Security Properties:

- Each customer is jailed (chroot) into their assigned directory
- No customer can see or access another customer's folder
- Parent directories are not accessible
- No shared storage or cross-tenant visibility

- Directory isolation is enforced at the server level

8. Firewall & Connectivity Requirements

To ensure proper FTPS connectivity, customers should allow outbound connections to:

Hostname: gator4269.hostgator.com

Protocol: FTPS Explicit (FTPES)

Port: 21 (control channel)

Passive Mode Ports: Typically 49152-65535 (as assigned by hosting provider)

Passive mode is required for most corporate firewalls.

9. Separation From Web Services

FTPS services are completely isolated from the mmcld.site web domain.

Key Distinctions:

- FTPS does not use Apache
- FTPS does not use .htaccess
- FTPS does not use the mmcld.site SSL certificate
- FTPS is not filtered by SiteLock or any web firewall
- FTPS runs on a separate server and protocol stack

This ensures web configuration changes cannot impact FTPS operations.

10. Operational Workflow

A typical customer workflow includes:

1. Customer receives FTPS credentials from MixMasters
2. Customer connects using FTPS Explicit mode through the embedded MixMaster FTPS client
3. Customer uploads files to their isolated directory
4. MixMasters retrieves files securely from the same directory

All FTPS operations are performed within MixMaster. No third-party FTP applications are required or supported.

11. Security Best Practices

MixMasters recommends the following for all customers:

- Use FTPS Explicit mode only
- Enable TLS certificate validation
- Use passive mode
- Restrict FTPS access to approved IP ranges
- Rotate credentials periodically
- Avoid storing credentials in plaintext

12. Overall Security Assessment

The MixMasters FTPS environment provides:

- Encrypted file transfers
- Strong authentication
- Directory isolation
- Certificate-based server identity
- Comprehensive logging
- Firewall-friendly passive mode
- Full separation from web services

This configuration meets or exceeds industry expectations for secure file transfer operations.

13. Contact Information

For FTPS support or additional security documentation, please contact:

MixMasters, Inc.

Technical Support & Security

https://www.mixmasters.com/contact