# Active Directory FTP Security Hardening Guide

**Important Notes:**

- Replace `domain.local` with YOUR actual domain name (e.g., `company.com`, `contoso.local`)
- Replace `FTPSERVER01` with YOUR actual FTP server hostname
- Replace `10.0.0.100` with YOUR FTP server's actual IP address
- Replace `C:\FTPRoot` with YOUR actual FTP root directory path
- Replace `192.168.1.0/24` with YOUR actual client network range
- When creating user accounts, use YOUR organization's naming conventions

---

## Table of Contents

---

## 1. Install FTP Server with IIS

**Install FTP Server Role:**

1. Open **Server Manager**
2. Click **Manage** > **Add Roles and Features**
3. Click **Next** through the Before You Begin page
4. Select **Role-based or feature-based installation**, click **Next**
5. Select your server from the Server Pool, click **Next**
6. Check **Web Server (IIS)**, click **Next**
7. Click **Next** on the Features page
8. Click **Next** on the Web Server Role (IIS) page
9. On **Role Services**, expand **Web Server** > **FTP Server**
10. Check the following:
    - ✓ **FTP Service**
    - ✓ **FTP Extensibility**
11. Expand **Web Server** > **Security** and check:
    - ✓ **Basic Authentication**
    - ✓ **Windows Authentication**
12. Click **Next**
13. Click **Install**
14. Wait for installation to complete, then click **Close**

**Verify Installation:**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Expand the server node (your server name, e.g., `FTPSERVER01`)
3. Verify **Sites** folder is present
4. Close IIS Manager

## 2. Configure FTP Site

**Create FTP Root Directory:**

1. Open **File Explorer**
2. Navigate to `C:\` (or your preferred drive)
3. Right-click in empty space > **New** > **Folder**
4. Name it `FTPRoot` (or your preferred name - remember this path)
5. Close File Explorer

**Create FTP Site:**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Expand the server node (e.g., `FTPSERVER01`)
3. Right-click **Sites** > **Add FTP Site**
4. **Site Information** page:
   - FTP site name: `Secure FTP Site` (or your preferred name)
   - Physical path: Click **...** and browse to `C:\FTPRoot` (the folder you created)
   - Click **Next**
5. **Binding and SSL Settings** page:
   - IP Address: Select **All Unassigned** (or select your server's specific IP)
   - Port: `21` (default FTP port)
   - Virtual Host: Leave blank
   - SSL: Select **No SSL** for now (we'll configure SSL in the next section)
   - Click **Next**
6. **Authentication and Authorization** page:
   - Authentication: Check **Basic** only (uncheck Anonymous)
   - Authorization: Select **Specified users**
   - Enter: `Domain Admins` (or create a specific FTP user group)
   - Permissions: Check **Read** and **Write**
   - Click **Finish**

**Verify FTP Site:**

1. In IIS Manager, expand **Sites**

2. You should see your FTP site listed (e.g., "Secure FTP Site")
3. Click on the FTP site
4. In the right **Actions** pane, verify **Start** is available (if so, click it)

---

## 3. Enable FTP over SSL/TLS (FTPS)

**CRITICAL**: Always use FTPS to encrypt FTP traffic. Plain FTP sends credentials in clear text.

**Create Self-Signed SSL Certificate (For Testing):**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Click on the server node (e.g., `FTPSERVER01`)
3. Double-click **Server Certificates**
4. In the right **Actions** pane, click **Create Self-Signed Certificate**
5. Specify a friendly name: `FTP SSL Certificate` (or your preferred name)
6. Select **Personal** for certificate store
7. Click **OK**
8. The certificate now appears in the list

**Note**: For production environments, obtain a certificate from a trusted Certificate Authority (CA) instead of using self-signed certificates.

**Configure FTP Site to Use SSL:**

1. In IIS Manager, expand **Sites**
2. Click on your FTP site (e.g., "Secure FTP Site")
3. Double-click **FTP SSL Settings**
4. Under **SSL Certificate**, select your certificate from the dropdown (e.g., "FTP SSL Certificate")
5. Under **SSL Policy**, select:
   - **Require SSL connections** (most secure - blocks unencrypted connections)
   - Or **Allow SSL connections** (allows both encrypted and unencrypted - not recommended)
6. Click **Apply** in the right **Actions** pane

**Update FTP Site Binding:**

1. In IIS Manager, right-click your FTP site > **Edit Bindings**
2. Select the FTP binding and click **Edit**

3. Verify SSL Certificate shows your certificate
4. Click **OK**, then **Close**

---

## 4. Configure FTP User Isolation

User isolation prevents users from browsing other users' directories.

**Enable User Isolation:**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Expand **Sites**
3. Click on your FTP site (e.g., "Secure FTP Site")
4. Double-click **FTP User Isolation**
5. Select one of the following options: **Option A - User name directory (Active Directory)**:
    - Select **User name directory (Active Directory)**
    - Click **Set** to configure AD settings
    - Username: Enter an AD service account (e.g., `domain\ftp_service`)
    - Password: Enter the service account password
    - Click **OK**
    - Click **Apply**

    **Option B - User name directory (isolate users)**:

    - Select **User name directory (isolate users)**
    - Create subdirectories under `C:\FTPRoot\LocalUser\[username]` for each user
    - Click **Apply**

    **Option C - User name physical root (restrict access)**:

    - Select **User name physical root (restrict access to the physical root directory)**
    - Click **Apply**
6. Recommended: **User name directory (Active Directory)** for AD-integrated environments

**Create User Directory Structure (If using Option B):**

1. Open **File Explorer**
2. Navigate to `C:\FTPRoot` (your FTP root)
3. Create folder: `LocalUser`

4. Inside `LocalUser`, create folders for each FTP user:
   - Example: `C:\FTPRoot\LocalUser\jsmith`
   - Example: `C:\FTPRoot\LocalUser\mjones`
5. Set NTFS permissions on each user folder (see Section 9)

---

## 5. Set Up FTP Authorization Rules

Control which users and groups can access your FTP site.

**Configure Authorization Rules:**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Expand **Sites**
3. Click on your FTP site (e.g., "Secure FTP Site")
4. Double-click **FTP Authorization Rules**

**Add Allow Rule for Domain Admins:**

1. In the right **Actions** pane, click **Add Allow Rule**
2. Select **Specified roles or user groups**
3. Enter: `Domain Admins` (or your preferred admin group - **use YOUR group name**)
4. Permissions: Check **Read** and **Write**
5. Click **OK**

**Add Allow Rule for Specific FTP Users Group:**

1. Click **Add Allow Rule** again
2. Select **Specified roles or user groups**
3. Enter: `FTP Users` (create this group in AD first - **use YOUR group name**)
4. Permissions: Check **Read** only (or Read and Write if needed)
5. Click **OK**

**Remove Default Rules (If Present):**

1. If you see a rule for "All Users" or "Anonymous", select it
2. Click **Remove** in the right **Actions** pane

3. Click **Yes** to confirm

**Add Deny Rule (Optional - Block Specific Users):**

1. Click **Add Deny Rule**
2. Select **Specified users**
3. Enter username to block (e.g., `domain\baduser` - **use actual username**)
4. Click **OK**

---

## 6. Configure FTP Firewall Settings

Allow FTP traffic through Windows Firewall and configure passive port range.

**Configure FTP Firewall Support:**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Click on the server node (e.g., `FTPSERVER01`)
3. Double-click **FTP Firewall Support**
4. Enter your server's **external IP address** in **Data Channel Port Range** field:
    - If behind NAT/firewall: Enter your **public IP address**
    - If direct internet: Enter your **server's IP** (e.g., `10.0.0.100`)
5. Set **Data Channel Port Range**: `50000-50100` (or your preferred range)
6. Click **Apply** in the right **Actions** pane

**Configure Windows Firewall Rules:**

1. Open **Server Manager** > **Tools** > **Windows Defender Firewall with Advanced Security**
2. Click **Inbound Rules**

**Allow FTP Control Port (Port 21):**

1. Click **New Rule** in the right **Actions** pane
2. Select **Port**, click **Next**
3. Select **TCP**, enter **21**, click **Next**
4. Select **Allow the connection**, click **Next**
5. Check **Domain** profile, click **Next**

6. Name: `FTP-Control-Port-21`, click **Finish**

**Allow FTP Data Port Range (Passive Mode):**

1. Click **New Rule** again
2. Select **Port**, click **Next**
3. Select **TCP**, enter **50000-50100** (match your configured range), click **Next**
4. Select **Allow the connection**, click **Next**
5. Check **Domain** profile, click **Next**
6. Name: `FTP-Data-Ports-Passive`, click **Finish**

**Restrict to Specific IP Ranges (Recommended):**

1. Right-click the **FTP-Control-Port-21** rule > **Properties**
2. Go to **Scope** tab
3. Under **Remote IP address**, select **These IP addresses**
4. Click **Add**
5. Enter your client network range (e.g., `192.168.1.0/24` **- use YOUR network**)
6. Click **OK**, then **OK** again
7. Repeat for **FTP-Data-Ports-Passive** rule

---

## 7. Implement FTP IP Restrictions

Restrict FTP access to specific IP addresses or ranges.

**Configure IP Address Restrictions:**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Expand **Sites**
3. Click on your FTP site (e.g., "Secure FTP Site")
4. Double-click **IPv4 Address and Domain Restrictions**

**Add Allow Entry for Internal Network:**

1. In the right **Actions** pane, click **Add Allow Entry**
2. Select **IP address range**
3. Enter your network range:

   - IP address: `192.168.1.0` (example - **use YOUR network**)
   - Subnet mask: `255.255.255.0`
4. Click **OK**

**Add Deny Entry for Specific IP (Optional):**

1. Click **Add Deny Entry**
2. Select **Specific IP address**
3. Enter the IP to block (e.g., `203.0.113.50` - **use actual IP to block**)
4. Click **OK**

**Set Default Deny Policy (Maximum Security):**

1. In the right **Actions** pane, click **Edit Feature Settings**
2. Select **Deny** for "Access for unspecified clients"
3. Click **OK**

**Note**: With default deny, you must explicitly allow all legitimate IP ranges.

---

## 8. Configure FTP Logging

Enable detailed FTP logging to monitor access and detect security incidents.

**Configure FTP Logging:**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Expand **Sites**
3. Click on your FTP site (e.g., "Secure FTP Site")
4. Double-click **FTP Logging**
5. Under **One log file per**, select **Site** (recommended)
6. Under **Log File Format**, select **W3C** (recommended for detailed logs)
7. Click **Select Fields** button
8. Ensure the following are checked:
   - ✓ **Date**
   - ✓ **Time**
   - ✓ **Client IP Address (c-ip)**

    - ✓ **User Name (cs-username)**
    - ✓ **Method (cs-method)**
    - ✓ **URI Stem (cs-uri-stem)**
    - ✓ **Protocol Status (sc-status)**
    - ✓ **Bytes Sent (sc-bytes)**
    - ✓ **Bytes Received (cs-bytes)**
    - ✓ **Time Taken (time-taken)**

9. Click **OK**
10. Under **Directory**, note the log file location (default: `C:\inetpub\logs\LogFiles`)
11. Click **Apply**

**View FTP Logs:**

1. Open **File Explorer**
2. Navigate to `C:\inetpub\logs\LogFiles`
3. Find the folder for your FTP site (e.g., `FTPSVC1`)
4. Open the most recent `.log` file with Notepad

---

## 9. Set Up FTP Directory Security

Configure NTFS permissions to secure FTP directories.

**Set NTFS Permissions on FTP Root:**

1. Open **File Explorer**
2. Navigate to `C:\FTPRoot` (your FTP root directory)
3. Right-click the folder > **Properties**
4. Go to **Security** tab
5. Click **Advanced**
6. Click **Disable inheritance**
7. Select **Convert inherited permissions into explicit permissions**
8. Click **OK**

### Remove Unnecessary Permissions:

1. Still in **Security** tab, select **Users** group
2. Click **Remove**
3. Select **Authenticated Users** if present
4. Click **Remove**

### Add Required Permissions:

1. Click **Edit**
2. Click **Add**
3. Click **Advanced** > **Find Now**
4. Select **Administrators**, click **OK**, click **OK**
5. Check **Full Control**, click **OK**
6. Click **Add** again
7. Enter: `IUSR` (IIS anonymous user account)
8. Click **Check Names**, click **OK**
9. Check **Read** only, click **OK**
10. Click **Add** again
11. Enter: `FTP Users` (or your FTP user group - **use YOUR group name**)
12. Click **Check Names**, click **OK**
13. Check **Read** and **Write** (or just Read if read-only access)
14. Click **OK**, then **OK** again

### Set Permissions on User Directories:

If using user isolation, set permissions on each user's folder:

1. Navigate to `C:\FTPRoot\LocalUser\jsmith` (example user folder)
2. Right-click > **Properties** > **Security** tab
3. Click **Edit** > **Add**
4. Enter: `domain\jsmith` (the specific user - **use actual username**)
5. Click **Check Names**, click **OK**
6. Check **Modify** permission
7. Click **OK**, then **OK** again
8. Repeat for each user folder

---

## 10. Configure FTP Bandwidth Throttling

Limit bandwidth usage to prevent FTP from consuming all available network resources.

**Configure Bandwidth Throttling:**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Click on the server node (e.g., `FTPSERVER01`)
3. Double-click **FTP Request Filtering**
4. In the right **Actions** pane, click **Edit Feature Settings**
5. Check **Enable file name filtering**
6. Check **Enable command filtering**
7. Click **OK**

**Limit Connection Bandwidth:**

1. In IIS Manager, expand **Sites**
2. Right-click your FTP site > **Manage FTP Site** > **Advanced Settings**
3. Expand **Connections**
4. Set **Maximum Bandwidth (Bytes/Second)**: Enter value in bytes
   - Example: `1048576` for 1 MB/s (1024 * 1024 bytes)
   - Example: `10485760` for 10 MB/s
   - **Use a value appropriate for YOUR network**
5. Set **Maximum Connections**: `100` (or your preferred limit)
6. Click **OK**

---

## 11. Disable Anonymous FTP Access

**CRITICAL**: Always disable anonymous FTP access in production environments.

**Disable Anonymous Authentication:**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Expand **Sites**

3. Click on your FTP site (e.g., "Secure FTP Site")
4. Double-click **FTP Authentication**
5. Select **Anonymous Authentication**
6. In the right **Actions** pane, click **Disable**
7. Verify **Basic Authentication** is **Enabled**
8. If **Windows Authentication** is available and you want to use it, click **Enable**

**Verify Anonymous Access is Blocked:**

1. In IIS Manager, click on your FTP site
2. Double-click **FTP Authorization Rules**
3. Verify there are NO rules allowing "Anonymous Users" or "All Users"
4. If present, select and click **Remove**

---

## 12. Configure FTP Session Timeouts

Automatically disconnect idle FTP sessions to improve security.

**Configure Session Timeouts:**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Expand **Sites**
3. Right-click your FTP site > **Manage FTP Site** > **Advanced Settings**
4. Expand **Connections**
5. Set **Connection Time-out (seconds)**: `300` (5 minutes - adjust as needed)
6. Set **Data Channel Idle Timeout (seconds)**: `120` (2 minutes)
7. Click **OK**

**Configure Control Channel Timeout:**

1. Still in IIS Manager, click on your FTP site
2. Double-click **FTP Site Settings** (may be listed as **FTP Site** in some versions)
3. Set **Control Channel Timeout**: `300` seconds
4. Set **Data Channel Timeout**: `120` seconds
5. Click **Apply**

## 13. Set Up FTP with Active Directory Authentication

Configure FTP to authenticate users against Active Directory.

**Prerequisites:**

1. Create an Active Directory group for FTP users (if not already created):
   - Open **Server Manager** > **Tools** > **Active Directory Users and Computers**
   - Right-click **Users** > **New** > **Group**
   - Group name: `FTP Users` (or your preferred name - **remember this name**)
   - Group scope: **Global**
   - Group type: **Security**
   - Click **OK**
2. Add users to the FTP Users group:
   - In Active Directory Users and Computers
   - Find the user (e.g., `jsmith`)
   - Right-click > **Add to a group**
   - Enter: `FTP Users`
   - Click **Check Names**, click **OK**

**Configure FTP to Use AD Authentication:**

1. Open **Server Manager** > **Tools** > **Internet Information Services (IIS) Manager**
2. Expand **Sites**
3. Click on your FTP site (e.g., "Secure FTP Site")
4. Double-click **FTP Authentication**
5. Ensure **Basic Authentication** is **Enabled**
6. Optional: Enable **Windows Authentication** if desired (more secure, requires client support)

**Configure Authorization for AD Groups:**

1. Click on your FTP site
2. Double-click **FTP Authorization Rules**
3. If not already done, click **Add Allow Rule**
4. Select **Specified roles or user groups**

5. Enter: `domain\FTP Users` (use format: `domain\groupname` - **YOUR domain and group**)
6. Permissions: Check **Read** and **Write** (or just Read as appropriate)
7. Click **OK**

### Test AD Authentication:

1. From a client computer, open **File Explorer**
2. In the address bar, type: `ftp://10.0.0.100` (use YOUR FTP server IP)
3. Press Enter
4. Enter credentials:
    - Username: `domain\username` (e.g., `contoso\jsmith` - **use YOUR domain**)
    - Password: User's AD password
5. Verify access is granted

---

## 14. Monitor FTP Activity

### View FTP Logs in Event Viewer:

1. Open **Server Manager** > **Tools** > **Event Viewer**
2. Expand **Applications and Services Logs** > **Microsoft** > **Windows**
3. Navigate to **IIS-Configuration** > **Operational**
4. Look for FTP-related events

### Review IIS FTP Logs:

1. Open **File Explorer**
2. Navigate to `C:\inetpub\logs\LogFiles\FTPSVC1` (your FTP site's log folder)
3. Open the most recent `.log` file
4. Look for:
    - Failed login attempts (status code 530)
    - Unauthorized access attempts (status code 550)
    - Large file transfers
    - Unusual activity patterns

### Key FTP Status Codes to Monitor:

| Status Code | Meaning | Action |
|---|---|---|
| **530** | Login incorrect | Monitor for brute-force attempts |
| **550** | Permission denied | Check authorization rules |
| **421** | Service not available | Server may be under attack or overloaded |
| **425** | Can't open data connection | Firewall/passive port issues |
| **426** | Connection closed; transfer aborted | Investigate connection stability |

### Create Event Viewer Custom View for FTP Security:

1. Open **Event Viewer**
2. Right-click **Custom Views** > **Create Custom View**
3. Select **By log**, expand **Applications and Services Logs**
4. Navigate to and check: **Microsoft** > **Windows** > **IIS-Configuration** > **Operational**
5. Click **OK**
6. Name: `FTP Security Events`
7. Click **OK**

### PowerShell Monitoring Script (Optional):

```powershell
# Monitor FTP logs for failed login attempts
# Replace path with YOUR actual FTP log directory
$logPath = "C:\inetpub\logs\LogFiles\FTPSVC1"
$latestLog = Get-ChildItem $logPath | Sort-Object LastWriteTime -Descending | Select-Object -First 1

# Search for failed logins (status 530)
Get-Content $latestLog.FullName | Where-Object {$_ -like "*530*"} |
    Select-Object -Last 20

# Count failed attempts by IP
Get-Content $latestLog.FullName | Where-Object {$_ -like "*530*"} |
    ForEach-Object {($_ -split " ")[8]} |
    Group-Object | Sort-Object Count -Descending
```

## 15. FTP Security Checklist

Use this checklist to verify your FTP security configuration:

**Installation & Configuration:**

□ FTP Server installed via IIS

□ FTP site created with proper physical path

□ FTP site is started and operational

**SSL/TLS Encryption:**

□ SSL certificate created or obtained

□ FTP site configured to use SSL

□ SSL policy set to "Require SSL connections"

□ FTP binding updated with SSL certificate

**Authentication & Authorization:**

□ Anonymous authentication **DISABLED**

□ Basic authentication or Windows authentication enabled

□ Authorization rules configured for specific AD groups only

□ No "All Users" or overly permissive rules present

**User Isolation:**

□ FTP User Isolation configured (AD or user directory mode)

□ User directory structure created (if applicable)

□ Each user has their own isolated directory

**Network Security:**

□ FTP Firewall Support configured with correct IP and port range

□ Windows Firewall rules created for port 21 and passive ports

□ Firewall rules restricted to internal IP ranges only

□ IP Address Restrictions configured (allow specific ranges only)

**Directory Security:**

□ NTFS permissions configured on FTP root directory

□ Unnecessary groups removed (Users, Authenticated Users)

□ FTP user group has appropriate permissions only

□ Individual user folders have per-user NTFS permissions

**Operational Security:**

□ Bandwidth throttling configured

□ Maximum connections limit set

□ Session timeouts configured (idle and control channel)

□ FTP logging enabled with W3C format

□ All necessary log fields selected

**Active Directory Integration:**

□ AD group created for FTP users

□ Users added to FTP group in AD

□ FTP authorization rules reference AD groups

□ AD authentication tested and working

**Monitoring:**

□ FTP logs reviewed for suspicious activity

□ Event Viewer custom view created for FTP events

□ Regular log review schedule established

□ Alert system for failed login attempts (if applicable)

**Best Practices:**

□ Strong password policy enforced via AD Group Policy

□ FTP server OS fully patched and updated

□ Antivirus/anti-malware installed and updated

□ Regular backups of FTP data configured

□ Documentation created for FTP configuration

---

## Quick Security Verification

**Manual Verification Steps:**

1. **Test SSL/TLS**: Use FTP client (FileZilla) to connect via FTPS (port 21, explicit TLS)
    - Should see "Certificate verified" or "Connection successful"
    - Connection should be encrypted

2. **Test Anonymous Access**: Attempt FTP connection without credentials
    - Should be **denied** (530 error)
3. **Test Authorization**: Login with non-authorized AD user
    - Should be **denied** (530 or 550 error)
4. **Test User Isolation**: Login as user, attempt to browse parent directory
    - Should be **denied** or not visible
5. **Check Logs**: Verify FTP logs are being written
    - Navigate to `C:\inetpub\logs\LogFiles\FTPSVC1`
    - Confirm recent log entries exist
6. **Test Firewall**: Attempt FTP connection from blocked IP range
    - Should be **blocked** (timeout or connection refused)

**PowerShell Verification Script:**

```powershell
```

```
# FTP Security Audit Script
Write-Host "=== FTP Security Audit ===" -ForegroundColor Cyan

# Import IIS module
Import-Module WebAdministration

# Replace "Secure FTP Site" with YOUR FTP site name
$siteName = "Secure FTP Site"

# Check if site exists
$site = Get-Website -Name $siteName
if ($site) {
    Write-Host "FTP Site Found: $($site.Name)" -ForegroundColor Green
} else {
    Write-Host "FTP Site NOT Found!" -ForegroundColor Red
    exit
}

# Check SSL configuration
$sslBinding = Get-WebBinding -Name $siteName -Protocol ftp | Where-Object {$_.certificateHash}
if ($sslBinding) {
    Write-Host "SSL Configured: YES" -ForegroundColor Green
} else {
    Write-Host "SSL Configured: NO" -ForegroundColor Red
}

# Check anonymous authentication (should be disabled)
$authConfig = Get-WebConfigurationProperty -Filter "/system.ftpServer/security/authentication/anonymousAuthentication" -
if ($authConfig.Value -eq $false) {
    Write-Host "Anonymous Auth: DISABLED (Good)" -ForegroundColor Green
} else {
    Write-Host "Anonymous Auth: ENABLED (Bad!)" -ForegroundColor Red
}

# Check basic authentication (should be enabled)
$basicAuth = Get-WebConfigurationProperty -Filter "/system.ftpServer/security/authentication/basicAuthentication" -PSPath
if ($basicAuth.Value -eq $true) {
    Write-Host "Basic Auth: ENABLED (Good)" -ForegroundColor Green
} else {
    Write-Host "Basic Auth: DISABLED" -ForegroundColor Yellow
}

# Check FTP logging
```

```
$logging = Get-WebConfigurationProperty -Filter "/system.ftpServer/log" -PSPath "IIS:\Sites\$siteName" -Name "logExtFile
if ($logging) {
    Write-Host "Logging Enabled: YES" -ForegroundColor Green
} else {
    Write-Host "Logging Enabled: NO" -ForegroundColor Red
}

Write-Host "`n=== Audit Complete ===" -ForegroundColor Cyan
```

---

## Example Names and Placeholders Used in This Guide

Throughout this guide, you'll need to replace example names with your actual values:

| Example Used | What to Replace With |
|---|---|
| `domain.local` | YOUR actual domain name (e.g., `contoso.com`, `company.local`) |
| `FTPSERVER01` | YOUR actual FTP server hostname |
| `10.0.0.100` | YOUR FTP server's IP address |
| `C:\FTPRoot` | YOUR actual FTP root directory path |
| `192.168.1.0/24` | YOUR actual internal network range |
| `FTP Users` | YOUR AD group name for FTP access |
| `Domain Admins` | Standard AD group (usually doesn't need changing) |
| `jsmith`, `mjones` | YOUR actual usernames |
| `domain\ftp_service` | YOUR AD service account (format: domain\username) |
| `Secure FTP Site` | YOUR FTP site name in IIS |
| `50000-50100` | YOUR passive port range (can customize) |
| `FTPSVC1` | IIS automatically assigns this (FTPSVC + site number) |

---

## Additional Resources

- **Microsoft IIS FTP Documentation**: https://docs.microsoft.com/iis/publish/using-the-ftp-service/
- **FTP over SSL (FTPS) Guide**: https://docs.microsoft.com/iis/publish/using-the-ftp-service/using-ftp-over-ssl
- **Configuring FTP User Isolation**: https://docs.microsoft.com/iis/publish/using-the-ftp-service/config