



DKIM Configuration Guide

Complete Implementation Guide for Email Authentication



GFI Software™

Table of Contents

- 1 Introduction: DKIM in GFI GFI MailEssentials AI
- 2 Prerequisites & System Requirements
- 3 Understanding GFI MailEssentials AI DKIM Implementation
- 4 Configuration Method 1: Windows Certificate Store
- 5 Configuration Method 2: PEM Key File
- 6 GFI MailEssentials AI Domain Configuration
- 7 DNS Setup for GFI MailEssentials AI DKIM
- 8 Testing Your GFI MailEssentials AI DKIM Setup
- 9 Managing DKIM in GFI MailEssentials AI
- 10 Troubleshooting GFI MailEssentials AI DKIM Issues

Introduction: DKIM in GFI MailEssentials AI

GFI MailEssentials AI provides integrated DKIM (DomainKeys Identified Mail) signing capabilities for outgoing emails through its Email Security module. When properly configured, GFI MailEssentials AI will automatically sign all outbound messages from your specified domains, improving email deliverability and protecting your organization's email reputation.

Prerequisites & System Requirements

Before configuring DKIM in GFI MailEssentials AI, ensure you have:

GFI MailEssentials AI Requirements:

- ✓ GFI MailEssentials AI installed and operational
- ✓ Administrative access to the GFI MailEssentials AI server
- ✓ GFI MailEssentials AI EmailSecurity module enabled

Infrastructure Requirements:

- ✓ Administrative access to your domain's DNS settings
- ✓ Windows Server with PowerShell (for certificate method)
- ✓ OpenSSL access (for PEM key method - can use WSL on Windows)

Important: GFI MailEssentials AI requires the DNS selector to be set to "default".

Understanding GFI MailEssentials AI DKIM Implementation

GFI MailEssentials AI DKIM Flow:



Supported Key Sources:

- 1 **Windows Certificate Store:** GFI MailEssentials AI reads from the local machine certificate store
- 2 **Imported PEM Key:** GFI MailEssentials AI imports and stores the private key internally

Configuration Method 1: Windows Certificate Store

This method integrates with Windows' native certificate infrastructure, making it ideal for Windows-centric environments where GFI MailEssentials AI is deployed.

1 Generate Certificate for GFI MailEssentials AI

Run PowerShell as Administrator on your GFI MailEssentials AI server:

```
powershell

# Configure variables for your GFI MailEssentials AI domain

$Domain = "yourdomain.com"

$Subject = "CN=DKIM $Domain"

$ValidYears = 2

$PfxPath = "$env:USERPROFILE\Desktop\mailessentials-dkim-$Domain.pfx"

# Prompt for PFX password (required for GFI MailEssentials AI import)

$PfxPassword = Read-Host -AsSecureString "Enter PFX password for MailEssentials
certificate"

# Create certificate compatible with GFI MailEssentials AI requirements

$cert = New-SelfSignedCertificate `
    -Subject $Subject `
    -Type Custom `
    -CertStoreLocation "Cert:\CurrentUser\My" `
    -KeyAlgorithm RSA `
    -KeyLength 2048 `
    -HashAlgorithm SHA256 `
    -Provider "Microsoft Enhanced Cryptographic Provider v1.0"
    -KeySpec Signature
```

```

-KeyExportPolicy Exportable `
-KeyUsage DigitalSignature `
-KeyUsageProperty Sign `
-NotAfter (Get-Date).AddYears($ValidYears)

# Verify certificate meets GFI MailEssentials AI requirements

Write-Host "Certificate created for MailEssentials:"

Write-Host "Thumbprint: $($cert.Thumbprint)"

Write-Host "Provider: $($cert.PrivateKey.CspKeyContainerInfo.ProviderName)"

Write-Host "Key Size: $($cert.PublicKey.Key.KeySize) bits"

Write-Host "Exportable: $($cert.PrivateKey.CspKeyContainerInfo.Exportable)"

```

2 Install Certificate for GFI MailEssentials AI Access

powershell

```

# Export certificate for GFI MailEssentials AI

Export-PfxCertificate `

    -Cert $cert.PSPath `

    -FilePath $PfxPath `

    -Password $PfxPassword `

    -ChainOption BuildChain | Out-Null

Write-Host "Exported certificate to: $PfxPath"

# Import to LocalMachine store where GFI MailEssentials AI can access it

$Imported = Import-PfxCertificate `

    -FilePath $PfxPath `

    -CertStoreLocation "Cert:\LocalMachine\My"

    -Password $PfxPassword

    -Exportable

```

```
Write-Host "Certificate imported to LocalMachine store for MailEssentials access"

Write-Host "Thumbprint in LocalMachine\My: $($imported.Thumbprint)"

# Clean up user store (optional)

Remove-Item -Path $cert.PSPath -Force

Write-Host "Original certificate removed from user store"
```

3 Verify Certificate for GFI MailEssentials AI

Open `certlm.msc` and navigate to **Personal** → **Certificates**. Confirm your certificate shows:

- **Intended Purpose:** Digital Signature
- **Status:** Valid
- **Private Key:** Yes, and exportable

Configuration Method 2: PEM Key File

This method creates a PEM-formatted private key that GFI MailEssentials AI will import and manage internally.

1 Generate PEM Key for GFI MailEssentials AI

Choose either PKCS#1 (traditional) or PKCS#8 (modern) format - both work with GFI MailEssentials AI:

```
bash

# Generate 2048-bit RSA private key for GFI MailEssentials AI

openssl genrsa -out mailessentials-dkim-private.pem 2048

# Extract public key for DNS configuration

openssl rsa -in mailessentials-dkim-private.pem -pubout -out mailessentials-dkim-public.pem
```

```
# Secure the files
```

```
chmod 600 mailessentials-dkim-private.pem mailessentials-dkim-public.pem
```

Option B: PKCS#8 Format (Modern)

```
bash
```

```
# Generate 2048-bit RSA private key for GFI MailEssentials AI
```

```
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out mailessentials-  
dkim-private.pem
```

```
# Extract public key for DNS configuration
```

```
openssl pkey -in mailessentials-dkim-private.pem -pubout -out mailessentials-dkim-  
public.pem
```

```
# Secure the files
```

```
chmod 600 mailessentials-dkim-private.pem mailessentials-dkim-public.pem
```

2 Validate PEM Key for GFI MailEssentials AI

Choose either PKCS#1 (traditional) or PKCS#8 (modern) format - both work with GFI MailEssentials AI:

```
bash
```

```
# Verify private key is valid for GFI MailEssentials AI import
```

```
openssl pkey -in mailessentials-dkim-private.pem -check -noout
```

```
echo "✓ Private key validation: $?"
```

```
# Verify public key extraction
```

```
openssl pkey -pubin -in mailessentials-dkim-public.pem -text -noout | head -5
```

```
echo "✓ Public key extracted successfully"
```

GFI MailEssentials AI Domain Configuration

1 Access GFI MailEssentials AI DKIM Settings

Open GFI MailEssentials AI Administration Interface

- Navigate to your GFI MailEssentials AI web interface
- Log in with administrative credentials

Navigate to Email Security

- Click **Email Security** in the main navigation menu
- Select **Outgoing Emails** from the submenu

Select Domain for DKIM Configuration

- From the domain list, click on the domain you want to configure with DKIM
- This domain must already be configured in GFI MailEssentials AI

2 Configure Email Headers in GFI MailEssentials AI

In the "Email Headers for DKIM Signing" section:

- Review the selected headers (all headers are selected by default)
- **Recommendation:** Keep all headers selected for maximum security
- GFI MailEssentials AI will sign these headers to prevent tampering

3 Configure Signing Key in GFI MailEssentials AI

For Windows Certificate Store Method:

- In the "Signing Key Information" section
- Set **Source** dropdown to "Windows Certificate Store"
- Click "Browse Certificate"
- Select your certificate from the list (only valid certificates appear)
- If your certificate doesn't appear, verify it's in LocalMachine\My and exportable

For PEM Key Method:

- In the "**Signing Key Information**" section
- Set **Source** dropdown to "**Imported Key**"
- Click "**Choose File**"
- Navigate to your `mailessentials-dkim-private.pem` file
- Click "**Import**"
- GFI MailEssentials AI will validate and import the key

4 Apply and Enable DKIM in GFI MailEssentials AI

Save Configuration

- Scroll to the top of the page
- Click "**Apply**" to save your DKIM configuration
- GFI MailEssentials AI will return you to the domain list

Enable DKIM for Domain

- Locate your configured domain in the list
- Check the checkbox next to the domain
- Click "**Enable Selected**"
- GFI MailEssentials AI will now sign outgoing emails from this domain

DNS Setup for GFI MailEssentials AI DKIM

1 Extract Public Key for DNS

From Windows Certificate:

powershell

```
# Get the certificate GFI MailEssentials AI is using

$thumbprint = "YOUR_CERTIFICATE_THUMBPRINT"

$cert = Get-Item "Cert:\LocalMachine\My\$thumbprint"

# Extract public key in format needed for DNS

$publicKeyBytes = $cert.PublicKey.EncodedKeyValue.RawData

$publicKeyBase64 = [Convert]::ToBase64String($publicKeyBytes)

# Format for DNS (remove line breaks)

$dnsPublicKey = $publicKeyBase64 -replace "`r`n", ""

Write-Host "Public key for DNS TXT record:"

Write-Host $dnsPublicKey
```

From PEM File:

bash

```
# Extract base64 public key string for DNS

grep -v '^-----' mailessentials-dkim-public.pem | tr -d '
' > dns-public-key.txt

cat dns-public-key.txt
```

2 Create DNS TXT Record for GFI MailEssentials AI

Critical Requirement: GFI MailEssentials AI requires the selector to be "default"

DNS Record Configuration:

- Host/Name: `default._domainkey.yourdomain.com`
- Type: `TXT`
- Value: `v=DKIM1; k=rsa; p=YOUR_PUBLIC_KEY_STRING_HERE`
- TTL: 300-3600 seconds

Example DNS Record:

Host: `default._domainkey.example.com` Type: `TXT` Value: `v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEA...` TTL: 3600

3 Validate DNS Configuration

bash

```
# Test DNS propagation for GFI MailEssentials AI DKIM
```

```
dig TXT default._domainkey.yourdomain.com
```

```
# Alternative using nslookup
```

```
nslookup -type=txt default._domainkey.yourdomain.com
```

Expected Response:

```
default._domainkey.yourdomain.com. 3600 IN TXT "v=DKIM1; k=rsa; p=MIIBIjAN..."
```

Testing Your GFI MailEssentials AI DKIM Setup

1 Send Test Email Through GFI MailEssentials AI

Send from Configured Domain

- Send an email from the domain configured in GFI MailEssentials AI
- Send to an external email service (Gmail, Outlook.com, etc.)
- Ensure the email routes through your GFI MailEssentials AI server

2 Verify GFI MailEssentials AI DKIM Signature

Check Email Headers: Look for the DKIM signature added by GFI MailEssentials AI:

```
DKIM-Signature: v=1; a=rsa-sha256; d=yourdomain.com; s=default;  
c=relaxed/relaxed; q=dns/txt; t=1234567890;  
h=from:to:subject:date:message-id; bh=hash_of_body;  
b=signature_hash
```

Verify Authentication Results:

```
Authentication-Results: mx.example.com; dkim=pass header.d=yourdomain.com  
header.s=default
```

3 Use Online DKIM Validators

Recommended Testing Tools:

- **Mail-Tester:** <https://www.mail-tester.com/>
- **DKIM Validator:** <https://dkimvalidator.com/>
- **MXToolbox DKIM Lookup:** <https://mxtoolbox.com/dkim.aspx>

Testing Process:

- Send email to the testing service's address
- Check the DKIM authentication status
- Verify your domain shows **dkim=pass**

Managing DKIM in GFI MailEssentials AI

1 Access GFI MailEssentials AI DKIM Settings

Enable/Disable DKIM for Domains

To Disable DKIM:

- Navigate to **EmailSecurity** → **Outgoing Emails**
- Check the domain(s) you want to disable
- Click "**Disable Selected**"
- GFI MailEssentials AI will stop signing emails from these domains

To Re-enable DKIM:

- Check the previously configured domain(s)
- Click "**Enable Selected**"
- GFI MailEssentials AI will resume signing emails

2 Update DKIM Configuration in GFI MailEssentials AI

To Modify Headers or Keys:

- Click on the domain name in the list
- Make your changes to headers or signing key
- Click "**Apply**"
- The domain remains enabled with new settings

3 Managing Multiple Domains in GFI MailEssentials AI

GFI MailEssentials AI supports DKIM for multiple domains:

- Each domain can have its own DKIM configuration
- Each domain can use different certificates/keys
- All domains must use the "default" selector
- Enable/disable domains independently

Troubleshooting GFI MailEssentials AI DKIM Issues

1 GFI MailEssentials AI Certificate Issues

Problem	Cause	Solution
Certificate not visible in GFI MailEssentials AI browser	Certificate not in LocalMachine\My store	Re-import certificate to <code>Cert:\LocalMachine\My</code>
"Certificate not valid" error	Certificate not exportable	Recreate certificate with - <code>KeyExportPolicy Exportable</code>
Certificate appears but fails to save	Incorrect key usage	Ensure certificate has <code>DigitalSignature</code> key usage

Verification Commands:

```
powershell

# Check certificate in GFI MailEssentials AI store location

Get-ChildItem "Cert:\LocalMachine\My" | Where-Object {$_.Subject -like "*DKIM*"}

# Verify certificate properties for GFI MailEssentials AI

$cert = Get-Item "Cert:\LocalMachine\My\THUMBPRINT"

$cert.PrivateKey.CspKeyContainerInfo.Exportable # Should be True
```

2 GFI MailEssentials AI PEM Import Issues

Problem	Cause	Solution
"Invalid key format" in GFI MailEssentials AI	Encrypted or wrong format PEM	Generate unencrypted PKCS#1 or PKCS#8 key
Import succeeds but signing fails	Key size unsupported	Ensure key is exactly 2048 or 4096 bits
"File not found" error	Path issues	Use full path to PEM file

PEM Validation for GFI MailEssentials AI:

```
bash

# Verify key format before GFI MailEssentials AI import

openssl pkey -in mailessentials-dkim-private.pem -text -noout | grep "Private-Key"

# Should show: Private-Key: (2048 bit) or (4096 bit)


# Check if key is encrypted (GFI MailEssentials AI requires unencrypted)

head -2 mailessentials-dkim-private.pem

# Should NOT contain "ENCRYPTED" in header
```

3 GFI MailEssentials AI DKIM Signing Not Working

Issue	Check	Fix
No DKIM-Signature header	Domain not enabled	Enable domain in GFI MailEssentials AI
DKIM signature present but validation fails	DNS record mismatch	Verify public key in DNS matches private key
Multiple DKIM signatures	Upstream server also signing	Disable DKIM on upstream or use different selector (not supported)

GFI MailEssentials AI Diagnostic Steps:

- Check GFI MailEssentials AI logs for DKIM-related errors
- Verify domain is enabled: **EmailSecurity** → **Outgoing Emails**
- Test with simple text email to eliminate formatting issues
- Confirm email is routing through GFI MailEssentials AI server

4 DNS-Related Issues

Common DNS Problems:

bash

```
# Check if DNS record exists for GFI MailEssentials AI selector
```

```
nslookup -type=txt default._domainkey.yourdomain.com
```

```
# Verify DNS propagation globally
```

```
# Use online tools like whatsmydns.net
```

```
# Test DKIM record parsing
```

```
# Use mxtoolbox.com/dkim.aspx
```

DNS Troubleshooting:

- Ensure selector is exactly "default" (case-insensitive)
- Verify no spaces in public key string
- Check TTL allows reasonable propagation time
- Confirm DNS provider supports long TXT records

Quick Reference

Essential MailEssentials DKIM Settings

- Selector: **default** (mandatory)
- Key Size: 2048 or 4096 bits
- DNS Record: **default._domainkey.yourdomain.com**
- MailEssentials Path: EmailSecurity → Outgoing Emails

powershell

```
# Certificate check for MailEssentials
```

```
Get-ChildItem "Cert:\LocalMachine\My" | Where-Object {$_.HasPrivateKey -eq $true}
```

bash

```
# PEM key validation for MailEssentials
```

```
openssl pkey -in mailessentials-dkim-private.pem -check -noout
```

bash

```
# DNS verification for MailEssentials DKIM
```

```
dig TXT default._domainkey.yourdomain.com
```

End of Guide

This comprehensive guide provides everything needed to successfully implement and maintain DKIM signing in GFI MailEssentials. For additional support, consult the MailEssentials administration documentation or contact GFI support.