GUIDE

DKIM Validation in GFI KerioConnect AI:
A Quick Guide

GFI Software™

Overview

DKIM (DomainKeys Identified Mail) is an email security standard that verifies if emails from a domain are authorized and unaltered. GFI KerioConnect AI supports DKIM validation for incoming emails, helping to reject unauthorized or harmful messages by checking the DKIM signature in the email's header.

Enabling DKIM Validation in GFI KerioConnect AI

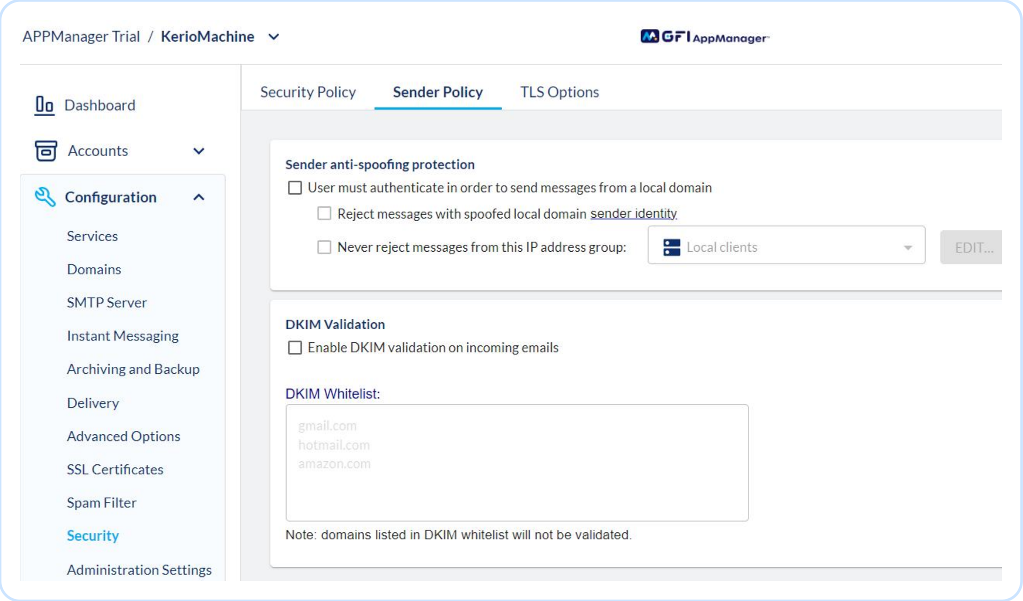
There are two ways to enable DKIM validation in GFI KerioConnect AI (which is by default off).

1. Via configuration changes in mailserver.cfg by editing the following variables:

```
<variable name="EnableDKIMValidation">1</variable>
<variable name="DKIMDomainWhiteList">gmail.com,hotmail.com</variable>
```

- Set '**EnableDKIMValidation**' to 1 to enable validation for all incoming emails. (*You can configure DKIM for your domains in GFI KerioConnect AI; more information is available here.*)
- Use '**DKIMDomainWhiteList**' to whitelist trusted domains (e.g., gmail.com, hotmail.com) to ensure their emails are not rejected, even without a DKIM signature, by listing them in a comma-separated format.

2. Enable DKIM Validation via GFI AppManager AI. You can find the DKIM validation settings in AppManager under *Configuration > Security > Sender Policy*



Sender anti-spoofing protection

□ User must authenticate in order to send messages from a local domain

□ Reject messages with spoofed local domain sender identity

□ Never reject messages from this IP address group: Local clients

DKIM Validation

□ Enable DKIM validation on incoming emails

DKIM Whitelist:

gmail.com
hotmail.com
amazon.com

Note: domains listed in DKIM whitelist will not be validated.

Note: available from GFI KerioConnect AI 10.0.6 (build 8452).

What Happens If Sender's Domain Lacks DKIM?

If a sender's domain does not have DKIM, the email will be rejected during the SMTP handshake. GFI KerioConnect AI checks DKIM during the handshake, and emails lacking valid signatures will fail to connect and will not be received (Whitelist known domains without DKIM).

Monitoring DKIM

If senders' emails fail you can verify from Debug and Security logs in GFI KerioConnect AI, if they are DKIM related in:

Debug Logs:

```
`SMTP: Message from IP address %s was rejected due to missing authentication. Sign the email with DKIM headers <%s>.`

`Command DATA failed: Authentication required for domain sender <%s>. DKIM header check failed.`
```

Security Logs:

```
`SMTP: Message from IP address %s rejected. DKIM header missing or invalid.`

`DKIM header check failed for domain sender <%s>.`
```

Sender:

In addition, the sender will receive the below message when DKIM validation fails.

```
`550 5.7.1 Authentication Required`
```

Important Note: Many domains still do not support DKIM, so monitor email traffic closely after enabling DKIM validation to avoid disruptions. Use whitelisting for trusted domains.