LEITFADEN

DKIM-Validierung in GFI KerioConnect AI:

Ein schneller Leitfaden

GFI Software™

Übersicht

DKIM (DomainKeys Identified Mail) ist ein E-Mail-Sicherheitsstandard, der überprüft, ob E-Mails von einer Domain autorisiert und unverändert sind. GFI KerioConnect AI unterstützt die DKIM-Validierung für eingehende E-Mails, um unautorisierte oder schädliche Nachrichten abzulehnen, indem die DKIM-Signatur im Header der E-Mail überprüft wird.

Aktivierung der DKIM-Validierung in GFI KerioConnect AI

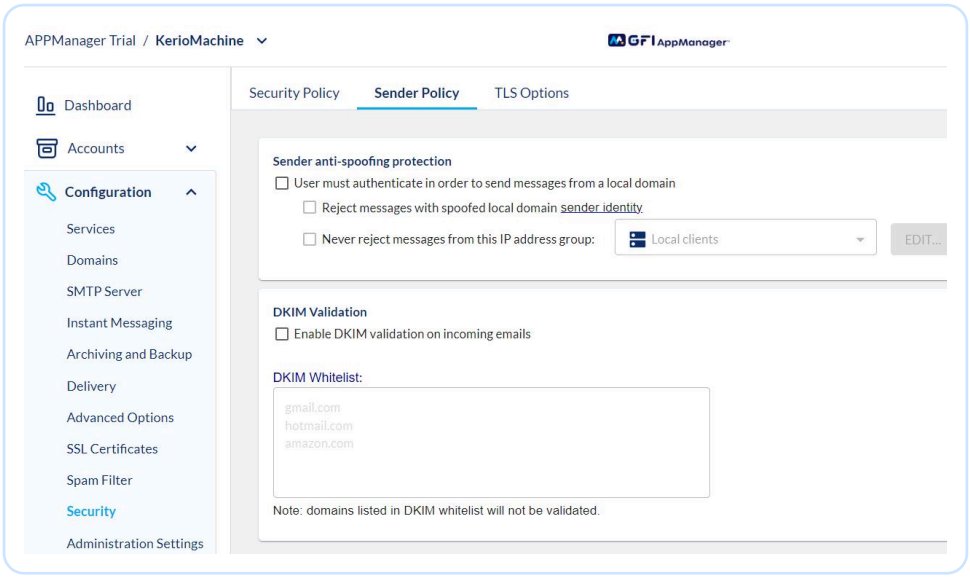
Es gibt zwei Möglichkeiten, die DKIM-Validierung in GFI KerioConnect AI zu aktivieren (standardmäßig ist sie deaktiviert).

1. Durch Konfigurationsänderungen in mailserver.cfg, indem die folgenden Variablen bearbeitet werden:

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

   - Setzen Sie ‚**EnableDKIMValidation**' auf 1, um die Validierung für alle eingehenden E-Mails zu aktivieren. (Sie können DKIM für Ihre Domains in GFI KerioConnect AI konfigurieren; weitere Informationen sind hier verfügbar.)
   - Verwenden Sie ‚**DKIMDomainWhiteList**', um vertrauenswürdige Domains (z.B. gmail.com, hotmail.com) auf die Whitelist zu setzen, um sicherzustellen, dass deren E-Mails nicht abgelehnt werden, selbst ohne DKIM-Signatur, indem Sie sie in einem durch Kommas getrennten Format auflisten.

2. Aktivieren Sie die DKIM-Validierung über GFI AppManager AI. Sie finden die DKIM-Validierungseinstellungen im AppManager unter Konfiguration > Sicherheit > Absenderrichtlinie.



Hinweis: verfügbar ab KerioConnect 10.0.6 (Build 8452).

Was passiert, wenn die Domain des Absenders DKIM nicht hat?

Wenn die Domain eines Absenders kein DKIM hat, wird die E-Mail während des SMTP-Handshakes abgelehnt. KerioConnect überprüft DKIM während des Handshakes, und E-Mails ohne gültige Signaturen können sich nicht verbinden und werden nicht empfangen (Whitelist bekannte Domains ohne DKIM).

Überwachung von DKIM

Wenn E-Mails von Absendern fehlschlagen, können Sie in den Debug- und Sicherheitsprotokollen in GFI KerioConnect überprüfen, ob sie DKIM-bezogen sind:

Debug-Protokolle:

```
`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.`
```

Sicherheitsprotokolle:

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

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

Sender:

Darüber hinaus erhält der Absender die folgende Nachricht, wenn die DKIM-Validierung fehlschlägt.

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

Wichtiger Hinweis: Viele Domains unterstützen immer noch kein DKIM, daher sollten Sie den E-Mail-Verkehr nach der Aktivierung der DKIM-Validierung genau überwachen, um Unterbrechungen zu vermeiden. Verwenden Sie Whitelisting für vertrauenswürdige Domains.