

ESA - 替换现有的DKIM键没有停工期

Contents

[Introduction](#)

[Requirements](#)

[创建一个新的DKIM签署的键](#)

[生成一个新的DKIM签署的配置文件并且发布DNS记录到DNS](#)

[删除老签署的配置文件并且从新的签署的配置文件去除占位符用户](#)

[测试邮件流量确认DKIM通行证](#)

Introduction

本文描述如何替换在一个ESA和DKIM公共密钥的现有的DKIM签署的键在DNS没有停工期。

Requirements

1. 对电子邮件安全工具(ESA)的访问。
2. 对添加的DNS的访问/删除TXT记录。
3. ESA一定已经签署与DKIM配置文件的消息。

创建新的DKIM签署的键

您首先将需要创建在ESA的一个新的DKIM签署的键：

1. 去邮件策略>签署的键并且选择"Add Key..."
2. 给出DKIM键，并且请生成一把新的专用密钥或粘贴在一现有的一个。 **Note:**在许多情况下，它建议您选择2048位专用密钥大小。
3. 确认更改。

Note:此更改不会影响签字的DKIM或邮件流量。我们就是添加一个DKIM签署的键和不适用它于任何DKIM签署的配置文件。

生成新的DKIM签署的配置文件并且发布DNS记录到DNS

其次，您将需要创建一个新的DKIM签署的配置文件，生成从那的一个DKIM DNS记录DKIM签署的配置文件并且发布该记录到DNS：

1. 去邮件策略>签署的配置文件并且点击"Add Profile..." 产生配置文件在字段“配置文件名字的一描述性名称”。输入您的域在字段“域名”。输入一个新的选择器字符串字段“选择器”。
Note:选择器是使用允许一个特定域的多个DKIM DNS记录的一个任意字符串。我们使用选择器允许超过在DNS的一个DKIM DNS记录您的域的。使用是与已经现有的DKIM签署的配置文件不同的新的选择器是重要的。
选择在字段“签署的键的前面的部分创建的DKIM签署的键”。在签署的配置文件的底部，请添加一个新的“用户”。此用户应该是一个unused占位符电子邮件地址。 **警告：**重要的是您添加一

个未使用的电子邮件地址作为此签署的配置文件的一个用户。否则，在发布造成DKIM验证的DKIM TXT记录发生故障前，此配置文件可能签署出局的消息。添加一个未使用的电子邮件地址作为用户保证此签署的配置文件不签署任何出局的消息。单击 **submit**。

2. 从这里，请点击"Generate"在列"DNS发短信给记录"您创建的签署的配置文件的并且复制生成的DNS记录。它应该看起来类似于以下：

```
selector2._domainkey.example.com. IN TXT "v=DKIM1;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMax6wMAk4iQoLNwiEkj0BrIRMDHXQ77430QUOYZQqEXS
s+ jMGomOknAZJp jR8TwmYHVPbD+30QRw0qEiRY3hYcmKOCWZ/hTo+NQ8qjlCSc1LTMDv0HWAi2AGsVOT8BdFHkxg40
oyGWgktzclq7zIgwM8usHfKVWFzYgnattNzyEqHsfI7lG1lz5gdHBOvmF8LrDSfN"
"KtGrTtvIxJM8pWeJm6pg6TM/cy0FypS2azkrl9riJcWWDvu38JXFL/eeYjGnB1zQeR5Pnbc3sVJd3cGaWx1bWjepyN
QZ1PrS6Zwr7ZxSRa316Oxc36uCid5JAq0z+IcH4KkHqUueSGuGhwIDAQAB;"
```

3. 确认更改。
4. 提交DKIM DNS TXT记录在第2步给DNS。
5. 请等待，直到充分地传播了DKIM DNS TXT记录。

删除老签署的配置文件并且从新的签署的配置文件去除占位符用户

一旦DKIM TXT记录被提交了给DNS，并且保证传播了，下一步将是删除老签署的配置文件和从新的签署的配置文件去除占位符用户：

Note: 我们极力推荐您在继续进行备份ESA配置文件以下步骤前。这是因为，如果删除老DKIM签署的配置文件，并且有需要恢复回到早先配置，您能容易地装载备份的配置文件。

1. 去邮件策略>签署的配置文件，选择老DKIM签署的配置文件并且点击"Delete."
2. 进入新的DKIM签署的配置文件，选择当前占位符用户并且点击"Remove."
3. 点击"Submit."
4. 在列下"请测试配置文件"为新的DKIM签署的配置文件点击"Test"。如果测试是成功的，请继续对下一步。否则，请确认充分地传播了DKIM DNS TXT记录。
5. 确认做的变动。

测试邮件流量确认DKIM通行证

这时，您用其中任一进一步配置DKIM完成。然而，您应该测试DKIM签字保证签署您的出局的消息正如所料并且通过DKIM验证：

1. 通过ESA传送信息保证获得另一台主机验证的DKIM签字由ESA和DKIM。
2. 一旦消息在另一端收到，请检查消息的报头报头"认证结果"。寻找报头的DKIM部分确认是否通过了DKIM验证。报头应该看起来类似于以下：

```
Authentication-Results: mx1.example.net; spf=SoftFail smtp.mailfrom=user1@example.net;
dkim=pass header.i=none; dmarc=fail (p=none dis=none) d=example.net
```

3. 寻找报头"DKIM签名"并且确认使用正确的选择器和域：

```
DKIM-Signature: a=rsa-sha256; d=example.net; s=selector2;
c=simple; q=dns/txt; i=@example.net;
t=1117574938; x=1118006938;
h=from:to:subject:date;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
b=dzdVYOfAKCdLXdJ0c9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
VoG4ZHRNiYzR
```

4. 一旦是满足的DKIM工作按照计划，请等待至少一周期前删除老DKIM TXT记录。这保证老DKIM键签字的所有消息被处理了。