

ESA - Remplacez la clé existante DKIM sans le temps d'arrêt

Contenu

[Introduction](#)

[Conditions requises](#)

[Créez une nouvelle clé de signature DKIM](#)

[Générez un nouveau profil de signature DKIM et éditez l'enregistrement DNS aux DN](#)

[Supprimez le vieux profil de signature et retirez l'utilisateur de texte d'attente du nouveau profil de signature](#)

[Flux de courrier de test pour confirmer des passages DKIM](#)

Introduction

Ce document décrit comment remplacer la clé de signature existante DKIM sur une clé publique ESA et DKIM dans des DN sans le temps d'arrêt.

Exigences

1. Accès à l'appliance de sécurité du courrier électronique (ESA).
2. Accès aux DN à ajouter/retirent des enregistrements TXT.
3. L'ESA doit déjà signer des messages avec un profil DKIM.

Créez une nouvelle clé de signature DKIM

Vous le premier besoin de créer une nouvelle clé de signature DKIM sur l'ESA :

1. Allez aux stratégies de messagerie > des clés de signature et sélectionnez « ajoutent la clé... »
2. Nommez la clé DKIM et générez une nouvelle clé privée ou la collez dans existante. **Note:** *Dans la plupart des cas, il a recommandé que vous choisissiez une taille de clé privée de 2048 bits.*
3. Commettez les modifications.
Note: Cette modification n'affectera pas DKIM signant ou flux de courrier. Nous juste ajoutons une clé de signature DKIM et ne nous appliquons pas l'à n'importe quel profil de signature DKIM encore.

Générez un nouveau profil de signature DKIM et éditez l'enregistrement DNS aux DN

Ensuite, vous devrez créer un nouveau profil de signature DKIM, générez un enregistrement DNS DKIM de cela profil de signature DKIM et éditez cet enregistrement aux DN :

1. Allez aux stratégies de messagerie > des profils de signature et le clic « ajoutent le profil... »
Donnez au profil un nom descriptif dans le domaine « nom de profil. » Entrez dans votre domaine dans le domaine « nom de domaine. » Écrivez une nouvelle chaîne de sélecteur dans le champ « sélecteur. »

Note: *Le sélecteur est une chaîne arbitraire qui est utilisée pour permettre de plusieurs enregistrements DNS DKIM pour un domaine donné. Nous allons utiliser le sélecteur pour permettre plus d'un enregistrement DNS DKIM dans des DN pour votre domaine. Il est important d'utiliser un nouveau sélecteur qui est différent du profil de signature déjà existant DKIM.*

Sélectionnez la clé de signature DKIM créée dans la section précédente dans le domaine « clé de signature. » Très à l'inférieur du profil de signature, ajoutez un nouvel « utilisateur. » Cet utilisateur devrait être une adresse e-mail unused de texte d'attente. **Attention :** *Il est important que vous ajoutiez une adresse e-mail inutilisée en tant qu'utilisateur pour ce profil de signature. Autrement, ce profil peut signer les messages sortants avant que l'enregistrement DKIM TXT soit édité faisant échouer la vérification DKIM. Ajouter une adresse e-mail inutilisée en tant qu'utilisateur s'assure que ce profil de signature ne signe aucun message sortant.* Cliquez sur **Submit**.

2. D'ici, le clic « se produisent » dans la colonne « DN textotent l'enregistrement » pour le profil de signature que vous avez juste créé et copient l'enregistrement DNS qui est généré. Il devrait sembler semblable à ce qui suit :

```
selector2._domainkey.example.com. IN TXT "v=DKIM1;  
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAWMaX6wMAk4iQoLNWiEkj0BrIRMDHXQ7743OQUOYZQqEXS  
s+jMGomOknAZJpjR8TwmYHVPbD+30QRw0qEiRY3hYcmKOCWZ/hTo+NQ8qj1CSc1LTmdV0HWAi2AGsVOT8BdFHkyxg40  
oyGWgktzclq7zIgwM8usHfKVVfzYgnattNzyEqHsfI7lGillz5gdHBOvmF8LrDSfN"  
"KtGrTtvIxJM8pWeJm6pg6TM/cy0FypS2azkr19riJcWWDvu38JXFL/eeYjGnB1zQeR5Pnbc3sVJd3cGaWx1bWjepyN  
QZ1PrS6Zwr7ZxSRa316Oxc36uCid5JAq0z+IcH4KkHqUueSGuGhwIDAQAB; "
```

3. Commettez les modifications.
4. Soumettez l'enregistrement des DN TXT DKIM dans l'étape 2 aux DN.
5. Attendez jusqu'à ce que l'enregistrement des DN TXT DKIM ait été entièrement propagé.

Supprimez le vieux profil de signature et retirez l'utilisateur de texte d'attente du nouveau profil de signature

Une fois que l'enregistrement DKIM TXT a été soumis aux DN et vous vous assurez qu'il a été propagé, l'étape suivante sera de supprimer le vieux profil de signature et de retirer l'utilisateur de texte d'attente du nouveau profil de signature :

Note: *On le recommande fortement que vous sauvegarde le fichier de configuration ESA avant de commencer avec les étapes suivantes. C'est parce que si vous supprimez le vieux profil de signature DKIM et il y a un besoin de revenir à la configuration précédente, vous pourrez charger facilement le fichier de configuration sauvegardé.*

1. Allez aux stratégies de messagerie > des profils de signature, sélectionnez le vieux profil de signature DKIM et cliquez sur le « effacement. »
2. Entrez dans le nouveau profil de signature DKIM, sélectionnez l'utilisateur en cours de texte d'attente et le clic « retirent. »
3. Le clic « soumettent. »

4. Sous le clic « de « profil de test » de colonne déterminez » le nouveau profil de signature DKIM. Si le test est réussi, continuez à l'étape suivante. Sinon, confirmez que l'enregistrement des DN TXT DKIM a été entièrement propagé.
5. Commettez les modifications apportées.

Flux de courrier de test pour confirmer des passages DKIM

En ce moment, vous êtes fait avec configurer DKIM pas plus. Cependant, vous devriez tester DKIM signant pour s'assurer qu'il signe vos messages sortants comme prévu et passe la vérification DKIM :

1. Envoyez un message par l'ESA en s'assurant qu'il obtient DKIM signé par l'ESA et DKIM vérifié par un autre hôte.
2. Une fois que le message est reçu sur l'autre extrémité, vérifiez les en-têtes du message pour l'en-tête « Authentification-résultats. » Recherchez la section DKIM de l'en-tête pour confirmer si elle passait la vérification DKIM ou pas. L'en-tête devrait sembler semblable à ce qui suit :

```
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. Recherchez l'en-tête « DKIM-signature » et la confirmez que le sélecteur et le domaine corrects sont utilisés :

```
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=dzdVyOfAKCdLXdJOc9G2q8LoXS1EniSbav+yuU4zGeeruD001szZ  
VoG4ZHRNiYzR
```

4. Une fois que vous êtes satisfait que DKIM fonctionne comme prévu, attendez au moins une semaine avant de retirer le vieil enregistrement DKIM TXT. Ceci s'assure que tous les messages signés par la vieille clé DKIM ont été traités.