

ESA - Vervang bestaande DKIM-toets zonder downtime

Inhoud

[Inleiding](#)

[Vereisten](#)

[Een nieuwe DKIM-signaalsleutel maken](#)

[genereert een nieuw DKIM-signaalprofiel en publiceert de DNS-record op DNS](#)

[Verwijdert het oude signaalprofiel en verwijdert de plaatsaanduiding gebruiker uit het nieuwe signaalprofiel](#)

[Test-mail flow om DKIM-passages te bevestigen](#)

Inleiding

In dit document wordt beschreven hoe de bestaande DKIM-signaaltoets op een ESA- en DKIM-openbare toets zonder downtime kan worden vervangen.

Vereisten

1. Toegang tot de e-mail security applicatie (ESR).
2. Toegang tot DNS om TXT-records toe te voegen of te verwijderen.
3. De ESA moet al berichten met een DKIM-profiel ondertekenen.

Een nieuwe DKIM-signaalsleutel maken

U moet eerst een nieuwe DKIM-gebarentaal op de ESA instellen:

1. Ga naar Mail Policy > Signing Keys en selecteer "Add Key..."
2. Geef de DKIM-toets een naam en genereer een nieuwe privé-toets of een bestaande.
Opmerking: *In de meeste gevallen is het aanbevolen om een 2048 bits private sleutelgrootte te kiezen.*
3. Breng de wijzigingen aan.
Opmerking: Deze wijziging heeft geen invloed op de gebaren of poststroom van DKIM. We voegen gewoon een DKIM-signaalsleutel toe en passen deze nog niet toe op een DKIM-signaalprofiel.

genereert een nieuw DKIM-signaalprofiel en publiceert de DNS-record op DNS

Daarna moet u een nieuw DKIM-signaalprofiel maken, een DKIM DNS-record uit dat DKIM-signaalprofiel genereren en dat record naar DNS publiceren:

1. Ga naar postbeleid > Signaleren profielen en klik op "Profiel toevoegen.." Geef het profiel een beschrijvende naam in het veld "Naam profiel". Typ uw domein in het veld "Domeinnaam". Voer een nieuwe selectietekens in in het veld "Selector."

Opmerking: *De selector is een arbitrair string die wordt gebruikt om meerdere DKIM DNS records voor een bepaald domein toe te staan. We gaan de selector gebruiken om meer dan één DKIM DNS record in DNS voor uw domein toe te staan. Het is belangrijk om een nieuwe selector te gebruiken die afwijkt van het reeds bestaande DKIM-signaalprofiel.*

Selecteer de DKIM-signaaltoets die in de vorige sectie is gemaakt in het veld "Signing Key." Voeg onder in het signaalprofiel een nieuwe "Gebruiker" toe. Deze gebruiker moet een niet-gebruikt, maar wel een e-mailadres zijn. **Voorzichtig:** *Het is belangrijk dat u een ongebruikt e-mailadres als gebruiker toevoegt voor dit signaalprofiel. Anders kan dit profiel uitgaande berichten ondertekenen voordat de DKIM TXT-record wordt gepubliceerd, waardoor de DKIM-verificatie kan mislukken. Wanneer u een ongebruikt e-mailadres als gebruiker toevoegt, zorgt dit signaalprofiel ervoor dat er geen uitgaande berichten worden verzonden.* Klik op Indienen.

2. Klik vanaf hier "Generate" in de kolom "DNS Tekst Record" voor het signaalprofiel dat u net hebt gemaakt en kopieer de DNS record die wordt gegenereerd. Het zou er ongeveer op moeten lijken:

```
selector2._domainkey.example.com. IN TXT "v=DKIM1;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAWaX6wMAk4iQoLNWiEkj0BrIRMDHXQ77430QUOYZQqEXS
s+jMGomOknAZJpjR8TwmYHVPbD+30QRw0qEiRY3hYcmKOCWZ/hTo+NQ8qj1CSc1LTmDv0HWAi2AGsVOT8BdFHkyxg40
oyGWgktzclq7zIqWM8usHfKVWFzYgnattNzyEqHsfI71GIlz5gdHBOvmF8LrDSfN"
"KtGrTtvIxJM8pWeJm6pg6TM/cy0FypS2azkr19riJcWWDvu38JXFL/eeYjGnB1zQeR5Pnbc3sVJd3cGaWx1bWjepyN
QZ1PrS6Zwr7ZxSRa3160xc36uCid5JAq0z+IcH4KkHqUueSGuGhwIDAQAB; "
```

3. Breng de wijzigingen aan.
4. dienen de DKIM DNS TXT-record in stap 2 in op DNS-indeling.
5. Wacht tot de DKIM DNS TXT-record volledig is verspreid.

Verwijdert het oude signaalprofiel en verwijder de plaatsaanduiding gebruiker uit het nieuwe signaalprofiel

Nadat de DKIM TXT-record is verzonden naar DNS-indeling en u er zeker van bent dat de record is verspreid, wordt de volgende stap uitgevoerd door het oude signaalprofiel te verwijderen en de plaatsaanduiding te verwijderen uit het nieuwe signaalprofiel:

Opmerking: *Het wordt ten zeerste aanbevolen een back-up te maken van het ESA configuratiebestand voordat u de volgende stappen doorgaat. Dit komt doordat als u het oude DKIM-signaalprofiel verwijdert en er een noodzaak is om terug te keren naar de vorige configuratie, dan kunt u het ondersteunde configuratiebestand eenvoudig laden.*

1. Ga naar Mail Policy > Signing Profiles, selecteer het oude DKIM signaalprofiel en klik op "Verwijderen".
2. Ga naar het nieuwe DKIM-signaalprofiel, selecteer de huidige plaatsaanduiding en klik op "Verwijderen."
3. Klik op "Inzenden".
4. Klik onder de kolom "Test Profile" op "Test" voor het nieuwe DKIM-signaalprofiel. Als de test succesvol is, ga verder met de volgende stap. Als dit niet het geval is, bevestig dan dat de

DKIM DNS TXT-record volledig is verspreid.

5. Voer de aangebrachte wijzigingen in.

Test-mail flow om DKIM-passages te bevestigen

Op dit punt kunt u DKIM verder configureren. U dient echter te testen of DKIM gebaren is om er zeker van te zijn dat het uw uitgaande berichten gebaart zoals verwacht en dat u DKIM-verificatie doorgeeft:

1. Stuur een bericht door de ESA, zodat de DKIM door de ESA en DKIM door een andere gastheer wordt gecontroleerd.
2. Nadat het bericht aan het andere einde is ontvangen, controleert u de kopregels van het bericht voor de kop "Verificatie-resultaten". Kijk in het DKIM gedeelte van de header om te bevestigen of de DKIM-verificatie is geslaagd. De header moet er als volgt uitzien:
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. Bekijk de kop "DKIM-Signature" en bevestig dat de juiste selector en het juiste domein worden gebruikt:

```
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=dzdVyOfAKCdLXdJ0c9G2q8LoXS1EniSbav+yuU4zGeeruD00lszZ  
VoG4ZHRNiYzR
```

4. Zodra u ervan overtuigd bent dat DKIM naar behoren werkt, wacht u minimaal een week voordat u de oude DKIM TXT-record verwijdert. Dit waarborgt dat alle berichten die door de oude DKIM-toets zijn ondertekend, zijn verwerkt.