MX-Relay

Outbound e-mail configuratie

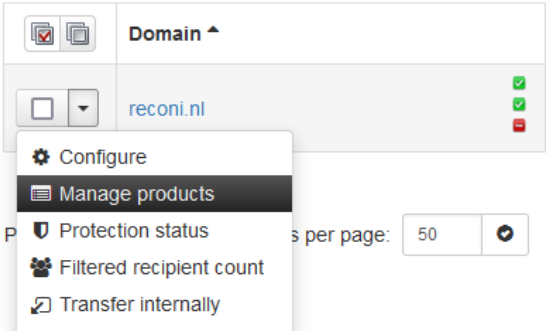
Inhoud

Inloggen

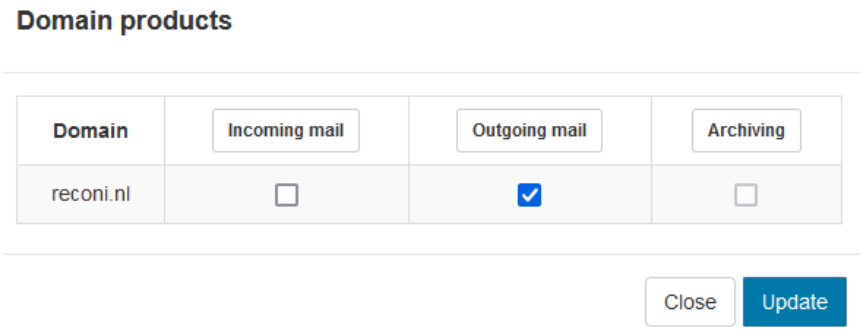
Inloggen op het nieuwe platform doe je op: https://login.mx-relay.com. Op de inlogpagina kan je tevens een password reset link verkrijgen, mocht je het wachtwoord kwijt zijn.

Domein toevoegen

1. Maak het domein aan en hou de instellingen op de default settings.
2. Zodra het domein is aangemaakt ga je terug naar het 'Overview', hier zoek je het domein op en kies je in het dropdown menu voor 'Manage products'.



3. Hier selecteer je vervolgens alleen 'Outgoing mail'.



4. Nu kan je verder met de configuratie van de uitgaande service.

Subadmin aanmaken

Je kan eventueel een subadmin aanmaken voor het nieuwe domein, mocht de klant ook in willen loggen:

1. Ga naar 'Users & Permissions' -> 'Manage domain users'.
2. Hier kan je het domein selecteren en de gebruiker gegevens invullen.
3. Klik op Save.

Configuratie (standaard mailserver)

Nu kan je voor de domeinen de Outgoing User en Authentication Method gaan configureren om de MTA vrij te geven voor uitgaande e-mail.

1. Ga naar 'Outgoing', -> 'Manage Users'.
2. Hier kan je vervolgens per User/Domain kiezen uit de volgende uitgaande methodes:
    a. Authenticating IP or range (uitgaande mail vrijgeven op basis van IP)
    b. Authenticating User (uitgaande mail vrijgeven dmv. Username/password)
    c. Authenticating Domain (uitgaande mail vrijgeven op basis van het domein)

Als laatste stap kan je nu je MTA instellen om de uitgaande e-mail via onze service te laten lopen. De hostname welke je hiervoor moet gebruiken is: **smtp.antispamcloud.com**

Configuratie (M365)

Als je vanuit M365 uit wilt gaan mailen via onze service kan je het beste mail vrij geven op basis van Authenticating Domain.

1. Log in op het Control panel.
2. Ga naar 'General', -> 'Domains overview' en klik op het betreffende domein.
3. Ga nu naar 'Outgoing', -> 'Manage users'.
4. Selecteer 'Authenticating Domain' en controleer of het M365 domein hier staat.
5. Geef een wachtwoord op. Dit wachtwoord is alleen nodig tijdens de configuratie.
6. Stel de Authentication method in als required en vink de optie 'Re-authentication permitted' aan.
7. Druk op Save.

Nu moet er nog een connector en een transport rule aangemaakt worden in Exchange om er voor te zorgen dat Exchange de mail via onze service gaat versturen.

Connector aanmaken

1. Log in op het Exchange online admin center.
2. Ga naar 'Mail flow', -> 'Connectors'.
3. Klik op + 'Add a connector'.
4. Zet de connection 'from' op 'Office 365'.
5. Zet de connection 'to' op 'partner organization'.
6. Klik 'Next'.
7. Geef de connector een logische naam.
8. Bij 'Use of Connector window', selecteert u 'Only when I have a transport rule set up that redirects messages to this connector'.
9. Selecteer 'Route email through these smarthosts' en stel hier deze in: smtp.antispamcloud.com
10. Klik op + en dan Next.
11. Bij de Security Restrictions tab kiest u voor 'Always use Transport Layer Security (TLS) to secure the connection' (recommended).
    a. Gebruik 'Issued by a trusted certificate authority' (CA).
    b. Klik Next.
12. Vul een geldig e-mail adres in (binnen het domein).
13. Klik + en dan Validate.
14. Soms gaat de validatie niet goed, maar wordt de validatie mail wel verzonden. Sla dan de validatie over en ga door met het aanmaken van de Transport rule.
15. Klik Next.
16. Kijk of alle details goed staan en klik dan op 'Create connector'.

Transport rule aanmaken

1. Log in op het Exchange online admin center.
2. Ga in het menu aan de linker kant naar het nieuwe admin center (dit is standaard).
3. Open de Mail flow.
4. Ga naar de Rules.
5. Maak een nieuwe rule aan door op '+ Add a rule' te drukken.
6. Kies 'Create a new rule'.
7. Geef de rule een logische naam.
8. Vul vervolgens deze gegevens in:
    a. 'Apply this rule if The sender's domain is' en voeg hier uw domein toe.

   b. Bij ‘Do the following’ kies je voor ‘Redirect messages to the following connector’ en selecteer je de connector die we in de vorige stap hebben aangemaakt.
   c. Bij ‘Except if’ kiest u voor ‘The recipient is external/internal’ en selecteert u hier ‘inside the organization’.
   d. Kies bij ‘a’: ‘mode for this rule’ voor ‘Enforce’.
9. Klik op Save.

Nu dit gedaan is zal het e-mail verkeer via de zojuist aangemaakte connector via onze uitgaande dienst worden verstuurd.

De standaard poort is 587, maar je kan ook poort 465 of 25 gebruiken. Let er ook op dat de MTA niet meer dan 10 concurrent SMTP connecties gebruikt.

SPF

Zorg er voor dat het SPF record van het betreffende domein onze include ‘include:_spf.mx-relay.com’ heeft staan.

DMARC

DMARC-records worden ingesteld in de DNS (Domain Name Server) van het domein. Wanneer je je DMARC-record instelt, kies je het beleidstype (afwijzen, quarantaine, geen). We raden aan om in eerste instantie op ‘geen’ in te stellen en vervolgens, na het controleren van de misbruikrapporten, naar quarantaine te gaan of indien nodig af te wijzen.

Dit record vertelt de server wat er moet gebeuren met berichten die niet voldoen aan de SPF/DKIM-controles. De volgende online tools kunnen helpen bij de configuratie:

https://easydmarc.com/tools/dmarc-record-generator hiermee kan je een DMARC-record opbouwen dat je vervolgens aan je DNS kunt toevoegen.

DKIM

Als het verzendende domein al met DKIM wordt ondertekend, mag dit niet worden gewijzigd. Wij sturen de met DKIM ondertekende berichten eenvoudig door naar de ontvanger.

Als er geen DKIM-ondertekening plaatsvindt, kan je ervoor kiezen om deze te ondertekenen op je verzendende MTA, of om te ondertekenen door ons. Het is niet verplicht om met DKIM te ondertekenen, maar vaak helpt het om afzenders zoveel mogelijk te ‘authenticeren’.

1. Ga in ons Control panel naar ‘General’, -> ‘Domains overview’ en klik op het domein waar je DKIM voor wilt instellen.
2. Ga naar ‘Outgoing’, -> ‘DKIM’.
3. Kies de gewenste DKIM length, wij raden aan: 2028 bits.
4. Vul een DKIM selector in, dit kan alles zijn wat je maar wilt, bv. selector1
5. Klik nu op ‘Generate’ and save new private/public par.
6. Zodra de sleutel is gegenereerd maak je een nieuw TXT DNS record aan in de DNS van het betreffende domein.
   a. Bv. selector1._domainkey.example.invalid.
   b. Hierbij is selector1 de selector die je in stap 4 hebt ingegeven
   c. _domainkey blijft zoals hij hier is
   d. example.invalid moet vervangen worden door de betreffende domein naam.

7. Voer de waarde van dit DNS-record in die gelijk is aan de sleutel die is opgegeven in het groene vak in stap 5. Dus bv.:
   v=DKIM1;
   k=rsa;
   p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMXXXXXXcqo8bs5hLiVqaraXopOAxV+1RAD5PolF4r7u1UPMmEnBo+ncGRxRN5W7vc01yeePr5D118gJPIFaeWz0fLKFORPYr44dWqCJuWhVz/BOg/+ih+1z1kCu6pfqP3Fkvh10ALsv8bDQRsfLY62s2Rc+r+1hJlVH5KpOxQ9BNDWO2g51iMjIJ4xCSnaNavZqEHyQSUmmi/mtJa/8tNRZ/ZxQOOh76mz2/9tlKHynns58cjfeVD+OszAdMjVxWigDCYIuv1XeLqjwZcrroPBJ4o/KAS/typvOn3BCsgSr5L2UmJmZnzSEhyiFGcwCT8owIDAQAB;
8. Ga nu naar ‘Outgoing’, -> ‘Manage users’.
9. Klik op de dropdown button van de betreffende Username/IP en kies voor ‘Edit’.
10. Vul hier bij de DKIM selector weer de door jou ingegeven selector bij stap 4.
    a. 

Meer informatie over DKIM kunt u via de volgende link vinden; https://dkim.org/info/dkim-faq.html