

## 16. MailPlus Server

Een mooie applicatie om te gebruiken is MailPlus Server. Deze applicatie van Synology stelt u in staat om uw eigen e-mailserver te installeren en te beheren. Het fijne hiervan is, dat u compleet onafhankelijk bent van iedereen en dat uw e-mail alleen door u kan worden bekeken. De applicatie bestaat uit twee onderdelen. Met de Synology MailPlus Server stelt u alles in en Synology MailPlus is uw e-mailprogramma. Wat u wel van tevoren moet weten, is dat uw bij de standaard installatie maar vijf e-mailadressen kunt gebruiken. Wilt u meer e-mailadressen in gebruik nemen, dan zult u extra licenties moeten aanschaffen.

Om een eigen e-mailserver te draaien hebt u een eigen domeinnaam nodig. Die kunt u al hebben voor vier euro per jaar. Let er bij het kiezen van een provider op, dat het u vrij staat om de DNS-records van het gekozen domein zelf aan te passen. Het inregelen van de e-mailserver is de eerste keer best wel lastig. Om die reden heb ik in dit hoofdstuk daar extra aandacht aan besteed, want het moet wel veilig gebeuren.

Een eigen e-mailserver brengt ook gevaren met zich mee, want hackers willen hier maar al te graag gebruik van maken, om op die manier duizenden spam-berichten te kunnen versturen. Om dit te voorkomen zult u zich moeten verdiepen in alle beveiligingsopties die de MailPlus Server biedt. Draait alles naar wens, dan kunt u met elk e-mailprogramma de e-mail ontvangen, online webmail gebruiken van Synology of op uw telefoon gebruik maken van de MailPlus app.

## 16.1 Installatie Synology MailPlus Server

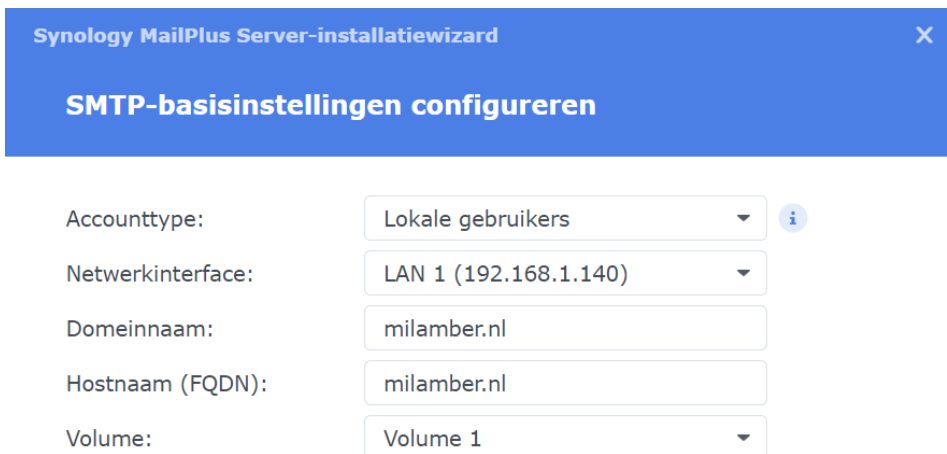
1. Ga naar het Package Center, zoek op mail en installeer Synology MailPlus Server.



2. Open MailPlus Server na de installatie.



3. Kies voor de standaard optie Een nieuw e-mailsysteem maken. Klik op Volgende.



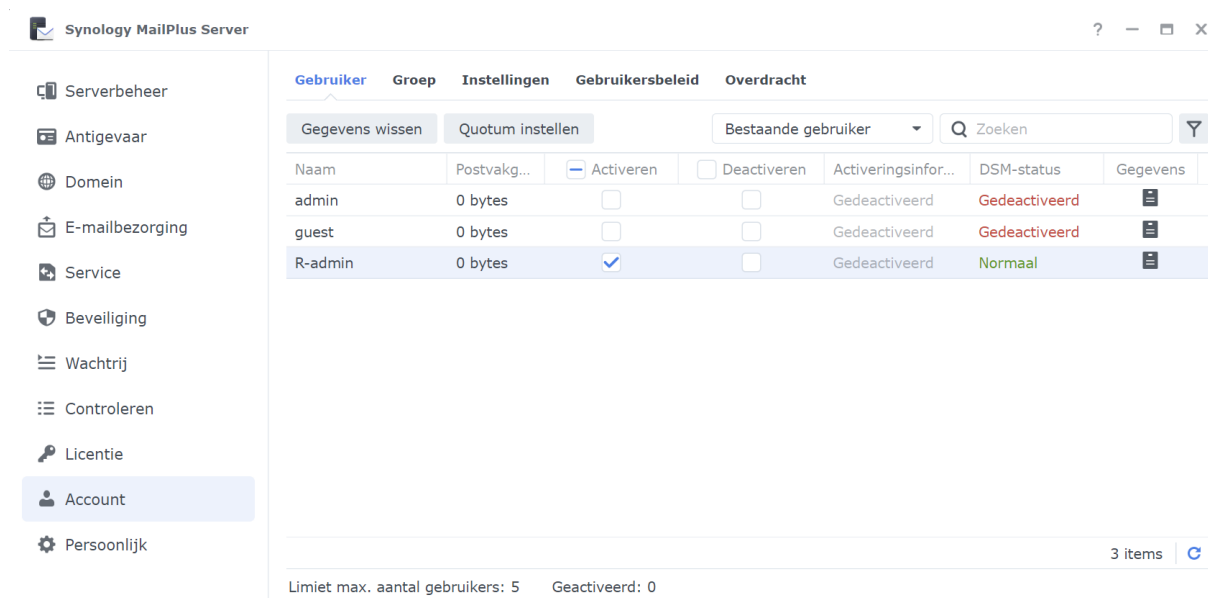
4. Vul bij Domeinnaam het domein in waarop u de e-mail wilt ontvangen. Vul bij Hostnaam (FQDN) het PTR-record in dat u krijgt via uw internetprovider. Een PTR-record (Pointer Record) is hetzelfde als rDNS oftewel Reverse DNS. Het geeft aan dat de hostnaam die u gebruikt daadwerkelijk is gekoppeld aan het IP-adres dat u van uw Internetprovider hebt gekregen. Veel mailservers voeren een check uit om dit te controleren. Is reverse DNS niet ingesteld, dan kan uw e-mail geweigerd worden of in de spambox terecht komen. Hebt u niet de mogelijkheid om een PTR-record te verkrijgen, dan zijn er nog een aantal andere manieren om door deze

check heen te komen. Hier kom ik later op terug. Omdat het veld wel moet worden ingevuld, geeft u hier uw domeinnaam op. Klik op Volgende.

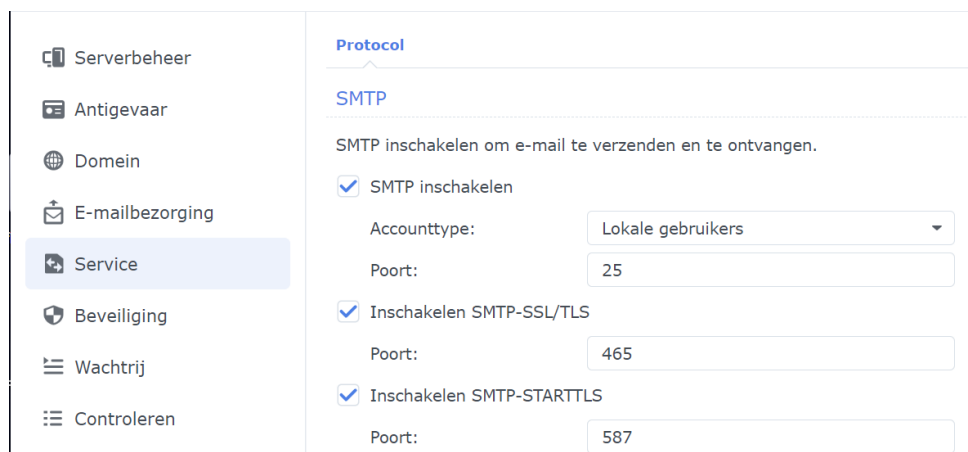
- U krijgt een samenvatting. Klik op Toepassen. De instellingen worden uitgevoerd.



- Klik op Voltooiën.
- Klik aan de linkerkant op Account en activeer de accounts die gebruik mogen maken van de e-mailserver. Zonder extra licenties mag u vijf accounts activeren. Klik op Toepassen.



- Klik aan de linkerkant op Service.



- Onder het kopje SMTP (Simple Mail Transfer Protocol) staan er al vinkjes bij SMTP, SMTP-SSL en SMTP-TLS. De eerste optie met standaard poort 25 is om e-mail te versturen of te ontvangen via de onbeveiligde poort. Om e-mail te versturen via de beveiligde poorten 465 voor SSL (Secure Socket Layer) en 587 voor het nieuwere TLS (Transport Layer Security) moet er op uw server een SSL-certificaat draaien. Zet deze drie poorten open op uw router.

Mailserver smtp		25,465,578	192.168.1.140		TCP	
-----------------	--	------------	---------------	--	-----	--

- Onder het kopje IMAP/POP3 geeft u aan welke cliënt-protocollen er mogen worden gebruikt om e-mail te ontvangen.

#### IMAP/POP3

De volgende clientprotocols inschakelen om e-mail te ontvangen via e-mailclients zoals Outlook.

- POP3 inschakelen
- POP3 SSL/TLS inschakelen
- IMAP inschakelen
- IMAP SSL/TLS inschakelen
- Tekst zonder opmaak-verificatie via ongecodeerde verbinding verbieden

Geavanceerd

- Haal de vinkjes weg van de protocollen die u niet wilt gebruiken. Bij het POP3 protocol, haalt u de e-mail van de server. Met de IMAP protocollen blijft de e-mail op de server staan. Wilt u POP3 gebruiken, forward dan de poorten 110 en 995 naar uw NAS.

Mailserver pop		110,995	192.168.1.140		TCP	
----------------	--	---------	---------------	--	-----	--

- Wilt u IMAP gebruiken, dan routeert u de poorten 143 (onbeveiligd) of 993 (beveiligd) naar uw NAS.

mailserver imap		143,993	192.168.1.140		TCP	
-----------------	--	---------	---------------	--	-----	--

- Klik aan de linkerkant op Beveiliging. Op het eerste tabblad Spam, schakelt u de Antispamengine in. Klik op Toepassen.
- Klik op Instellingen voor bijwerken.
- De Spamregels worden automatisch geüpdatet, maar de eerste keer klikt u op Handmatig bijwerken en daarna op Opslaan.
- Plaats een vinkje bij DNSBL-instellingen om de DNS-Blackhole List te activeren. De afzender van de e-mail wordt gecontroleerd of die op deze bekende spammer lijst staat. Klik op Toepassen.

Antispam    AntiVirus    Verificatie    Inhoudscan    Gegevensbeveiliging

#### Antispamprogramma

Antispamengine inschakelen (aanbevolen)

Programma: Rspamd

Versie: 1873061 (Normaal) | 13-03-2020 13:31:54

Instellingen voor bijwerken

Instellingen voor bijwerken ×

Antispamregels automatisch updaten 05 : 45

Engine-informatie

**Regelversie:** 1902275

**Tijdstip Laatst bijgewerkt:** 28-06-2022 13:39:56

Handmatig bijwerken

17. Ga naar het tabblad AntiVirus en schakel de Antivirusengine in en klik op Toepassen.

Antispam **AntiVirus** Verificatie Inhoudscan Gegevensbeveiliging

---

Antivirusprogramma

Antivirusengine inschakelen i

Programma: ClamAV ▾

Virusdefinitieversie: - (Normaal) | -

Instellingen voor bijwerken

Google Safe Browsing gebruiken om kwaadaardige links in e-mails te detecteren i

Databases van derde partijen gebruiken om hun virusdefinities te downloaden

18. Schakel de Google SafeBrowsing-database in om kwaadaardige URL's uit de e-mail te vissen.
19. Activeer de optie om de detectie van malware en phishing te verbeteren en klik op Toepassen.
20. Klik op Instellingen voor bijwerken en klik op Handmatig Bijwerken.

#### Instellingen voor bijwerken

Virusdefinities automatisch updaten 05 ▾ : 45 ▾

Systeeminformatie antivirusengine

**Productversie:** 0.103.1

**Virusgegevensversie:** 26587

**Uitgavetijd:** 28-06-2022 10:07:12

**Tijdstip Laatste bijgewerkt:** 28-06-2022 13:47:46

**Status:** Normaal

Handmatig bijwerken

21. Klik op Opslaan. Plaats een vinkje onder Actie bij Onderwerp voorvoegsel toevoegen aan geïnfecteerde e-mailberichten.

#### Acties

Antivirusactie: Opslaan in quarantaine ▾

Onderwerpvoorvoegsel toevoegen aan geïnfecteerde e-mailberichten {Virus?}

Stuur meldingen naar ontvangers na het verwijderen of in quarantaine plaatsen van virussen

Sjablooninstellingen

22. Bepaal wat er moet worden gedaan met de e-mails die een virus bevatten. Verwijder deze e-mails, plaats ze in quarantaine, of verstuur ze toch naar het e-mailprogramma. Klik op Toepassen.

23. Ga naar het tabblad Verificatie. Plaats een vinkje bij SPF-verificatie inschakelen (Sender Policy Framework). De mailserver voert nu een check uit om te controleren of de afzender wel mail mag versturen volgens de afzender. De e-mailserver doet een check op de DNS-instellingen. Daar moet een SPF-record staan. Later gaan we dat record ook maken voor uw DNS-instellingen.

Spam | AntiVirus | **Verificatie** | Inhoudscan | Gegevensbeveiliging

### SPF

SPF is een e-mailvalidatiesysteem ontworpen om de identiteit van de afzender te verifiëren en spamberichten te voorkomen door de detectie van valse adressen van afzenders.

SPF-verificatie inschakelen

SPF softfail weigeren

24. Plaats tevens een vinkje bij SPF softfail weigeren om e-mail te weigeren die niet door deze check heenkomen.
25. Plaats een vinkje bij DKIM-verificatie inschakelen voor inkomende e-mailberichten. DomainKeys Identified Mail (DKIM) wordt gebruikt om e-mail te voorzien van een digitale handtekening die is opgenomen in de DNS-instellingen van het domein. Hierdoor kan spam worden tegengegaan.

### DKIM

Met DKIM kan de ontvanger een openbare sleutel gebruiken om de handtekening van de afzender te valideren om potentiële kwaadaardige e-mailberichten of spamberichten te beperken.

- DKIM-verificatie inschakelen voor inkomende e-mailberichten

Minimum sleutellengte voor DKIM-verificatie:  [i](#)

Wilt u uitgaande e-mailberichten van specifieke IP-adressen ondertekenen met DKIM voeg dan het IP-adres toe aan de DKIM witte lijst.

[Witte lijst](#)

26. De eerste stap voor DKIM is gedaan. Klik op Toepassen.
27. Plaats een vinkje voor DMARC inschakelen.

### DMARC

Met DMARC kan de ontvanger het e-maildomein van de afzender valideren.

- DMARC inschakelen

28. Door de Domain-based Message Authentication Reporting and Conformance (DMARC) te activeren kan de ontvangende e-mailserver bepalen wat hij moet doen als uw e-mail niet door de SPF of DKIM check heen komt. Wat de keuze is, wordt bepaald door de DMARC DNS record in je DNS. Klik op Toepassen.
29. Klik aan de linkerkant op Domein.

Synology MailPlus Server

Serverbeheer | Antigevaar | **Domein**

Toevoegen | Bewerken

Domeinnaam

milamber.nl (Primair)

30. Dubbelklik op het actieve domein.

**milamber.nl**

---

**Algemeen**   Gebruiker   Groep   Alias   Auto BCC   Gebruikslimiet   Disclaimer

---

Domeinnaam:  Extra domein

Beschrijving:

Standaard e-mailadresindeling:  i

Nieuw gebruikers automatisch toevoegen aan dit domein

Geavanceerd

31. Klik op Geavanceerd en plaats een vinkje bij DKIM-ondertekening inschakelen voor uitgaande e-mailberichten.

**Geavanceerd** X

---

**DKIM**

DKIM-ondertekening inschakelen voor uitgaande e-mailberichten

DKIM-sleutellengte: 2048

DKIM-selectorvoorvoegsel:

Openbare sleutel:

Openbare sleutel genereren

- 32. Geef een naam op bij DKIM-selector voorvoegsel. U hebt die naam zo meteen nodig voor het aanmaken van het DNS-record.
- 33. Klik op Openbare sleutel genereren. Kopieer de sleutel naar een tekstbestand. U hebt deze sleutel zo meteen nodig voor het DNS-record. Klik op OK en Opslaan.
- 34. U hebt nu de belangrijkste instellingen ingesteld. Hoogste tijd om nu de DNS-instellingen van uw domein in te stellen.