

Inhoudsopgave

Aansluiting op de maildienst van Gemeente Utrecht	2
Introductie	2
Achtergrond	2
Reikwijdte Beleid	2
Leeswijzer	2
1. Verzenden vanuit één vast email adres	2
Functionele vraag	2
Voorbeeld toepassing	2
Richtlijnen	3
Invulling van de dienst	3
Technische eisen	3
Aandachtspunten	3
2. Verzenden vanuit meerdere (bestaande) emailadressen	4
Functionele vraag	4
Voorbeeld toepassing	4
Richtlijnen	4
Technische eisen	5
Automatische verwerking van email en/of agenda items (intern en extern)	6
Functionele vraag	6
Richtlijn	6
Technische eisen	7
Versiebeheer	7

Aansluiting op de maildienst van Gemeente Utrecht

Introductie

Deze richtlijn beschrijft de wijze van aansluiten van zowel interne als externe applicaties, apparaten en/of leveranciers op de mailomgeving van de Gemeente Utrecht.

De richtlijn geldt voor het verzenden, ontvangen en verwerken van mail naar zowel interne als externe adressen gebruik makend van een door de Gemeente beheerd emailadres.

Achtergrond informatie

De Gemeente Utrecht kent een hybride mail omgeving op basis van Exchange 2016 en Office 365. Voor het versturen, ontvangen van uitgaande en inkomende email wordt gebruik gemaakt van Exchange Online Protection (EOP). Mailboxen kunnen zowel op Exchange 2016 als Office365 worden geplaatst.

Reikwijdte Beleid

Dit beleid geldt voor alle interne en externe applicaties, apparaten of leveranciers (aansluitpunt(en)), hierna te noemen aansluitpunt gebruik makend van de mail dienst van de Gemeente Utrecht.

Leeswijzer

Invulling van het beleid is gericht op de functionele email behoefte van het aansluitpunt in afstemming met de Gemeente Utrecht. Er zijn drie scenario's beschikbaar, welke binnen de gestelde criteria toegepast kunnen worden.

De functionele email behoefte van een aansluitpunt ten opzichte van email dient altijd beschreven te worden in het functioneel ontwerp.

1. Verzenden van mail vanuit één vast email adres

Functionele vraag

Het verzenden van email middels een aan het aansluitpunt specifiek toegekende mailbox. Verzonden email wordt altijd namens één uniek email adres (primair email adres) verstuurd. Gebruik van deze mailbox is mogelijk voor één of meerdere aansluitpunten. Bij gebruik door meerdere aansluitpunten worden de inloggegevens gedeeld.

Voorbeeld toepassing

Voorbeeld 1: Multifunctionals (Printers) verzenden in gescande documenten, hiervoor wordt als afzender printer@utrecht.nl voor gebruikt. Deze mailbox wordt op alle MFP's ingesteld zodat alle printers vanuit het zelfde email adres verzenden.

Voorbeeld 2: Een SaaS applicatie verzendt uit een vast email adres berichten naar interne en externe ontvangers, hiervoor wordt een eigen mailbox gebruikt met het email adres SaaSapplicatie@utrecht.nl

Richtlijnen

Voor koppeling met een specifieke mailbox wordt gebruik gemaakt van de [SMTP cliënt Submission](#) dienst van Office 365. De door Microsoft gestelde richtlijnen zijn hiervoor van toepassing.

Invulling van de dienst

- Het aansluitpunt maakt verbinding met smtp.office365.com
- Het aansluitpunt logt in op de mailbox middels de gebruiker en het wachtwoord;
- Het aansluitpunt verstuurd de mail via SMTP submission naar de ontvangers;
- De ontvanger ziet het email adres als afzender van de verstuurd mail;
- Verstuurd mail wordt zowel bij interne als externe geadresseerde afgeleverd;

Het ontvangen van email door het aansluitpunt is niet mogelijk, er wordt een autoreply ingesteld op de mailbox met de mededeling dat deze mailbox niet wordt uitgelezen en wordt verwezen naar een algemeen email adres.

Het email adres gebruikt voor verzending dient uniek te zijn en te voldoen aan de naamgevingsconventie. Standaard is dit <naam>@Utrecht.nl maar dit kan ook een ander domein zijn mits dit een door Utrecht beheerd email domein betreft.

Technische eisen

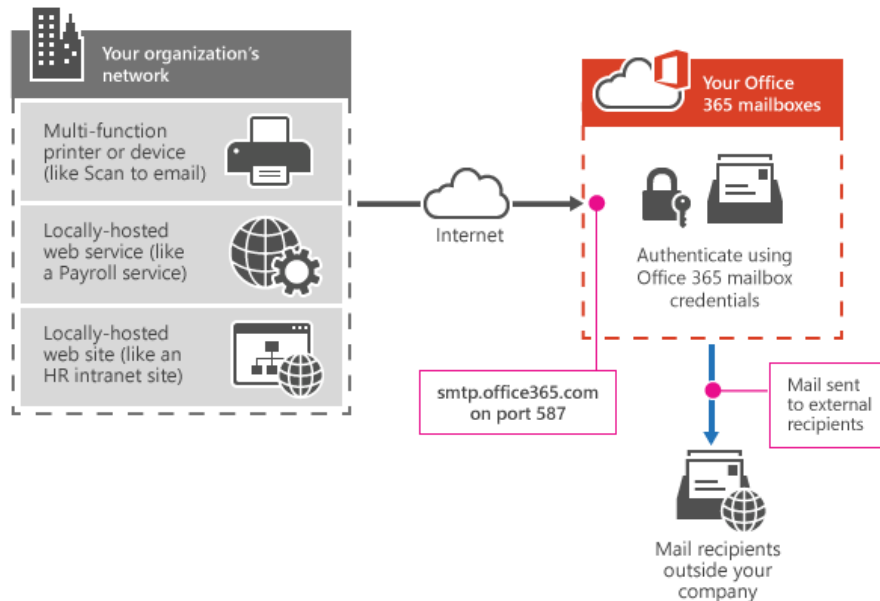
Om email te verzenden middels Office 365 SMTP cliënt submission gelden de volgende vereisten;

- smtp.office365.com en poort 587 dient bereikbaar te zijn;
- TLS 1.2 of hoger ondersteuning;
- Authenticatie moet worden ondersteund door het aansluitpunt;
- DNS resolving dient beschikbaar te zijn;
- Beschikking over een eigen mailbox en bijbehorende inloggegevens;
- Shared mailboxen worden niet ondersteund;
- Een Exchange online licentie is vereist per mailbox.

Aandachtspunten

- Eén mailbox kan worden gedeeld door meerdere (gelijksoortige) aansluitpunten (bijv. printers@utrecht.nl voor meerdere printers).
- SMTP submission ondersteund maximaal 30 berichten per minuut, 10.000 ontvangers per dag per mailbox (bulkmail);
- Maximaal 3 gelijktijdige SMTP connecties worden ondersteund;
- De verzonden items worden bewaard in de mailbox sent items folder;
- Verzonden items worden periodiek geautomatiseerd opgeschoond;

- De specifieke mailbox wordt alleen gebruikt voor dit doeleinde;
- Het toekennen van rechten op andere mailboxen (bijv. send as) is niet toegestaan;



Figuur 1 Office 365 Client Submission

Het verzenden van mail middels SMTP client submission geldt als de standaard methodiek voor alle aansluitpunten.

In specifieke uitzonderingen is toepassing van SMTP relay op Office 365 (scenario 2) mogelijk.

Dit kan zijn in de situatie van;

- Versturen van bulk email en/of nieuwsbrieven;
- Verzending uit naam van meerdere email adressen van de Gemeente Utrecht.

2. Verzenden van mail vanuit meerdere emailadressen

Functionele vraag

Het versturen van email namens meerdere door gemeente Utrecht beheerde (bestaande) mail adressen en/of het verzenden van bulk email.

Bij toepassing van dit type dienst dient de eigenaar akkoord te gaan met de geldende richtlijnen voor het gebruik van deze dienst.

Voorbeeld toepassing

Een applicatie stuurt uit naam van meerdere gebruikers mail naar zowel interne als externe ontvangers. Hiervoor is SMTP cliënt submission niet geschikt.

Richtlijnen

- Versturen van email namens meer dan 1 bestaande gebruikers (emailadressen);

- Aansluitpunten welke gebruik maakt van bulk mail verzendingen.

Functionele eisen: Er dient te worden opgenomen in het functioneel ontwerp dat email verstuurd vanuit een aansluitpunt alleen mogelijk is voor binnen de applicatie aangesloten identiteiten en email adressen.

Technische eisen

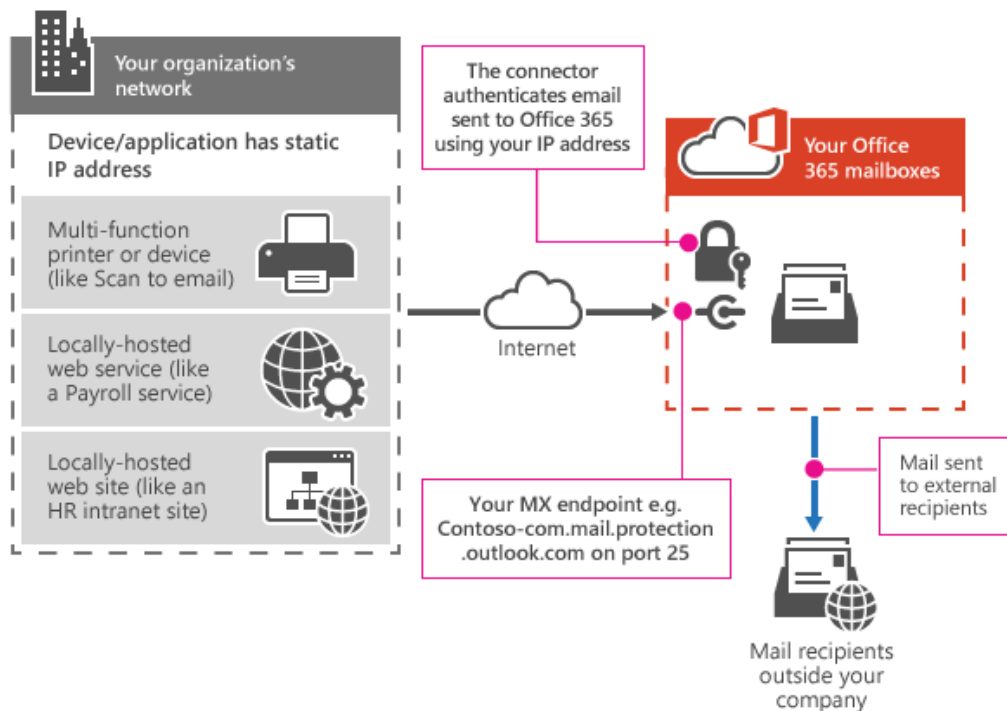
Office 365 SMTP relay wordt middels een Office 365 connector gerealiseerd.
Hiervoor gelden de volgende eisen;

- DNS resolving dient beschikbaar te zijn naar xxxxx.mail.protection.outlook.com;
- De verzendende dienst dient over een vast IP-adres te beschikken;
- Het IP-adres wordt als SPF-record opgenomen in de externe DNS van de Gemeente Utrecht;¹
- Verzending vindt plaats over poort 25;
- Toepassing van TLS 1.2 encryptie is verplicht;
- Een op naam van Utrecht email geregistreerde domeinnaam dient gebruikt worden;

Aandachtspunten

- Toepassing van SMTP relay is alleen mogelijk indien voldaan wordt aan de vermelde richtlijnen;
- Dynamische IP-adressen worden niet ondersteund;
- Toepassing van deze oplossing wordt in de nabije toekomst heroverwogen en wijzigt daarmee mogelijk.

¹ SPF ondersteund 255 karakters, toepassing van sub-spf records is mogelijk.



Figuur 2 Office 365 SMTP relay

3. Automatische verwerking van email en/of agenda items (intern en extern)

Functionele vraag

Het geautomatiseerd verwerken van email en/of agenda items vanuit een aansluitpunt.

Hiervoor wordt een specifieke mailbox ter beschikking gesteld.

EWS (Exchange Web Services) is beschikbaar als API koppeling voor het (geautomatiseerd) uitlezen, verwerken en verzenden van mail, agenda en contacten. IMAPS voor het uitlezen en verwerken van alleen mail.

Richtlijn

- EWS en IMAPS zijn altijd gekoppeld aan een eigen mailbox;
- Voor het uitlezen, verwerken en verzenden van agenda en contacten dient EWS te worden gebruikt;
- EWS wordt toegepast middels een API integratie met een SaaS dienst;
- Middels EWS kan zowel ontvangen als verzonden worden;
- IMAPS is alleen beschikbaar voor het uitlezen van email;
- IMAPS is **niet** beschikbaar voor het verzenden van email;
- POP3 functionaliteit is **niet** beschikbaar;

- Verzenden van mail i.c.m. IMAPS middels SMTP Client submission (zie: Verzenden van mail vanuit één vast email adres);
- EWS en IMAP worden altijd gekoppeld aan een eigen mailbox;

Technische eisen

Toegang verloopt altijd via de firewall van de Gemeente en een vooraf gedefinieerde URL. Toegang tot EWS/IPMAPS vindt altijd plaats via een vast IP-adres van de verwerkende partij. Het verkeer wordt altijd versleuteld middels een certificaat.

De volgende technische eisen gelden voor deze toepassing;

- Authenticatie dient altijd plaats te vinden;
- Een specifieke mailbox dient beschikbaar gesteld te worden met inloggegevens;
- IMAPS dient per mailbox aangezet te worden;
- Toegang tot IMAPS vindt altijd plaats met TLS encryptie;
- Publicatie van IMAPS vindt plaats over poort 993;
- De verwerkende dienst dient over een statisch IP-adres te beschikken;
- Toegang tot EWS vindt plaats via het HTTPS protocol over poort 443;
- Toegang tot EWS en IMAPS vindt altijd plaats op basis van source IP-adres(sen);

Aandachtspunten

Aansluiting via EWS of IMAPS kent de volgende aandachtspunten.

- Verzending van berichten vindt plaats via SMTP cliënt submission met TLS 1.2 encryptie;
- Toepassing van EWS of IMAPS dient in de functionele eisen voor het betreffende aansluitpunt te worden opgenomen.

Versiebeheer

Versie	Datum	Wijziging	Auteur	Contact
0.6	05-03-2019	Initiële versie	Martijn Spelt	m.spelt@utrecht.nl
0.8	03-10-2019	Review architectuur	Martijn Spelt	m.spelt@utrecht.nl
0.85	11-10-2019	Opmerkingen verwerkt	Martijn Spelt	m.spelt@utrecht.nl
1.0	14-10-2019	Definitief Architectuur review	Martijn Spelt	m.spelt@utrecht.nl