

Inside Microsoft 365": Exchange Online ohne SMTP BasicAuth

Aaron Siller
Frank Carius



Über mich

Frank Carius

Microsoft MVP Microsoft 365 (Exchange, Teams)

Microsoft Certified Master (Lync)

Webseite: <https://www.msxfaq.de>

 frank.carius@netatwork.de

 <https://de.linkedin.com/in/frankcarius>

Systemhaus/Softwarehaus

Solution Partner „Modern Work“ and „Security“

Seit 1995, Paderborn, Germany, 150+ Mitarbeiter



Microsoft 365 Message Center Post MC 786329

(Updated) Exchange Online to retire Basic Auth for Client Submission (SMTP AUTH)

 Archive  Share  Copy link  Mark as unread

Summary

Exchange Online will retire SMTP AUTH Basic Authentication by default starting December 2026, with OAuth as the supported method. Basic Auth removal is on hold until 2027, when a final date will be announced. Administrators can enable Basic Auth temporarily, but should prepare to switch to OAuth or alternatives.

Updated January 27, 2026: Based on customer feedback and visibility into adoption progress, we are refining the Exchange Online SMTP AUTH Basic Authentication Deprecation timeline to provide clearer milestones and additional runway.

- Now to December 2026: SMTP AUTH Basic Authentication behavior remains unchanged.
- End of December 2026: SMTP AUTH Basic Authentication will be disabled by default for existing tenants. Administrators will still be able to enable it if needed.
- New tenants created after December 2026: SMTP AUTH Basic Authentication will be unavailable by default. OAuth will be the supported authentication method.
- Second half of 2027: Microsoft will announce the final removal date for SMTP AUTH Basic Authentication.

Relevance

■■■ High

Service & monthly active users

 Exchange Online

Message ID

MC786329

Published

Apr 26, 2024

Last updated

Jan 27, 2026

Tag

MAJOR UPDATE

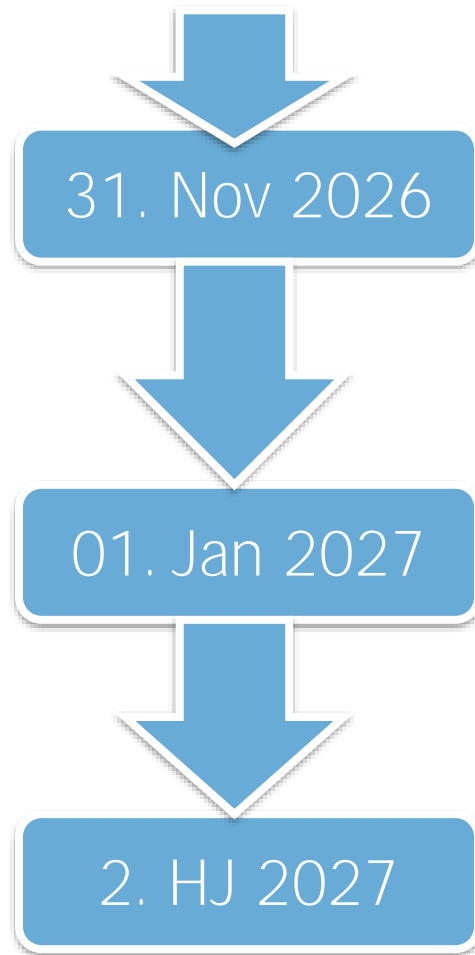
ADMIN IMPACT

RETIREMENT

USER IMPACT



Zeitlicher Ablauf

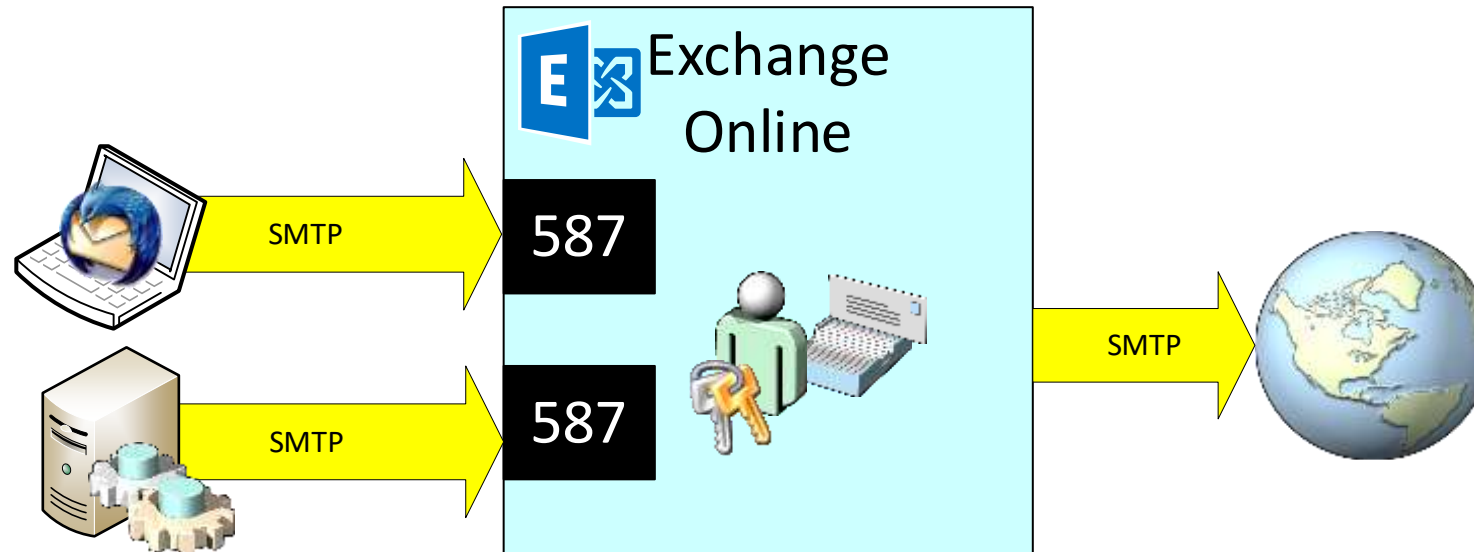


- Bis 31. Nov 2026 - Keine Änderung
 - > Basic Authentication ist weiterhin aktiv
 - > Administrator kann Report auswerten
 - > Administrator kann Basic Authentication selbst deaktivieren
- 01. Jan 2027 – Rollout
 - > Neue Tenants: Default = „OFF“
 - > Bestehende Tenants: „Weckruf“ an Admins“
 - Rollout der Abschaltung
 - Reaktivierung möglich
- 2. HJ 2027 – Deaktivierung erzwungen



Worum geht es?

- Mailversand über SMTP-Einlieferung
- Anmeldung mit Username + Kennwort ist nicht sicher
- Empfänger im Internet
- Nicht Outlook, nicht OWA, nicht ActiveSync!



Wer nutzt diesen Weg?

- Exchange Admin Center

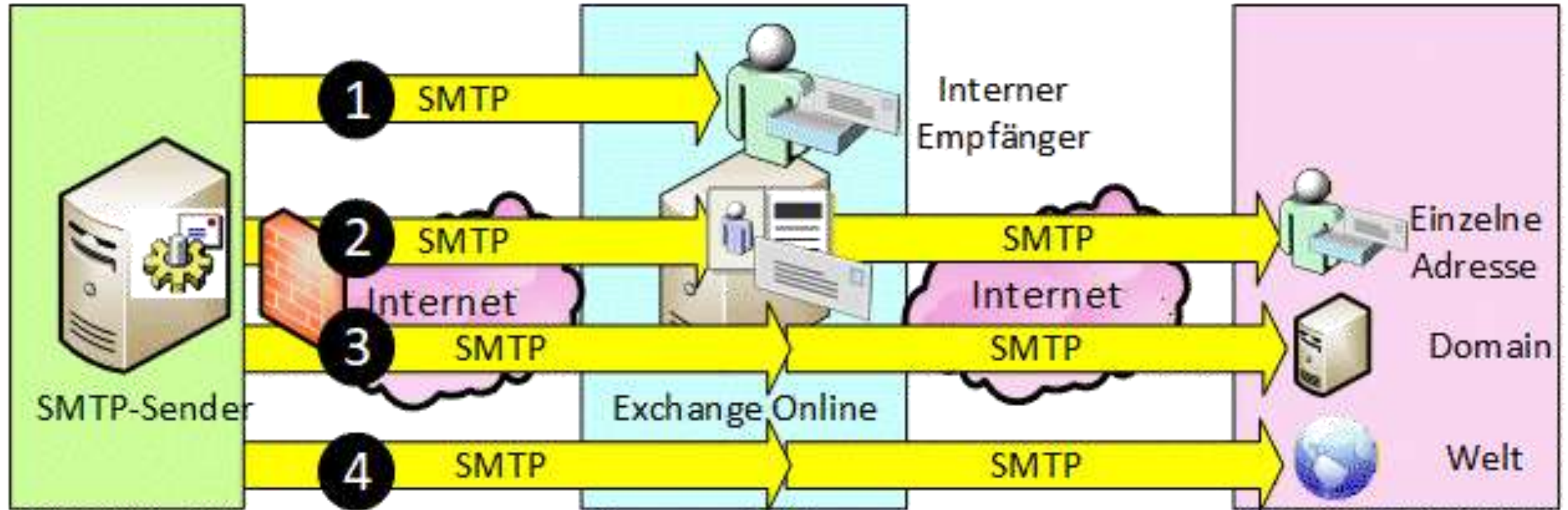
<https://admin.cloud.microsoft/exchange?#/reports/smtpauthmailflowdetails>

The screenshot displays the Exchange Admin Center interface. The left-hand navigation pane shows the 'Mail flow' option highlighted with a red rectangular box. The main content area is titled 'Reports > Mail flow > SMTP AUTH clients report'. A yellow information banner at the top states: 'The Authentication Protocol column is a new addition and the data for this column will take 90 days to build up.' Below this, the section 'SMTP AUTH clients' includes a descriptive paragraph: 'Use this report to check for unusual activity and TLS used by clients or devices using SMTP AUTH. SMTP AUTH client submission protocol only offers basic authentication and is a less-secure protocol used by devices, such as printers, to send email messages. [Learn more](#)'.

Under the heading 'Messages sent using SMTP AUTH', there is a dropdown menu currently set to '7 days'. The dropdown options are: 7 days, 30 days, 90 days, and Custom start date. Below the dropdown, the interface shows '0 items' and buttons for 'Export', 'Request report', 'Filter', and 'Search'. A table header is visible with columns: 'Sender Address', 'Domain', 'Authentication P...', and 'TLS 1.0'. At the bottom of the table area, the text 'No data available for given query' is partially visible.



Wer sendet wohin per SMTP?



Mail an interne Empfänger

- Anwendungsfälle

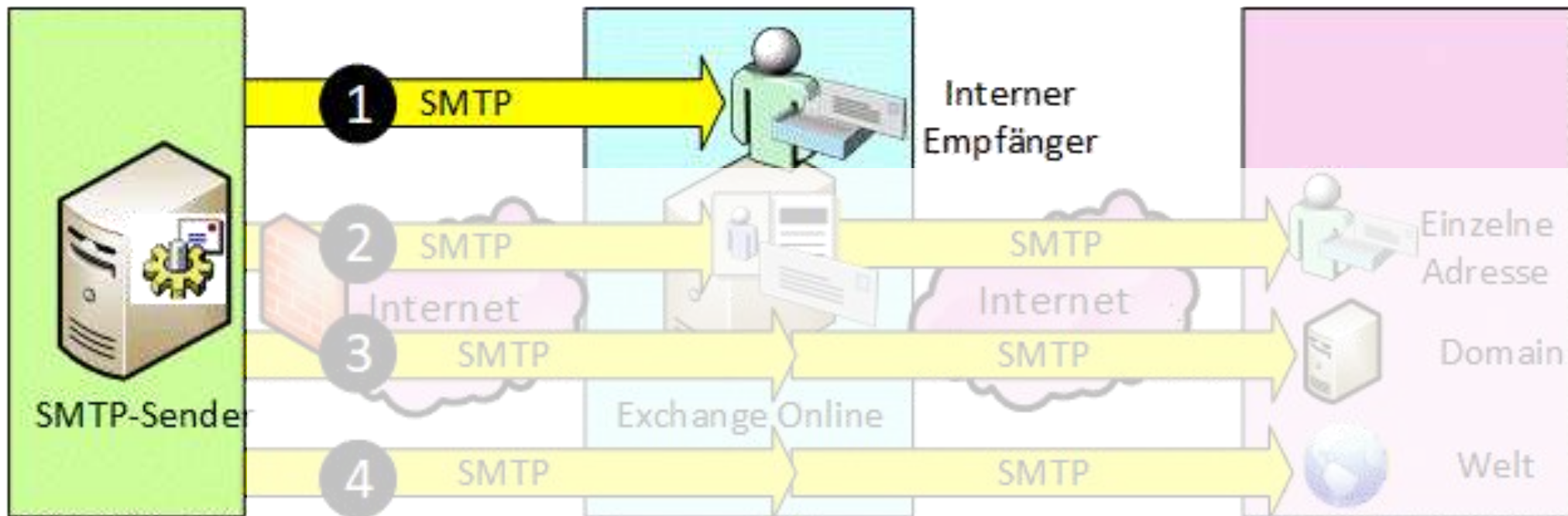
- > Scan2Mail
- > „Backup erfolgreich“
- > Monitoring-Meldungen
- > Formulare auf Webseiten

- Anonym zustellen

- > Risiko Spamfilter
- > Erkennen als Phishing

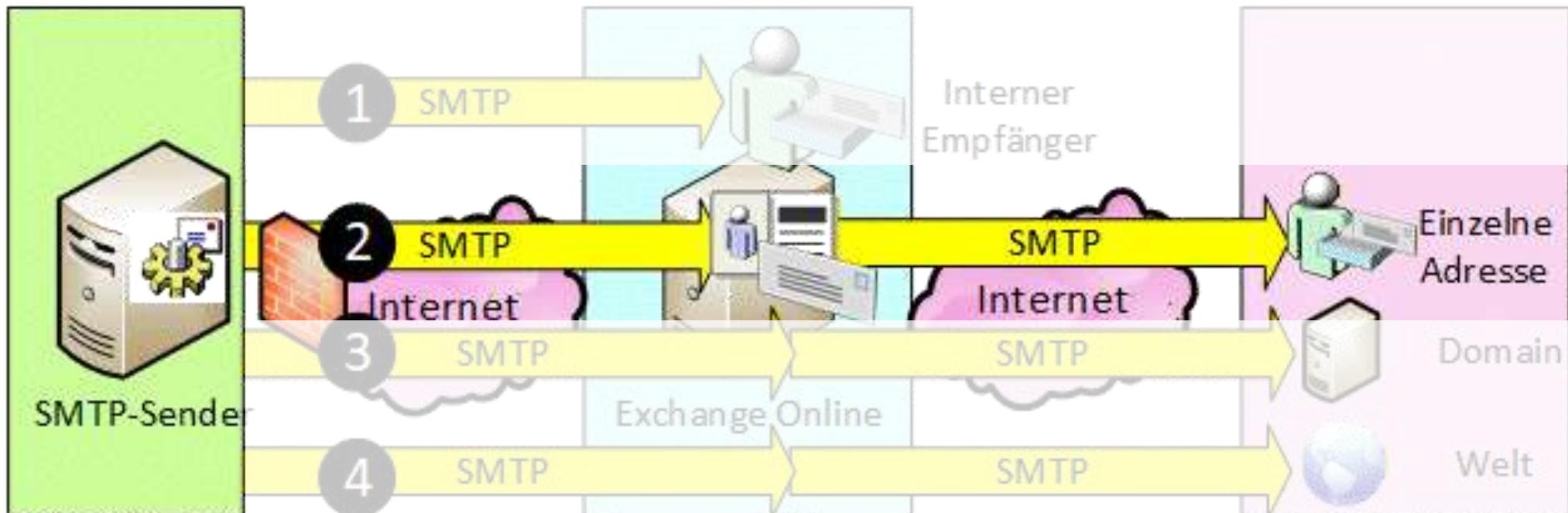
- DirectSend

- > Inbound Connector
- > SPF-Eintrag
- > Absender fälschbar



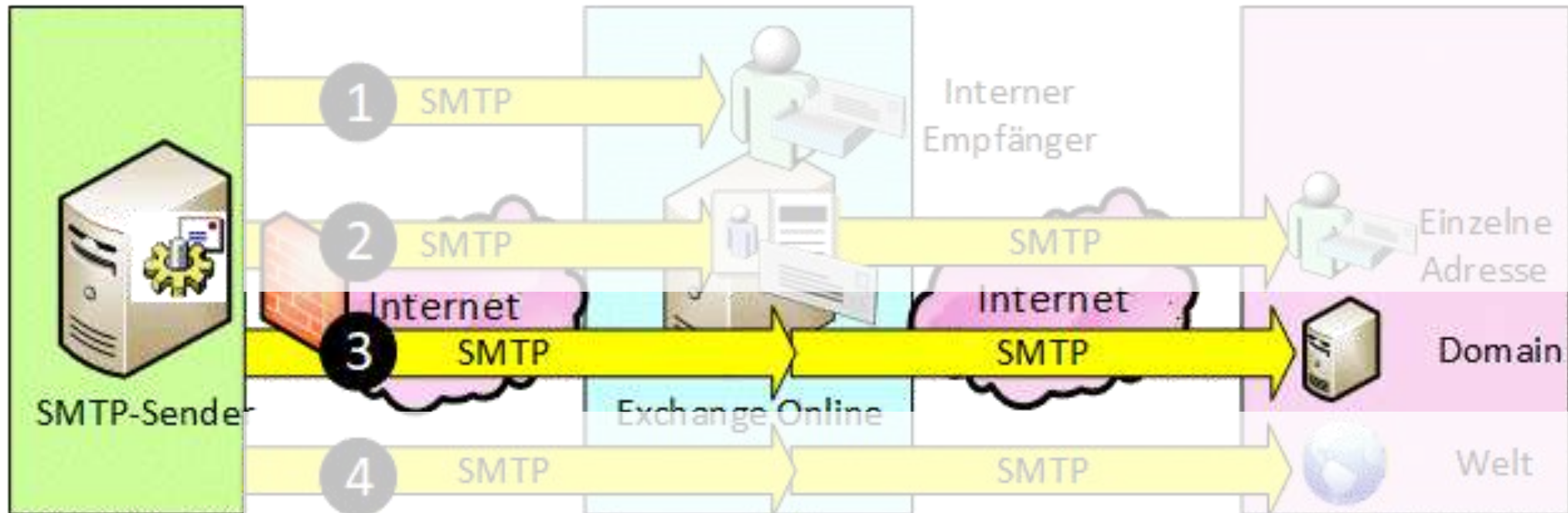
Mail an 1x externen Empfänger

- Einsatzfall
 - › Druckerwartung (Toner Low)
 - › Alarmmails an externen Dienstleister
 - › Externe Support-Postächer
- Mailkontakt in Exchange Online
 - › ProxyAdresse aus eigener Domain
 - › Zieladresse ist extern
 - › Oder Transportregel
- Anonym einliefern
 - › Absicherung mit (DirectSend)



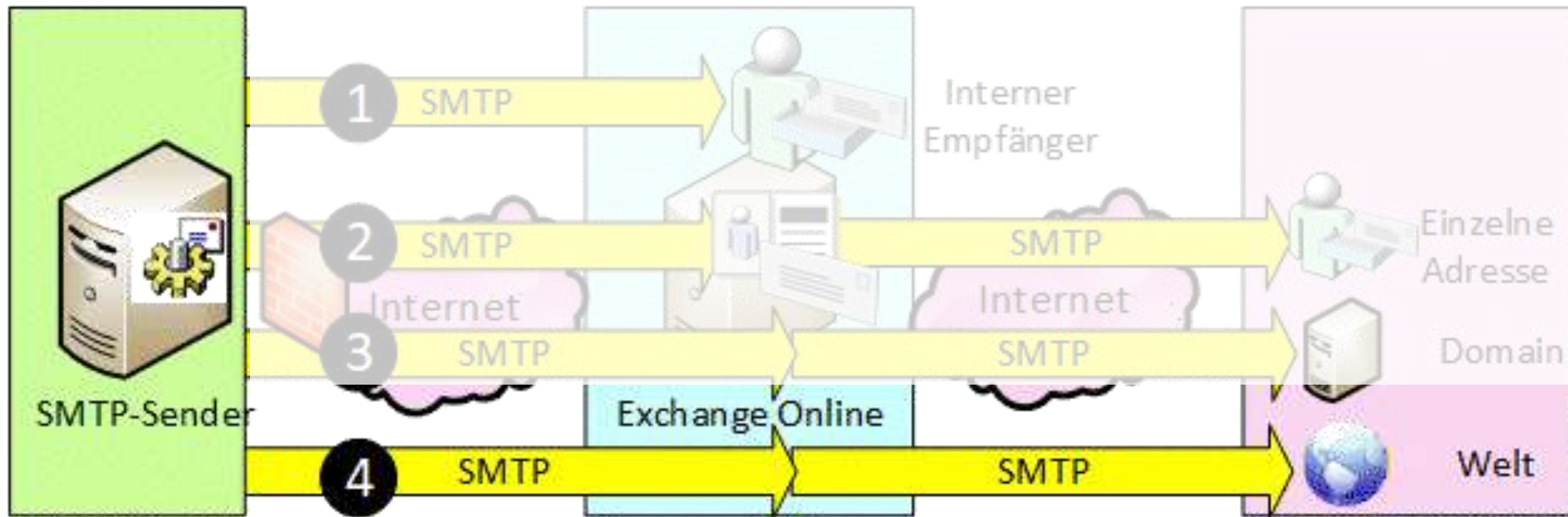
Mail an eine externe Domain

- Einsatzzweck
 - › Partnerunternehmen, Konzernmitglieder
- OnPremises: Accepted Domain: External Relay + Connector
- Online: OnPrem-Connector (Zertifikat oder IP-Adresse, Absenderdomain aus AcceptedDomain)



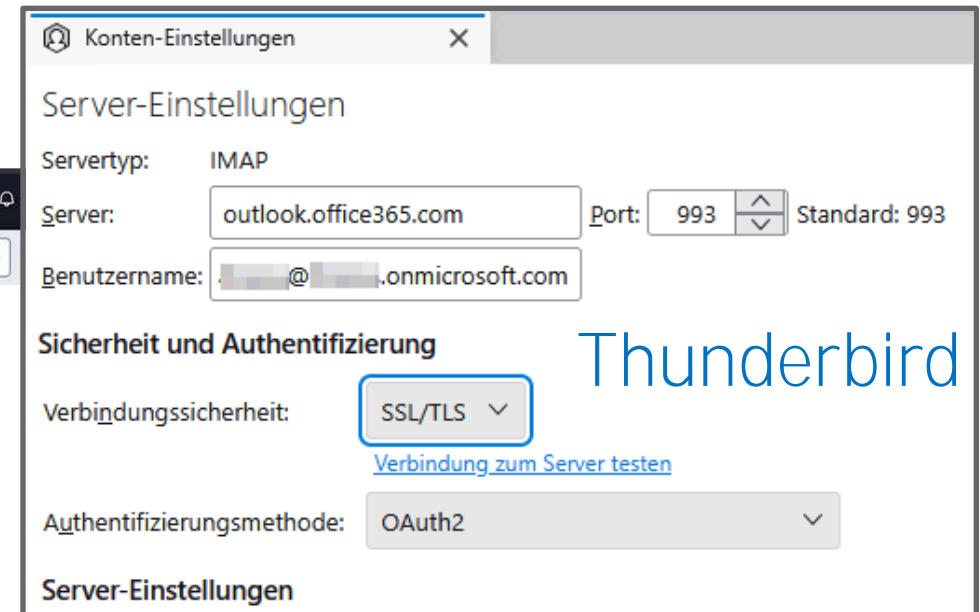
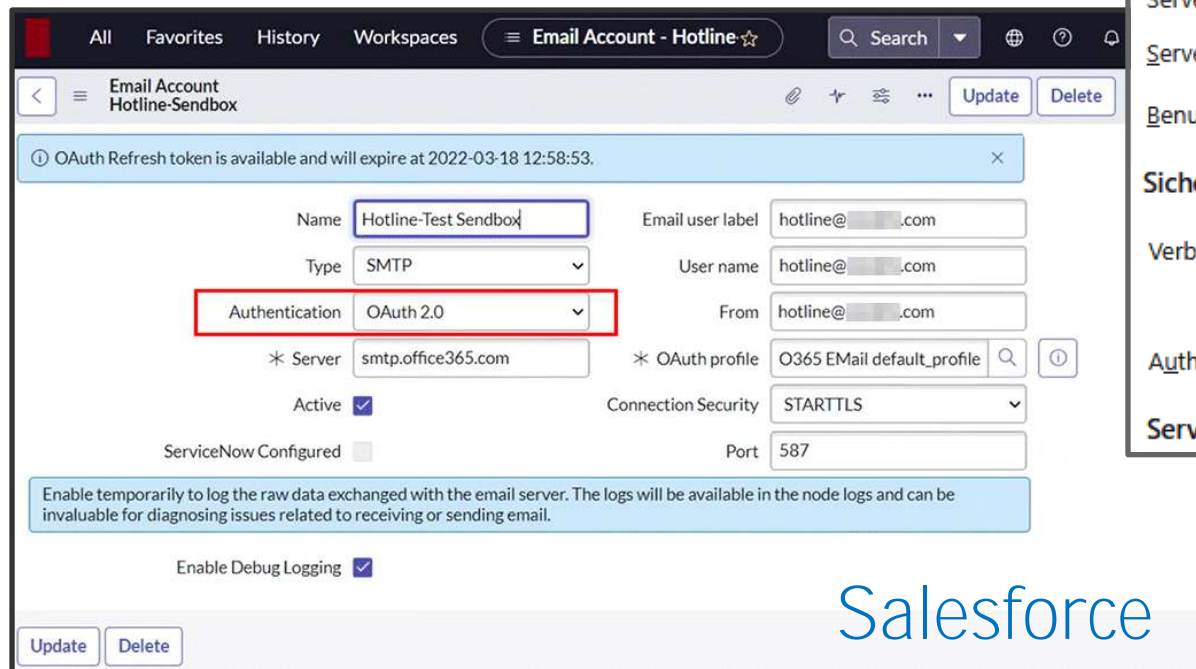
Versand in die Welt

- Das ist der einzige Weg, der durch die Abschaltung wirklich betroffen ist



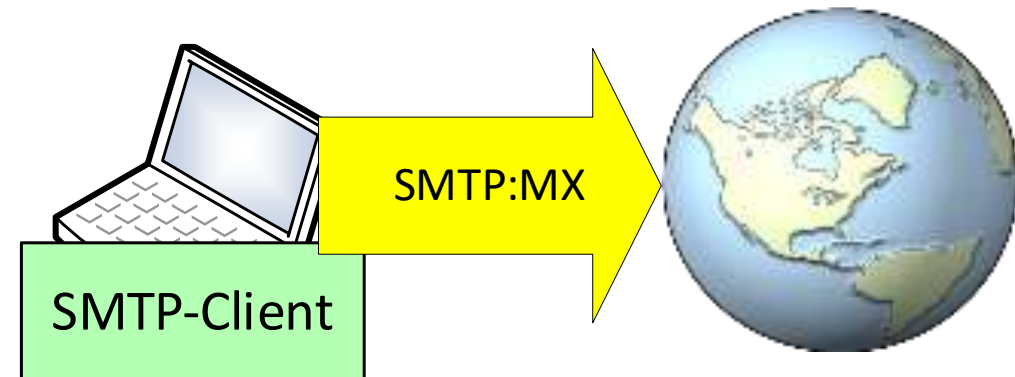
Option 1: OAUTH

- Client kann OAUTH
- Administrator muss AppID zulassen (Consent)
- Client nutzt Username/Kennwort/AppID gegen Entra ID um ein SAML/OAUTH-Token zu holen
- SMTP-Client meldet sich per OAUTH-Token an
- Exchange Online Postfach + Lizenz



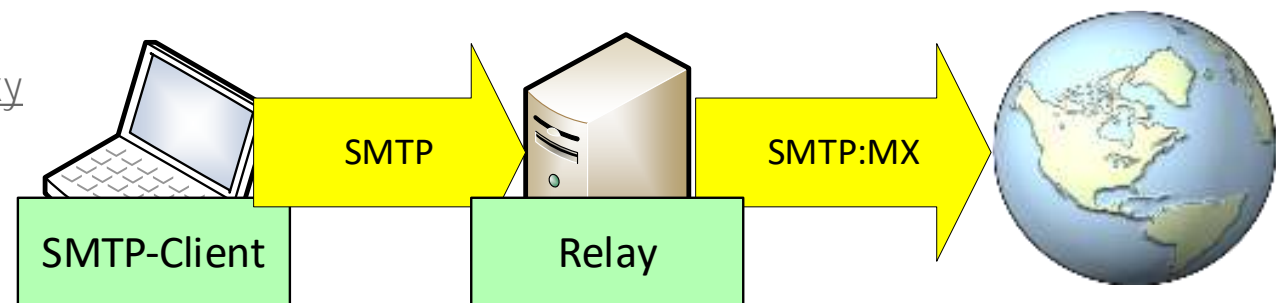
Option 2: Direkter Eigenversand

- Software/Skript sendet selbst
- Firewall-Freischaltung
- DNS-Auflösung: MX-Record
- SPF-Eintrag für die Domain!
- Queuing, Fehlerbehandlung



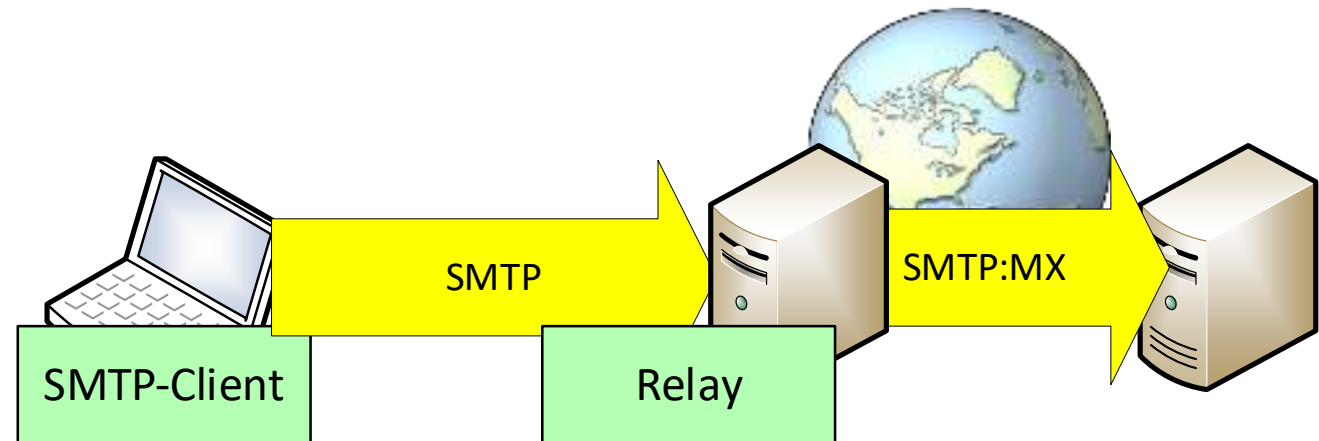
Option 2: Versand über eigenen Smarthost/Relay

- Lokaler SMTP-Server
 - › Postfix, SendMail, Exim
 - › Windows SMTP-Service ist EOL
 - › HMailServer u.a. lange ohne Updates (<https://www.hmailserver.com/state>)
 - › Bestandteil der Firewall
 - › Betriebskosten
- Exchange Hybrid Server
 - › Könnte auch POP3/IMAP4 mit BasicAuth intern bereitstellen
 - › Local Bridgehead für eingehendes SMTP
- SMTP-Proxy mit OAUTH
 - › O2Popper
<https://www.nips.ac.jp/~murata/o2popper/>
 - › Email OAuth 2.0 Proxy
<https://github.com/simonrob/email-oauth2-proxy>
- SPF/DKIM



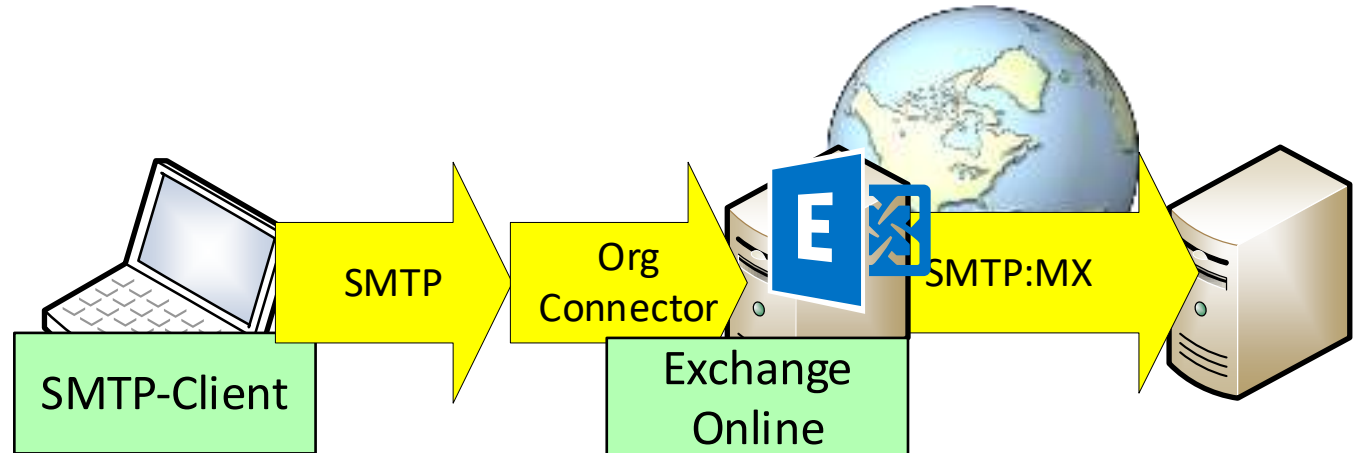
Option 3: Versanddienstleister

- Externe 3rd Party Relays
 - > Azure Communication Services
 - > Amazon AWS SMTP-Relay, SendGrid, MailGun, Mailchimp, etc.
- Webhoster
 - > Meist bieten Sie auch SMTP mit BasicAuth an
 - > Webseiten sendet sowieso per PHP-Mail
- Dran denken
 - > SPF/DKIM
 - > Geeignete Domain



Option 4: Exchange Online Organization Connector

- Achtung: Versender kann sich als „Exchange Server“ ausgeben
- Source-IP oder MTLS mit Zertifikat
- Inbound Org Connector
- Absenderdomain muss in „AcceptedDomain“ sein
- TERRL/ERRL gelten weiter



Nicht vergessen

- Default Domain „<tenant>.onmicrosoft.com“
 - › 100 Mails/Tag-Limit
- TERRL
 - › $9500 + 500 * \text{Lizenzen}^{0,7}$ Mails/Tag
 - › https://www.msxfaq.de/cloud/exchangeonline/transport/terrl_tenant_external_recipient_rate_limit.htm
- ERRL
 - › 1800 Mail/Stunde und max. 10.000/Tag, davon max. 2000 extern
 - › https://www.msxfaq.de/cloud/exchangeonline/transport/mailbox_external_recipient_rate_limit.htm
- Andere Abschaltungen
 - › Okt 2026: EWS-Abschaltung (Option auf April 2027)
 - › Apr 2026: Kerberos AES Default
 - › Jul 2026: UEFI-SecureBoot-Zertifikate



Weitere Links

- [Updated Exchange Online SMTP AUTH Basic Authentication Deprecation Timeline](https://techcommunity.microsoft.com/blog/exchange/updated-exchange-online-smtp-auth-basic-authentication-deprecation-timeline/4489835)
<https://techcommunity.microsoft.com/blog/exchange/updated-exchange-online-smtp-auth-basic-authentication-deprecation-timeline/4489835>
- [Exchange Online to retire Basic auth for Client Submission \(SMTP AUTH\)](https://techcommunity.microsoft.com/blog/exchange/exchange-online-to-retire-basic-auth-for-client-submission-smtp-auth/4114750)
<https://techcommunity.microsoft.com/blog/exchange/exchange-online-to-retire-basic-auth-for-client-submission-smtp-auth/4114750>
- [Exchange Online SMTP BasicAuth Abschaltung](https://www.msxfaq.de/cloud/exchangeonline/betrieb/exchange-online-smtp-basic-auth-abschaltung.htm)
<https://www.msxfaq.de/cloud/exchangeonline/betrieb/exchange-online-smtp-basic-auth-abschaltung.htm>
- [BasicAuth Ende mit POP3/IMAP4 umgehen](https://www.msxfaq.de/cloud/exchangeonline/betrieb/basic-auth-ende-umgehen.htm)
<https://www.msxfaq.de/cloud/exchangeonline/betrieb/basic-auth-ende-umgehen.htm>
- [TERRL - Tenant External Recipient Rate Limit](https://www.msxfaq.de/cloud/exchangeonline/transport/terrl-tenant-external-recipient-rate-limit.htm)
<https://www.msxfaq.de/cloud/exchangeonline/transport/terrl-tenant-external-recipient-rate-limit.htm>
- [Mailbox External Recipient Rate \(ERR\) Limit](https://www.msxfaq.de/cloud/exchangeonline/transport/mailbox-external-recipient-rate-limit.htm)
<https://www.msxfaq.de/cloud/exchangeonline/transport/mailbox-external-recipient-rate-limit.htm>



Vielen Dank für Ihre Aufmerksamkeit.

Net at Work GmbH
Am Hoppenhof 32 A
33104 Paderborn

Kontakt
jane.doe@netatwork.de
john.doe@netatwork.de

Building IT-Excellence.
www.netatwork.de

