

# MS365 Zero Tolerance Microsoft Policy

# Exchange Onprem Version

<https://techcommunity.microsoft.com/blog/exchange/end-of-support-for-exchange-server-2016-and-exchange-server-2019-t-12-months/4268516>

- Dal 14.10.25 le versioni Exch 2016 e 2019 non saranno più supportate né emesse patch da Microsoft
- Nessun blocco verrà applicato a queste versioni, ma non saranno più aggiornate a livello security né Microsoft ne risponderà
- L' unica versione che verrà supportata è la Exchange SE  
<https://techcommunity.microsoft.com/blog/exchange/exchange-server-roadmap-update/4132742>

- We will release one final Cumulative Update (CU) for Exchange Server 2019—the 2024 H2 CU aka CU15—later this year.
- We will release Exchange Server Subscription Edition (Exchange Server SE) early in the third quarter of calendar year 2025.
- We will release the first CU for Exchange Server SE—CU1—in late 2025.

- Si potrà installare come in-place upgrade provenendo da un Exch2019 CU15  
*n.b. livello funzionale AD 2012R2 (come per l' Exch2019)*
- Le licenze per mailbox Onprem verranno migrate come Subscription (come quelle cloud)  
<https://practical365.com/exchange-server-subscription-edition/>  
<https://techcommunity.microsoft.com/blog/exchange/upgrading-your-organization-from-current-versions-to-exchange-server-se/4241305>

**n.b. prevista installazione di due nuovi Exch2019 in round robin per la risoluzione DNS ma senza DAG (prevista dismissione lungo in favore di Tesi entro Settembre, rimangono oltre alle lungo altre 30 mbx Onprem che nessuno ha reclamato)**

# Exchange Online Limits change

<https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#receiving-and-sending-limits>

I limiti di invio cambieranno:

- Fino a oggi erano 10.000 recipients per mailbox nelle 24h, sia che fossero per interne/esterne
- Da Ottobre 2025 diventeranno 8.000 per interni + 2.000 per esterni, o in alternativa 10.000 per interni

Quelli di ricezione invece rimarranno gli stessi:

- max 1.200 mail/ora da stesso mittente, al di là del mittente 3600 mail/ora per mailbox

Per vedere le mailbox che hanno superato il limite in ricezione (nessuna a oggi)

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

Per vedere i mailbox usage (invio/ricezione)

<https://admin.microsoft.com/#/reportsUsage/EmailActivity>

**Top Sender nei 7gg:**

srv2022043@ima.it – SAP Noreply = 17.000 mail INT/3.000 mail EXT

srv2022048@ima.it - noreply.projectarchive@ima.it = 14.000 mail INT/1.000 mail EXT

HdauserH@ima.it = 10.000 mail INT/10.000 mail EXT

srv2023020@ima.it – Noreply IMA ScanToMail = 7.000 mail INT/1.500 mail EXT

srv2020026@ima.it – IMAXfilesService = 8.500 mail INT/4.000 mail EXT

srv2023017@ima.it - Alert Veeam = 1.000 mail INT/ 4.000 mail EXT

srv2024001@ima.it – Alert Veeam2 = 120 mail INT/400 mail EXT

# Basic Authentication deprecation in Cloud

<https://techcommunity.microsoft.com/t5/exchange-team-blog/exchange-online-to-retire-basic-auth-for-client-submission-smtp/ba-p/4114750>  
<https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online>

La Basic Authentication verrà deprecata in cloud dall' 1 Marzo 2026.  
Tutto ciò che si presenterà in cloud con utenza e password «in chiaro» verrà bloccato.

## How will this change happen

In mid-October 2024, we will update the SMTP AUTH Clients Submission Report in the Exchange admin center to show if Basic auth or OAuth is being used to submit email to Exchange Online. In January 2025, we will send a Message Center post to tenants who are using Basic auth with Client Submission (SMTP AUTH) to alert them to the upcoming change. In August 2025, about 30 days before we disable Basic auth we will send another Message Center post to tenants who are still using Basic auth with Client Submission (SMTP AUTH).

During September 2025, we will remove support for Basic auth with the Client Submission (SMTP AUTH) endpoints:

```
smtp.office365.com  
smtp-legacy.office365.com
```

Once Basic auth is permanently disabled, any clients or apps connecting using Basic auth with Client Submission (SMTP AUTH) will receive this response:

```
550 5.7.30 Basic authentication is not supported for Client Submission.
```

E' presente un report che può essere consultato per vedere quali connessioni ancora vanno in Basic Auth  
<https://admin.exchange.microsoft.com/#/reports/smtpauthmailflowdetails>

n.b. il report si aggiorna settimanalmente, Microsoft ne conferma l' attendibilità

# Options available

Abbiamo svariate opzioni, alcune vincolate dai limiti EXO e altre no.

Opzioni che applicano i limiti EXO:

- 1) EXO Connectors
- 2) Azure App Registration (Graph)
- 3) High Volume Email (HVE)

Opzioni completamente svincolate dai limiti EXO:

- 4) Azure Communication Services (ACS)

Opzione onprem vincolata dai limiti settati sul mail flow onprem:

- 5) Exchange Server (anonymous o no)

Ciascuna di queste scelte ha pro e contro.

Andiamo ad analizzarli insieme nelle prossime slide.

# 1) EXO Connectors

<https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365#option-3-configure-a-connector-to-send-emails-using-microsoft-365-or-office-365-smtp-relay>

Si può creare un connettore che accetta tutto il traffico posta da uno specifico IP pubblico.  
Se una filiale esce con uno specifico IP pubblico il connettore può essere configurato in questo modo

## Mail flow scenario

From: Your organization's email server

To: Office 365

## Name

Receive Connector

## Status

On

[Edit name or status](#)

## How to identify email sent from your email server

Identify incoming messages from your email server by verifying that the sending server's IP address is within these IP address ranges: XX.XX.XX.XX and the sender's or recipient's email address is an accepted domain for your organization.

[Edit sent email identity](#)

## Pro:

Tutti i relay posta della filiale escono così, non serve entrare nel dettaglio di ognuno.  
Non usando la Basic Auth continuerà ad essere accettata.

## Contro:

Comporta un rischio security, chiunque sia connesso dalla filiale potrà fare relay verso Office365.  
Se si superano i limiti è facile essere blacklistati da Microsoft.  
E' soggetto ai limiti EXO per cui:

- max 1.200 mail/h da singolo mittente, 3600 mail/h per mbx
- max 8.000 invii interni + 2.000 esterni/10.000 interni

## 2) Azure App Registration con Graph

[Send Mail with PowerShell and Microsoft Graph API - TechGuy](#)

E' possibile definire una Azure App Registration a cui applicare permessi di lettura/scrittura filtrati per una singola mailbox.

A questo punto è possibile da powershell graph utilizzare la mailbox per spedire, collegandosi alla Azure App tramite i suoi AppID e SecretKey.

### **Pro:**

Utilizza una mailbox cloud consultabile

Il Secret Key è impostato con scadenza ciclica, aumentando la security

### **Contro:**

Può essere invocata solo da script

E' comunque soggetta ai limiti EXO (8.000+2.000/10.000 recipients in invio)

Necessita di una licenza cloud EXO per la mailbox utilizzata

Il Secret Key va rinnovato nel codice ciclicamente

### 3) HVE – High Volume Email

<https://learn.microsoft.com/en-us/Exchange/mail-flow-best-practices/high-volume-mails-m365>

Sono account pure cloud (senza mailbox annessa) che è possibile creare per invii principalmente ad interni.

<https://admin.cloud.microsoft/exchange#/highvolumeemail>

*n.b. Basic Authentication da abilitare sull' utente HVE, Microsoft ha confermato verrà ritirata a Settembre 2028*

Per spedire impostare:

Server : smtp-hve.office365.com

Port : 587

Authentication : Username (email address of the HVE account) and password

TLS/STARTTLS : TLS 1.2 or TLS 1.3

#### **Pro:**

Non necessitano di licenze EXO cloud

Facili da gestire come oggetti, sono di fatto mail user cloud

Nessun limite sugli invii interni

Basic Auth accettata fino a Settembre 2028

#### **Contro:**

Invii esterni bloccati

Max 100 HVE accounts per tenant

Max message size 10 Mb

Al momento free, a regime si pagherà per il n.ro di email inviate (sotto il link per gli ACS, non si ancora per gli HVE)

<https://azure.microsoft.com/en-us/pricing/calculator/> Es. 10K di mail da 10 Mb l' una = 15\$

## 4) ACS – Azure Communication Services

<https://learn.microsoft.com/en-us/azure/communication-services/quickstarts/email/send-email>

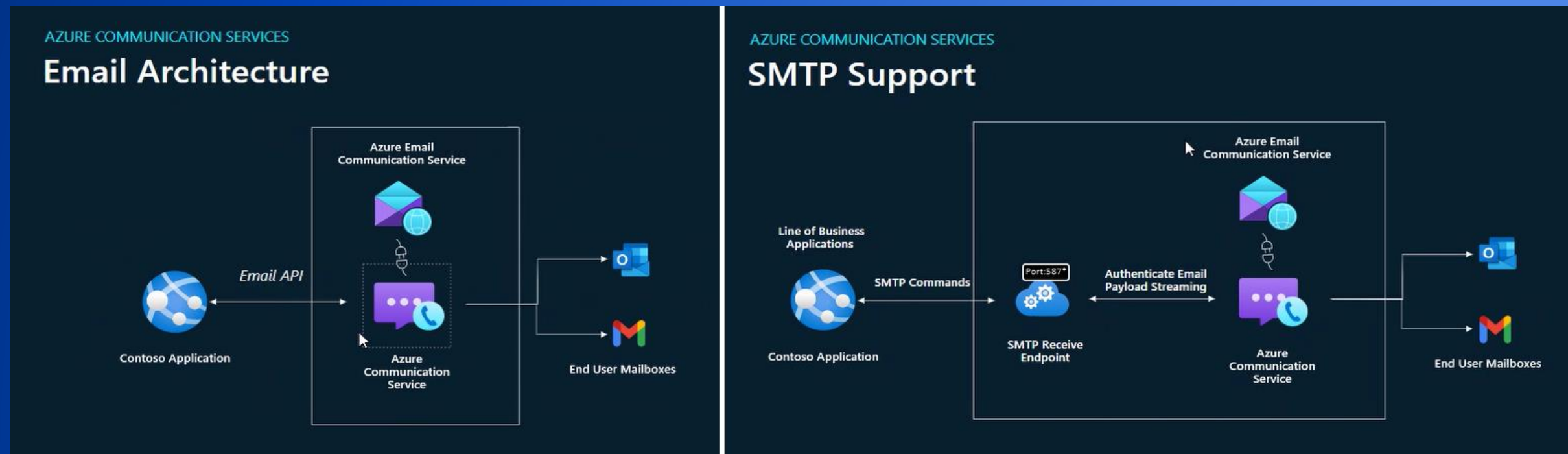
Gli ACS sono l'alternativa migliore se si vuole spedire a esterni senza essere legati a vincoli EXO.

Prevede la creazione di un Azure Email Communication Services Resource, connessa al dominio da cui si vuole spedire (dominio che deve essere tra gli Accepted del tenant).

<https://learn.microsoft.com/en-us/azure/communication-services/quickstarts/email/create-email-communication-resource?pivots=platform-azp>  
<https://learn.microsoft.com/en-us/azure/communication-services/quickstarts/email/connect-email-communication-resource?pivots=azure-portal>

Può essere acceduto tramite API da Azure App (ACS), o tramite servizio SMTP (ECS)

L'ECS richiede la creazione anche di una Entra App con accesso alla Azure Resource



# ECS – Azure Email Communication Services

<https://learn.microsoft.com/en-us/azure/communication-services/quickstarts/email/send-email-smtp/smtp-authentication>

<https://learn.microsoft.com/en-us/azure/communication-services/quickstarts/email/send-email-smtp/send-email-smtp>

Step by step creation



## Email

*How to onboard – explained in simple steps*

*Steps are not exhaustive. Please refer to our Quick Start section for more details.*

- 1** Create email comm. resource 
- 2** Add and verify custom domains, and add sender addresses 
- 3** Create azure comm. resource and connect domain(s) 
- 4** Send test email with our "Try email" blade 
- 5** Set-up SMTP Auth and send email using SMTP 
- 6** Set-up ACS email logs, insights, and/or subscribe to real-time events 

Per spedire impostare:

Server: smtp.azurecomm.net

Port: 587

TLS/StartTLS: Abilitato

Username: <ACSResourceName>.<EntraAppID>.<TenantID>

Password: client secret.

# Explanation

1 - creazione Email Communication Service resources (oggetto che spedisce)

<https://learn.microsoft.com/en-us/azure/communication-services/quickstarts/email/create-email-communication-resource?pivots=platform-azp>

2 - Add and verify Custom Domain (per poter usare il proprio dominio Custom)

<https://learn.microsoft.com/en-us/azure/communication-services/quickstarts/email/connect-email-communication-resource?pivots=azure-portal>

3 - Creazione Azure Communication Resource (oggetto che richiama l' ECS per spedire)

<https://learn.microsoft.com/en-us/azure/communication-services/quickstarts/create-communication-resource?tabs=windows&pivots=platform-azp>

4 - Try Email

<https://learn.microsoft.com/en-us/azure/communication-services/quickstarts/email/send-email?tabs=windows%2Cconnection-string%2Csend-email-and-get-status-async%2Csync-client&pivots=platform-azportal>

5 – Create Entra App and Set up SMTP Auth (si legherà all' ACS aggiungendolo come permissions – vedi 2° link sotto)

[Register a Microsoft Entra app and create a service principal - Microsoft identity platform | Microsoft Learn](#)

<https://learn.microsoft.com/en-us/azure/communication-services/quickstarts/email/send-email-smtp/smtp-authentication>

6 - Eventuale Log Analyzer (per il trace basta quello EXO)

# Pro e Contro

## Pro:

Non è soggetto ai vincoli EXO sull' inviato/ricevuto.

Non necessita di licenze Exchange non usando mailbox per spedire.

I limiti presenti possono essere alzati con ticket a Microsoft (valuterà la situazione prima di procedere)

<https://learn.microsoft.com/en-us/azure/communication-services/concepts/email/email-quota-increase>

Email quota increase requests aren't automatically approved. The reviewing team considers your overall sender reputation when determining approval status. Sender reputation includes factors such as your email delivery failure rates, your domain reputation, and reports of spam and abuse.

## Contro:

password a 40 caratteri, troppo lunga per SMTP Legacy mask

Richiede accessi tramite Oauth 2.0, non supportato da molti device

Max 100 mail per ora

Max 50 recipients ad invio (aumentabile fino a 200)

Al momento free, a regime si pagherà per il n.ro di email inviate (andare in fondo nel link sotto)

<https://azure.microsoft.com/en-us/pricing/calculator/>

Es. 10K di mail da 10 Mb l' una = 15\$

# Conclusione

## ACS (Azure Communication Services)

- Se devono inviare a interni ed esterni
- Se accettano la password a 40 caratteri
- Non necessitano di mailbox di servizio
- Supportano la OAuth 2.0

## HVE (High Volume Email)

- Se devono inviare solo ad interni
- Non necessitano di mailbox di servizio
- Accettano solo la Basic Auth (attiva SOLO per gli HVE fino a Settembre 2028)

## App Registration (necessaria licenza cloud per mailbox)

- Se devono inviare a interni ed esterni
- Necessitano di mailbox di servizio
- Lavorano solo tramite script
- Supportano la OAuth 2.0

## Exchange Server on-prem (necessaria licenza cloud per mailbox)

- Se devono inviare a interni ed esterni
- Necessitano di mailbox di servizio
- Accettano solo l'anonimo

PREFERRED ACS!

È quello che avrà meno cambiamenti futuri e nessun blocco dichiarato

Per customizzarlo bisogna aprire un ticket a Microsoft con esempio pratico e valuteranno se procedere o no

### **ATTENZIONE:**

**Note: The Email Limits can only be increased for when the Custom Domain has been used for at least 2 weeks and generated traffic with failure rate less than 1%.**

# Next Change

## Aprile 2025

- SPF/DKIM/DMARC richiesto, Outlook si è unito a Gmail/Yahoo/Live nei check in ingresso
- Se il mittente invia più di 5.000 mail al giorno e non ha i record sopra compilato correttamente verrà inizialmente messo in Junk, poi rifiutato. Altri checks saranno
  - Che il from sia allineato con il reply-to come dominio di invio
  - In caso di newsletter il pulsante Unsubscribe deve essere visibile nella mail
  - Deceptive headers rientreranno nel blocco sopra

## Maggio 2025

- Numero massimo mail giornaliere per tenant =  $[500 * (n.ro\_licenze^{0.7}) + 9500]$

## Ottobre 2025

- Exchange Legacy token disabilitati
- Exchange Server 2016 e 2019 non più patchati

## Ottobre 2025 (nuovi tenant)/Ottobre 2026 (tenant già esistenti)

- Max 10.000 mail giornaliere per mailbox/indirizzo, o tutte interne o 8.000 interne e 2.000 esterne

## Marzo 2026

- Blocco Basic Authentication in cloud (eccetto per gli HVE fino a Settembre 2028)

## Ottobre 2026

- EWS disabilitati online, migrare a Microsoft Graph  
<https://admin.microsoft.com/Adminportal/Home#/reportsUsage/EWSWeeklyUsage>

N.ro_licenze	Tenant External RecipientRate Limit 24h
1	10.000
2	10.312
10	12.006
25	14.259
100	22.059
1.000	72.446
10.000	324.979
100.000	1.590.639