

Produkt: NetOrchestra® MA

Kurzbeschreibung: Archivierung aus Exchange Online konfigurieren

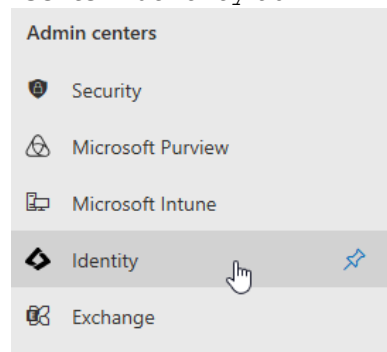
*Diese Anleitung hilft Ihnen, das nachfolgend geschilderte Problem zu beheben. Dazu sollten Sie über gute bis sehr gute Kenntnisse im Betriebssystem Windows verfügen. Im Zweifelsfall empfehlen wir, einen Spezialisten hinzuzuziehen. **Die com2 Communications & Security GmbH gibt keine Funktionsgarantie und übernimmt keine Haftung für Schäden oder Verlust an Hard- oder Software und/oder Datenbeständen, die durch Anwendung dieser Anleitung entstehen könnten.***

Benutzerpostfacharchivierung über Graph API

Unternehmensanwendung erstellen

Die Authentifizierung des Mailarchives (MA) an Microsoft 365 erfolgt über OAuth2. Hierzu muss zunächst eine Unternehmensanwendung erstellt werden:

- Rufen Sie das Entra Admin Center Identity auf.



- Wechseln Sie in die Ansicht Entra ID > App registrations und klicken auf [New registration]



- Vergeben Sie der Anwendung einen Namen, belassen die anderen Einstellungen und klicken auf [Register].

* Name

The user-facing display name for this application (this can be changed later).

NetOrchestra Mailarchiv ✓

Supported account types

Choose the account types that can use this application or access this API

Single tenant only - com2test

[Help me choose](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform e.g. <https://example.com/auth>

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

- Notieren Sie sich aus der Übersichtsseite der Anwendung die Application (client) ID und die Directory (tenant) ID.

^ Essentials

Display name
[NetOrchestra Mailarchiv](#)

Application (client) ID

Object ID

Directory (tenant) ID

Supported account types
[My organization only](#)

Client credentials
[Add a certificate or secret](#)

Redirect URIs
[Add a Redirect URI](#)

Application ID URI
[Add an Application ID URI](#)

Managed application in local directory
[NetOrchestra Mailarchiv](#)

- Klicken Sie nun auf Add a certificate or secret..

^ Essentials

Display name
[NetOrchestra Mailarchiv](#)

Application (client) ID

Client credentials
[Add a certificate or secret](#)

Redirect URIs
[Add a Redirect URI](#)

- ..und dann auf [New client secret].

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token

+ New client secret

Description	Expires	Value
New client secret		

No client secrets have been created for this application.

- Geben Sie eine Beschreibung an, wählen die Gültigkeitsdauer des Client Secrets aus und klicken auf [Add].

Nach Ablauf muss ein neues Client-Secret erstellt werden.

Add a client secret

Description

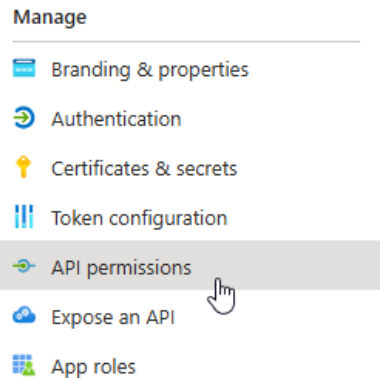
Expires

- Notieren Sie sich das Client-Secret. Nun haben Sie alle Informationen für die Konfiguration auf dem Mailarchiv.

Description	Expires	Value	Copy to clipboard	et ID
NetOrchestra Mailarchiv	7/9/2027	U1G8Q...	AR...	051a1b83-b8c7-4705-a2f7-dd9b...

API-Berechtigungen zuweisen

- Öffnen Sie für die neu erstellte Anwendung die Ansicht API permissions.



- Klicken Sie auf [Add a permission] und wählen unter Microsoft Graph > Application permissions folgende aus:
 - o Mail.ReadWrite
 - o User.ReadBasic.All

☒	Mail.ReadWrite ⓘ Read and write mail in all mailboxes	Yes
☒	User.ReadBasic.All ⓘ Read all users' basic profiles	Yes

- Klicken Sie auf [Grant admin consent for <domain>] > [Yes]. Der Status sollte überall grün sein.

+ Add a permission ✓ Grant admin consent for com2test

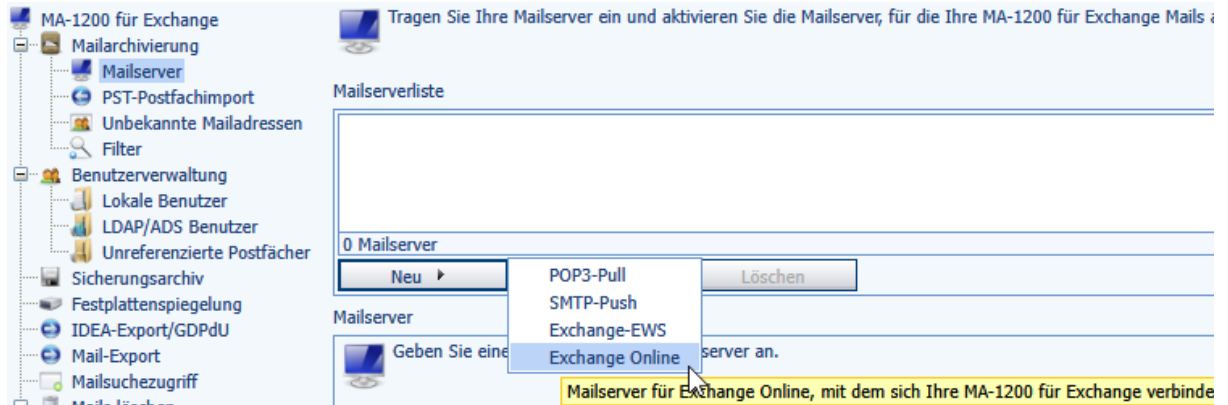
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✓ Granted for com2test
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for com2test
User.ReadBasic.All	Application	Read all users' basic profiles	Yes	✓ Granted for com2test

Mailserver-Eintrag hinzufügen

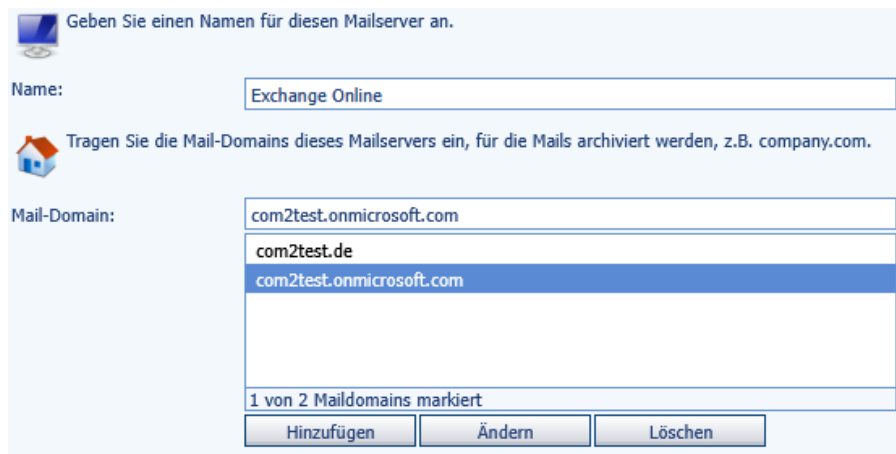
Die Konfiguration erfolgt auf der Admin-Weboberfläche des Mailarchives:

<https://<MA-Adresse>/admin>

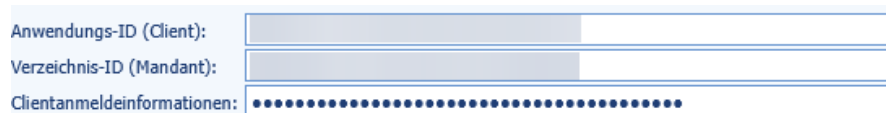
- Öffnen Sie die Ansicht Mailarchivierung > Mailserver.
- Erstellen Sie einen neuen Mailserver-Eintrag. [Neu] > Exchange Online.



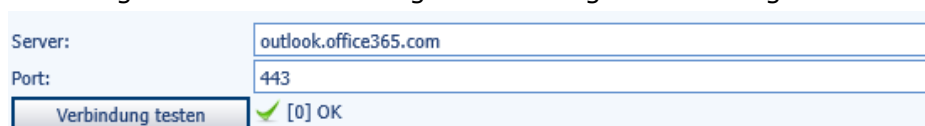
- **Name:** Vergeben Sie für den Listeneintrag einen Anzeigenamen.
- **Mail-Domain:** Geben Sie alle Maildomänen an, für die archiviert werden soll.



- **Anwendungs-ID (Client):** Die zuvor notierte ID der Unternehmensanwendung.
- **Verzeichnis-ID (Mandant):** Die zuvor notierte ID des M365 Tenants.
- **Clientanmeldeinformationen:** Das für die Anwendung erstellte Client-Secret.



- Speichern Sie die Konfiguration. (Diskette in Symbolleiste)
- Mit der Schaltfläche [Verbindung testen] prüfen Sie, ob mit den eingegebenen Daten erfolgreich eine Verbindung mit Exchange Online hergestellt werden kann.



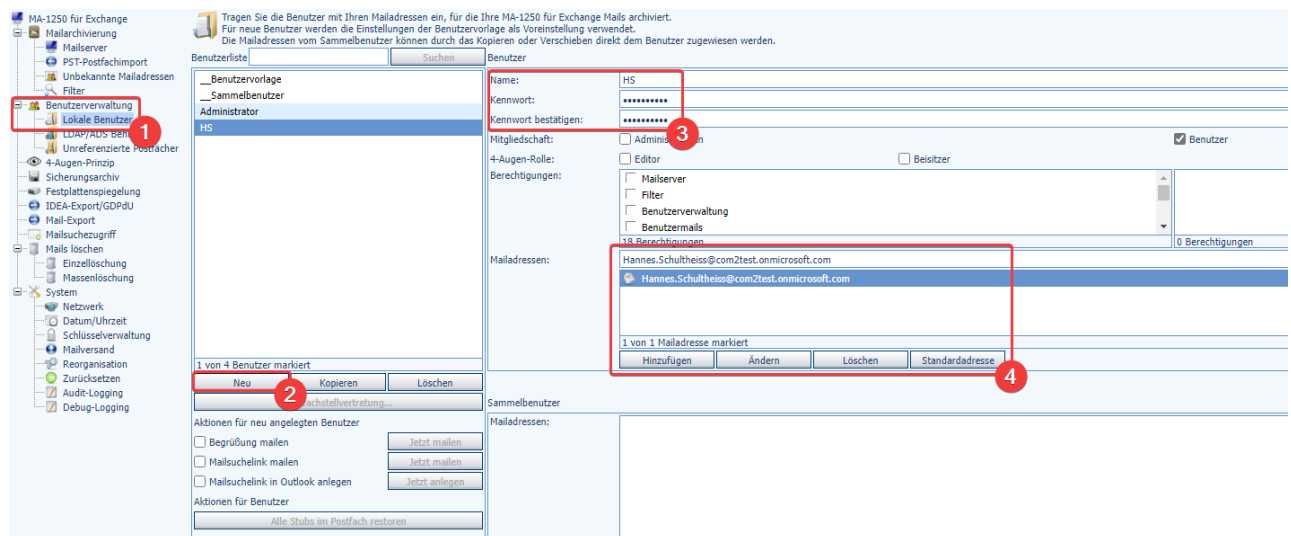
- Lassen Sie die Archivierung vorerst noch deaktiviert.

Benutzer hinzufügen

Für alle zu archivierenden Postfächer müssen die dazugehörigen Mailadressen in der Benutzerverwaltung einem Benutzer zugewiesen sein.

Werden diese per LDAP nicht importiert, können Sie dazu lokale Benutzer erstellen:

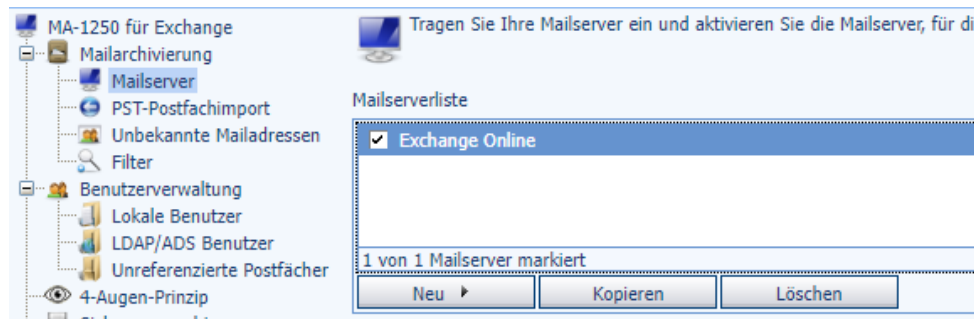
- Wechseln Sie in die Ansicht Benutzerverwaltung > Lokale Benutzer (1)
- Legen Sie mit [Neu] einen neuen Benutzer an. (2)
- Vergeben Sie einen Namen und ein Kennwort. Diese Daten werden für die Anmeldung an der Mailsuche verwendet. (3)
- Fügen Sie dem Benutzer alle seine Mailadressen hinzu. (4)



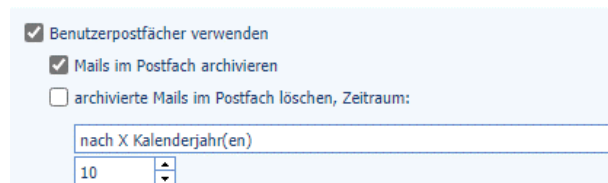
Benutzerpostfacharchivierung aktivieren

Ist alles vorbereitet, kann die Archivierung aktiviert werden.

- Öffnen Sie die Ansicht Mailarchivierung > Mailserver.
- Aktivieren Sie in der Mailserverliste die Checkbox für den neu erstellten Mailserver-Eintrag.



- Aktivieren Sie die Checkboxes für Benutzerpostfächer verwenden und Mails im Postfach archivieren.



Nachdem Sie die Konfiguration gespeichert haben, werden zunächst nicht sichtbare Suchordner in den Benutzerpostfächern erstellt. Nach wenigen Minuten sollten die ersten Mails archiviert werden.

Hinweis: Möchten Sie die Anhänge aus den archivierten Mails stubben, kontaktieren Sie bitte unsere Support-Hotline.

Journalpostfacharchivierung (empfohlen / optional)

Löscht ein Benutzer eine Mail bevor diese archiviert werden konnte, kann diese noch aus dem Journalpostfach archiviert werden.

Mit einer Journalregel werden alle ein- und ausgehenden Mails an ein Journalpostfach gesendet. Das Mailarchiv holt sich die Mails aus dem Postfach ab und entfernt diese nach erfolgreicher Archivierung aus dem Postfach.

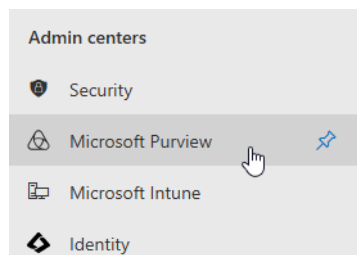
Voraussetzung bei Exchange Online ist das sich das Journalpostfach außerhalb der eigenen Organisation befinden muss, dessen Mailserver mit dem Mailarchiv angebunden werden müsste. In hybriden Umgebungen darf sich das Postfach auf dem OnPrem-Server befinden. Lesen Sie bitte die Sektion *Journaling in hybride Umgebungen*.

Alternativ besteht die Möglichkeit per Transportregel jeder Mail ein organisationsinternes Journalpostfach als BCC-Empfänger beizufügen. Bitte beachten Sie, dass bei dieser Methode keine Envelope-Informationen übergeben werden. Daher gilt diese Lösung als Workaround, wenn kein externes Postfach für das Journaling zur Verfügung steht.

Im Folgenden wird die Konfiguration beider Varianten beschrieben.

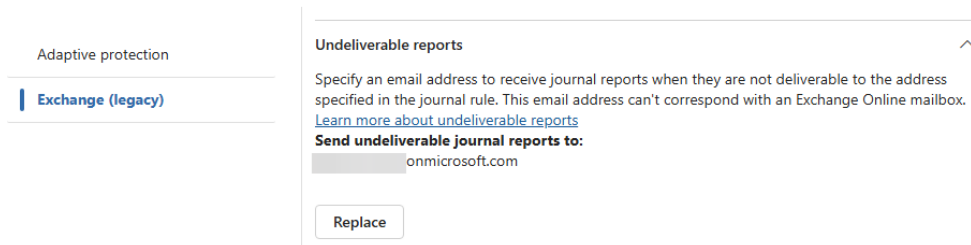
Variante 1 - Journalregel:

- Die Konfiguration erfolgt in Microsoft Purview.

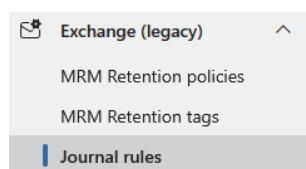


- Rufen Sie **Settings** > Data Lifecycle Management > Exchange (legacy) auf.
- Geben ein Postfach für Unzustellbarkeitsberichte an. Das Postfach sollte Ihrer Microsoft365-Domäne angehören.

Data Lifecycle Management settings



- Rufen Sie **Solutions** > Data Lifecycle Management > Exchange (legacy) > Journal rules auf.



- Klicken Sie auf [New Rule] und geben das externe Journalpostfach an.
- Wählen Sie Everyone und All messages aus.

Journal rule settings

Messages matching the rule's conditions will be delivered to the journaling address specified in the rule. [Learn more to manage journaling in Exchange Online](#)

Send journal reports to *

Journal@com2.de

Journal rule name *

[Apply to all messages]

Journal messages sent or received from *

☒ Everyone

☐ A specific user or group

Type of message to journal *

☒ All messages

☐ Internal messages only

☐ External messages only

Next Cancel

- Klicken Sie auf [Next] und [Submit].

+ New rule Edit Delete Disable Refresh

Name	Status	User
☒ Journal	On	

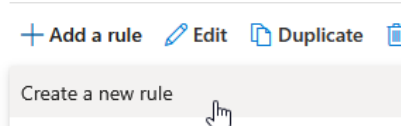
Hinweis:

Achten Sie darauf das die Regel aktiviert ist (Status = On). Es ist empfehlenswert die Funktionalität der Journalregel zu prüfen.

Variante 2 - Transportregel:

Bei diesem Workaround werden keine Envelope-Informationen an das Journalpostfach gesendet. Ist wie im Falle von Spammails der in der Mail dargestellte Absender nicht der im Envelope aufgeführte bzw. nicht der tatsächliche Absender, kann dies nicht widerlegt werden. Zudem fehlen BCC-Informationen um die BCC-Archivierung unterstützen zu können.

- Die Konfiguration erfolgt im Exchange Admin Center.
- Wechseln Sie in die Ansicht Mailflow > Rules und fügen eine neue Regel hinzu.



- **Name:** Vergeben Sie der Regel einen Namen.

Name *

- **Apply this rule if:** Apply to all messages
- **Do the following:** Add recipients > to the Bcc box > Wählen Sie das Journalpostfach aus.
- **Except if:** The message properties > Include the message type > Calendering

Name *

Apply this rule if *

Apply to all messages ▼ Select one ▼ +

Do the following *

Add recipients ▼ to the Bcc box ▼ +

Blind carbon copy (bcc) the message to :

Except if

The message properties ▼ include the message type ▼ +

The message type is 'Calendering'

- Klicken Sie auf [Next].
- Die Einstellungen auf der nächsten Seite sind Ihnen überlassen.
- Klicken Sie, wenn Sie fertig sind, auf [Next] und [Finish].
- Prüfen Sie ob die Regel aktiviert ist und funktioniert.

Journaling in hybride Umgebungen

In einer hybriden Umgebung kann folgende Konstellation an Journalregeln konfiguriert werden:

- Exchange Online sendet Journalmails an ein OnPrem-Postfach.
- OnPrem Exchange sendet an das gleiche OnPrem-Postfach.

Nur wenn auf beiden Seiten eine Journalregel konfiguriert ist, ist sichergestellt das für alle Postfächer Journalmails generiert werden.

(!) Dies kann jedoch auch zu Problemen führen:

1. Doppelte Journalberichte

Hat eine der beiden Endpunkte für eine Mail bereits eine Journalmail versendet, wird in den Header der originalen Mail ein Flag gesetzt. Erfahrungsgemäß kann es passieren, das dieses Flag ignoriert wird und beide Gegenstellen eine Journalmail senden und somit doppelt im Postfach landet. I.d.R. sind diese Mails identisch und werden vom Archiv als Dubletten erkannt.

Lösung:

Von Microsoft gibt es zu diesem Thema einen Beitrag: [Journale in Exchange Online | Microsoft Learn](#)

2. Es werden Journalberichte für Journalberichte erstellt

Sendet Exchange Online eine Journalmail an ein auf OnPrem gehostetes Journalpostfach, erstellt der OnPrem-Server aufgrund der eingehenden Mail ebenfalls eine Journalmail.

Resultierend landen im Journalpostfach zwei Mails:

- Die Journalmail von Exchange Online mit der originalen Mail als Anhang.
- Die Journalmail von OnPrem mit der Exchange Online Journalmail als Anhang.

Da sich die Mails unterscheiden, werden diese nicht als Dublette erkannt und somit zweimal archiviert.

Lösung:

Erstellen Sie eine neue Mailbox-Datenbank und verschieben das Journalpostfach auf diese.

- Für diese Datenbank bleibt das Journaling deaktiviert.
- Für die Datenbank der Benutzerpostfächer bleibt das Journaling aktiviert.

Vorgehensweise:

- Öffnen Sie das Exchange Admin Center (ECP) des OnPrem-Servers
- **Datenbank erstellen:** Server > Datenbanken > [+]
- **Postfach verschieben:** Empfänger > Postfächer > Journalpostfach selektieren > Postfach verschieben: In eine andere Datenbank.
- **Journaling:** Server > Datenbanken
 - o Öffnen Sie die Konfiguration beider Datenbanken > Wartung.
 - o Für die neue DB darf bei Journalempfänger nichts drinnen stehen.
 - o Für die bestehende Benutzerpostfachdatenbank steht hier das Journalpostfach.

Journalpostfacharchivierung aktivieren

Fügen Sie einen neuen Mailserver-Eintrag für den Mailserver hinzu, auf dem sich das Journalpostfach befindet.

Hinweis: Befindet sich das Journalpostfach auf Exchange Online, können Sie dieses in dem Mailservereintrag für Exchange Online angeben.

- Wechseln Sie in die Ansicht `Mailarchivierung > Mailserver`.
- Klicken Sie in der Mailserverliste auf `[Neu]` und wählen den für den Mailserver passenden Servertyp aus.
- **Name:** Vergeben Sie für den Listeneintrag einen Anzeigenamen.
- **Mail-Domain:** Geben Sie alle Maildomänen an, für die archiviert werden soll.
- Geben Sie die Verbindungsdaten des Mailservers an.

Mailserverliste

☒ Exchange Online
☒ Exchange-Online Journaling

1 von 2 Mailserver markiert

Neu Kopieren Löschen

Mailserver

Geben Sie einen Namen für diesen Mailserver an.

Name: Exchange-Online Journaling

Tragen Sie die Mail-Domains dieses Mailservers ein, für die Mails archiviert werden, z.B. company.com.

Mail-Domain: com2test.onmicrosoft.com

1 Maildomain

Hinzufügen Ändern Löschen

Tragen Sie den EWS-Server ein. Wenn Sie On-Premises verwenden geben Sie den voll qualifizierten Rechnernamen oder die IP-Adresse an, z.B. company.com oder 10.0.0.15. Wenn Sie Office365 verwenden sind die Werte von Microsoft vorgegeben.

Servertyp: ☒ On-Premises ☐ Office365

EWS-Server: 10.5.5.235

EWS-Port: 443

Verbindung testen

Tragen Sie den Benutzer für die Impersonierung ein.

Authentifizierung: ☐ Negotiate ☒ NTLM

Domäne: com2test.de

Benutzer: Administrator

Kennwort:

- Aktivieren Sie die Checkbox für `Journalpostfach verwenden`.
- Geben Sie die Mailadresse des Journalpostfaches an.

☒ Journalpostfach verwenden

Mailadresse: Journal@com2test.de

Ist in der Mailserverliste die Checkbox für den Mailserver aktiviert, sollten nach Speichern der Konfiguration die ersten Mails aus dem Journalpostfach abgeholt werden.

Benutzerpostfacharchivierung über EWS

Ab Oktober 2026 wird EWS in Exchange Online organisationsweit deaktiviert, kann aber vorübergehend wieder aktiviert werden. **Ab April 2027 wird EWS komplett abgeschaltet.**

EWS reaktivieren

Bis April 2027 kann EWS mit Hilfe der Powershell wieder aktiviert werden, indem Sie ein Liste der für EWS erlaubten Anwendungen erstellen.

```
Install-Module ExchangeOnlineManagement -Scope CurrentUser
Connect-ExchangeOnline
Get-OrganizationConfig | Select-Object *EWS*
Set-OrganizationConfig -EwsEnabled $true
Set-OrganizationConfig -EwsAllowedAppIDs "<AppID>"
```

Hinweis: Geben Sie in dem letzten Command die Applikations-ID der zuvor erstellten Unternehmensanwendung an.

Mehr zu dem Thema finden Sie in den folgenden Artikeln:

- [Exchange Online EWS, Your Time is Almost Up | Microsoft Community Hub](#)
- [Introducing EWSAllowedAppIDs: Preparing for the Final Phase of EWS Retirement | Microsoft Community Hub](#)

API-Berechtigungen der Unternehmenanwendung

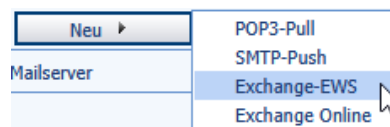
Für EWS wird eine andere API-Permission benötigt. Die Graph Permissions werden nicht gebraucht.

Öffnen Sie in M365 > Identity die für das Mailarchiv erstellte Unternehmensanwendung und wechseln in die Ansicht der API-Permissions. Fügen Sie folgende Permission hinzu:

APIs my organization uses > Office 365 Exchange Online > Application Permissions > full_access_as_app

Mailservereintrag auf dem Mailarchiv hinzufügen

- Öffnen Sie die Admin-Weboberfläche und wechseln in die Ansicht Mailserver.
- Fügen einen Mailservereintrag des Typs Exchange-EWS hinzu.



- **Name:** Vergeben Sie für den Listeneintrag einen Anzeigenamen.
- **Mail-Domain:** Geben Sie alle Maildomänen an, für die archiviert werden soll.
- **Server-Typ:** Exchange Online
- **Authentifizierung:** OAuth2
- Geben Sie die Anwendungs-ID, Verzeichnis-ID und das Client-Secret an.
- Läuft der Verbindungstest erfolgreich durch und sind die Benutzer konfiguriert, können Sie die Archivierung starten.