

Produkt: NetOrchestra® MA
Kurzbeschreibung: **Archivierung eines Office365 Postfaches konfigurieren**

Für den Zugriff und Archivierung von Office365 Postfächern werden die beiden Authentifizierungsmethoden OAuth2 und Basic (ab Oktober 2022 deprecated) unterstützt.

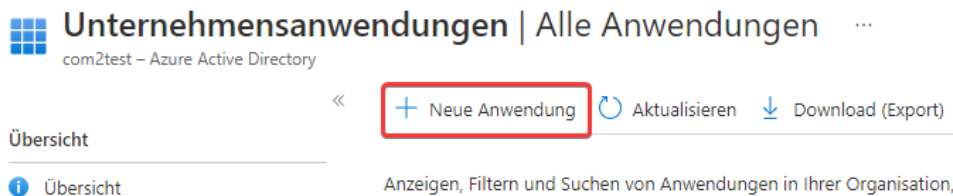
Dieses Dokument begleitet Sie dabei wie Sie die NetOrchestra MA über die jeweilige Authentifizierungsmethode mit Exchange Online verbinden.

Vorbereitungen für den Zugriff über OAuth2 in Exchange Online

Melden Sie sich mit Ihrem Webbrowser bei Exchange Online an und rufen im Admin Center das Azure Active Directory Portal auf. (Direktlink: <https://aad.portal.azure.com/>)

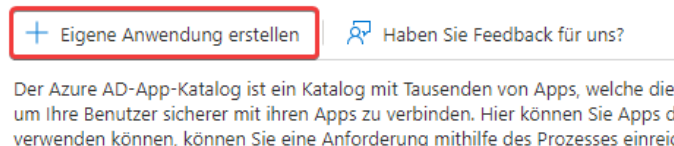
Unternehmensanwendung erstellen

Im Ersten Schritt wird eine neue Unternehmensanwendung benötigt. Navigieren Sie zu „Alle Dienste“ > „Unternehmensanwendungen“ und klicken auf [+ Neue Anwendung].



Klicken Sie auf der Folgeseite auf [+Eigene Anwendung erstellen].

Azure AD-Katalog durchsuchen



Vergeben Sie der Anwendung einen beliebigen Namen und wählen die Option „Register an application to integrate with Azure AD (App you’re developing)“ aus.

Wie lautet der Name der App?

Was haben Sie mit Ihrer Anwendung vor?

- Anwendungsproxy für sicheren Remotezugriff auf eine lokale Anwendung konfigurieren
- Register an application to integrate with Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

Klicken Sie im Abschluss auf [Erstellen].

Sie gelangen nun in die Ansicht „Anwendung Registrieren“.

* Name

Der dem Benutzer gezeigte Anzeigename für diese Anwendung. (Dieser kann später geändert werden.)

Unterstützte Kontotypen

Wer kann diese Anwendung verwenden oder auf diese API zugreifen?

- Nur Konten in diesem Organisationsverzeichnis (nur "com2test" – einzelner Mandant)
- Konten in einem beliebigen Organisationsverzeichnis (beliebiges Azure AD-Verzeichnis – mehrinstanzenfähig)
- Konten in einem beliebigen Organisationsverzeichnis (beliebiges Azure AD-Verzeichnis – mehrinstanzenfähig) und persönliche Microsoft-Konten (z. B. Skype, Xbox)
- Nur persönliche Microsoft-Konten

[Entscheidungshilfe...](#)

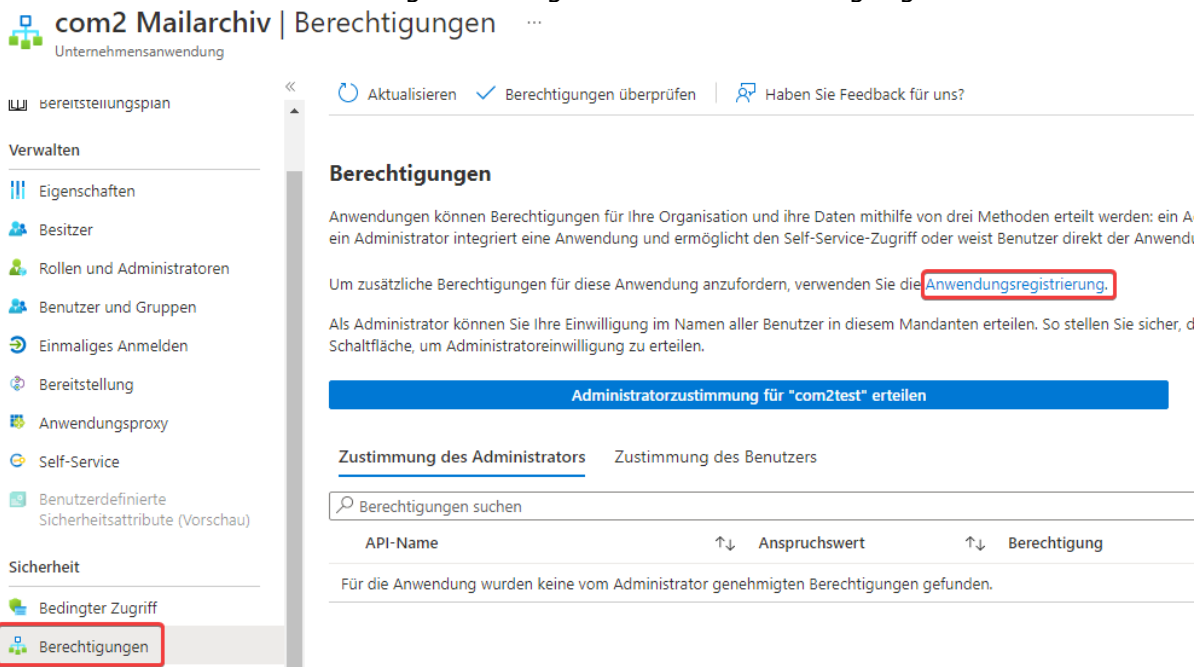
Umleitungs-URI (optional)

Die Authentifizierungsantwort wird nach erfolgreicher Authentifizierung des Benutzers an diesen URI zurückgegeben. Die Angabe ist zum jetzigen Zeitpunkt optional und kann später geändert werden. Für die meisten Authentifizierungsszenarien ist jedoch ein Wert erforderlich.

Die angebotenen Default-Einstellungen können beibehalten werden, sodass Sie direkt auf [Registrieren] klicken können.

Der Anwendung Berechtigungen zuweisen

Im nächsten Schritt müssen die Berechtigungen der Anwendung ergänzt werden. Klicken Sie hierzu in der Ansicht „Unternehmensanwendungen“ > „Alle Anwendungen“ auf die neu erstellte Anwendung und navigieren zu den Berechtigungen.



The screenshot shows the 'Permissions' page for the application 'com2 Mailarchiv'. The left-hand navigation pane has 'Berechtigungen' (Permissions) highlighted. The main content area shows instructions on how to grant permissions, including a link to 'Anwendungsregistrierung' (Application Registration) which is highlighted with a red box. Below the instructions, there is a blue button 'Administratorzustimmung für "com2test" erteilen' (Grant administrator consent for "com2test"). Underneath, there are tabs for 'Zustimmung des Administrators' (Administrator consent) and 'Zustimmung des Benutzers' (User consent). A search bar for permissions is visible, and a message states: 'Für die Anwendung wurden keine vom Administrator genehmigten Berechtigungen gefunden.' (No permissions approved by the administrator were found for the application.)

Auf dieser Seite finden Sie in der Beschreibung einen Link zu der Ansicht „Anwendungsregistrierung“.

Klicken Sie nun auf [+ Berechtigung hinzufügen] und wählen unterhalb „Von meiner Organisation verwendete APIs“ den Eintrag „Office 365 Exchange Online“ aus.

Microsoft-APIs Von meiner Organisation verwendete APIs Eigene APIs

Apps in Ihrem Verzeichnis, die APIs verfügbar machen, werden unten angezeigt.

🔍 Beginnen Sie mit der Eingabe eines API-Namens oder einer Anwendungs-ID.

| Name | Anwendungs-ID (Client) |
|----------------------------|--------------------------------------|
| Call Recorder | 4580fd1d-e5a3-4f56-9ad1-aab0e3bf8f76 |
| Office 365 Exchange Online | 00000002-0000-0ff1-ce00-000000000000 |

Klicken Sie auf „Anwendungsberechtigungen“, wählen in der Liste unter „Andere Berechtigungen“ das Recht „full_access_as_app“ aus und klicken auf [Berechtigung hinzufügen].

Delegierte Berechtigungen

Ihre Anwendung muss als der angemeldete Benutzer auf die API zugreifen.

Anwendungsberechtigungen

Ihre Anwendung wird als Hintergrunddienst oder Daemon ohne angemeldeten Benutzer ausgeführt.

Berechtigungen auswählen Alle aufklappen

🔍 Beginnen Sie mit der Eingabe einer Berechtigung, um diese Ergebnisse zu filtern.

| Berechtigung | Administratoreinwilligung erforderlich... |
|---|---|
| ▾ Andere Berechtigungen (1) | |
| <input checked="" type="checkbox"/> full_access_as_app ⓘ Use Exchange Web Services with full access to all mailboxes | Ja |

Sie werden nun sehen das für dieses Recht noch die Zustimmung des Administrators erteilt werden muss. Wenn Sie als Administrator angemeldet sind können Sie hierzu auf [✓ Administratorzustimmung für „<domain>“ erteilen] und anschließend auf [Ja] klicken.

+ Berechtigung hinzufügen ✓ Administratorzustimmung für "com2test" erteilen

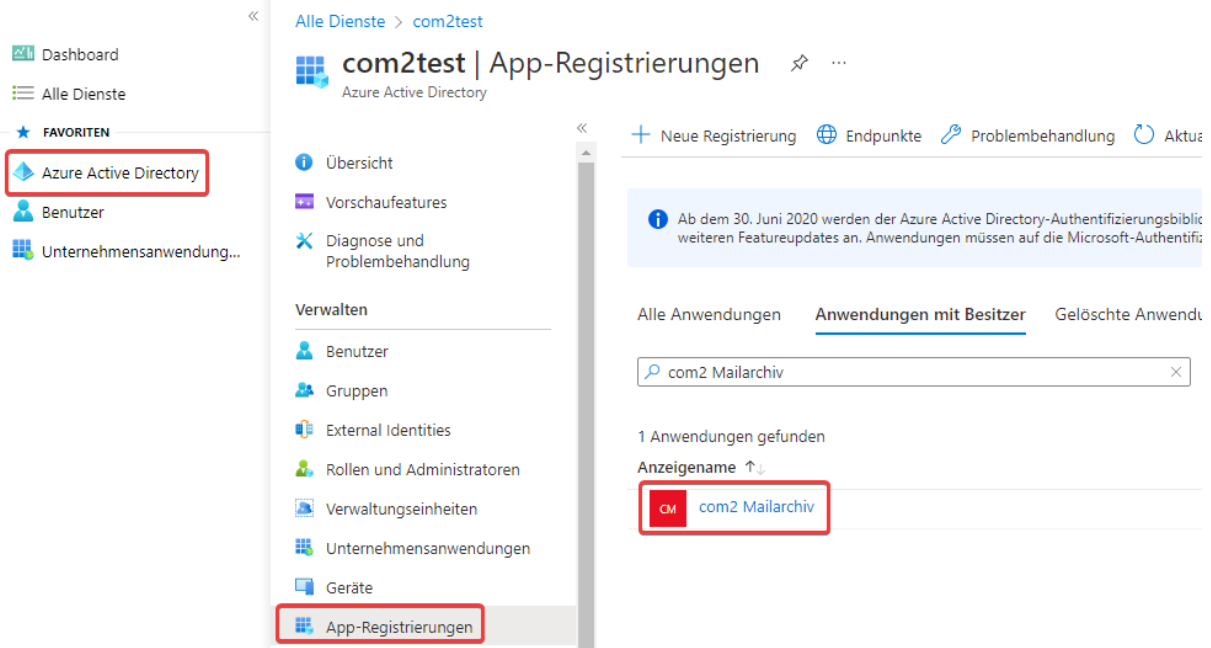
| API/Berechtigungsname | Typ | Beschreibung | Administratoreinwilligung erforderlich. | Status |
|----------------------------------|-----------|------------------|---|--------------------------------|
| ▾ Office 365 Exchange Online (1) | | | | |
| full_access_as_app | Anwendung | Use Exchange ... | Ja | ⚠ Für "com2test" nicht erteilt |

Der Status sollte nun wie folgt aussehen:

| API/Berechtigungsname | Typ | Beschreibung | Administratoreinwill... | Status |
|----------------------------------|-----------|---|-------------------------|--------------------------|
| ▾ Office 365 Exchange Online (1) | | | | |
| full_access_as_app | Anwendung | Use Exchange Web Services with full access to all mailboxes | Ja | ✔ Gewährt für "com2test" |

Geheimen Clientschlüssel erstellen

Als nächstes muss der Anwendung noch ein Clientschlüssel hinzugefügt werden. Wechseln Sie in der Ansicht „Azure Active Directory“ zu „App-Registrierungen“ und klicken auf die neue Anwendung.

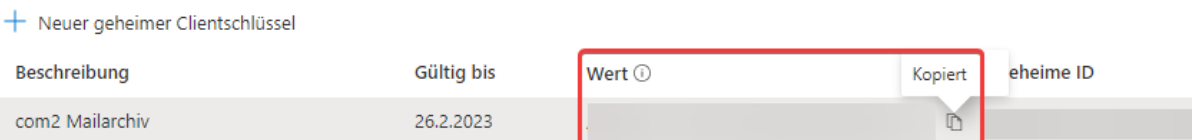


Notieren Sie sich auf der Folgeseite die Anwendungs-ID (ClientID) sowie die Verzeichnis-ID (MandantenID). Diese Informationen werden später in der Konfiguration der NetOrchestra MA benötigt.



Klicken Sie auf „Ein Zertifikat oder Geheimnis hinzufügen“ und im Anschluss auf [+ Neuer geheimer Clientschlüssel]. Vergeben Sie diesem einen Namen, geben an wie lange dieser gültig sein soll und klicken auf [Hinzufügen].

Kopieren Sie sich nun den Wert des Clientschlüssels und notieren sich diesen zusammen mit der ClientID und MandantenID.



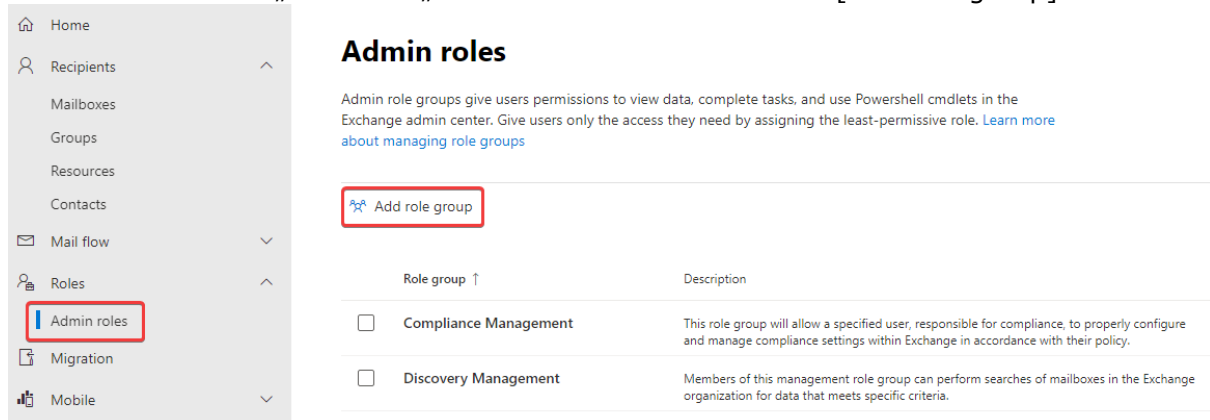
Mit der ClientID, MandantenID und dem ClientSecret-Wert haben Sie nun alle Informationen um mit der Konfiguration der NetOrchestra MA fortzusetzen.

Vorbereitungen für den Zugriff über BasicAuth in Exchange Online

Um aus allen Benutzerpostfächern archivieren zu können, muss der Benutzer mit dem sich die NetOrchestra MA bei Exchange Online anmeldet das Impersonationsrecht besitzen.

Melden Sie sich mit Ihrem Webbrowser bei Exchange Online an und rufen im Admin Center das Exchange Admin Center auf. (Direktlink: <https://admin.exchange.microsoft.com/>)

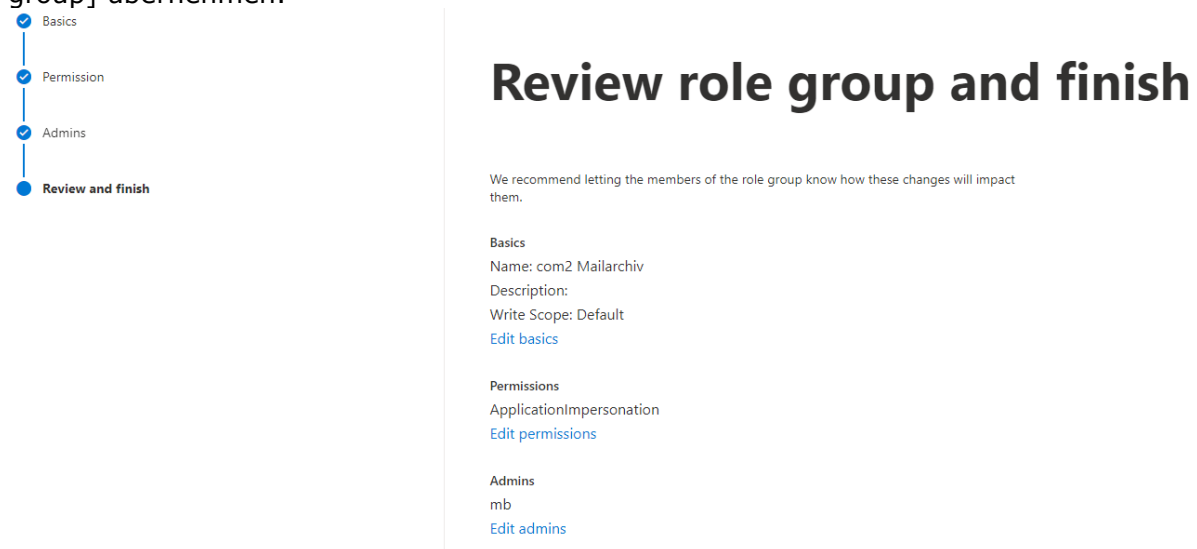
Wechseln Sie unter „Roles“ zu „Admin Roles“ und klicken auf [Add role group].



| Role group ↑ | Description |
|--|--|
| <input type="checkbox"/> Compliance Management | This role group will allow a specified user, responsible for compliance, to properly configure and manage compliance settings within Exchange in accordance with their policy. |
| <input type="checkbox"/> Discovery Management | Members of this management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria. |

Vergeben Sie der Rolle einen passenden Namen, wählen auf der zweiten Seite das Recht ApplicationImpersonation aus und geben auf der dritten Seite den Benutzer an mit dem sich die NetOrchestra MA bei Exchange Online anmelden soll.

Auf der letzten Seite können Sie die Einstellungen nochmal überprüfen und per [Add role group] übernehmen.



Review role group and finish

We recommend letting the members of the role group know how these changes will impact them.

Basics
Name: com2 Mailarchiv
Description:
Write Scope: Default
[Edit basics](#)

Permissions
ApplicationImpersonation
[Edit permissions](#)

Admins
mb
[Edit admins](#)

Vorbereitungen der Journalpostfacharchivierung in Exchange Online

Mit einer Journalregel haben Sie die Möglichkeit für alle ein- und ausgehenden Mails in der Organisation eine Kopie an ein sogenanntes Journalpostfach zu senden. Mit der Journalpostfacharchivierung holt sich die NetOrchestra MA die Mails aus dem Journalpostfach ab, archiviert und entfernt diese damit das Postfach nicht voll wird.

Bei Exchange Online muss sich das Journalpostfach außerhalb der eigenen Organisation befinden. Damit die Mails aus dem Postfach abgeholt werden, muss der Mailserver des Journalpostfaches in der NetOrchestra MA für die Archivierung angebunden werden. Bei hybriden Umgebungen kann ein sich auf dem OnPrem-Server befindendes Postfach als Journalpostfach konfiguriert werden.

Alternativ besteht auch die Möglichkeit mit einer Transportregel eine Kopie der Mails an ein organisationseigenes Postfach zu senden. Bitte beachten Sie, dass bei dieser Methode keine Envelope-Informationen übergeben werden. Daher gilt diese Lösung mehr als Workaround wenn kein externes Postfach für das Journaling zur Verfügung steht.

Im Folgenden wird die Konfiguration beider Varianten beschrieben.

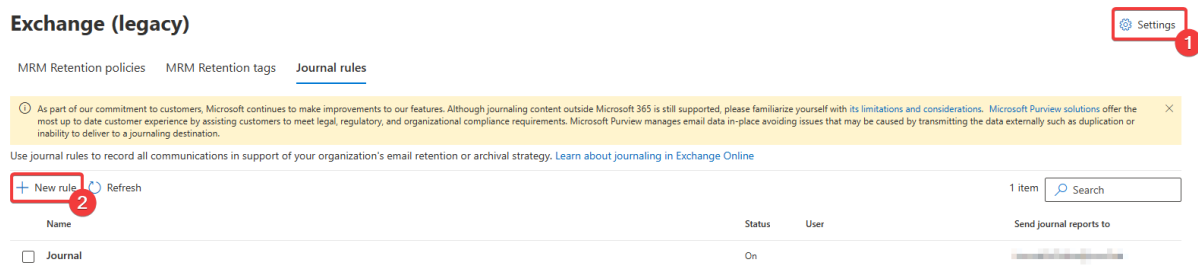
Option 1: Journalregel erstellen:

Rufen Sie das Compliance Admin Center auf und wechseln in die folgende Ansicht: *Data lifecycle management > Exchange (legacy) > Journal rules*.

<https://compliance.microsoft.com/exchangeinformationgovernance?viewid=exoJournal-Rule>

Bevor eine Journalregel erstellt werden darf, muss sichergestellt sein das ein Postfach für nicht zustellbare Journalberichte konfiguriert ist.

Rufen Sie dazu über das Zahnradsymbol die Settings auf, geben die dafür vorgesehene Mailadresse an und wechseln wieder in die vorherige Ansicht. (1)



Anschließend können Sie mit der Schaltfläche [+] eine neue Regel hinzufügen. (2)

Define 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 rule name *

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

Geben Sie die Mailadresse des Postfaches an welches als Journalpostfach verwendet werden soll. Bei einer hybriden Umgebung kann dies ein Postfach sein welches sich auf dem OnPrem-Server befindet.

Vergeben Sie der Regel einen Namen und definieren unter welchen Bedingungen eine Kopie der Mails dem Journalpostfach übergeben werden soll.

Nachdem die Regel aktiviert wurde ist es empfehlenswert zu prüfen ob auch tatsächlich für eingehende und ausgehende Mails eine Kopie in dem Journalpostfach abgelegt wird. In dem Postfach das für nicht zustellbare Journalberichte konfiguriert wurde, landen in einem solchen Fall NDR's die bei der Problemerkennung helfen sollten.

Option 2: Transportregel erstellen:

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.

Wechseln Sie in die Ansicht *Nachrichtenfluss* > *Regeln* und fügen mit der Schaltfläche [+] eine neue Regel hinzu.

Exchange Admin Center

- Dashboard
- Empfänger
- Berechtigungen
- Complianceverwaltung
- Organisation
- Schutz
- Nachrichtenfluss**
- Mobil
- Öffentliche Ordner
- Unified Messaging
- Hybrid



The screenshot shows the 'Regeln' (Rules) page in the Exchange Admin Center. The 'Nachrichtenfluss' (Message Flow) menu item is highlighted with a red box and a '1'. The 'Regeln' tab is selected with a red box and a '2'. A red box with a '3' highlights the '+ ' button used to add a new rule. Below the button, there is a table with columns 'EIN', 'REGEL', and 'PRIORITÄT'. The table is currently empty, with a message below it stating 'Es gibt keine Elemente, die in dieser Ansicht angezeigt werden können.'

Nachfolgend öffnet sich ein Dialog.

Neue Regel

Name:
Journalregel

*Diese Regel anwenden, wenn...
[Auf alle Nachrichten anwenden]

*Folgendermaßen vorgehen...
Bcc der Nachricht an... 'journal@com2gm...

Eigenschaften dieser Regel:

Diese Regel mit folgendem Schweregrad überwachen:
Nicht angegeben

Modus für diese Regel auswählen:

Erzwingen
 Test mit Richtlinientipps
 Test ohne Richtlinientipps

[Weitere Optionen...](#)

i Reichtverwaltungsdienste (Rights Management Services, RMS) sind eine Premium-Funktion und erfordern eine Enterprise-Clientzugriffslizenz (CAL) oder eine RMS-Onlinelizenz für jedes Benutzerpostfach. [Weitere Informationen](#)

Speichern Abbrechen

(1) *Diese Regel anwenden, wenn..*

- Sollen ein- und ausgehende Mails erfasst werden, wählen Sie die Option *[Auf alle Nachrichten anwenden]* aus.
- Für nur ausgehende Mails, wählen Sie die Option „Der Absender befindet sich in..“ und anschließend „...innerhalb der Organisation“ aus.
- Für nur eingehende Mails, wählen Sie auch hier die Option „Der Absender befindet sich in..“ aus, jedoch diesmal „...außerhalb der Organisation“.

(2) *Folgendermaßen vorgehen...*

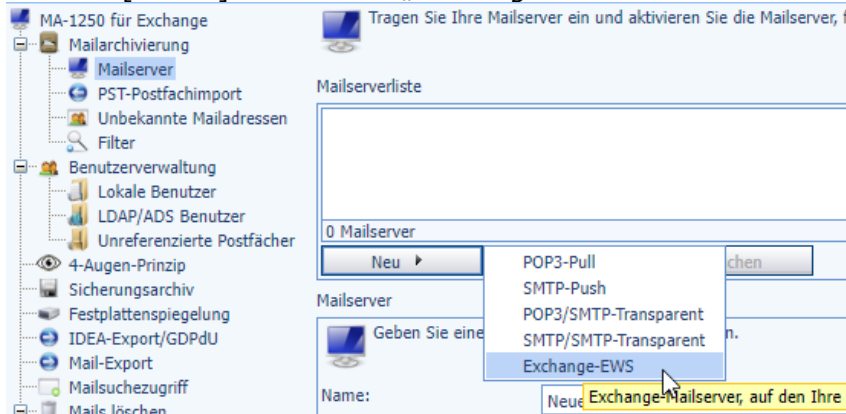
- Wählen Sie die Option „BCC der Nachricht an...“ aus und geben das gewünschte Journalpostfach an.

Für die restlichen Einstellungen können die Default-Werte beibehalten werden. Drücken Sie nun auf [Speichern] und prüfen ob die Regel aktiviert ist.

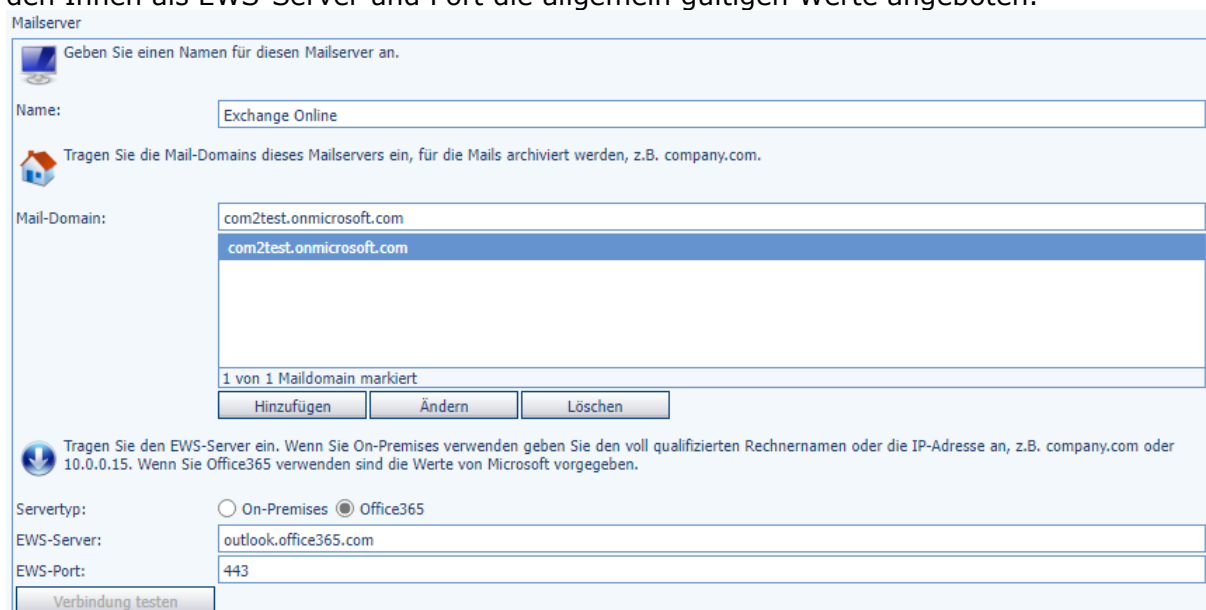
Einstellungen auf der NetOrchestra MA für die Anbindung an Exchange Online

Rufen Sie mit einem Webbrowser die Weboberfläche der NetOrchestra MA auf und melden sich als Administrator an: <https://<IP-Adresse der MA>/admin>

Wechseln Sie zu der Ansicht „Mailarchivierung“ > „Mailserver“, klicken in der Mailserverliste auf [Neu >] und wählen „Exchange-EWS“ aus.



Vergeben Sie dem Mailserver-Eintrag einen passenden Namen, geben die Maildomänen an für die archiviert werden soll und wählen als Servertyp Office365 aus. Dadurch werden Ihnen als EWS-Server und Port die allgemein gültigen Werte angeboten.



Konfiguration für den Zugriff über OAuth2

Es werden die bei der Konfiguration von Exchange Online notierten Daten benötigt.

Wählen Sie bei Authentifizierung OAuth2 aus und geben die MandantenID ($\hat{=}$ Verzeichnis-ID), ClientID ($\hat{=}$ Anwendungs-ID) sowie den ClientSecret-Wert an.



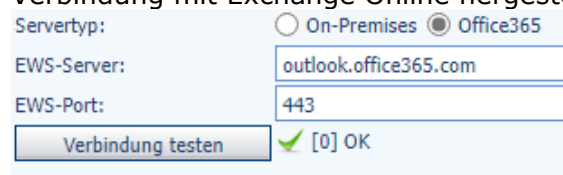
Authentifizierung: OAuth2 Basic

MandantenID:

ClientID:

ClientSecret-Wert:

Wenn Sie nun die Konfiguration speichern (Diskette in Symbolleiste) können Sie mit der Schaltfläche [Verbindung testen] prüfen ob mit den eingegebenen Daten erfolgreich eine Verbindung mit Exchange Online hergestellt werden kann.



Servertyp: On-Premises Office365

EWS-Server:

EWS-Port:


[0] OK

Konfiguration für den Zugriff über BasicAuth

Es werden die Daten des Benutzers mit dem zuvor erstellten Impersonationsrecht benötigt.

Wählen Sie bei Authentifizierung Basic aus und geben die Domäne, Mailadresse sowie das Kennwort des Benutzers an mit dem sich die NetOrchestra MA bei Exchange Online authentifizieren soll.



 Tragen Sie den Benutzer für die Impersonierung ein.

Authentifizierung: OAuth2 Basic

Domäne:

Benutzer:

Kennwort:

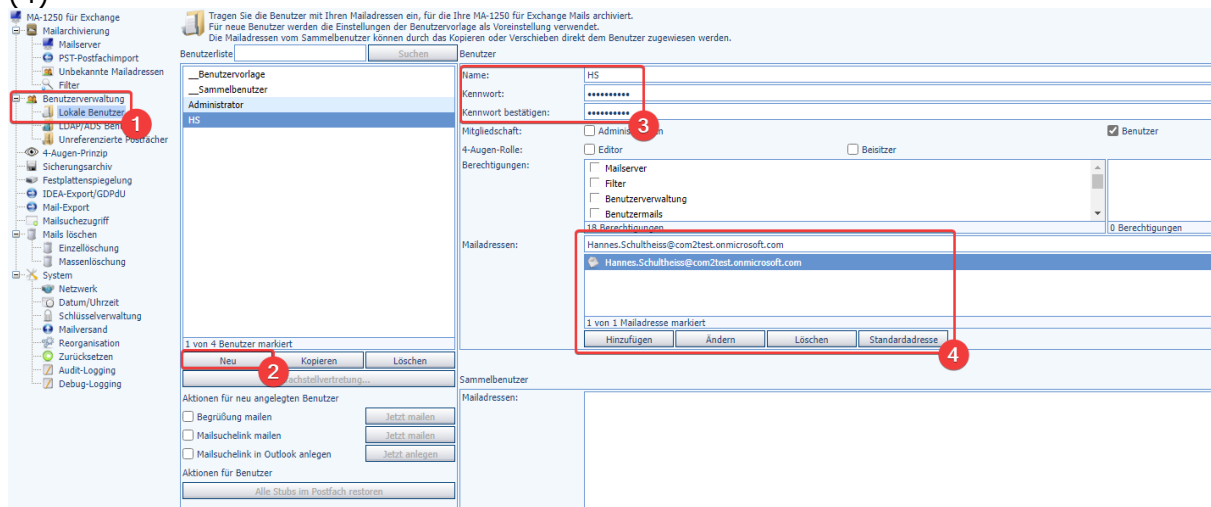
Zu archivierende Postfächer in der Benutzerverwaltung hinzufügen

Alle Mailadressen der Postfächer aus denen archiviert werden sollen müssen in der lokalen Benutzerliste hinzugefügt werden.

Wechseln Sie zu der Ansicht „Benutzerverwaltung“ > „Lokale Benutzer“ (1) und legen mit der Schaltfläche [Neu] einen neuen Benutzereintrag an. (2)

Vergeben Sie diesem Benutzer einen Namen und ein Kennwort. Mit diesen Daten kann sich der Benutzer später in der Mailsuche anmelden. (3)

Fügen Sie in den Mailadressen alle Mailadressen des einzelnen Benutzers an für die archiviert werden sollen und auf die der Benutzer Zugriff für die Mailsuche erhalten darf. (4)

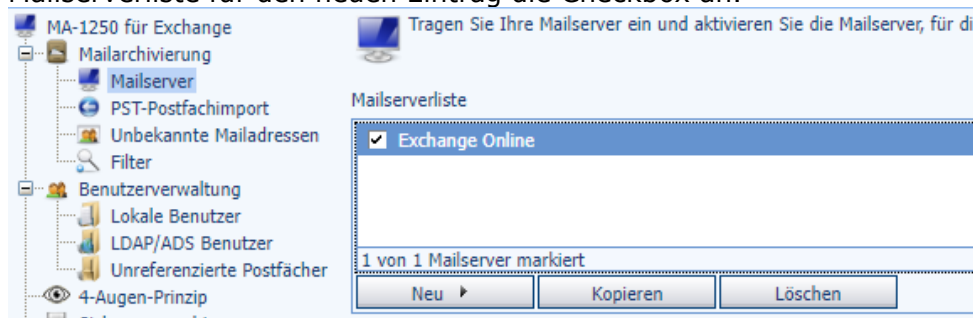


Archivierung auf der NetOrchestra MA aktivieren

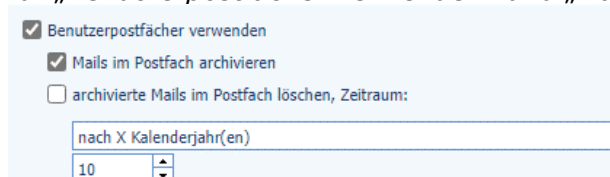
Sind die vorherigen Schritte alle umgesetzt kann nun die Archivierung aktiviert werden.

Benutzerpostfacharchivierung aktivieren

Wechseln Sie dazu in die Ansicht „Mailarchivierung“ > „Mailserver“ und ticken in der Mailserverliste für den neuen Eintrag die Checkbox an.



Nachdem Sie den Eintrag ausgewählt haben können Sie nun noch die beiden Checkboxes für „Benutzerpostfächer verwenden“ und „Mails im Postfach archivieren“ aktivieren.



Nach Speichern der Konfiguration sollten die ersten Mails archiviert werden.

Journalpostfacharchivierung aktivieren

Da bei Exchange Online für das Journaling nur ein externes Journalpostfach angegeben werden kann, müssen auf der NetOrchestra MA die Verbindungsdaten des Mailservers angegeben werden der dieses Postfach verwaltet.

Wechseln Sie zu der Ansicht „Mailarchivierung“ > „Mailserver“, klicken in der Mailserverliste auf [Neu >] und wählen „Exchange-EWS“ aus.

Vergeben Sie dem Mailserver-Eintrag einen passenden Namen, geben die Maildomänen an für die archiviert werden soll und geben die Verbindungsdaten des entsprechenden 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 und geben die Mailadresse des Journalpostfachs an.

Journalpostfach verwenden

Mailadresse: Journal@com2test.de

Ist auch die Checkbox für den Eintrag in der Mailserverliste aktiviert und die Konfiguration gespeichert, sollten die ersten Mails aus dem Journalpostfach abgeholt werden.