

Produkt: NetOrchestra® MA

Kurzbeschreibung: Archivierung eines O365 Postfaches 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.***

Einführung

Der Zugriff auf die O365 Postfächer erfolgt über die Authentifizierungsmethode OAuth2. Basic gilt seit Ende 2022 als deprecated und sollte daher nicht mehr verwendet werden.

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

OAuth2 in Exchange Online konfigurieren

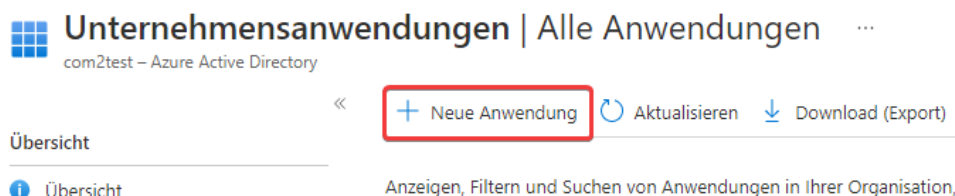
Rufen Sie die Webseite von Exchange Online auf und melden sich mit Ihrem Konto an.

Navigieren Sie anschließend über das Admin Center in das Azure Active Directory Portal. (Direktlink: <https://aad.portal.azure.com/>)

Unternehmensanwendung erstellen

Für das Mailarchiv muss eine neue Unternehmensanwendung erstellt werden.

- Navigieren Sie zu Alle Dienste > Unternehmensanwendungen ...
- ... und klicken auf [Neue Anwendung].



- Klicken Sie auf [Eigene Anwendung erstellen].

Azure AD-Katalog durchsuchen



Der Azure AD-App-Katalog ist ein Katalog mit Tausenden von Apps, welche die um Ihre Benutzer sicherer mit ihren Apps zu verbinden. Hier können Sie Apps d verwenden können, können Sie eine Anforderung mithilfe des Prozesses einreic

- Vergeben Sie der Anwendung einen beliebigen Namen
- Wählen Sie die Option Register an application to integrate with Azure AD (App you're developing) aus.

Wie lautet der Name der App?

com2 Mailarchiv ✓

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 auf [Erstellen].
- In der Ansicht Anwendung Registrieren können die Default-Einstellungen beibehalten werden. Klicken Sie auf [Registrieren].

* Name

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

com2 Mailarchiv

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.

Plattform auswählen ▼ Beispiel: https://example.com/auth

Der Anwendung Berechtigungen zuweisen

Der neu erstellten Unternehmensanwendung müssen nun die benötigten Berechtigungen zugewiesen werden.

- Wechseln Sie in die Ansicht Unternehmensanwendungen > Alle Anwendungen.
- Klicken Sie auf die neu erstellte Anwendung und wechseln zu den Berechtigungen.
- Klicken Sie auf Anwendungsregistrierung (siehe Screenshot).

com2 Mailarchiv | Berechtigungen

Unternehmensanwendung

Aktualisieren | Berechtigungen überprüfen | Haben Sie Feedback für uns?

Berechtigungen

Anwendungen können Berechtigungen für Ihre Organisation und ihre Daten mithilfe von drei Methoden erteilt werden: ein Administrator integriert eine Anwendung und ermöglicht den Self-Service-Zugriff oder weist Benutzer direkt der Anwendung Berechtigungen zu.

Um zusätzliche Berechtigungen für diese Anwendung anzufordern, verwenden Sie die **Anwendungsregistrierung**.

Als Administrator können Sie Ihre Einwilligung im Namen aller Benutzer in diesem Mandanten erteilen. So stellen Sie sicher, dass die Schaltfläche, um Administratoreinwilligung zu erteilen.

Administratorzustimmung für "com2test" erteilen

Zustimmung des Administrators | Zustimmung des Benutzers

Berechtigungen suchen

API-Name	↑↓ Anspruchswert	↑↓ Berechtigung
Für die Anwendung wurden keine vom Administrator genehmigten Berechtigungen gefunden.		

- Klicken Sie auf [Berechtigung hinzufügen]
- Wechseln Sie zu Von meiner Organisation verwendete APIs.
- Wählen Sie nun 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** ...
- ... und wählen in der Liste **Andere Berechtigungen** das Recht **full_access_as_app** aus.
- Klicken Sie 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](#)

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

Abschließend muss der Administrator der Erteilung des Rechts zustimmen.

- Klicken Sie auf **[Administratorzustimmung für <domain> erteilen]** ...
- ... und anschließend auf **[Ja]**.

[+ 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

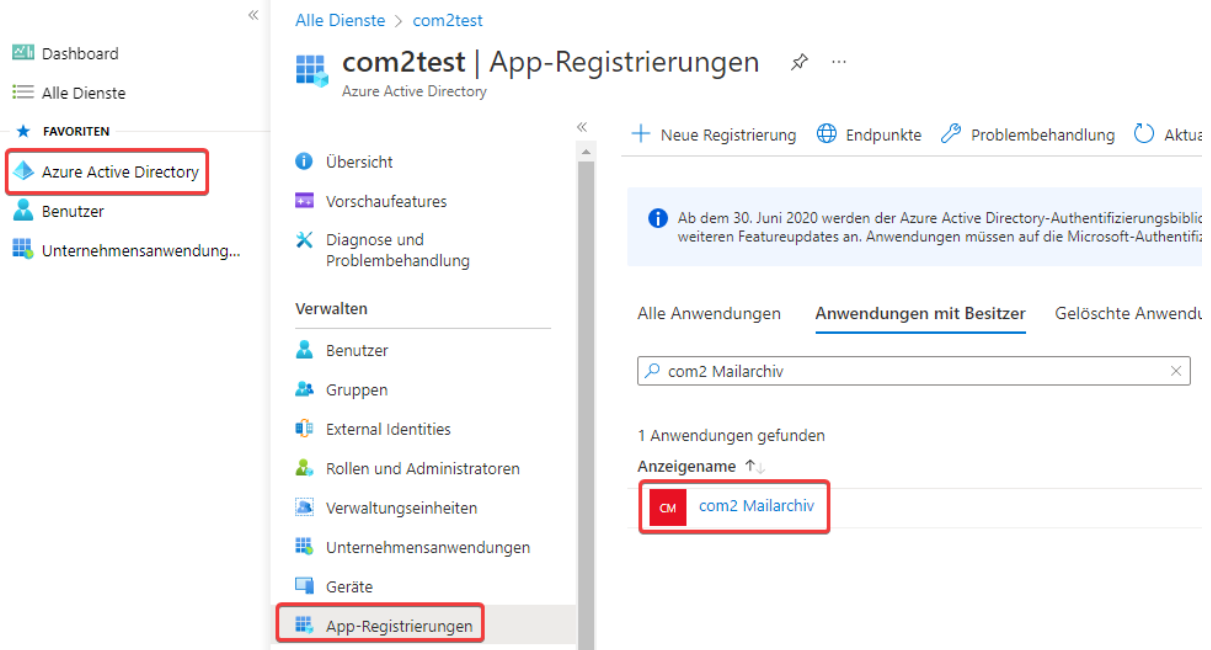
Der Status sollte nun wie folgt aussehen:

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 ein Clientschlüssel zugewiesen werden.

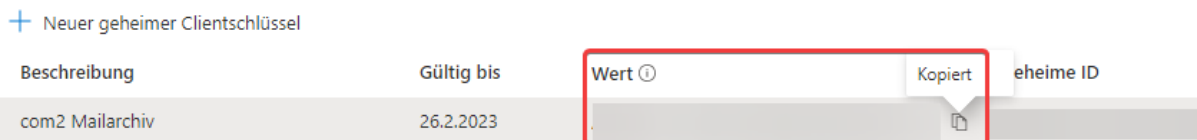
- Wechseln Sie in die Ansicht Azure Active Directory > App-Registrierungen.
- Klicken Sie auf die neue Unternehmensanwendung.



- Notieren Sie sich die Anwendungs-ID und die Verzeichnis-ID.



- Klicken Sie auf [Ein Zertifikat oder Geheimnis hinzufügen](#).
- Klicken Sie auf [\[Neuer geheimer Clientschlüssel\]](#).
- Vergeben Sie dem Schlüssel einen Namen, wählen die Gültigkeitsdauer und klicken auf [\[Hinzufügen\]](#).
- Kopieren und notieren Sie sich den Wert des Clientschlüssels.



Hinweis: Die Anwendungs-ID, Verzeichnis-ID und der Clientschlüssel werden später für die Konfiguration auf der NetOrchestra MA benötigt.

Journalpostfach in Exchange Online konfigurieren

Alle ein- und ausgehenden Mails Ihrer Organisation können mit einer Journalregel an ein Journalpostfach gesendet werden. Über die Journalpostfacharchivierung holt sich die NetOrchestra MA die Mails aus dem Postfach ab, archiviert und entfernt diese aus dem Postfach.

Bei Exchange Online muss sich das Journalpostfach außerhalb der eigenen Organisation befinden. Damit die Mails aus dem Postfach archiviert werden, muss der Mailserver des Journalpostfaches zusätzlich in der NetOrchestra MA mit angebinden 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.

Variante 1 - Journalregel:

- Rufen Sie das Compliance Admin Center auf und wechseln in die Ansicht Data lifecycle management > Exchange (legacy) > Journal rules.
(Direktlink: <https://compliance.microsoft.com/exchangeinformationgovernance?viewid=exoJournalRule>)
- Stellen Sie sicher das ein Postfach für nicht zustellbare Journalberichte konfiguriert ist.
- Klicken Sie dazu auf die Settings, geben die Mailadresse an und kehren zu der vorherigen Seite zurück. (1)
- Klicken Sie auf [New Rule]. (2)

Exchange (legacy)

MRM Retention policies MRM Retention tags Journal rules

As part of our commitment to customers, Microsoft continues to make improvements to our features. Although journaling content outside Microsoft 365 is still supported, please familiarize yourself with its limitations and considerations. Microsoft Purview solutions offer the most up to date customer experience by assisting customers to meet legal, regulatory, and organizational compliance requirements. Microsoft Purview manages email data in-place avoiding issues that may be caused by transmitting the data externally such as duplication or inability to deliver to a journaling destination.

Use journal rules to record all communications in support of your organization's email retention or archival strategy. [Learn about journaling in Exchange Online](#)

1 item Search

Name	Status	User	Send journal reports to
<input type="checkbox"/> Journal	Off		

- Geben Sie die Mailadresse des Postfaches an, welches als Journalpostfach verwendet werden soll.
- Vergeben Sie der Regel einen Namen und geben an unter welchen Bedingungen eine Mail an das Journalpostfach gesendet werden soll.

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

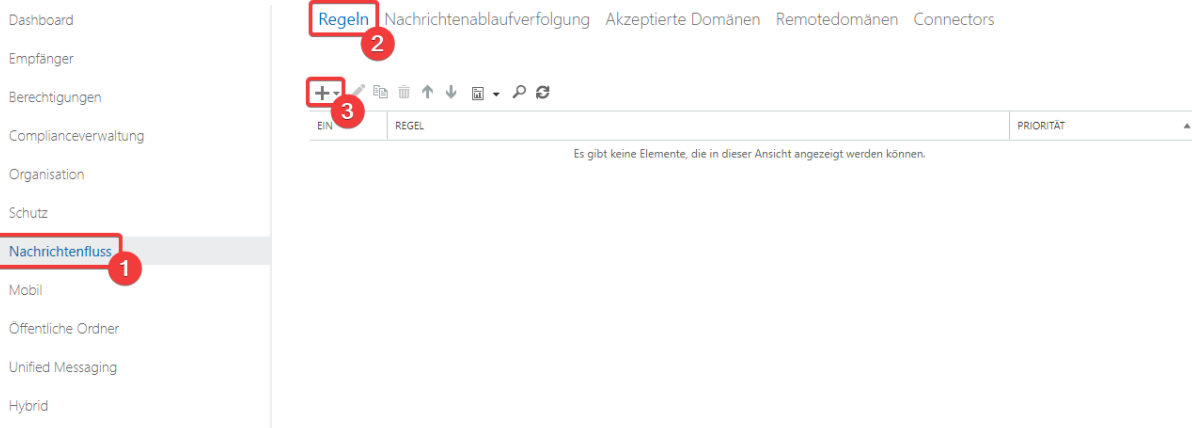
Nachdem die Regel aktiviert wurde ist es empfehlenswert zu prüfen ob auch tatsächlich für eingehende und ausgehende Mails eine Kopie in dem Journalpostfach abgelegt wird. In dem Postfach das für nicht zustellbare Journalberichte konfiguriert wurde, landen in einem solchen Fall NDR's die bei der Problemerkennung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

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.

- Wechseln Sie in die Ansicht Nachrichtenfluss > Regeln.
- Fügen Sie mit [+] eine neue Regel hinzu.

Exchange Admin Center



The screenshot shows the Exchange Admin Center interface. On the left, the 'Nachrichtenfluss' (Message Flow) link is highlighted with a red box and a '1' in a circle. In the main content area, the 'Regeln' (Rules) link is highlighted with a red box and a '2' in a circle. Below it, the '+' icon for adding a new rule is highlighted with a red box and a '3' in a circle. The main content area shows a table with columns 'EIN', 'REGEL', and 'PRIORITÄT'. The table is currently empty, with the message 'Es gibt keine Elemente, die in dieser Ansicht angezeigt werden können.' (There are no elements that can be displayed in this view.)

Nachfolgend öffnet sich ein Dialog:

(1) Diese Regel anwenden, wenn...

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

(2) Folgendermaßen vorgehen...

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

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-Clientszugriffslizenz (CAL) oder eine RMS-Onlinelizenz für jedes Benutzerpostfach. [Weitere Informationen](#)

Speichern Abbrechen

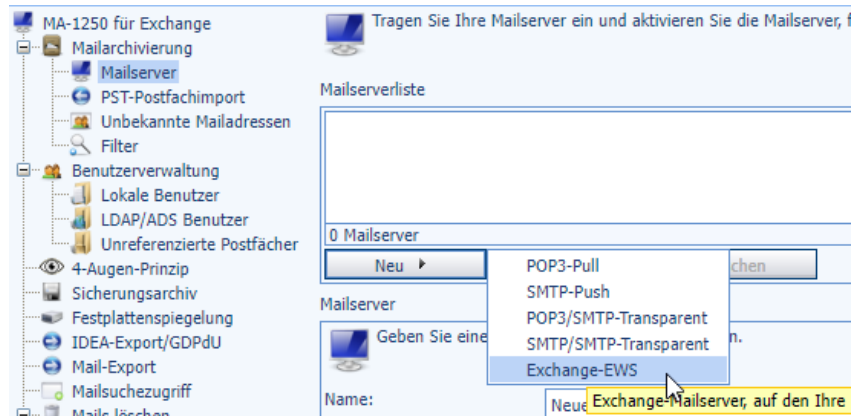
Für die restlichen Einstellungen können die Default-Werte beibehalten werden.

- Klicken Sie auf [Speichern] und prüfen ob die Regel aktiviert ist.

Konfiguration auf der NetOrchestra MA

Die Konfiguration erfolgt auf der Admin-Weboberfläche des Mailarchivs.
(<https://<MA-Adresse>/admin>)

- Wechseln Sie in die Ansicht Mailarchivierung > Mailserver.
- Erstellen Sie in der Mailserverliste mit [Neu] einen neuen Eintrag des Typs Exchange-EWS.



- Vergeben Sie einen passenden Namen.
- Geben Sie die Maildomänen an für die archiviert werden sollen.
- Wählen Sie den Servertyp Office365 aus.

Mailserver

Geben Sie einen Namen für diesen Mailserver an.

Name:

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

Mail-Domain:

1 von 1 Maildomain markiert

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:

EWS-Port:

Konfiguration für den Zugriff über OAuth2

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

- Wählen Sie als Authentifizierungstyp OAuth2 aus.
- Geben Sie die nachfolgenden Informationen an:
 - o MandantenID (Verzeichnis-ID)
 - o ClientID (Anwendungs-ID)
 - o ClientSecret-Wert (Clientschlüssel)

- 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.

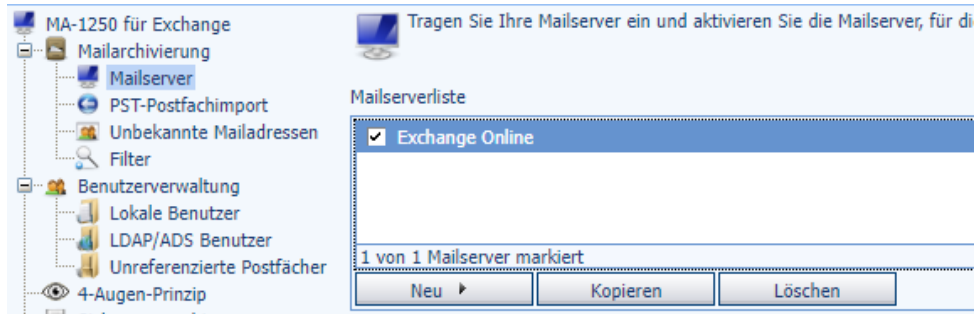
Zu archivierende Postfächer in der Benutzerverwaltung hinzufügen

Für alle Postfächer für die archiviert werden soll, müssen die dazugehörigen Mailadressen einem Benutzer in der Benutzerverwaltung zugewiesen werden. Im Nachfolgenden werden hierzu lokale Benutzer erstellt:

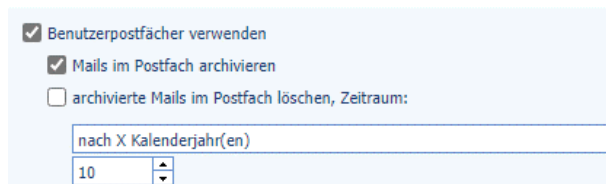
- Wechseln Sie in die Ansicht Benutzerverwaltung > Lokale Benutzer (1)
- Legen Sie mit [Neu] einen neuen Benutzer an. (2)
- Vergeben Sie einen Namen und ein Kennwort. Diese Daten werden für die Anmeldung an der Mailsuche verwendet. (3)
- Fügen Sie dem Benutzer alle seine Mailadressen hinzu. (4)

Benutzerpostfacharchivierung aktivieren

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



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



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, muss auf der NetOrchestra MA ein Mailservereintrag des Servers hinzugefügt werden, der das Journalpostfach verwaltet:

- Wechseln Sie in die Ansicht Mailarchivierung > Mailserver.
- Klicken Sie in der Mailserverliste auf [Neu] und wählen Exchange-EWS aus.
- Vergeben Sie einen Namen.
- Geben Sie die 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.