



Restrict Access to Mailboxes

Luware
Nimbus

 **Luware**

Contents

1	Introduction	2
2	Configuring Email Distribution in Luware Nimbus	3
2.1	Setting Up Email Distribution in Luware Nimbus	3
2.2	Email Modality Workflow	5
2.3	Configure Service Settings for Distributing Emails	6
3	Restricting Access to Selected Mailboxes	8
3.1	Connect via PowerShell to Exchange Online	10

1 Introduction

This white paper delves into the functionality and configuration options of **Luware Nimbus' Email Distribution feature**. Further, it explains how to use the My Service Sessions page to manage incoming and outgoing emails. This document is intended for Luware Nimbus administrators and users.

Email distribution for Luware Nimbus allows you to distribute emails from Exchange Online to users via the Luware Nimbus service. The user will be able to answer emails from a shared exchange mailbox in his My Service Sessions page in Luware Nimbus. With this, users can:

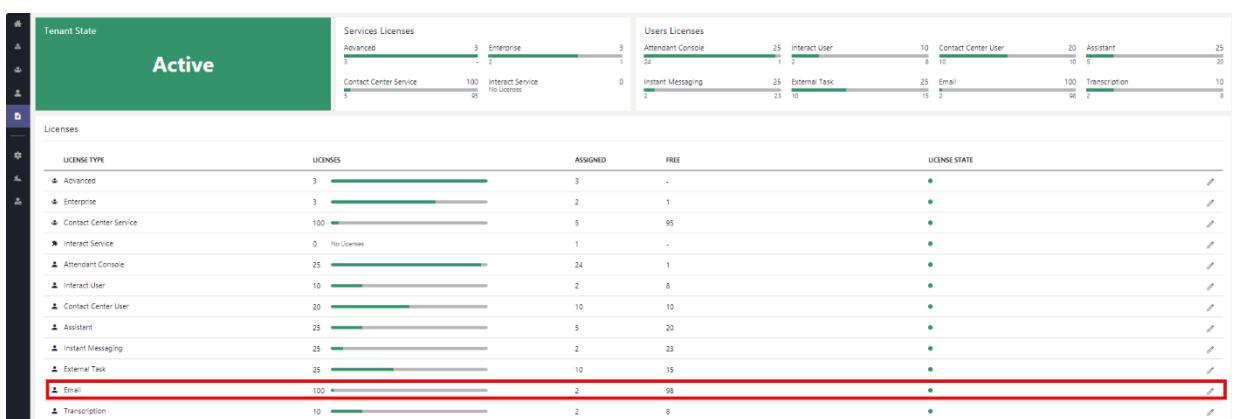
- Use an efficient routing engine to handle emails from different sources and channels in one unified platform.
- Enhance customer service and satisfaction by delivering more timely and personalized responses.
- Track the performance of your email service using Nimbus reporting.

2 Configuring Email Distribution in Luware Nimbus

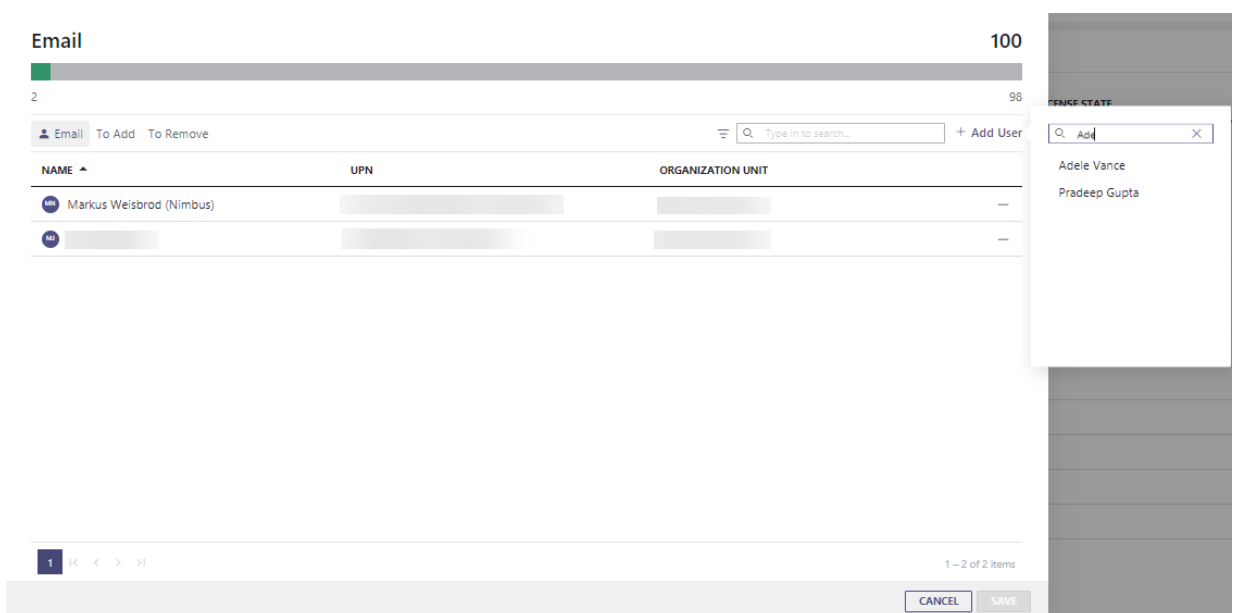
2.1 Setting Up Email Distribution in Luware Nimbus

The first step to enable email distribution for an Exchange Online mailbox through Luware Nimbus is to acquire licenses for this specific feature. Please contact your Luware sales representative to obtain the required licenses.

After successful acquisition, the licenses will be added to your tenant. Now, you can proceed with the configuration of email settings within Luware Nimbus.



To ensure users can access email functionality, you'll need to assign them email licenses. This process is straightforward: Click the **Edit** button on the licenses page to add a user to the List of licensed users.



After the licenses are added to the tenant and assigned to the users, you can start adding your mailboxes to the system:

1. Access the mailbox configuration: Within the Nimbus admin portal, navigate to **Configuration > Service > Mailboxes**.
2. Create a new mailbox: Click the **Create New** button to initiate the mailbox addition process.
3. **Enter User Principal Name (UPN)**. Simply provide the correct UPN of the mailbox you want to integrate.
4. Luware Nimbus will automatically locate the mailbox based on the entered UPN.
5. Once you've verified the information, click **Save** to confirm the mailbox configuration.

With these steps, you'll have successfully added and integrated your users' mailboxes within Luware Nimbus.

Mailboxes

Name *
Support Service Mailbox

Organization Unit *
-- Benelux

Mailbox UPN *
support@mycompany.com

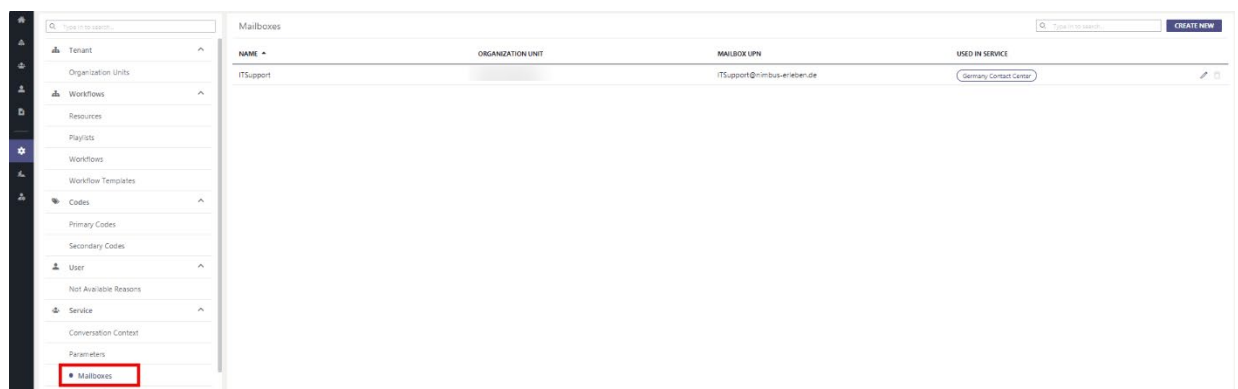
Now, fill in a name, select an organization unit and add the mailbox UPN. The mailbox is now ready to use and can be assigned to a Luware Nimbus service.

In Exchange, you can also assign a mailbox to one or more teams, which will decide who can access and manage the emails in this mailbox.

You can edit or remove a mailbox configuration at any time by clicking the **Edit** or **Delete** button next to the mailbox name.

Only mailbox configurations that are not assigned to any Luware Nimbus Service can be deleted.

Deleting a mailbox configuration from Luware Nimbus will not remove the mailbox from Exchange Online, but it will stop the distribution of emails from that mailbox via Luware Nimbus.



2.2 Email Modality Workflow

The distribution engine in Nimbus needs to know how to handle emails in a specific service. This is described within a workflow. The workflow defines how emails from a mailbox are routed to agents and how they are prioritized and handled.

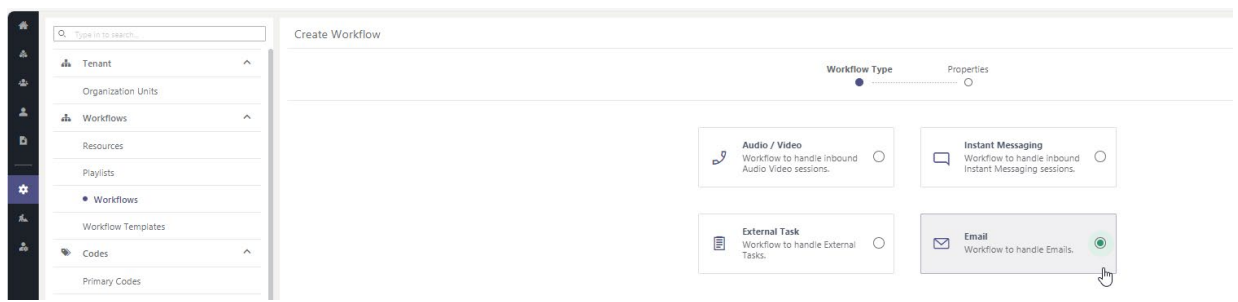
If you want to create a new workflow to distribute emails, go to the configuration page within the admin portal. Select the **workflow** section. Here, you have the choice to create either:

New Email Workflow: Customize how emails from a mailbox are routed to specific agents based on your unique needs.

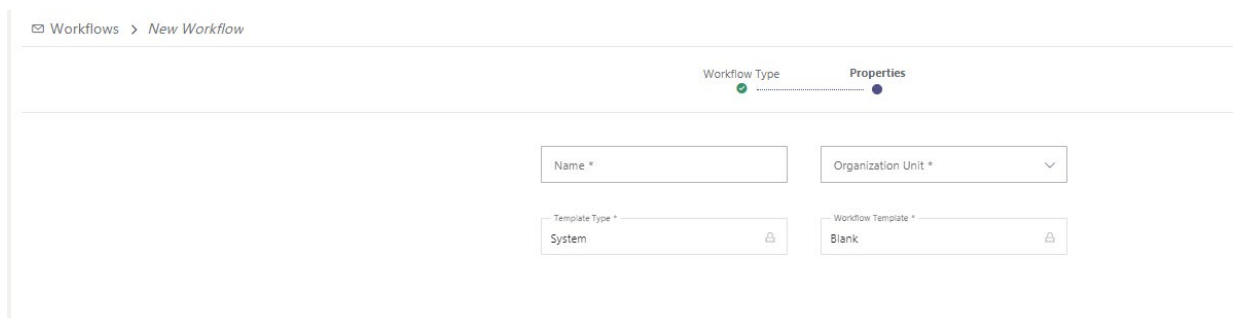
Email Workflow Template: Establish a set of workflow settings for emails. This reusable template can then be applied to multiple workflows.

To start creating your workflow, click the **Create New** button and select **Email**.

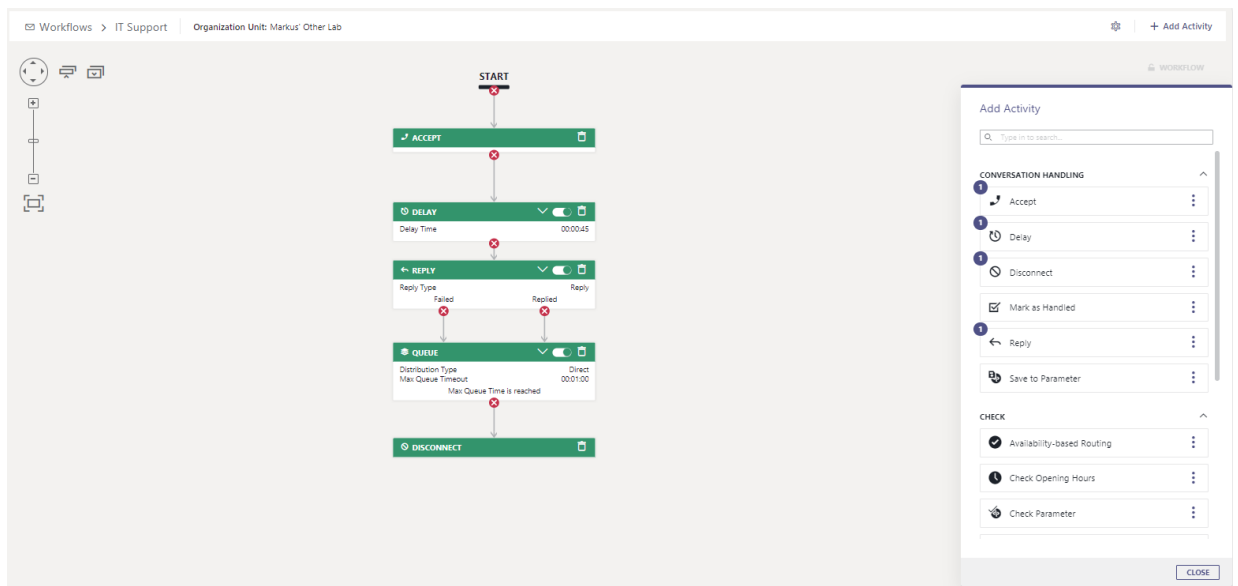
In this example we will create a new workflow.



Now, you can enter a name and select an **organization unit**. Then you can choose to use a blank workflow or an existing template.



Add and configure the workflow elements you need, and then save the workflow.

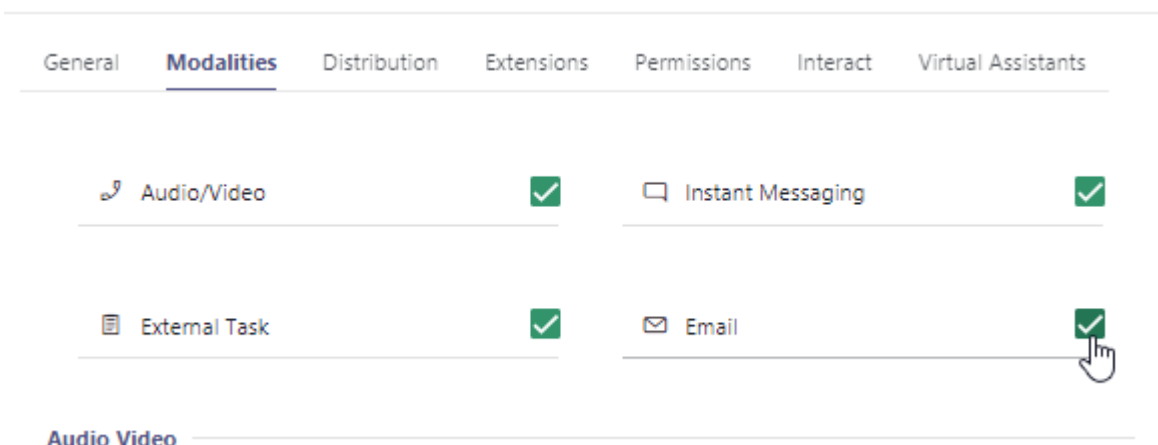


You are now able to assign an email workflow to a service.

2.3 Configure Service Settings for Distributing Emails

Once you've saved your workflow, it's time to select the service you want to enable email for.

Go to the **Modalities** tab and check the box next to **Email**.



Select the mailbox configuration and email workflow you created from the drop-down menus and save the service settings.

Edit Service > Contact Center

General **Modalities** Distribution Extensions Permissions Interact Virtual Assistants

START

ACCEPT

DISTRIBUTION PRIORITY

Priority High

Email

Email Workflow * IT Support

Mailbox * ITSupport

Subscription is enabled.

START

ACCEPT

DELAY

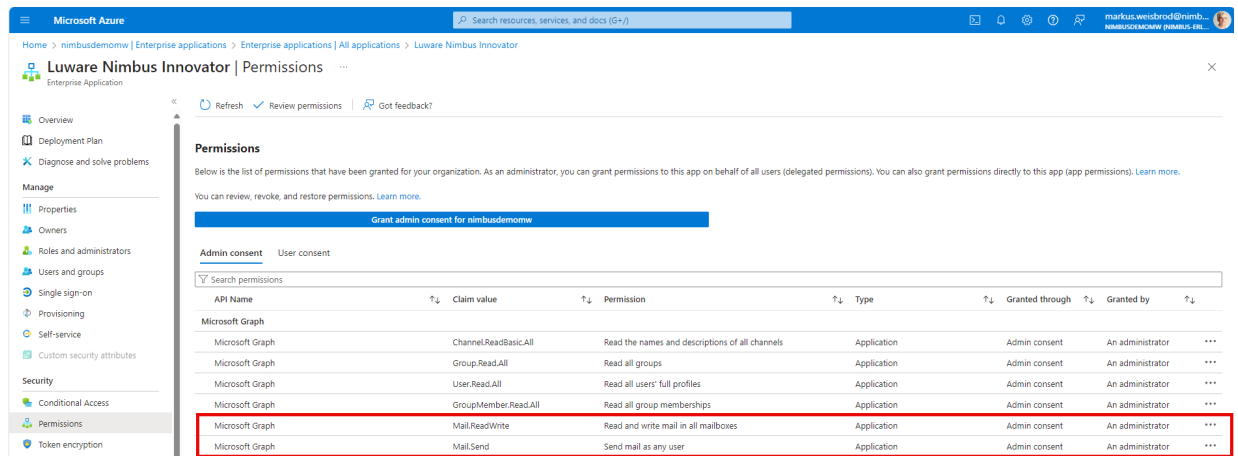
Delay Time 00:00:45

You have successfully configured the service to distribute emails according to your mailbox configuration and workflow. You can test the functionality by sending an email to the service.

3 Restricting Access to Selected Mailboxes

Once you run the Provisioning script, it will try to get two new application permissions:

- Mail.ReadWrite
- Mail.Send



If you wish to restrict Luware Nimbus access to certain mailboxes, you have to create an application access policy. Further information can be found on this Microsoft Website.

To limit Luware Nimbus access to selected mailboxes perform the following steps:

1. Connect to Exchange Online via PowerShell.
2. Identify a mail-enabled security group to restrict the app's access to.
3. Please take note of the AppId that corresponds to your Luware Nimbus deployment:
 - **Production Cluster:** af85ba37-5817-43d6-82e7-09004f08664e
 - **Innovator Cluster:** 953900f0-0e95-4116-80bf-de894301fa29
4. Run New-ApplicationAccessPolicy with the following parameters: **-AccessRight**

The AccessRight parameter specifies the restriction type that you want to assign in the application access policy. Valid values are:

- **RestrictAccess:** Allows the associated app to only access data that's associated with mailboxes specified by the PolicyScopeGroupID parameter.
- **DenyAccess:** Allows the associated app to only access data that's not associated with mailboxes specified by the PolicyScopeGroupID parameter.

-AppId

The Identity parameter specifies the GUID of apps to include in the policy. To find the GUID value of an app, run the command `Get-App | Format-Table -Auto DisplayName,AppId`.

For Luware Nimbus productive clusters use the following **AppId:** **af85ba37-5817-43d6-82e7-09004f08664e**

-PolicyScopeGroupID

The PolicyScopeGroupID parameter specifies the recipient to define in the policy. Valid recipient types are security principals in Exchange Online (users or groups that can have permissions assigned to them). For example:

- Mailboxes with associated user accounts (UserMailbox)
- Mail users, also known as mail-enabled users (MailUser)
- Mail-enabled security groups (MailUniversalSecurityGroup)

Use the MailUniversalSecurity Group option to add additional mailboxes in future (see chapter 2.6).

Connect to Exchange Online via PowerShell (see chapter 2.5) and run the

```
New-ApplicationAccessPolicy -AccessRight RestrictAccess -AppId "<Luware Nimbus AppId>" -  
PolicyScopeGroupId "<your MailUniversalSecurityGroup>" -Description "<your Description>"
```

e.g.

```
PS C:\Users\mweisbrod> New-ApplicationAccessPolicy -AccessRight RestrictAccess -AppId 953900f0-0e95-4116-80bf-de894301fa29 -PolicyScopeGroupId LuwareNimbusRestriction@nimbus-erleben.de -Description "Restrict Access to Nimbus Mailboxes only"
```

ScopeName	: Nimbus Luware Service Mailboxes
ScopeIdentity	: Nimbus Luware Service Mailboxes20240415122059
Identity	: 41f895-...
AppId	: 953900f0-...
ScopeIdentityRaw	: S-1-5-21-...
Description	: Restrict Access to Nimbus Mailboxes only
AccessRight	: RestrictAccess
ShardType	: All
IsValid	: True
ObjectState	: Unchanged

If you want to add additional mailboxes, you can add them as member to the MailUniversalSecurity Group.

You can test your **ApplicationAccessPolicy** with the following cmdlets.

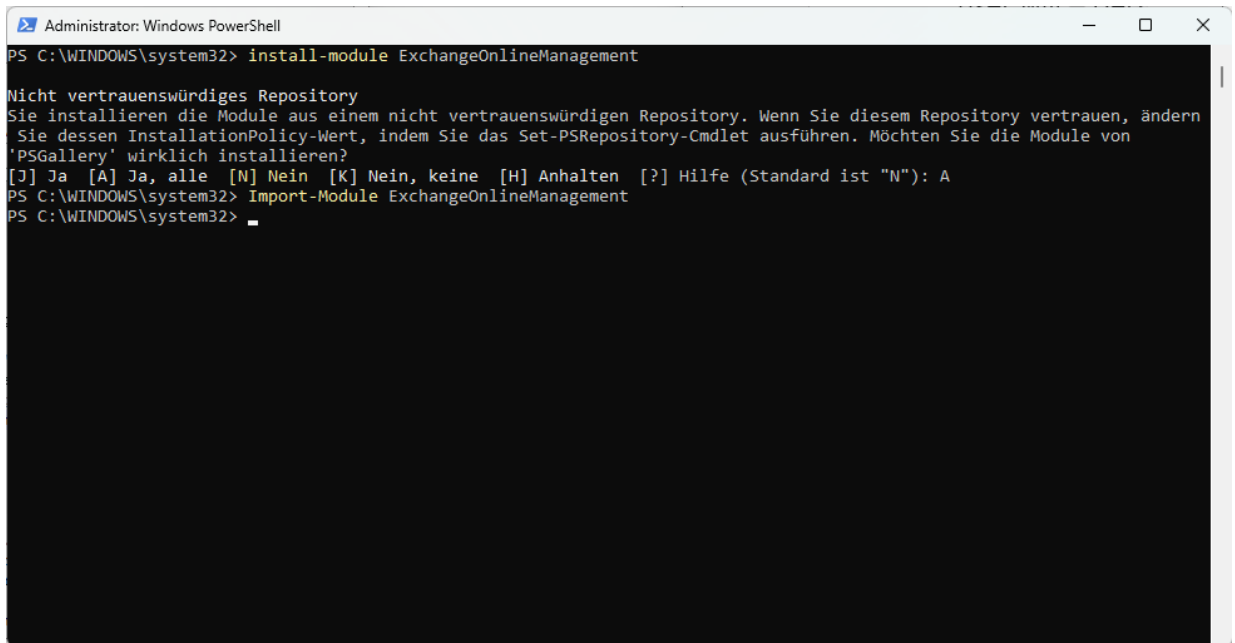
```
PS C:\Users\mweisbrod> test-ApplicationAccessPolicy -AppId 953900f0-0e95-4116-80bf-de894301fa29  
Cmdlet Test-ApplicationAccessPolicy an der Befehlspipelineposition 1  
Geben Sie Werte für die folgenden Parameter an:  
Identity: SalesSupport@nimbus-erleben.de
```

AppId	: 953900f0-...
Mailbox	: Sales Support
MailboxId	: 3fa4f188-...
MailboxSid	: S-1-...
AccessCheckResult	: Abgelehnt

3.1 Connect via PowerShell to Exchange Online

Open PowerShell in admin mode.

If you connect to Exchange Online through PowerShell on your computer, you will have to run the install and import cmdlets.



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> install-module ExchangeOnlineManagement

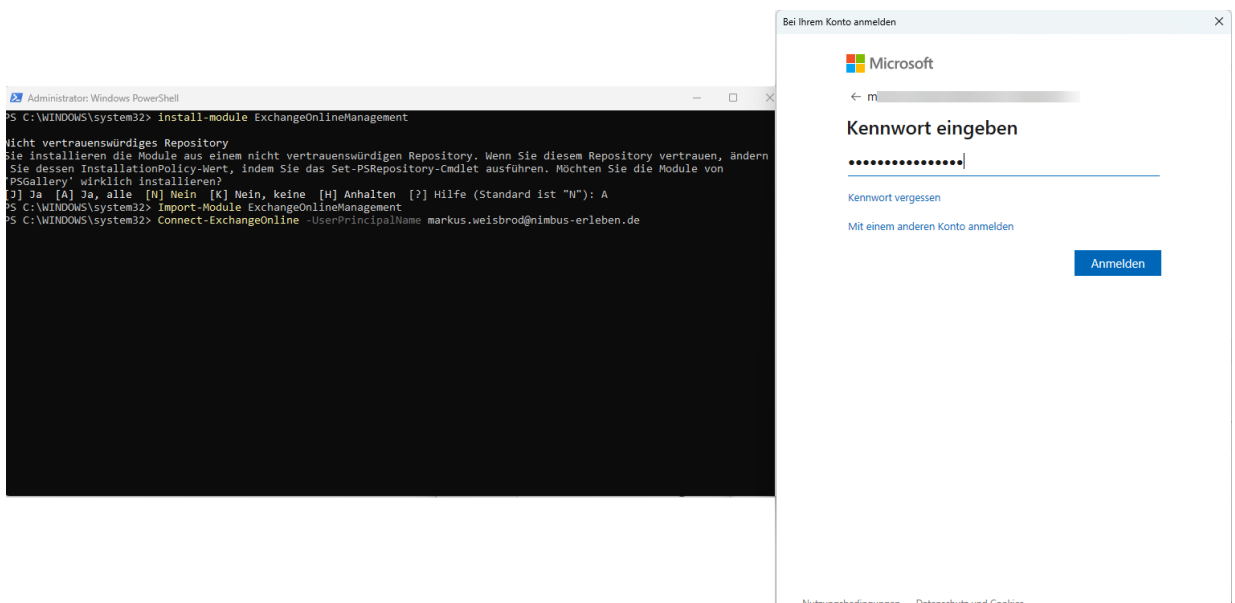
Nicht vertrauenswürdiges Repository
Sie installieren die Module aus einem nicht vertrauenswürdigen Repository. Wenn Sie diesem Repository vertrauen, ändern
Sie dessen InstallationPolicy-Wert, indem Sie das Set-PSRepository-Cmdlet ausführen. Möchten Sie die Module von
'PSGallery' wirklich installieren?
[?] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "N"): A
PS C:\WINDOWS\system32> Import-Module ExchangeOnlineManagement
PS C:\WINDOWS\system32>
```

If the module is already installed, you can usually skip this step and run Connect-ExchangeOnline without manually loading the module first.

Next, connect to Exchange Online.

Connect-ExchangeOnline -UserPrincipalName <UPN>

Please replace “<UPN>” by the UPN of an exchange administrator.



You are now connected to Exchange Online.

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> install-module ExchangeOnlineManagement

Nicht vertrauenswürdiges Repository
Sie installieren die Module aus einem nicht vertrauenswürdigem Repository. Wenn Sie diesem Repository vertrauen, ändern Sie dessen InstallationPolicy-Wert, indem Sie das Set-PSRepository-Cmdlet ausführen. Möchten Sie die Module von 'PSGallery' wirklich installieren?
[?] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "N"): A
PS C:\WINDOWS\system32> Import-Module ExchangeOnlineManagement
PS C:\WINDOWS\system32> Connect-ExchangeOnline -UserPrincipalName markus.weisbrod@nimbus-erleben.de

-----
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't require WinRM for Client-Server communication. You can now run these cmdlets after turning off WinRM Basic Auth in your client machine thus making it more secure.

Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with the RPS (V1) cmdlets.

V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and throttling errors inherently.

REST backed EOP and SCC cmdlets are also available in the V3 module. Similar to EXO, the cmdlets can be run without WinRM basic auth enabled.

For more information check https://aka.ms/exov3-module
-----

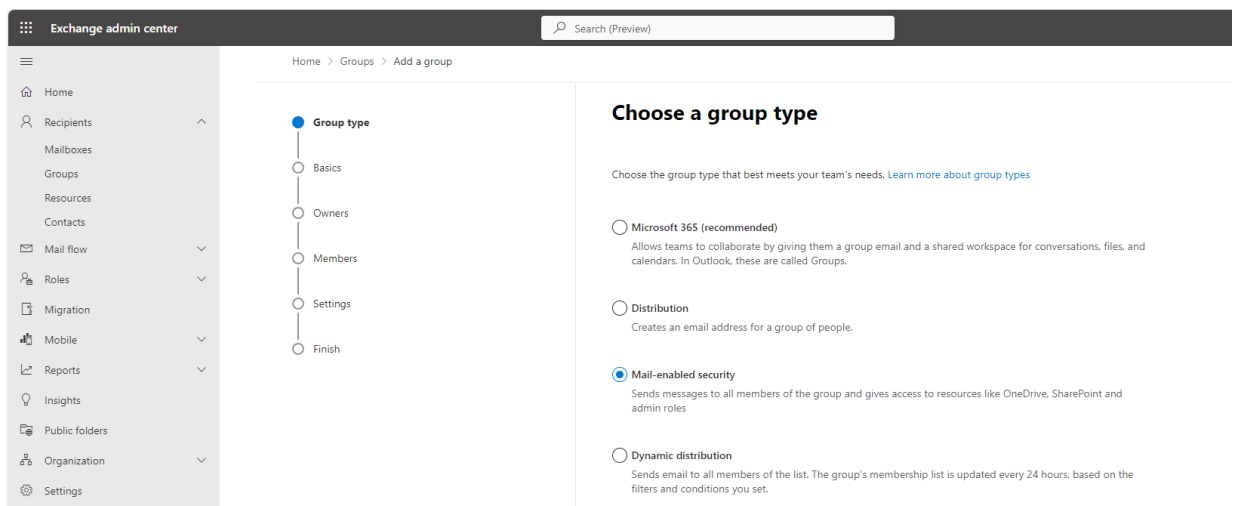
PS C:\WINDOWS\system32> _
```

and can run the `New-ApplicationAccessPolicy` command (see chapter 2.2).

3.2 Create a MailUniversalSecurity Group

Go to your Exchange admin center as an administrator. Choose **Groups** from the **Recipients** section. Click on **add a new group**.

Choose “Mail-enabled security” on the left.



Fill in Name and add a description.

Home > Groups > Add a group

- Group type
- Basics**
- Owners
- Members
- Settings
- Finish

Set up the basics

To get started, fill out some basic info about the group you'd like to create.

Name *

Description

Select the group owners.

Home > Groups > Add a group


- Group type
- Basics
- Owners**
- Members
- Settings
- Finish

Assign owners

Group owners have unique permissions to manage the group. They can add and remove members, chat settings, rename the group, update its description, and more.

ⓘ You have to have at least one owner. We recommend adding two, so one can help out in the other's absence.

+ Assign owners

- Display name
-  **Markus Weisbrod (Nimbus)**
markus.⋮

Select the mailboxes, which should be part of this restriction.


Home > Groups > Add a group

Add members

Group members have access to everything the group can access, and will receive email messages sent to email address. By default, they can invite guests to join your group, but they can't edit group settings.

+ Add members

Display name

 IT Support
ITS

Select an email address and the settings you would like to enforce.

Home > Groups > Add a group

Edit settings

Mail-enabled security group

Has all the functionality of a distribution list and additionally can be used to control access to OneDrive and SharePoint.

Group email address * Domains

Communication

Allow people outside of my organization to send email to this Mail-enabled security group

Approval

Require owner approval to join the group

Please note that you can only create a limited number of policies in your organization, based on a fixed amount of space. If your organization runs out of space for these policies, you will encounter an error message stating that the total size of **App Access Policies** has exceeded the limit.



solutions@luware.com

+41 58 404 28 00

www.luware.com

