



## **Microsoft Exchange Online Basic Authentication deprecation**

---

Documentation

---

---

# Document details

Version: Microsoft Exchange Online Basic Authentication deprecation  
Authors: Lisa Pulsinger, Diego Schleis  
Date: 30 September 2022

## Summary

This document explains the deprecation of the Microsoft Exchange Online Basic Authentication. It contains action steps that ensure continuous email sending with dox42.

## Basic Authentication Deprecation for Microsoft Exchange Online

Microsoft has deprecated Basic Authentication for Exchange Online on October 1<sup>st</sup> 2022:

<https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online>

That means, that if you use Exchange Online and Basic authentication (username and password) to send your dox42 emails, this may no longer work for you.

**If Microsoft has disabled Basic Authentication for your tenant, you have the possibility to re-enable the basic authentication once, during the period of October to December 2022.**

**From January 2023 onwards, Basic Authentication cannot be used any longer with Exchange online.**

Here you find a guide on how to re-enable basic authentication for Exchange Online:

<https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-deprecation-in-exchange-online-september/ba-p/3609437> (Re-Enabling Basic for protocols)

If you run into any troubles while sending emails with dox42, you can do the following:

### Option 1: Re-enable Basic Authentication

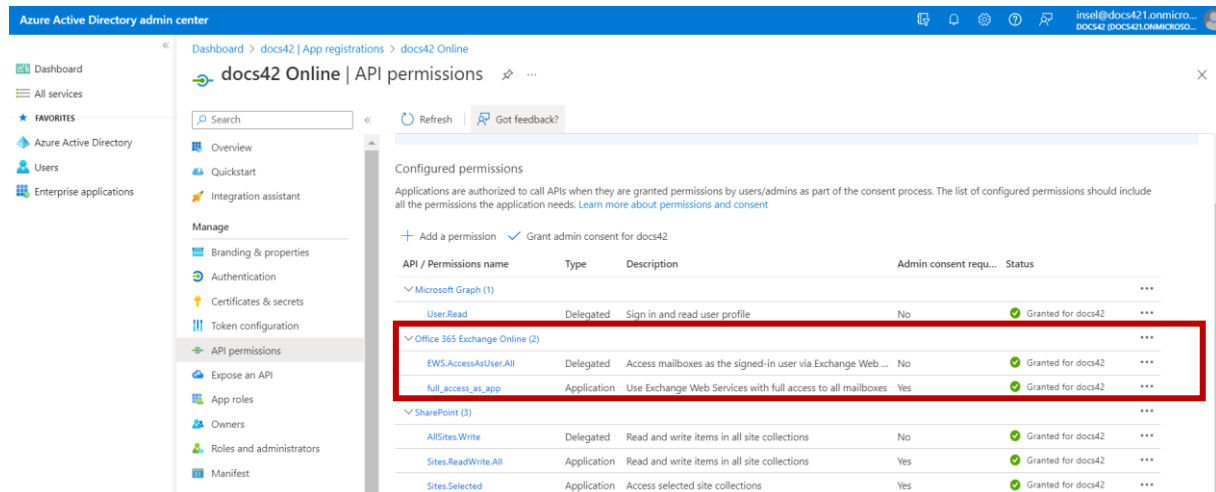
As a quick fix, you can switch back to Basic authentication, following the guideline in this link (Re-Enabling Basic for protocols) **(Only possible once between October and December 2022):**

<https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-deprecation-in-exchange-online-september/ba-p/3609437>

## Option 2: Add Exchange Online E-Mail method to your dox42 Server

Secondly, install the latest dox42 version (4.4.1.7 or later) and follow the instructions in this chapter to enable emails to be sent with Exchange Online and Azure Active Directory:

In your Azure AD App registration, add additional API Permissions and a client secret. You need the following permissions for Office 365 Exchange Online:



Azure Active Directory admin center

docs42 Online | API permissions

Configured permissions

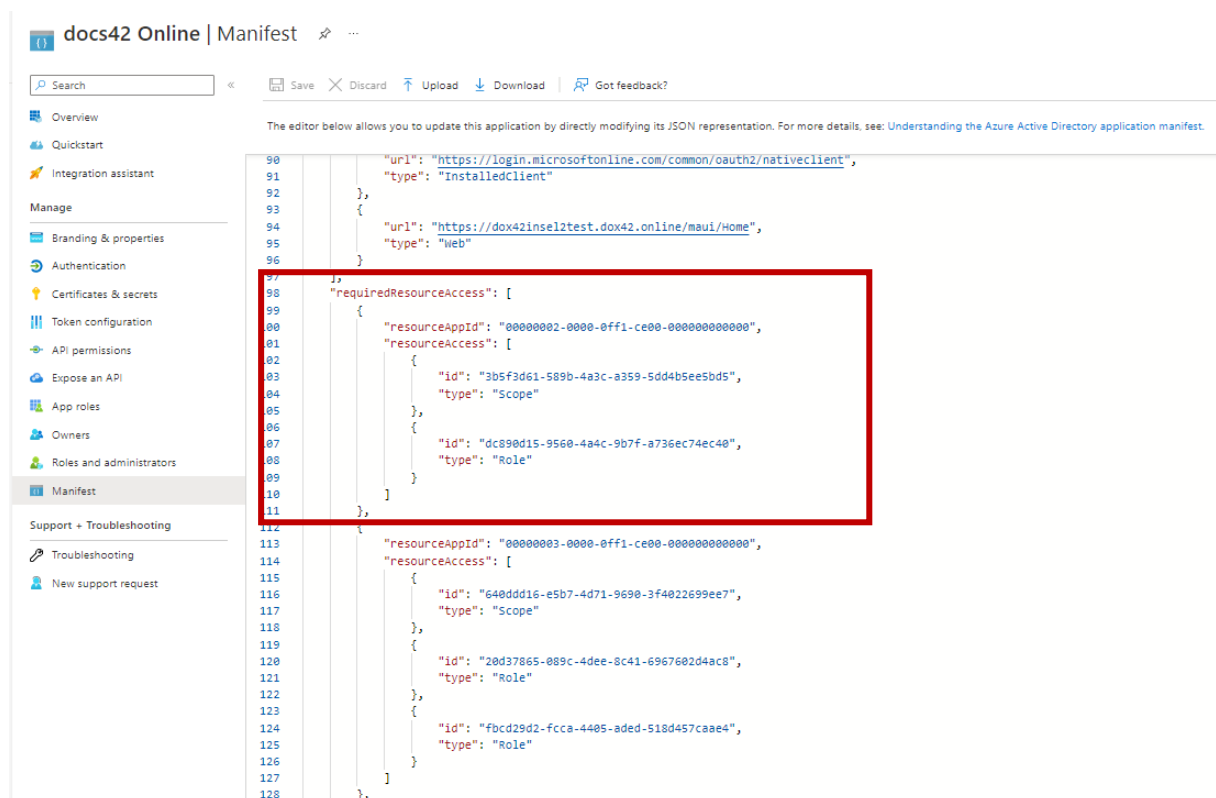
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for docs42

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for docs42
▼ Office 365 Exchange Online (2)				
EWS.AccessAsUser.All	Delegated	Access mailboxes as the signed-in user via Exchange Web ...	No	✓ Granted for docs42
Full access to all mailboxes	Application	Use Exchange Web Services with full access to all mailboxes	Yes	✓ Granted for docs42
▼ SharePoint (3)				
AllSites.Write	Delegated	Read and write items in all site collections	No	✓ Granted for docs42
Sites.ReadWrite.All	Application	Read and write items in all site collections	Yes	✓ Granted for docs42
Sites.Selected	Application	Access selected site collections	Yes	✓ Granted for docs42

Those permissions can be added via the manifest:

Under the „requiredResourceAccess“ Section, you need to add a new JSON object with the following values:



docs42 Online | Manifest

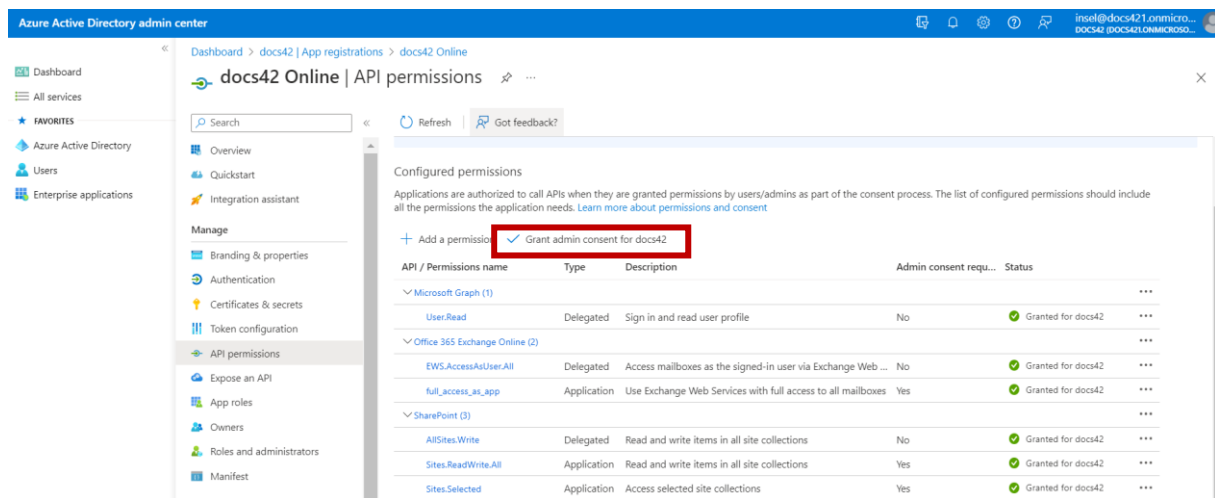
The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: [Understanding the Azure Active Directory application manifest](#).

```
90      "url": "https://login.microsoftonline.com/common/oauth2/nativeclient",
91      "type": "InstalledClient"
92    },
93    {
94      "url": "https://dox42insel2test.dox42.online/maui/home",
95      "type": "Web"
96    }
97  ],
98  "requiredResourceAccess": [
99    {
100      "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
101      "resourceAccess": [
102        {
103          "id": "3b5f3d61-589b-4a3c-a359-5dd4b5ee5bds",
104          "type": "Scope"
105        },
106        {
107          "id": "dc890d15-9560-4a4c-9b7f-a736ec74ec40",
108          "type": "Role"
109        }
110      ]
111    },
112    {
113      "resourceAppId": "00000003-0000-0ff1-ce00-000000000000",
114      "resourceAccess": [
115        {
116          "id": "640dd16-e5b7-4d71-9690-3f4022699ee7",
117          "type": "Scope"
118        },
119        {
120          "id": "20d37865-089c-4dee-8c41-6967602d4ac8",
121          "type": "Role"
122        },
123        {
124          "id": "fbcd29d2-fcca-4405-aded-518d457caae4",
125          "type": "Role"
126        }
127      ]
128    }
129  ]
130}
```

You can copy and paste it from here:

```
{  
  "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",  
  "resourceAccess": [  
    {  
      "id": "3b5f3d61-589b-4a3c-a359-5dd4b5ee5bd5",  
      "type": "Scope"  
    },  
    {  
      "id": "dc890d15-9560-4a4c-9b7f-a736ec74ec40",  
      "type": "Role"  
    }  
  ]  
}
```

Afterwards go to the API permissions section and click on “Grant admin Consent.



If you don't have a valid client secret yet, you need to add one to the app registration and copy the **value**. You can do this via the menu option “Certificates & Secrets”.

Search << Got feedback?

Overview  
Quickstart  
Integration assistant

Manage  
Branding & properties  
Authentication  
Certificates & secrets  
Token configuration  
API permissions  
Expose an API  
App roles  
Owners  
Roles and administrators

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (3) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Testing exchange	3/22/2023	-T6*****	e894fcd0-0aea-4f67-8a40-f85a77eec4d6
Testing exchange 2	3/22/2023	YwN*****	c79684f0-ee9c-4290-a3be-7025bd5d24c8
test exchange online new	3/27/2023	0vZ*****	23c7c119-f56b-4356-9c2a-85568a911a58

Further information on Azure AD app registrations can be found in our SharePoint and D365 CE documentations: [https://www.dox42.com/Resources?filter\[\]=dokumentation&](https://www.dox42.com/Resources?filter[]=dokumentation&)

If you use dox42 online, create a new SharePoint Site in MAUI with the Url <https://outlook.office365.com/>

Don't forget to add the AppId, Tenant ID and Client Secret.

Settings

Save and Deploy Cancel

Last deployed: 04.08.2022 16:43:48 WEST (UTC+01:00)

E-mail server smtps.tund1.de

E-mail address dox42online@dox42.com

Password

Error e-mail address

Sharepoint Online Sites

SharePoint

Url https://outlook.office365.com/

App ID app-id

Tenant ID tenant-id

Client Secret \*\*\*\*\*

Changes have to be deployed!

Cancel Confirm

Trusted Template Locations

Location

Add +

SharePoint

Url https://your/your-site

App ID

Tenant ID

Client Secret

Changes have to be deployed!

Cancel Confirm

Trusted Template Locations

Location

Add +

If you work with dox42 on-premise, you need to add the new SharePoint site to the Azure AD section of your web.config.

```
<azureAD>
  <add resource365=https://outlook.office365.com/
    appID="<client_id>" tenant="<tenant_id>" clientKey="<client_secret>" />
</azureAD>
```

**If you now use the dox42 Email Action with the parameter MailMethod "ExchangeOnline" and use a valid email address that can be impersonated by the app registration, the email should send successfully.**

Alternatively, you can also add the additional necessary parameters directly to your dox42 email call. However, since you pass sensitive information in that call (Client Secret), **we recommend using the configuration mentioned above in your web.config or your MAUI SharePoint sites** and to only add the parameter MailMethod "exchangeonline" to your email call.

The additional parameters for the Email Action are the following:

Name	Value
AzureADAppId	Application ID of app registration that has the necessary API permissions configured (can be configured in server too)
AzureADTenantId	Tenant ID in which the above app is registered (can be configured in server too)
AzureADClientSecret	Client secret that is associated with the application ID (can be configured in server too)
ExchangeOnlineUrl	This has a default value (" <a href="https://outlook.office365.com/EWS/Exchange.asmx">https://outlook.office365.com/EWS/Exchange.asmx</a> "), so can be sent without a value
MailMethod	"ExchangeOnline" shall be used as the value to trigger the exchange online send mode