Single sign-on for DocuWare Cloud

Installation guide

June 2020

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between DocuWare GmbH and the client and remains the exclusive property of DocuWare. If you find any problems in the documentation, please report them to us in writing. DocuWare does not warranty that this document is error-free.

This document was created using AuthorIT™, Total Document Creation.

Disclaimer

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by DocuWare GmbH. DocuWare GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

DocuWare GmbH

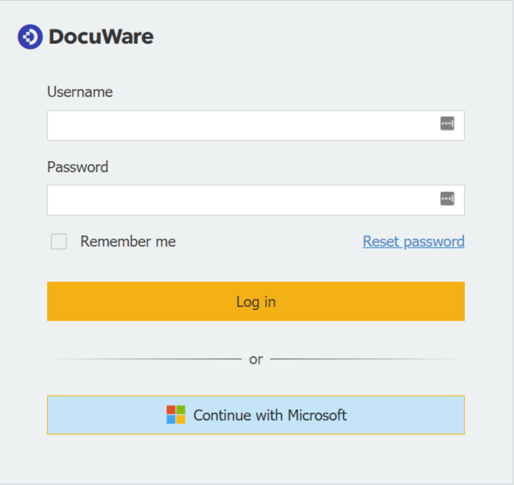
Planegger Straße 1

82110 Germering

www.docuware.com

Single sign-on for DocuWare Cloud

DocuWare supports Microsoft Azure Active Directory as an identity provider. DocuWare Cloud customers can now log in to DocuWare using single sign-on. Once a user has been registered with Azure Active Directory, a single login is enough to automatically log in to multiple parts of DocuWare like Web Client, the Desktop Apps, Configuration and Administration, as well as for user synchronization.

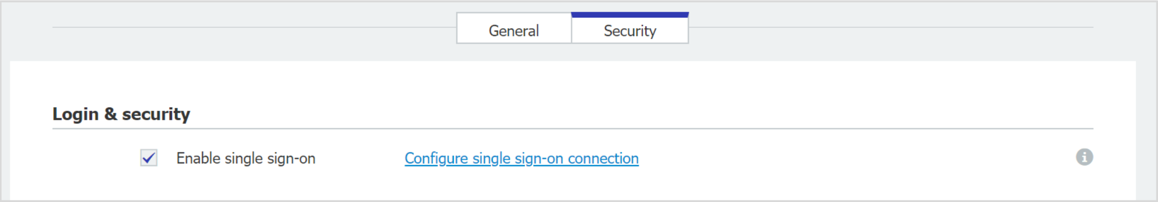


The new login dialog with single sign-on is now standardized everywhere in DocuWare Cloud – from the Web Client to DocuWare Configuration.

By clicking on the Single Sign-on button in the DocuWare login dialog, the user is forwarded to the Identity Provider. After successful authentication, the user automatically logs in to DocuWare, including the Web Client, Desktop Apps, Configuration and Administration and User Synchronization.

Connect DocuWare to Azure Active Directory

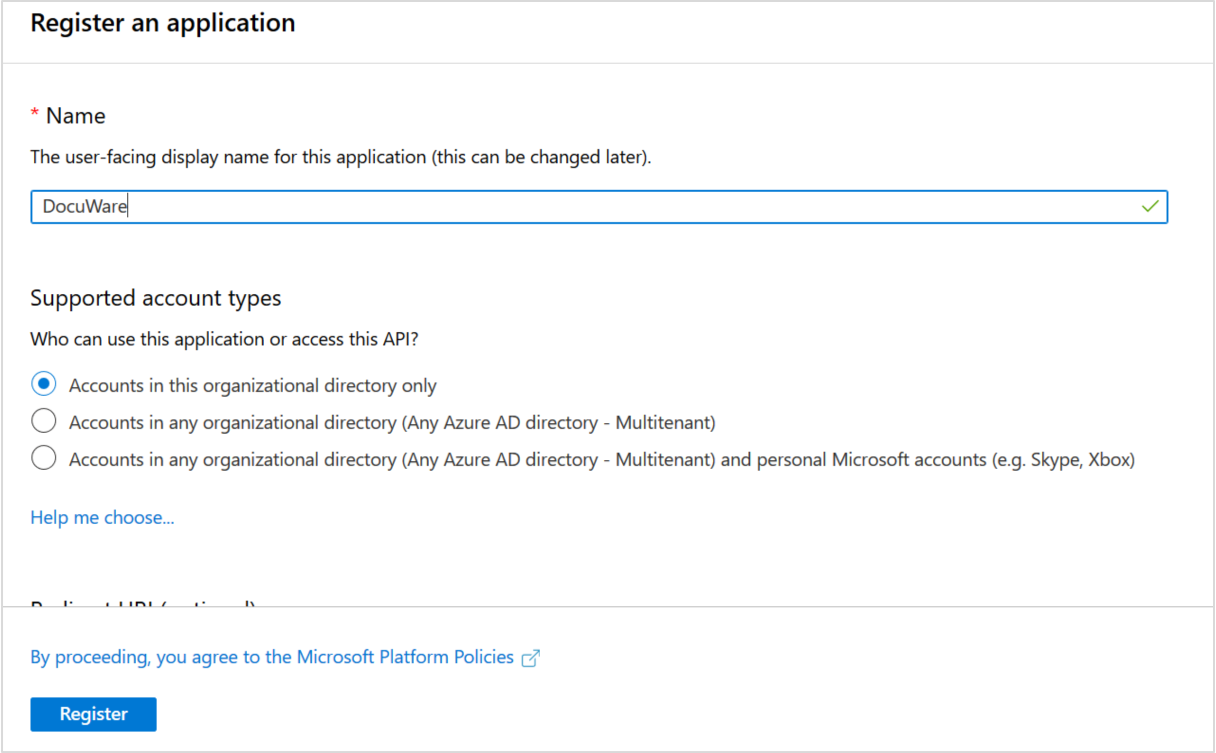
1. In *DocuWare configuration > Organization Settings > Security*, activate *Enable Single Sign-on.*



Login & security

☑ Enable single sign-on

2. Add a new app registration in Microsoft Azure Active Directory.



Register an application

* Name

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

DocuWare

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only

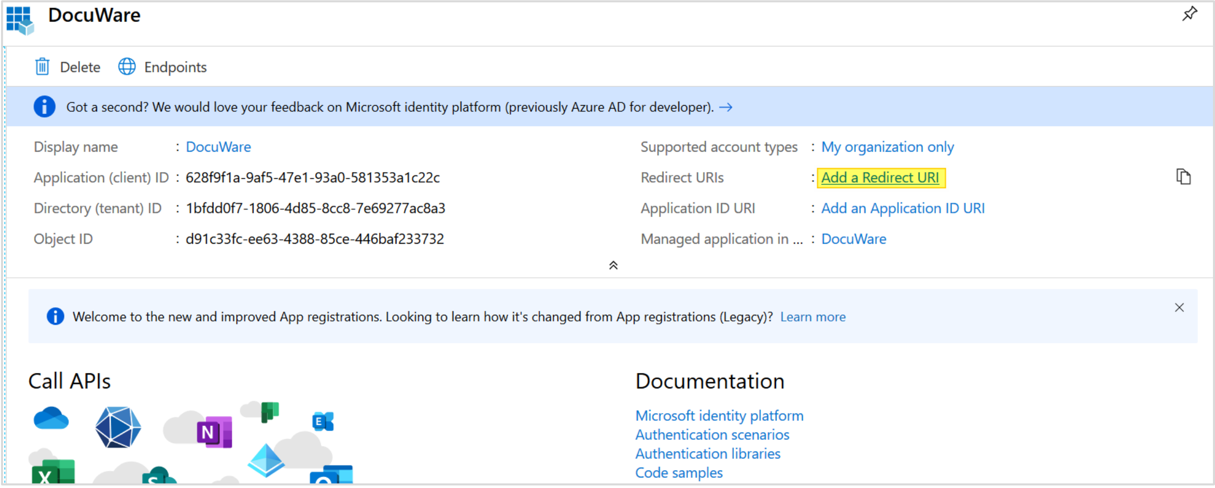
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

By proceeding, you agree to the Microsoft Platform Policies

3. Add a new Redirect URI for the created app registration.



DocuWare

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name	: DocuWare	Supported account types	: My organization only
Application (client) ID	: 628f9f1a-9af5-47e1-93a0-581353a1c22c	Redirect URIs	: Add a Redirect URI
Directory (tenant) ID	: 1bfdd0f7-1806-4d85-8cc8-7e69277ac8a3	Application ID URI	: Add an Application ID URI
Object ID	: d91c33fc-ee63-4388-85ce-446baf233732	Managed application in ...	: DocuWare

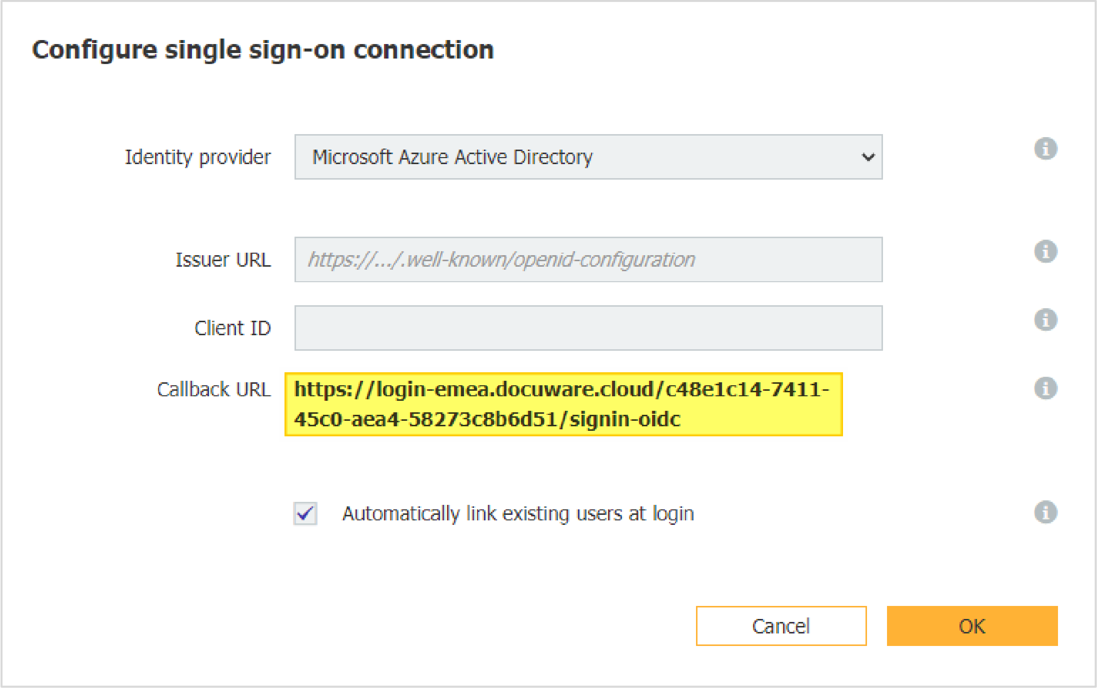
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Call APIs

Documentation

Microsoft identity platform
Authentication scenarios
Authentication libraries
Code samples

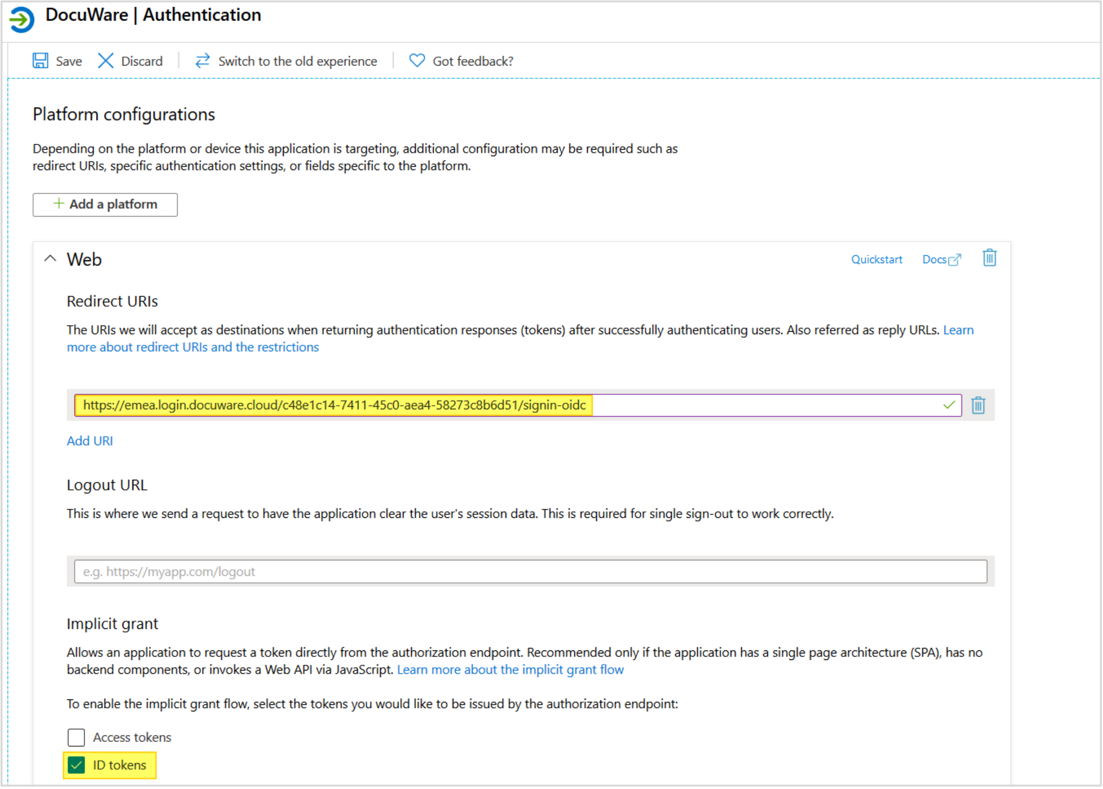
4. Copy the Callback URL from the DocuWare configuration in the *Organization Settings > Security > Configure Connection for single sign-on* area into the URI (Web) field and activate *ID tokens*.



Configure single sign-on connection

Identity provider	Microsoft Azure Active Directory
Issuer URL	*https://.../.well-known/openid-configuration*
Client ID	
Callback URL	**https://login-emea.docuware.cloud/c48e1c14-7411-45c0-aea4-58273c8b6d51/signin-oidc**

☑ Automatically link existing users at login



DocuWare | Authentication

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

Web

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred as reply URLs. Learn more about redirect URIs and the restrictions

https://emea.login.docuware.cloud/c48e1c14-7411-45c0-aea4-58273c8b6d51/signin-oidc

Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://myapp.com/logout

Implicit grant

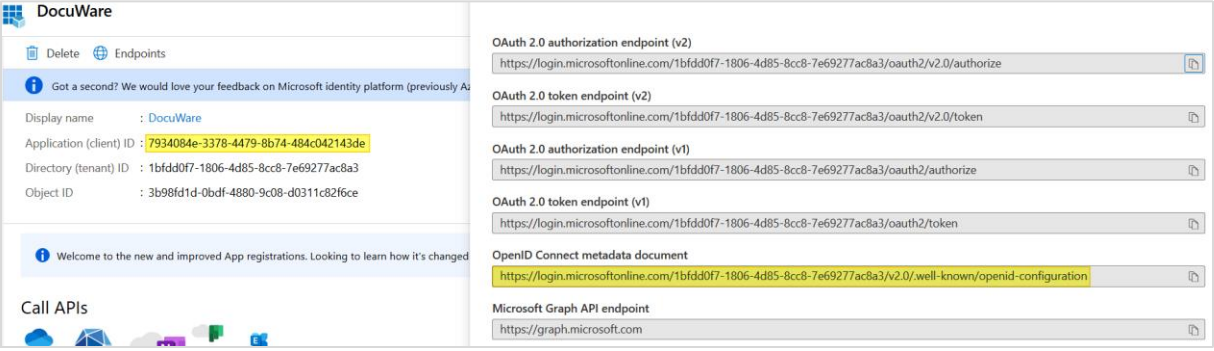
Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript. Learn more about the implicit grant flow

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens

☑ ID tokens

5. In the app registration overview, copy the *Application (client) ID* and under *Endpoints* the URL to the *OpenID Connect metadata document* and paste it into DocuWare under *Organization Settings > Security > Configure single sign-on connection* > for *Client ID* or *Issuer URL*



DocuWare

Delete Endpoints

Got a second? We would love your feedback on Microsoft identity platform (previously Az

Display name : DocuWare
Application (client) ID : 7934084e-3378-4479-8b74-484c042143de
Directory (tenant) ID : 1bfdd0f7-1806-4d85-8cc8-7e69277ac8a3
Object ID : 3b98fd1d-0bdf-4880-9c08-d0311c82f6ce

Welcome to the new and improved App registrations. Looking to learn how it's changed

Call APIs

OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/1bfdd0f7-1806-4d85-8cc8-7e69277ac8a3/oauth2/v2.0/authorize

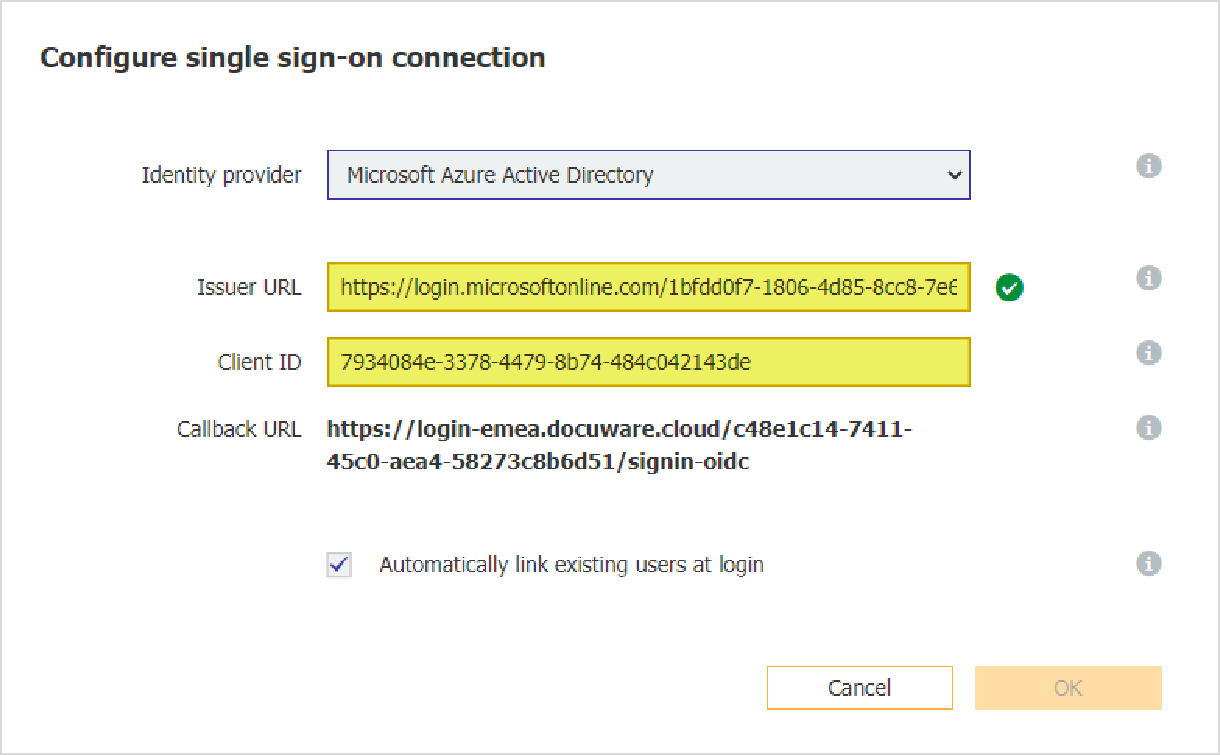
OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/1bfdd0f7-1806-4d85-8cc8-7e69277ac8a3/oauth2/v2.0/token

OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/1bfdd0f7-1806-4d85-8cc8-7e69277ac8a3/oauth2/authorize

OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/1bfdd0f7-1806-4d85-8cc8-7e69277ac8a3/oauth2/token

OpenID Connect metadata document
https://login.microsoftonline.com/1bfdd0f7-1806-4d85-8cc8-7e69277ac8a3/v2.0/.well-known/openid-configuration

Microsoft Graph API endpoint
https://graph.microsoft.com



Configure single sign-on connection

Identity provider: Microsoft Azure Active Directory

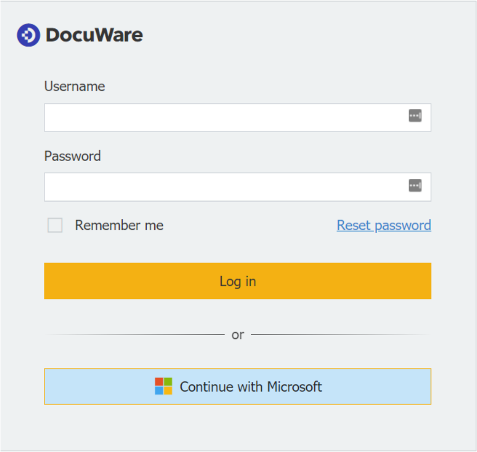
Issuer URL: https://login.microsoftonline.com/1bfdd0f7-1806-4d85-8cc8-7e€

Client ID: 7934084e-3378-4479-8b74-484c042143de

Callback URL: https://login-emea.docuware.cloud/c48e1c14-7411-45c0-aea4-58273c8b6d51/signin-oidc

☑ Automatically link existing users at login

6. After saving the settings, users can log in with DocuWare user name and password and also use single sign-on via Microsoft. Logging in using DocuWare credentials cannot currently be deactivated.



Note about the option *Automatically link existing users at login*

If this option is enabled, DocuWare searches for a matching existing DocuWare user with the corresponding username and email address the first time a user logs on with single sign-on. The DocuWare username must match the local part (first part to @) and the DocuWare email address must match the complete username in Azure Active Directory.

Only if username AND email address match will the Azure Active Directory user account and the DocuWare user account be connected.

Example:

Azure AD username:	*peggy.jenkins@peters-engineering.net*
DocuWare username:	*peggy.jenkins*
DocuWare Email address:	*peggy.jenkins@peters-engineering.net*

It is not necessary to create DocuWare users via the User Synchronization app in order to use single sign-on. Even if you create new users manually or import them via an interface, the external user account and the DocuWare account are automatically synchronized.

Once a user has been assigned, the user is recognized from this point on by his external object ID. This means that even if the email address and/or username no longer match, the user will still be recognized.