Documentation

> CDM-Server documentation is still a work-in-progress.

Please be sure to review these:

- Privacy Policy
- Privacy Policy [apis.de]
- Terms and Conditions [apis.de]
- CDM System Requirements

1 - Getting Started

How to install CDM-Server

> Installation/Maintenance requires an admin familiar with linux.

1.1 - System Requirements

Things you need for the server to run.

Processor

- x86-64 compatible server CPU
- 8-cores or more
- Example: Intel Xeon E5 or later/equivalent AMD Epyc

Memory (RAM)

- Minimum `16 GB`
- `32 GB` or more recommended

Storage

- SSD with at least `10 GB` free storage space for application, database, and container
- Or more, depending on the data volume

Operating System

> As we use Linux OCI images (Docker), it should run without any problems on any current operating system with Docker support that can handle Linux.

Recommended OS: Ubuntu `20.04` LTS and Ubuntu `24.04` LTS

We do not support Windows at this moment. If you still want to run it on Windows, here's a guide.

Software requirements

Common Linux Utils

- `curl`, `tar`, `nano` (or alternatives)

Docker

- Docker Engine `v27.2.0+` with docker-compose-plugin `v2.29.7+`
- Example:

```
➜  docker --version
Docker version 27.3.1, build ce12230
➜  docker compose version
Docker Compose version v2.29.7
```

You may also try alternatives such as Podman, we do not support it at the moment.

Network requirements

- Stable network connection with sufficient bandwidth for data transfer between server and clients. `1+ gbps` recommended

Security requirements

User privileges

- Make sure that the server has the appropriate user rights for managing Docker containers.

Firewall

- Configure the firewall to allow the traffic required to access the application.
  - Incoming Port 443 (or custom) for HTTPS (For IQ-Software, CDM-Server Webapp).
  - Outgoing Port 636 (or custom) for LDAPS
  - Outgoing Port 443 for HTTPS for Azure, OCI Image Pulls, etc.

1.2 - Installation

How to install CDM-Server

> **Linux Knowledge Required**
>
> Installation requires an admin familiar with Linux. You will need to enter the commands in a terminal. The instructions here assumes you have common utilities like `curl`, `tar`, `nano` installed.

Step 1: Install Docker Compose

Make sure Docker Engine (with `docker-compose-plugin`) is installed on your system. See System Requirements for more details.

Step 2: Download the Docker-Compose and Other Files

Automatic

Go to the directory you want to CDM-Server run from, and execute:

Version | latest | v1.1.1 | Older Versions

```
curl -s https://get.apis.de/cdm.sh | bash
```

CDM-Server changelogs are available here.

Manual

Step 3: Create the `DotEnv` Files

To use the server, you need to provide some data in the form of **two** `DotEnv` files:

- `.env`
- `.env.idp`

Create new `DotEnv` files, copy the contents of the example files, and update the values with your own configuration.

`.env` File

Example: `.env.example`

```
cp .env.example .env && nano .env
```

`.env.idp` File

Example: IdP (ID Provider) specific `DotEnv` files:

- `.env.idp.azure.example`
- `.env.idp.ldaps.example`
- `.env.idp.local.example`

Select Identity Provider | Local | Azure | LDAPS

```
cp .env.idp.local.example .env.idp && nano .env.idp
```

> **Detailed DotEnv Guide**
>
> More details here: Setting Up DotEnv Files

Step 4: Login and Download CDM-Server Images

Use the following command to login and download the `CDM-Server images`. You'll be asked to enter username and password.

APIS CDM-Server Account

You need to have a valid account to download the images. If you don't have one yet, please contact customer service through Support Page

```
sudo ./download
```

Step 5. Start the CDM-Server Services

```
sudo ./start
```

How to Stop

In case, you need to stop CDM-Server services:

```
sudo ./stop
```

Step 6. Access CDM-Server

Please see Login for more information.

1.3 - Update

How to Update CDM-Server

If you want to update your CDM-Server instance to a new version, the steps are quite simple:

Step 1: Take a Backup

Please see this page for backup instructions.

Step 2: Update

> IMPORTANT
>
> Stop the server before performing update. You can do this by calling `./stop`

You need to download the new version and (re)start the server.

This is essentially, Step 2, Step 4 and Step 5 of installation process.

So just follow those steps again. In other words:

- Follow Installation Step 2 (Download the Docker Compose and Other Files)
- Follow Installation Step 4 (Download the CDM Images)
- Start the server

> Changelogs
>
> You can find the changelogs for each version here.

1.4 - Setup Environment

How to set up your environment to use the server.

Please set some basic details of the server in the `.env` file. You can find the `.env.example` file in the root directory of the project.

> **Warning**
>
> Securing file-system access of the host is important. Please make sure that your custom certificate files, `.env`, `.env.idp` files etc. are not accessible to unauthorized users.
> You should also ensure unauthorized persons do not have access to the docker containers.
> Ensuring the host server is secured, is your responsibility.

Configuration

```
cp .env.example .env && nano .env
```

```
## HELP
# https://get.apis.de/docs/server/env/

## ABOUT
# This will be used to create the root business unit
# Do not use special characters
COMPANY_NAME=

## CDM HOST and PORT
# The hostname to access the server.
# Must not contain protocol such as https://
# Must not have port number
# Must not have trailing slash
# Example: cdm.example.com
CDM_HOST=localhost

# Just the port number; 443 recommended
# Default port is 443
CDM_PORT=443
```

```
## USE CUSTOM HTTPS CERTIFICATE FOR CDM-SERVER (PRIVATE-KEY)
# If you have a custom certificate (private-key), set this to true.
# You need to place the custom certificate in the same directory as your `docker-compose.ym
# The certificate file name must be `cdm-server.pfx`
# For a false value, a self-signed certificate will be created and used for HTTPS.
# Please check [help docs for more information](https://get.apis.de/docs/server/https/).
# Default is false
USE_CUSTOM_CERT=false

### CUSTOM CERTIFICATE PASSWORD
# If you are using a custom certificate (`USE_CUSTOM_CERT=true`) and your certificate is pa
# Otherwise, leave it empty.
CUSTOM_CERT_PASS=
```

Example

```
COMPANY_NAME=APIS Informationtechnologien GmbH
CDM_HOST=cdm.apis.de
CDM_PORT=443
USE_CUSTOM_CERT=true
CUSTOM_CERT_PASS=supersecretpassword
```

COMPANY_NAME

This is the name of your company. It will be used to create the root business unit.

USE_CUSTOM_CERT

See HTTPS for more information.

Setup Up ID Provider (IdP)

After you are done setting up `.env`, please head over to the IdP Docs to setup `.env.idp` file.

Permissions for the `DotEnv` Files

It is recommended that you do not allow other users in same server system to read the `DotEnv` files as some of them can contain credentials. You can try `chmod 600` on all of them.

1.5 - HTTPS

How to use HTTPS to secure against various threats

CDM-Server takes the secure-by-design approach and thus enforces HTTPS.

HTTPS to Access CDM-Server

If you set the `USE_CUSTOM_CERT` environment variable to `true`:

- You can provide your own certificate. The server will use these files to serve HTTPS.
- This can be self-signed or CA-signed (recommended).
- There is a dummy file `./cdm-server.pfx` where you have downloaded the CDM-Server. Just replace it with your own certificate.

> ### Warning
>
> If your certificate has a password, please set `CUSTOM_CERT_PASS` environment variable. Otherwise, leave it empty.

> ### PFX
>
> If you have a `.cer` and `.key` file, you can convert it to `.pfx`. More details here: Create PFX.

Renew Certificate

> ### Live Reload
>
> At this moment, CDM-Server does not support on-the-fly certificate renewal. This will be supported in a future release.

Once you have the renewed certificate file

- Stop the server
- Replace the file

- Restart the server

This will apply the new certificate.

Self-Signed Certificate

If the variable is set to `false`, the server will generate and use a self-signed certificate. You can find it in

- `./.data/certs/<CDM_HOST>.cert.p7b` - X.509 certificate (contains the public key) that you can import to your browser.
- `./.data/certs/<CDM_HOST>.pfx` - Certificate in `PKCS#12` format. It contains private Key **that you should not share**.

> **Warning**
>
> Using self-signed certificate is not recommended for production.

Install Self-Signed Certificate on User's Machine

Please see Install Self-Signed Certificate for more information.

LDAP over SSL

For this, look into LDAP documentation.

1.6 - Login

How to login to CDM-Server

1. Open your browser and navigate to the CDM-Server URL. The module select page will appear.
2. Click `Dashboard`
3. In case of `Local` or `Ldaps`, enter your username and password
4. In case of `Azure`, you will be redirected to Azure login page.

> ### CDM-Server URL
>
> This is always `https://<CDM_HOST>:<CDM_PORT>/`.
> For example,
>
> - `https://cdm.example.com/` (default port 443; no need to specify)
> - or `https://cdm.example.com:8443/` (if you are using a different port)

2 - ID Provider

Details on the ID Providers supported by the CDM-Server and how to configure `.env.idp` file.

The CDM-Server supports various ID Providers (IdP) for authentication and user management. You need to choose one according to your organization's requirements and configure it accordingly.

What is the Benefit

Main reason to use non-local IdP is to allow users to use their existing corporate credentials to log in to the CDM-Server.

The CDM-Server supports the following ID Providers:

- Local - Users are managed internally by the CDM-Server. Easiest to set up and use.
- LDAPS - Users are managed by an LDAP server. Requires an external LDAP server present.
- Azure - CDM-Server uses Microsoft Azure for authentication. **This will be available soon**.
- Jazz - CDM-Server uses IBM Jazz for authentication. **This is not available yet**.

How to Configure

- The ID Provider configuration is done using the `.env.idp` file.
- For information about `.env` file, please go to the Setting Up .env File page.

WARNING

At this moment, you can not change the ID provider once the server is started. Please be sure to finalize the configuration before starting the server.

2.1 - Local

How to set up the local identity provider.

This IdP is the default IdP for the CDM-Server. It is used to authenticate users against the local user database. It uses an industry standard hashing algorithm to store passwords securely and authenticate users against the stored hash. All passwords require rotation every 180 days and must be at least 8 characters long. The admin can reset passwords for users if needed.

Configuration

In the `.env.idp` file, the following variables are used to configure the local IdP:

```
## HELP
# https://get.apis.de/docs/idproviders/local/

## USER MANAGEMENT
# Available options: local, azure, ldaps
ID_PROVIDER=local

### User Management -> LOCAL
# Only required if ID_PROVIDER=local
# We will create one root admin user using credentials below
# You will need to change password after login

## Root User Login
# Example: admin
ROOT_LOGIN=

## Root User Password
# Must be at least 8 characters long.
# Don't use special characters.
ROOT_PASSWORD=
```

> **Note**
>
> It is recommended to use simple English characters for the `ROOT_LOGIN` and `ROOT_PASSWORD` values.

Example

```
ID_PROVIDER=local
ROOT_LOGIN=admin
ROOT_PASSWORD=admin
```

> **WARNING**
>
> The admin should login as soon as possible and should change the password.

2.2 - LDAPS

How to set up the LDAPS identity provider.

Setup Instructions for connecting CDM Server to LDAP

Purpose

This guide provides information and instructions for configuring CDM Server to log in using an LDAP as Identity Provider.

The LDAPS ID Provider

The CDM Server provides an embedded LDAPS ID-Provider which enables LDAPS connections to e.g. a Company's LDAP server. The connection(s) to the LDAP are established using a connection pool which needs an LDAP user account to connect.

This LDAP connection account is used for every query from CDM-Server to the configured LDAP independent of the rights of the authenticated user. This means all queries are executed on LDAP with the LDAP permissions of the configured Connection Pool user.

CDM Server only needs the permissions to read users and groups in sub nodes under one parent node which are relevant to be used in CDM Server workflows.

Prerequisites

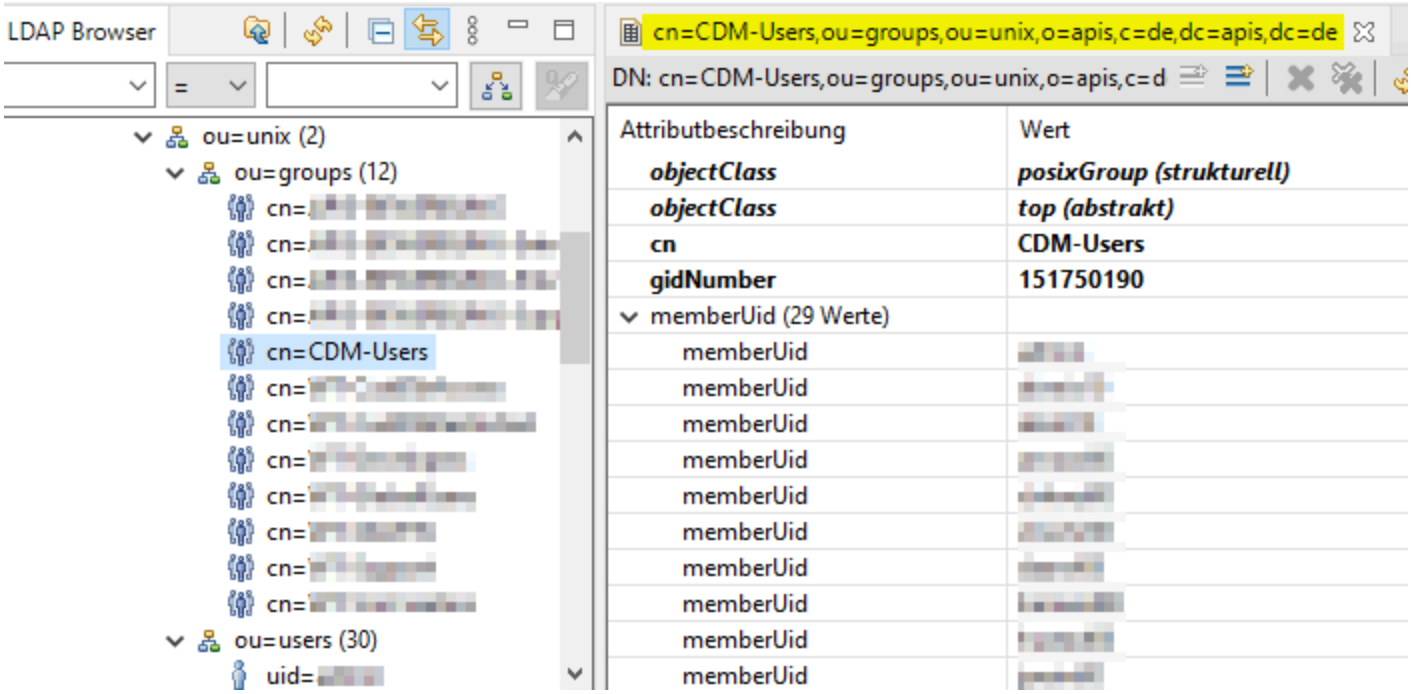
The CDM Server supports authentication of users on behalf of an LDAP Service. An existing or new Login-Group and an Admin-User is needed to configure the CDM-Server.

LDAP Authentication of users via CDM-Server

The CDM-Server embedded LDAPS ID-Provider can be used to authenticate user LDAP credentials against the companies LDAP. LDAP group informations can also be connected to cdm server roles. After this configuration in CDM-SERVER setup CDM users automatically are linked to roles matching the users group - role configuration.

> Tipp

> CDM Server users from external systems which should be able to access CDM-Server must be member of the same group. This group must be configured by Admin user as Login Group at first CDM-Server start.



In the image above a CDM-Users group is defined which contains the users that are allowed to use the CDM Server. All of them can log in after configuration is finalized.

LDAP Authentication of users via CDM-Server

The CDM Servers embedded LDAPS ID-Provider can be used to authenticate users LDAP credentials agains the companies LDAP. LDAP group information can also be connected to cdm server roles. After this configuration in cdm server setup CDM users automatically are linked to roles matching the users group - role configuration.

Here is a sample `.env.idp` file with the `ldaps` IdP configured:

```
## HELP
# https://get.apis.de/docs/idproviders/ldaps/

## User Management
# Available options: local, azure, ldaps
ID_PROVIDER=ldaps

### User Management -> LDAP
# Only required if ID_PROVIDER=ldaps
# LDAPS server host
```

```
AUTH_HOST=

## LDAPS server port
# Change it if you are using a different port
AUTH_PORT=636

## The DN of the user to use to query the LDAP server. This user must have read access to t
# Example: uid=admin,ou=users,o=companyname,dc=domainname,dc=country
AUTH_USER=

## Password for that user
AUTH_PASSWORD=

## User Management -> LDAP -> Internal References
# The full DN of the user in LDAP who is considered admin (This account is needed for serve
# Example: uid=admin,ou=users,o=companyname,dc=domainname,dc=country
LDAP_ADMIN_DN=

## The base DN for the LDAP group tree
# Example: ou=groups,o=companyname,dc=domainname,dc=country
LDAP_GROUP_TREE_DN=

## The template for the login name. This is used to construct the full DN of the user to au
# Must contain {loginName} as a placeholder for the login name.
# Example: uid={loginName},ou=users,o=companyname,dc=domainname,dc=country
LDAP_LOGIN_TEMPLATE=

## USE CUSTOM HTTPS CERTIFICATE FOR LDAPS (PUBLIC-KEY)
# We always use HTTPS for LDAP.
# If you have a self-signed certificate for your LDAP instance, set this to true.
# You need to place the custom certificate (public key) in the same directory as your `dock
# The certificate file name must be `cdm-ldaps.pfx`
# For a false value, we will attempt to validate the LDAP-Server certificate and it will fa
# Default is false
LDAP_CUSTOM_CERT=false
```

Inital CDM Server configuration workflow

Before first CDM-Server start an ID Provider specific configuration for the Admin User has to be setup in the environment of the docker container. Therefore the parameters LDAP_ADMIN_DN and LDAP_LOGIN_TEMPLATE have to be set to a valid LDAP DN (Distinguished Name) and matching login template. The LDAP_GROUP_TREE_DN parameter is needed, too.

The following table shows an example configuration.

Environment Parameter	Value
LDAP_ADMIN_DN	uid=admin,ou=users,o=companyname,dc=domainname,dc=country
LDAP_LOGIN_TEMPLATE	uid={loginName},ou=users,o=companyname,dc=domainname,dc=country
LDAP_GROUP_TREE_DN	ou=groups,o=companyname,dc=domainname,dc=country

2.3 - Azure

How to set up the Azure identity provider.

Setup Instructions for connecting CDM Server to Azure

Purpose

This guide provides information and instructions for configuring CDM Server to log in using Microsoft Azure AD as Identity Provider.

Prerequisites

To be able to use Microsofts Azure Entra ID as ID Provider in CDM Server you need to make some configurations in Azure. Therefor you need

- Access to the Azure Portal.
- Permissions to create and manage Azure AD applications.
- The client redirect URI from the CDM-Server.

> Tipp
>
> CDM Server users from external systems which should be able to access CDM-Server must be member of the same group. This group must be configured by Admin user as Login Group at first CDM-Server start.

Step 1: Configure an Azure application as ID-Provider for CDM Server

- Azure - Configure Application

Step 2: Configure the CDM Server to use the azure application for authentication in CDM Server using the azure users.

- Azure - Configure CDM-Server

After succedding above steps the Azure Users which are in the configured group should be able to log in to the CDM Server!

Warning About Data Loss

Please note that, at this moment, we do not support changing the IdP without clearing all data. This means, if you set up a CDM-Server instance for testing using `Local` or `Ldaps` for now, you will have to clear all data and start fresh when you want to switch to `Azure`.

Here is a sample `.env.idp` file with the `azure` IdP configured:

```
## HELP
# https://get.apis.de/docs/idproviders/azure/

## User Management
# Available options: local, azure, ldaps
ID_PROVIDER=azure

## User Management -> AZURE
# Only required if ID_PROVIDER=azure

# The Microsoft Azure AD Directory (Tenant) ID
# The Tenant ID is an UUID and contains hexadecimal numbers (0-9a-f) seperated by - and
# can be found in Azure Portal on the Entra-ID welcome page.
#
# Example: "e53f2a45-f4d2-a11d-223a-77b654c12df5"
AZURE_TENANT_ID=

# The Azure Application (Client) ID
# The Application client ID is an UUID and belongs to the application which is configured
# for the authentication and authorization of azure users for CDM Server. The Id can be
# found in Azure Portal -> App registrations.
#
# Example: "53a12b45-1234-5566-8fe4-93b787a787d6"
AZURE_CLIENT_ID=

# The Azure Application (Client) Name
# The Application client Name is a Text and belongs to the application which is configured
# for the authentication and authorization of azure users for CDM Server. The Name can be
# found in Azure Portal -> App registrations.
#
# Example apis_cdm_authentication
AZURE_CLIENT_NAME=

# The Azure Admin UUID
# The Azure admin UUID must be the id of the Azure user who is going to configure CDM Serve
```

```
# The user which belongs to the id is then an admin user and the only user which is able to
# CDM Server to complete the configuration.
#
# To get your Azure user id log in to https://portal.azure.com/ click on view entra and in
# in the middle area of the entra welcome page the user id is shown.
#
# Example fd163a2f-112a-7291-bdf4-a4325b78910a
AZURE_ADMIN_UUID=
```

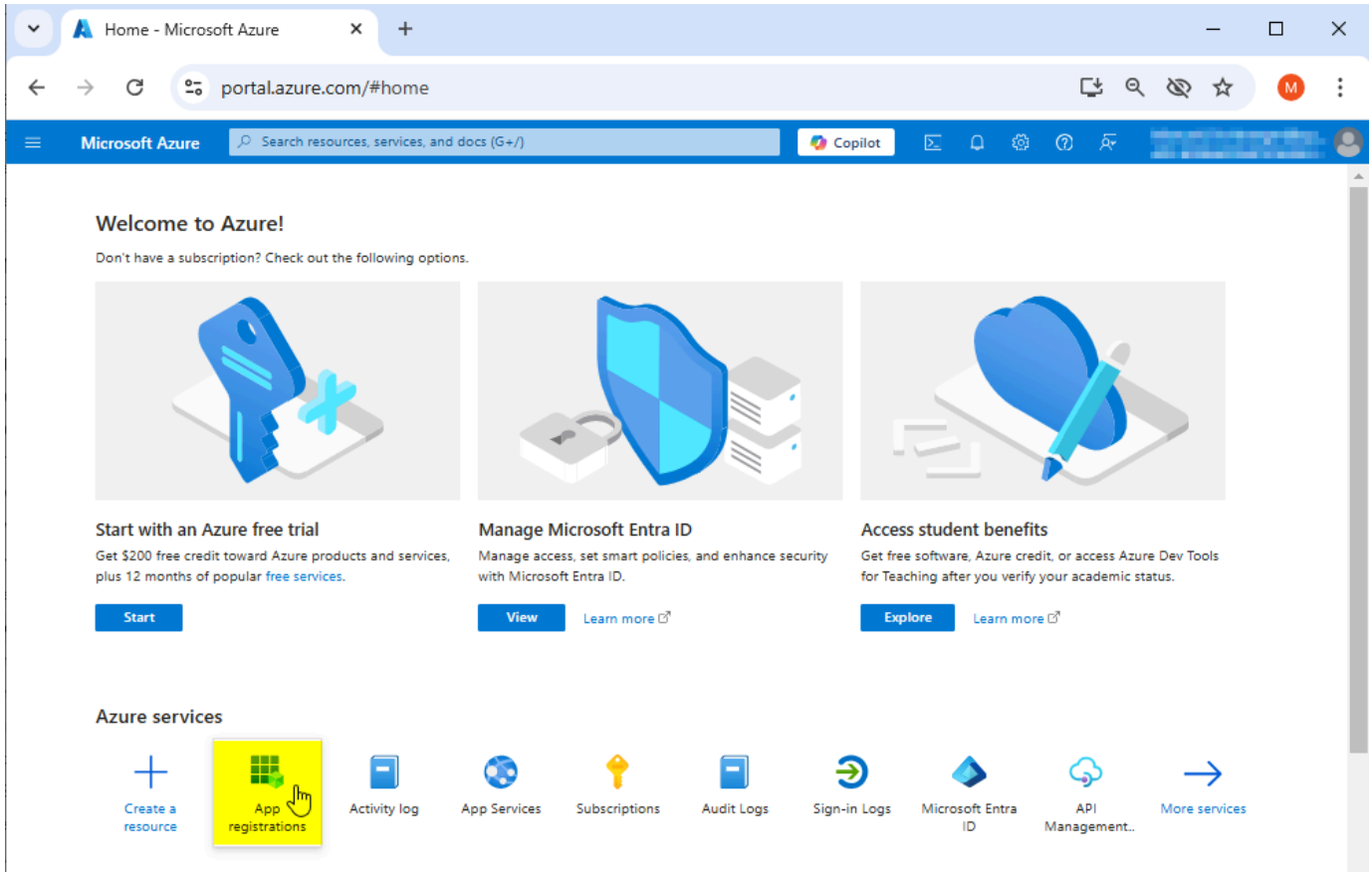
2.3.1 - Azure Portal Setup

How to configure an Azure application as Identity Provider.

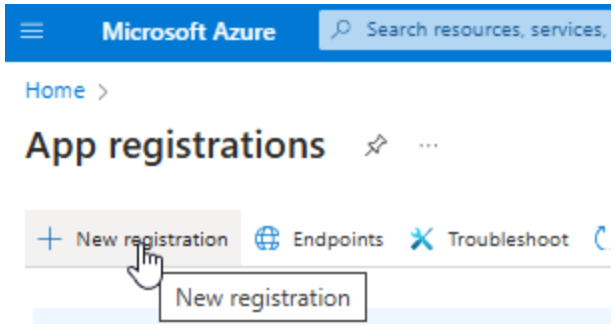
The CDM Server supports authentication of users on behalf of Microsoft Azure. In Azure an application needs to be configured which provides the authentication flow.

Step 1: Start with the app registration

- Open azure portal in Web Browser and click on **App registrations**

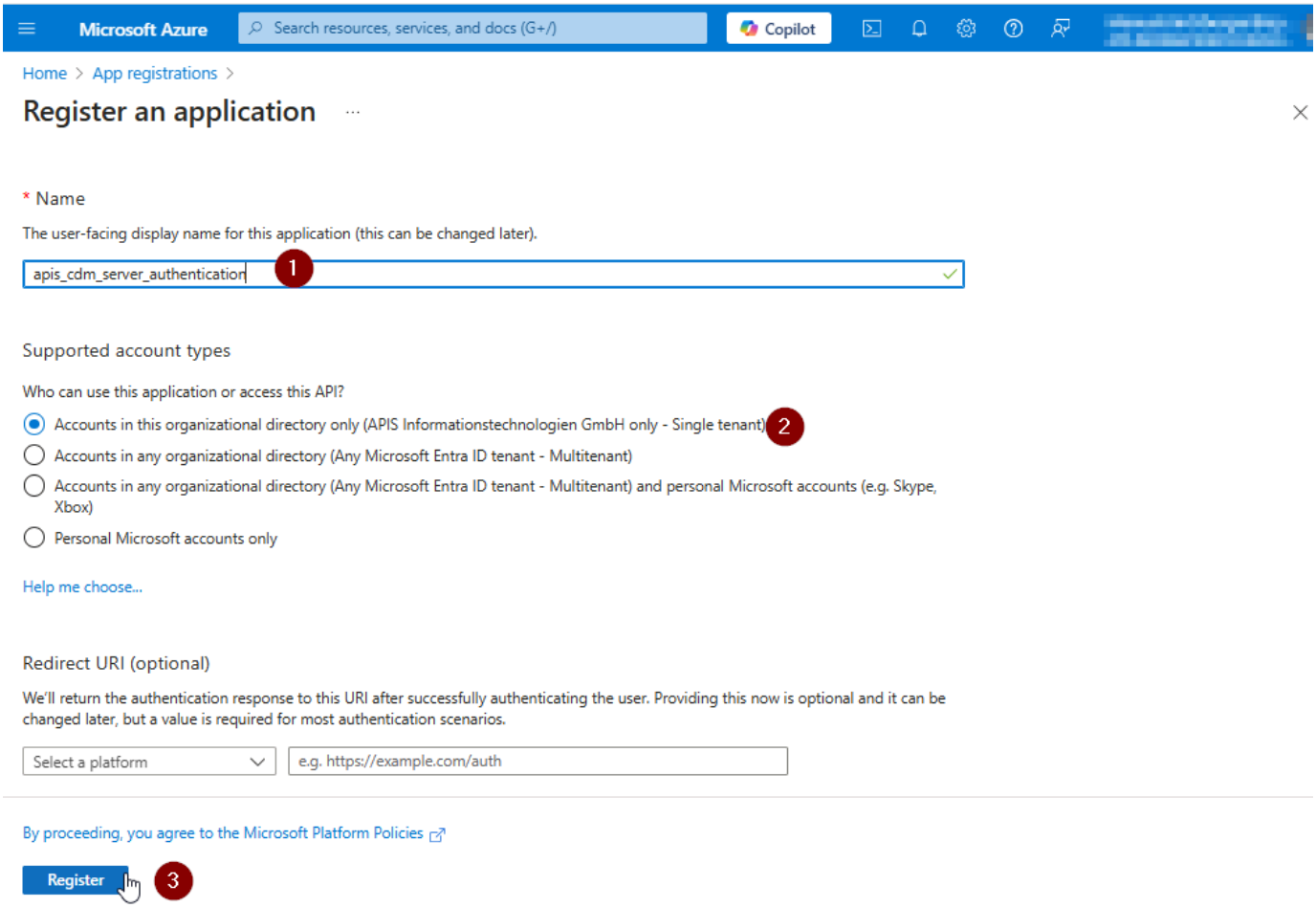


- Now the app registrations page shows the registered azure apps.



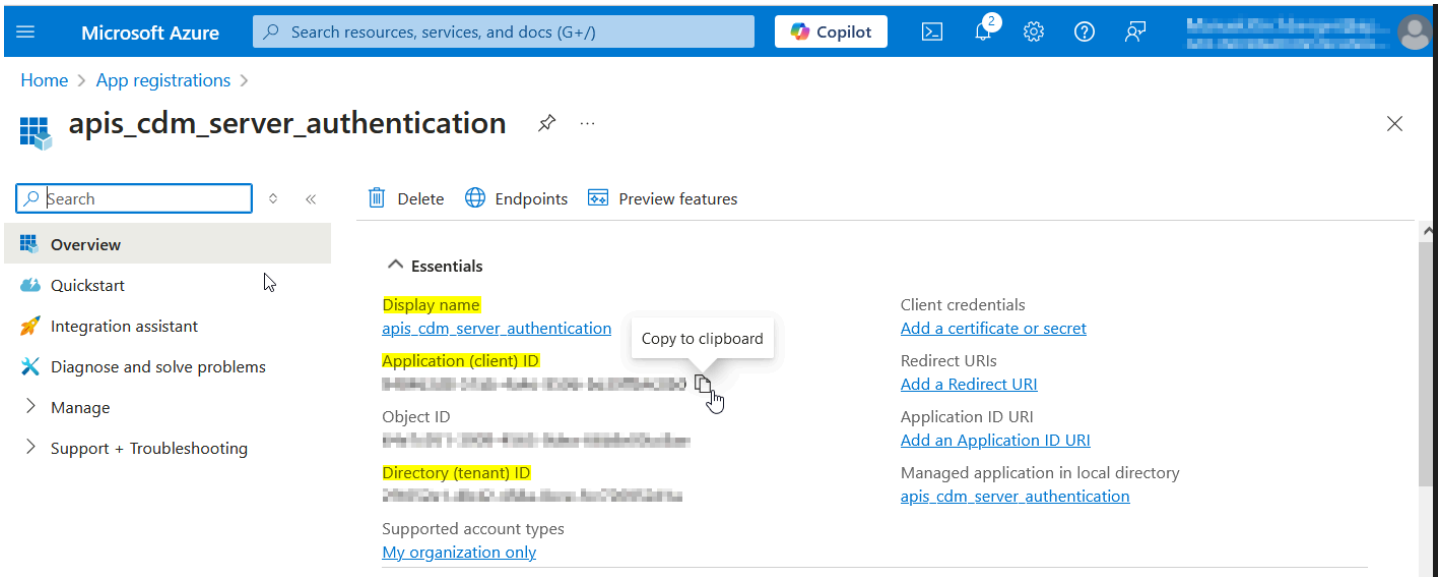
1. Click on "**+ New registration**" to register a new application in azure

- An application registration form is shown



1. Enter the mandatory name
2. Select a supported account type which matches your requirement
3. Skip the step to add redirect URL here for now, we need more than one url, this can be done later.
4. Click on Register, you will see the details of the registered app next

Step 2: Configure Application details



The values of the yellow highlighted fields are necessary for later use in CDM Server configuration. The Ids can be copied moving the mouse pointer to the right end of the value.

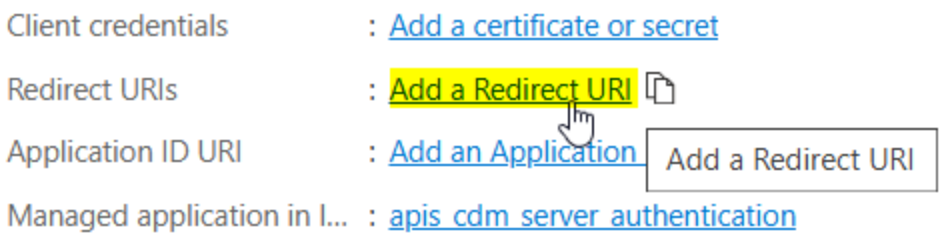
Please note the values for the following CDM Parameters for later use:

CDM Parameter	From
AZURE_CLIENT_NAME	Display name
AZURE_CLIENT_ID	Application (client) ID
AZURE_TENANT_ID	Directory (tenant) ID

Redirect URIs

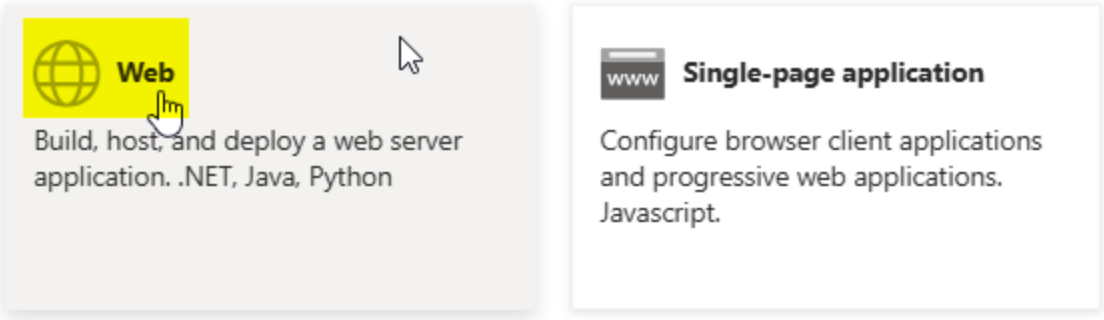
> **Note**
>
> Once a user is authenticated by Azure, it sends an authentication information back to the CDM Server. The same happens in the logout workflow. Therefore some Redirect URIs must be defined for the Application.

To configure allowed redirect destinations click on **Add a Redirect URI** on the Application details page.

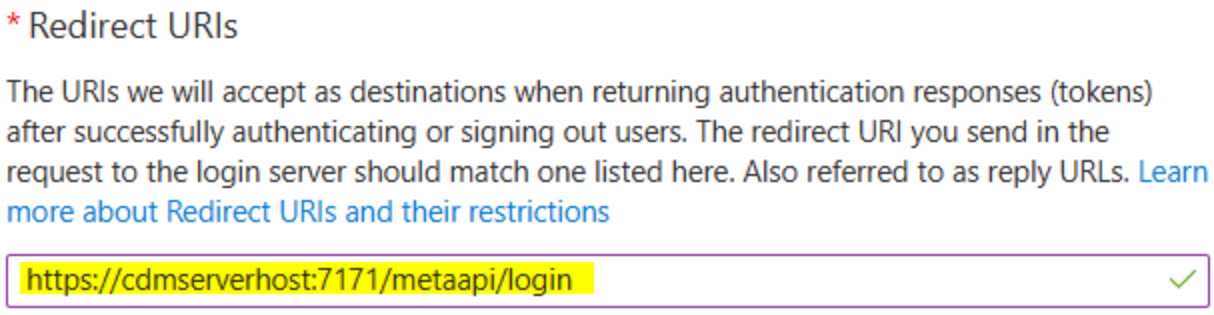


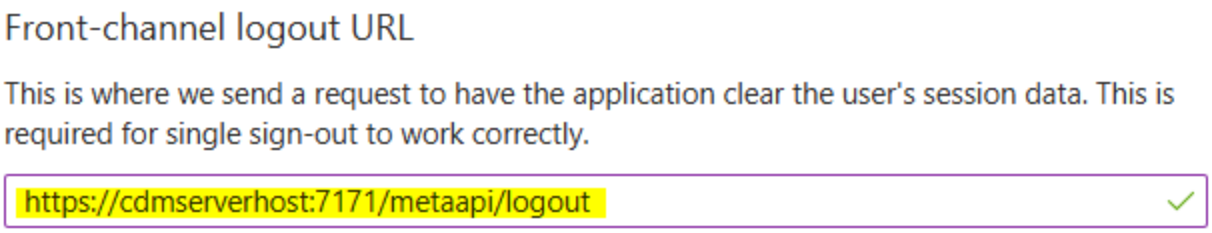
In the following page click on **+ Add a platform**. As a result a new form opens on the right side where you can select the type of platform.

Choose **Web** here.



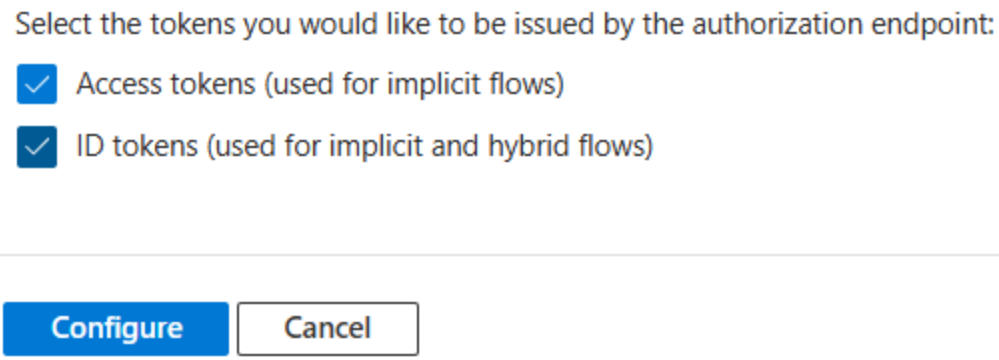
Enter Redirect URI in the Redirect URIs field, enter the URI provided by the third-party software.





> **Warning**
>
> Make sure the URIs here are exact, as mismatched URIs will cause authentication errors.

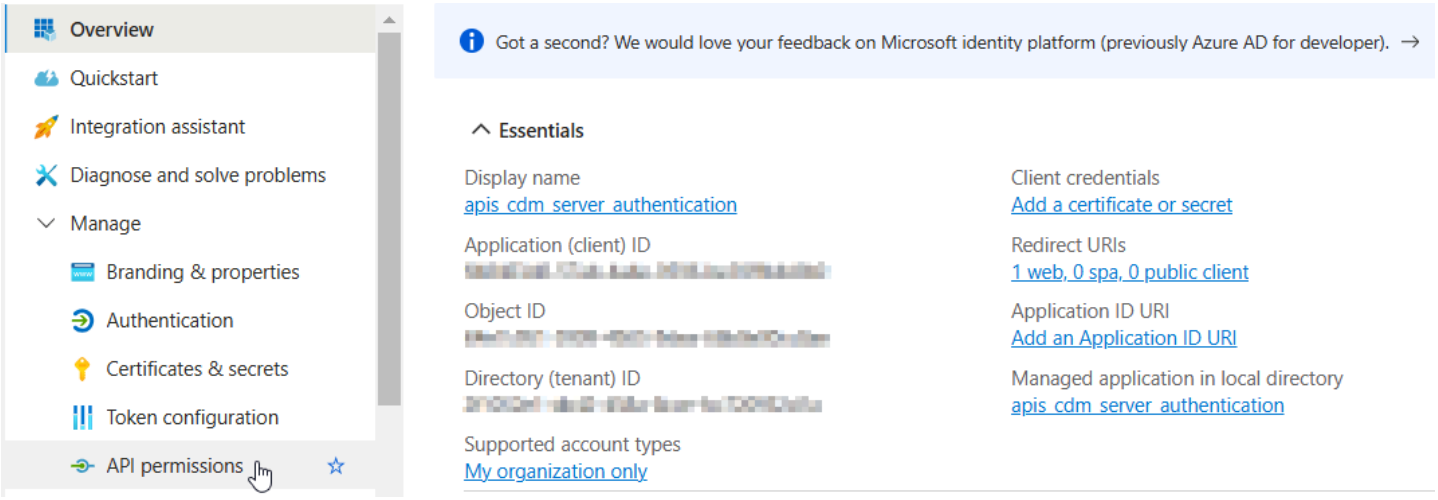
At the bottom of the form enable Access tokens and ID tokens:



Then click on **Configure** to finish the configuration.

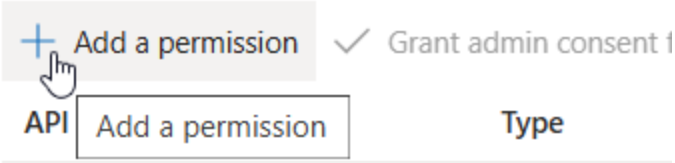
Application Permissions

In the left menu select API permissions.



Add Permissions:

Click **+ Add a permission**.

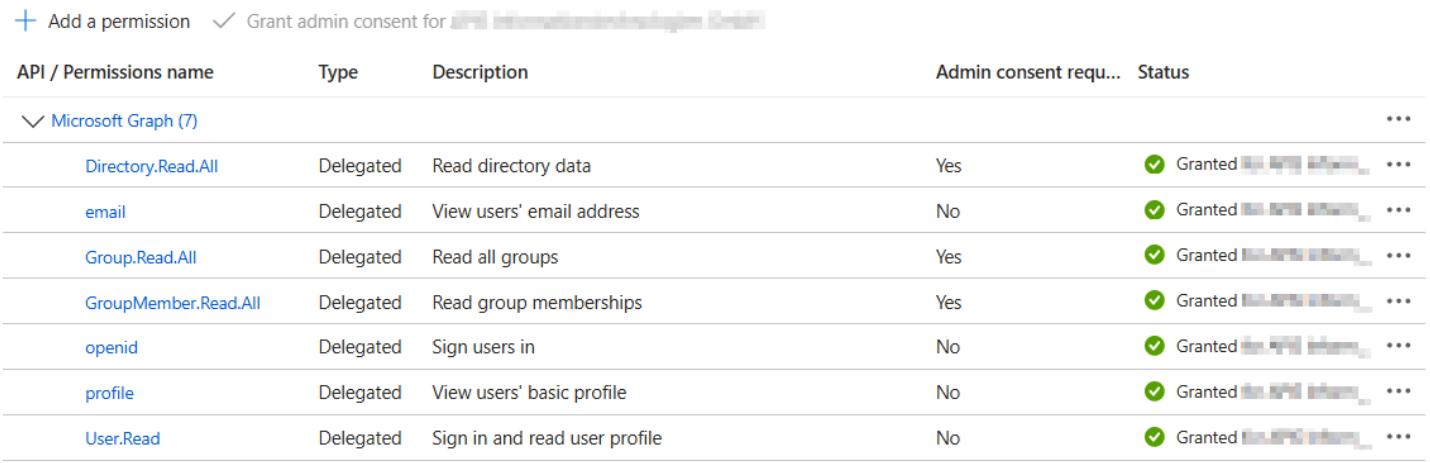


Select Microsoft Graph and then Delegated permissions. Add the permissions

- openid
- profile
- email
- User.Read
- Directory.Read.All
- Group.Read.All
- GroupMember.Read.All

If prompted, click Grant admin consent for the selected permissions. (This step may require admin privileges.)

The result should look like this:



The permissions Directory.Read.All, Group.Read.All and Group.Member.Read.All need Admin consent and are necessary to be able to read members of groups and groups of users which is necessary to provide RBAC flows in CDM Server which are based on group structures in external ID Providers.

2.3.2 - Configure CDM-Server

How to configure CDM-Server to use the Azure application for authentication.

Prerequisites

To be able to configure the CDM-Server to start and for later use by members of a configured group, you need some values from the **Azure Portal**.

Values to collect from Azure Portal

#	Name	Description	Usage
0	ID_PROVIDER	Fixed value "*azure*"	Environment
1	AZURE_TENANT_ID	The Directory (Tenant) ID	Environment
2	AZURE_ADMIN_UUID	The Admin User's Object ID	Environment
3	AZURE_LOGIN_GROUP_UUID	The Login Group's Object ID	Start Config
4	AZURE_SCOPE	Fixed value "*Read.users*"	Environment
5	AZURE_CLIENT_NAME	Name of the application	Environment
6	AZURE_CLIENT_ID	ID of the application	Environment
7	AZURE_CLIENT_SECRET	Secret value of the application	Environment

---

Collect the values provided by Azure

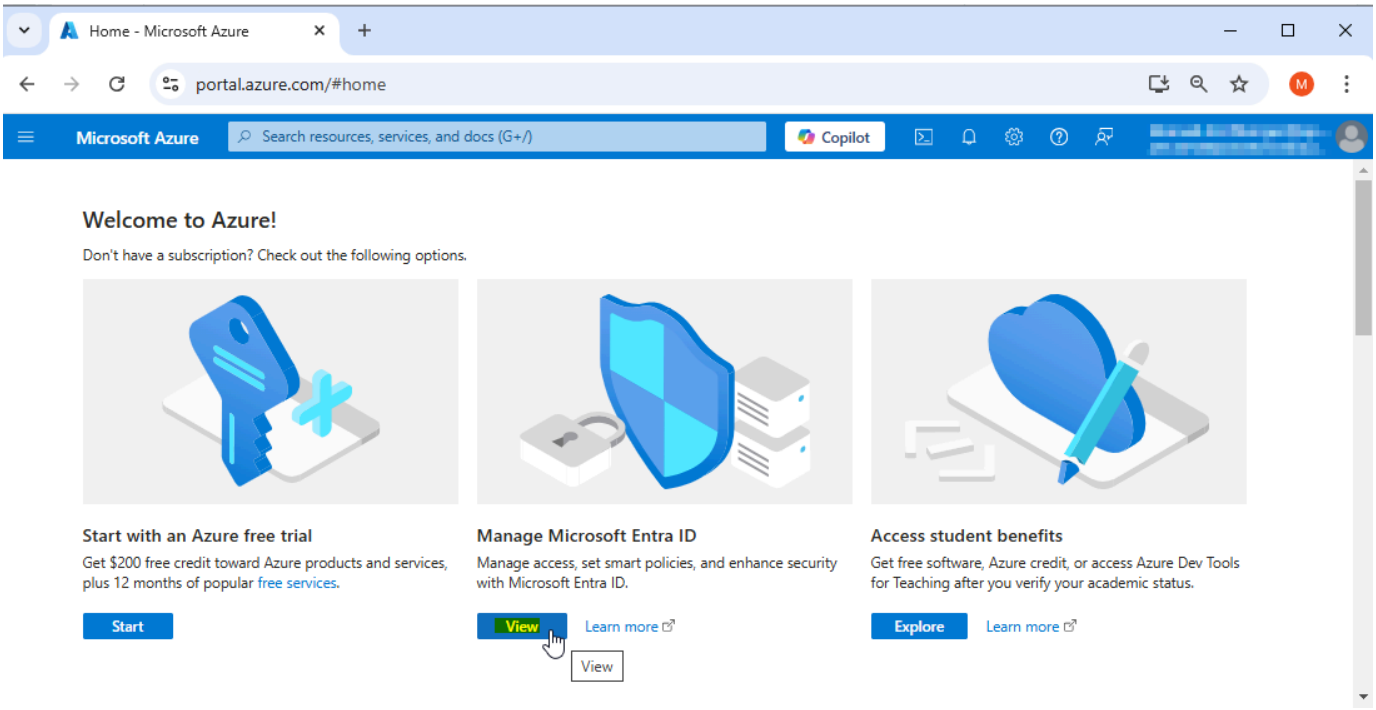
The *ID_PROVIDER* for Azure is fixed and must be set to value **azure** in the environment.

First we will collect the Azure Tenant-ID, an admin user ID and a login group id.

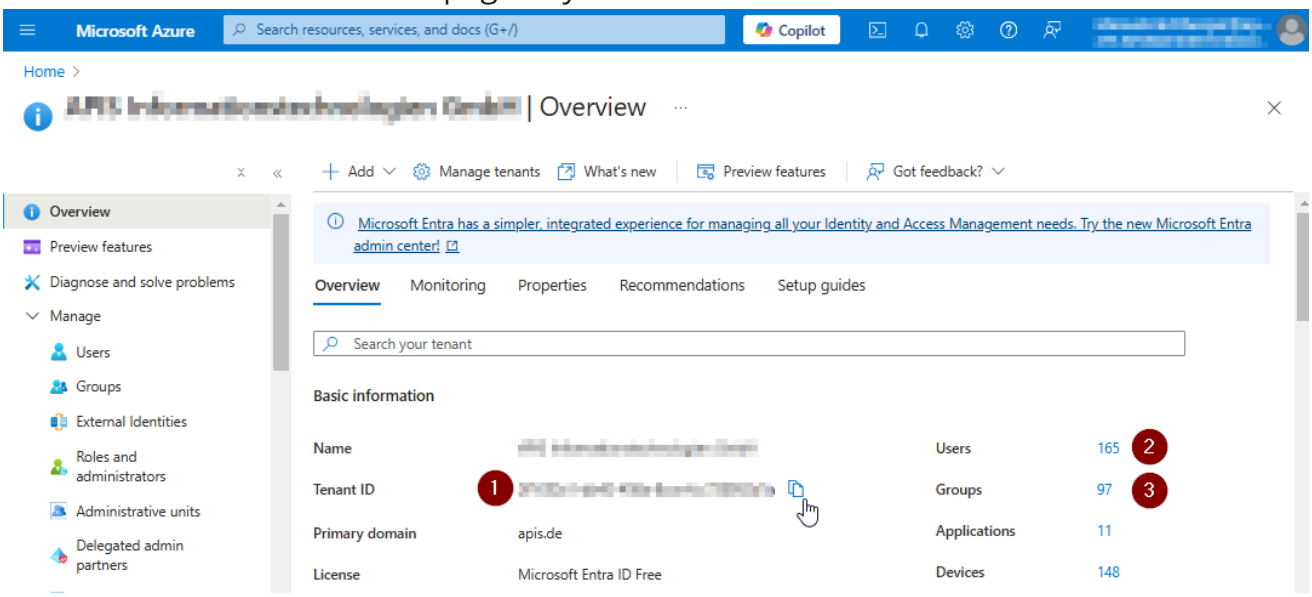
The Admin user is able to log in to a fresh system to configure the necessary base settings.

- Log in to Azure Portal

- On the Welcome Page below Manage Microsoft Entra ID click on **View** button

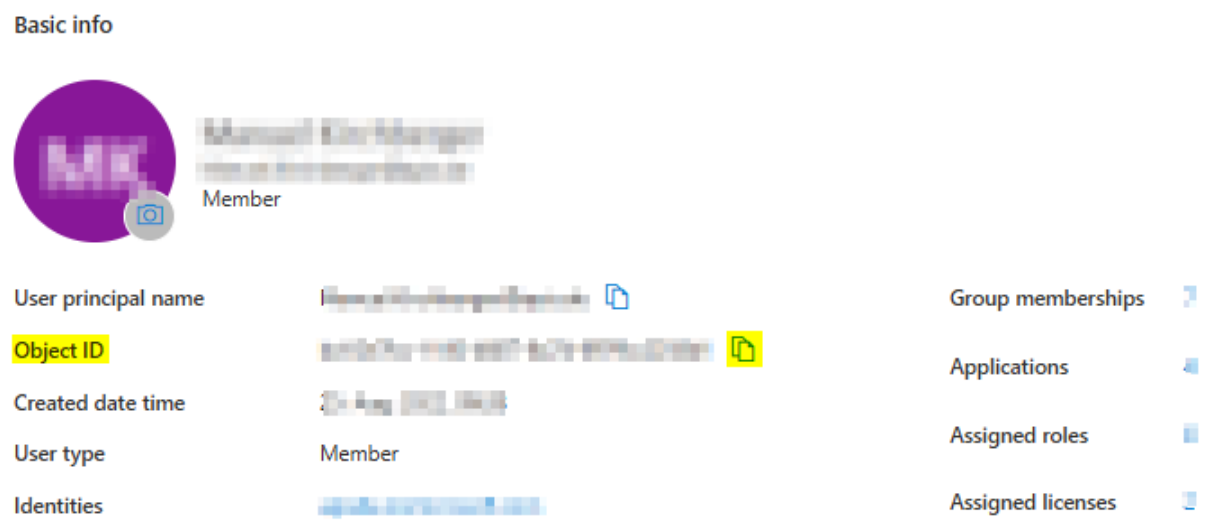


  - You are now on the welcome page of your Tenant:



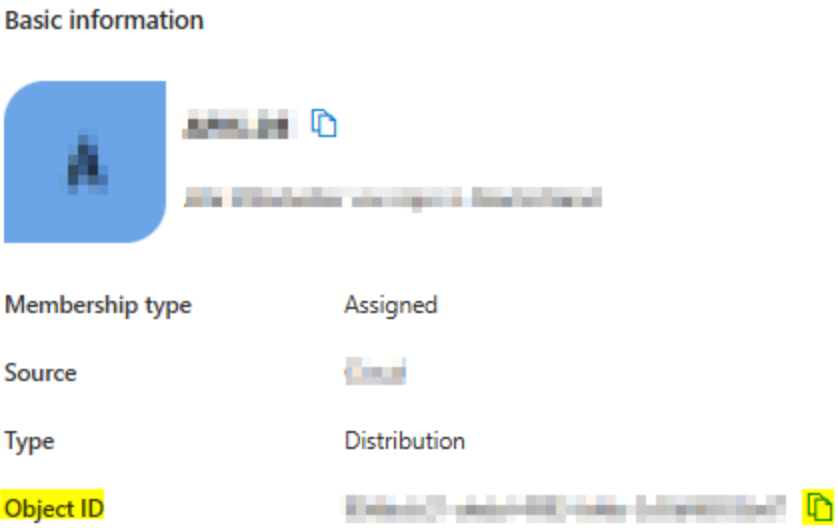
1. Tenant-ID: You can click on the copy Icon after the value to copy it. Needed for *AZURE_TENANT_ID*.

2. Click on the Number link on the right side of Users. In the appearing User list click on the name of the user, which is going to do the initial system configuration, in the column *Display name*.



The *Object ID* value is needed in *AZURE_ADMIN_UUID*

3. On the same page you can click on the Number link on the right side of Group memberships. In the appearing list of Groups click on the name of the group which you want to use as login group for all allowed users.

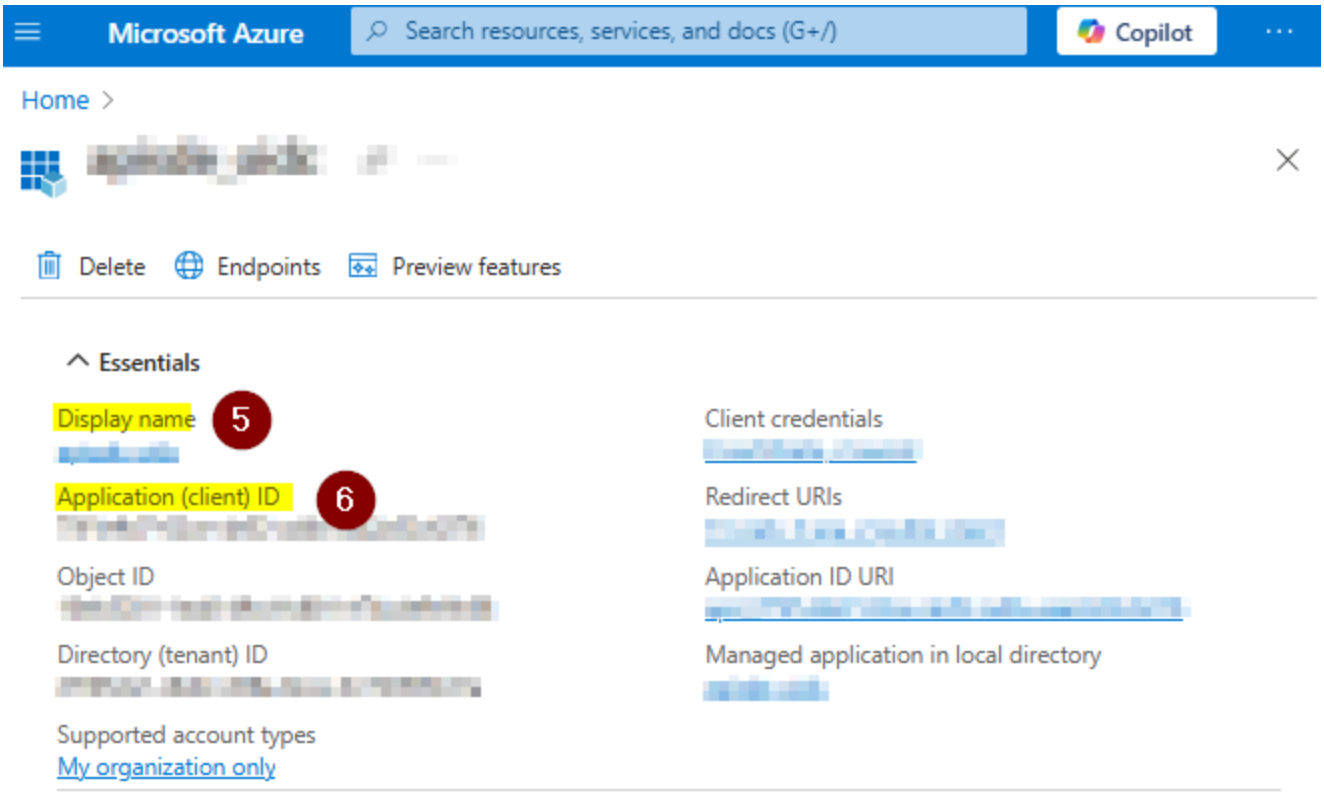


The *Object ID* value is needed as *AZURE_LOGIN_GROUP_UUID*. This configuration setting is not part of environment setup, but it's needed on first start.

4. The *AZURE_SCOPE* value should be set to the value **User.read**

Go back to Azure Portal Home

Click in the left area menu on *App registrations* and click on your app to see the details:



5. The *Display Name* value is needed as *AZURE_CLIENT_NAME*

6. The *Application (client) ID* is needed as *AZURE_CLIENT_ID*

7. The CLIENT_SECRET is configured in the App details below *Client credentials* on secret. Its value must be saved for later use when creating it, since it is only readable directly after adding it.

   If you missed that and the value is unknown you have to recreate it as described in Azure - Configure Application and save the value as CLIENT_SECRET.

Configure the CDM Server Environment

Go to the instance installation directory and open the .env.idp file with a text editor of your choice. In the file you have to write the parameter names and their assigned values in the schema *ID_PROVIDER*=**azure**

Example:

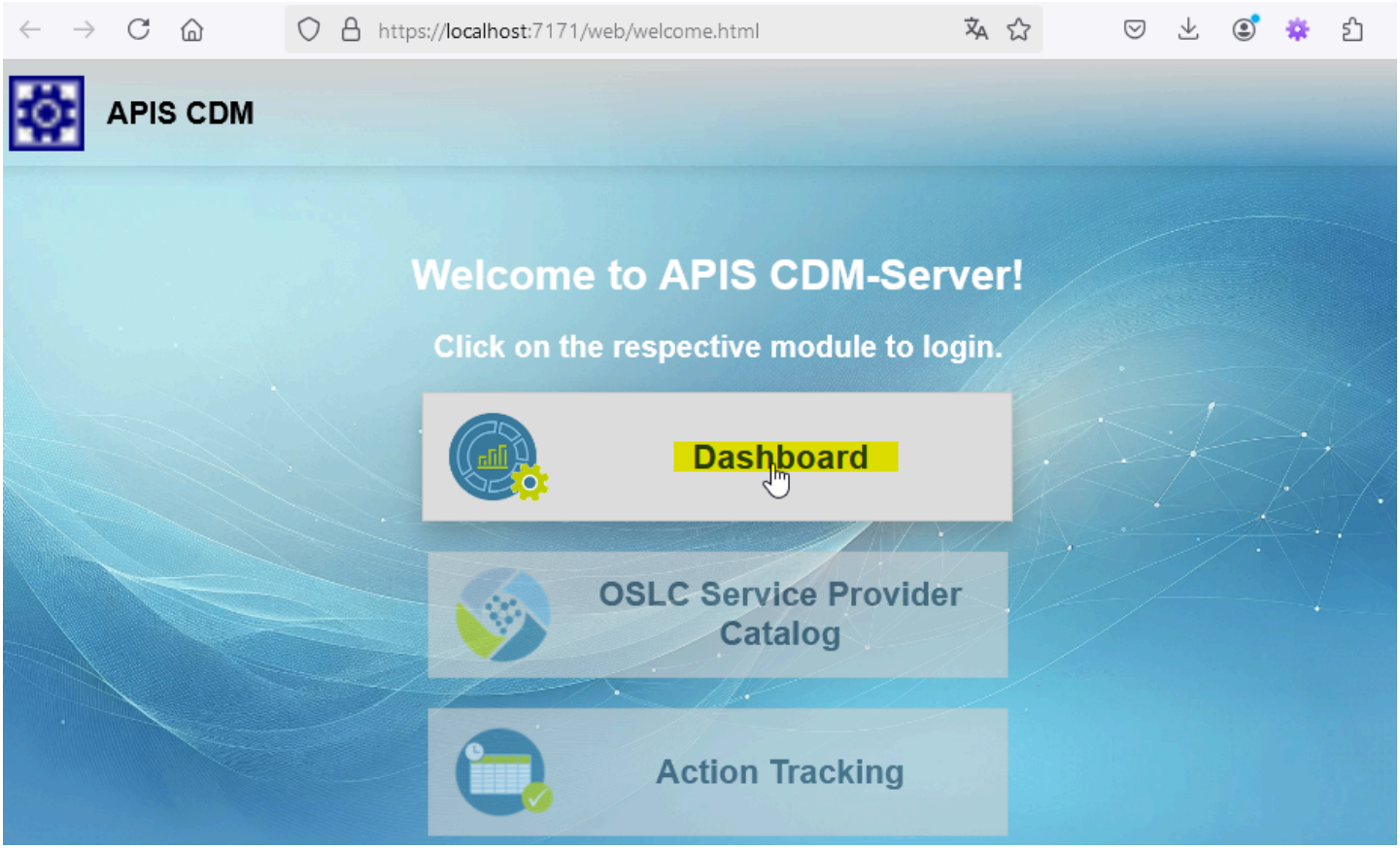
```
## HELP
# https://get.apis.de/docs/idproviders/azure/

## User Management
# Available options: local, azure, ldaps
ID_PROVIDER=azure

## User Management -> AZURE
# Only required if ID_PROVIDER=azure
CLIENT_ID=
CLIENT_SECRET=
AZURE_CLIENT_ID=
AZURE_CLIENT_NAME=
AZURE_TENANT_ID=
AZURE_ADMIN_UUID=
```

Test the Authentication Flow

Open the CDM-Server web interface and click on **Dashboard** to initialize the Authentication Flow.



You should be redirected to Azure AD for login. Log in using the credentials **of the configured admin** user!

After a successful login, you'll be redirected back to the third-party software. Confirm that the authentication and authorization are working as expected.

Initial startup and configuration

Log in as admin user

> **Note**
>
> If your user is not the declared admin user in the environment setup, authentication will fail!

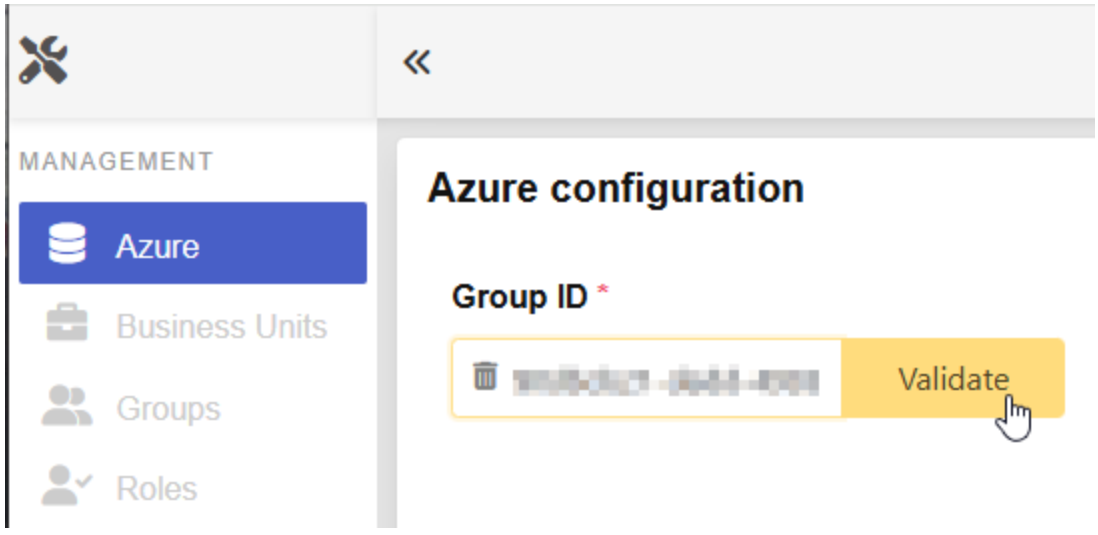
Open the public CDM Server Welcome Page in browser and click on **Dashboard** to start Azure authentication.

- In the popup window enter your azure credentials to login.

  If you are the admin user and configuration is completely valid you will get logged in to the CDM Server and the Admin Dashboard is shown.

Configure Login Group

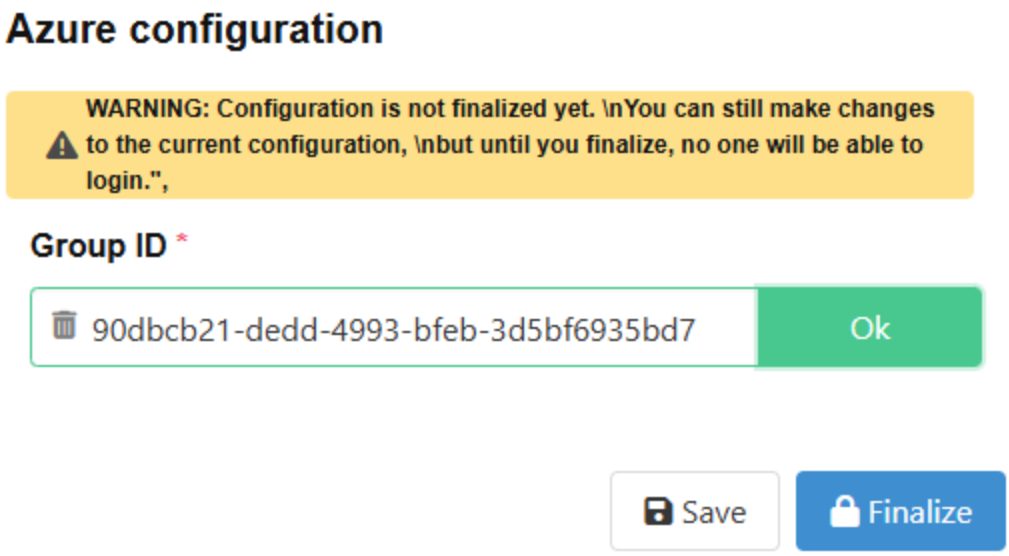
- Now add the ID of the group of the azure users which are allowed to log in to CDM Server in the form and click on validate.



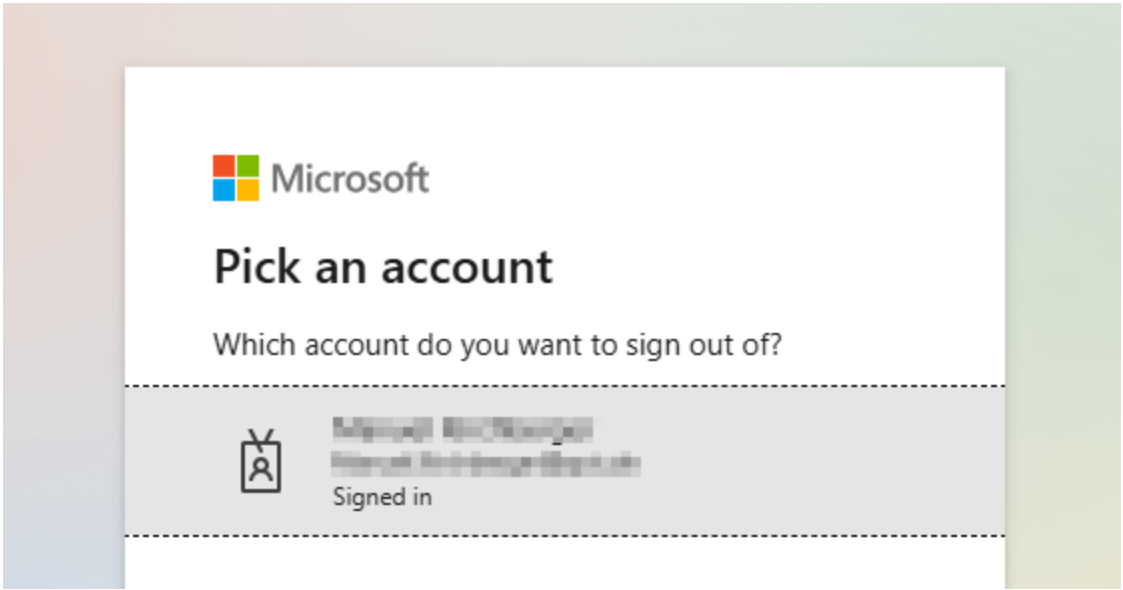
- When validation succeeds the validate button changes to green

- Then click on the button "*Save*" to store the initial configuration in the database.

- To finally activate the change you have to click the "*Finalize*" Button. This means the configuration gets locked and is no longer editable. But you have to finalize when you are sure to enable all users in the configured group to log in to the CDM-Server.



After clicking on finalize you have to confirm that you are sure and want to proceed. Confirm and select your account to log out your current azure session.



In case you logged out your current azure session you get redirected to the welcome screen and all users which are member of the login group can now log in to CDM-Server using Azure.

Possible Error Szenarios

- The Login Group ID does not or no longer exist in Azure:
  An error message will be displayed and saving the configuration is not possible.
- Admin user is not member of the login group:
  It is not possible to lock out the admin user, in this case an error message gets displayed.

Congratulations!

After succeeding all of these steps the Azure Users which are in the configured group can log in to the CDM Server!

Step 8: Maintain the Application

Periodically review and renew the client secret before expiration.
Adjust permissions or application settings in Azure AD if required by the third-party software or organizational policies.

Warning About Data Loss

Please note that, at this moment, we do not support changing the IdP without clearing all data. This means, if you set up a CDM-Server instance for testing using `Local` or `Ldaps` for now, you will have to clear all data and start fresh when you want to switch to `Azure`.

Here is a sample `.env.idp` file with the `azure` IdP configured:

```
## HELP
# https://get.apis.de/docs/idproviders/azure/

## User Management
# Available options: local, azure, ldaps
ID_PROVIDER=azure

## User Management -> AZURE
# Only required if ID_PROVIDER=azure

# The Microsoft Azure AD Directory (Tenant) ID
# The Tenant ID is an UUID and contains hexadecimal numbers (0-9a-f) seperated by - and
# can be found in Azure Portal on the Entra-ID welcome page.
#
```

```
# Example: "e53f2a45-f4d2-a11d-223a-77b654c12df5"
AZURE_TENANT_ID=

# The Azure Application (Client) ID
# The Application client ID is an UUID and belongs to the application which is configured
# for the authentication and authorization of azure users for CDM Server. The Id can be
# found in Azure Portal -> App registrations.
#
# Example: "53a12b45-1234-5566-8fe4-93b787a787d6"
AZURE_CLIENT_ID=

# The Azure Application (Client) Name
# The Application client Name is a Text and belongs to the application which is configured
# for the authentication and authorization of azure users for CDM Server. The Name can be
# found in Azure Portal -> App registrations.
#
# Example apis_cdm_authentication
AZURE_CLIENT_NAME=

# The Azure Admin UUID
# The Azure admin UUID must be the id of the Azure user who is going to configure CDM Serve
# The user which belongs to the id is then an admin user and the only user which is able to
# CDM Server to complete the configuration.
#
# To get your Azure user id log in to https://portal.azure.com/ click on view entra and in
# in the middle area of the entra welcome page the user id is shown.
#
# Example fd163a2f-112a-7291-bdf4-a4325b78910a
AZURE_ADMIN_UUID=
```

2.4 - Jazz

How to set up the IBM Jazz identity provider.

> **Not Supported**
>
> IBM Jazz is not supported in the current version of the CDM-Server.

3 - IQ-Software

How to use the IQ-Software with the CDM-Server

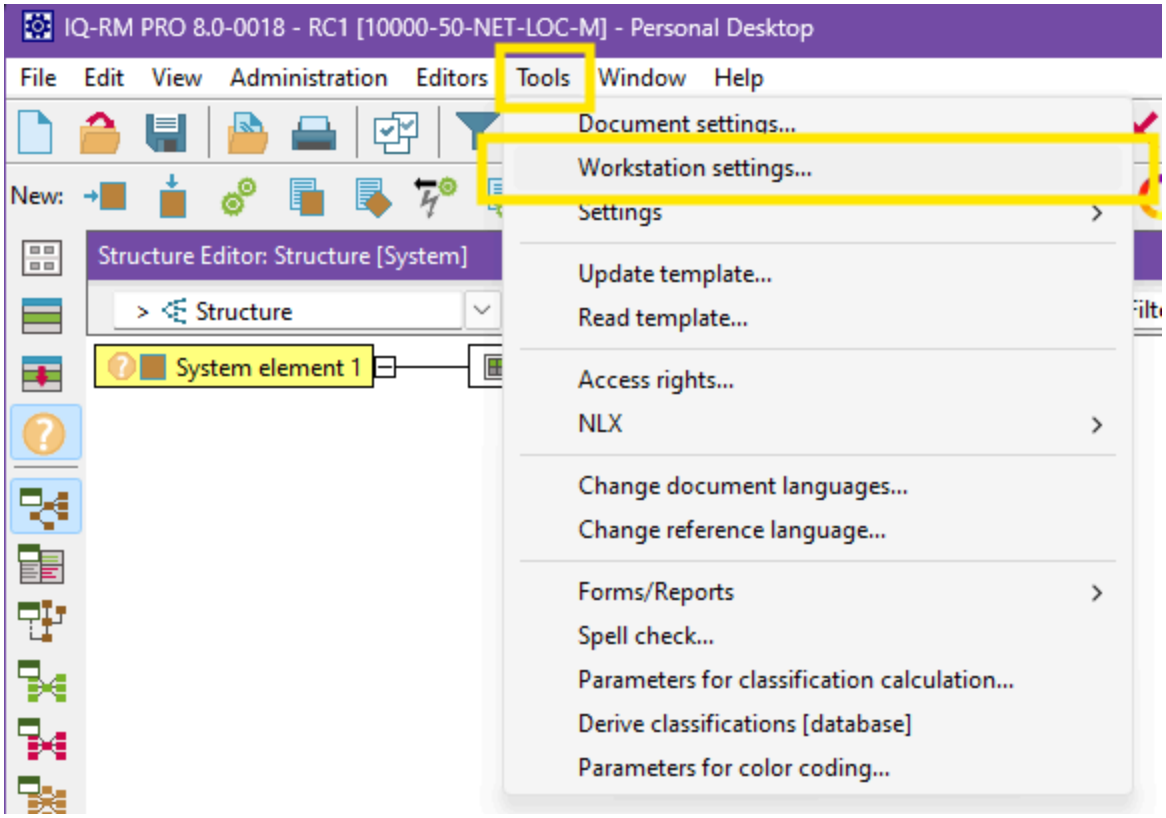
3.1 - Connect to CDM-Server

How to connect to the CDM-Server from the IQ-Software

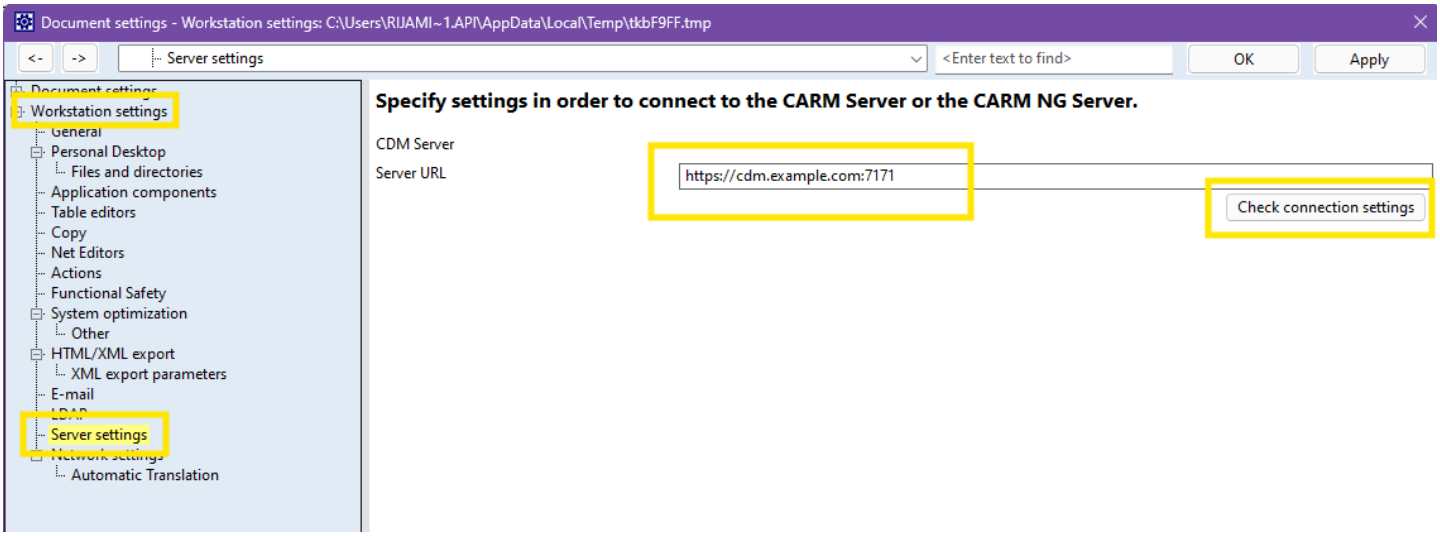
> Version
>
> To connect with CDM-Server, you must have at least IQ-Software version 8.0 or later.

Step 1: Open the IQ-Software

Step 2: (Top Menu) Tools -> Workstation Settings



Step 3: (Left Menu) Server Settings



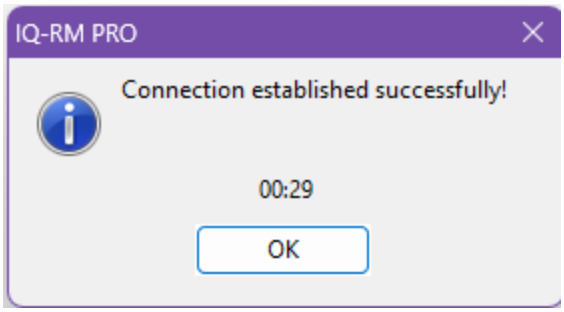
Please enter the `Server URL` which must include:

- `https://` at start
- The domain name part you will get from your administrator
- `:XYZ` the port number at the end

> ### Enable CDM-Server
>
> If the `Server Settings` entry is not available or there is no possibility to enter a `Server URL` for the CDM-Server please enable `Application components | CDM-Server`, confirm with `OK` button and reopen the `Workstation Settings` dialog.

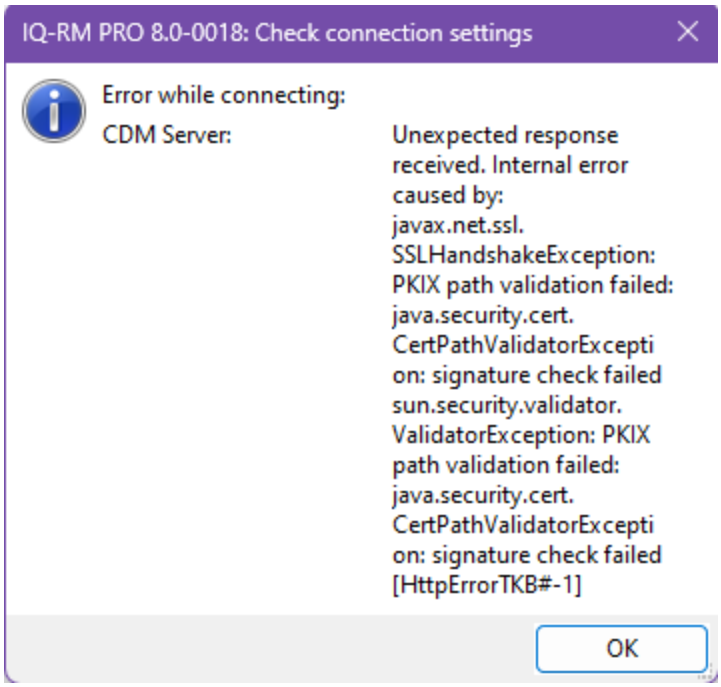
Step 4: Check Connection

Click on the `Check Connection Settings` button to verify the connection. You should see the following message box.



Certificate Error

If the CDM-Server has been setup using a self-signed certificate, you will see the following error if the certificate is not installed on your system.



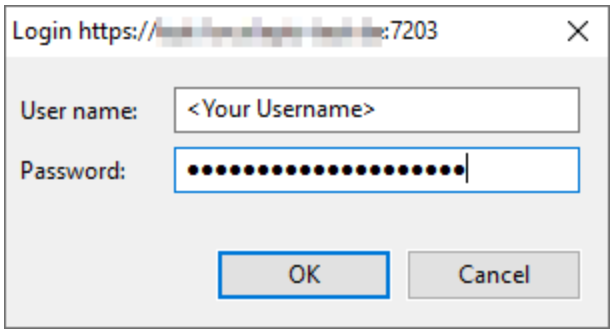
The administrator can install it using group-policy or you can install it manually. Please see Install Self-Signed Certificate for more information.

3.2 - Login to CDM-Server

How to log in to the CDM-Server from the IQ-Software

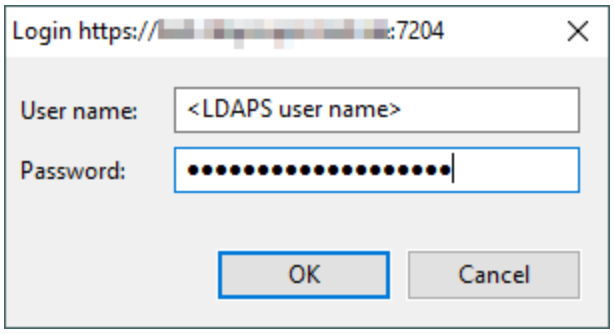
After starting the IQ-Software you have to login to the CDM-Server when performing your first command related to the CDM server (e.g. opening the `Administration | CDM Administration`). IQ-Software automatically prompts you for your credentials. Depending on the configured ID Provider on your CDM-Server the login procedure varies:

Local



Please enter the your username and your password as set up by your CDM administrator.

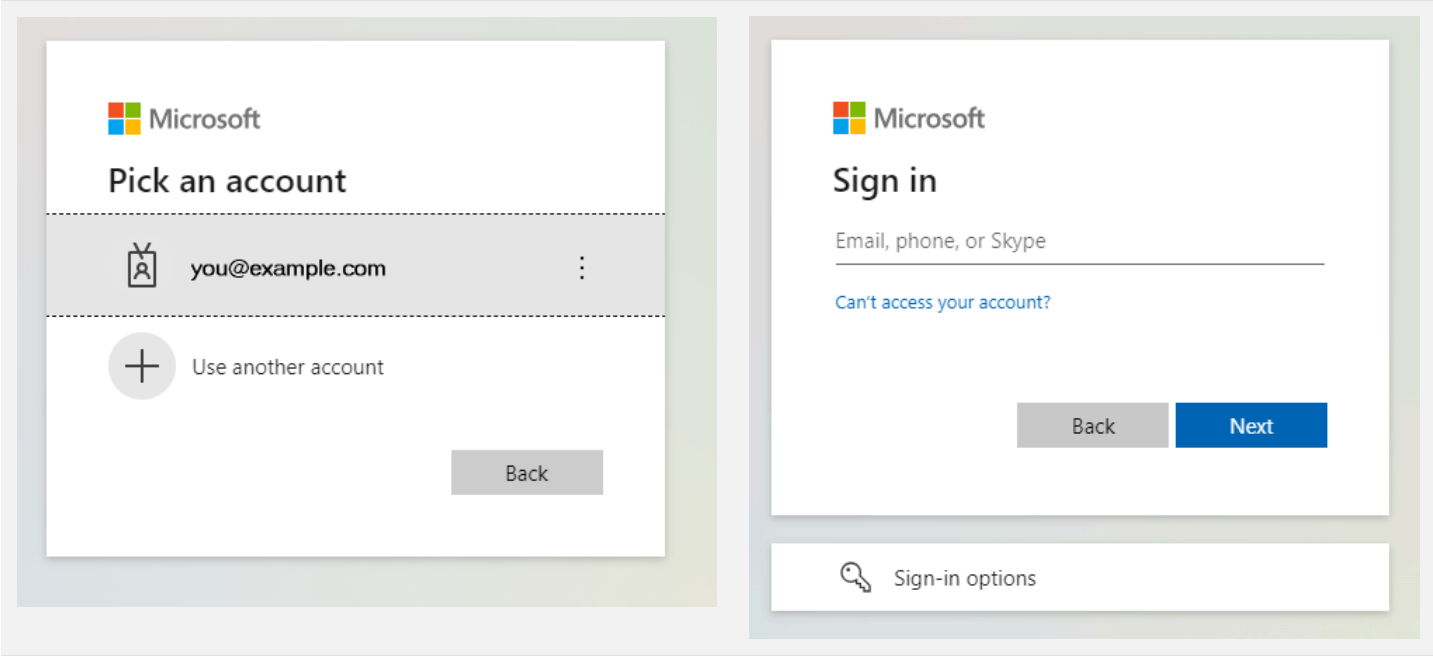
LDAPS



Please enter your LDAPS username and password.

Azure

You are redirected to your webbrowser which shows the Azure Login page (depending on your previous activity one of the following pages will be shown):



Select the account you want to use by clicking on it or providing your account name and clicking *Next*. Then enter your password on the following screen. After successful authentication, this message is shown in the browser:

```
Authentication complete. You can close the browser and return to the application.
```

Now you can close the browser (tab) and switch back to the *IQ-Software* window.

On subsequent login attempts you might not even need to provide your username and password and are at once redirected to a page showing the above "Authentication complete" message. In this case, simply close the browser (tab) and switch back to the *IQ-Software* window.

Jazz

> ## Not Supported
>
> IBM Jazz is not supported in the current version of the CDM-Server.

Logout

When closing the IQ-Software your login session on the CDM-Server is automatically terminated.

Should you need to log out and log in with a different user while using the IQ-Software, please use the `File | Logout` and `File | Login` menu commands in the `Administration | CDM Administration` window.

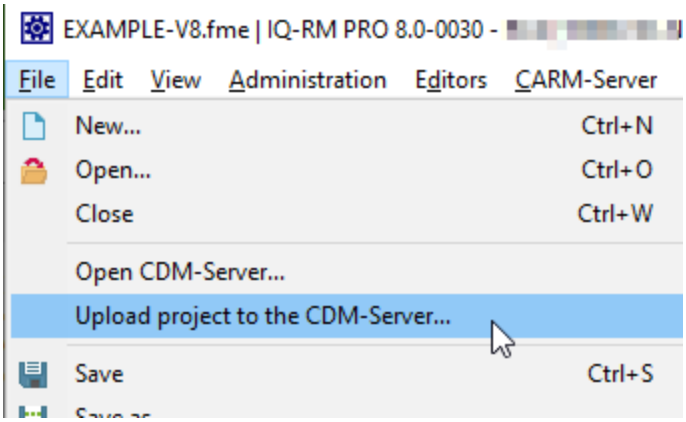
3.3 - Managing Projects

How to manage projects using IQ-Software on the CDM-Server

The CDM Server manages your IQ-Software data in seperate *Projects*. Each *Project* is stored on the CDM-Server in a *Business Unit*. These *Business Units* can be nested (one inside another) so that you can create tree-like structures similar to folders and subfolders within a regular file system.

> ### Login on first use
>
> The first time you interact with CDM-Server after starting the IQ-Software client, the software prompts you for your credentials (username/password), see Login to CDM-Server.

Uploading .fme Files as CDM-Server Projects



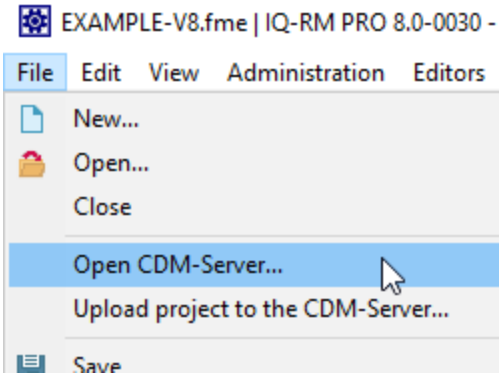
The first step to working with the CDM-Server is to upload an existing project from one of your .fme files:

1. Open the .fme file in the IQ-Software
2. Choose `File | Upload Project to the CDM-Server...`
3. Choose the *Business Unit* into which the project should be uploaded

Note that you can only upload a project if the file contains **exactly one** project. If this is not the case please reorganize the data in the file in this respect.

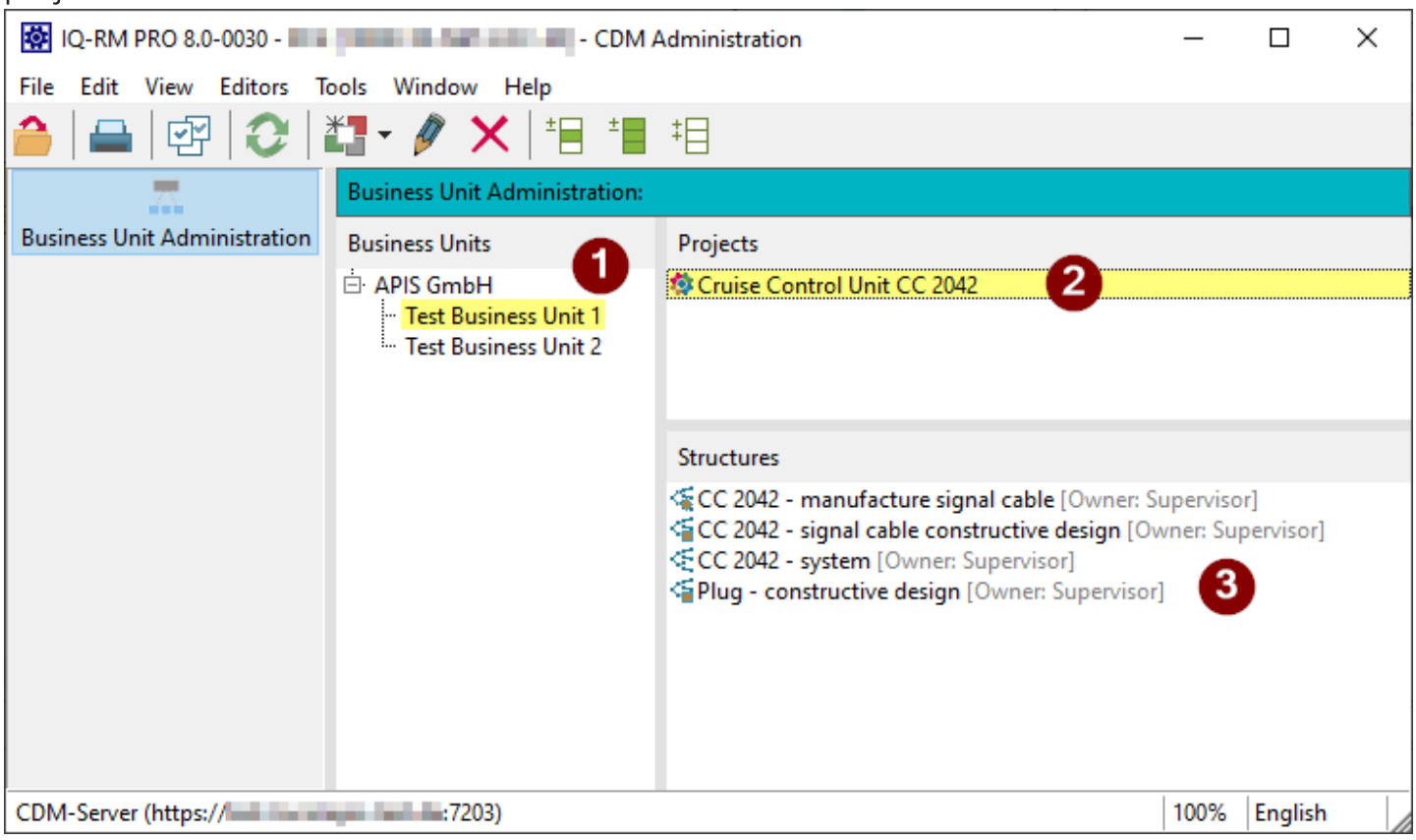
Alternatively, you can create a new project via context menu directly in the *CDM Administration* (see below).

Opening a Project from the CDM-Server

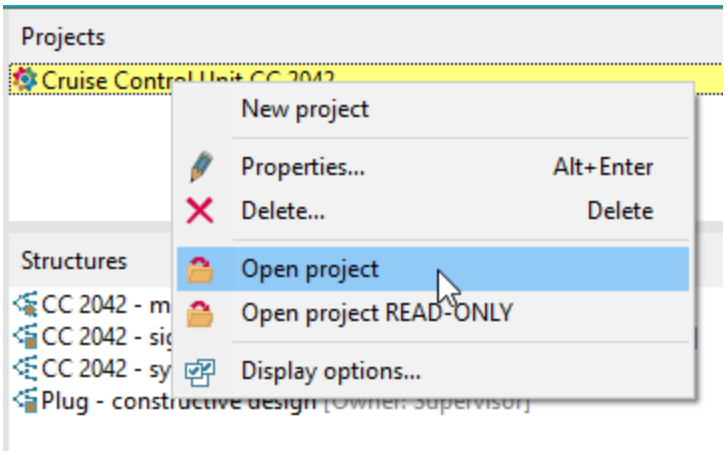


Once there are projects available on the CDM-Server, you can open a project in the IQ-Software as easy as opening an .fme file: Choose `File | Open CDM-Server...` (alternatively you can also use `Administration | CDM Administration`).

This opens the *CDM Administration* view, showing you the available *Business Units* and their projects:



Selecting a *Business Unit* (1) shows you the contained *Projects*. When you select a *Project* (2), the contained structures are shown (3).



You can open a *Project* via the context menu or by double clicking it.

> ### Close CDM Administration automatically
>
> If you activate the display option `Options | Close CDM Administration when opening a project` the *CDM Administration* is closed automatically after opening a *Project*.

CDM Administration

In the *CDM Administration* (`File | Open CDM-Server...` or `Administration | CDM Administration`) you can also do the following things apart from opening a *Project*:

1. Create a new *Project* or *Business Unit*
2. Change the name of a *Project* or *Business Unit* (in multiple languages)
3. Delete a *Project* or *Business Unit* from CDM-Server
4. Move a *Project* from onen *Business Unit* to another using Drag&Drop
5. Perform an explicit `File | Login...` or `File | Logout`

Points 1 to 3 are available from the context menu (right-click).

4 - User Interface

Basic Information about the CDM Web Application

4.1 - Azure Initial Configuration

How to configure azure in the CDM Web Application

The *Azure* page allows you to add the necessary configuration to use Azure.

Group ID

This is the Group's Object ID of the Azure Active Directory that includes all the users who need to log in to the CDM Server. The group ID identifies the specific group in your Azure AD tenant, ensuring that only users within this group are granted access to the CDM Server through Azure login.

After you have finished the setup of the **Group ID**, you have the possibility to **save** and **finalize** the configuration. If you wish to modify it again, before you have finalized the configuration, you are free to do so. Please note, as long as you do not finalize the configuration, **no** user except the admin will be able to login.

4.2 - LDAP Attribute Mapping Configuration

How to configure the attribute mapping in the CDM Web Application

The *LDAP Attribute Mapping* page allows you to configure how user's attributes from an **external** *LDAP* connection will be translated to the *CDM-Server*'s internal representation. In the first section you will be able to set a *group dn*, which will determine the users available in the system. Afterwards you can configure the individual mapping between attributes in the next section. Finally you will be able to **save**, **review** and **finalize** the configuration.

Key Features Overview

- Two distinguished configuration sections for more oversight
- Easy mapping possibility with validation

Procedure

Introduction

The first time you login (and after that as long as you have not finalized the mapping) to a freshly configured instance with an *LDAP* ID-Provider as the admin user, you will be automatically redirected to the LDAP Attribute Mapping Configuration page.

Group DN

The next action should be to configure the *group dn*. Therefore navigate to the text field and enter a previously copied (to prevent typing errors) *group dn* into this field. Next you should validate it by clicking on the validate button.

The following results are possible:

- The *group dn* is **valid**: Everything is fine and you can procede to the next bottom section.
- The *group dn* is **not valid**: Please check the *group dn* for errors and validate again.

Attribute Mapping

The goal of this section is to configure a mapping between *CDM* and *LDAP* attributes, so that the *CDM*-Server will have a proper translation between those.

It contains a table with two columns, the *CDM* attributes on the left side and the *LDAP* attributes on the right.

On the left upper side next to the table, you can choose the type of your *LDAP* installation (*Unix* or *Microsoft*) depending on the type of OS on the *LDAP* host machine, which is used to apply a preconfigured mapping. If you do not wish for this automatism, you can choose *Manual* instead.

For each attribute on the left you have the following options to procede on the right:

- **Enter the name of an *LDAP* attribute**: After typing in the name of an *LDAP* attribute you wish to map, please validate it directly afterwards. If it is valid, you will find additional information by clicking on the information icon to the right of the text field. If it is not valid, please adjust the entered name and validate again.
- **Enter nothing**: If you enter nothing, the attribute will not be mapped.

All attributes except those marked with a star (*) are **optional**, you can finish the mapping without those.

After you have finished the mapping, you have the possibility to **save the mapping** and **finalize the configuration**. To do so, you may click on *Finalize*, which will present you a side by side comparison of your chosen mapping. Please review it **carefully**, because it can **not** be changed after you finalize the configuration.

If you wish to modify the mapping again, before you have finalized the configuration, you are free to do so. Please note, as long as you do not finalize the configuration, **no** user except the admin will be able to login.

4.3 - Business Units & Projects

How to Create and Manage Business Units and Projects in the CDM Web Application

The **Business Units** & **Projects** Management section allows you to organize and manage your **Business Units** structure and **Projects**. This section provides hierarchical representation of the relationships between business units and projects, and allows for easy navigation and updates.

Key Features Overview

- **Hierarchical Structure**: The business units and projects are displayed in a tree-like format, making it easy to visualize their relationships. Business units can contain other business units and projects, helping you clearly organize your company's structure.
- **Search Functionality**: At the top of this section, you will find a search input that allows you to quickly locate a specific business unit or project by name.

Working with Business Units and Projects

You can manage both **Business Units** and **Projects** using a context menu that appears when you right-click on an item. Here are the available actions:

Business Unit Actions

- **New Business Unit**: Create a new business unit within the selected unit.
- **New Project**: Create a new project within the selected business unit.
- **Update Business Unit**: Modify the name of the selected business unit.
- **Delete Business Unit**: Remove the selected business unit from the hierarchy.

Project Actions

- **Update Project**: Modify the name of the selected project.

- **Delete Project**: Remove the selected project from the hierarchy.

Adding or Editing Names in Multiple Languages

Each **Business Unit** and **Project** has a **Name** field, which can be defined in multiple languages. When adding or editing a name, you will see a language selector on the right side of the input field. Use this selector to specify the language for the name, allowing for multilingual support throughout your structure.

Reorganizing the Structure

The hierarchical representation of business units and projects can be easily reorganized using drag-and-drop functionality. You can drag both business units and projects to different positions within the hierarchy to adjust the structure as needed. This makes it simple to adapt to changes in your company's organization.

4.4 - Groups Management

How to Create and Manage Groups in the CDM Web Application

The *Groups Management* Interface provides administrators with the tools to organize users into groups, a fundamental component of the Role-Based Access Control (RBAC) inside the CDM-Server.

This page allows you to create, view, update, and delete groups within the system, ensuring flexible and secure user management.

Types of Groups

There are three types of groups available on the Groups Management page:

- **Local Groups:** These groups are fully managed within the system. Administrators can add or remove users from these groups as needed to align with access requirements.
- **Remote Groups:** Remote groups are synchronized from external ID-provider (LDAPS and Azure). These groups list remote users in a read-only mode.
- **Singleton Groups:** These are system-generated groups that are automatically created when a user is either created (for local) or registered (for LDAPS and Azure). Each Singleton Group contains only the individual user for whom it was created. Singleton Groups are read-only, meaning additional users cannot be added to them, nor can the user be removed from their Singleton Group. A Singleton Group is a special case of a Local Group.

Creating a Group

- Click on the + button in the table header to open the Create Group dialog.
- Fill the **Name** field (multiple languages are allowed) and the **Remote Id** field (only for LDAPS and Azure)
- Click Save to add the group to the system. The new group will appear in the groups table.

Assigning and Removing Users

Once a Group has been selected, in the right panel of the Groups Management page, administrators can assign or remove users from **normal groups** to adjust access as needed:

- **Assign Users:** Click on the + button of the panel and select a one or more users from the “search users dialog” and add them to the selected group, granting them the permissions associated with the group’s roles.

- **Remove Users:** Click on the “trash” icon button once at least one user has been selected to revoke the associated permissions.

> **Note**
>
> For remote groups, the user list is displayed in read-only mode, meaning users cannot be added or removed from within the system.

4.5 - Roles Management

How to Create and Manage Roles in the CDM Web Application

The *Roles Management* Interface allows administrators to define and organize roles within the CDM-Server.

On this page, you can create, view, and delete roles as needed, though roles cannot be updated once created. After creating roles, you can assign or remove groups to manage which users have specific access rights.

Creating a Role

- Click on the + button in the table header to open the Create Role dialog.
- Define the new role by selecting the Role Template and level in the organization's tree (see RBAC integration).
- Click Save to add the role to the system. The new role will appear in the roles table.

Assigning and Removing Groups

Once a role has been selected, in the right panel of the Roles Management page, administrators can assign or remove groups as needed:

- **Assign Groups:** Click on the + button of the panel and select a one or more groups from the "search groups dialog" and add them to the selected role. This will grant all users in those groups the permissions defined by the role.
- **Remove Groups:** Click on the "trash" icon button once at least one group has been selected to detach it from the role. This action will revoke the permissions associated with that role for all the users of the group.

4.6 - Users Management

How to Create and Manage Users in the CDM Web Application

The *Users Management* Interface provides the capability to create, view, and manage user accounts.

Key Features Overview

This view provides a centralized interface to view and manage user profiles along with simplified user creation with optional system-generated passwords, workflows for password resets and forced password changes.

Creating a New User

(This option is available only when Local is selected as the Id-Provider)

- Click on the + button in the table header to open the Create User dialog.
- Fill in the required fields. Login should be a unique identifier for the user. Password should be either entered manually or click Generate Password for a secure system-generated password.
- Click Save to add the user to the system. The new account will appear in the user table.

Editing Existing Users

Locate the user in the table and click the Edit (pencil icon) to open the Edit User form. Update user details as necessary.

Password Reset

(This option is available only when Local is selected as the Id-Provider)
When a password reset is initiated for a user, a Temporary Password is generated and displayed in a pop-up. The administrator can copy this password and share it with the user. Temporary Password Validity Temporary passwords are valid for a limited period (e.g., 2 days). If the password expires, a new reset must be initiated by the administrator.

User Workflow with Temporary Passwords

When a user logs in using the temporary password, the system redirects the user to the Change Password dialog. The user must enter the current password (the temporary password). A new password must be set and confirmed before access is granted. Once the password is changed, the temporary password becomes invalid, and the user gains access to the system.

Self-Service Password Management for Users

Users have the ability to manage their passwords directly

From the user menu in the header, select Change Password. In the Change Password dialog, enter the current password. Set and confirm a new password. Click Continue to complete the password update.

Register a User

(This option is available only for LDAP and Azure as Id-Provider)
Registering an external user in the system is a crucial task that enables the CDM-Server to effectively manage and track users. Rather than duplicating user data, the server creates a reference entry in the database, allowing seamless integration of the external user into RBAC and other essential processes. This approach ensures that external users are fully enabled within the system without redundant data storage, maintaining efficient and streamlined access management.

4.7 - IQ & CDM Users map

How to map CDM Users with IQ Persons in the CDM Web Application

The **IQ & CDM Users Map** section enables you to link IQ Persons (referred to as candidates) with CDM users.

Procedure

1. Selection of a project

To begin, select a project containing unapproved candidates. Only projects with unapproved candidates will be available in the project selection dialog. Candidates are considered **approved** once they are mapped/linked to a CDM user. Selecting a project will lock it to prevent simultaneous modifications by other users. If another user has locked the project, you will not be able to select it until they release the lock.

2. List of candidates

Once a project is selected, the left-side list will display IQ Persons (candidates) pending a match. Use the additional filter at the top of the list to refine your list as needed. Candidates are displayed with their Name, First Name, and E-mail by default. To reveal more details, click the button next to the “UNAPPROVED CANDIDATES” title. Changes to the displayed attributes are saved automatically and will be applied the next time you use the tool.

3. List of users

In the next step, you can search for CDM users by applying search criteria, then clicking “Search”. Users appear with their Login and First Name by default, but additional details can be displayed by clicking the button next to the “USERS” title. These display settings are saved for future sessions.

Create new Users (Local only)

If the required CDM user does not exist, you can create a new user by selecting the “New User” option. This option is available only if you are using local as the IdProvider on the CDM Server

and you have admin privileges.

Creating Users

- **Right-click on “New User”** to open a dialog with all fields for a CDM user. Fill in the necessary information and submit to create the user.
- **Create from Selected Candidates** option is enabled when selecting at least one candidate and right-click “New User”. A dialog will open with all fields for a CDM user, with the option to select one of the previously selected candidates as template to pre-fill some of the fields and make the creation process faster.

4. Match Candidates with Users

To match a candidate with a user, select at least one candidate from the left list and exactly one user from the right list. This enables the " » " button, allowing you to move candidates to the user.
NOTE: This won’t perform any definitive change.

5. Review and apply changes

After mapping candidates to users, review the changes before applying them. Each candidate (IQ Person) can be mapped **ONLY ONCE**; this is a permanent action and cannot be undone. If you are ready to proceed, click the confirmation button to finalize the mappings.

6. Approved candidates

Once a candidate is mapped, they are considered **approved** and will be removed from the candidate list. If no candidates remain, the project selector will clear, and the project lock will automatically be released.

Reset changes

Click “Reset” to clear your progress, including any selected project, releasing the lock on the project and clearing all changes made in the current session.

4.8 - Settings

Configuration options for managing languages, user interface, and system preferences

The *Settings* page allows all users to customize system preferences, including language settings and user interface layout. Changes made on this page are applied upon saving, and the page will automatically reload to reflect the updates.

Configuring General Settings

The **General** tab in the Settings page allows users to adjust their system-wide preferences, including language options and UI layout.

- **Content Language** The Content Language dropdown allows users to set the language for system content. For example, you can select “Deutsch” or “English” based on your preferred language for viewing data and content within the system.
- **Interface Language** The Interface Language dropdown allows users to change the language of the application’s user interface. This ensures that menus, buttons, and labels are displayed in the selected language.
- **Identity Provider** The IdProvider dropdown displays the authentication provider for your account. This setting can not be changed.
- **Left-Side Menu Layout** Left side menu collapsed: Checking this box collapses the menu on the left-hand side of the interface by default.
- **Saving Changes** Adjust the settings as needed in the General tab. Click Save to apply your changes. The page will reload automatically, and the new settings will be reflected immediately.

Configuring User-Specific Settings

The **Users** tab in the Settings page allows users to configure how attributes are displayed in the Users Management interface.

Attribute Order The Attributes Order section lets users reorder the fields displayed in the Users table, such as Title, Name, Login, Department, Email, Phone, and more. To reorder attributes:

- Drag and drop the fields to arrange them in your desired order.
- Click Save to apply the changes.

- The page will reload automatically, and the new order will be reflected in the Users table

Configuring Administrative Settings

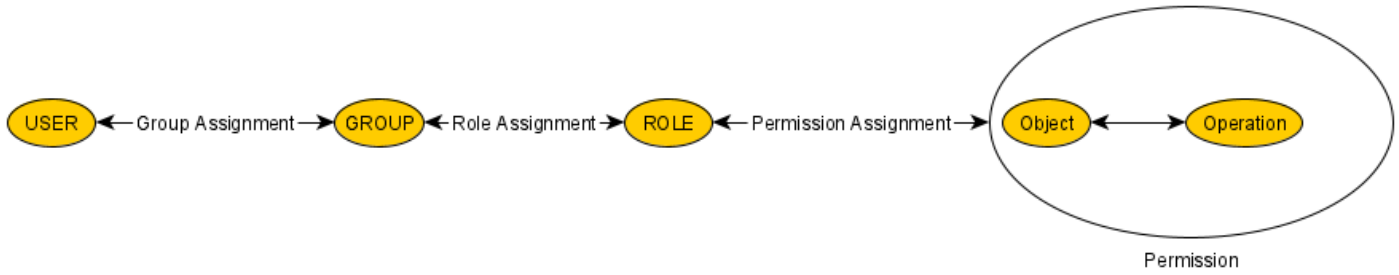
The **Administration** tab in the Settings page allows the Administrators to change configuration properties.

- **Contact Email** The email address you provide will be used exclusively for display purposes, allowing other users to contact the Administrator. Please note that no email system or messaging service is configured for this address—it is read-only and cannot be used to send or receive emails. This value is visible only to other users who need to reach out to the Administrator.

5 - Role-Based Access Control

How to manage users, groups, roles and permissions

The *Role-Based Access Control (RBAC)* section enables efficient management of user permissions across your organization by assigning users to groups, groups to roles and roles to permissions.



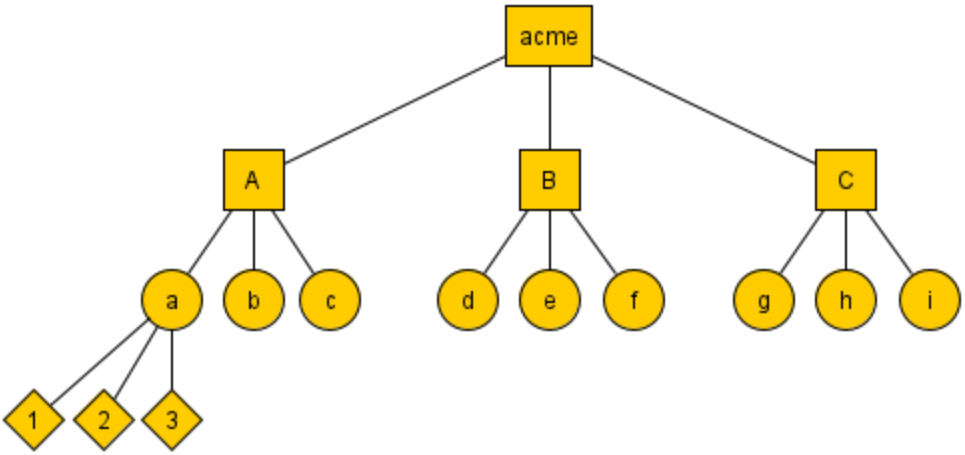
Role-Based Access Control (RBAC) centers on using a small set of rules to determine whether a particular user is permitted to perform an operation x on an object o. In the RBAC model, the constructs of groups and roles facilitate the efficient assignment of permissions to a potentialy large set of users. Groups aggregate users into a smaller number of entities, which are equivalent from an RBAC perspective, while roles bundle permissions into manageable units that can be assigned collectively, enabling users to carry out specific tasks. A permission, in this context, represents the combination of an operation with an object.

Regarding operations, the CDM RBAC model supports only two: READ and WRITE. Important: The permission to WRITE an object also allows to READ that object. A key aspect of permissions is efficiently defining sets of objects. The model takes advantage of the fact that objects within the IQ FMEA model can be organized as part of a vast family tree. Unlike a traditional family tree, however, the RBAC tree does not differentiate by gender—it simply consists of parent and child members.

Child members fall into two categories: some are intended to become parents themselves (e.g., business units), while others remain terminal (e.g., projects). In a conventional family tree, the structure starts with a progenitor. In contrast, the RBAC tree begins with a business unit representing the entire organization managed by the CDM server. From this root, children can either be parent elements (business units) or terminal elements (projects), allowing the tree to grow recursively to capture increasingly detailed levels of the organization.

In CDM RBAC roles need not be created globally but can be restricted to parts of the organization. Roles are created from Role templates and a member of the tree. Let’s assume your organization is divided into three departments called A, B and C whose common parent is the progenitor (member representing the organisation as a whole).

An abstract tree view of this organization called acme would look like the following diagram



CDM RBAC Role templates

The CDM RBAC provides three role templates:

1. Permission to write the member the template it is applied to and all its descendants; this Role-template is called **Admin** for short.
2. Permission to write all descendants of the associated tree member but not the associated member itself; this Role-template is called **Editor** for short.
3. Permission to read the member the template it is applied to and all its descendants; this Role-template is called **Viewer** for short.

Admin users and normal users

Users are classified into two categories based on the given rights at the specified level in the organization's tree:

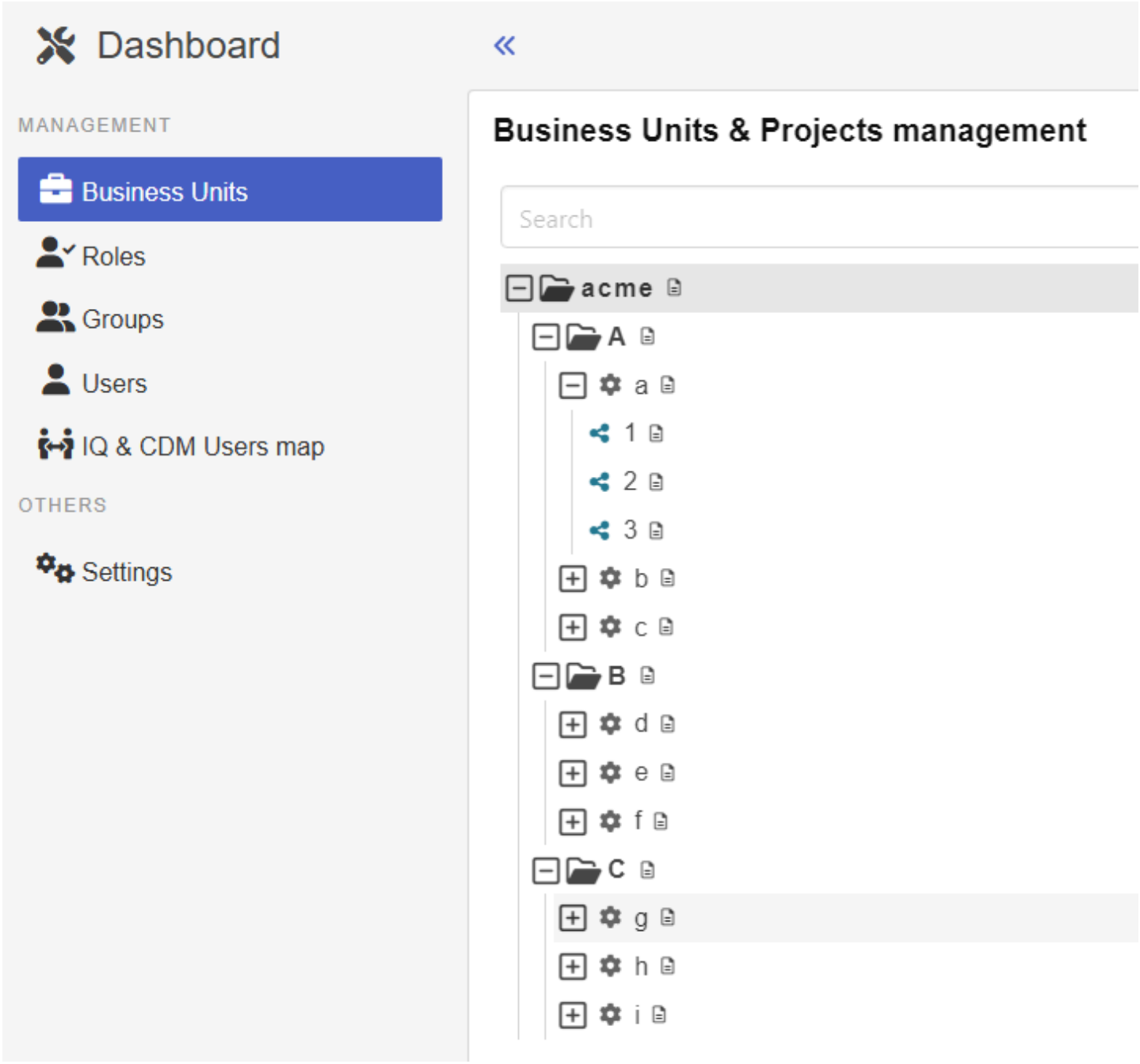
- **Admin Users:** These users have **admin** rights (write permissions) at the root level of the organization's tree. Ony these users are allowed to create, modify or delete users, groups and roles.
- **Non-Admin Users:** These users lack write permissions on the root level of the organizational tree, restricting some functionalities and access to sections (see Roles page for more information).

A tour through *RBAC of APIS CDM-Server* functionality

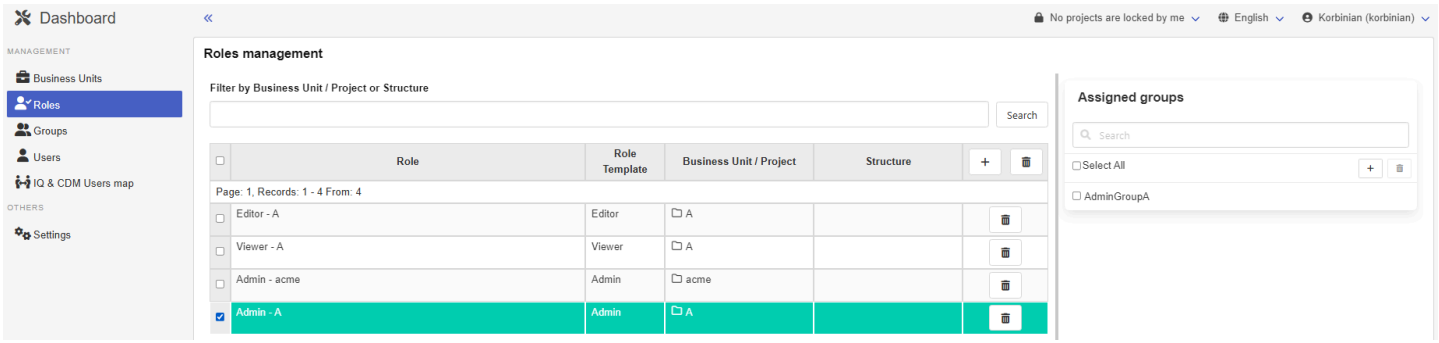
You may create an Admin, an Editor and a Viewer role for department A (called *Admin - A*, *Editor - A*, *Viewer - A*). These three roles in isolation have no effect. You need to create groups in addition. Let's assume you create three groups called AdminGroupA, EditorGroupA and ViewerGroupA and assign the AdminGroupA to role *Admin of A*, EditorGroupA to role *Editor of A* and ViewerGroupA to role *Viewer of A*. As the last step users are assigned to the three groups. Assuming 10 users work in department A, and you assign Chad and Julia to the AdminGroupA, John, Vitali, Manuel to the EditorGroupA Christoph, Andreas, Johannes and Conny to group ViewerGroupA. In addition there are two admins named Donald and Korbinian.

A user with administrator permissions

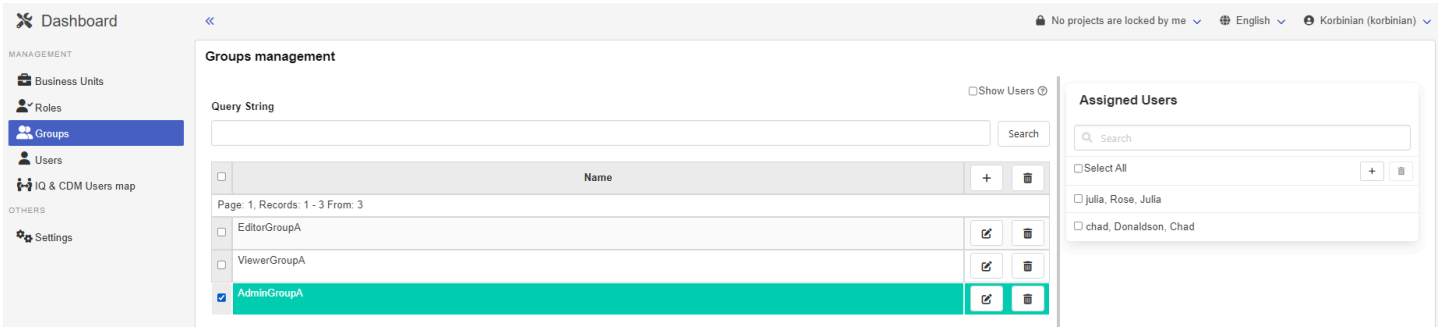
As a first step Korbinian logs into the Dashboard of the CDM-Server. After clicking on *Business units* he would see the following



Clicking on *Roles* and selecting the *Admin - A* role this is presented



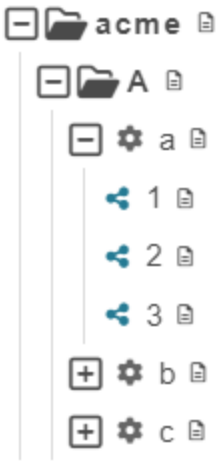
And after clicking on *Groups* and selecting *AdminGroupA* this:



What effect will this have on the individual users after the login to the CDM-Server?

Admin role on a business unit

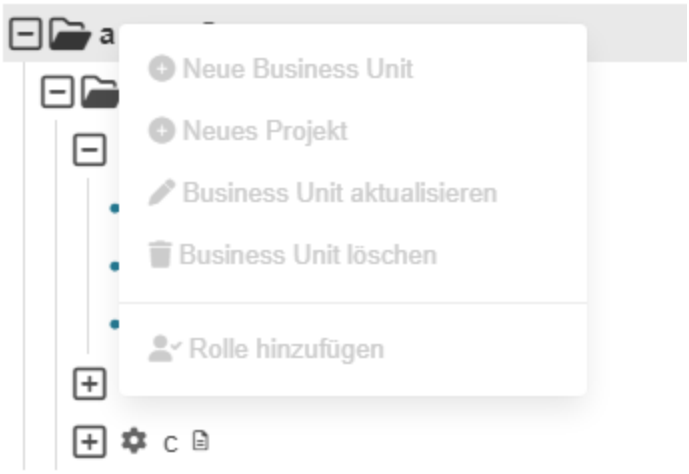
To answer this question Julia logs into the Dashboard and clicks on *Business Units*



Julia cannot see the Business Units *B* and *C* because she does not own Roles that gives her read permissions on those Business Units. But she can see Business Units *acme* and *A* and all descendants of *A*. She owns the *Admin - A* role which according to the definition above assigns write permissions for *A* and its descendants to Julia. Two additional rules of *RBAC of CDM-Server* are at play here that extends the permissions of Julia beyond those explicitly defined by the roles:

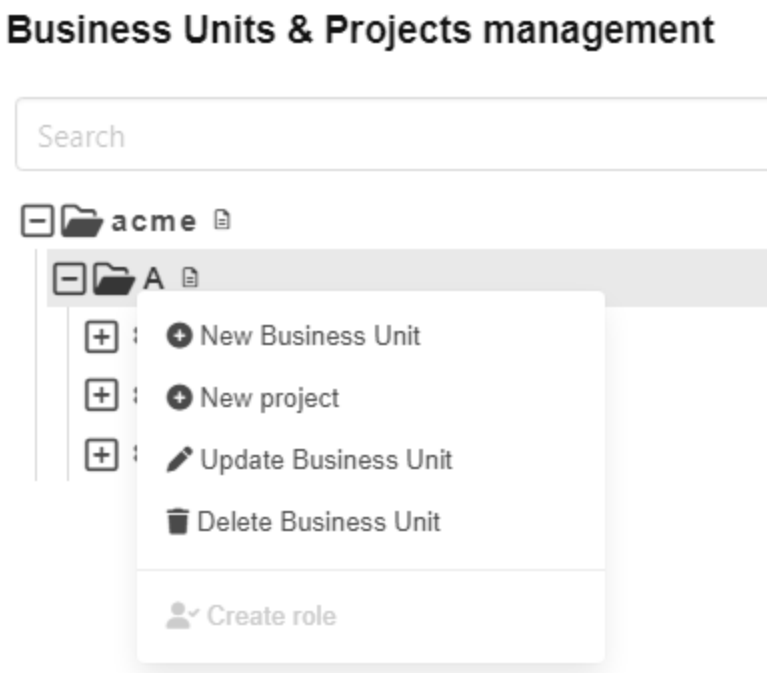
1. If a user owns write permissions on a member of the tree via the roles the user owns this user automatically gains read permissions on that member.
2. If a user owns read or write permissions on a member of the tree via the roles the user owns this user also gains read permissions on the ancestors of that member.

The first rule allows Julia to read *A* and all its descendants and the second rule allows Julia to read the *acme* node of the tree. If she clicks right on the Business Unit acme a context menu is shown



All potentially possible actions are shown but in this case each one is shown deactivated because Julia does not have write permissions on this tree node.

The context menu of Business Unit *A*



Here the picture is mixed. 3 actions are activated and 2 are deactivated. This situation relates to the third rule of *RBAC of CDM-Server*

3. The deletion or creation of a tree member is possible only if the user owns write permissions (a) on that member **and** (b) on the *parent* of that member.

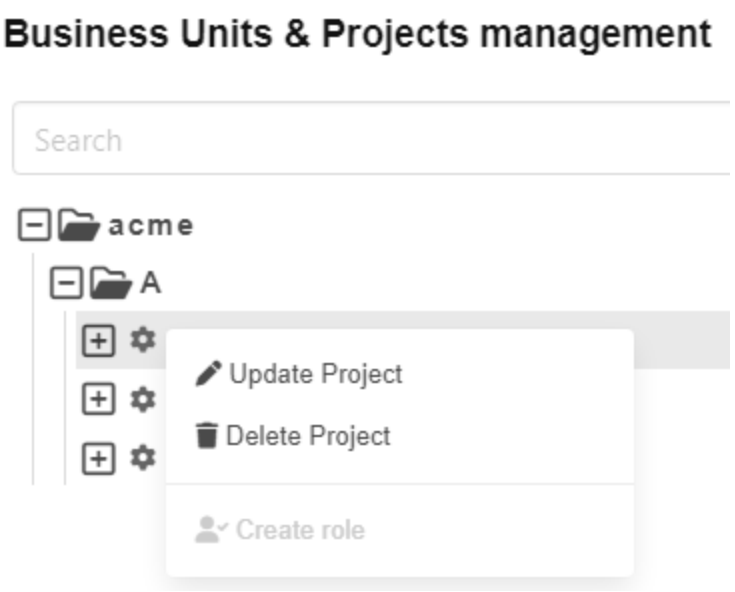
> Business Units and Projects (but not Structures) can be moved by drag and drop in the *Business Units* view.Assume a user wants to move a tree node *n* with parent *s* (source parent) to a new parent *t* (target parent). Such a move is sequence of actions:

1. remove *n* from *s*
2. add *n* to *t*.

Consequently, considering rule *3*, the user needs the following permissions:

(a) write permission on *n* (b) write permission on *s* (c) write permission on *t*

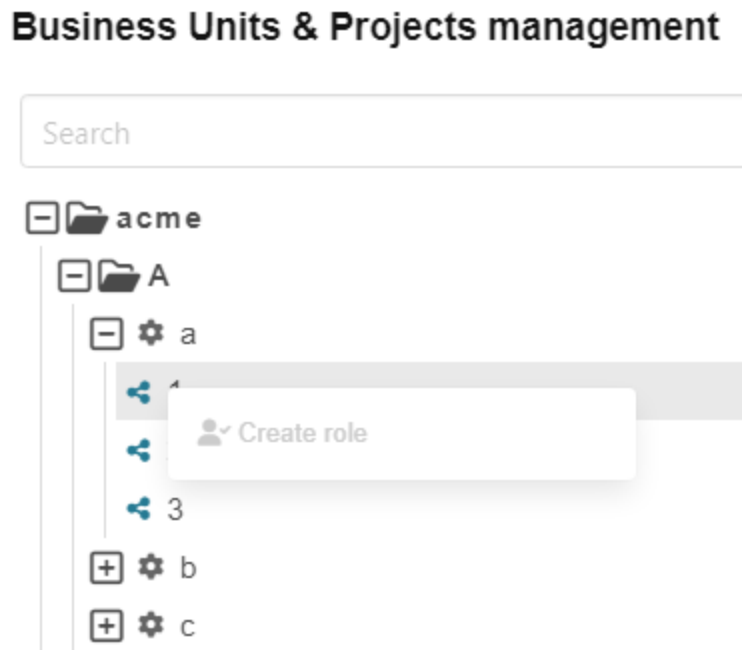
Now Julia opens the context menu of Project *a*



As Julia owns the write permission on A all actions for non admin users are possible. Roles can only be created by admin users (see below).

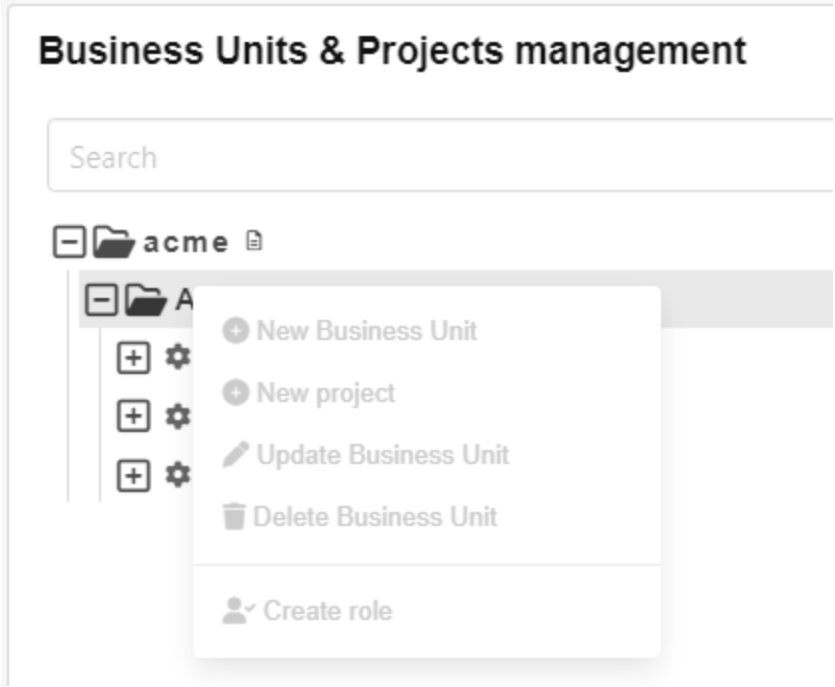
You might miss the action ‘Create structure’ here. But this is beyond the functionality of the dashboard and is only offered by the *APIS IQ-Software*. The *RBAC of CDM-Server* is not restricting this.

Last but not least Julia right-clicks on the structure *1*



Editor role on a business unit

Next Vitali logs into the Dashboard of the CDM-Server. He sees the same tree as Julia in the *Business Units* view. The context menu of *acme* is also identical but the context menu of *A* is different.



Vitali is in the EditorGroupA group which is connected to Role *Editor - A*. Recalling the definition of the Role template *Editor* above let's you note that this role does not include WRITE permission on the tree node it is defined on. In combination with rule *3* it is evident that Vitali cannot use any action provided in the Dashboard on tree node *A*.

As follows from the discussion above the context menus for Project *a* and Structure *1* are identical to Julia's.

Viewer role on a business unit

Finally Johannes logs into the Dashboard of CDM-Server.

The *Business Unit* view is the same as for Julia and Vitali. The context menus of all levels that Johannes can see will only contain deactivated actions because the only Role that Johannes owns is the Viewer - A Role. The description of the Role template *Viewer* specified that only READ permissions are given to a user by that role. Because all actions change some aspects of the data model, and therefore would need WRITE permissions, none of the actions is available if a user only owns READ permissions.

This ends the tour!

The major elements of *RBAC of Apis CDM-Server* have been presented. More information can be found in the sections on ID_PROVIDERs LOCAL, LDAP and Azure and special sections on Users, Groups and Roles.

5.1 - Users

CDM-Server Users as part of the RBAC

The *Users Management* is the essential first step in defining and organizing access permissions, as all subsequent groups, roles and permissions rely on the accurate setup of user accounts.

Regardless of the chosen ID Provider, configuring users in the User Management section establishes the essential foundation for RBAC (Role-Based Access Control), enabling robust, secure, and scalable access control across the system.

How Users integrate with RBAC

By establishing users first, the organization can easily assign them to groups and later link these groups to roles as needed, creating a scalable, manageable RBAC hierarchy.

> **Admin only**
>
> The workflows described below can only be performed by administrators.

Typical Workflow

- **User Registration:** Users are created or imported from an external source (LDAPS or Azure). This provides a central repository for user accounts.
- **Assign Users to Groups:** Once added, users are assigned to Groups. Groups are logical collections of users with similar access requirements, such as departments, teams, or project members.
- **Link Groups to Roles:** Groups are then connected to Roles. Roles define the specific permissions for each group, streamlining the process by allowing permissions to be assigned collectively rather than individually.

For detailed guidance on managing users, visit the Users page.

5.2 - Groups

CDM-Server Groups as part of the RBAC

The *Groups Management* is a central component in the system's Role-Based Access Control (RBAC) in the CDM-Server. It enables administrators to create, edit, view, and delete Groups—the critical link between users and roles. By assigning users to groups, and then associating those groups with roles, you can efficiently manage permissions across the organization without needing to configure each user individually.

How Groups integrate with RBAC

Groups act as a bridge between users and roles. By defining permissions at the group level, administrators can simplify access control, making it easier to manage permissions for multiple users at once.

> ### Admin only
>
> The workflows described below can only be performed by administrators.

Typical Workflow

- **Create a Group:** Define a new group and specify its purpose (e.g., "Project Managers" or "Quality Assurance").
- **Assign Users:** Add users to the group who need similar access levels.
- **Associate Roles:** Link the group to specific roles that define permissions.
- **Review and Adjust:** Regularly view and update group memberships and role associations as team compositions change.

For detailed guidance on managing groups, visit the Groups page.

5.3 - Roles

CDM-Server Roles as part of the RBAC

The *Roles Management* section is the final and essential piece of the Role-Based Access Control (RBAC) in the CDM-Server.

Roles define specific permissions within the system, determining what actions can be taken and what resources can be accessed by groups and their members. Roles are the end-point in the RBAC hierarchy, serving as the permission layer that applies to users indirectly through their assigned groups.

How Groups integrate with RBAC

In the CDM-Server there are 3 predefined ***Role Template*** s which already have specific permissions:

- **Admin:** Grants full write permissions on the selected level within the organization's tree, including all subordinate levels. Admin users have complete control over the selected node and any of its child nodes, allowing them to modify, add, or delete resources.
- **Editor:** Provides write permissions **ONLY** on the child nodes of the selected level within the organization's tree. Editors can modify content and make updates at subordinate levels without altering permissions or resources at the main (selected) level, preserving the structure while enabling focused updates.
- **Viewer:** Offers read-only access on the selected level within the organization's tree, including all subordinate levels. Viewers can view resources and data within these levels but cannot make any changes, ensuring secure and restricted access for users who need visibility without modification rights.

> ### Admin only
>
> The workflows described below can only be performed by administrators.

Typical Workflow

- **Create a Role:** Define a new role by selecting the Role Template and level in the organization's tree (Business Unit or Project).
- **Assign Groups:** Add groups to the role.

- **Review and Adjust:** Regularly view and update group and role associations as team compositions change.

For detailed guidance on managing roles, visit the Roles page.

6 - Miscellaneous

6.1 - Changelogs

CDM-Server Update Notes

v1.1.1

Release Date: 2025-03-26

Fixes

- rs-2200: Permission Error After Upgrading from v1.0.0 to v1.1.0
- rs-2204: Improved error logging
- rs-2213: IQ-Software connectivity error (TLS certificate related)

v1.1.0

Release Date: 2025-03-13

Features

- IQ-Software – CDM-Server now supports ***IQ-Software V8.0 - 0040***.
- Login URL – The login URL has been updated to `/` instead of `web/welcome.html` (Documentation).
- RBAC for CDM-Server – Roles can be defined on Business Units, Projects and Structures and the access to these elements is controlled by the Groups and Roles defined. (Documentation).
- Business Unit – A reload button has been added in Business Unit.
- Database Enhancements – Added automatic backup & manual restore functionality, and performance optimizations. (Documentation)
- Settings Panel – Added a settings panel that allows the user to change the language. Admin can also set a contact email. (Documentation)
- Bill of Materials – This has been updated. (Documentation)

Fixes

- Better Login & Group Handling – Fixed login issues and improved group management in the initial setup.
- Azure & LDAP Integration – Bug fixes.
- Optimized Dashboard – Fixed missing or incorrect translations for a better user experience.
- Candidate Approval – Minor UI tweaks.
- Various improvements across the board for a smoother and more secure experience.

v1.0.1

Release Date: 2024-11-19

Features

- Support for *IQ-Software V8.0*
- Azure (Entra) integration

Fixes

- Minor bug fixes

v1.0.0

Release Date: 2024-11-06

Features

- Server support for *IQ-Software V8.0*
- Candidate approval workflow
- Local user management
- LDAP integration
- Role-based access control (RBAC) (No Enforcement)
- User and group management

6.2 - Data Backup/Restore and Maintenance

About how to backup/restore your data, as well as scheduled daily/weekly maintenance tasks.

Backup

Automatic backup

The automatic backup system is integrated into the CDM-Server. It does not function when the CDM server is down.

Every night at 2:00 AM, a daily compressed backup file in the `.tar.gz` format is created in the `.backups` folder. This file, in turn, contains a highly compressed file named `db.tar.gz`, which holds all the database files required for restoring a database. Additionally, the backup file in the `uploads` folder contains binary blob files that belong to the CDM server's data model but are stored outside the database for performance reasons. The name of the backup file is generated according to the following pattern:

```
cdm_backup_<database-version>_<date>.tar.gz
```

The date follows the format `%Y%m%d%H%M%S` and is based on the host system's time zone. Here is an example of a backup file name created on December 12, 2024, starting at 2:00 AM, with the database version 16:

```
cdm_backup_16_20241212020000.tar.gz
```

Backup files older than 30 days are automatically deleted. The backup files are created without significantly affecting the database operations.

Preserving backup files for longer than 30 days is your task. Please make sure you copy the backup files to a save place before they get deleted.

Manual Backup Execution

Backups can also be manually initiated if needed (e.g., before deploying a new CDM server version). To do so, simply run the shell script:

```
./backup
```

The CDM-Server needs to be active for the backup to work. The backup is created without significantly affecting database operations. A manual backup must not be started while an automatic backup is running. The backup file is generated using the same pattern as the automatically created backup files and is located in the same folder. It is also named according to the same format and is also automatically deleted after 30 days.

Restore

To do this, run the script

```
./restore
```

Then, the instructions of the script must be followed. The script instructions are only available in English. The script stops the CDM-Server. If the script runs successfully, start the CDM-Server again using

```
./start
```

Maintenance

We automatically run some maintenance tasks on the data and database every week on Sunday at 00:00 and 04:00 (Server time).

Examples runs of `./backup` and `./restore`

Execute manual backup

```
./backup
pg_basebackup: initiating base backup, waiting for checkpoint to complete
pg_basebackup: checkpoint completed
```

```
pg_basebackup: write-ahead log start point: 0/E6000028 on timeline 1
pg_basebackup: starting background WAL receiver
pg_basebackup: created temporary replication slot "pg_basebackup_292042"
pg_basebackup: write-ahead log end point: 0/E6000100
pg_basebackup: waiting for background process to finish streaming ...
pg_basebackup: syncing data to disk ...
pg_basebackup: renaming backup_manifest.tmp to backup_manifest
pg_basebackup: base backup completed
Database and files backup completed.
Backup of database and files completed.
```

Execute restore

```
./restore
Page: 1 of 4

1. cdm_backup_16_20250221080438.tar.gz
2. cdm_backup_16_20250221075006.tar.gz
3. cdm_backup_16_20250221020000.tar.gz
4. cdm_backup_16_20250220020000.tar.gz
5. cdm_backup_16_20250219020000.tar.gz
6. cdm_backup_16_20250218020000.tar.gz
7. cdm_backup_16_20250217020000.tar.gz
8. cdm_backup_16_20250216020000.tar.gz
9. cdm_backup_16_20250215020000.tar.gz
10. cdm_backup_16_20250214020000.tar.gz

Enter the number to select a backup, 'n' for next page, 'q' to quit.
Choose an option: 1
Selected backup: cdm_backup_16_20250221080438.tar.gz
Are you sure you want to restore this backup? (y/n): y
Validating the backup file...
Backup file validated successfully.
Stopping the app and database container...
Stopping the server with Docker Compose...
[+] Running 7/7
✓ Container main-proxy-1   Removed
✓ Container pfx-converter  Removed
✓ Container cdm-web-1      Removed
✓ Container cdm-app-1      Removed
✓ Container main-db-1      Removed
✓ Network main_default     Removed
✓ Network main_common-net  Removed
Server stopped successfully!
```

```
Server stopped successfully!
Restoring the backup...
Database and file restoration process completed.

./start
```

6.3 - Service Worker

This document describes how the service worker enhances the application's behavior, including its supported features like session management, client communication, and request tracking, as well as the potential impact if it fails or becomes unavailable.

Supported Features

Session Management

- **Auto Logout:** Monitors active browser tabs and automatically logs out the user from the backend session when no clients are active.
- **Session Check:** Periodically pings the backend to verify the session status. If the session is invalid or expired, the service worker informs all open tabs.
- **Session Update Notifications:** Broadcasts session-related updates (login, logout, expiration) to all clients, ensuring users receive timely notifications.

Client Communication and Coordination

- **Multi-Tab Synchronization:** Listens for events such as "NewTab" and "TabClosed" to update the list of active clients and coordinate actions across them.
- **Language & Project Updates:** Relays language changes and locked project updates among all active tabs, ensuring a unified experience.
- **PostMessage Communication:** Uses a dedicated messaging system to send updates and notifications to clients, keeping the application state in sync.

Impact When the Service Worker Is Not Working

If the service worker fails or is unavailable, the following issues may arise:

- **Compromised Session Management:** Without the service worker, automatic logout and periodic session validation may not occur. This could lead to stale sessions or unexpected logouts.
- **Delayed or Missing Notifications:** Real-time notifications regarding session updates, language changes, or locked projects may not be delivered, causing inconsistencies across tabs.

- **Inter-Tab Coordination Breakdowns:** Multi-tab synchronization will be impaired, potentially leading to conflicting application states and user confusion.

Troubleshooting

If you notice issues that may be related to the service worker, consider the following steps:

- **Verify Browser Support:** Ensure that your browser supports service workers.
- **Check Service Worker Registration:** Use the browser's developer tools to confirm that the service worker is registered and active.
- **Clear Cache:** Unregister old service workers and clear the browser cache to resolve potential conflicts.
- **Look for Fallback Notifications:** The application may display a warning if the service worker is unavailable.

6.4 - Logs

Where to find logs and how to manage them.

> Logs Rotation
>
> We have implemented log rotation for the server logs and docker logs. If you find a log file that is not being rotated, please submit a bug report.

Application Logs

In the `.logs` directory, you can find all the logs generated by the server.

Container Logs

There are also some logs generated by OCI containers. You can find them in the `/var/lib/docker/containers` (or equivalent if you are using something else) directory. For database, `10x` `10mb` files are retained. For application, `10x` `100mb` files are retained.

6.5 - Setup on Windows

Running CDM-Server on Windows using WSL2

> **Unsupported**
>
> At this moment, we do not support running CDM-Server on Windows. This guide is for informational purposes only.

Prerequisites

- Latest Windows Version with WSL2 Support
  - Recommended: Windows Server 2022
  - Should Work: Windows 11 23H2+
- Access to Windows Store
- Internet Connection

Installation Steps

1. Install: Ubuntu LTS on Windows Store
   - Alternatively, open `Windows Store`, Search for `Ubuntu` (by Canonical Group Limited) and Install it
2. Open `Ubuntu` from START and follow the instructions to set up your user inside WSL Ubuntu
3. Install Docker Engine with Docker Compose Plugin
   - (Recommended) Uninstall Old Versions
   - From the official Docker website: Install Docker Engine
     - This involves two steps: add canonical apt repository and then installing docker engine
4. Once done, optionally type: `cd ~ && mkdir cdm && cd cdm`
5. Now that you have a working linux inside windows, you can follow the CDM-Server installation on linux steps: See here
6. After the installation, you can find the CDM-Server in `~/cdm` directory

Troubleshooting

- I can access CDM-Server from the server computer but not from other devices
  - Check your firewall settings and make sure the port is open
  - The specified `CDM_HOST` should resolve to the server's IP address
- I want to run CDM-Server as a service in Ubuntu
  - You need to follow WSL2 Systemd Guide to run services in WSL2

6.6 - Bill of Materials

Software Bill of Materials for CDM-Server

> ### Software Bill of Materials
>
> Software Bill of Materials (SBOM) is a complete list of all the software components used in a project. It is a critical part of the software supply chain and helps in identifying and mitigating security vulnerabilities.

CDM-Server SBOM

We provide the SBOM in OWASP's `CycloneDX v1.5/v1.6` format which has been officially ratified as an *Ecma International* standard.

You can find the SBOM for CDM-Server here:

- `v1.1.1` : JSON 1 | Summary 1 || JSON 2 | Summary 2
- `v1.1.0` : JSON 1 | Summary 1 || JSON 2 | Summary 2
- `v1.0.1` : JSON | Summary
- `v1.0.0` : JSON | Summary

Additional Information

CDM-Server also utilizes:

- Java 21 (Temurin JRE 21.0.5)
- PostgreSQL v16 (postgres:16-alpine)
- Alpine Linux
- pg_repack 1.5.0
- Bulma 0.9.4
- font-awesome 6.1.2
- Caddy 2.9.1
- Traefik 3.3.3

6.7 - Install Self-Signed Certificate

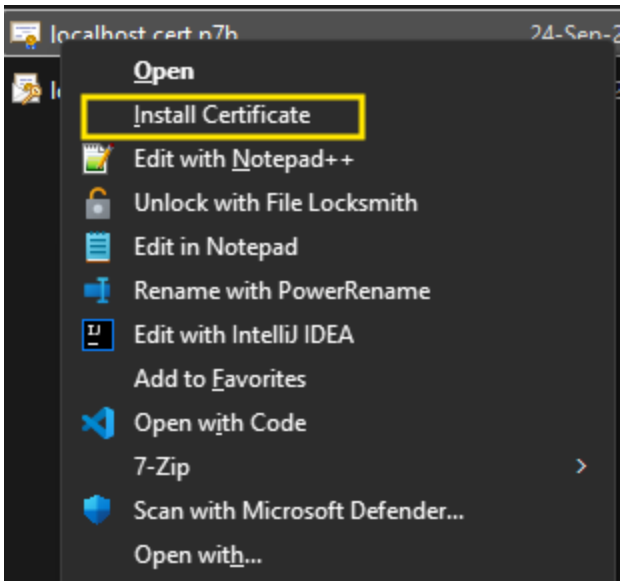
How to Install Self-Signed Certificate on the Client

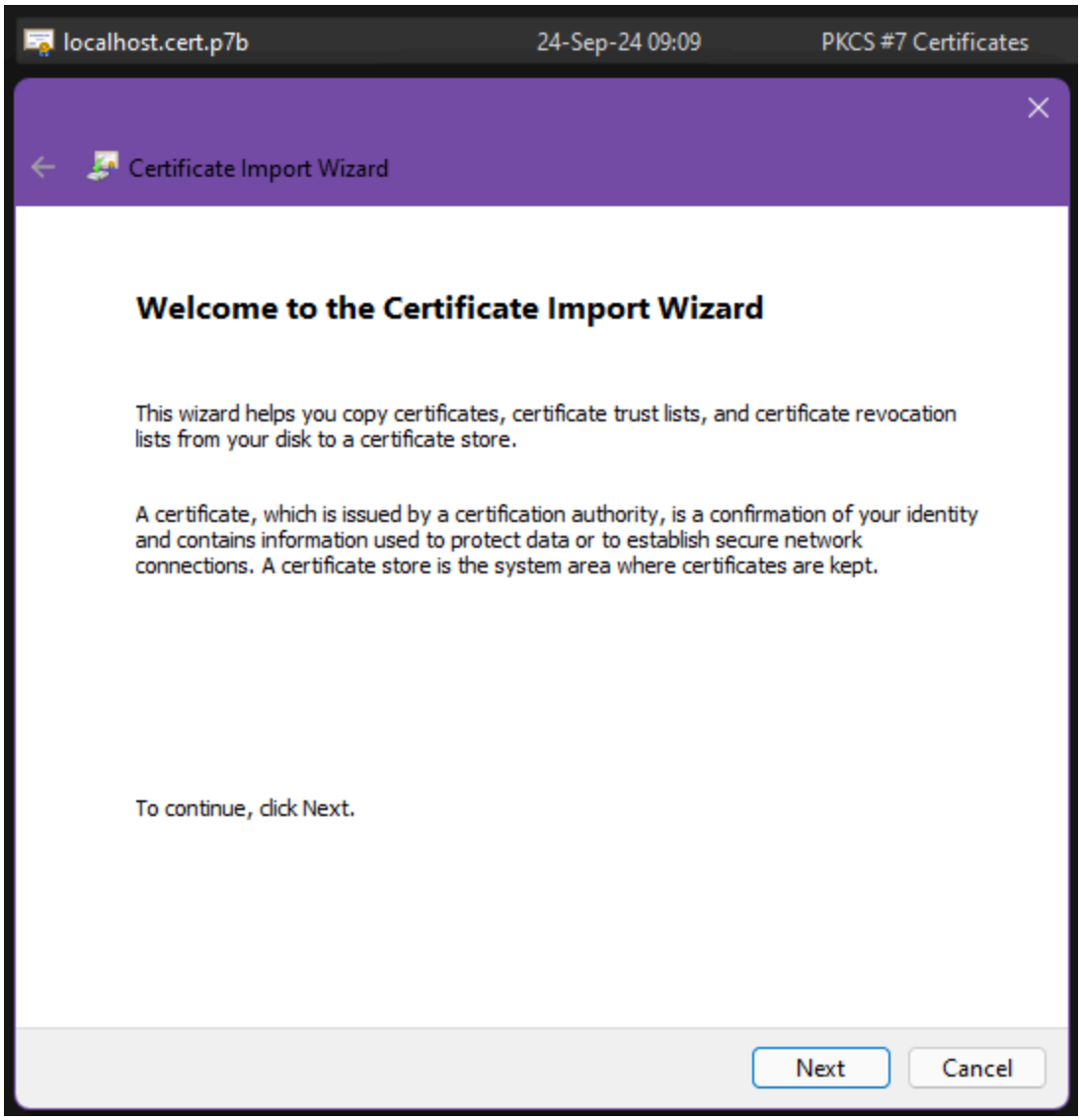
Manual Installation Steps

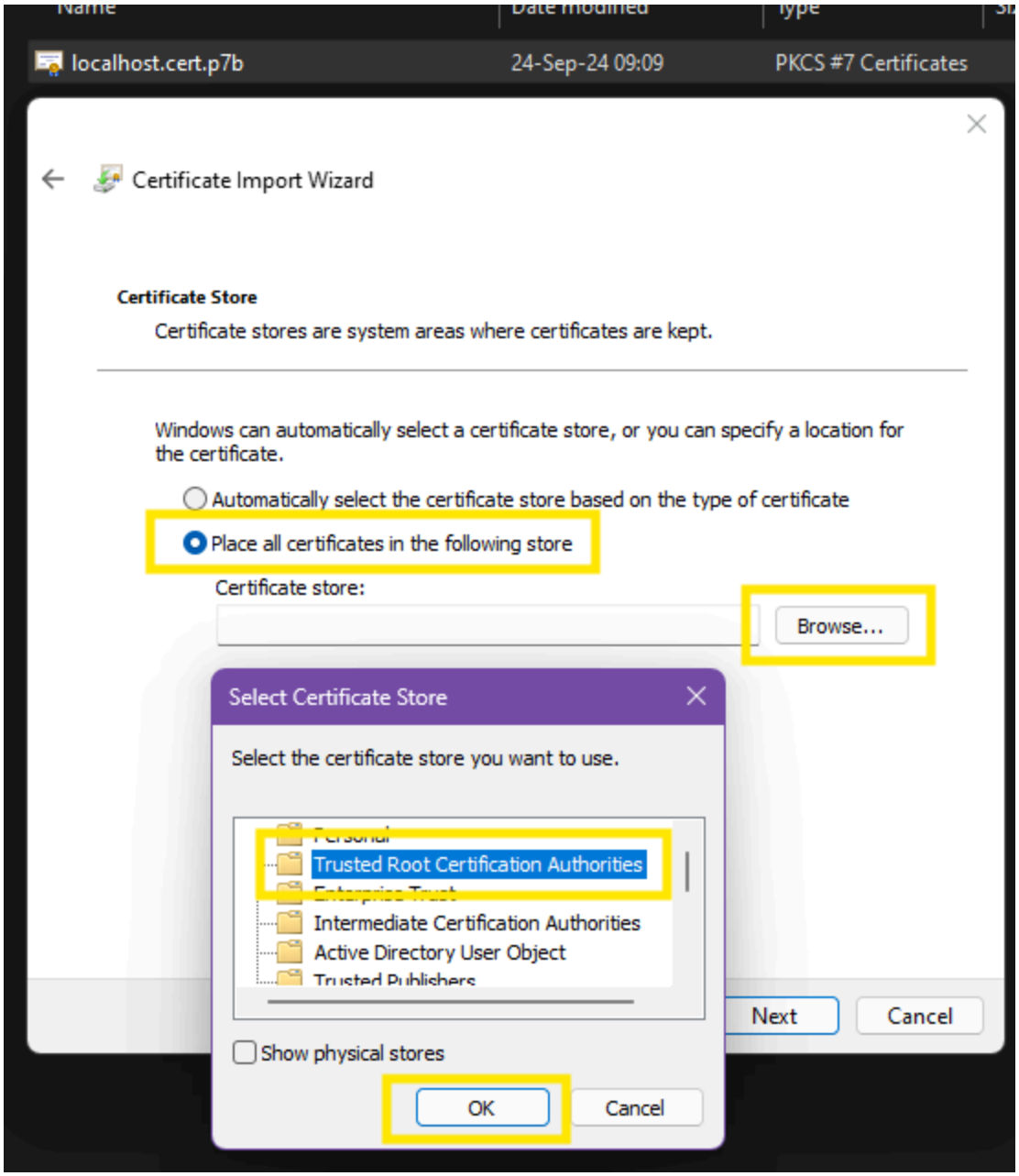
First, you receive the certificate from the administrator. Then, you can install it using the following steps:

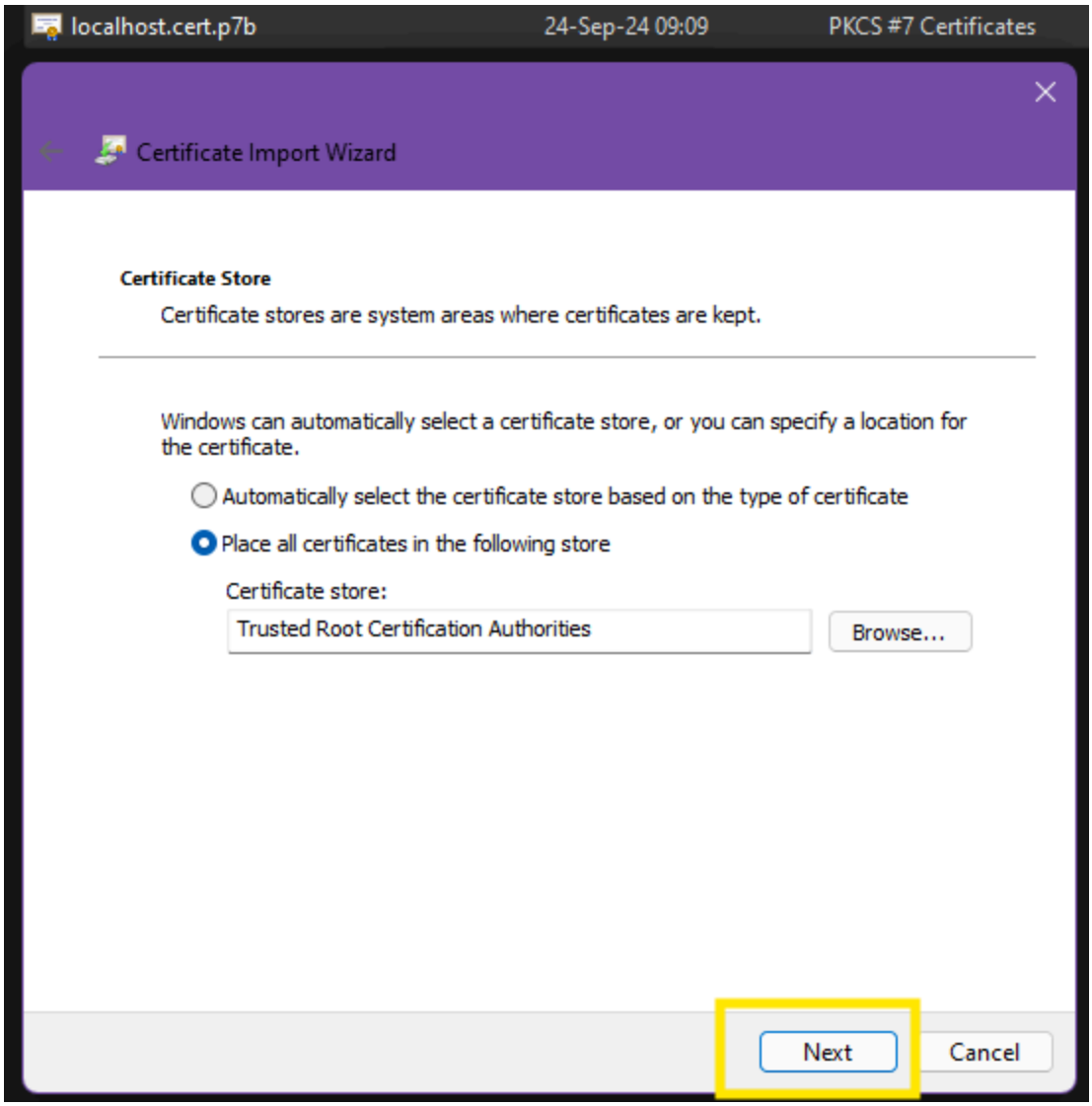
> ### Certificate Location
>
> For Admins: The system generated self-signed certificate location is given here.

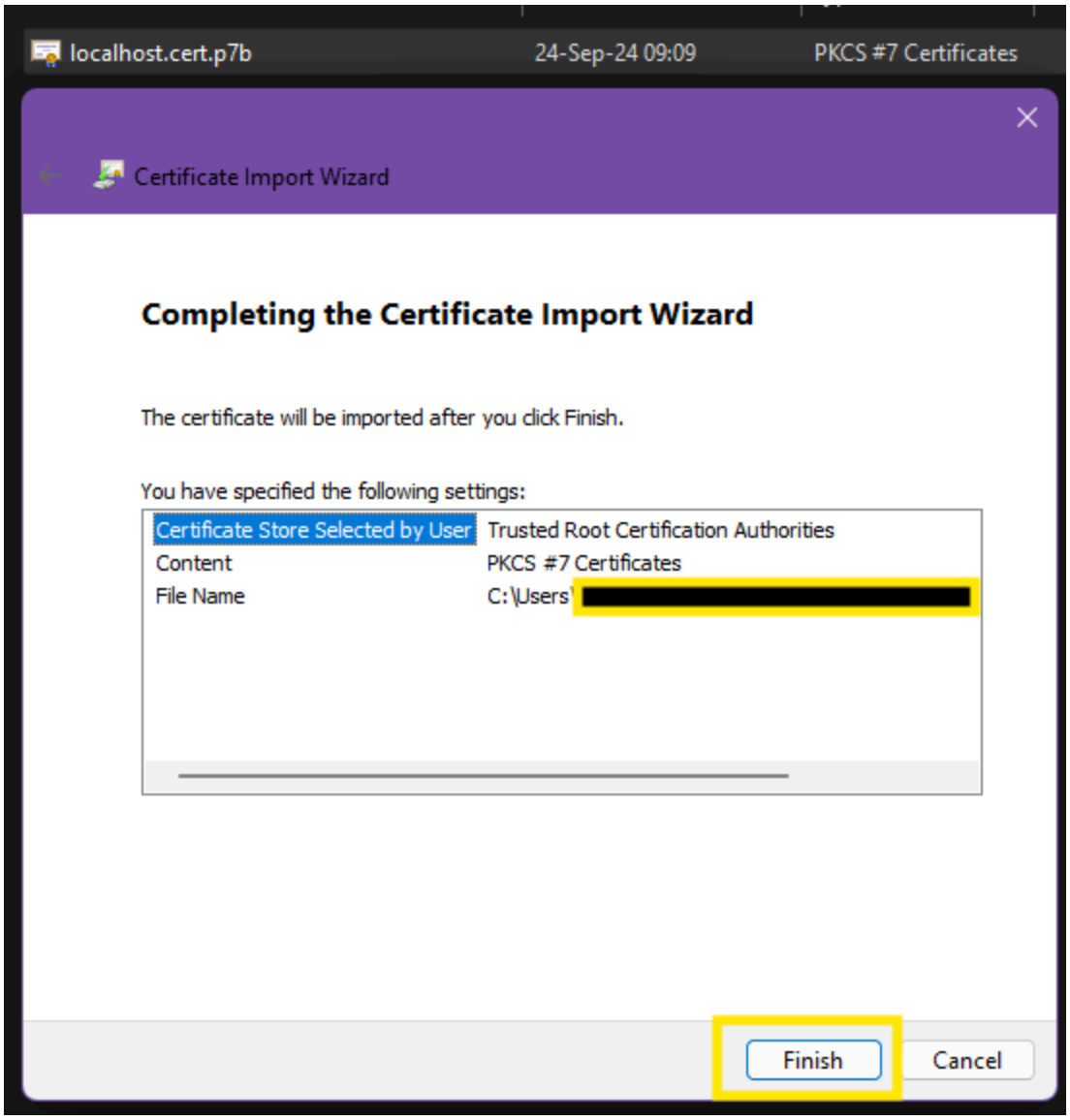
> ### Consult with Your Administrator
>
> Please consult with your administrator before installing the certificate.

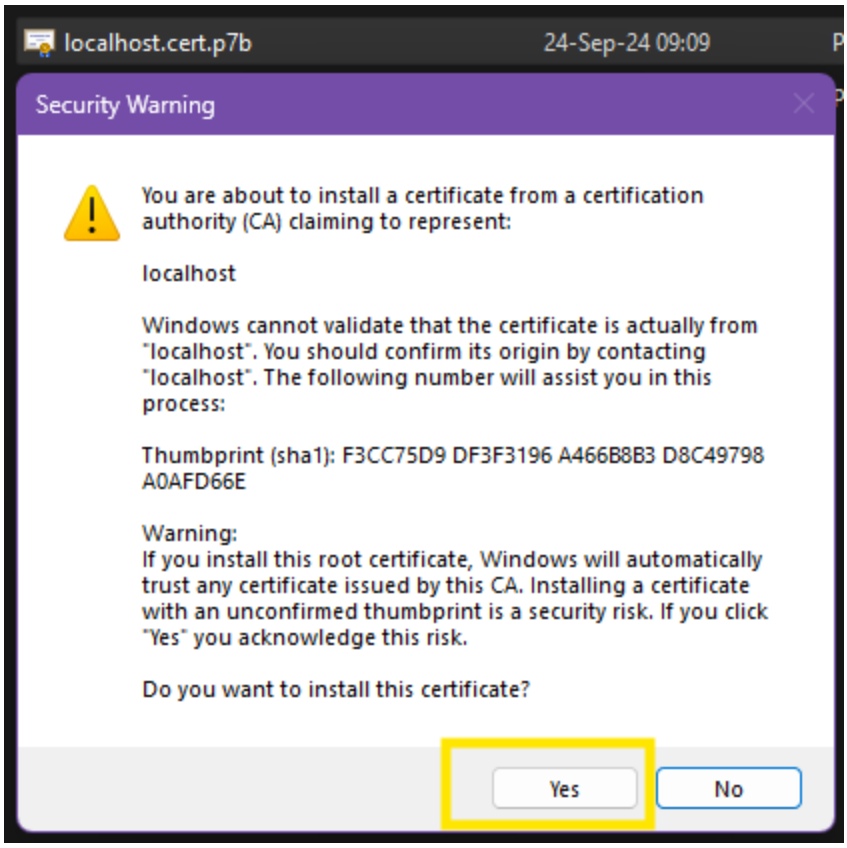



localhost.cert.p7b
24-Sep-24 09:09
PKCS #7 Certificates
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
Next
Cancel


Name
Date modified
Type
localhost.cert.p7b
24-Sep-24 09:09
PKCS #7 Certificates
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
Select Certificate Store
Select the certificate store you want to use.
Trusted Root Certification Authorities
Intermediate Certification Authorities
Active Directory User Object
Show physical stores
OK
Cancel
Next
Cancel


localhost.cert.p7b
24-Sep-24 09:09
PKCS #7 Certificates
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
Next
Cancel


localhost.cert.p7b
24-Sep-24 09:09
PKCS #7 Certificates
Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certification Authorities
Content
PKCS #7 Certificates
File Name
C:\Users\
Finish
Cancel


localhost.cert.p7b
24-Sep-24 09:09
Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
localhost
Windows cannot validate that the certificate is actually from "localhost". You should confirm its origin by contacting "localhost". The following number will assist you in this process:
Thumbprint (sha1): F3CC75D9 DF3F3196 A466B8B3 D8C49798 A0AFD66E
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

6.8 - Create PFX

How to Create a PFX File from CER/KEY Files

At the moment, we only support `.pfx` file for custom certificates. If you have a different format, you can convert it to `.pfx` using the following command:

```
openssl pkcs12 -export -out cdm-server.pfx -inkey example.key -in example.cer -certfile ful
```

Where:

- example.key: Your private key file.
- example.cer: Your certificate file.
- fullchain.cer: The additional CA certificate chain.

> **OpenSSL Version**
>
> You should use a recent version of OpenSSL (at least v3+).