iVIEW
Data Automation Framework

Installation guide

Company	informatec experience the sense of tomorrow
Date	30. March 2026
Subject	Installation of the iVIEW Data Automation Framework
Content	iVIEW Data Automation Framework – Installation and configuration parameters

Table of Contents

Table Index

Figure Index

1 Introduction

This manual provides the iVIEW Dataflow / iVIEW Library user with information and pointers on how to install, configure, and maintain the tool.

1.1 Purpose and main benefits of the iVIEW Data Automation Framework

1.1.1 iVIEW Dataflow

The iVIEW Library is a standalone application that allows users to standardizing the use of code within your business and enabling your business to move towards a self-service environment.

The key features are

- A low-code framework for Qlik (automated code)
- Automated coding process that is universal and easy to replicate
- Create once and apply across relevant apps
- A secure and structured way to define ETL and business logic, while the code engine delivers automated Qlik script
- Standardized generated code is compatible with Qlik Sense
- Datatransfer for QlikCloud

1.1.1 iVIEW Library

The iVIEW Library is a standalone application that allows users to manage and deploy master data and content definitions to Qlik.

The tool lets users navigate through a central library and select master data items that can be deployed and subscribed to one or more Qlik applications. Data items or variables can be easily added, edited, or deleted and assigned to specific data models.

The iVIEW Library is first and foremost, a next level of self-service for all Qlik users, allowing them to populate applications, do sandboxing and more.

1.2 Reading notation

As a support for reading and faster consumption the following notation is provided:

⊕ This represents an advantage for a best practice, or a benefit that is worth highlighting.

⊖ This represents a disadvantage or misleading practice.

This highlights advice and provides insights on things the user should know when using a function.

This is an advice or topic of special importance that the user should pay attention to.

2 System requirements

This chapter covers the required specifications a device must have to run the iVIEW Data Automation Framework.

2.1 Server hardware

Resource	Details
CPU	Cores: 2 minimum, 4 recommended
RAM	4 GB minimum (one product), 8 GB recommended
Disk	6 GB minimum (for IVIEW Dataflow additional space is needed for data repository depending on workflow requirements)

Table 1: Server hardware

2.2 Server Operating Systems

OS	Details / Versions
Windows	Microsoft Windows Server 2016 or higher

Table 2: Server Operating Systems

2.3 Browser software

Browser	Details
Chrome	Tested on version 80.0.3987 up to latest
Edge	Tested on version 89.0.774.5 (64-bit) up to latest

Table 3: Browser software

2.4 Supported databases

Database	Details
H2	2.1.214 (embedded / single user)
MariaDB	11.02 (embedded / recommended)
MS SQL Server	from 2016 to 2022 latest tested & supported

Table 4: Supported Databases

2.5 Qlik Sense

Editions / Versions	Details
Qliksense Enterprise on Windows	February 2020 Patch 1 onwards – tested on latest November 2025 Patch 5
Qlik Cloud	Tested & supported

Table 5: Supported Qlik Sense Versions

2.6 SSL Certificate

Files	Details
SSL Certificate	Used to secure communications between iVIEW services and user authentication. Can be provided as a CRT file and key file or a PFX file. Requirements: - Issued to a domain (*.domain.com) or to a server in that domain - Key Usage: Digital Signature, Key Encipherment - Enhanced Key Usage: Server Authentication

Table 6: SSL – public and private key

3 Installation

With all system requirements gathered, the user can proceed to the actual installation of the iVIEW Data Automation Framework. The iVIEW installer allows for the configuration of a specific iVIEW Data Automation Framework according to the user's requirements.

3.1 Installation package

The following software package and additional files are provided by Informatec:

Product	Files
iVIEW Installer 1.1	iVIEW-Iinstaller.zip
License key	License

Table 7: Software package and additional files

3.2 iVIEW installer

To start the installation of the iVIEW Data Automation Framework, the first action is to unzip iVIEWInstaller_XXXX_X_X.zip file in a free empty folder.

After unzipping the iVIEWInstaller_XXXX_X_X.zip file launch the Installer over the "startInstaller.bat" file.

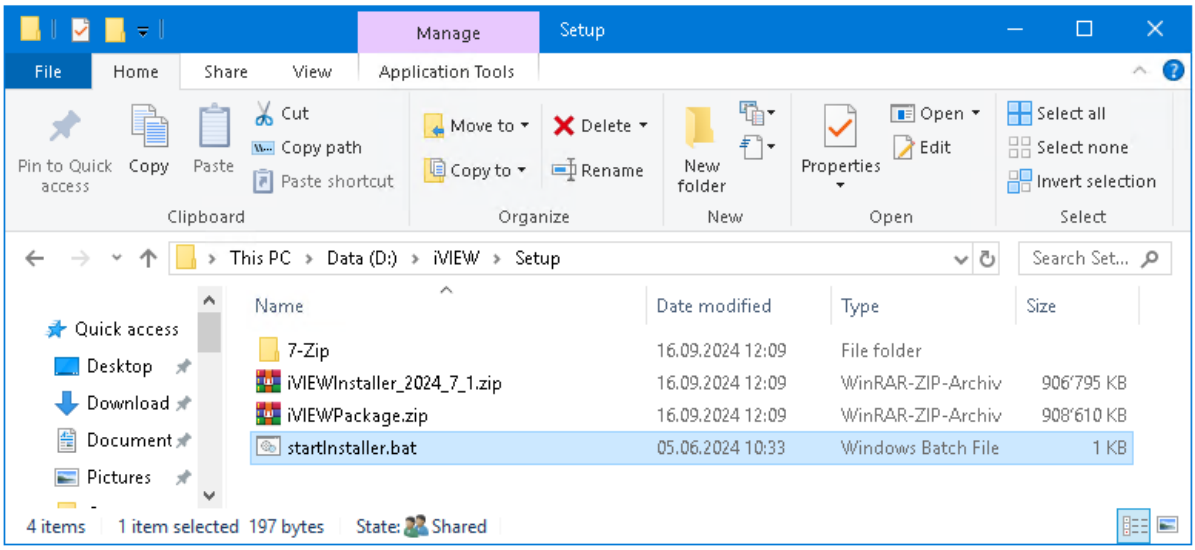

Figure 1: iVIEW Installer Zip

The installation process is partitioned in several logic steps as described in the following subsections.

3.2.1 Step 1: Chose an option to process

In the entry menu you can chose between different options:

- Install: Install a module (iVIEW Dataflow / iVIEW Library)
- Update: Update a module (iVIEW Dataflow / iVIEW Library)
- Uninstall: Uninstall a module (iVIEW Dataflow / iVIEW Library complete or only the services)
- Certificate: Renew a web certificate

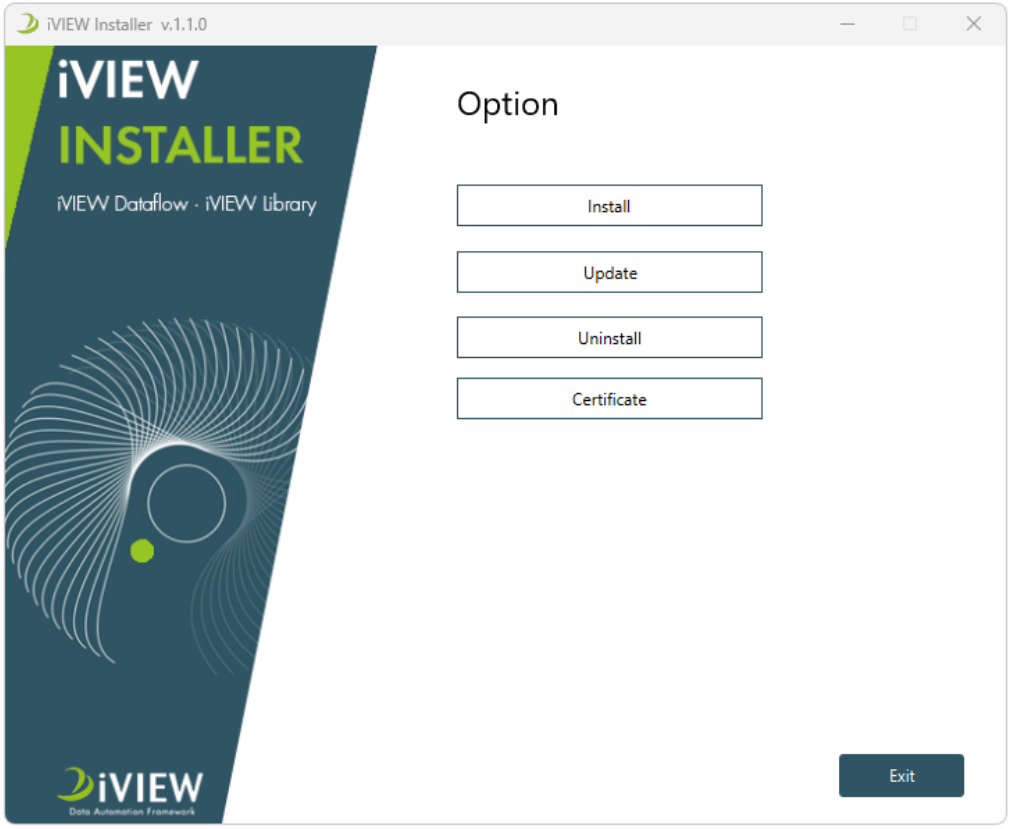

Figure 2 - Step 1: iVIEW Installer Options

For the first time chose install

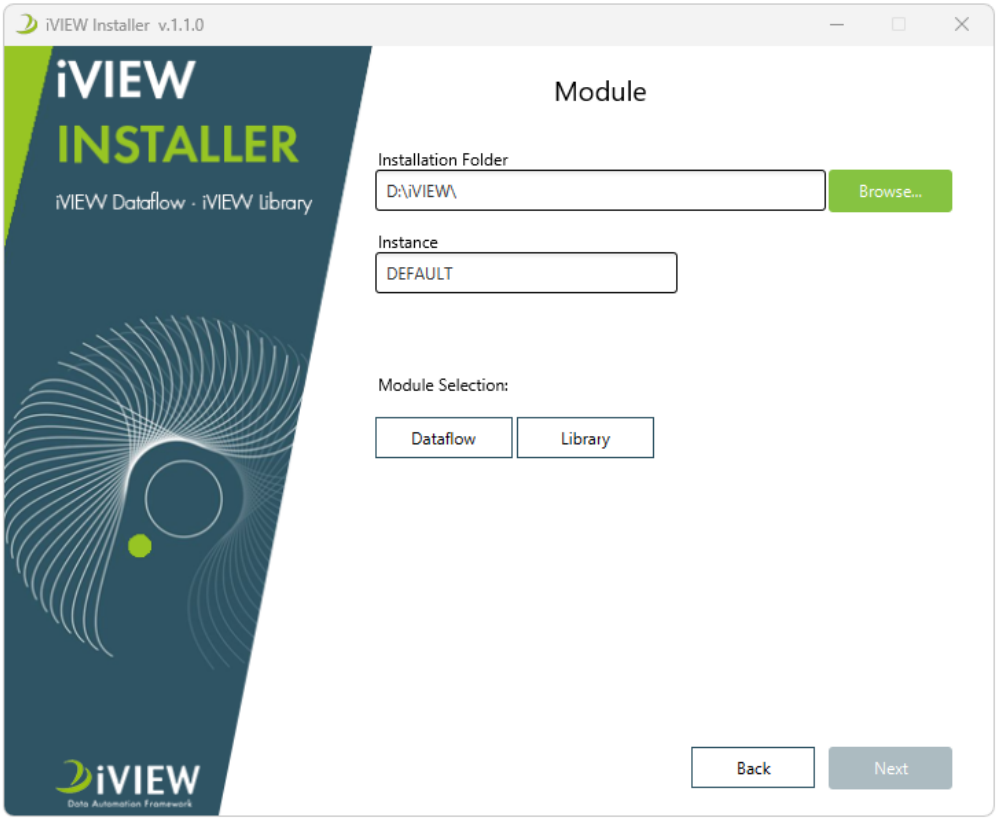

Figure 3: Step 1: Configure installation path and select modules

For the start of the installation, the process will be for the user to select the destination folder where iVIEW Data Automation Framework will be installed (the Instance if only one is needed can be retained to “DEFAULT”.

Before to continue to the next step at least one module (iVIEW Dataflow/ iVIEW Library) must be selected.

Installation will be performed for a “Default” instance.
iVIEW Data Automation Framework can be installed for several instances, which will run under the same root folder, but on different ports (defined in steps 3 and 4).

After selecting the iVIEW module to install / update, the user can proceed to the next step by clicking ‘*Next*’.

3.2.2 Step 2: Host name

Once the iVIEW module to install / update has been selected, the user should select a designated server where the iVIEW Data Automation Framework services will run. This can be done directly on Qlik or on a virtual dedicated machine for the iVIEW module. After selecting the Host, the user can proceed to the next step by clicking ‘*Next*’.

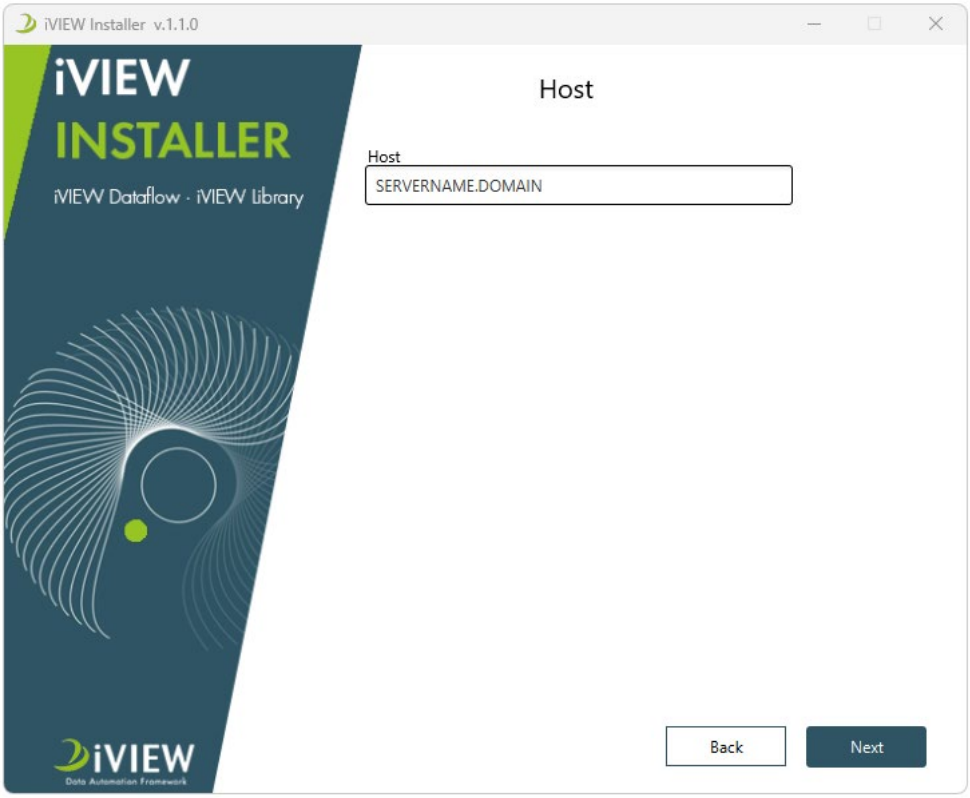

Figure 4: Step 2: Input Host

Web access to a module:
The defined host name will also be used as URL to access IVIEW Dataflow / iVIEW Library. If users should access over an alias instead of server name, the alias must be used as host

3.2.3 Step 3: Service User

If iVIEW Dataflow was selected for the installation or update, a service user must be defined which must have access to the filesystem (read, write, execute).

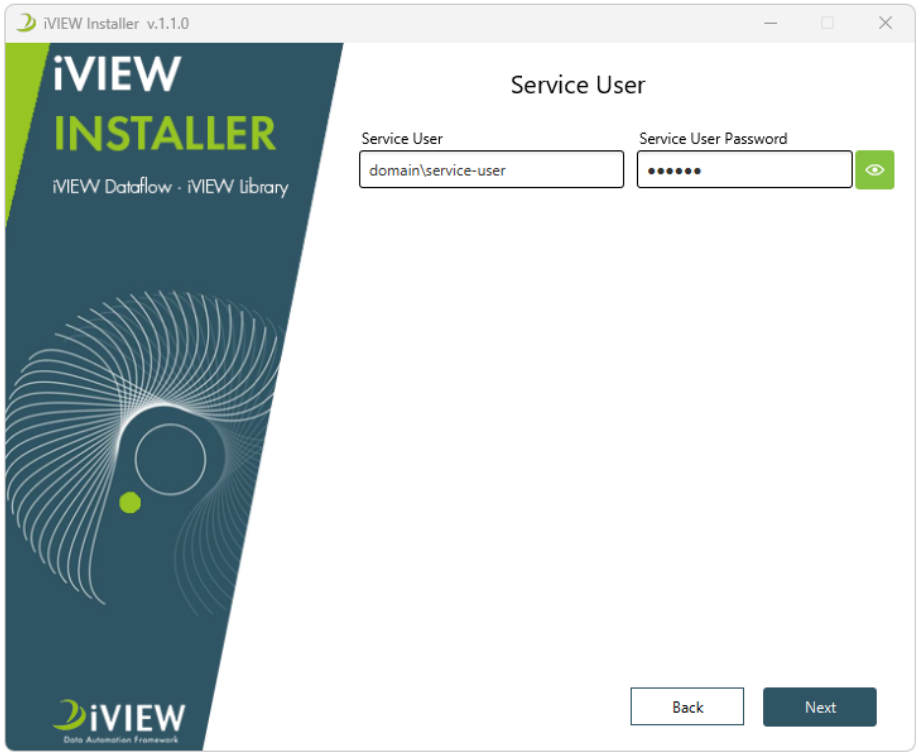

Figure 5: Step 3: Service User

iVIEW Dataflow repository:
In iVIEW Dataflow it is also possible to create the repository on a different server/share. This means that the service user must also have access to this directory (read, write, execute)

Allowed characters for the service user password:
The characters must be part of a standard char set. Only the following characters are allowed: A-Z a-z 0-9 + ? \ - * # _ ! $ % . , : ; & @ = /

3.2.4 Step 4: Keycloak

In this step, the user will be provided a port to be used for Keycloak. We strongly recommend using the default one that has been created.

It is also possible to add the the LDAP host (Active Directory) if Keycloak must access the Active Directory over a secure LDAPS connection.

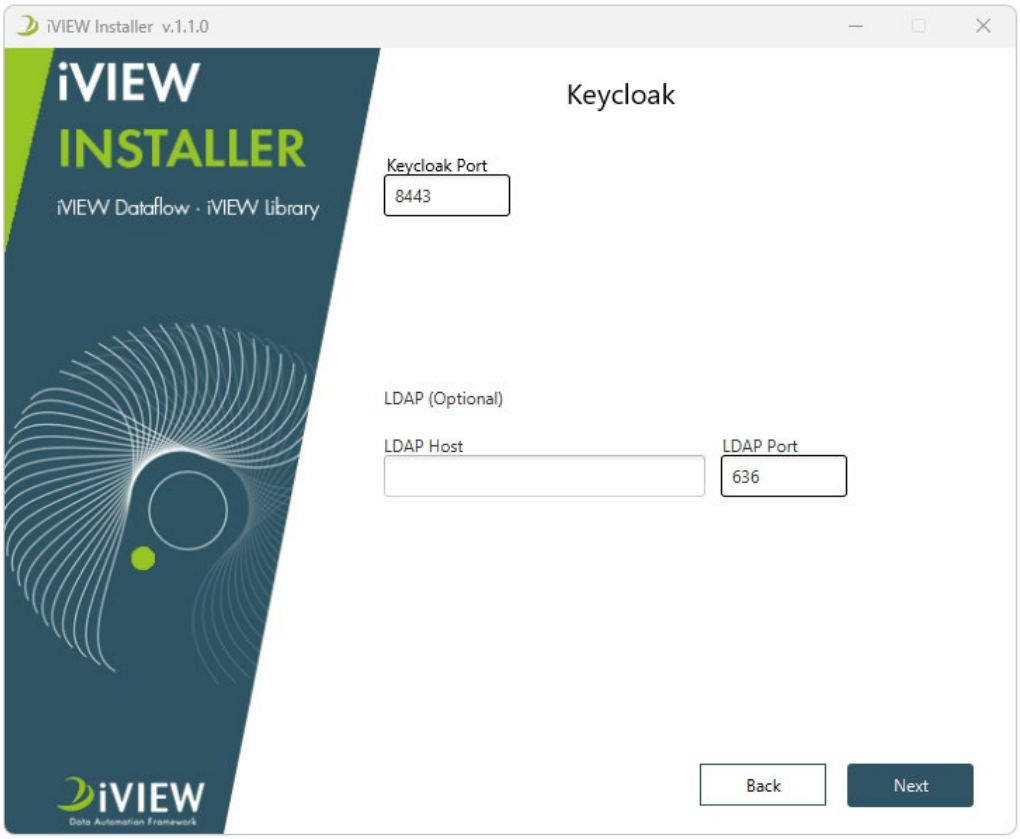

Figure 6: Step 4: Keycloak parameters

3.2.5 Step 5: Certificates

These certificates are used to secure all communications through the Https protocol.

1st Option - PFX keystore file:

The user should set-up a private key (PFX) with a password for the certificate/key file. *Recommendation is that this is done by IT.* The password is protected in keystore.

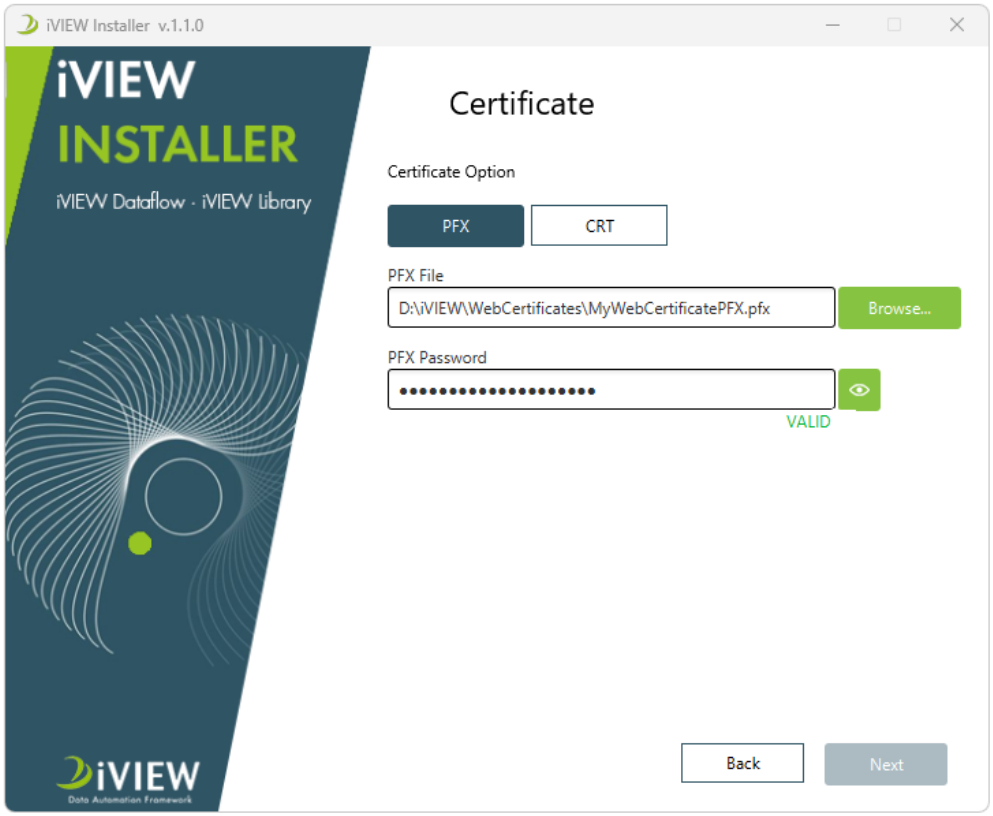

Figure 7: Step 5: Certificates (PFX)

The PFX password is required to extract the certificates that will be used by the iVIEW Dataflow / iVIEW Library.

2nd Option – Public and Private Key files (CRT):

The user should upload the server.crt file in the Public Key (CRT) and the server in the Private Key.

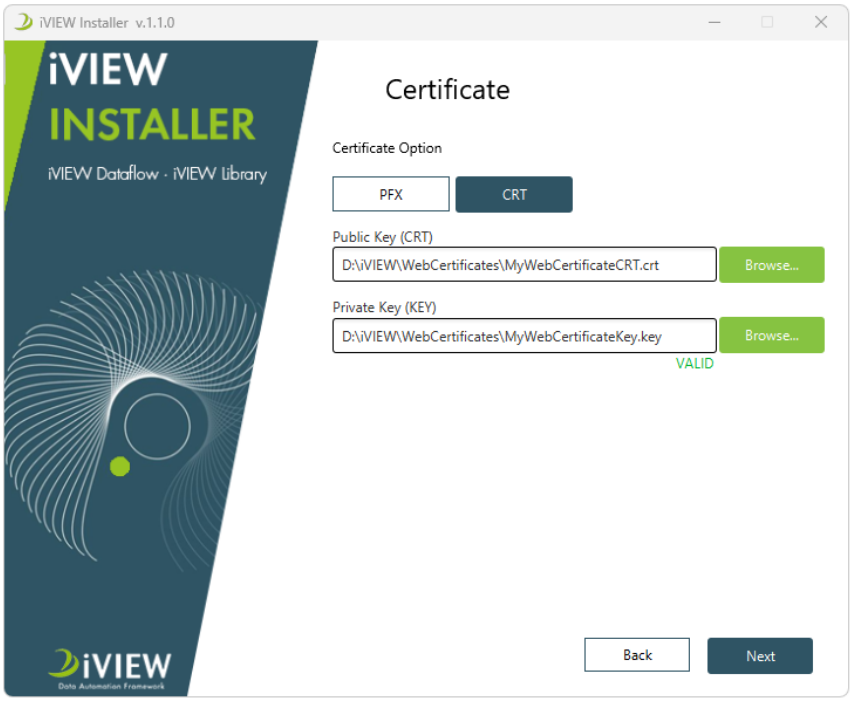

Figure 8: Step 5: Certificates (CRT)

3.2.6 Step 6: Dataflow

If iVIEW Dataflow was selected for install or update the user can change ports if some of them are already in use. By first installation the database password must be defined.

➔ As database, the option MariaDB is recommended.

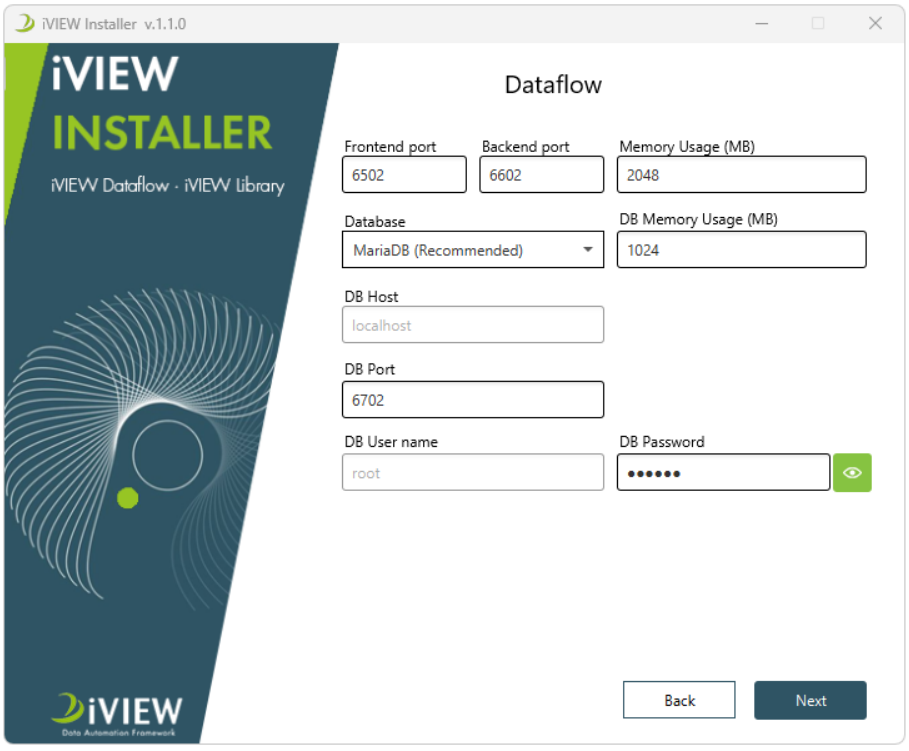

Figure 9: Step 6: Dataflow

3.2.7 Step 7: Library

If iVIEW Library was selected for install or update the user can change ports if some of them are already in use. By first installation the database password must be defined.

➔ As database, the option MariaDB is recommended.

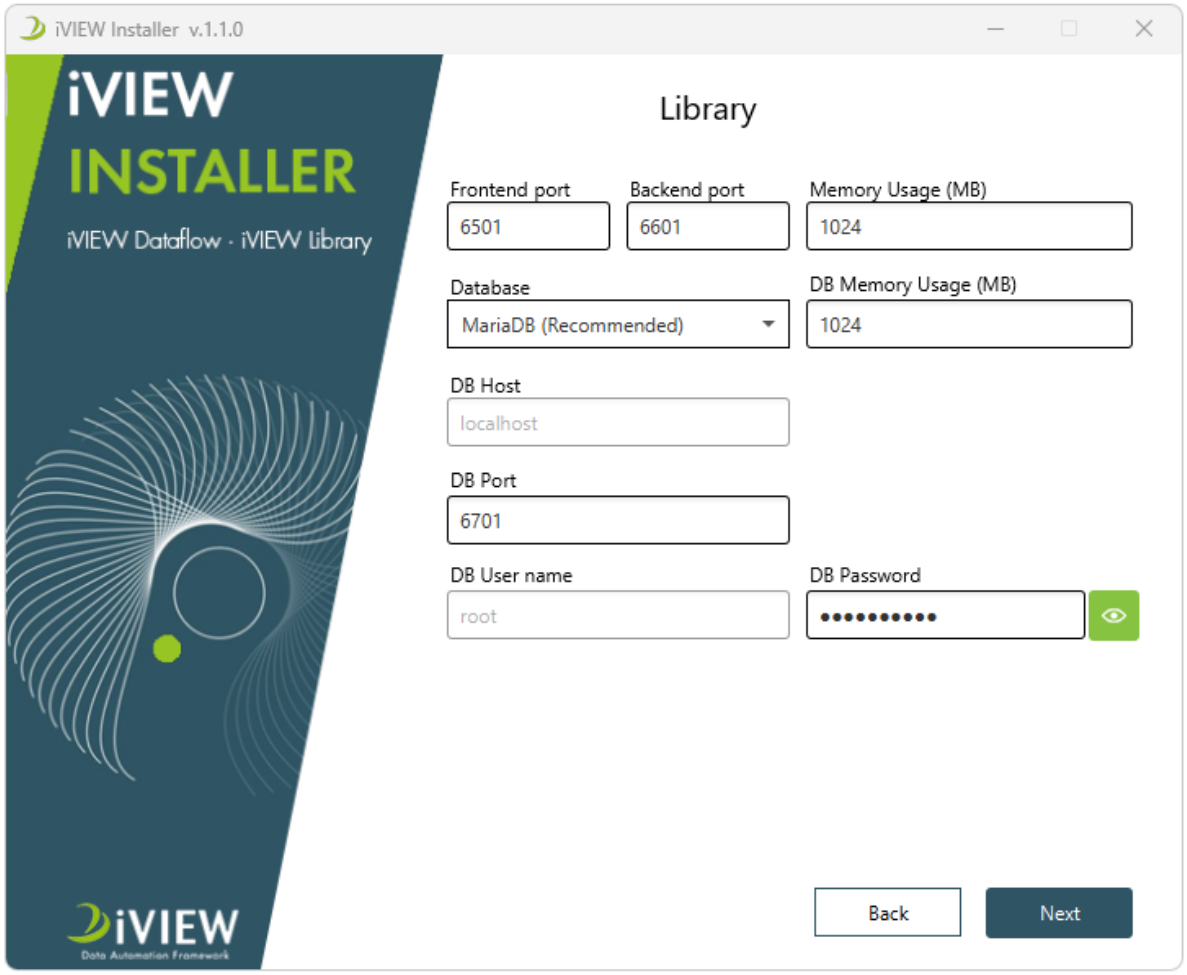

Figure 10: Step 7: Library

3.2.8 Step 8: Install

To finalize the installation, the user can click the '*Install'* button, thus copying the iVIEW Dataflow / iVIEW Library to the destination folder, together with the specified configurations. The installation might take a few minutes to complete.

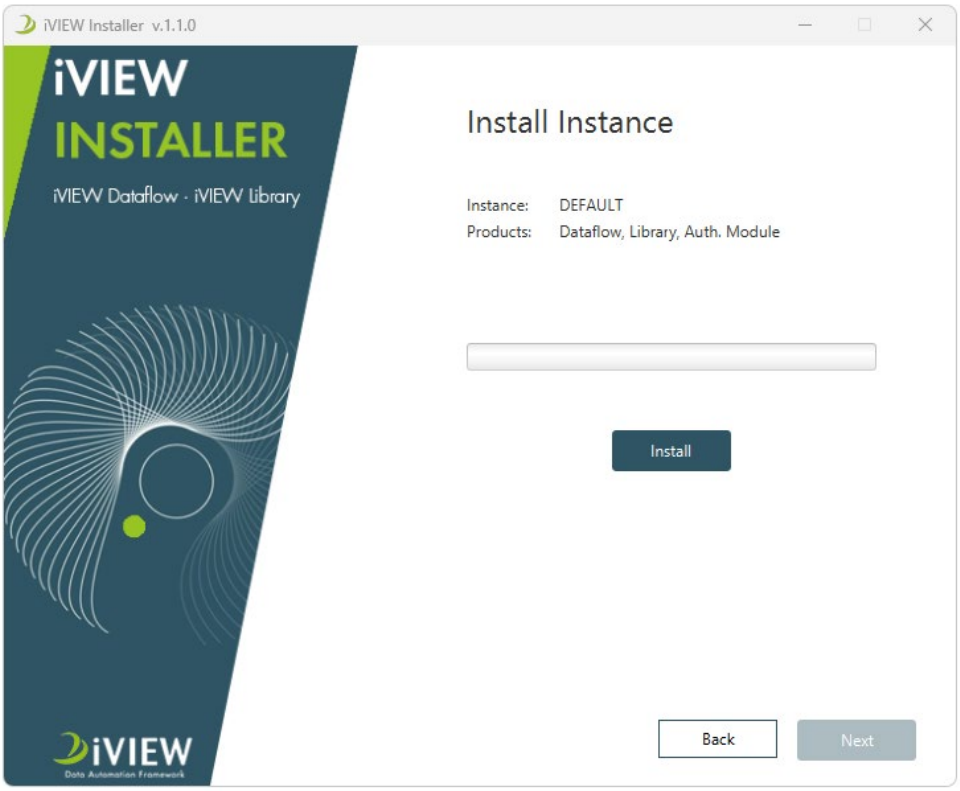

Figure 11: Step 8: Install

3.2.9 Step 9: Validation

Once the installation is complete, the iVIEW installer allows you to validate the services and the ability for the user to configure their Keycloak instance:

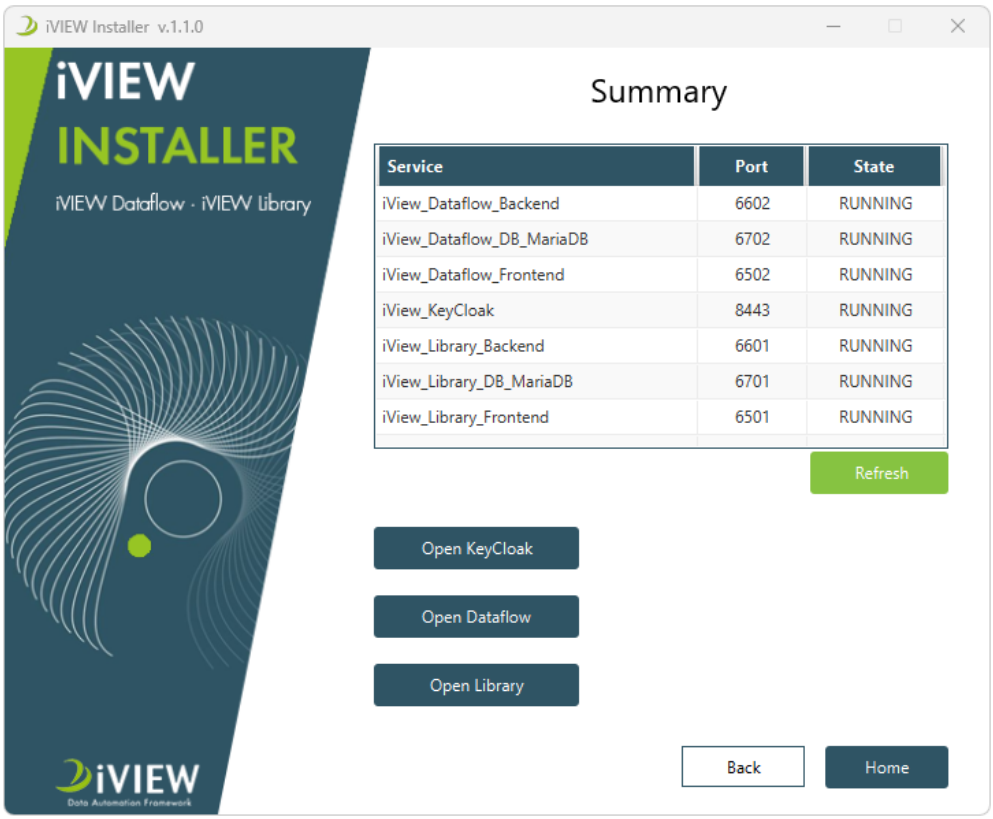

Figure 12: Step 9: Validation

If the installation was successful, the following Windows Services should be running:

Service	Description
iVIEW_Dataflow_Frontend iVIEW_Library_Frontend	Acts as a webserver and handles all direct interactions with users.
iVIEW_Dataflow_Backend iVIEW_Library_Backend	Manages application data, providing a secure REST API for frontend request.
MariaDB: iView_Dataflow_DB_MariaDB iView_Library_DB_MariaDB H2: iVIEW_Dataflow_DB iVIEW_Library_DB	MariaDB database service for application use H2 database service for application use
iVIEW_Keycloak	Identity management with authentication and authorization service for applications.

Table 10: Services

All services run under "*Local System*" – no service user needed expept iVIEW_Dataflow_Backend as local file access is required

3.3 Keycloak Configuration

3.3.1 Step 1: Access Keycloak welcome page

Access the Keycloak using the defined server on step 2 and select “Administration Console”.

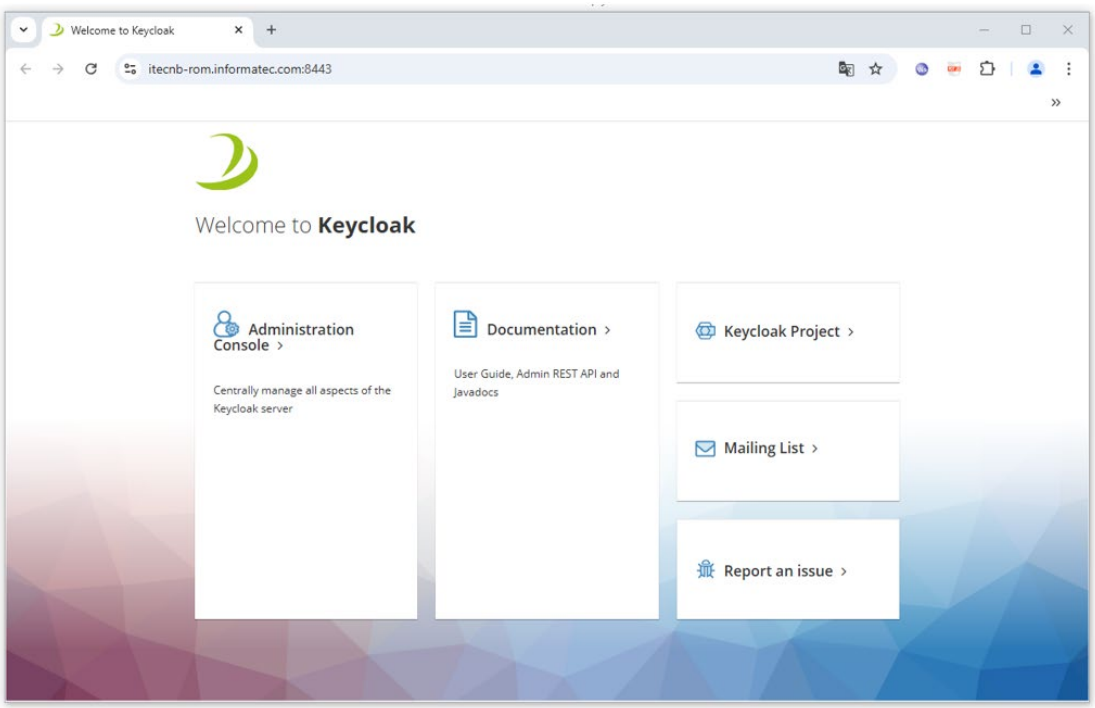

Figure 13: Step 1: Access Keycloak main board

3.3.2 Step 2: Keycloak account log in

Log in the administration console using the default account (Username: Admin, Password: 123456).

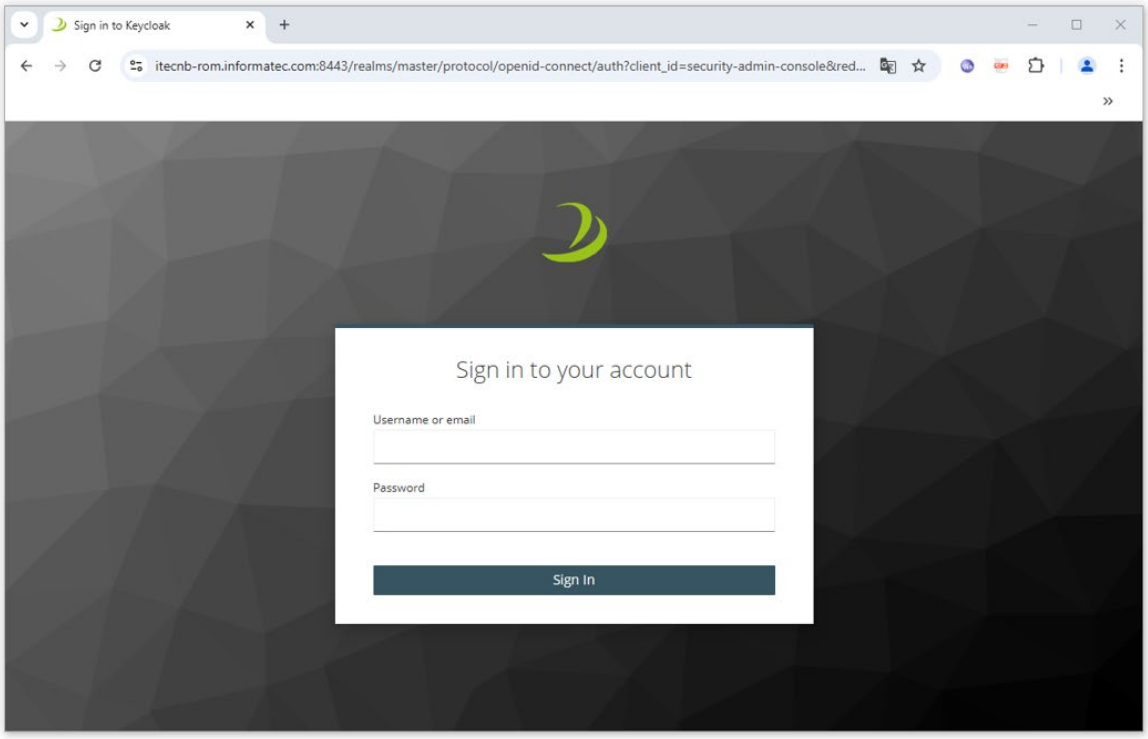

Figure 14: Step 2: Keycloak account log in

3.3.3 Step 3: Configure LDAP settings (LDAP Users).

Before assigning user roles, please make sure if LDAP is needed or not. iVIEW provides two type of user configuration. If you want to assign user roles without LDAP proceed to step 5.

1. Under the ‘’Configure’’ tab, click ‘’User federation’’.
2. Click ‘’LdapIVIEW’’.

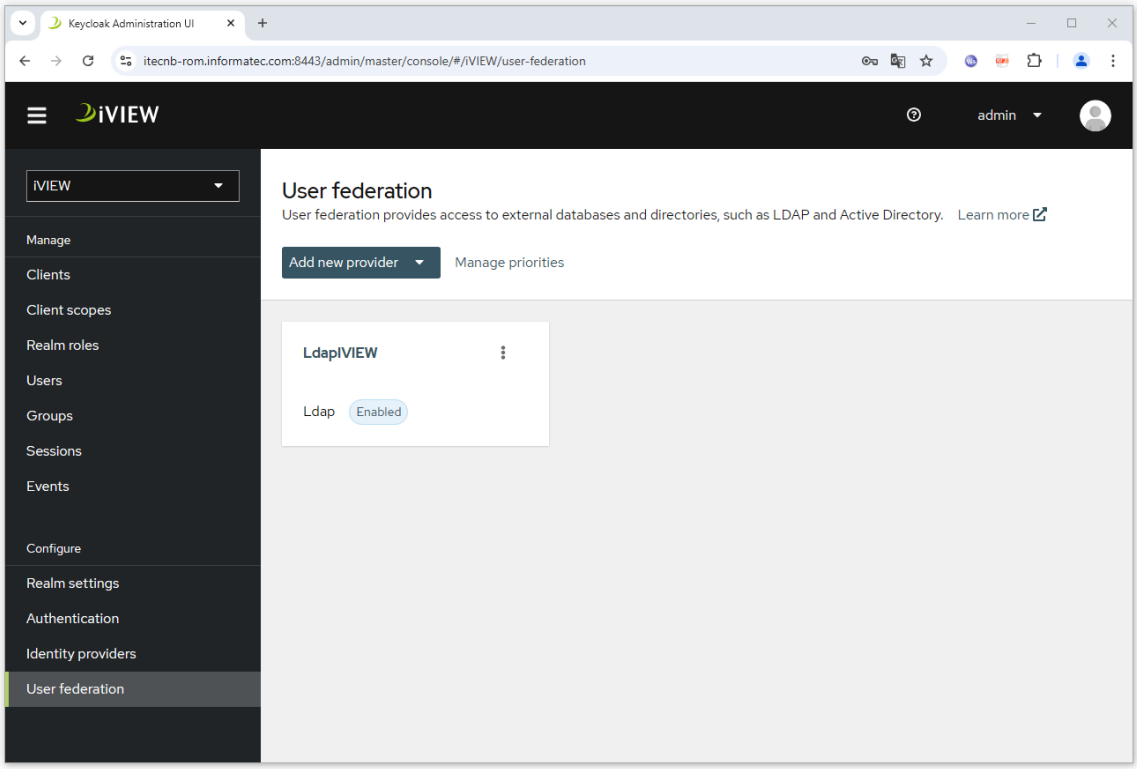

Figure 15: Step 3: Configure LDAP settings - Access User federation

3. Open the windows console and use the command “nslookup-type=srv_ldap._tcp.(my domain)” to get the LDAP connection URL.
4. For the LDAP connection URL you can use the “Address” or the “svr hostname”.

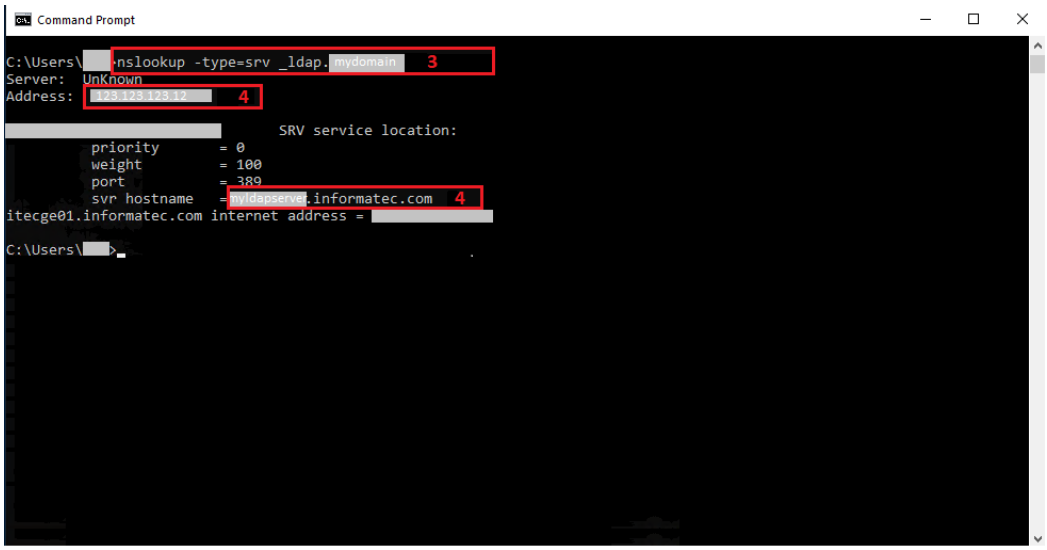

Figure 16: Step 3: Configure LDAP settings - Get LDAP Connection URL

5. Go back to the browser and paste the LDAP connection URL.
6. Insert the username for LDAP user (this user must have at least read rights).
7. Insert the password for LDAP user.

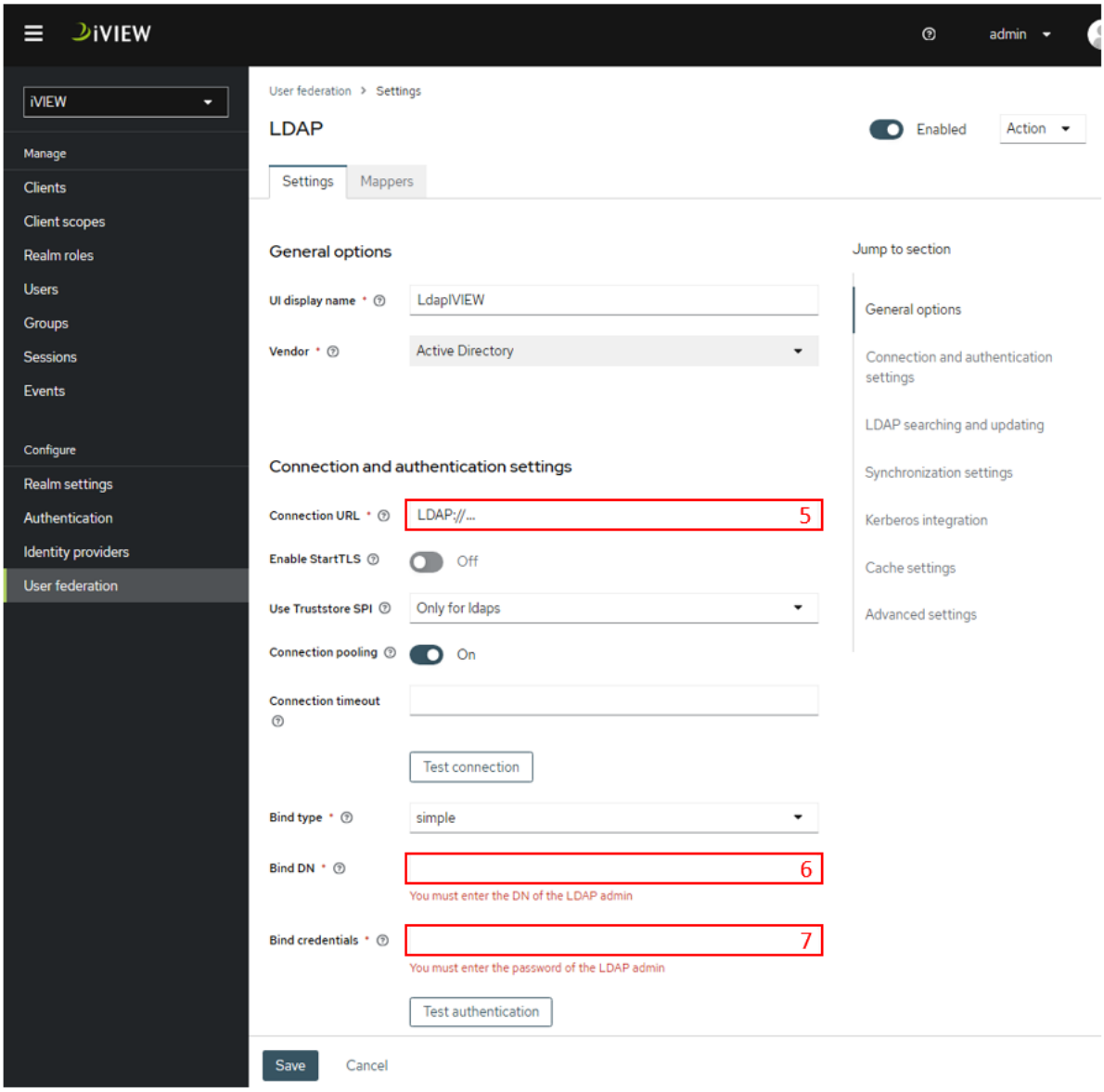

Figure 17: Step 3: Configure LDAP settings- General options

8. Select in the edit mode “READ_ONLY” to allow only read the LDAP store.
9. This DN is the parent of LDAP users. The structure will be: “ou=users,dc=example,dc=com”.

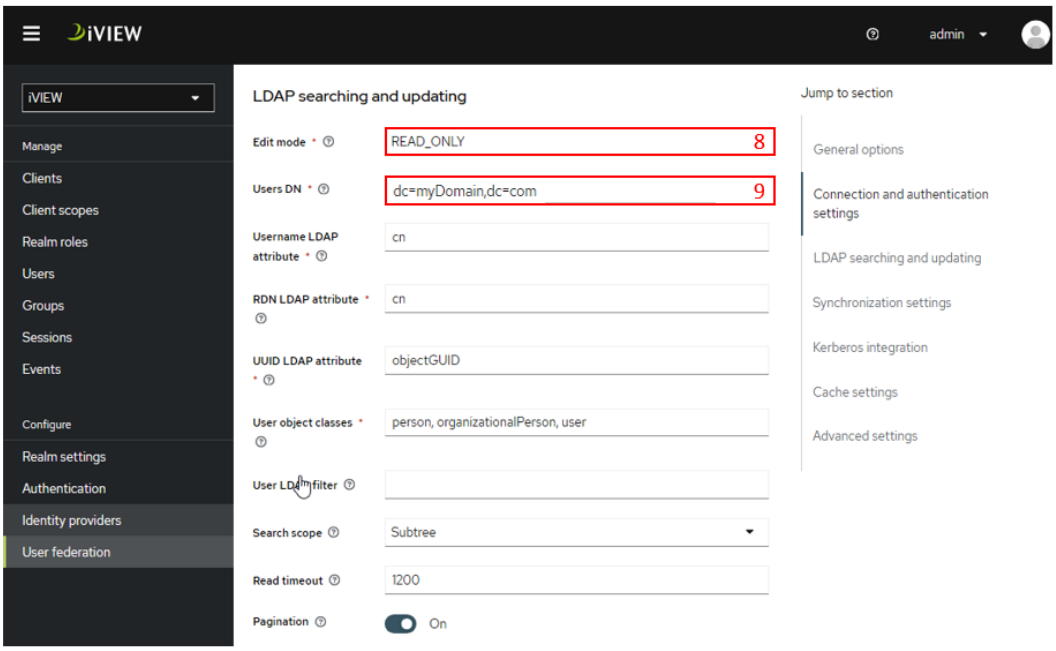

Figure 18: Step 3: Configure LDAP settings - Connection and authentication settings

10. Open windows console and use the command “gpresult /r” to get the user settings.
11. Copy the first line of the User Settings, starting on “OU=…,OU=…,DC=…,DC=…”.

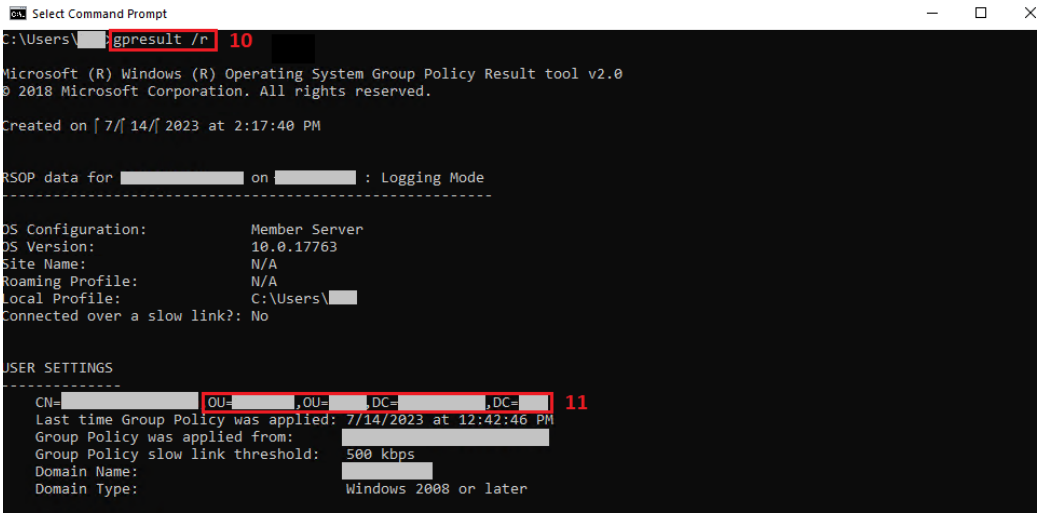

Figure 19: Step 3: Configure LDAP settings - Find Users DN

12. Return to the browser and select “Action” in the header.
13. Select “Sync all users”.

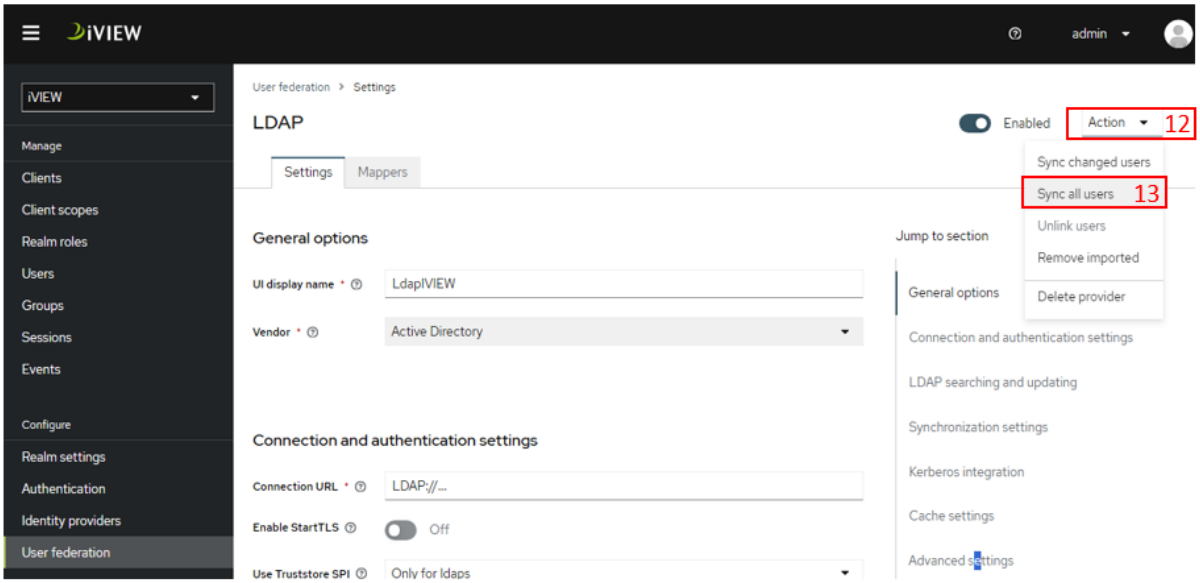

Figure 20: Step 3: Configure LDAP settings: Find Users DN

14. Select “Mappers”.
15. Select “QlikUserDomainFederation”.

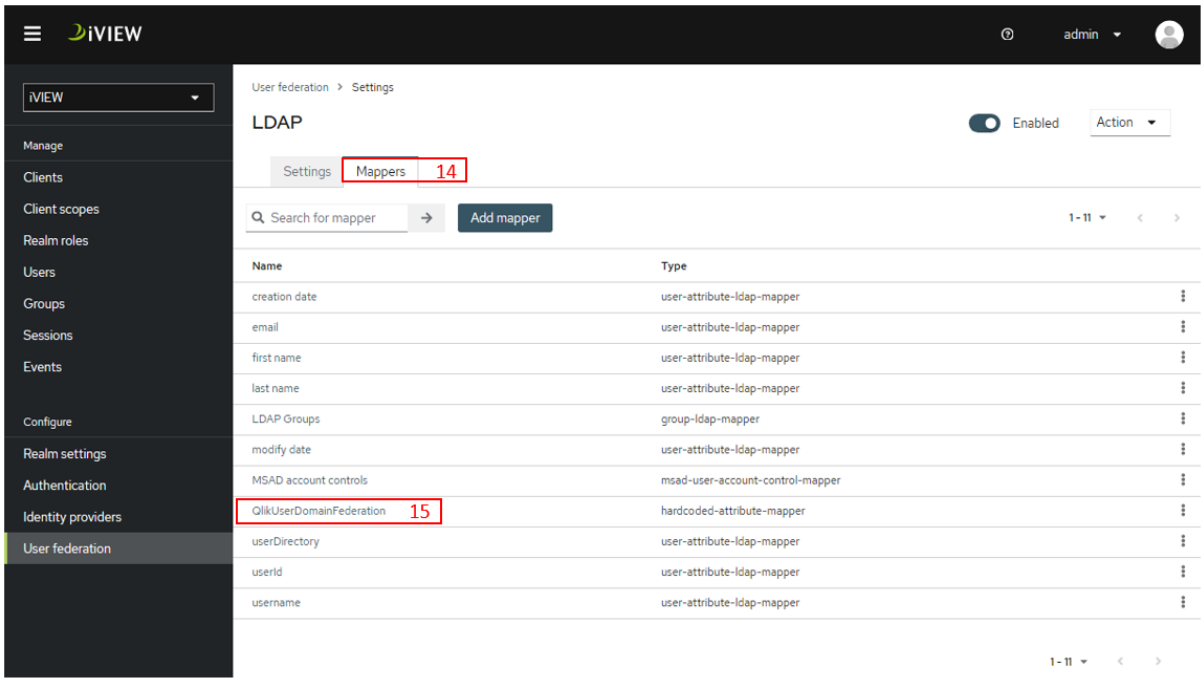

Figure 21: Step 3: Configure LDAP settings: LDAP Mapper for Qlik User Domain Federation

16. In the Qlik Sense QMC under the Users tab you may find the “User directory”, check if it matches the LDAP Userdomain.

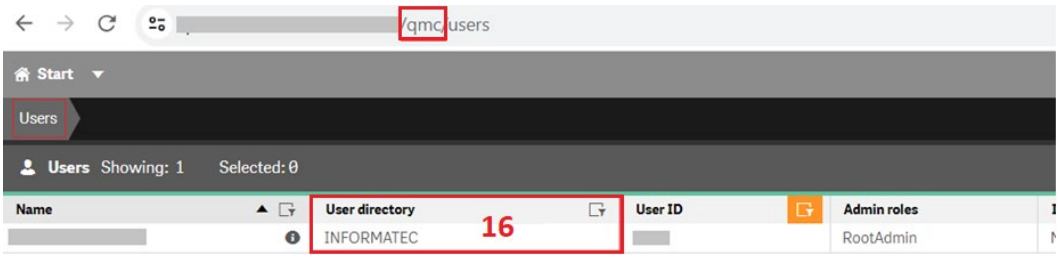

Figure 22: Step 3: Configure LDAP settings: User directory in Qlik Sense

17. Please enter the “User Directory” which is set in the QMC in this case “INFORMATEC”, check in the previous step.

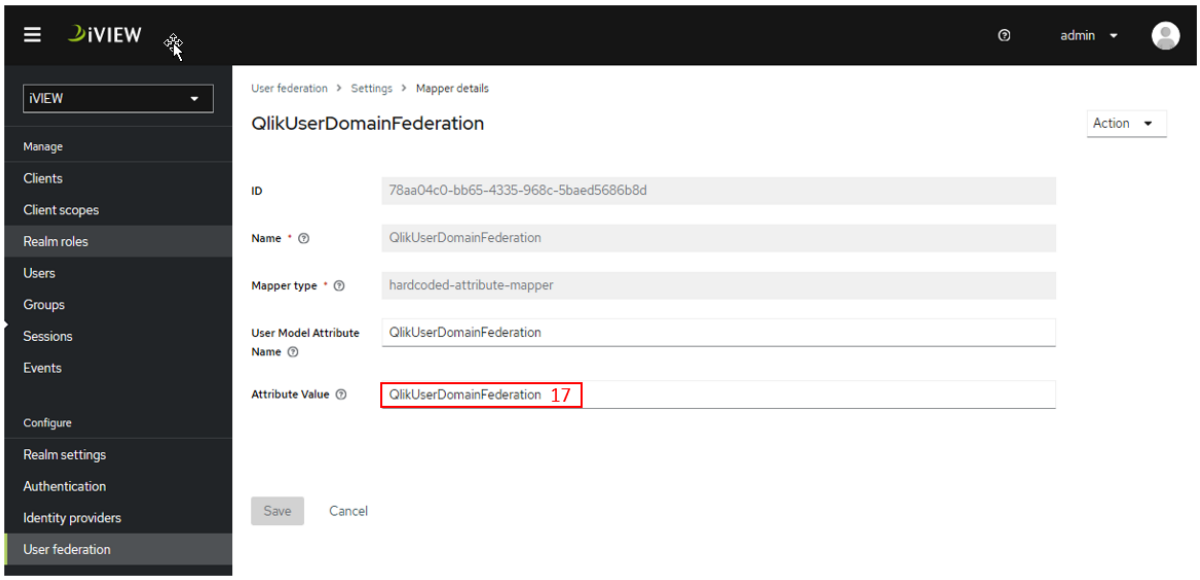

Figure 23: Step 3: Configure LDAP settings: QlikUserDomainFederation

3.3.4 Step 4: Assign user roles without LDAP

1. Before assigning roles to users without LDAP, make sure LDAP is disabled.

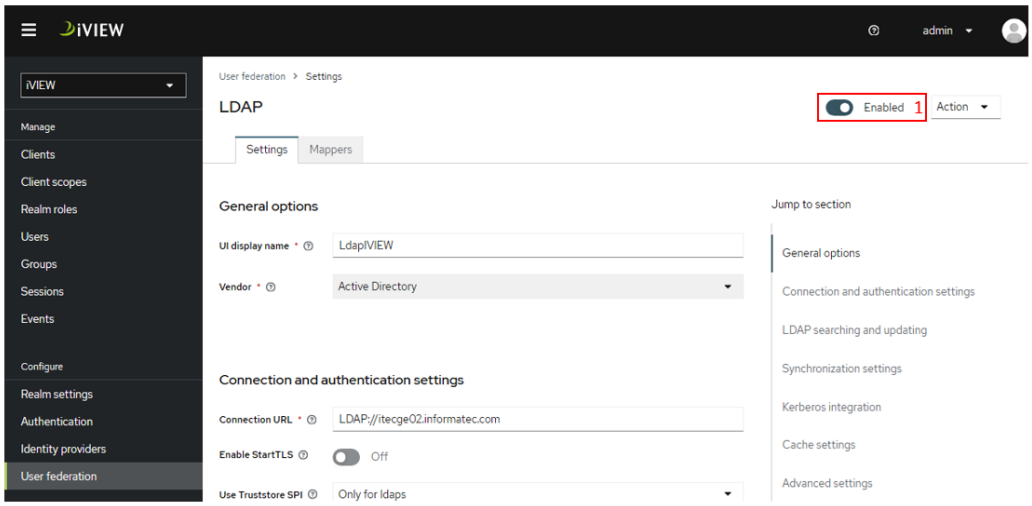

Figure 24: Step 4: Assign user roles without LDAP: Disable LDAP

2. Under the “Manage” tab, select “Users”.
3. Select “Add user”

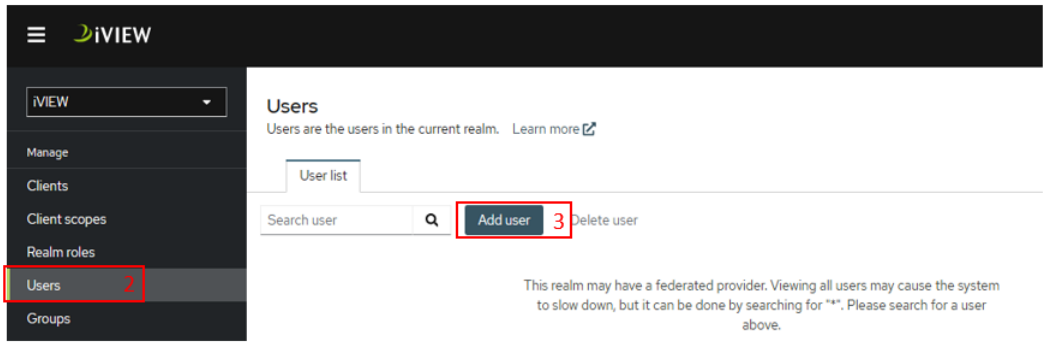

Figure 25: Step 4: Assign user roles without LDAP: Add User

4. Add a username and click on the “Create” button.

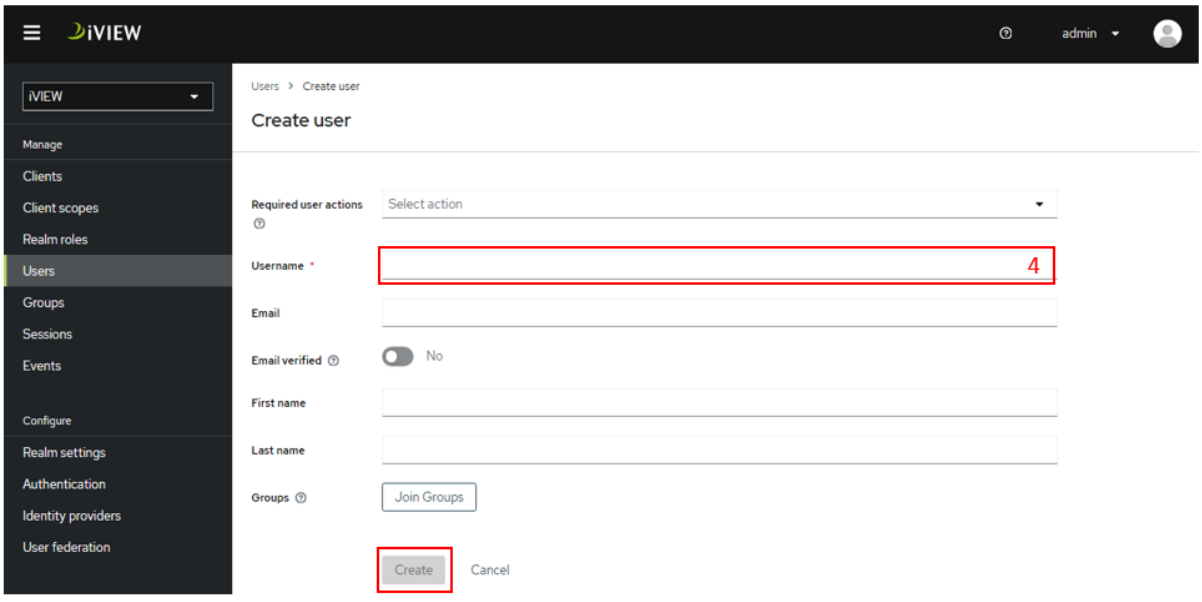

Figure 26: Step 4: Assign user roles without LDAP: Define Username

5. Click in “users” under the “manage” tab.
6. Select “Role mapping”.
7. Click “Assign Role”.

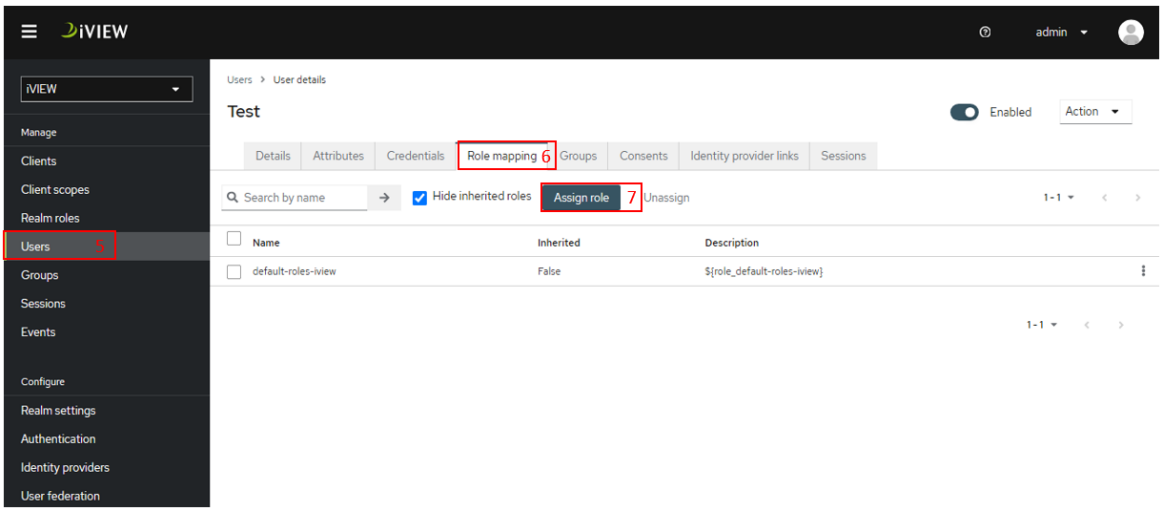

Figure 27: Step 4: Assign user roles without LDAP: Assign Role

8. Select “Global”.
9. Click “Assign”.

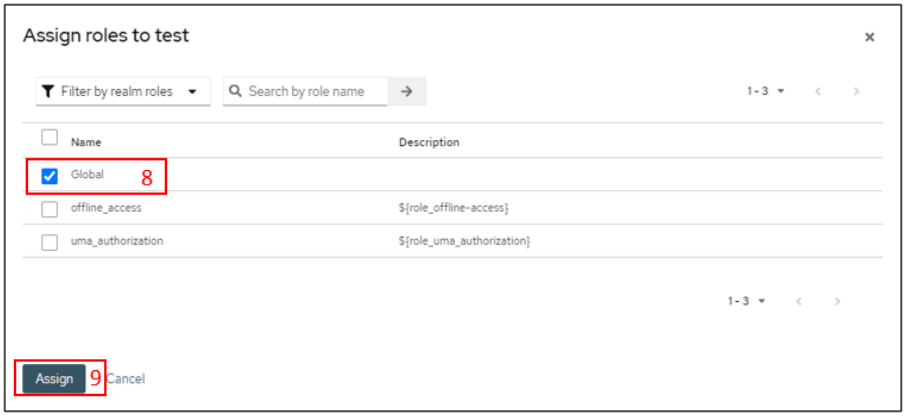

Figure 28: Step 4: Assign user roles without LDAP: Assign Roles to User

10. Filter by clients.
11. Show pages 1-20.
12. Check Dataflow-Admin
13. Check Dataflow-Superadmin
14. Check Library-Admin
15. Click on “Assign”

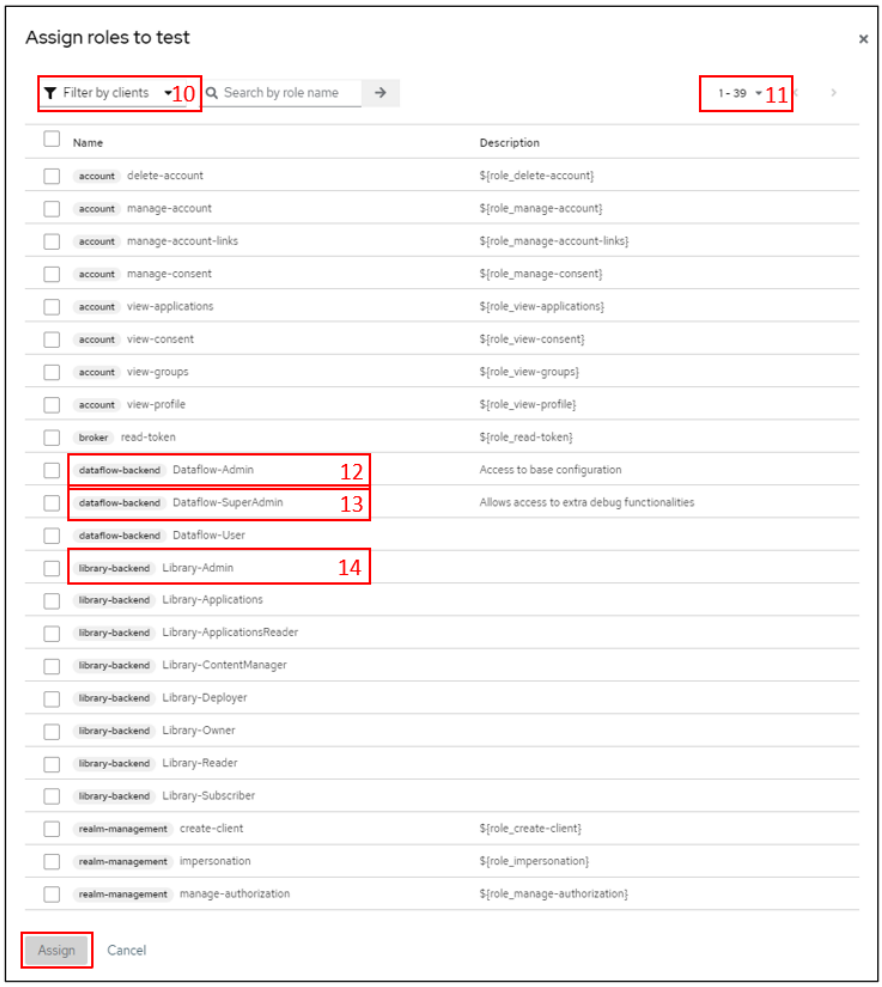

Figure 29: Step 4: Assign user roles without LDAP: Assign Roles to User

16. Select the “Attributes” tab.
17. Select “Add an attribute”

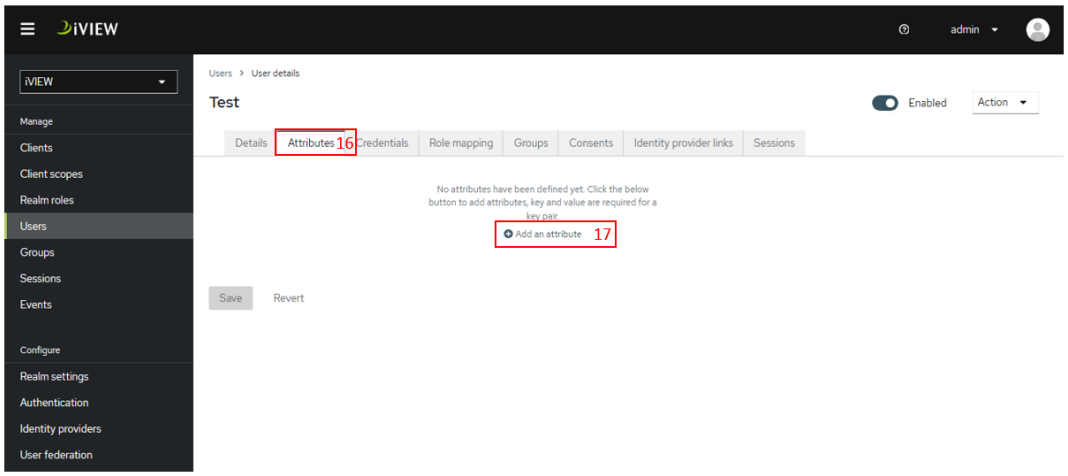

Figure 30: Step 4: Assign user roles without LDAP: Add an attribute

18. Fill “Key” as “userId” (cased sensitive)
19. Fill “Value” as your windows login name.

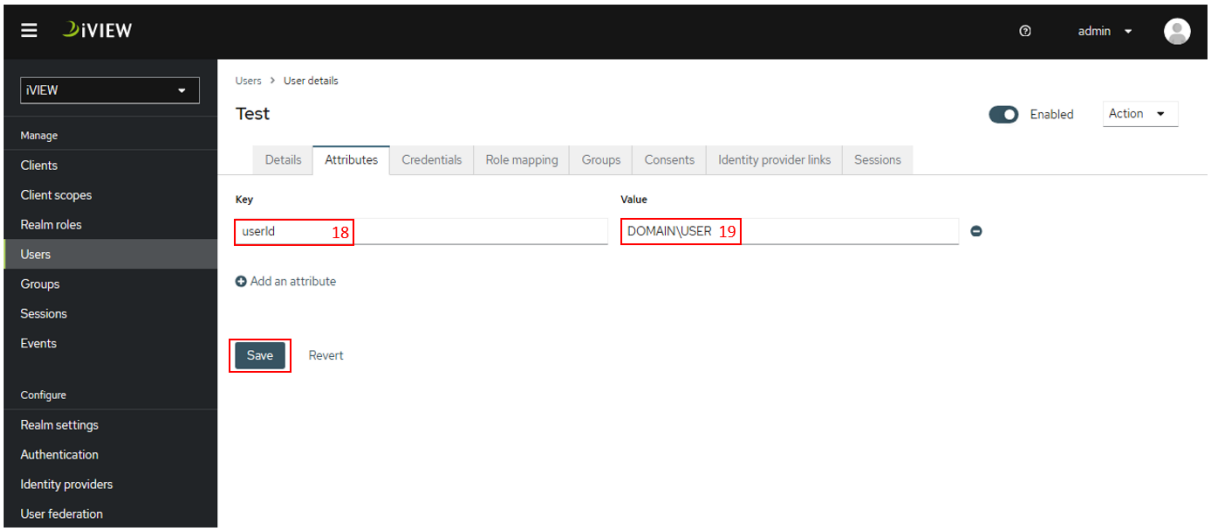

Figure 31: Step 4: Assign user roles without LDAP: Defining attributes

20. Go to the tab “Credentials”.
21. Click the “Set password”.

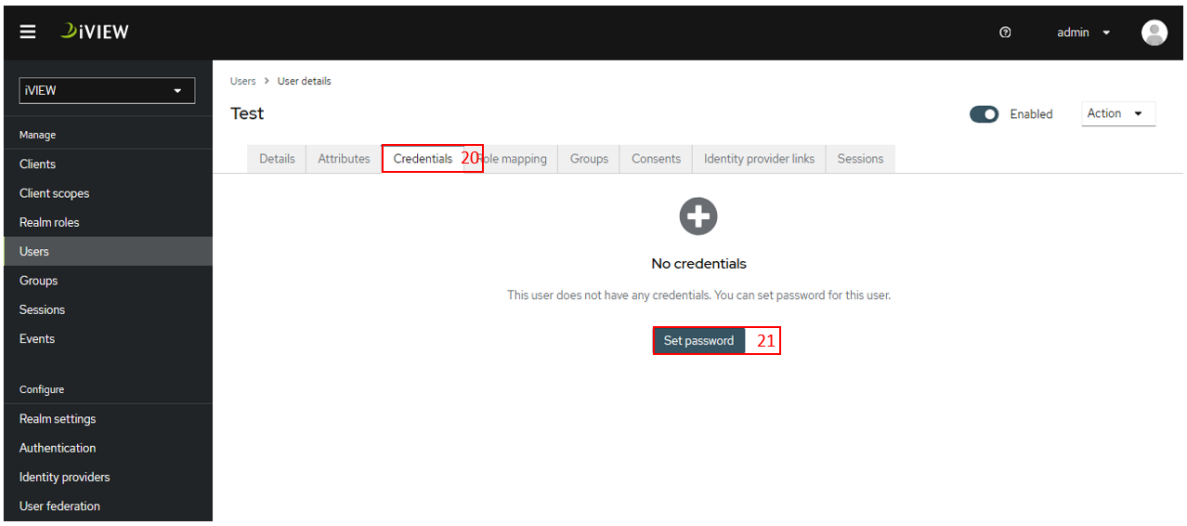

Figure 32: Step 4: Assign user roles without LDAP: Credentials

22. Set your password.
23. Confirm your password.
24. The administrator will set a temporary password (set temporary to on) and once the final user logs in, he will define the permanent password.

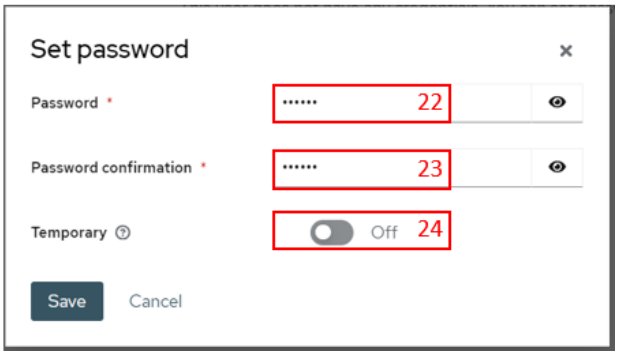

Figure 33: Assign user roles without LDAP: Set passw

3.3.5 Step 5: Prepare Qlik Sense Certificates for iVIEW

1. On the server open the iVIEW folder and create a new folder called Certificate.
2. Create a subfolder with the name of the Qlik Sense server to export the certification to the iVIEW folder.

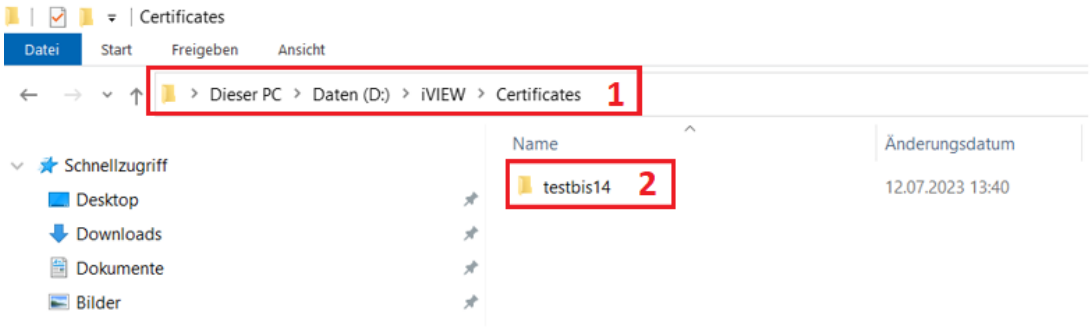

Figure 34: Step 5: Assign user roles without LDAP: Subfolder of Qlik Sense server

3. In the Qlik Sense QMC select the Certificates tab, click in “Add machine name”.
4. Type in the Qlik Sense server name.
5. Add a certificate password.
6. Retype the password.
7. Check “Include secret key”.
8. Click in “Export file format for certificates” and select the option “Platform independent PEM-format”. You will be able to see the path where you exported the Qlik Sense certificates.

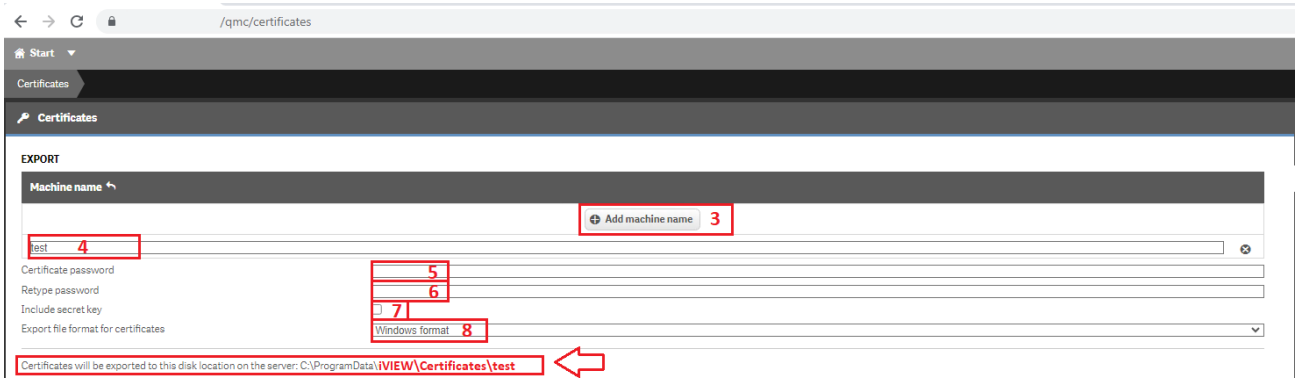

Figure 35: Step 5: Assign user roles without LDAP: Set up Qlik certificate in QMC

4 Post-installation

After the installation and its validation, the user needs to follow up with some actions described in the sections of this chapter.

4.1 Export Qlik Sense certificates

It is necessary to export the Qlik Sense certificates. To do so, the user must observe the following steps:

1. In the QMC, under Certificates:
   i. Add a machine name (set the name of the server)
   ii. Ensure the <include key> option is checked
   iii. Select "*Platform Independent PEM-format*".
   iv. Click "*Export Certificates*".

The generated files can be found here:

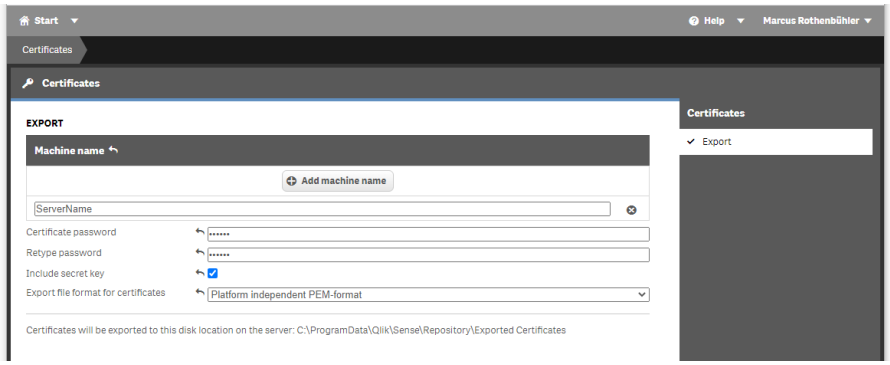

Figure 36: Post Installation: Export QMC Certificates

2. Copy the exported certificates from the default folder on the Qlik Sense server *C:\ProgramData\Qlik\Sense\Repository\Exported Certificates* to *<root-install-folder>*.

4.1.1 Administration console

Here the first step is to open the Keycloak's administration console at https://<server>:<keycloak port>/auth.

Use the server from step 3.2.2 and the port of 3.2.3.

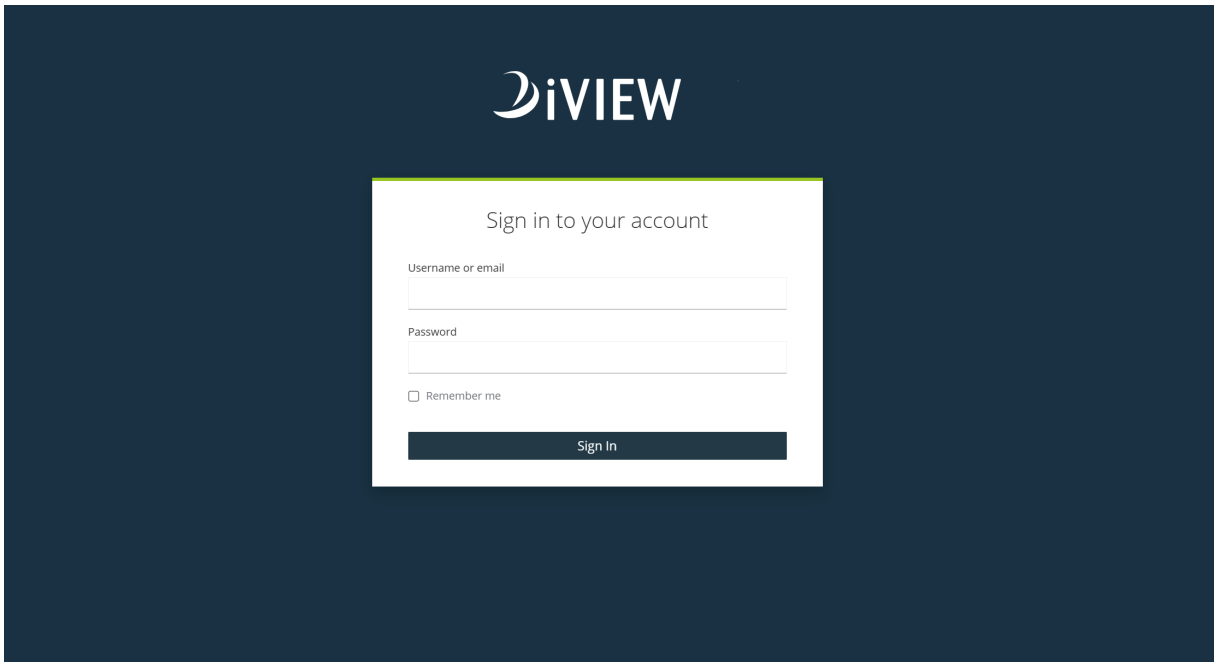

Figure 37: Post Installation: Sign in page

Here the user can sign in with the credentials of username “admin” and initial password “123456”.

> It is recommended that the user later change the initial password.

The following default page might appear:

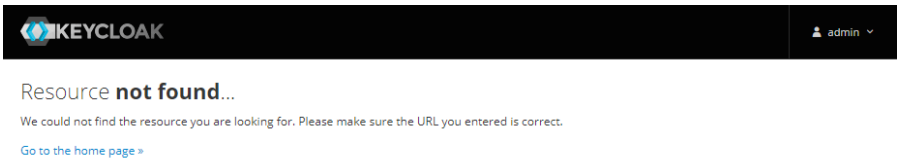

Figure 38: Post Installation: Keycloak Administration console redirection

The user should click on “*Go to the home page”* to proceed.

4.1.2 Configuration of User Federation

User Storage Federation

Most companies use a standard user directory or LDAP to hold information about users and their passwords or other credentials. Keycloak can federate existing external user databases. By default, Keycloak supports LDAP and Active Directory. Alternatively Keycloak supports also common Identity Providers, using SAML or OpenID protocols.

The way it works is that when a user logs in, Keycloak will look into its own internal user store to find the user. If it cannot find it there, it will iterate over every User Storage provider you have configured, until it finds a match. Data from the external store is mapped into a common user model that is consumed by the Keycloak runtime. This common user model can then be mapped to OIDC token claims and SAML assertion attributes.

External user databases rarely have every piece of data needed to support all the features that Keycloak has. Therefore, the User Storage Provider can opt to store some things locally in the Keycloak user store. Some providers even import the user locally and sync periodically with the external store. This approach depends on the capabilities of the provider and how it is configured. For example, the user's external user store may not support OTP. Depending on the provider, this OTP can be handled and stored by Keycloak.

More at https://www.keycloak.org/docs/latest/server_admin/#_ldap.

Even though a bare Keycloak instance comes configured, most configurations are dependent on the specific environment. By default, a pre-configured user federation provider (for LDAP) is already defined. A few of its configurations are merely placeholders that must be set for the specific environment, while others can be adjusted from their default value, if need be.

In case the user federation/provider is drastically different than default, one can start creating it from scratch. As such, the following steps illustrate the required changes the user must implement.

4.1.2.1 Step 1: Configure LDAP to get users

The user needs to configure a new User Federation to synchronize users and groups from an LDAP server:

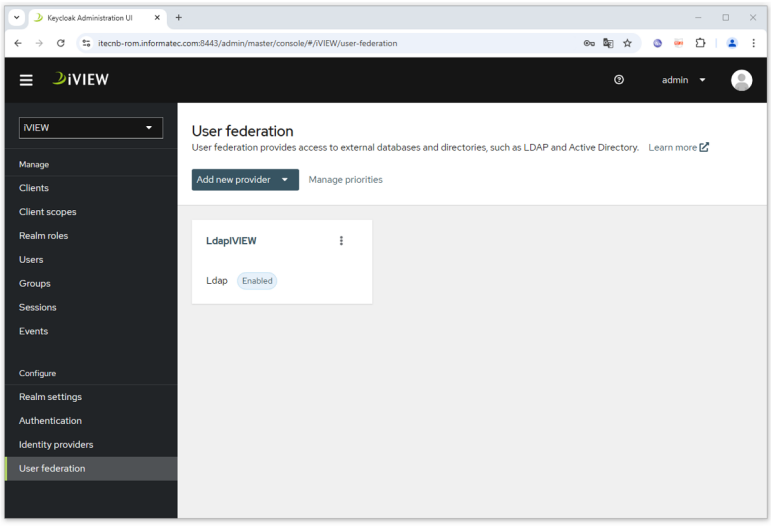

Figure 39: Post Installation : Keycloak User Federation – Configure LDAP to get users

4.1.3 Step 2: Required settings

Following having specified a provider, the user must also complete the Ldap iVIEW section:

1. Define the LDAP path / User DN path
2. LDAP-User to access LDAP - *Recommended: Service-User*

Test the connection and authentication – this should be successful and then successfully synchronize all users and save.

Saving and synchronizing all users

To finish configuring the *User Federation*, all that is left is for the user to click the "*Save*" button, followed by the "*Synchronize all users*" button.

If all steps were followed and the settings were properly configured, a success message should pop-up letting the user now that the sync of users finished successfully.

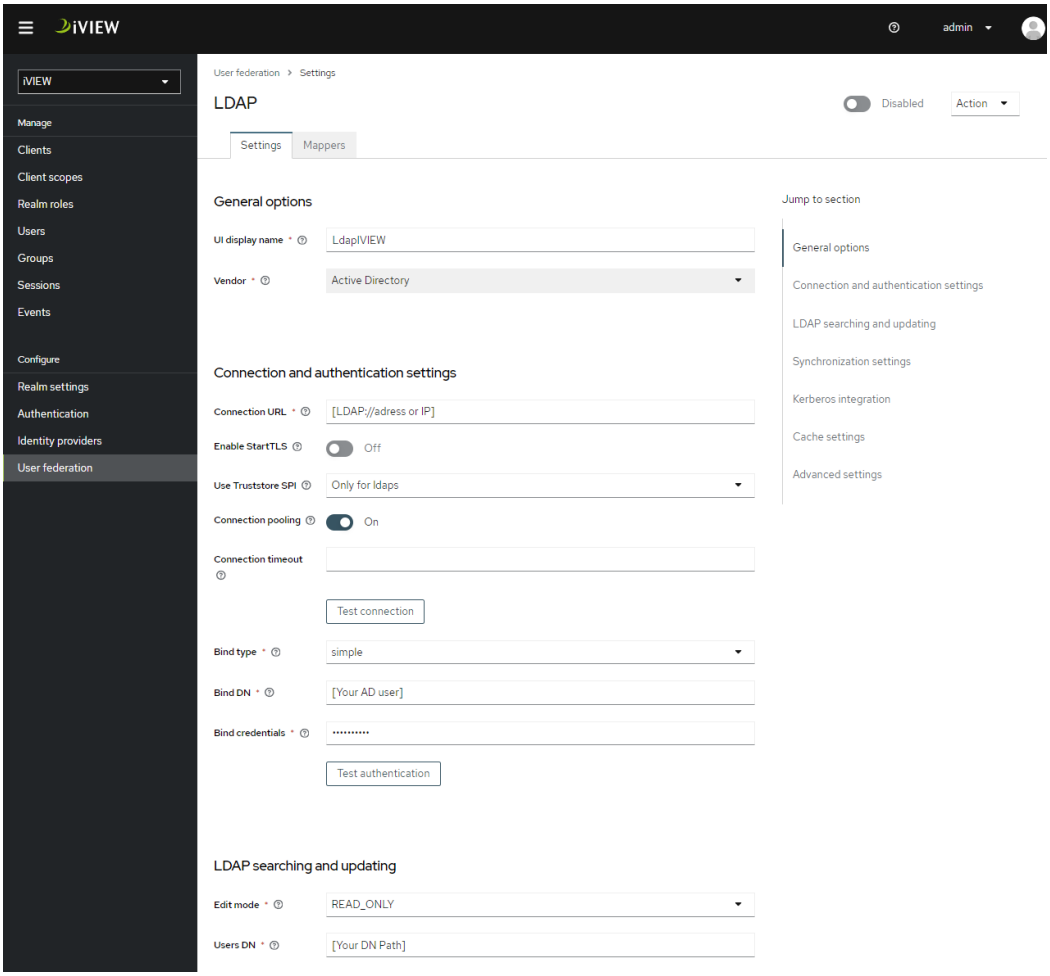

Figure 40: Post Installation: Keycloak User Federation – LdapiVIEW

For LDAP "*Active Directory*" refer to https://www.keycloak.org/docs/latest/server_admin/#_ldap.

If the user uses LDAPS for a secure connection to his LDAP, the SSL certificate needs to be imported into Keycloak's truststore.

For more information, please refer to:

https://www.keycloak.org/docs/latest/server_admin/#connect-to-ldap-over-ssl.

4.1.3.1 Step 4: Defining a Role

In the Library front-end, the admin can grant user access by defining a role. You can view all users and select one from the User list.

Under Client roles: select «Library Backend» and define user roles i.e., admin, deployer etc.

Aside from enabling secured content sections with the realm roles ("Galaxies"), the iVIEW Library also allows for functionality partitioning between users. It does so by giving permissions to users according to the roles they are assigned to their functions (*please refer to the "Feature Guide" – Section 9 named* ***Functionality Roles*** *pg. 22).*

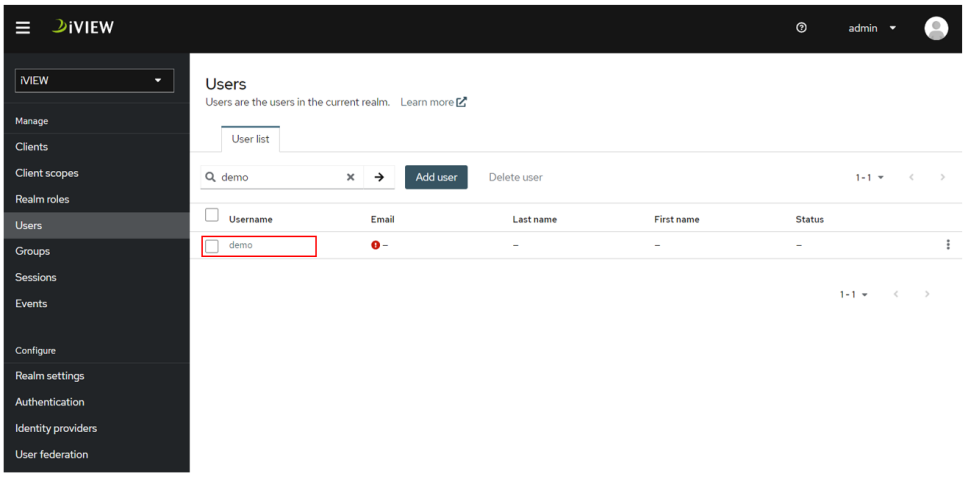

Figure 41: Post Installation: Keycloak Users

Assign Global

1. Select Role mapping
2. Assign role

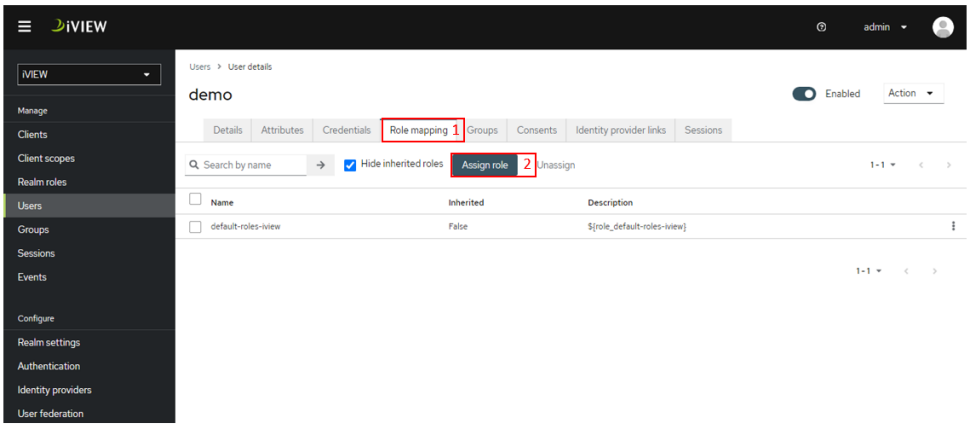

Figure 42: Post Installation: Keycloak Role Mapping

3. To assign “Global” the filter must be set to “Filter by realm roles”
4. Select Global
5. Assing the selection

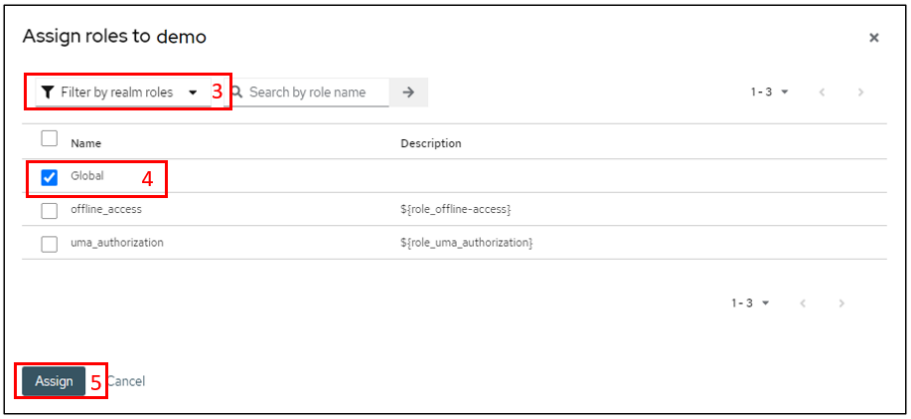

Figure 43: Post Installation: Keycloak Assign Content Role "Global"

Assign Access for iVIEW Dataflow and/or iVIEW Dataflow

1. Select Role mapping
2. Assign roles
3. To assign rules for iVIEW Dataflow or iVIEW Library the filte must be set to “Filter by clients”
4. If too less rules are visible, it is possible to increase the amount visible records over this dropdown
5. Example: Select “Dataflow-Admin” if user has admin permissions for iVIEW Dataflow
6. Example: Select “Library-Admin” if user has admin permissions for iVIEW Library
7. After selection the specific permissions the rules needed to be assigned

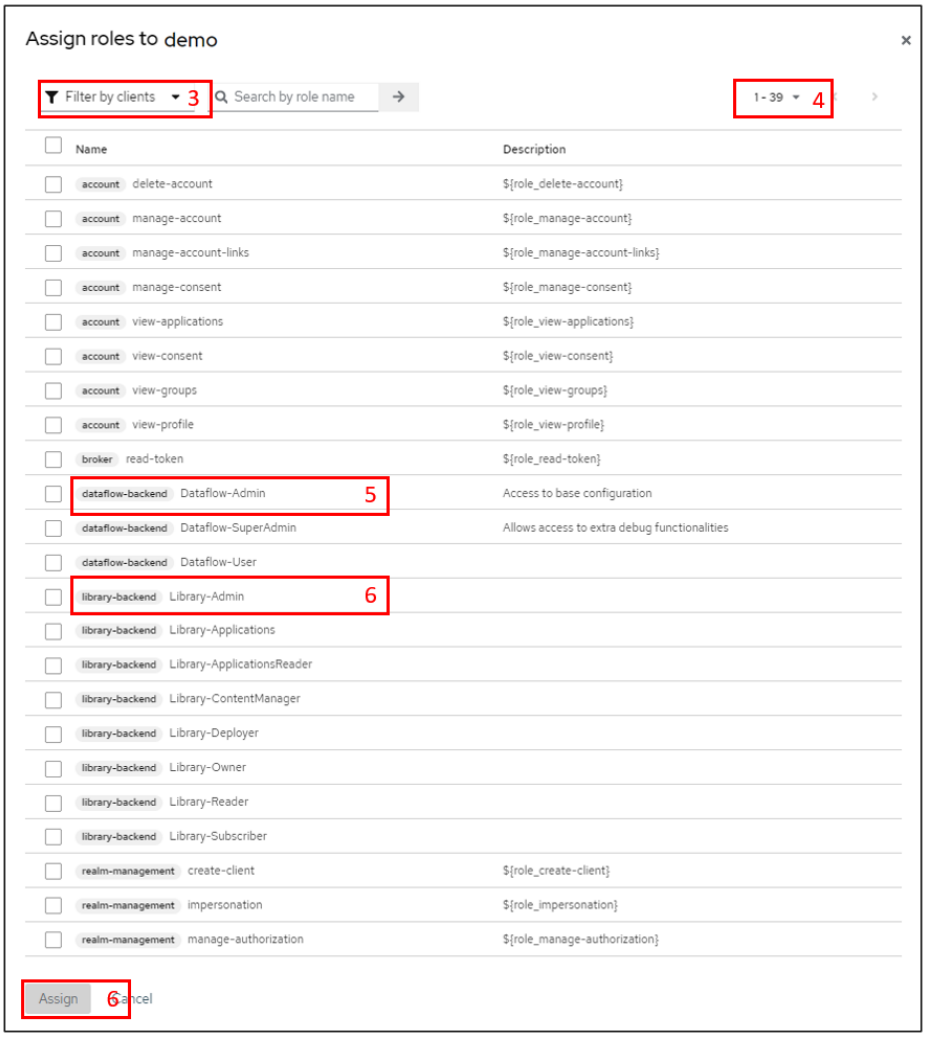

Figure 44: Post Installation: Keycloak Assign Admin Roles

⚠ **As an admin the role "Library-Admin" is required to be able to initialize iVIEW Library: entering the license and creating a connection to a Qlik Sense Server.**

⚠ **Do not delete or change the role name of any library-backend roles as this will remove functionality from the iVIEW Library and ultimately prevent interaction with the tool.**

Realm Roles
Realm-level roles are a global namespace to define your roles.

More at https://www.keycloak.org/docs/latest/server_admin/#realm-roles.

4.2 Initializing the iVIEW Dataflow or iVIEW Library

Having met all previous post-installation requirements, the user is now ready to make the final necessary configurations from inside the iVIEW Library. To do so he must follow the subsequent steps:

4.2.1 Step 1: Sign in

To access the iVIEW Dataflow the user should use the URL https://<iview-url>:6502/dataflow.
To access the iVIEW Library the user should use the URL https://<iview-url>:6501/library.

Once there, the user can enter his windows credentials, according to the configured Identity Provider:

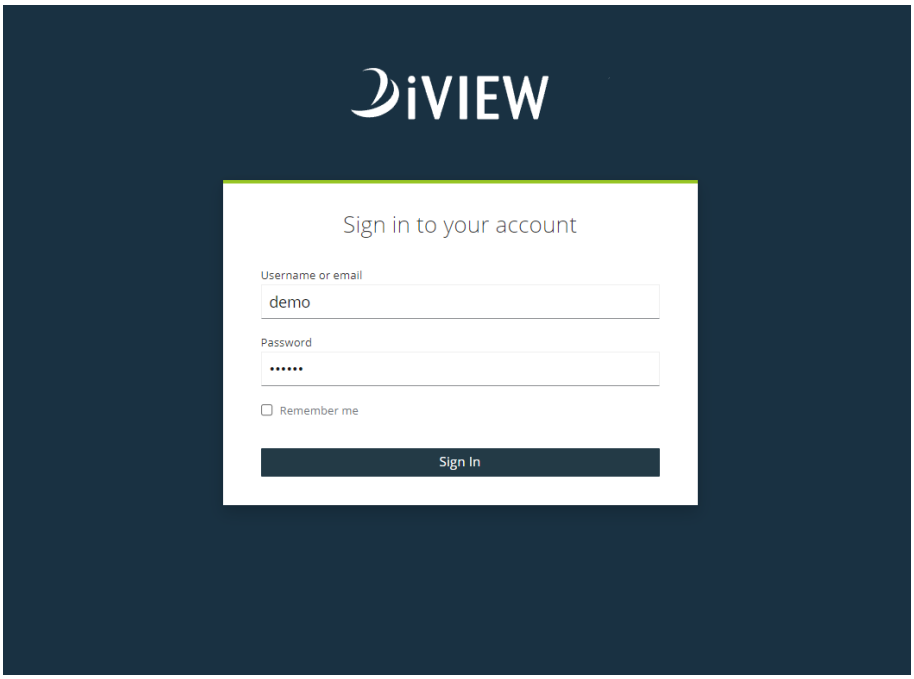

Figure 45: Initializing the iVIEW Library: Sign in prompt

> The username and email are configured in the identity provider, meaning that this field's input needs to match the ones specified there.

If the sign in is successful, the user is redirected to the main page where his username is displayed on the top right of the navigation menu.

4.2.2 Step 2: Upload license file

Once signed in, the user can click on the configurations' icon in the navigation menu. This opens the *Configurations* dialog inside the *License* tab:

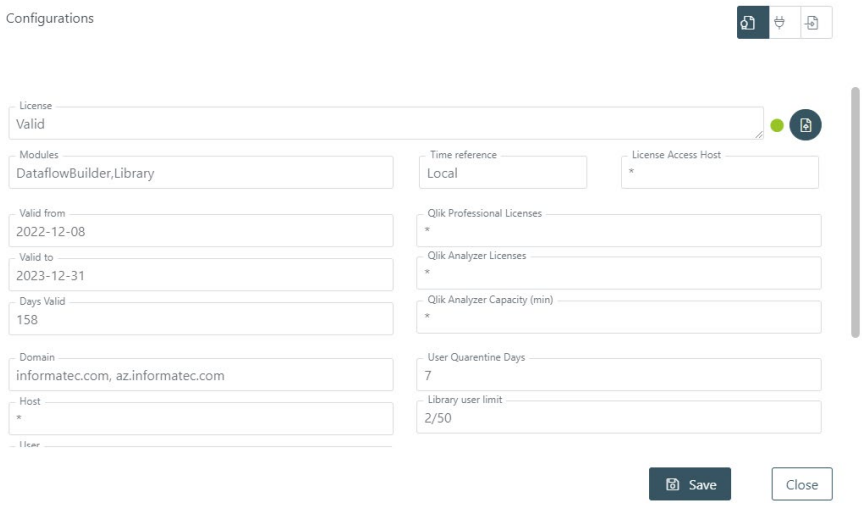

Figure 46: Activating the iVIEW Dataflow / iVIEW Library: License Tab

To unlock all functionalities, a license must be then uploaded. To upload license the user must click the button.

> The license is part of the installation package provided by Informatec.

4.2.3 Step 3: Create lead server connection 1

The final step of the configuration of iVIEW Library takes place from inside the *Configurations* dialog. More specifically, from within the dialog's *Connections* tab:

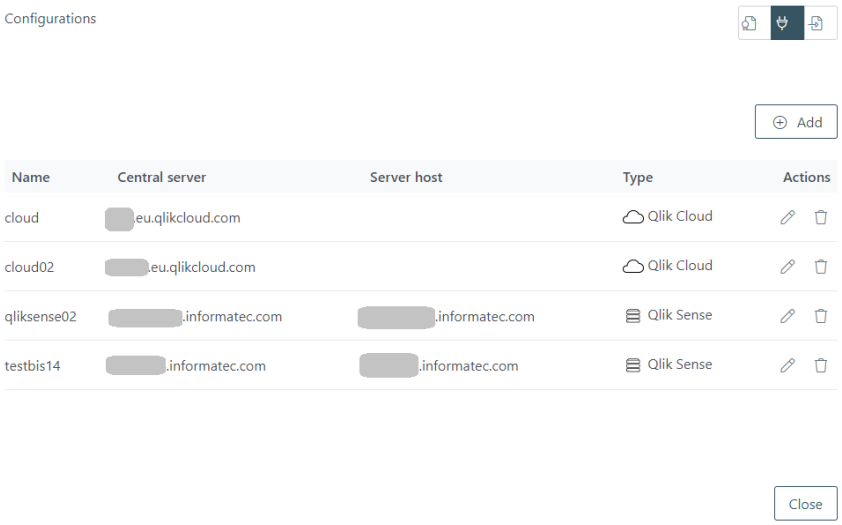

Figure 47: Initializing the iVIEW Library: Connections tab

Here the user can create a new connection by clicking the create icon and editing the available fields displayed in the figure above such as: server name, server URL, central node URL.

To include the certificate folder path the user must field the input field and click the create KeyStore button .

It is also possible to test the new connection by clicking the refresh button .

Finally, the user should click on the save button to create this new connection.

5 Operations and maintenance

This chapter covers services, port mapping, software upgrade and how to uninstall the iVIEW Library.

5.1 Services

Service	Description
iVIEW_Dataflow_Frontend	Acts as a webserver and handles all direct interactions with users.
iVIEW_Library_Frontend	Acts as a webserver and handles all direct interactions with users.
iVIEW_Dataflow_Backend	Manages application data, providing a secure REST API for frontend request.
iVIEW_Library_Backend	Manages application data, providing a secure REST API for frontend request.
iVIEW_Dataflow_DB_MariaDB iVIEW_Dataflow_DB (H2)	Database service for application use (embedded by default).
iVIEW_Dataflow_DB_MariaDB iVIEW_Library_DB (H2)	Database service for application use (embedded by default).
iVIEW_Keycloak	Identity Management with authentication and authorization service for apps.

Table 8: Services

5.2 Port mapping

Service	Port
Frontend Library	6501 (default)
Frontend Dataflow	6502 (default)
Backend Library	6601 (default)
Backend Dataflow	6602 (default)
Database Library (Web Console)	6801 (default, localhost only)
Database Dataflow (Web Console)	6802 (default, localhost only)
Database (TCP)	6701 (default, localhost only)
Database (TCP)	6702 (default, localhost only)
Keycloak Console	8443 (default)

Table 9: Port mapping

⚠ **If a firewall exists between frontend and backend and/or database, please ensure that the above--mentioned ports are open.**

5.3 Software upgrade

To upgrade the iVIEW Dataflow and/or iVIEW Library, the user should run the iVIEW-installer. This process is similar to when the iVIEW Dataflow and/or iVIEW Library was installed for the first time. By Choosing “Update” the installer will try to detect the currently installed instances in the specified installation folder.

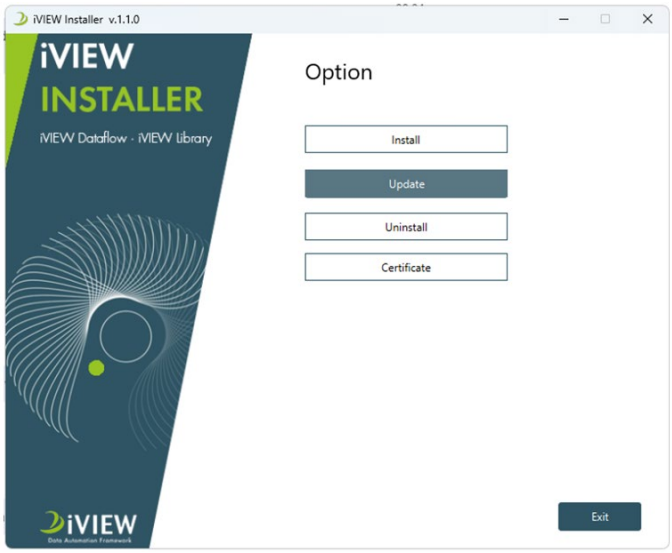

Figure 48: Software upgrade: Step Welcome

Select the module(s) to update and proceed the process (“Next”)

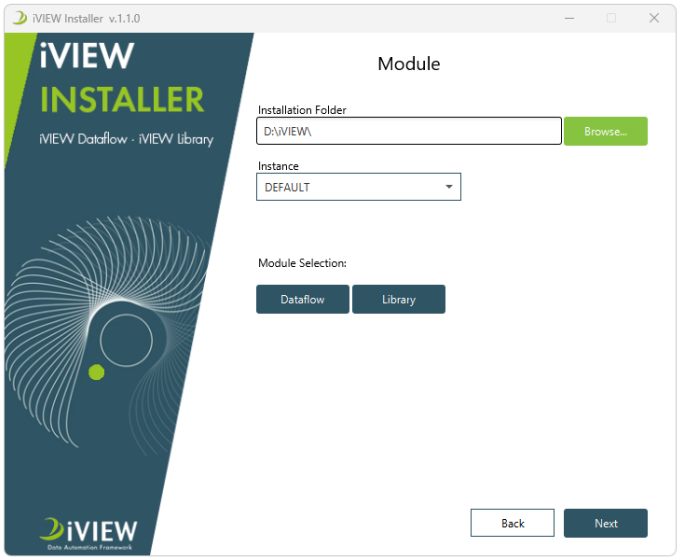

Figure 49: Software upgrade: Step Welcome

The user should click *“Next”* until the user reaches the update step:

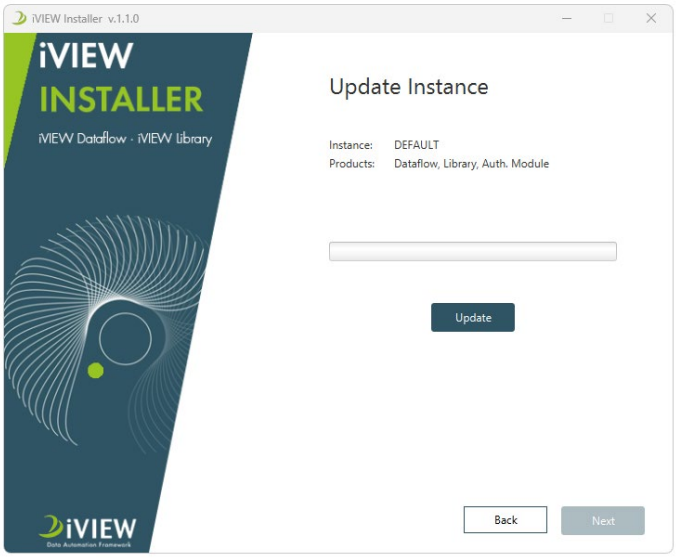

Figure 50: Software upgrade: Step Update

After clicking "*Update*", the update is performed. *It will take into consideration any configurations that have been done previously.*

Once the update is complete, the iVIEW installer offers the opportunity to validate services and the ability for the user to configure their Keycloak instance:

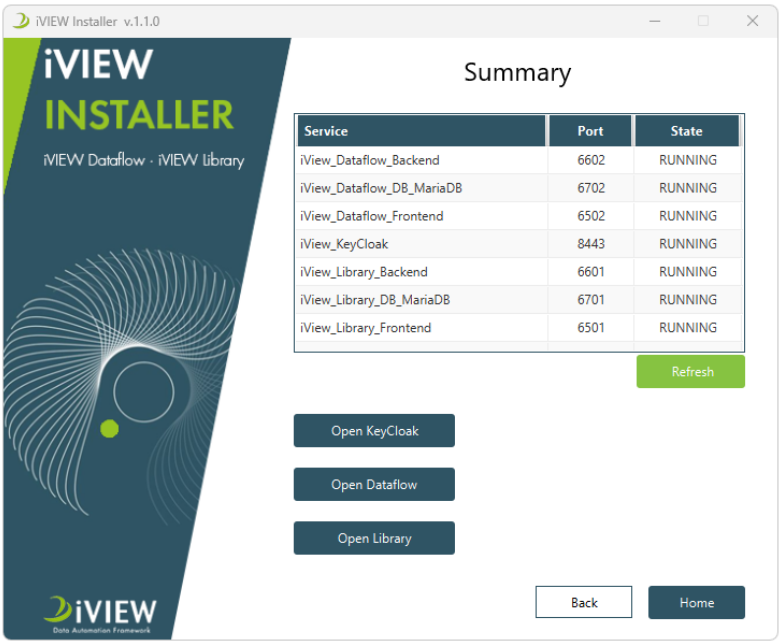

Figure 51: Software upgrade: Step Validation

It is highly recommended to always upgrade to the newest major release.

5.4 Uninstall

To uninstall the iVIEW Dataflow and/or iVIEW Library use the iVIEW Installer and choose the option “Uninstall”

5.5 Update Web Certificate

To update web certificate for the iVIEW Data automation Framework use the iVIEW Installer and choose the option “Certificate”