



Qloud Cover Writeback – Installation Guide Local Deployment

Stretch | www.stretch.se

For questions and inquiries contact support:
servicedesk@stretch.dk



Contents

Qloud Cover Writeback - Guide	0
Introduction	2
Installation Guide	3
Prerequisites	3
Step 1: Configure App Settings	4
Step 2: Create and Update License file	7
Step 3: Register the program and set up as a Service	8
Step 4: Run the service and validate.....	9
Step 5: Security Settings	10
Troubleshoot and Known issues	11



Introduction

This Guide is designed to give a walkthrough of how to install and get started using Qloud Cover – Writeback for local deployment.

Installation Guide

Prerequisites

The following is a list of prerequisites for installing Qloud Cover - Writeback:

- Admin access to a server which will run the service.
- .NET 8.0.10 Runtime and .NET core Runtime 8.0.10. **It is important that the Runtimes are installed in the correct order: first .NET Runtime and afterwards .NET core Runtime. If this is done wrong, uninstall both Runtimes with the desired URL below and install them again.**
 - Download the .NET 8.0.10 Runtime via:

<https://download.visualstudio.microsoft.com/download/pr/f55ed80e-ba58-4ac8-a2b3-f2227cd628de/6fabf1c613cf9386d14ddbaaca1a5eb8/dotnet-runtime-8.0.10-win-x64.exe>
 - Download the ASP.NET Core 8.0.10 Runtime via:
<https://download.visualstudio.microsoft.com/download/pr/a17b907f-8457-45a8-90db-53f2665ee49e/49bccd33593ebceb2847674fe5fd768e/aspnetcore-runtime-8.0.10-win-x64.exe>
- (Optional) Password and Email for an Email account.
- Certificate to Qloud Cover – Writeback on the server.
- **If using Azure AD** Instance, Domain, TenantID and ClientID for the Azure AD which the service should use to authenticate users.
 - Create an App Registration in Azure and find the Configurations which must be placed in the Configuration File in Qloud Cover – Writeback.

Step 1: Configure App Settings

To configure the file appsettings.json find the appsettings_template.json file and follow the setup in the guide. Afterwards rename the file to “appsettings.json” or copy the content into a new file with the required filename.

The following values appear (some of the fields are optional, others should not be configured):

1. *If Using OrganizationAzureAd Authentication*

Create an app registration in Azure and find the Configurations for *Instance*, *Domain*, *TenantId* and *ClientId*

2. Serilog

Configure the Logging Level for the service to use.

We recommend having the “Default” value to Information. But the following can be chosen if required:

- a. **Trace:** Logs that contain the most detailed messages.
- b. **Debug:** Logs that are used for interactive investigation during debugging.
- c. **Information:** Logs that track the general flow of the application.
- d. **Warning:** Logs that highlights abnormal or unexpected events in the program flow.
- e. **Error:** Logs that highlights errors.

Other values should not be changed.

3. Logging

Does not need to be configured when using local deployment.

4. DeployOptions

- a. **ApplicationAuthenticationProvider:** Choose which authentication provider to use for this application
 - i. **OrganizationAzureAd:** When using Azure AD
 - ii. **Negotiate:** When using Windows Active Directory
 - iii. **OpenId:** When using OpenId

Other steps does not needs to be configured, but ensure the correct values are set as specified in the appsettings_template file.

5. TenantDefinition

- a. **TenantOrganizationName:** Optional field to specify the the tenant name displayed in the GUI for all users. If field is blank the default name Qloud Cover - Writeback will be used.
- b. **TenantOwnerId:** Specify the ID of the tenant owner.
 - i. **Using OrganiztionAzureAd or OpenId:** Use the Email of the owner of the tenant. We recommend creating a SAC Account for this purpose.
 - ii. **Using Negotiate:** Enter the windows username for the user who should be the owner of the tenant, in the following format: "azuread\\username". Double backslash is required for escaping in .json file.
- c. **TenantOwnerEmail:** Enter the email we should use to send email notifications to.

NB these values cannot be changed without deleting the application database. Multiple owners can be created in the GUI when logged in with the Email of the original Tenant Owner.

6. Kestrel

Configure the certificate options. Follow what is specified in the appsettings_template file.

- a. **Subject:** To configure the subject, navigate to computer certificates, find the issued certificate. Open the certificate and find the Subject. Copy paste the subject and insert it in the subject section in the appsettings file.
- b. **If using another port than the default specified** update Http URL and HttpsInLinceCertStore with the port matching the desired port for the service.

7. EmailSettings

Optional fields to update the Email Settings for the Qloud Cover – Writeback service. This will use the specified email account to send emails with the system. Leave blank if you do not want to use the Email Service.

8. BackgroundEventOptions

- a. **Domain:** Match the Domain you wish to use for this application. We recommend using the DNS name of the Virtual Machine, if accessing it over the internet. Otherwise, use localhost.
- b. **Port:** Should match the HTTPS port configured for this application. Ensure that it matches the HTTPS port in section 5. Kestrel.

9. AllowedHosts



Update the allowed hosts if required. Use "*" for all hosts. Separate with ; for multiple hosts. E.g. "Host1.com;Host2.com;Host3.com"

Step 2: Create and Update License file

For Creating License:

Place the License file in the folder “License”. The file must have the name “license.slc”. If it does not have this, change the name of the file to “license.slc”.

Ensure the file is in the License folder.

For Updating License:

Retrieve the new license file from the service provider. Create a copy of the old license file. Ensure that the new license file is called “license.slc”. Restart the service and check the log files to validate that license file has been successfully updated.

Step 3: Register the program and set up as a Service

If you are not already on the server where the program should run, move the files to the server.

Under **Program Files (Do not use the X86 version)**. Create a folder with the name **Qloud Cover**, inside that folder create a folder called **Qloud Cover – Writeback**. Place all the files inside this folder.

Find the Install folder. Run the **Install.bat** file as an **administrator**. Go to services afterwards and validate that the service has been registered. It will have the name “Qloud Cover – Writeback”.

Step 4: Run the service and validate

Ensure that .NET Core 8.0 is downloaded. See more under Prerequisites.

Start the Service under services. Check the logfiles generated in the folder “Logs”. Ensure that everything runs successfully or change the configuration according to the log messages.

Go to a browser on the server and go to the url: <https://localhost:port> to check if you can access the GUI.

Step 5 will go over how to ensure that writeback can be accessed outside the server.

Step 5: Security Settings

The following settings must be set on the server for ports and firewalls. This ensures that the service can be accessed outside the server, and that it has access to Qlik Cloud and the chosen datastore.

1. On the server go to Windows Defender Firewall with Advanced Security
 - a. Create a new Inbound Rule
 - i. **Rule Type:** Choose *Port*
 - ii. **Protocol and Ports:** Choose *TCP*, Specify the Port the Writeback Service is running on
 - iii. **Action:** Allow the connection
 - iv. **Profile:** Select all by default, choose either if desired
 - v. **Name:** Give appropriate name
 - b. Go to where the Virtual Machine is hosted. This uses Azure for reference. Go to Network Settings and create new Inbound port rule
 - i. **Source:** IP Adresses.
 - ii. **Source Ip Adresses:** Choose the desired IP addresses that should be able to connect to this service.
 - iii. **Source port ranges:** *.
 - iv. **Destination:** Any.
 - v. **Service:** Custom.
 - vi. **Destination port ranges:** Choose the port matching the HTTPS for the service.
 - vii. **Protocol:** TCP.
 - viii. **Action:** Allow.
 - ix. **Priority:** Choose appropriate or default.
 - x. **Give useful names and description.**

Go to the URL *DNS:PORT* and verify that you can access the Writeback Application.

Enjoy 😊

Troubleshoot and Known issues

- .NET CORE 8.0 is missing. Check prerequisite and follow the provided URL to download .NET CORE 8.0.