Qlik Catalog® + Qlik Sense® Integration Guide

Qlik Catalog®

August 2021

TABLE OF CONTENTS

REQUIREMENTS FOR INTEGRATION 2

QVD IMPORT 3

1. Prerequisites + Environment Setup for QVD Import 3

2. Qlik Catalog + Qlik Sense Relationships 4

3. Security 5

4. Mounting Qlik Sense Windows Directory on Qlik Catalog Linux Host 5

5. Configuration of *core_env.properties* file on Qlik Catalog machine 8

6. Catalog Deployments Using SSL (Optional): Export Keystore Public Certificate to Qlik Sense server 8

7. Configure Qlik Sense for Catalog Connections 8

8. Copy Certificates from Qlik Sense Server to Qlik Catalog Server 12

9. QVD Import Workflow 13

10. Loading Encrypted QVDs 16

PUBLISH TO QLIK 23

1. Create a Connector in Qlik Sense 23

2. Copy Certificates from Qlik Sense Server to Qlik Catalog node 26

3. Configuration of *core_env.properties* file on Qlik Catalog machine 27

EMBEDDED CATALOG IN QLIK SENSE 30

NOTES ON USER ACCESS TO QVDS IN QLIK SENSE AND CATALOG 30

APPENDIX 33

1. Configuring Qlik Catalog to Validate a Certificate Issued by an Internal Certificate Authority 33

2. Qlik Catalog Active Directory User Import 35

Requirements for Integration

Integration between Qlik Catalog & Qlik Sense is dependent upon the following requirements:

- **Qlik Sense release version**
    - It is recommended that clients install a release of Qlik Sense from November 2020 forward for enhancements that simplify configuration processes.
    - The oldest version of Qlik Sense which may be integrated with Qlik Catalog is the November 2020 release.
- **Network connectivity**
    - *QVD Import* must have access to the Qlik Sense server over the following ports:
        - 443 - HTTPS communication
        - 445 - SMB communication (Windows-based file server shares)
        - 4242 - Qlik Sense Repository Service (QRS REST API)
    - *Publish To Qlik* must have access to the Qlik Sense server over the following ports:
        - 443 – HTTPS communication
        - 4243 – Qlik Sense Proxy Port
        - 4747 – Qlik Sense Engine Port
- **Server Administrative Access**
    - Qlik Catalog server:
        - Sudo “root” access
    - Qlik Sense server:
        - Local Windows Administrator access is required on the Qlik Sense server
        - RootAdmin access is required within the Qlik Sense Management Console (QMC)
- **Maintenance Window**:
    - *QVD Import*: The initial QVD import process may place a significant load on the Qlik Sense server system resources depending upon the number of QVD files be scanned & imported into Qlik Catalog. Administrators may want to consider performing this operation within a maintenance window or off-hours if the number of QVD files being processed is over 10,000.

QVD Import

Qlik Catalog allows users to import QVDs (Qlik View Data) files from a mapped instance of Qlik Sense. Qlik APIs are used to pull metadata directly from Qlik Sense into Qlik Catalog, and QVDs are then ingested and cataloged as source type QVD.

The process of **QVD Ingest** requires Administrators to provide information about Qlik Sense servers in the Qlik Catalog application (Admin→QVD Import). Once configured, Qlik Catalog queries the Sense server to obtain a list of connections and corresponding paths that have been tagged "QVD Catalog." Qlik Catalog dedupes the list and constructs a list of unique paths, and a Catalog Admin must then provide a unique source name for each of those paths. Qlik Catalog stores this mapping between folders and source names for use in entity creation.

This document details environment setup in both Qlik Sense and Qlik Catalog.

1. Prerequisites + Environment Setup for QVD Import
2. Qlik Catalog + Qlik Sense Relationships
3. Security
4. Mounting Qlik Sense Host Windows Directory Share on Qlik Catalog Linux Host
5. Copy Certificates from Qlik Sense Server to Qlik Catalog Server
6. Qlik Catalog QVD Import Workflow
7. Appendix
   A. Configuring Qlik Catalog to Accept A Certificate Issued by an Internal Certificate Authority
   B. Importing a Certificate Authority (CA) root certificate into the JVM Trust Store

1. Prerequisites + Environment Setup for QVD Import

Prerequisites: Follow the Qlik Catalog Installation Guide Section 3: Installation Prerequisites. In particular, section 3.5 on Qlik Sense Integration provides details on how to install Node.js and Docker:

- **Docker**: Qlik Core is a core set of components (that includes a utility enabling conversion of proprietary Qlik format into CSV/Text Tab Delimited) that runs in a Docker container.

- **Node.js**: Used to execute Qlik Core JavaScript APIs to allow data and metadata to flow between Qlik Sense and Qlik Catalog. This must be installed on both application servers (Qlik Sense and Qlik Catalog).

Note: QVD Import is NOT currently supported for multi-node Qlik Catalog deployments using Oracle as a metadata database.

Environment Setup Overview

The **Qlik Catalog Installer** configures and enables Qlik Core and automatically populates the core_env property `qvd.openconnector.script.path`. This property provides the file path to a key shell script responsible for loading data. The script interacts with Qlik Core (running as a Docker container) and puts the data formatted as CSV into QDC Loading Dock directory. The file can then be read like any other source in Qlik Catalog.

Active Directory Sync: The ***same*** users and groups must be present in Qlik Catalog and Qlik Sense from the same Active Directory. Qlik Sense users will either be created manually in Qlik Catalog and Qlik Sense or will be synchronized with the same Active Directory that is in use by Qlik Sense. While it is possible to manually check that the same users and groups exist in both applications, AD Sync is strongly encouraged as the preferred mechanism to ensure all users and groups are available in both applications.

Linux Mount Point of Qlik Sense Data Share: Qlik Sense Data Connection Windows folders must be shared, and then mounted on the Qlik Catalog Linux server. See Windows Network Share Creation + Mounting Windows Directory

Copy Qlik Sense Server Certificates: Authentication to Qlik Sense is provided to the Qlik Catalog server using certificates which are located on the Qlik Sense server.

Qlik Sense configuration: From the Qlik Management Console (QMC) in Qlik Sense, Administrators tag connectors that contain QVDs of interest with the "QVD Catalog" tag.

QVD Ingest: From the **QVD Ingest** tab in the Admin section of the Qlik Catalog, Administrators add connectors (entry points into Qlik Sense) by providing:

- Directory paths to folders – this is a mapping of a Qlik Sense Windows path to a Qlik Catalog Linux path

Paths can be listed from "Show QVD Paths" to see which paths have QVDs that have been "Added", "Removed" or "Changed". Users accept those statuses and the connectors are then updated accordingly. These QVDs populate into the Source module, where data can be loaded like any other source type in Qlik Catalog. See QVD Ingest Workflow section for detailed steps. Note that *metadata* load is incremental loadtype and QVD *data* load is snapshot.

2. Qlik Catalog + Qlik Sense Relationships

The following table describes objects in Qlik Catalog and corresponding objects in Qlik Sense.

Qlik Sense	Qlik Catalog	Comments
User	**User**	Every Qlik Sense user must be the same user in Qlik Catalog with the same name. Syncing through shared Active Directory domains is strongly encouraged.

		Users should have access to the same QVDs between the two applications. Qlik Sense is the master application where access to QVDs is defined as part of QVD authoring/administration and Qlik Catalog honors these privileges.
QVD file	**Entity**	Every Qlik Sense QVD will be represented as one Entity in Qlik Catalog.
Qlik Sense Connection	**Group**	Each Qlik Sense Connection will have a corresponding group in Qlik Catalog. This mapping is done for security purposes and access control management. Note that Security Groups are automatically generated, named, and synced by capturing the Qlik Sense Connector Globally Unique ID which is 36 characters and removing the hyphens to comply with Linux Group name 32-character limit.
Folder	**Source**	Each unique folder in Qlik Sense will be represented as one unique Source in Qlik Catalog containing all Entities that represent QVDs under that folder. User access to QVDs will be governed by user access privileges as defined in Qlik Sense (via folder access).

3. Security

User access to QVDs will be governed by user access privileges as defined in Qlik Sense (via folder access). The logged in user is able to access and sync QVDs for Qlik Sense connections that the user has access to and, when ingested, a Qlik Catalog group (and name) will be auto-retrieved capturing the Qlik Sense Connection GUID (Globally Unique Identifier).

The folders are mapped between applications and when the user signs in their access to security connections in Qlik Sense are transferred to the security groups in Qlik Catalog.

4. Mounting Qlik Sense Windows Directory on Qlik Catalog Linux Host

Each Qlik Sense Data Connection Windows folder that will be catalogued by Qlik Catalog must be accessible via a Linux mount point created on the Qlik Catalog server.
For example, if all Data Connection folders and QVDs are contained under C:\data on the Qlik Sense Windows server this folder should be shared and mounted as a directory on the Qlik Catalog linux file system (e.g., /usr/local/qdc/source/qvd-share). If there are multiple different Windows folders to share, then multiple Linux mounts may be needed.

Part I: Create a Windows Network Share on the *Qlik Sense* server

1) Create a shared QVD repository on the Qlik Sense server:

Create a **Service User**:

- In the Windows **Start** menu, type *Computer Management* to open the app.
- Open **Local Users and Groups > Users**.
- Right-click and select **New User**.
- Enter **User name**: *qvd_scanner*, **Full name**: *QVD Scanner*, and **Description**: *QVD Scanner*.
- Enter a password, and, optionally, modify the password settings.
- Click **Create**.

Create **QVD file share**:

- On your *C:* drive, create a new folder called *qvd_repository*.
- Right-click your new folder *qvd_repository* and select **Properties**.
- Open the **Sharing** tab and click **Share**.
- Enter *qvd_scanner* and click **Add**.
- Click **Share** and then **Done**.
- Open the folder *qvd_repository*.
- In the folder, right-click and select **New>Text Document**.
- Edit the file name and extension so that it reads *readme.txt*.
- Open a command prompt and type *net view \\<host name>*.
- Verify that *qvd_repository* is present as a shared resource.

Create **firewall exceptions**:

- Open **Windows Defender Firewall** in the control panel.
- Verify that **Domain networks** have *Connected* status.
- To the left, select **Advanced Settings**.
- To the left, select **Inbound Rules**.
- To the right, select **New Rule...**
- Select **Port** and click **next**.
- Enter the Qlik Sense Engine port: *4747*, click **next**.
- Allow the connection, click **next**.
- Deselect **Public**, click **next**.
- **Name**: *Qlik Sense Engine*, click **finish**.

- Repeat above steps to create an additional firewall exception for *Qlik Sense Repository Service port: 4242*
- Repeat above steps to create an additional firewall exception for *Qlik Sense Proxy port*: *4243*

  Refer to Qlik Sense documentation for more information regarding ports: https://help.qlik.com/en-US/sense/November2020/Subsystems/PlanningQlikSenseDeployments/Content/Sense_Deployment/Ports.htm

Part II: Mount the Qlik Sense Windows Share on the *Qlik Catalog* Linux Server

Note: Use of CIFS for mounting Windows network shares on Linux servers is well-documented online; there are various methods for creating these mount points.

1) Create a mount point on Linux server:

   - Login to the Qlik Catalog server (SSH login).
   - In a bash (CLI) terminal, enter the following using the Catalog Service Account to create a mount point:

     ```
     (qdc) $ mkdir -p /usr/local/qdc/source/qvd_repositories/<windows_hostname>
     ```

     Note: This directory must now be under the directory specified in core_env.properties:

     ```
     localfile.base.dir.source.connection=/usr/local/qdc/source
     ```

   - Create a permissions file:

     ```
     sudo vi /root/.<windows_hostname>_credentials
     ```

     ```
     Example:  sudo vi /root/.sense1_credentials
     ```

     Add the following lines using the credentials created in Part I Step 1 above:

     ```
     domain=<SENSE SERVER HOSTNAME>
     password=<password>
     username=<qvd_scanner>
     ```

2) Using the text editor of your choice, EDIT /etc/fstab to auto-mount the CIFS share during boot. Append /etc/fstab with the following:

   ```
   sudo vi /etc/fstab

     //<windows_hostname>/qvd_repository /usr/local/qdc/source/qvd_repositories/<windows_hostname>    cifs
     credentials=/root/.<windows_hostname>_credentials 0 0
   ```

   Issue the following command to mount the Windows share:

   ```
   # sudo mount -a
   ```

3) Issue the following command to verify the contents of the new share:

```
# ls /usr/local/qdc/source/qvd_repositories/<windows_hostname>

Example:  ls /usr/local/qdc/source/qvd_repositories/sense1
```

5. Configuration of *core_env.properties* file on Qlik Catalog machine

The ***core_env.properties*** is located in the TOMCAT_HOME/conf directory. (TOMCAT_HOME was defined during the Qlik Catalog installation process. The installation default is /usr/local/apache-tomcat-<version-number>). The following property within core_env.properties is essential to QVD Import:

- **podium.qlik.qsockclient.script.directory**: Path to qsocks client script directory. This is the directory where qsock client scripts are placed and used for creating, updating, and listing apps. The default location is $QDC_HOME/qlikpublish.

  Example:
  ```
  podium.qlik.qsockclient.script.directory=/usr/local/qdc/qlikpublish/
  ```

6. Catalog Deployments Using SSL (Optional): Export Keystore Public Certificate to Qlik Sense server

If Qlik Catalog has been configured to use HTTPS a public key certificate must be issued from the keystore on the Catalog server and copied to the Qlik Sense server. (Instructions for configuring SSL and HTTPS re-direct are included in the Qlik Catalog Installation Guide).

1) Export the public certificate from the Catalog server keystore:

   ```
   keytool -alias qdc -keystore ./keystore -storetype jks -export -rfc -file ./keystore_pub.pem
   ```

2) Copy the keystore_pub.pem file to a directory on the Qlik Sense server (e.g. C:\ProgramData\Qlik\Sense). (The location of keystore_pub.pem on the Qlik Sense server will be needed in Step 7).

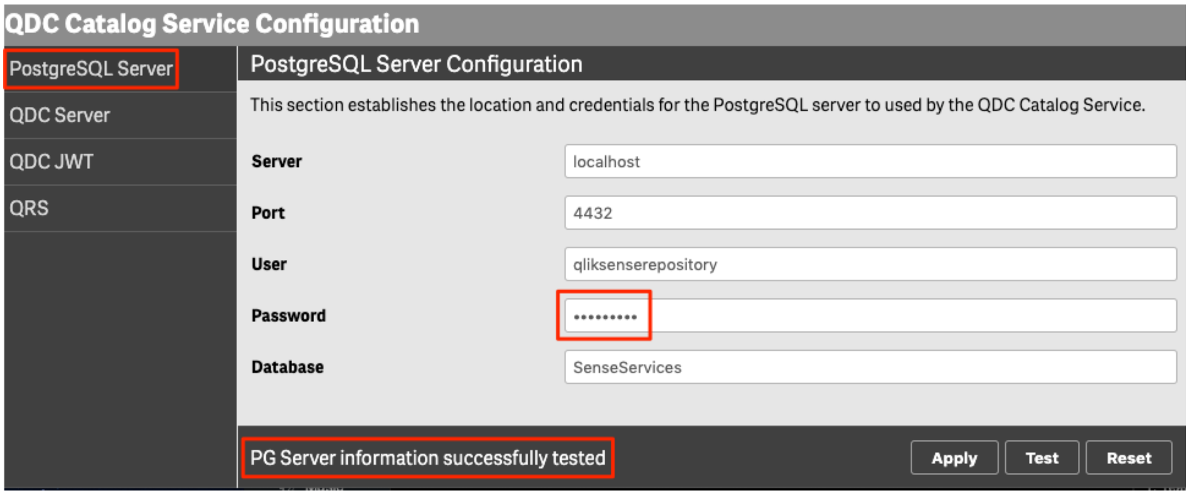
7. Configure Qlik Sense for Catalog Connections

Note: Qlik Sense RootAdmin access is required to perform these operations. This can only be granted to a user after first QMC (Qlik Management Console) login.

1. On the Sense server, navigate to the Qlik Management Console page: https://<qlik-sense-hostname>/qmc and authenticate.

2. On a new tab, navigate to the setup page for the QDC Catalog Service, located here: https://<qlik-sense-hostname>/api/qdc/v1/setup/ui/page.html. There are 4 configuration screens in the left sidebar.

3. PostgreSQL Server configuration screen



QDC Catalog Service Configuration

PostgreSQL Server Configuration

This section establishes the location and credentials for the PostgreSQL server to used by the QDC Catalog Service.

Server: localhost

Port: 4432

User: qliksenserepository

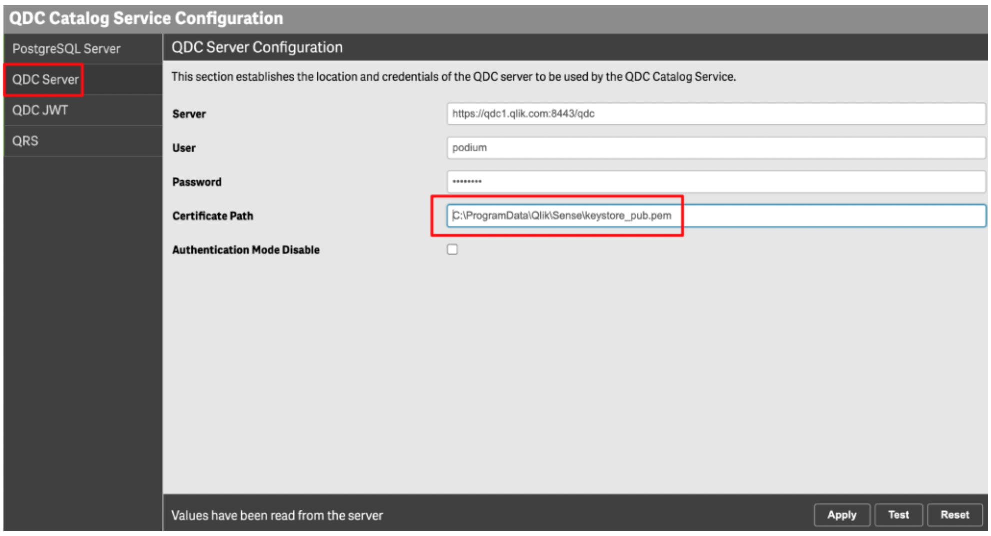
Password: •••••••••

Database: SenseServices

PG Server information successfully tested

a) Supply password for the qliksenserepository user account.
b) Click “Test.”
c) If the test is successful click “Apply”

4. QDC Server configuration screen



QDC Server Configuration

This section establishes the location and credentials of the QDC server to be used by the QDC Catalog Service.

Server: https://qdc1.qlik.com:8443/qdc

User: podium

Password: ••••••••

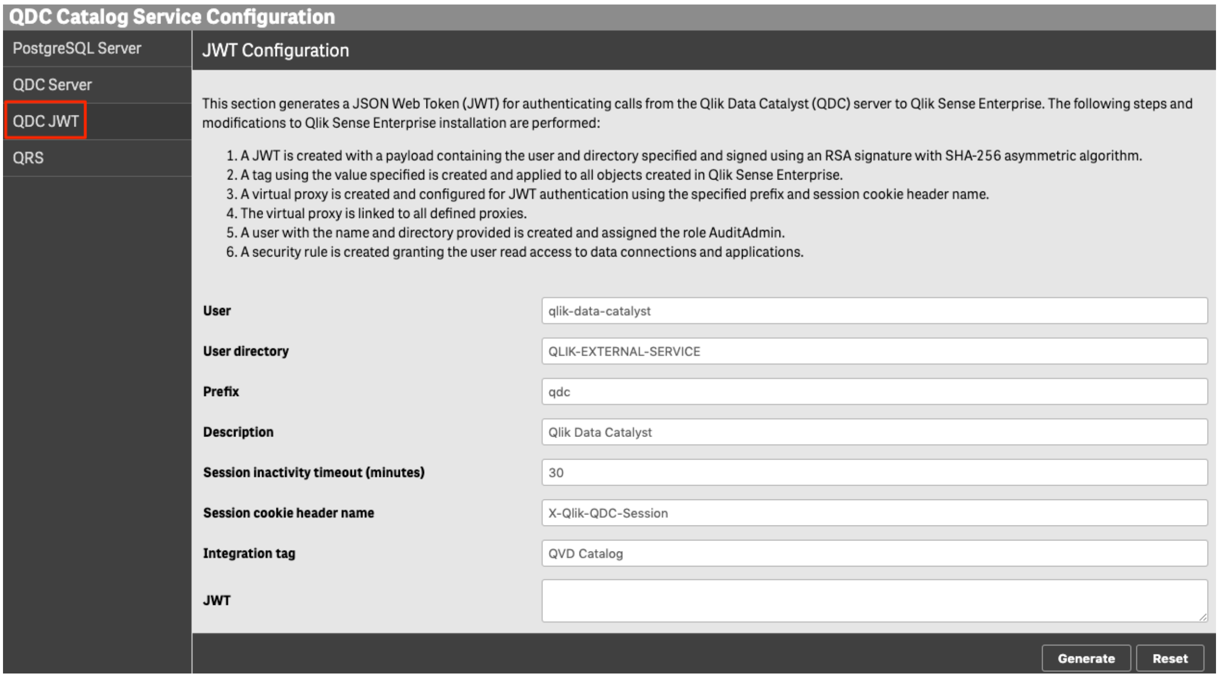
Certificate Path: C:\ProgramData\Qlik\Sense\keystore_pub.pem

Authentication Mode Disable □

Values have been read from the server

a) Server: Enter the URL the QDC server (https://<hostname>:8443/qdc)
b) User: Enter the QDC admin account (default is ‘podium’)
c) Password: Enter the QDC admin account password
d) Certificate Path: ONLY REQUIRED FOR CATALOG DEPLOYMENTS USING HTTPS → enter the Qlik Sense server directory path of the QDC Certificate (copied to Sense server in Step 6)
e) Clik “Test.”
f) If the test is successful, click “Apply

5. QDC JWT configuration screen



JWT Configuration

This section generates a JSON Web Token (JWT) for authenticating calls from the Qlik Data Catalyst (QDC) server to Qlik Sense Enterprise. The following steps and modifications to Qlik Sense Enterprise installation are performed:

1. A JWT is created with a payload containing the user and directory specified and signed using an RSA signature with SHA-256 asymmetric algorithm.
2. A tag using the value specified is created and applied to all objects created in Qlik Sense Enterprise.
3. A virtual proxy is created and configured for JWT authentication using the specified prefix and session cookie header name.
4. The virtual proxy is linked to all defined proxies.
5. A user with the name and directory provided is created and assigned the role AuditAdmin.
6. A security rule is created granting the user read access to data connections and applications.

User: qlik-data-catalyst

User directory: QLIK-EXTERNAL-SERVICE

Prefix: qdc

Description: Qlik Data Catalyst

Session inactivity timeout (minutes): 30

Session cookie header name: X-Qlik-QDC-Session

Integration tag: QVD Catalog

JWT:

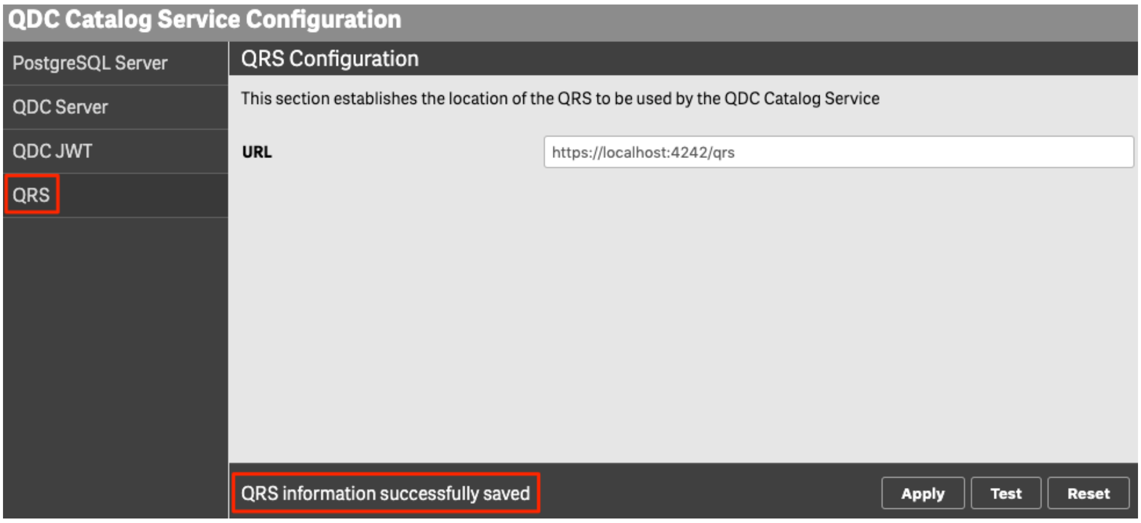
a) Review the values for the different fields and click **Generate**.

b) A message is displayed: *Successfully updated QDC-QSE security settings*.

c) Verify Settings in the Qlik Management Console:

a) In the Qlik Management Console, open the **Users** section and verify that *qlik-data-catalyst* is present.
b) Open the **Security rules** section and verify that **Qlik Data Catalyst Security...** is present.
c) Open the **Tags** section and verify that QVD Catalog is present.
d) Open the **Virtual proxies** section and verify that Qlik Data Catalyst is present.

6. QRS configuration screen
   a) Accept default value and click “Apply.”



This section establishes the location of the QRS to be used by the QDC Catalog Service

URL https://localhost:4242/qrs

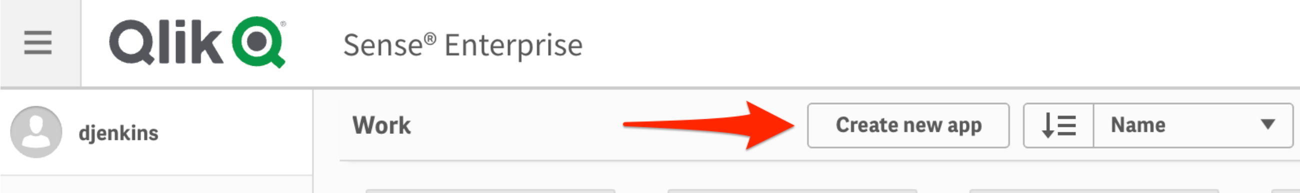
QRS information successfully saved

7. Verify Configuration in Qlik Sense QMC:

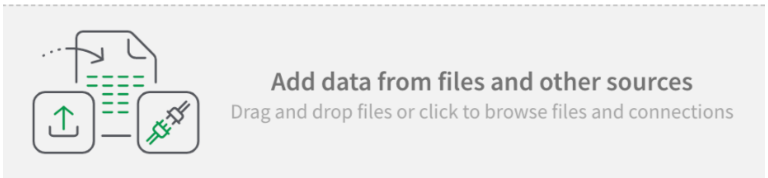
   a) Navigate to the Qlik Management Console page: *https://<qlik-sense-hostname>/qmc* and authenticate.
   b) In the Qlik Management Console, open the **Users** section and verify that **qlik-data-catalyst**. is present.
   c) Open the **Security rules** section and verify that ***Qlik Data Catalyst Security Rule*** is present.
   d) Open the **Tags** section and verify that **QVD Catalog** is present.
   e) Open the **Virtual proxies** section and verify that ***Qlik Data Catalyst*** is present.

8. Prepare the data connection in Qlik Sense Hub:

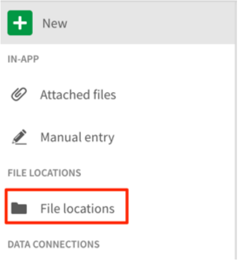
   a) Open Qlik Sense **Hub**.
   b) **Create** a new app and **open** it:



   c) Click **Add data** from files and other sources:

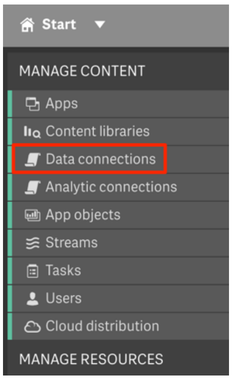

Add data from files and other sources
Drag and drop files or click to browse files and connections

d) In the menu to the left, click **File locations**:

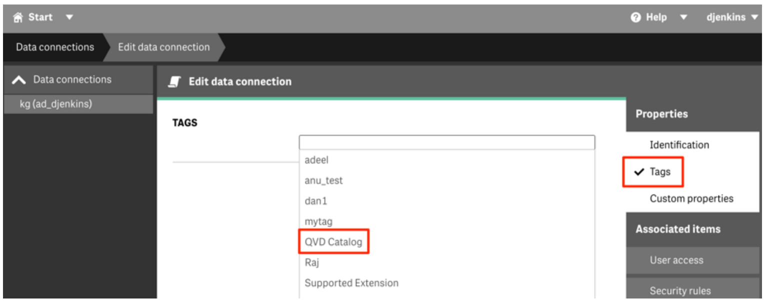


.

e) Navigate to the *qvd_repository* folder on your C: drive.
f) Select one of the QVDs and click **Next**.
g) In the Qlik Management Console, open the section **Data connections**:



h) Select the *qvd_repository* data connection and click **Edit**.
i) In the **Properties menu** to the right, select **Tags**.
j) Click in the **Tags** field, select QVD Catalog and click **Apply**:



8. Copy Certificates from Qlik Sense Server to Qlik Catalog Server

1) Export certificates from Qlik Sense using the Management Console (QMC).
To export the public and private keys from a Qlik Sense server, please see https://help.qlik.com/en-US/sense/June2019/Subsystems/ManagementConsole/Content/Sense_QMC/export-certificates.htm

The default location for the exported certificates is the following directory ***on the Qlik Sense server***:

```
C:\ProgramData\Qlik\Sense\Repository\Exported Certificates
```

(A folder will be created within the “Exported Certificates” directory with whatever name is entered during the export process described in the link above).

2) Copy the certificates exported in step1 from the Qlik Sense server into the “**certs”** directory on the Qlik Catalog server. The **certs** directory will be located in the QDC_HOME directory. (QDC_HOME was defined during the Qlik Catalog installation process. The installation default is /usr/local/qdc/qlikpublish/certs). The following files should be copied:

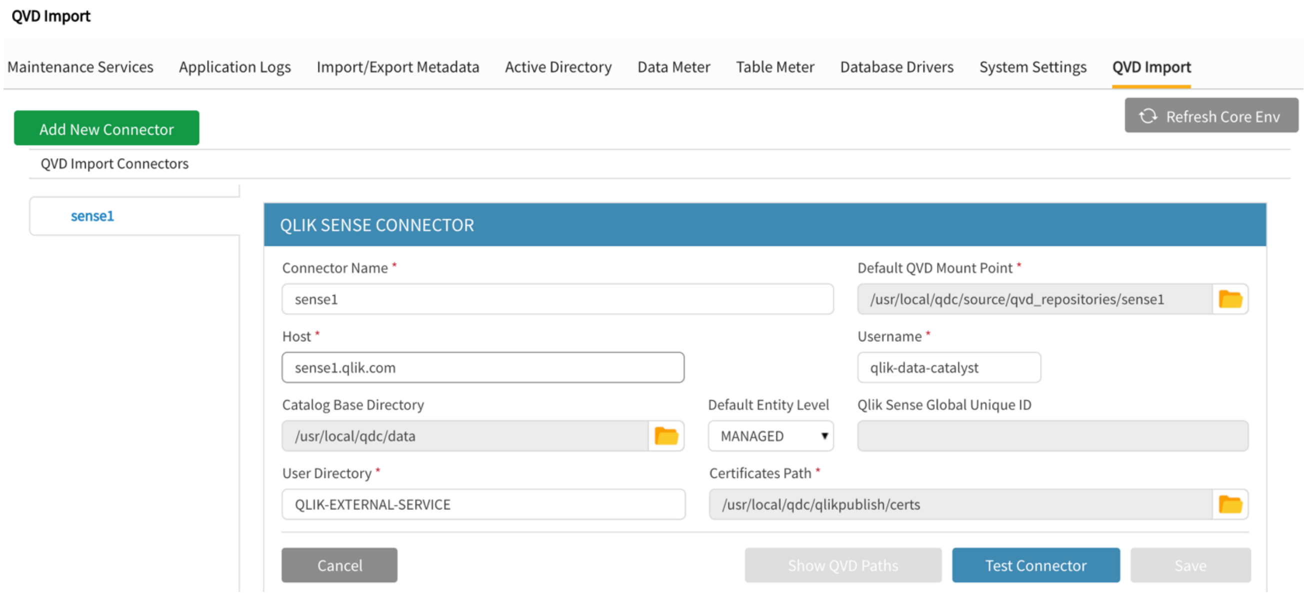
```
client.pem
client_key.pem
root.pem
server.pem
server_key.pem
```

9. QVD Import Workflow

To begin importing QVDs, Admins access a **data source** in Qlik Sense. [If needed, refer to Qlik Sense documentation to create a connection and add data: https://help.qlik.com/en-US/connectors/Subsystems/Integrated_Web_Connectors_help/Content/Connectors_QWC_BuiltIn/Introduction/Creating-a-connection.htm]

The following steps detail creation of a Connector in Qlik Catalog and import of QVDs.

1. Login to Qlik Catalog with valid credentials.
   --User must have Admin privileges to access and manage Admin tab.
2. Click on **Admin** on top right-hand side of top task bar
3. Click on **QVD Import** tab
4. Select **Add New Connector**



Connector Name * sense1
Default QVD Mount Point * /usr/local/qdc/source/qvd_repositories/sense1
Host * sense1.qlik.com
Username * qlik-data-catalyst
Catalog Base Directory /usr/local/qdc/data
Default Entity Level MANAGED
Qlik Sense Global Unique ID
User Directory * QLIK-EXTERNAL-SERVICE
Certificates Path * /usr/local/qdc/qlikpublish/certs

5. On the **QLIK SENSE CONNECTOR** tab enter:

Connector Name: Required, User defined
Default QVD Mount Point: Required. This value can be entered manually or found in Linux Path when editing the connection in Qlik Sense
Host: Required, Qlik Sense Host URL (example: sense1.qlik.com)
Username: Qlik Sense service username created previously: qlik-data-catalyst
Catalog Base Directory: This is where Qlik Catalog stores the data on local file system (e.g., ‘/usr/local/qdc/data/’)

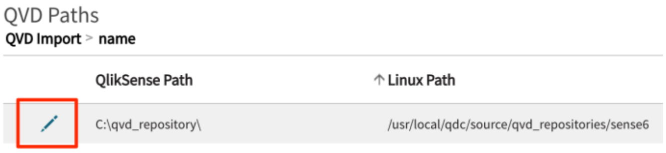
Default Entity Level: This is populated from System Settings and can be overwritten (options are MANAGED or REGISTERED)
Qlik Sense Global Unique ID: Auto-retrieved upon "Test Connection", every installation of Qlik Sense has a Globally Unique Identifier (GUID).
User Directory: QLIK-EXTERNAL-SERVICE
Certificates Path: Location of the Qlik Sense server certificates which were copied in Step 5 above.

6. Click **Test Connector**. Upon Connection Success, **Save** the Connection

7. Click on **Show QVD Paths** to set up paths

8. In the **QVD Paths** screen, click on **Sync Paths.** All available Qlik Sense connections that have had the "QVD Catalog" tag applied are filtered and imported into Qlik Catalog. When the paths are synced, the Qlik Sense Windows folder must be mapped to the Linux path folder, thereby making Qlik Catalog aware of each QVD in these folders. Every QVD in Qlik Sense corresponds to a new QVD entity in Qlik Catalog.

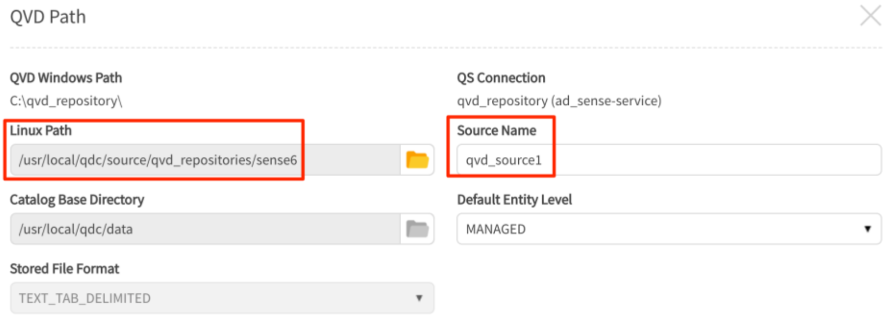
9. Click on the **pencil icon** on any Qlik Sense Path.



QVD Paths
QVD Import > name

	QlikSense Path	↑ Linux Path
✎	C:\qvd_repository\	/usr/local/qdc/source/qvd_repositories/sense6

   a. Name the Source
   b. Be sure that the Linux path specified is the mount point for the Windows shared folder containing QVD files on the Qlik Sense server.

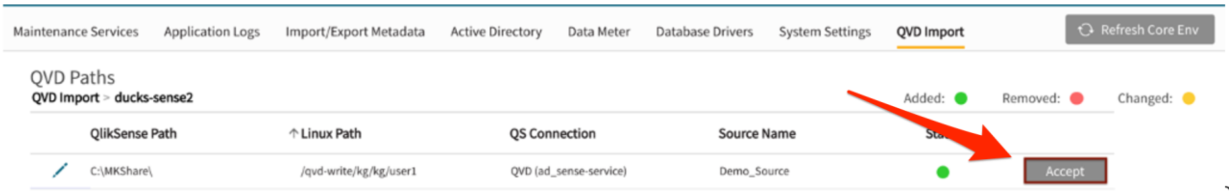


QVD Path

QVD Windows Path: C:\qvd_repository\
QS Connection: qvd_repository (ad_sense-service)
Linux Path: /usr/local/qdc/source/qvd_repositories/sense6
Source Name: qvd_source1
Catalog Base Directory: /usr/local/qdc/data
Default Entity Level: MANAGED
Stored File Format: TEXT_TAB_DELIMITED

   c. Click OK

10. **Accept** the path to save the metadata. An Admin must select ***Accept*** to the right of the paths in order to persist the path in Qlik Catalog so that the application knows to scan the folder path and extract information for that folder.

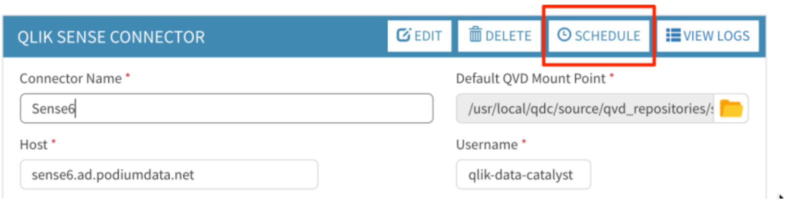


QVD Paths

QVD Import > ducks-sense2

QlikSense Path	Linux Path	QS Connection	Source Name	Sta
C:\MKShare\	/qvd-write/kg/kg/user1	QVD (ad_sense-service)	Demo_Source	●

11. Go back to QVD Import page. Open the QVD Import Connector > select **Schedule**



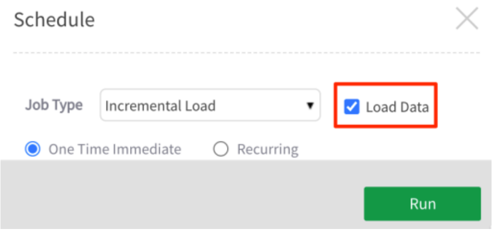
Connector Name * Sense6

Default QVD Mount Point * /usr/local/qdc/source/qvd_repositories/:

Host * sense6.ad.podiumdata.net

Username * qlik-data-catalyst

12. Select "Load Data" box, and then **Run**. The mounted folder (Linux path) is scanned and the QVD entities are added to the created source ("Demo_Source" in pictured example) created on the Paths screen.



Job Type Incremental Load ☑ Load Data

● One Time Immediate ○ Recurring

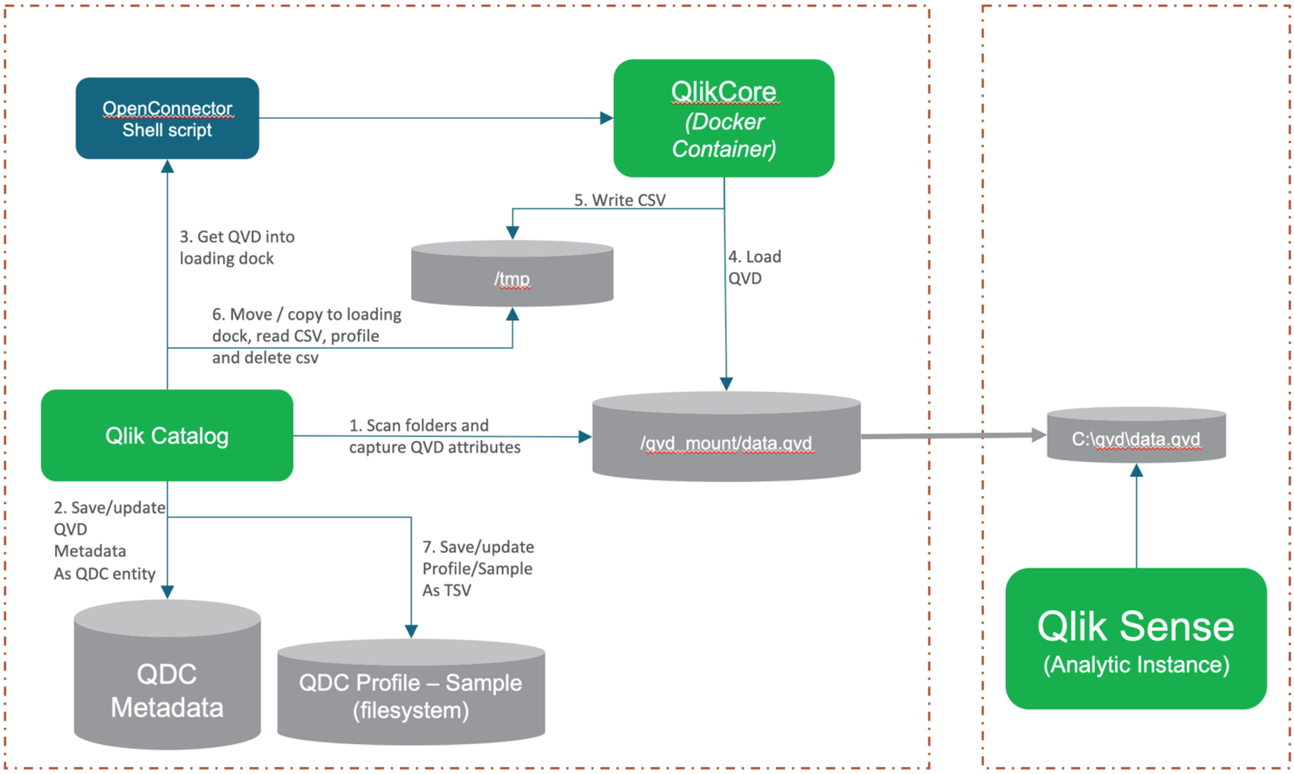
When Run is initiated, Qlik Catalog scans the folder, finds QVDs, and creates/updates/deletes QVDs in Qlik Catalog. File attributes are read from the XML Header of the originating QVD, and information about the QVD required to build a metadata environment (e.g., Fields/Columns) for a QVD entity in Qlik Catalog is extracted in this step.

13. Note that data has to be loaded after the metadata environment is established. Users load data for QVD entities like any other Source Type from the Entity grid in the Source Module.

For enhanced security, see Appendix section "Configuring Qlik Catalog to Validate a Certificate Issued by an Internal Certificate Authority".

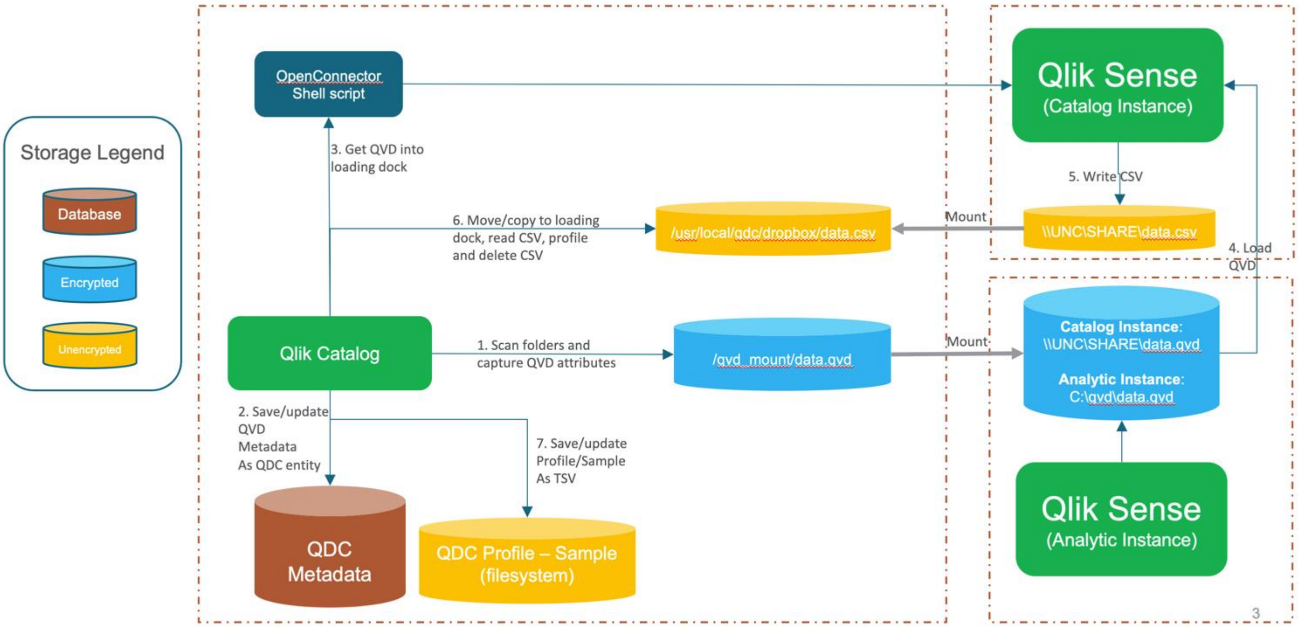
10. Loading Encrypted QVDs

Traditionally, QVDs are loaded using a Qlik Core engine running in a Docker container on the same host as Qlik Catalog:


OpenConnector Shell script
QlikCore (Docker Container)
5. Write CSV
3. Get QVD into loading dock
/tmp
4. Load QVD
6. Move / copy to loading dock, read CSV, profile and delete csv
Qlik Catalog
1. Scan folders and capture QVD attributes
/qvd_mount/data.qvd
C:\qvd\data.qvd
2. Save/update QVD Metadata As QDC entity
7. Save/update Profile/Sample As TSV
QDC Metadata
QDC Profile – Sample (filesystem)
Qlik Sense (Analytic Instance)

However, the Qlik Core engine in the Docker container cannot sample, profile and otherwise process data embedded in encrypted QVDs. Only an engine running on a Microsoft Windows Qlik Sense server can decrypt QVD data.

Qlik Catalog may now be configured to load encrypted QVDs using an engine running on a Microsoft Windows Qlik Sense server:


Storage Legend
Database
Encrypted
Unencrypted
OpenConnector Shell script
Qlik Sense (Catalog Instance)
3. Get QVD into loading dock
5. Write CSV
6. Move/copy to loading dock, read CSV, profile and delete CSV
/usr/local/qdc/dropbox/data.csv
Mount
\\UNC\SHARE\data.csv
4. Load QVD
Qlik Catalog
1. Scan folders and capture QVD attributes
/qvd_mount/data.qvd
Mount
Catalog Instance: \\UNC\SHARE\data.qvd
Analytic Instance: C:\qvd\data.qvd
2. Save/update QVD Metadata As QDC entity
7. Save/update Profile/Sample As TSV
QDC Metadata
QDC Profile – Sample (filesystem)
Qlik Sense (Analytic Instance)
3

It is assumed a second Qlik Sense server will be setup to load the encrypted QVDs and convert them to CSV files. This is to ensure the primary Qlik Sense server, labelled “Analytic Instance” in the above diagram, is not impacted/overloaded. The Qlik Sense server in the top-right corner, labelled “Catalog Instance”, converts the encrypted QVDs to CSV files. It is possible to use a single Qlik Sense server, but the solution has been designed to support separate Qlik Sense instances on different servers.

As the two Qlik Sense servers may be running on different hosts, the paths used to access QVDs may differ. For example, in the above diagram, the “Analytic Instance” server refers to QVDs on local disk, (e.g., C:\qvd\data.qvd). This is the full Windows path recorded in the Qlik Catalog metadata database during the inventory process (“1. Scan folders and capture QVD attributes”). The “Catalog Instance” server refers to the same QVDs using a UNC path (e.g., \\SERVER\SHARE\data.qvd). The configuration of Qlik Catalog must support transforming the local path to the UNC path – the text “C:\qvd” must be replaced with “\\SERVER\SHARE”.

Property “qvd.openconnector.script.path”, in the Qlik Catalog core_env.properties file, must be modified to enable processing of encrypted QVDs. It will resemble:

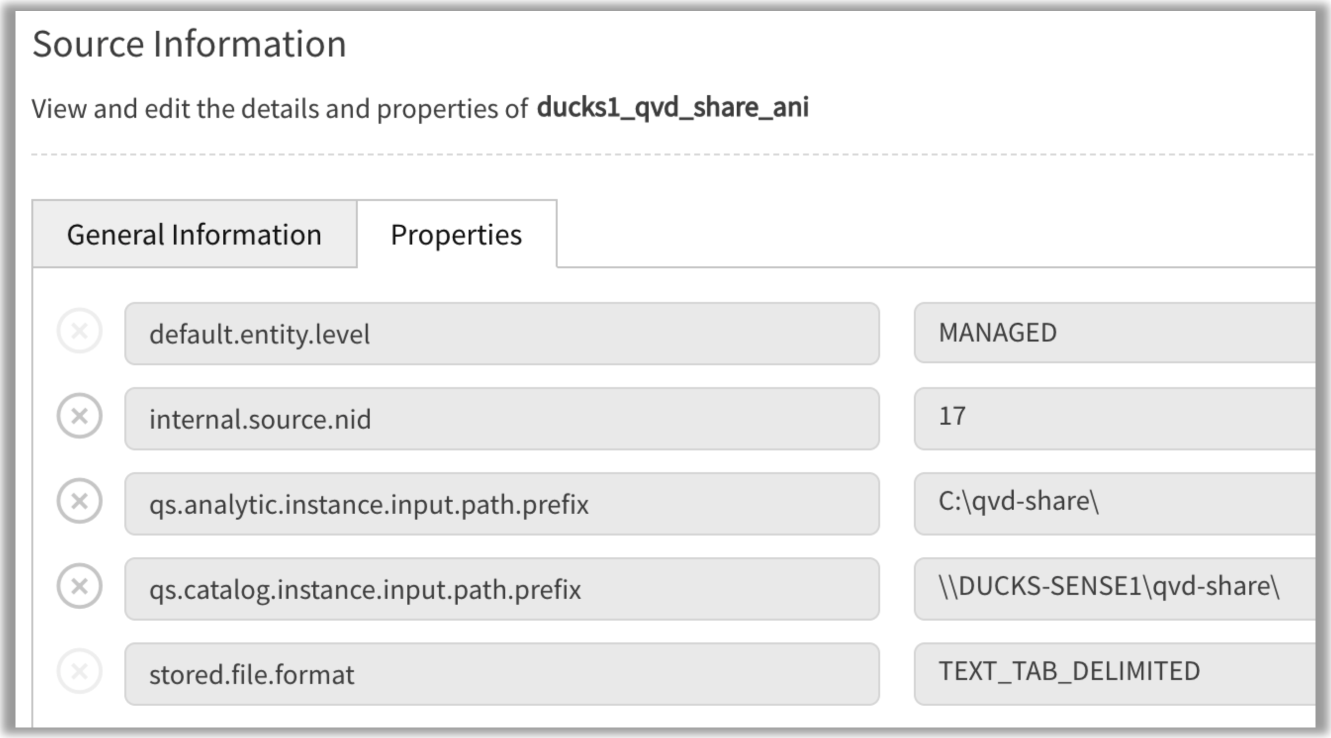
```
qvd.openconnector.script.path=/usr/local/qdc/qlikcore/qdc_qvd_2_csv_remote.sh %prop.qvd.file.windows.full.path \
    %prop.qs.analytic.instance.input.path.prefix %prop.qs.catalog.instance.input.path.prefix \
    qs.catalog.instance.host=beauty-sense1.ad.podiumdata.net qs.catalog.instance.port=4747 \
    qs.catalog.instance.user.directory=AD qs.catalog.instance.user.id=sense-service \
    qs.catalog.instance.output.path=\\\\installer1\\dropbox-beauty-sense1 catalog.linux.instance.output.path=/usr/local/qdc/dropbox-beauty-sense1 \
    %loadingDockLocation %loadingDockUri %qlikCoreScript
```

The following table explains each argument:

Argument	**Description**
/usr/local/qdc/qlikcore/qdc_qvd_2_csv_remote.sh	Path to OpenConnector script. Script will be present in directory post-install.
%prop.qvd.file.windows.full.path	When the script is invoked, this argument will be automatically replaced with the Entity property containing the full Windows path to the QVD (e.g., C:\qvd\data.qvd).
%prop.qs.analytic.instance.input.path.prefix	When the script is invoked, this argument will be automatically replaced with the Source property containing the portion of the full Windows path to be replaced (e.g., C:\qvd). This property must be **manually** added to the Source – see below.
%prop.qs.catalog.instance.input.path.prefix	When the script is invoked, this argument will be automatically replaced with the Source property containing the portion of the full Windows path to be inserted (e.g., \\SERVER\SHARE). This property must be **manually** added to the Source – see below.
qs.catalog.instance.host=beauty-sense1.ad.podiumdata.net	The hostname and port of the Qlik Sense server which will be used to convert the encrypted QVD to a CSV file (aka, the “Catalog Instance”).
qs.catalog.instance.port=4747	
qs.catalog.instance.user.directory=AD	

Argument	Description
qs.catalog.instance.user.id=sense-service	The Windows DOMAIN\username which is running the Qlik Sense Engine Service on the Qlik Sense “Catalog Instance” server.
qs.catalog.instance.output.path=\\\\catalog1\\dropbox	The UNC path to which the Qlik Sense engine will output the CSV file. It is a mount of a directory on the Qlik Catalog server. **Notice** that each Windows slash must be escaped. See below for instructions on setting up this mount.
catalog.linux.instance.output.path=/usr/local/qdc/dropbox	The directory on the Qlik Catalog server from which the OpenConnector script will retrieve the CSV file. This is the directory to which the mount refers.
%loadingDockLocation	Standard, internal arguments.
%loadingDockUri	
%qlikCoreScript	

Each Qlik Catalog Source represents a unique Qlik Sense Windows path that was inventoried. A search-and-replace is performed to transform the Windows path accessible on the “Analytics Instance” to a UNC path accessible on the “Cataog Instance”. This is driven by the two “prefix” properties in the table above. These prefix properties must be added as Source properties as follows:



Source Information

View and edit the details and properties of **ducks1_qvd_share_ani**

default.entity.level	MANAGED
internal.source.nid	17
qs.analytic.instance.input.path.prefix	C:\qvd-share\
qs.catalog.instance.input.path.prefix	\\DUCKS-SENSE1\qvd-share\
stored.file.format	TEXT_TAB_DELIMITED

Applying the above two prefix properties to each full Windows path to a QVD, the beginning portion “C:\qvd-share\” will be replaced with “\\DUCKS-SENSE1\qvd-share\” -- this will enable the “Catalog Instance” to load the QVD using a full UNC path.

NOTE: when the core_env property “qvd.openconnector.script.path” is first changed, the Admin / “Refresh Core Env” button should be pressed, and a QVD “Full Reload” scheduled. The order of operations is:

- Change the core_env property
- Press “Refresh Core Env”
- Schedule a “Full Reload” – do NOT check the “Load Data” box, unless the prefix properties have already been added to the Source
- Add the prefix properties to each Source
- Load the desired Entities – once the prefix properties have been added to the Source, manually load a QVD first; then, a QVD “Re-Sync” can be scheduled, with the “Load Data” box checked

Additional Mandatory Configuration

Three additional initial steps are required.

(1) Configure Sense API Authentication on Qlik Catalog Linux Server

Copy the five certificate files from the Qlik Sense “Catalog Instance” to a “certs” directory in the same directory as the OpenConnector script (e.g., /usr/local/qdc/qlikcore/certs). The “certs” directory should contain files client.pem, client_key.pem, root.pem, server.pem and server_key.pem. The directory must be named “certs”. (Use the process previously described here, but do so on the Sense ***Catalog*** Instance).

(2) Configure QVD Decryption on the Sense "Catalog Instance"

QVDs are encrypted using a **certificate** on the Sense "Analytics Instance." This certificate must be *exported* from the Sense "Analytics Instance" and then *imported* to the Sense "Catalog Instance" to enable decryption. This process for exporting and importing is described in detail in the following Qlik Sense Help article:

https://help.qlik.com/en-US/sense-admin/November2020/Subsystems/DeployAdministerQSE/Content/Sense_DeployAdminister/QSEoW/Administer_QSEoW/Managing_QSEoW/encryption-certificates.htm#Specifyi

(3) Create a Shared “dropbox” Directory on the Qlik Catalog Linux Server

The Qlik Sense "Catalog Instance" requires a directory on the Qlik Catalog server for temporary output of CSV files. Create a directory on the Qlik Catalog (Linux) server, which can be accessed by the Qlik Sense "Catalog Instance" (Windows). In the above table, the “Catalog Instance” writes CSV files to “qs.catalog.instance.output.path=\\\\catalog1\\dropbox”. “catalog1” is the name of the Qlik Catalog Linux host. Qlik Catalog retrieves the CSV files from “catalog.linux.instance.output.path=/usr/local/qdc/dropbox”.

The following instructions describe how to configure the required output directory on the Qlik Catalog server:

Create CSV file output directory:

```
# mkdir -p /usr/local/qdc/dropbox
# chmod -R 0775 /usr/local/qdc/dropbox
# chown -R nobody:nobody /usr/local/qdc/dropbox
```

If SELinux is enabled:

```
# chcon -t samba_share_t /usr/local/qdc/dropbox
```

Install Samba and Winbind packages for Windows interoperability:

```
# yum install -y samba samba-client samba-common authconfig samba-winbind samba-winbind-clients ntpdate
```

Add Active Directory hostname of Qlik Catalog Linux server to /etc/hosts (if record does not exist in DNS):

```
# vi /etc/hosts
10.118.1.83            catalog1.ad.podiumdata.net       catalog1
```

Modify Samba configuration file **/etc/smb.conf**:

NOTE: The following is a *sample* configuration file using Qlik development resources. Customer will need to provide environment-specific values for the fields with **bold** font.

```
# vi /etc/samba/smb.conf
```

Add the following to the "global" section of smb.conf:

```
[global]
  workgroup = AD
  password server = sid2.ad.podiumdata.net
  realm = AD.PODIUMDATA.NET
  security = ads
  idmap config * : range = 16777216-33554431
  template shell = /bin/bash
  kerberos method = secrets only
  winbind use default domain = true
  winbind offline logon = true

  # netbios name: enter the hostname of the Qlik Catalog linux server
  # the name defined will appear in Windwos network broadcast
  netbios name = catalog1

  map to guest = bad user
  dns proxy = no
  passdb backend = tdbsam

  # hosts allow: enter IP address of the Sense "Catalog Instance"
  hosts allow = 10.118.0.121
```

Add the following to the bottom of the smb.conf file:

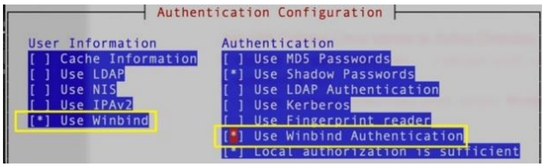
```
# Define share information
# The name within the brackets will appear in Windows network broadcast
[dropbox]
  comment = CSV Output Directory for Qlik Sense "Catalog Instance"
  path = /usr/local/qdc/dropbox
  valid users = @qdc
  create mask = 765
  force create mode = 765
  security mask = 765
  force security mode = 765
  browsable = yes
  writable = yes
  guest ok = yes
  read only = no
  force user = qdc
  force group = qdc
```

Join Qlik Catalog Linux server to Active Directory

# ntpdate ad.podiumdata.net   (replace with customer Active Directory name)

# authconfig-tui

- Leave default selections plus select **Use Winbind** and **Winbind Authentication**

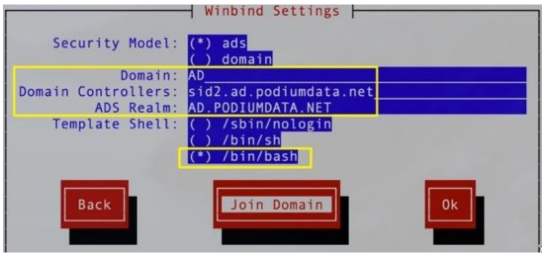


```
Authentication Configuration

User Information              Authentication
[ ] Cache Information         [ ] Use MD5 Passwords
[ ] Use LDAP                  [*] Use Shadow Passwords
[ ] Use NIS                   [ ] Use LDAP Authentication
[ ] Use IPAv2                 [ ] Use Kerberos
[*] Use Winbind               [ ] Use Fingerprint reader
                              [*] Use Winbind Authentication
                              [*] Local authorization is sufficient
```

- Verify Domain, Domain Controllers, and ADS Realm

- Template Shell: select /bin/bash



```
Winbind Settings

    Security Model: (*) ads
                    ( ) domain
            Domain: AD
Domain Controllers: sid2.ad.podiumdata.net
         ADS Realm: AD.PODIUMDATA.NET
    Template Shell: ( ) /sbin/nologin
                    ( ) /bin/sh
                    (*) /bin/bash
```

# systemctl restart winbind

Add Qlik Sense service account to Qlik Catalog service account group:

# usermod sense-service -aG qdc

# id sense-service   (verify QDC service account group membership)

Set Samba services to auto-start at during boot:

# systemctl enable smb.service

# systemctl enable nmb.service

# systemctl start smb.service

# systemctl start nmb.service

Create firewall exception for samba:

# firewall-cmd --permanent --zone=public --add-service=samba

# firewall-cmd --reload

Test

On the Sense “Catalog Instance”, open a Command Prompt, using “Run as a Different User” – enter the credentials for the Windows DOMAIN\username that is running the Qlik Sense Engine Service. Using the prompt, test two items:

- Test reading of a file from the Sense Analytics Instance using the UNC path (e.g., \\DUCKS-SENSE1\qvd-share\data.qvd)
- Test writing of a file to the Qlik Catalog Linux server using the UNC path (e.g., \\catalog1\dropbox\test.txt)

Alternate Configuration

There is one alternate configuration: if all Sources will share the same two prefix properties, the two prefixes may be set globally rather than being set for every Source. If this is the case, replace this line in the core_env property:

```
%prop.qs.analytic.instance.input.path.prefix %prop.qs.catalog.instance.input.path.prefix \
```

Instead, use this line:

```
qs.analytic.instance.input.path.prefix=C:\\qvd-share qs.catalog.instance.input.path.prefix=\\\\DUCKS-SENSE1\\qvd-share \
```

Publish to Qlik

The following instructions detail the setup for Qlik Catalog (server-side) to push data to Qlik Sense (webapp client-side) through the launch of node.js script.

NOTE:

- If Active Directory Qlik Sense users have not yet been imported in Qlik Catalog STOP and follow the instructions in the Appendix for importing Active Directory users.
- Publish to Qlik is not currently supported for Qlik Catalog deployments running on Oracle (metadata database).

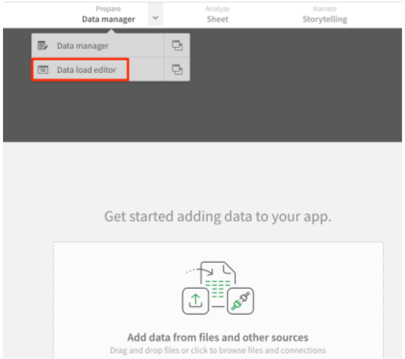
1. Create a Connector in Qlik Sense

Single Node Deployments: Create A Connector to PostgreSQL

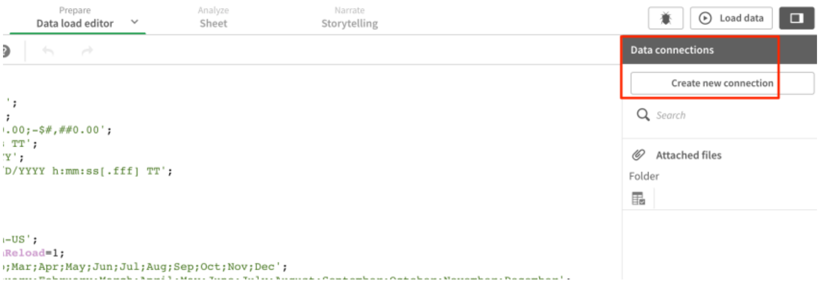
When publishing to Qlik Sense from Qlik Catalog running in a Single Node configuration (versus multi-node/ Hadoop deployment) users should create a ***connector*** to the PostgreSQL distribution tables that hold views of the entities and data in Qlik Catalog.

The following steps demonstrate creation of a PostgreSQL connector. (These steps are consistent with the creation of any type of Qlik Sense connector). More information about creating PostgreSQL connectors in Qlik Sense can be found here.

1) Log into Qlik Sense *using an Active Directory account which also exists in Catalog*.
2) Select **Create New App** > enter **Name Of My App** > click **Create**
3) Select **Open App.**
4) New browser tab opens. Navigate to **Prepare: Data Manager** at the top of the screen. Select **Data Load Editor** from the drop-down list.


Prepare
Data manager
Analyze
Sheet
Narrate
Storytelling
Data manager
Data load editor
Get started adding data to your app.
Add data from files and other sources
Drag and drop files or click to browse files and connections

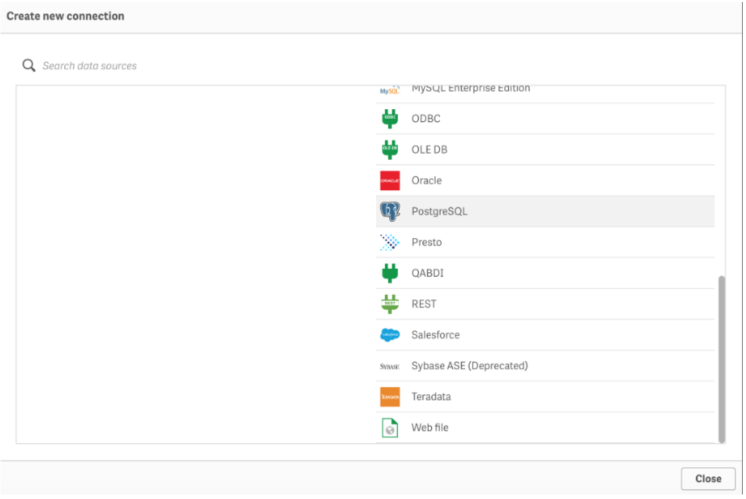
5) Select **'Create new connection'** from ‘**Data connections’** sidebar on right side of screen:



```
';
;
.00;-$#,##0.00';
 TT';
Y';
D/YYYY h:mm:ss[.fff] TT';


-US';
Reload=1;
;Mar;Apr;May;Jun;Jul;Aug;Sep;Oct;Nov;Dec';
```

6) Select ‘PostgreSQL’ data source from popup displaying available data source types.



7) Complete the following fields in the PostgreSQL Connection dialog box that opens:

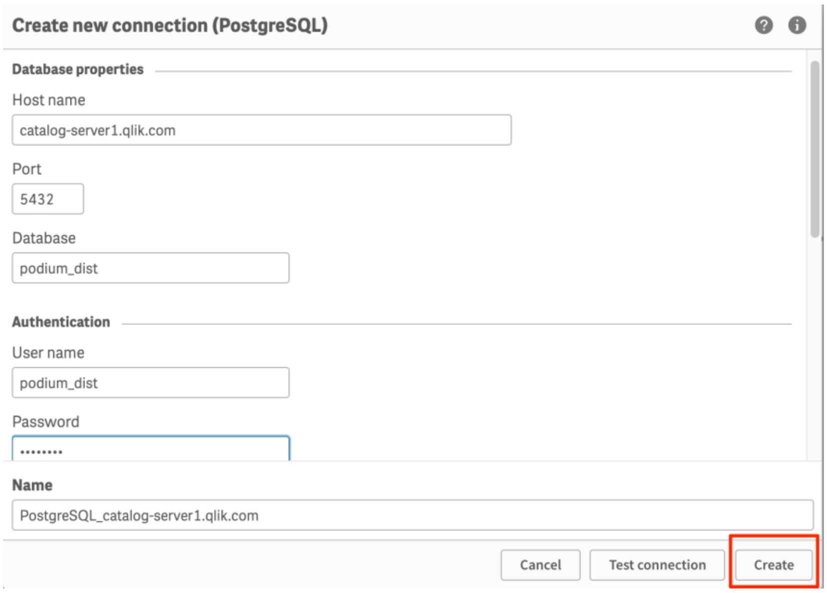
Database Properties
Hostname: Enter the host name of the Qlik Catalog server
Port: Enter the TCP port that PostgreSQL is listening on (defined in postgresql.conf)
Database: ***podium_dist***

Authentication Information
User name: ***podium_dist***
Password: enter the password associated with the PostgreSQL user. Default for podium_dist is**: *nvs2014!*)**

SSL Options
SSL Mode: *prefer*

8) **Test** the connection.
9) Click **Create** to save the connection. Once created the connector populates in the right sidebar.
10) Note the **NAME** of the new connection since it will be needed later in the guide. The name will look something like this by default:

PostgreSQL_catalog-server1.qlik.com (domain_username)



Create new connection (PostgreSQL)

Database properties

Host name: catalog-server1.qlik.com

Port: 5432

Database: podium_dist

Authentication

User name: podium_dist

Password: ••••••••

Name: PostgreSQL_catalog-server1.qlik.com

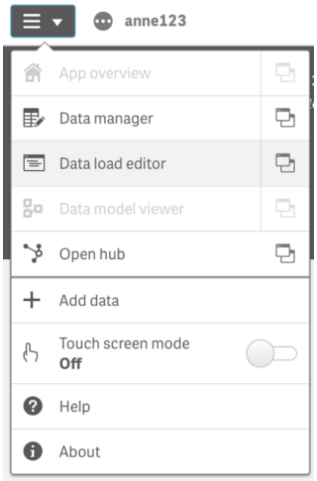
Multi-Node Deployments: Create A Connector to Hive

When publishing to Qlik Sense from Qlik Catalog running in a Multi-Node Hadoop environment, users should create a ***connector*** to the **Hive** distribution tables that hold views of the entities and data in Catalog.

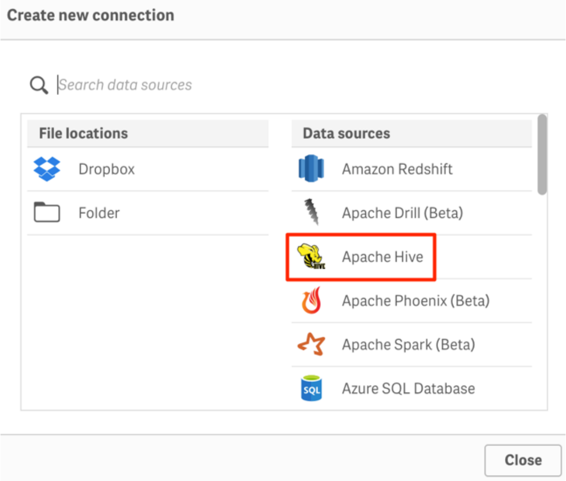
The following steps demonstrate creation of a Hive connector. (These steps are consistent with the creation of any type of Qlik Sense connector).

More information about creating Hive connectors in Qlik Sense can be found here.

1) Log into Qlik Sense.
2) Select **Create New App** > enter **Name Of My App** > click **Create**
3) **App Overview** opens. Select **Data Load Editor** from upper-left drop-down



4) Select 'Create new connection' from ‘Data connections’ sidebar on right side of screen. Select ‘Hive’ data source from popup displaying available data source types.



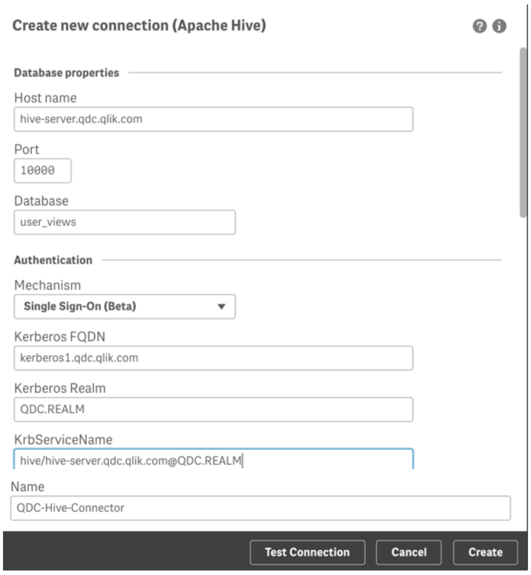
5) Complete the following fields in the Apache Hive Connection dialog box that opens:

Database Properties

Hostname: Enter the host name of the server running the Hive Server for the Hadoop cluster
Port: Enter the TCP port that Hive is listening on (typically 10000)
Database: user_views

Authentication Information

Mechanism: Single Sign-On
Kerberos FQDN: Enter the fully-qualified domain name of the Kerberos authentication server. (In Active Directory environments this would be a domain controller).
Kerberos Realm: Enter the Kerberos realm associated with the Hadoop cluster
KrbServiceName: Enter the cluster Kerberos service principal being used by Hive
Name: Enter a name for the Hive connector



Create new connection (Apache Hive)

Database properties

Host name: hive-server.qdc.qlik.com

Port: 10000

Database: user_views

Authentication

Mechanism: Single Sign-On (Beta)

Kerberos FQDN: kerberos1.qdc.qlik.com

Kerberos Realm: QDC.REALM

KrbServiceName: hive/hive-server.qdc.qlik.com@QDC.REALM

Name: QDC-Hive-Connector

6) **Test** the connection.

7) **Save** the connection. Once created the connector populates in the right sidebar.

2. Copy Certificates from Qlik Sense Server to Qlik Catalog node

(This step may be skipped if already completed for the QVD Import integration)

1) Export certificates from Qlik Sense using the Qlik Management Console (QMC).

To export the public and private keys from a Qlik Sense server, please see https://help.qlik.com/en-US/sense/June2019/Subsystems/ManagementConsole/Content/Sense_QMC/export-certificates.htm

The default location for the exported certificates is the following directory ***on the Qlik Sense server***:

```
C:\ProgramData\Qlik\Sense\Repository\Exported Certificates
```

(A folder will be created within the "Exported Certificates" directory with whatever name is entered during the export process described in the link above).

2) Copy the certificates exported in step1 from the Qlik Sense server into the "**certs"** directory on the Qlik Catalog server. The **certs** directory will be located in the QDC_HOME directory. (QDC_HOME was defined during the Qlik Catalog installation process. The installation default is /usr/local/qdc/qlikpublish/certs). The following files should be copied:

```
client.pem
client_key.pem
root.pem
server.pem
server_key.pem
```

3. Configuration of *core_env.properties* file on Qlik Catalog machine

Set the following properties in the ***core_env.properties*** file. The core_env.properties is located in the TOMCAT_HOME/conf directory. (TOMCAT_HOME was defined during the Qlik Catalog installation process. The installation default is /usr/local/apache-tomcat-<version-number>).

- **is.publish.to.qlik.enabled**: Set this property to ***true*** to display the 'Publish to Qlik' option in the Catalog UI cart checkout:

  ```
  is.publish.to.qlik.enabled=true
  ```
  (Note that the user must logout and login to see the button after core_env refresh.)

- **podium.qlik.dataconnection.name**: Set this property to the NAME of the data connection created in Qlik Sense (Publish To Qlik Part 1 – Step 7 above):

  Example:
  ```
  podium.qlik.dataconnection.name= PostgreSQL_QDC.qlik.com(ad_qdc1)
  ```

- **podium.qlik.qsockclient.script.directory**: Path to qsocks client script directory. This is the directory where qsock client scripts are placed and usedfor creating, updating, and listing apps. The default location is $QDC_HOME/qlikpublish.

  Example:
  ```
  podium.qlik.qsockclient.script.directory=/usr/local/qdc/qlikpublish
  ```

- **qlik.sense.url:** URL to Qlik Sense Server. It should be defined using the following format:

  qlik.sense.url=https://<**qliksense-host-ip-address-or-host-name>**/sense/app/<podium-gen-app-id>

  Note: The URL must end with "<podium-gen-app-id>" as shown in the examples below. Qlik Catalog generates this value and will substitute it into the URL when Publish To Qlik is invoked.

  Examples:

  ```
  qlik.sense.url=https://10.111.2.163/sense/app/<podium-gen-app-id>
  qlik.sense.url=https://sense01.dev.qlik.com/sense/app/<podium-gen-app-id>
  ```

- **qlik.sense.active.directory.name**: Directory name (aka domain name) which is combined with either the logged in user name or property 'podium.qlik.username'. Qlik Sense applications are then listed and created/updated using the user represented by this combination. This user should have previously logged in to Qlik Sense. Required property when 'is.publish.to.qlik.enabled' is set to true.

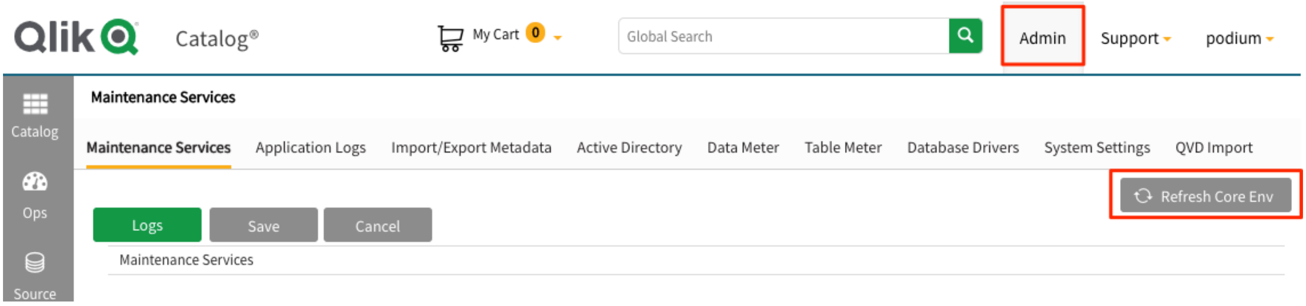
  Multiple directories may be specified by using commas to separate each. In this case, Qlik Sense will be queried for each directory\user combination -- if that user previously logged in, that directory\user combination will be used for Publish to Qlik operations.

  Examples:
  ```
  qlik.sense.active.directory.name=QLIKTECH
  qlik.sense.active.directory.name=ACME-US,ACME-EU
  ```

  If multiple directories are specified in property 'qlik.sense.active.directory.name', then a Qlik Sense 'RootAdmin' user is required to query Qlik Sense. Enter the directory and user names of a 'RootAdmin' user using properties 'qlik.sense.root.admin.directory.name' and 'qlik.sense.root.admin.user.name'.

After setting the property values above within core_env.properties:

1) Login to Qlik Catalog with administrative permissions and "Refresh Core Env"

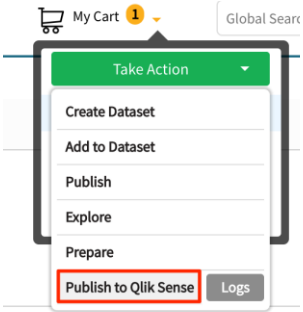


2) Logout of Qlik Catalog

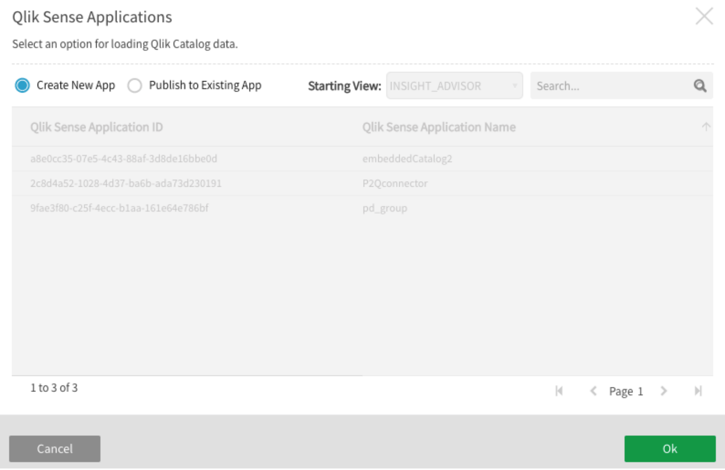
3) Log back into Qlik Catalog *using the account that was used to create the Postgres Connector* above. A Publish To Qlik option will now appear in UI cart checkouts.

4) To Publish To Qlik Sense:

1) Add a data set into the cart
2) From the Cart menu, Select **Take Action** > ***Publish To Qlik Sense*** option



3) Accept "Create New App" default > click **OK**. This action will spawn a new browser tab which connects to Qlik Sense. (Pop-up blocker authorization may be required for new tab)


Qlik Sense Applications

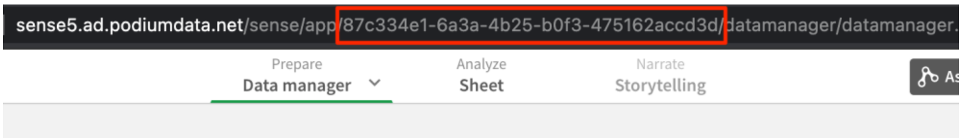
Select an option for loading Qlik Catalog data.

● Create New App ○ Publish to Existing App   Starting View: INSIGHT_ADVISOR

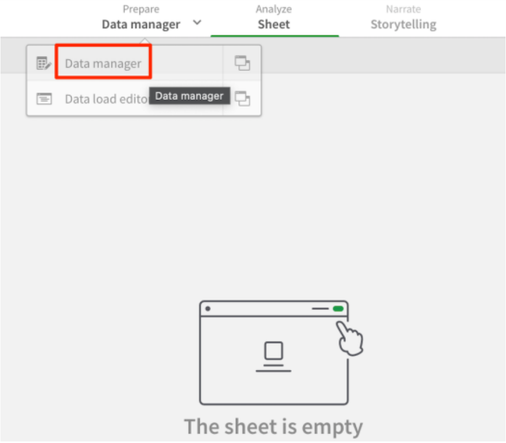
Qlik Sense Application ID	Qlik Sense Application Name
a8e0cc35-07e5-4c43-88af-3d8de16bbe0d	embeddedCatalog2
2c8d4a52-1028-4d37-ba6b-ada73d230191	P2Qconnector
9fae3f80-c25f-4ecc-b1aa-161e64e786bf	pd_group

1 to 3 of 3   Page 1

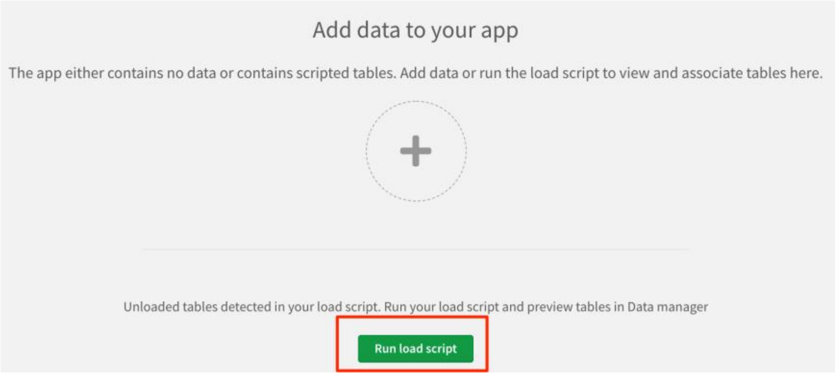
Note: Qlik Catalog generates the <podium-gen-app-id> value used in the URL when Publish To Qlik is invoked. This value becomes the application (or report) id/url in Qlik Sense


sense5.ad.podiumdata.net/sense/app/87c334e1-6a3a-4b25-b0f3-475162accd3d/datamanager/datamanager.

4) Within the new Qlik Sense tab, select **Data Manager**



e. Click Run Load Script


Add data to your app

The app either contains no data or contains scripted tables. Add data or run the load script to view and associate tables here.

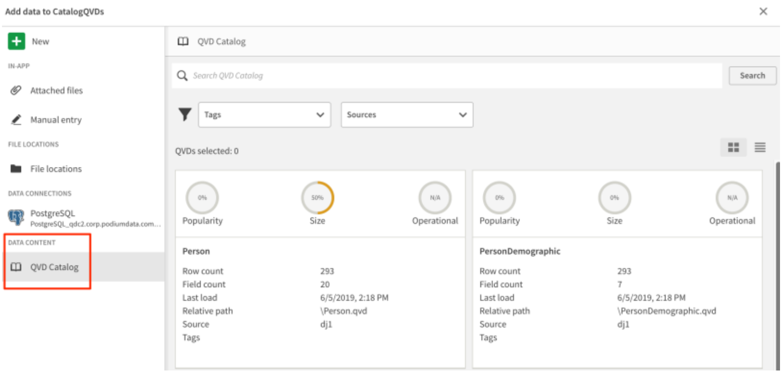
Unloaded tables detected in your load script. Run your load script and preview tables in Data manager

Congratulations! Publish to Qlik is now configured.

Embedded Catalog in Qlik Sense

There is a simplified version of Catalog embedded in Sense.

1) Open Qlik Sense hub
2) **Create** a new app and **Open** the app
3) Click "**Add Data from files and other sources**" in the middle of the screen
4) In the menu to the left, click QVD Catalog. Available QVDs display



QVDs selected: 0

Person

Row count	293
Field count	20
Last load	6/5/2019, 2:18 PM
Relative path	\Person.qvd
Source	dj1
Tags	

PersonDemographic

Row count	293
Field count	7
Last load	6/5/2019, 2:18 PM
Relative path	\PersonDemographic.qvd
Source	dj1
Tags	

Notes on User Access to QVDs in Qlik Sense and Catalog

Background: QVD Import is configured by a Catalog user with ADMIN role access. However, when a "normal" user, sync'ed from Active Directory, logs into Catalog, that user does so with ANALYST role access. When a user logs in, Catalog makes an API call to Sense to determine those Data Connections to which the user has access. Only QVDs (Entities) in Groups mapping to permitted Data Connections are seen by normal ANALYST users in Catalog. The same logic applies to the embedded Catalog in Sense (although the Sources drop-down is not currently filtered).

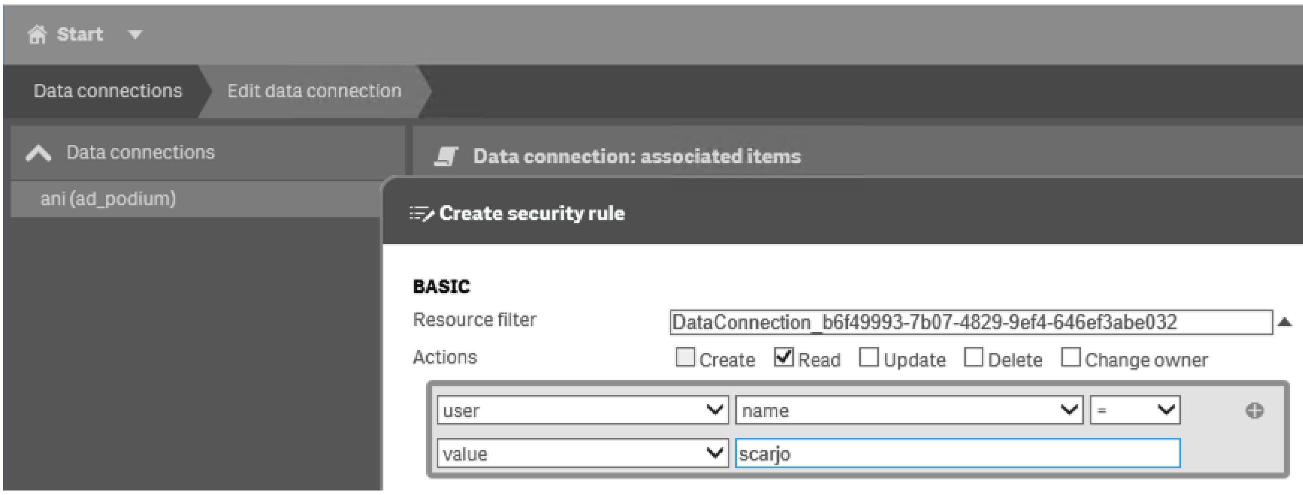
In summary: if an AD user logged into Sense can view a QVD, then the same AD user logged into Catalog should be able to view the same QVD.

There are a variety of techniques to manage the QVDs to which a Sense user has access -- this is a Sense administration topic covered elsewhere. However, below, two techniques are discussed for the novice administrator.

(1) Security Rules

Using the Qlik Management Console, Security Rules can be configured to grant Users access to Data Connections.

1. Select a specific Data Connection. Select the Security rules tab. Create an associated rule. Fill in the user value with the user's login name.



BASIC

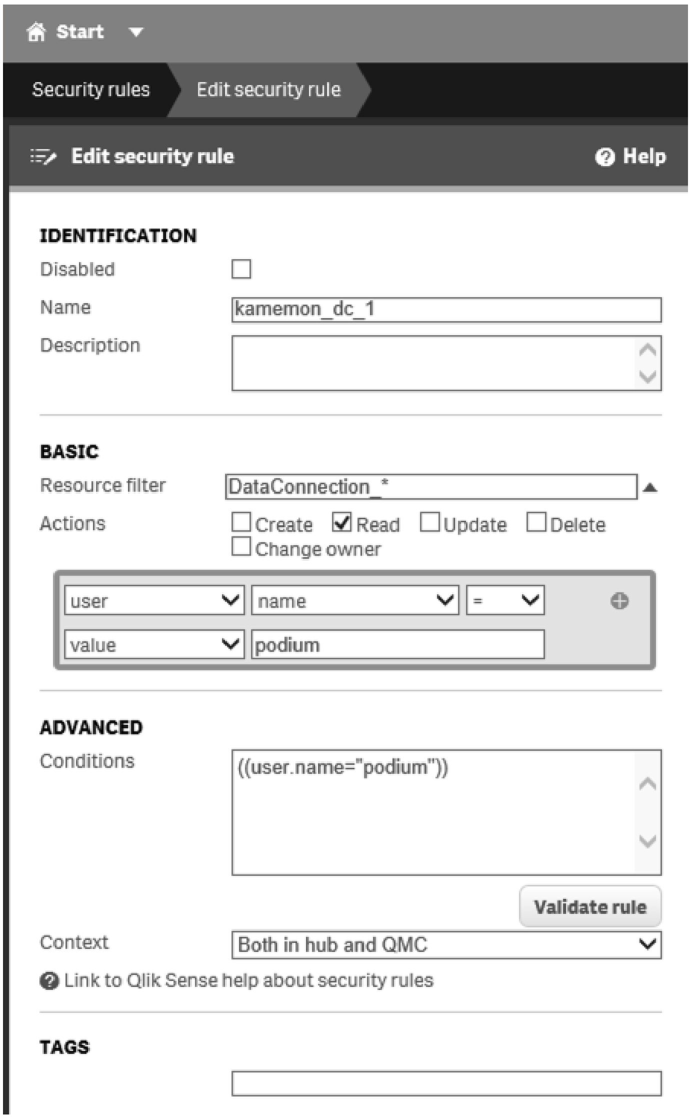
Resource filter: DataConnection_b6f49993-7b07-4829-9ef4-646ef3abe032

Actions: □ Create ☑ Read □ Update □ Delete □ Change owner

user | name | =

value | scarjo

2. Alternative: Go to Security Rules. Create new. Specify a resource filter consisting of a DataConnection, possibly using a wildcard. Specify a user name filter.



IDENTIFICATION

Disabled: □

Name: kamemon_dc_1

Description:

BASIC

Resource filter: DataConnection_*

Actions: □ Create ☑ Read □ Update □ Delete □ Change owner

user | name | =

value | podium

ADVANCED

Conditions: ((user.name="podium"))

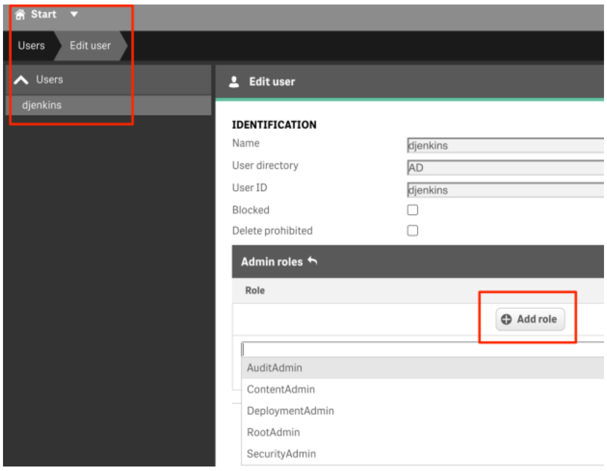
Context: Both in hub and QMC

TAGS

(2) Add Role to User

The Qlik Sense user can be granted appropriate user *role* to display Catalog QVDs within Qlik Sense. Roles may be assigned to users by administrators within the Qlik Management Console:

1. Login to QMC with rootAdmin permission
2. Navigate to Users
3. Select user acount > Edit
4. Add role with sufficient priviledge



IDENTIFICATION

Name djenkins

User directory AD

User ID djenkins

Blocked □

Delete prohibited □

Appendix

1. Configuring Qlik Catalog to Validate a Certificate Issued by an Internal Certificate Authority

Many Qlik Sense servers are assigned certificates issued by an internal Certificate Authority (e.g., Active Directory), or use self-signed certificates. By default, Qlik Catalog will trust such certificates as the Qlik Sense server is presumed to be within the corporate firewall. To not trust these certificates, and require Qlik Catalog to validate them, uncomment the property **qlik.trust.all.certs** within **core_env.properties** and set it to **false**.

When this property is set to false, the SSL certificate presented by the Qlik Sense server will be validated. In order to validate it, you must acquire the CA Root certificate (or self-signed certificate) and add it to the Java runtime's cacerts file. Instructions for this process follow.

Importing a Certificate Authority (CA) root certificate into the JVM Trust Store

1. *Obtain the root certificate and copy it to the Qlik Catalog server*

   The Qlik Sense “self-signed” root certificate can be found on the Qlik Sense server in the following directory:

   ```
   C:\ProgramData\Qlik\Sense\Repository\Exported Certificates\.Local Certificates\root.pem
   ```

   If the Qlik Sense server is using a certificate issue by an internal Certificate Authority, the root certificate must be obtained from the internal Certificate Authority.

2. *Convert the root certificate to DER format*

   This can be done with help of the **openssl** toolkit, where root.pem is the original certificate filename in PEM format, and root.der the filename to output, in DER format (which the Java keytool utility can understand).

   ```
   openssl x509 -in root.pem -inform pem -out root.der -outform der
   ```

3. *Validate the root certificate content*

   Ensure that the Java keytool can parse the certificate and display its content:

   ```
   keytool -v -printcert -file root.der
   ```

4. *Import the root certificate into the JVM trust store*

   Enter the following command where $JAVA_HOME is a shell environment variable that points to your Java installation:

   - The Qlik Catalog JAVA_HOME is defined in the Tomcat ***setenv.sh*** configuration file located in the /bin directory of the Tomcat instance being used by QDC:

     e.g. /usr/local/qdc/apache-tomcat-7.0.94/bin/setenv.sh

   - For “alias” pick some unique name for the certificate in the store. e.g. “qliksense” or “internalCA”

     ```
     keytool -importcert -alias qliksense -keystore $JAVA_HOME/jre/lib/security/cacerts -storepass changeit -file root.der
     ```

     (the default password for the CA store is: changeit)

   The keytool will prompt you for confirmation, enter yes to complete the operation.

5. *Verify that the root certificate has been imported*

   List the trust store content and filter for the certificate alias (name) with grep:

   ```
   keytool -keystore "$JAVA_HOME/jre/lib/security/cacerts" -storepass changeit -list | grep qliksense
   ```

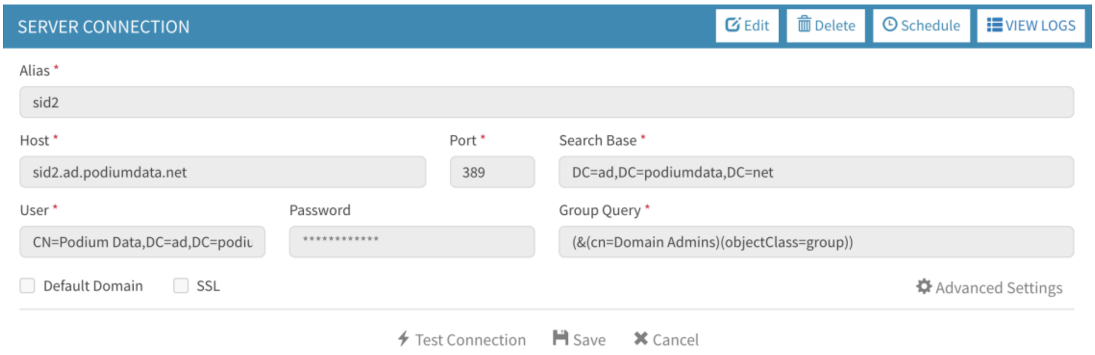
6. *Restart the Qlik Catalog Tomcat instance*

2. Qlik Catalog Active Directory User Import

Qlik Catalog can sync existing users and their groups from AD by specifying the necessary parameters in the Qlik Catalog UI within the **Admin** section.

Example Qlik Catalog Active Directory Server Connection:

Alias: sid2
Host: sid2.ad.podiumdata.net
LDAP Port: 389
Active Directory/LDAP Search Base: DC=ad,DC=podiumdata,DC=net
Active Directory/LDAP Search User: CN=Podium Data,DC=ad,DC=podiumdata,DC=net
Active Directory/LDAP Search User Password: Qwerty123!
Active Directory/LDAP Group Query (filter): (&(cn=Domain Users)(objectClass=group))



SERVER CONNECTION

Alias *: sid2
Host *: sid2.ad.podiumdata.net
Port *: 389
Search Base *: DC=ad,DC=podiumdata,DC=net
User *: CN=Podium Data,DC=ad,DC=podiu
Password: ************
Group Query *: (&(cn=Domain Admins)(objectClass=group))
□ Default Domain □ SSL

About Qlik

Qlik is on a mission to create a data-literate world, where everyone can use data to solve their most challenging problems. Only Qlik's end-to-end data management and analytics platform brings together all of an organization's data from any source, enabling people at any skill level to use their curiosity to uncover new insights. Companies use Qlik products to see more deeply into customer behavior, reinvent business processes, discover new revenue streams, and balance risk and reward. Qlik does business in more than 100 countries and serves over 48,000 customers around the world.

LEAD WITH DATA™