

PoC Install Guide for Qlik Sense Enterprise

November 2018

This document guides you in the preparation, installation and configuration of a Qlik Sense Enterprise server used for evaluation or proof of concept (PoC) deployments. It is NOT meant to be used for production deployments of Qlik Sense.





TABLE OF CONTENTS

Qlik Sense Enterprise for Windows Installation Prerequisites	5
Qlik Sense Cloud Services Prerequisites	6
Server Prerequisites	6
Windows Prerequisites	7
User Accounts	7
Service Account Setup	7
Windows File Share Setup	10
Download Qlik Sense	13
Run the Qlik Sense Installer	14
Launch Qlik Management Console Setup	18
Apply License	18
Token Allocation	19
Professional/Analyzer Allocation	20
PoC License Rule	20
Proxy Setup	21
Configure Security	24
Connect to Qlik Cloud Services	24
Custom Properties	25
Distribution Policy	25
Deploy an Application	25
Option #1 – Use HTTP	26
Option #2 – Use a trusted certificate	26
Desktop Authentication Link Setup	27
Security Rule Setup	27
Connect to the Qlik Sense Enterprise Server	29
Security Groups	34

Key Pair	34
Launch the Instance	35
Elastic IP	36
RDP	36
Windows 2012 & 2016	44
Generate Certificate Signing Request for Trusted Certificate	45
Import Certificate to Windows Certificate Store	45
Import Certificate Thumbprint to Qlik Sense Proxy	47
Log Files	50
Connection Lost	50
HTTP 500 Error	50
Could not start services in a timely manner	50

How to Use This Guide

Qlik Sense can be deployed in a multitude of environments. While this guide tries to keep all deployments the same, some variation may be required because of the deployment environment. These variations are identified throughout the document with the graphics below:

Location		Domain	
Instance installed on Amazon EC2 or Microsoft Azure	Instance installed on a Virtual Machine or Physical Server	Windows is on domain controller (Active Directory)	Windows is on local domain (No Active Directory)
			

Do not start the installation of Qlik Sense until you have answered the questions and satisfied the prerequisites outlined in the next section.

Before You Begin

Please review and attend to the following prerequisites before starting the Qlik Sense installation.

Qlik Sense Enterprise for Windows Installation Prerequisites

1. Determine where Qlik Sense Enterprise is to be installed. Supported environments include, a virtual machine on premise, a physical server, or a cloud provider (such as Amazon, Azure or Google Cloud Platform).
2. Determine whether the Windows Server will be connected to a domain controller.
3. Validate that the target server meets the following requirements:
 - Windows 2012, Windows 2012 R2, or Windows 2016 – 64 bit. (Note Windows 7, 8.1 and 10 can be used in some situations but is not recommended).
 - At least 4 cores and 16 GB of RAM is recommended, but this will depend on data volumes and the number of users accessing the server.
 - A clean Windows Server OS installation is desirable.
 - Microsoft .NET 4.5.2 installed and updates applied (the default is 4.5 for Windows 2012). The Qlik Sense installation software will automatically install or update .NET if required.
 - IPv4, IPv6, IPv4 and IPv6 (dual stack)
 - Internet access from server is needed for license registration. If Internet access is not available, you will need to obtain an LEF file from a Qlik representative to license the server.
4. Obtain administrative rights and Remote Desktop access to the target server.
5. Obtain a service account with local administrative rights on the server. Ideally the service account will be a domain account if the server is attached to a domain controller, but a local account will also work.
6. Install database drivers on the server for any databases that Qlik Sense needs to access.
7. Identify data sources and credentials for any database that Qlik Sense needs to access.
8. Obtain the Qlik Sense Enterprise site license (serial number and control number). If the server on which you will be installing Qlik Sense does not have Internet access, you will need to obtain an LEF file from a Qlik representative.
9. Client browser requirement:
 - **Windows 7:** IE 11, Chrome, Firefox
 - **Windows 8.1:** IE 11, Chrome, Firefox
 - **Windows 10:** Edge, IE 11, Chrome, Firefox
 - **OS X 10.11 and 10.12:** Safari, Chrome, Firefox
 - **iOS:** iOS 10.3.2 or above, iOS 11 recommended
 - **Android 4.3, 4.4.4, 5.1.1, and 6.0:** Chrome
 - **Windows Phone 8.1:** IE 11

Qlik Sense Cloud Services Prerequisites

For Proof of Concepts involving Qlik Cloud Services, have the prerequisites completed before beginning a PoC. If you are not using Qlik Cloud Services, you can skip this section.

1. Have a license ready. Ensure that CLOUD_SERVICES;YES;; in the LEF.
2. Obtain a subdomain on qlikcloud.com and have the information provided during registration ready. For your subdomain, use the format POC{company}.{region}.qlikcloud.com.
3. Have Identity Provider (IdP) configuration ready that conforms to OpenID and SAML (ex: Auth0, Okta). It is highly recommended to have prep call in advance with the security administrators of the IdP and have them available to work together on IdP configuration.

Qlik Presales: Contact an Enterprise Architect for help with this.

Server Prerequisites



If you are installing into Amazon EC2 follow the steps in the **Appendix: Amazon EC2 – Launch an Instance**. At this point, make sure you can RDP to the server and that ports 80, 443 are open in the EC2 console.



If you are installing into Microsoft Azure follow the steps in the **Appendix: Microsoft Azure – Launch an Instance**. At this point, make sure you can RDP to the server and that ports 80, 443 are open in the Azure console.



If you are installing onto physical hardware or a virtual machine on premise, make sure you can RDP to the server at this point.

Windows Prerequisites



If you plan to rename the machine or workgroup, **do so before installing Qlik Sense.**



Disable Windows Firewall completely (if this is not acceptable, open inbound ports 80, 443). For help with this, see **Appendix: Windows Firewall.**



Disable Windows Internet Explorer Enhanced Security Configuration (IE ESC). For help with this, see **Appendix: IE Enhanced Security Configuration.**



Download and install Chrome on the server (**optional**). The Chrome browser is faster than IE.



If another installation of Qlik Sense already exists on this machine, follow the cleanup steps outlined in **Appendix: Qlik Sense Uninstall.**



If other software is installed on this machine, check for known conflicts – IIS, Skype, VMWare Workstation, Tableau, and SQL Server all are known to use port 443. These should be disabled and/or configured to not use port 443. For additional information, see **Appendix: Known Conflicts.**

User Accounts

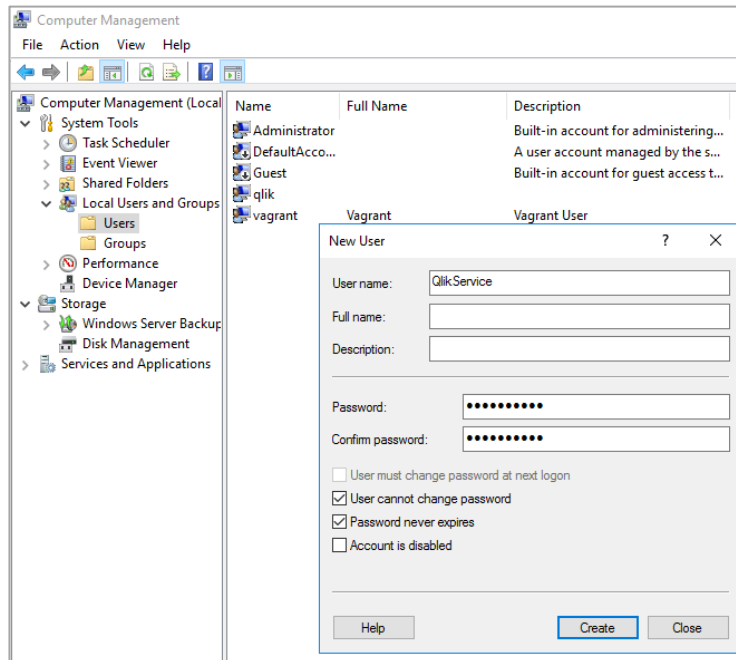
Service Account Setup

If you do not already have a service account to run Qlik Sense, follow the procedures below to create one; otherwise, you can move on to the User Account Setup section.

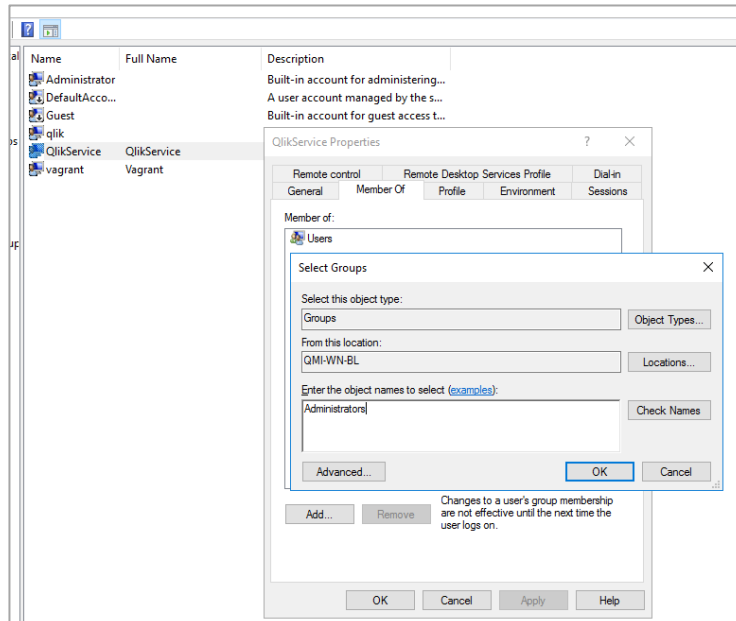
- On the Qlik Sense server, Click **Start** and search for **Computer Management**.



- Find the **Users** folder, then click **Action > New User...**
- Enter user name **QlikService** and password **Qlik1234!**
- Uncheck **User must change password at next logon**
- Check **User cannot change password** and **Password never expires**
- Click **Create**



- Double click on **QlikService**
 - Click **Member Of**
 - Click **Add...**
 - Type **Administrators**
 - Click **Check Names**
 - Click **OK**



This account will be used during the installation of Qlik Sense.

User Account Setup



If the server is connected to a domain controller (Active Directory), skip this section and move on to the Installation section.

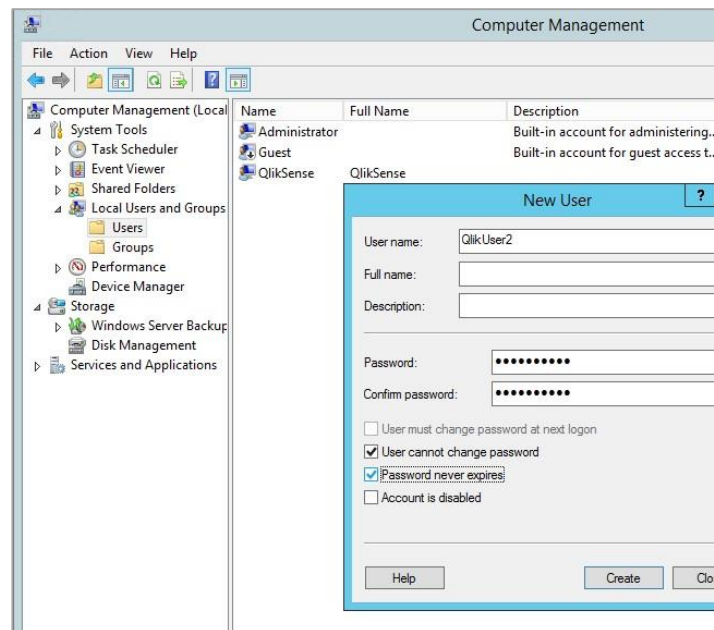


If the server is **NOT** connected to a domain controller, follow the procedures below to create some local users that can be used to login into Qlik Sense.

- On the Qlik Sense server, Click **Start** and search for **Computer Management**.



- Find the **Users** folder, then click **Action > New User...**
- Add user **QlikUser1**
 - Password **Qlik1234!**
 - Uncheck **User must change password at next logon**
 - Check **User cannot change password**
 - Check **Password never expires**
- Click **Create**
- Repeat steps above for **QlikUser2** and **QlikUser3**

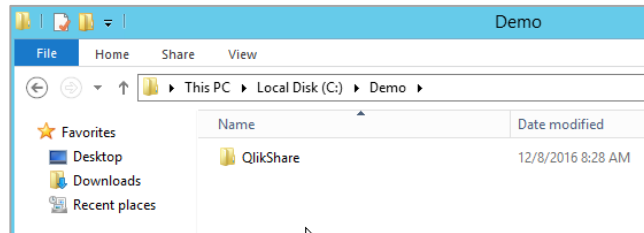




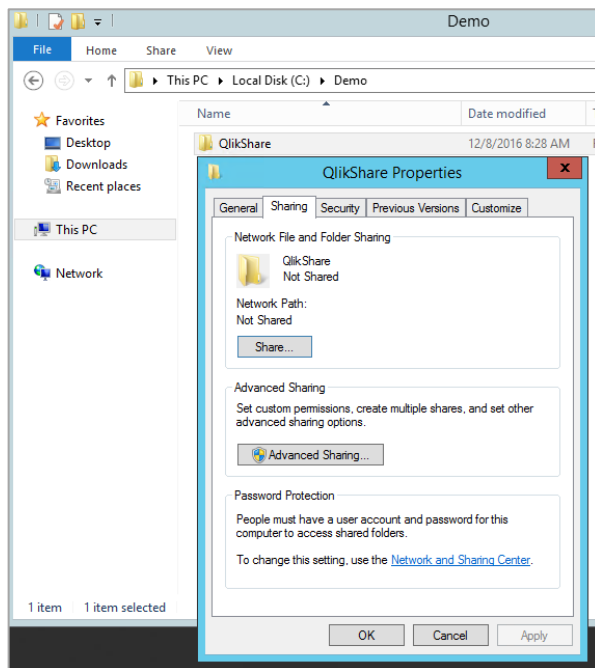
These will be the user accounts and passwords you hand out so people can login and evaluate Qlik Sense. You can add more or fewer user accounts based on your needs. You can also use different user names and passwords if desired.

Windows File Share Setup

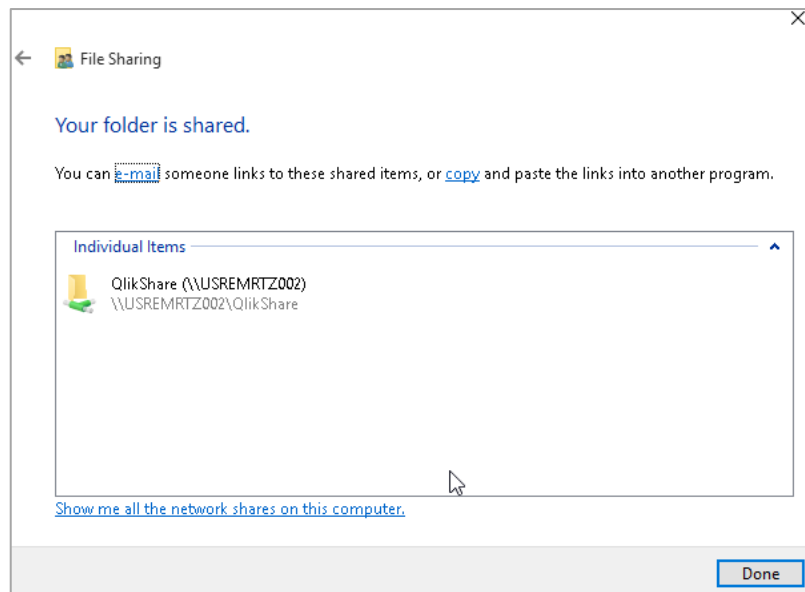
- Navigate to “D:\” and create a folder titled “QlikShare” (If there is no D:\ available then use C:\ or preferred attached drive).



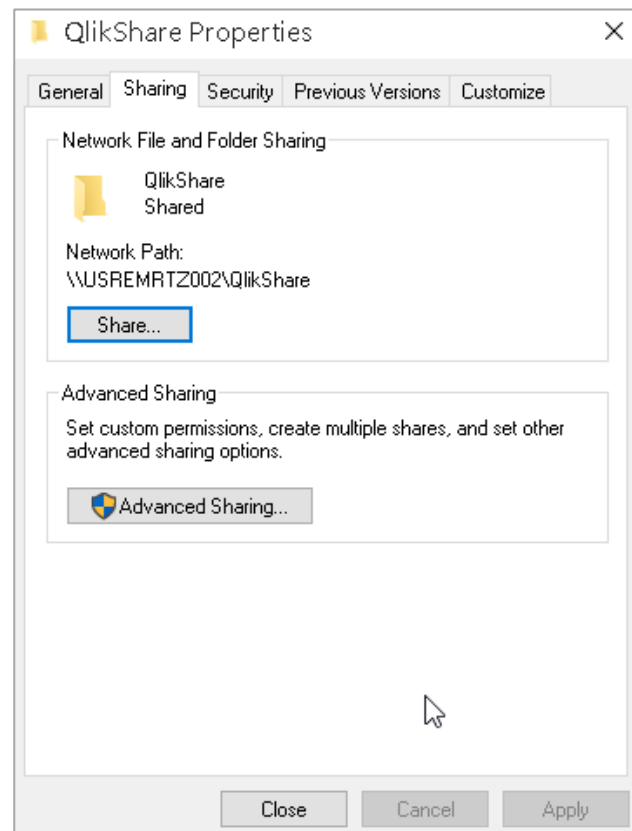
- Right click on the folder and click “Properties”.
- Click “Sharing” tab.
- Select the “Share” button.
- Select the Qlik service account
- Click “Add”
- Set Permission Level to ‘Read/Write’
- Click “Share”.



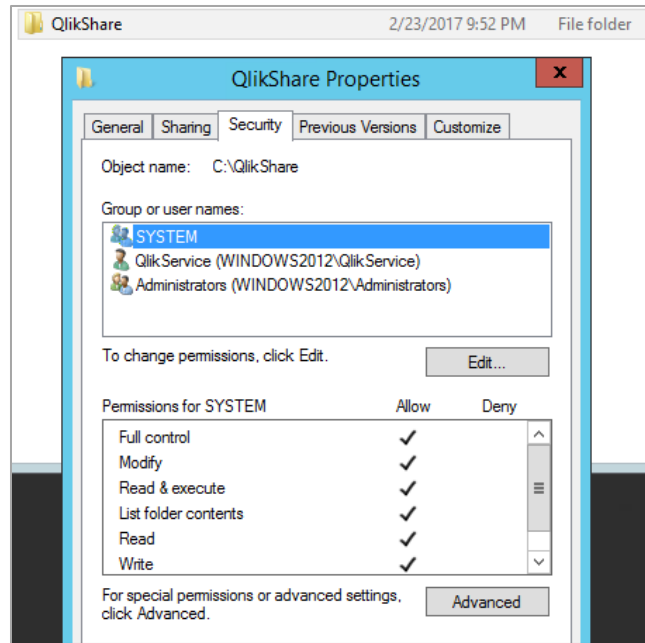
- You should see the new UNC path created in the confirmation screen:



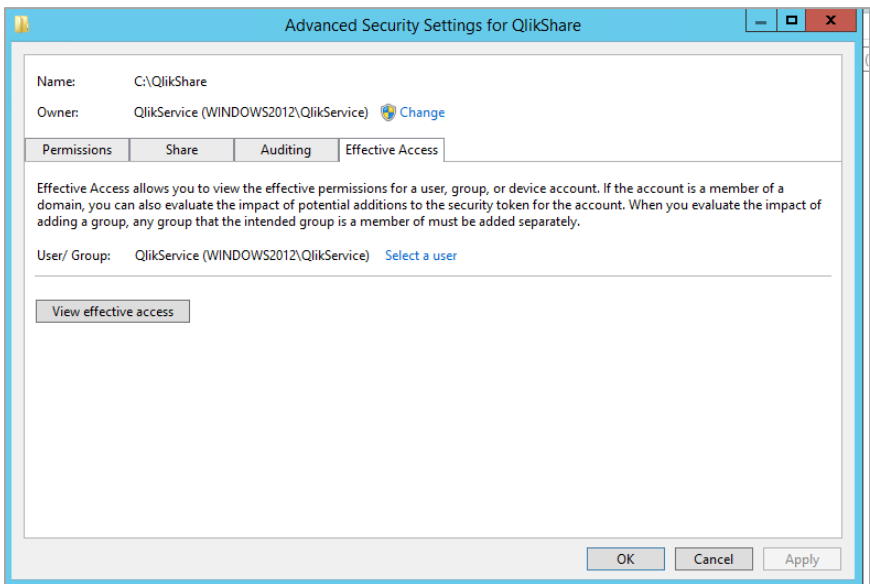
- Verify that the Network Path is visible under the Sharing tab. This is what will be used later on in the installation for your Root folder location.



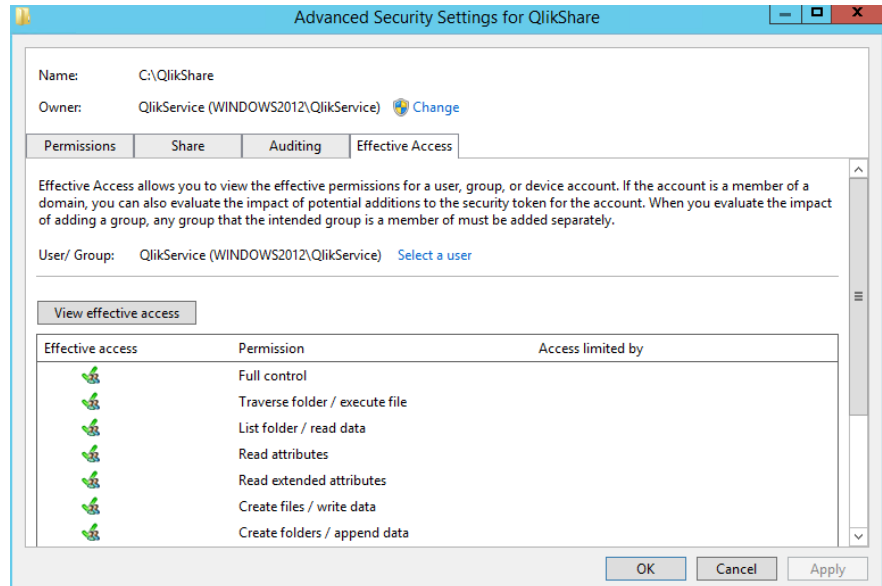
- Ensure permission levels are set to full control for the Qlik service account by doing the following:
 - Under the folder properties>security, select Advanced



- Select the service account user for the “Select a user” link by entering the service account name in at the prompt.
- Select “View effective access”



- Verify the service account has Full control effective permissions and select “OK” to close out of the window.



Installation

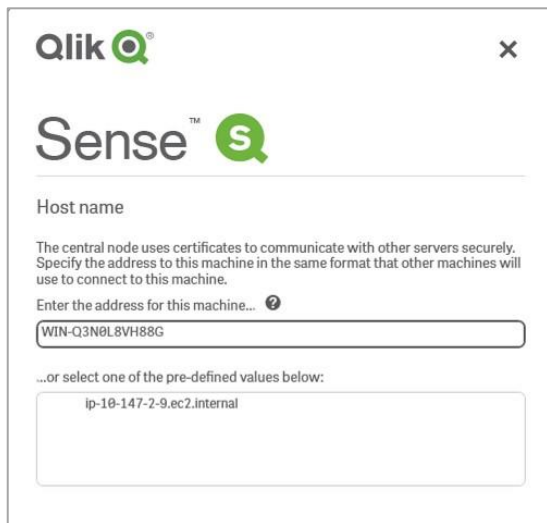
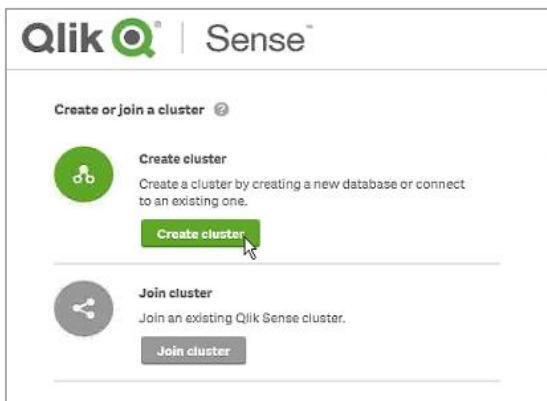
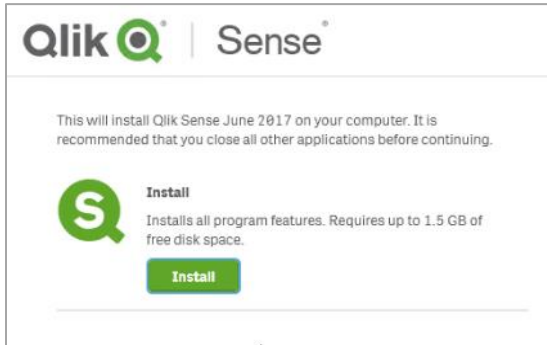
It is now time to install the Qlik Sense services. To begin, remote desktop into the Qlik Sense server and login with the service account you created or that was provided to you. **This account must have local administrative rights and full access to the file share created previously in Step 11.**

Download Qlik Sense

If you don't have the Qlik Sense server installation media, following the procedures below:

1. Open a browser and navigate to www.qlik.com
2. Choose **Login**
3. Navigate to **Services > Customer Downloads** and locate **Qlik_Sense_setup.exe**

Run the Qlik Sense Installer



- Right click on Qlik_Sense_setup.exe, and choose **Run as administrator**
- Select **Install**
- Accept the license agreement
- Choose **Create Cluster**



This is a critical step! If it is not completed correctly, you will not be able to access the server.

- Address of the machine should use the **machine name without the domain name**

Example

IP Address: 10.1.123.234

Machine Name: WIN-Q3NOL8VH88G

Fully Qualified Domain Name: WIN-Q3NOL8VH88G.CUSTOMER.COM

Qlik Sense

Shared persistence database connection settings

You need to keep these settings for reference when adding additional nodes to the Qlik Sense cluster!

Install local database

Database host name: localhost

Database port: 4432

Database user: qliksenserepository

Database user password: [Empty]

An empty password compromises database security.

Cancel Back Next

- Check “**Install local database**”
- Enter the Database user password. For a PoC, it is recommended that you use the same password as the service account “Qlik1234!”. If you use a different password, write it down so you don’t forget it.
- Click **Next**.

Database configuration

Click Next to accept the default configuration settings and install a single-node site. The default settings will allow database connections from the local machine but will not open up the database to the network.

Configure the Advanced Settings if you want to allow connections from other nodes in the cluster. You can also configure these settings manually after the installation has finished.

► **Advanced settings**

- Accept the default settings and click **Next**.

Qlik Sense

Shared persistence storage

These folders contain data and resources that need to be accessible from all nodes in the Qlik Sense cluster.

Root folder: \\WINDOWS2012\QlikShare

Apps folder: \\WINDOWS2012\QlikShare\Apps

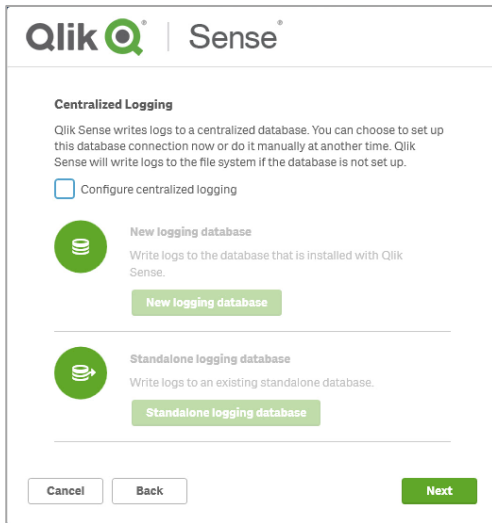
Archived logs folder: \\WINDOWS2012\QlikShare\ArchivedLogs

Custom data folder: \\WINDOWS2012\QlikShare\CustomData

Static content folder: \\WINDOWS2012\QlikShare\StaticContent

Cancel Back Next

- Enter the file share path in the “Root folder” input box. Example: \\Windows2012\QlikShare. This is the share you created in section “Qlik Sense Installation Prerequisites”, Step #11.
- Click **Next**.



Qlik Sense

Centralized Logging

Qlik Sense writes logs to a centralized database. You can choose to set up this database connection now or do it manually at another time. Qlik Sense will write logs to the file system if the database is not set up.

Configure centralized logging

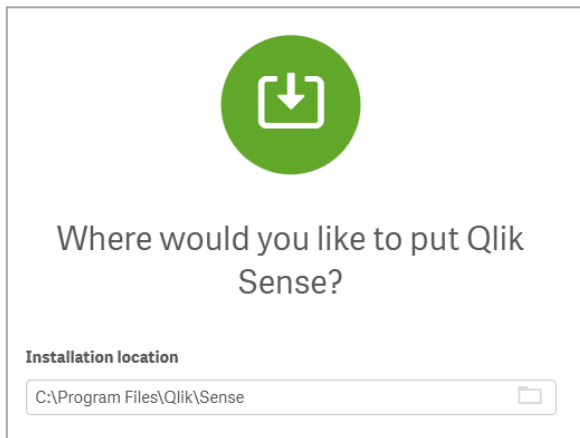
New logging database
Write logs to the database that is installed with Qlik Sense.
New logging database

Standalone logging database
Write logs to an existing standalone database.
Standalone logging database

Cancel **Back** **Next**

- Uncheck “Configure centralized logging”.
- Click **Next**.

Tip! Centralized logging will log to a database. Unchecking Centralized logging will instead store logs in text files on the machine.

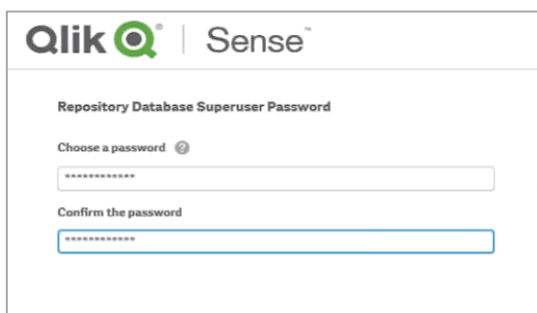


Where would you like to put Qlik Sense?

Installation location

C:\Program Files\Qlik\Sense

- Accept the default **Next**. If you would like to choose a different installation directory, please do so.



Qlik Sense

Repository Database Superuser Password

Choose a password

Confirm the password

- Enter the same Repository Database Superuser Password entered previously for the “Database user Password” and click Next.

- Enter the service account username and password



If you are using a domain account, the format will be DOMAIN\USER

If you are using a local account, the format will be MACHINENAME\USER

Whichever you choose, the account should belong to the **Administrators** group on the server.

The service account is often used when Qlik Sense needs to access the file system, databases and user directory connectors. For this reason, a domain account is recommended

- Check 'Install extension bundles'
- Check 'Dashboard bundle'
- Click **Next**
- Accept the License Agreement
- Click **Install**
- When complete, click **Finish**.

Note: If a patch is available for this version, download the latest patch version and install it after successfully completing the initial installation. The patch install should be a Next > Next > Next > Finish with no additional configuration needed.

Configuration

Launch Qlik Management Console Setup

It is now time to configure the Qlik Sense installation using the Qlik Management Console (QMC). Launch QMC using the icon on your server's desktop or via a browser using the server address provided during the installation. For example, <https://ipaddress/qmc> or <https://machinename/qmc>.



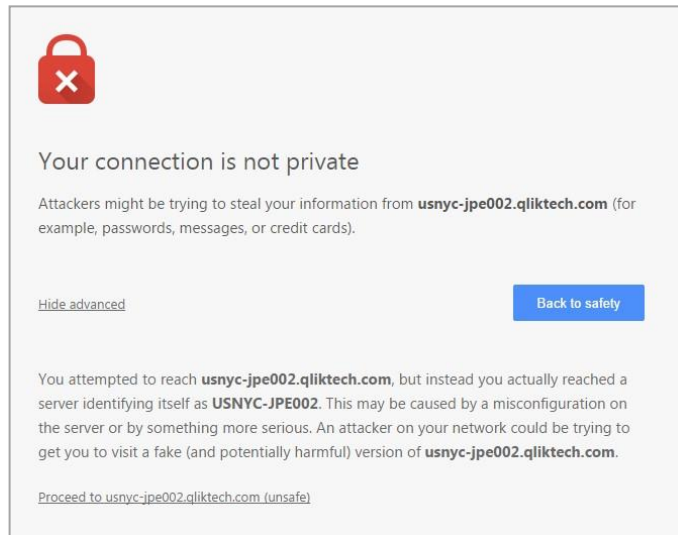
If the QMC doesn't start the first time, give it 60 seconds. The Qlik Sense services are configured for delayed start.



You may get a security warning. If so, click through it.



If you are prompted to login to the QMC, login with the same user and password you used to Remote Desktop to the server.



Apply License

You will be prompted to enter the site license information. Complete the form and click **Get LEF and preview the license** from server.



If the server does not have access to the Internet, you will need to obtain an LEF file from a Qlik representative

SITE LICENSE	
Owner name	Marcus
Owner organization	QT
Serial number	9999000000000038
Control number	
▼ LEF access	
<input type="button" value="Get LEF and preview the license"/>	

When the site license has been successfully applied, you will see a confirmation message.

✓ **Successfully licensed**

You have successfully applied a license to the Qlik Sense server. Before users can begin to create and view Qlik Sense apps there are a number of common configuration items you may wish to review to ensure that users get the best experience possible. These include:

- Connecting to a user directory
- Allocating licenses for users
- Setting up permissions to create and read apps

The following guide walks through the most commonly used configuration steps when getting started with Qlik Sense.

[? View the guide for Setting up your Qlik Sense site](#)

Token Allocation

If you have a token based license, follow these instructions. Tokens must be allocated to users for them to access Qlik Sense.

- Navigate to **Start > License and Tokens > User Access Allocations**
- Click the **Allocate** button
- Select the User ID you are logged in with and click **Allocate**



Tip!

This is so the administrator always has a license

Users			
User name	User directory	User ID	Tags
jpe	QTSEL	jpe	
sa_engine	INTERNAL	sa_engine	
sa_proxy	INTERNAL	sa_proxy	
sa_repository	INTERNAL	sa_repository	
sa_scheduler	INTERNAL	sa_scheduler	

Professional/Analyzer Allocation

If you have a professional/analyzer based license, follow these instructions. Manual allocation for Professional user access. Process is the same for Analyzer.

- Navigate to **Start > License management> Professional access allocations**
- Click the **Allocate** button
- Select the User ID you are logged in with and click **Allocate**



This is to allocate Professional access. For Analyzer follow the same step but instead navigate to **Analyzer access allocations**.

Name	User directory	User ID
mai	QTSEL	mai
qlikservice	USCHI-MSI4	qlikservice
aa_api	INTERNAL	aa_api
aa_converter	INTERNAL	aa_converter
aa_engine	INTERNAL	aa_engine
aa_hub	INTERNAL	aa_hub
aa_printing	INTERNAL	aa_printing
aa_proxy	INTERNAL	aa_proxy
aa_qlikview	INTERNAL	aa_qlikview
aa_reporting	INTERNAL	aa_reporting
aa_repository	INTERNAL	aa_repository
aa_scheduler	INTERNAL	aa_scheduler

PoC License Rule

In addition to manual allocation of tokens or professional and analyzer licenses, users can be granted a token via a rule.

- Navigate to **Start > License and Tokens > User Access Rules** or **Professional access rules**
- Click **Create New**
- Click **Basic**
- Populate the BASIC rule with **user name like value ***
- Click **Apply**

User access rule edit

IDENTIFICATION

Name: License rule to grant user access

Disabled:

Description: Rule to setup automatic user access

BASIC

Actions: Allow access

user name like +

value *



This rule grants a token to any user connecting to Qlik Sense. This is useful for a PoC but rarely used in production.

Proxy Setup

This section describes steps to allow HTTP access and support access using alternate URL formats.

- Navigate to **Start > Proxies > Central > Edit**
- Click **Ports**
- Check **Allow HTTP**
- Click **Apply**



access Qlik Sense using HTTP instead of HTTPS and will avoid browser security warnings

IDENTIFICATION	
Name	Central Proxy
PORTS	
Service listen port HTTPS (default)	443
Authentication listen port HTTPS (default)	4244
Kerberos authentication	<input type="checkbox"/>
REST API listen port	4243
Allow HTTP*	<input checked="" type="checkbox"/>
	Service listen port HTTP and Authentication listen po
Service listen port HTTP	80
Authentication listen port HTTP	4248

- Navigate to **Start > Virtual Proxies > Central Proxy (Default) > Edit**
- Click **Advanced**
- Scroll down to **Host white list**
- Click **Add new value**
- Add **IP Address** and **Machine name** of your server
- Click **Apply**



Adding these values to the Host white list allows Qlik Sense to accept URLs of these formats



AWS Instances: Add the **external IP address, Public DNS, and public Domain** found in *EC2 > Instances > machine > Public IP / Public DNS fields*

- Public IP Example: 54.196.234.38
- Public DNS Example: ec2-54-196-234-38.compute-1.amazonaws.com
- Public Domain: compute-1.amazonaws.com



Azure Instances: Add the **hostname** and the **Public DNS**

- Hostname Example: WIN-Q3N0L8VHHHG
- Public DNS Example: WIN-Q3N0L8VHHHG.cloudapp.net



Servers on a domain: Add the **fully qualified domain name** and **domain name**

- Fully Qualified Domain Example: WIN-Q3N0L8VHHHG.CUSTOMER.COM
- Domain Example: CUSTOMER.COM



If the customer has created any DNS entries (e.g., qlikbi.company.com), add this to the whitelist, too. Customers having done this *may* ask to import their own SSL certificate. See Appendix: [Client Provided Browser Certificate](#).

Validation

At this point, you should be able to login to the QMC and HUB directly on the server. Use the shortcuts created on the desktop to validate that the QMC and HUB open successfully. Qlik Sense is setup correctly if the browser gives no security warnings.

Now open Qlik Sense QMC and Hub from a desktop or laptop. The URL used to access Qlik Sense QMC and Hub will be as follows:

- <http://<ipaddress>/QMC> or <http://<machinename>/QMC> or <http://<publicdns>/QMC>
- <http://<ipaddress>/Hub> or <http://<machinename>/Hub> or <http://<publicdns>/Hub>



EC2 installations – use the Public DNS

Example: <http://ec2-54-196-234-38.compute-1.amazonaws.com/hub>

Note: Getting rid of the HTTPS security warnings in EC2 requires additional configuration (DNS and customer SSL certificates) and is beyond the scope of this PoC installation guide. Use HTTP in your URLs instead of HTTPS or click through the security warning when launching Qlik Sense.



Azure installations – use the Public DNS

Example: <http://WIN-Q3N0L8VHHHG.cloudapp.net>

Note: Getting rid of the HTTPS security warnings in Azure requires additional configuration (DNS and customer SSL certificates) and is beyond the scope of this PoC installation guide. Use HTTP in your URLs instead of HTTPS or click through the security warning when launching Qlik Sense.



On premise installations – use machine name

Example: <https://WIN-Q3N0L8VHHHG/hub>

Note: If you can access the hub via machine name, you will not get security warnings. If this is not possible, use HTTP in your URLs instead of HTTPS or click through the security warning when you launch Qlik Sense.

Import an Application

1. Open the Qlik Sense Management Console
2. Click **Start > Apps > Import**
3. Click **Browse**
4. Navigate to the Qlik Sense application you would like to import into the server. The default location for Qlik Sense Desktop applications is C:\Users*<user>*\Documents\Qlik\Sense\Apps.
5. Click **Import**
6. Once the import is complete, highlight the application and click **Publish**, select a **Stream** and click **OK**.

Qlik Sense Cloud Services Configuration

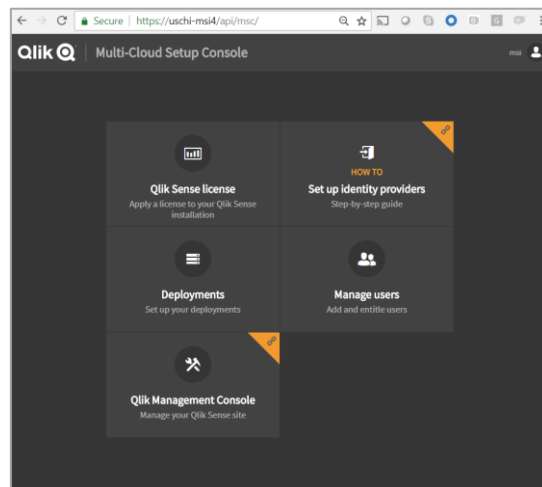
Configure Security

This is beyond the scope of this document. At present, the IdP must support OpenID for authentication to Qlik Cloud Services and SAML for authentication to Qlik Sense Enterprise for Windows. If both are already configured such that the same user can login to both environments, then proceed. If not, contact an Enterprise Architect.

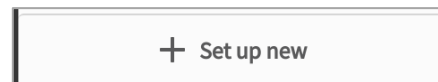
Connect to Qlik Cloud Services

Navigate to <http://<machinename>/api/msc> to access the Multi-Cloud Setup Console.

Click **Deployments**



Click **Set up new**



Enter the following information:

Deployment name:
QlikCloudServices

ClientID, Client Secret, Token Endpoint:
Provided by Identity Provider

API endpoint:
The domain provided for your Qlik Cloud Services PoC.

Audience:
qlik.api

Click **Apply**.

Set up new deployment

The setup values are available from your identity provider

Deployment name

API endpoint

Audience

Use local bearer token

Client ID

Client secret

Token endpoint

Custom Properties

In the QMC, Create custom properties via Start > Custom Properties > Create New.

Name: collections, **Resource Types:** Apps, **Values:** Finance, Sales, Etc.

Name: groupswithaccess, **Resource Types:** Apps, **Values:** Everyone

Name: sendto, **Resource Types:** Apps, **Values:** QlikCloudServices

Distribution Policy

In the QMC, Create a Distribution Policy via Start > Distribution Policies> Create New.

Rule from Template: Distribution_App

Name: QlikCloudServices

Rule:

subject.name = value
QlikCloudServices

AND

#App.@sendto = value
QlikCloudServices

The screenshot shows the 'IDENTIFICATION' and 'BASIC' sections of a distribution policy configuration. In the 'IDENTIFICATION' section, 'Create rule from template' is set to 'Distribution_App', 'Name' is 'QlikCloudServices', and 'Description' is empty. In the 'BASIC' section, 'Resource filter' is 'App_*' and 'Actions' includes 'Distribute'. A rule editor shows two conditions: 'subject.name = value' with 'value' set to 'QlikCloudServices', and '#App.@sendto = value' with 'value' set to 'QlikCloudServices'. The conditions are joined by 'AND'.



Tip!

The subject.name must match the deployment name created in the section "Connect to QlikCloudServices". Use "QlikCloudServices" throughout.

Deploy an Application

In the QMC, set custom properties on an app via Start > Apps > {app} > Edit > Custom properties.

Publish that app to a stream by clicking the Publish button.

The screenshot shows the 'CUSTOM PROPERTIES' section of an application configuration. It lists three properties: 'collections' with value 'Finance', 'groupswithaccess' with value 'Everyone', and 'sendto' with value 'QlikCloudServices'. Each value is shown in a blue pill-shaped button with a close icon.

APPENDIX I - Apple iOS Mobile Safari Browser Access

Customers wishing access the Qlik Sense server from an iOS device should recognize that as of iOS version 8, untrusted certificates are not allowed. This means that the self-signed certificates that Qlik Sense uses out of the box are not sufficient to enable Hub access on iOS devices.

Option #1 – Use HTTP

This is the simplest option for Proof of Concepts. See the section titled [Proxy Setup](#) to learn how to enable HTTP. Direct users on iOS mobile devices to navigate to the server via **HTTP** and not **HTTPS**.

Option #2 – Use a trusted certificate

Install a **customer provided** certificate with private key from a trusted root certificate authority (e.g. Symantec, GoDaddy, Thawte, DigiCert, or many others) and add this certificate's security thumbprint to the thumbprint text box in the Proxy configuration. See the section titled [Client Provided Browser Certificate](#) to learn how to enable this.



On premise installations – Customer provide a certificate that can be used with the server.

Example: *.company.com

Example: qliksense.company.com



AWS and Azure – Installing a trusted certificate in EC2 or Azure requires additional configuration and is beyond the scope of this PoC installation guide. Unless the customer is able to register a domain, purchase a certificate, and associate with the Qlik Sense instance in EC2 or Azure, use HTTP in your URLs instead of HTTPS or click through the security warning when launching Qlik Sense.

APPENDIX II - iOS Mobile App Setup and Configuration

Desktop Authentication Link Setup

For the iOS Client to know where to connect, we generate a client authentication link via:

- Start > Virtual Proxies > “Central Proxy (Default)” > Client Authentication Link
 - Host URL is the same as how you access Qlik Sense in the browser, without /hub
 - Friendly Name is the name that shows up on the iOS device
 - Click Generate, Click Apply, and you get a URL like this:

qliksense://enterpriseurl?action=add&url=http%3A%2F%2F34.211.33.62&name=QLIKAWS&version=0.1&signature=008a750e10a8a8fe4194a1f9257e64baa35e9d2fc1094e50f534c335be131d5d

DESKTOP AUTHENTICATION LINK	
Desktop authentication link host URI	<input type="text" value="http://34.211.33.62"/>
Desktop authentication link friendly name	<input type="text" value="QLIKAWS"/> <small>This friendly name can be used to simplify the identification of the host. You can, for example, use your company name.</small>
Generate desktop authentication link	<input type="button" value="Generate"/> <pre>qliksense://enterpriseurl?action=add&url=http%3A%2F%2F34.211.33.62&name=QLIKAWS&version=0.1&signature=008a750e10a8a8fe4194a1f9257e64baa35e9d2fc1094e50f534c335be131d5d</pre> <small>The generated result is available above. You can select the text and copy it for use.</small>

Security Rule Setup

For an app to be downloadable, the basic requirement is that a user must have ‘Export’ permissions on App_* via the security rules and be able to read the app.

Create a Custom Property called “MobileOffline” and apply it to an application.



Note that this custom property isn’t strictly required. It just makes the security rule easier to manage.

- In the QMC, go to Start > Custom Properties > Create New > Name = ‘Mobile Offline’, Resource Types = ‘Apps’, Custom Property Values = ‘True’

IDENTIFICATION

Name

RESOURCE TYPES

<input type="checkbox"/> Analytic connections	<input type="checkbox"/> Proxies
<input checked="" type="checkbox"/> Apps	<input type="checkbox"/> Reload tasks
<input type="checkbox"/> Content libraries	<input type="checkbox"/> Repositories
<input type="checkbox"/> Data connections	<input type="checkbox"/> Schedulers
<input type="checkbox"/> Engines	<input type="checkbox"/> Streams
<input type="checkbox"/> Extensions	<input type="checkbox"/> User synchronization tasks
<input type="checkbox"/> Nodes	<input type="checkbox"/> Users
<input type="checkbox"/> Printing	<input type="checkbox"/> Virtual proxies

VALUES

Custom property values

Values

- In the QMC, go to Start > Apps > <select an app> > Custom Properties, Set MobileOffline = True

IDENTIFICATION

Name

Owner

Created

Last modified

File size (MB)

CUSTOM PROPERTIES

MobileOffline

Create a Security Rule called “_Mobile Offline”

- Start > Security Rules > Create New > Create Rule from Template = “App Access”
 - Name = ‘_Mobile Offline’
 - Resource Filter = ‘App_*’;
 - Actions = Access Offline
 - Conditions = resource.HasPrivilege ("read") and resource.@MobileOffline="True"
 - Context = Only in Hub

IDENTIFICATION

Disabled

Name

Description

BASIC

Resource filter

Actions Create Read Update Delete Export Publish Change owner
 Export data Access offline

This condition cannot be displayed in the rule editor because it is too complex.

ADVANCED

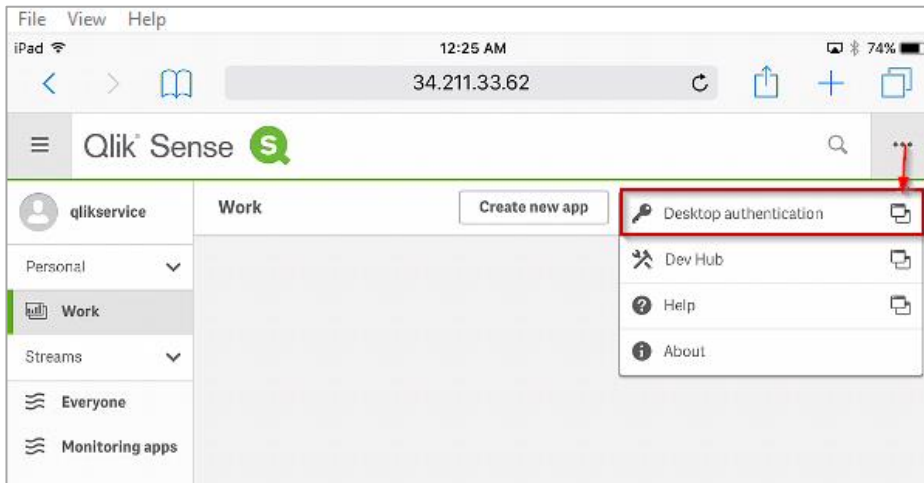
Conditions

The rule is valid.

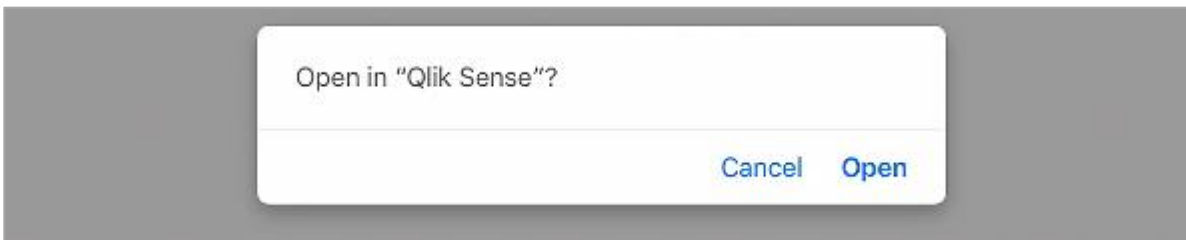
Context

Connect to the Qlik Sense Enterprise Server

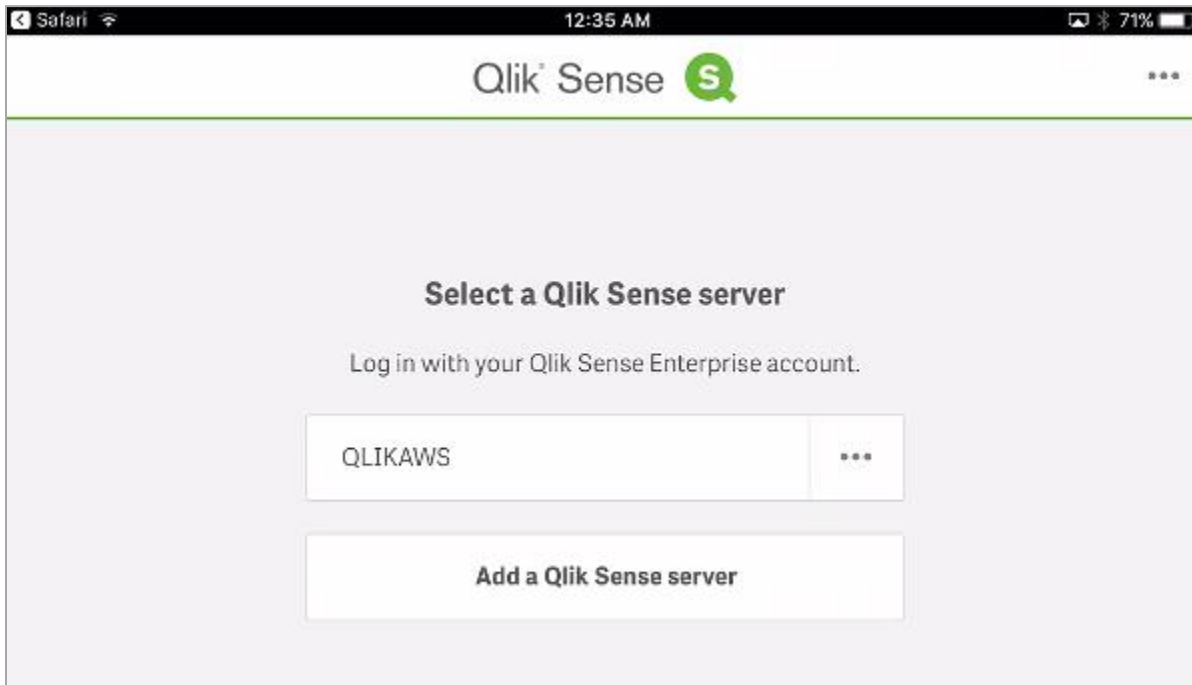
- Using Mobile Safari on the iPad, connect to the Qlik Sense Enterprise Server Hub.
- Touch the ellipses on the top right, and select the Desktop Authentication link.



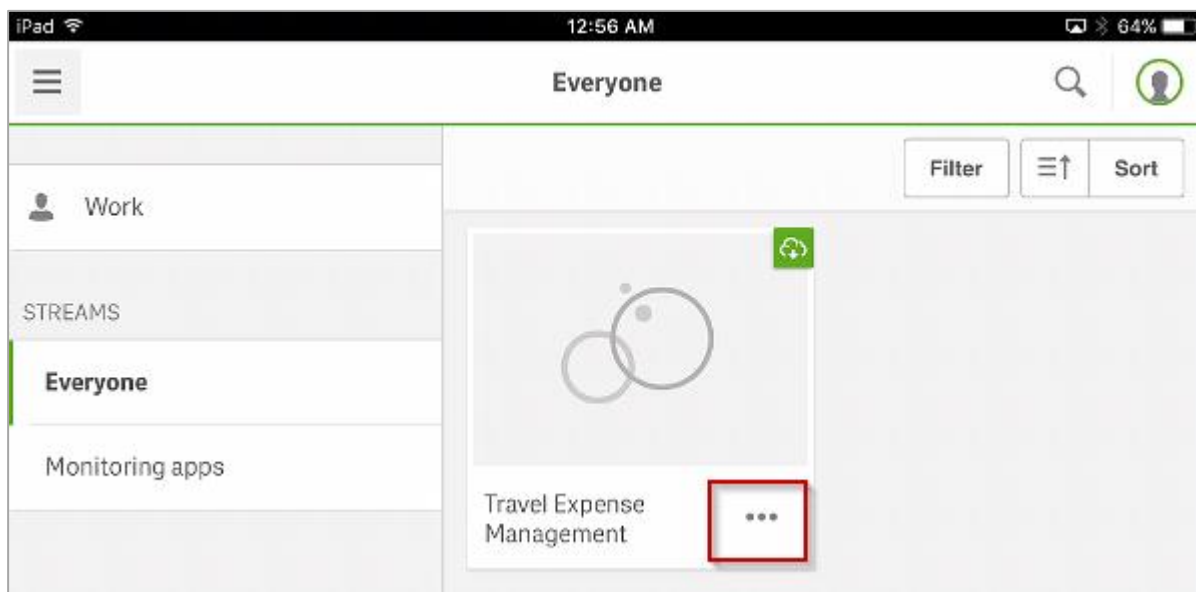
- When prompted, select **“Open in Qlik Sense”**. The iOS native app should automatically open with the friendly name of the Desktop Authentication Link you previously entered in the QMC.



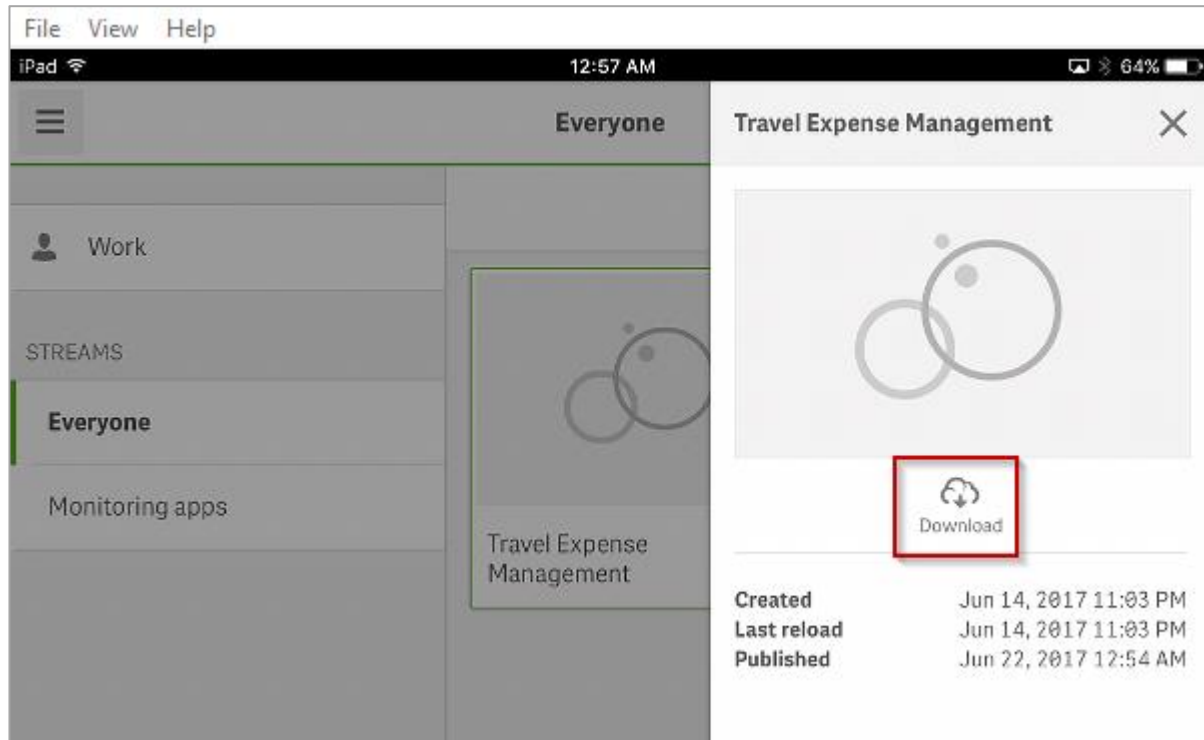
- Tap 'Open'



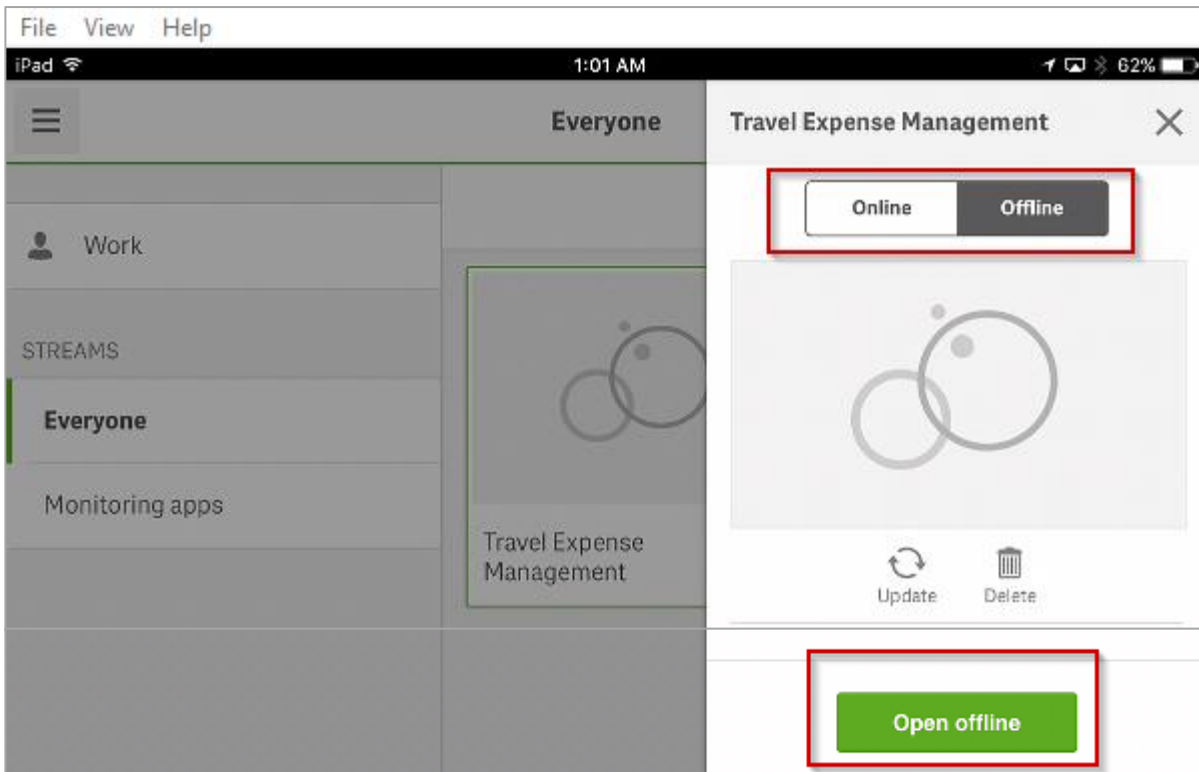
- Select the Qlik Sense Enterprise friendly name on the landing page.
- You will be directed to a forms login page. Here enter the username and password of the user account you wish to use. This example uses the user account created earlier in this document.
 - Username: **.QlikUser1**
 - Password: **QlikSense!**
- The Hub should now open and show available applications. Note the “download” icon on the top right of any application specified to be Offline=True via the custom property previously created in the QMC. Touch the ellipses in the bottom right of the application you want to use offline.



- A sidebar will pop in. Select the “Download” icon to download the app.



- Once the app has completed downloading, you will now see Online/Offline tabs and the ability to open an app offline. Select the "Open Offline" button to begin using the offline capability in the iOS app.



APPENDIX III - Amazon EC2 – Launch an Instance



If you are able to provide the EC2 instance for the customer, the best way to get started quickly is to request an EC2 instance through ServiceNow. From there you can choose predefined AMLs for a quick start. Detailed instructions on how to do so can be found here: [link](#).

Security Groups

Create a security group called Qlik Sense with the rules in the screenshot below. This is found in **EC2 > Security Groups** in the left navigation of the EC2 control panel. Then click **Create Security Group**.

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Anywhere	e.g. SSH for Admin Desktop
HTTP	TCP	80	Anywhere	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Anywhere	e.g. SSH for Admin Desktop

Name Qlik Sense
Inbound Rules HTTP, HTTPS, RDP


Key Pair

Create a key pair called **Qlik Sense** via **EC2 > Key Pairs > Click Create Key Pair**. Save this file (Qlik Sense.pem) somewhere *and don't lose it!*



Launch the Instance

- **EC2 > Instances > Click Launch Instance**
- Choose **Windows Server 2016 Base** instance, 64 bit

 **Microsoft Windows Server 2016 Base - ami-8b1886f3**


Windows Microsoft Windows 2016 Datacenter edition. [English]

Free tier eligible Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

- Choose an **Instance Type**
 - R3.2xlarge is a good choice with 8 cores / 60 GB RAM
 - R3.4xlarge is a good choice with 16 cores / 122 GB RAM
 - Other larger instances are available. Some of the larger servers require an email to AWS support first.

- Click **Review and Launch**

- You will get a warning about **security groups**. Change from the default security group to **Qlik Sense**

 **Improve your instance's security. Your security group, launch-wizard-1, is open to the world.**

Your instance may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

- **Launch**

- You will get a warning about key pairs. Choose the **Qlik Sense** key pair you have created and saved.

Select an existing key pair or create a new key pair
✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Select a key pair

I acknowledge that I have access to the selected private key file (Qlik Sense.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

Elastic IP

- Create an elastic IP via **EC2 > Elastic IPs > Allocate New Address > Yes, Allocate**
- Select the new Elastic IP address, and click **Associate Address**
- Choose the running instance and click **Associate**
- You will associate this with your instance so that the server IP address doesn't change if you stop and start the instance.

RDP

- Go back to the EC2 console and wait for the new instance to say "running" and "2/2 checks passed".

<input type="checkbox"/>	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
<input checked="" type="checkbox"/>		i-1a506af1	m3.2xlarge	us-east-1c	● running	✔ 2/2 checks passed

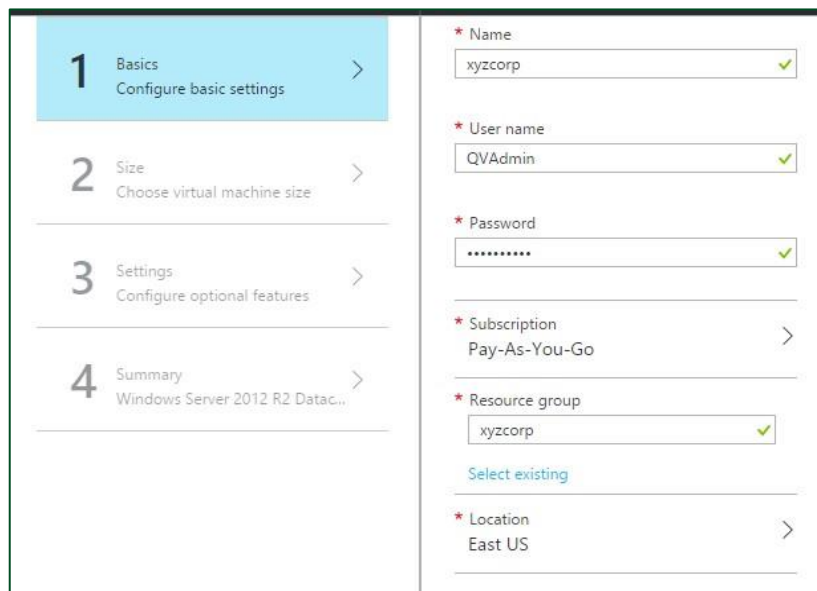
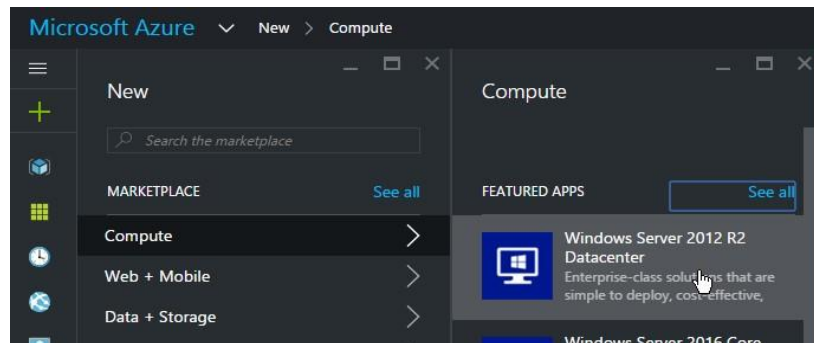
- Click **EC2 > Instances > Choose your instance > Connect**
 - Click **Download Remote Desktop File** > Saves a RDP link you can use to connect
 - Click **Get Password** > Choose your **QlikSense.pem** file > Click **Decrypt password**
 - Save this somewhere for reference
- At this point you should have a Remote Desktop session on the server. If you can't connect, review this section for proper setup of security groups and key pairs.

APPENDIX IV - Microsoft Azure – Launch an Instance

Tip!

It is easy to get an Azure account at <http://portal.azure.com/> and click on Free Trial (or buy now). You can sign up and try this on your own! Just make sure to shut down any machines you launch so as not to incur an unnecessary charges.

- Choose **New > Compute > Windows Server 2012 R2 Datacenter**
- Click **Create**
- Enter a **Username** and **Password** for your instance (for Remote Desktop)
- Enter a **Resource group** (can be anything, suggest project or customer name)
- Choose a **location**
- Click **OK**
- Choose an instance size. **DS3 v2** or **DS4 v2** is recommended for basic workloads. **DS13 v2** or **DS14 v2** is recommended for large workloads. *Note the pricing of each before deciding.*

A screenshot of the Azure VM configuration wizard, specifically the 'Basics' step. The wizard is divided into four numbered steps: 1. Basics (selected), 2. Size, 3. Settings, and 4. Summary. The 'Basics' step contains several configuration fields: 'Name' (xyzcorp), 'User name' (QVAdmin), 'Password' (masked with dots), 'Subscription' (Pay-As-You-Go), 'Resource group' (xyzcorp), and 'Location' (East US). Each field has a green checkmark indicating it is valid.

- Review the settings and click **OK** and **OK** again.
- Now wait... this can take up to 30 minutes. You will see the picture on the right.
- Once the VM is online, you will set a security group to allow traffic to the VM.

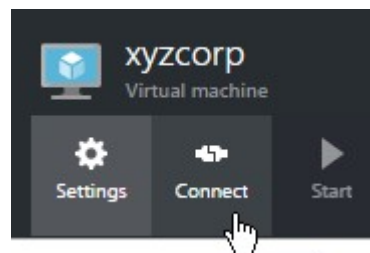


- Resource Group (looks like a box)
- Network Security Group (looks like a shield)
- Inbound Security Rules
- Click **Add**, then add inbound security rules in the table to the right (leave unlisted settings as is)



Name	Protocol	Destination Port
HTTP	TCP	80
HTTPS	TCP	443

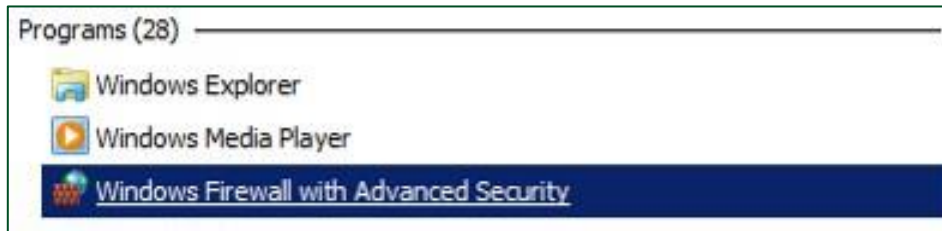
- Finally, RDP to it by clicking on Connect



APPENDIX V - Windows Firewall

This section details how to disable or open specific ports that Qlik Sense needs open.

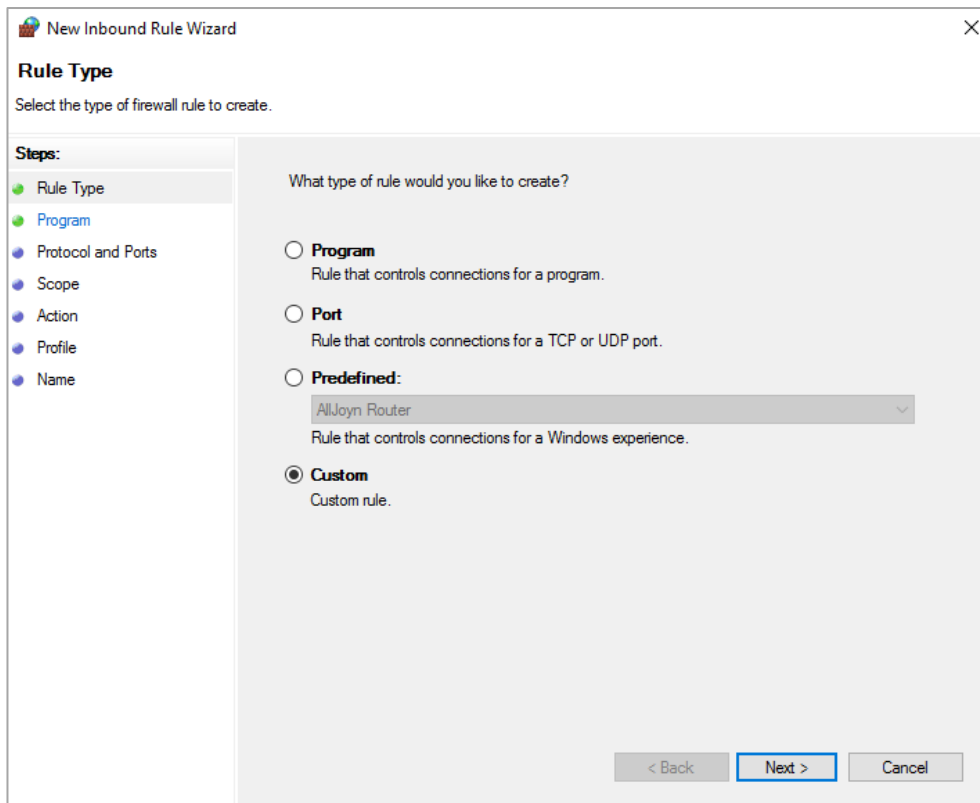
On the Qlik Sense server, click **Start** and search for **Advanced Firewall**. Click on **Windows Firewall with Advanced Security**



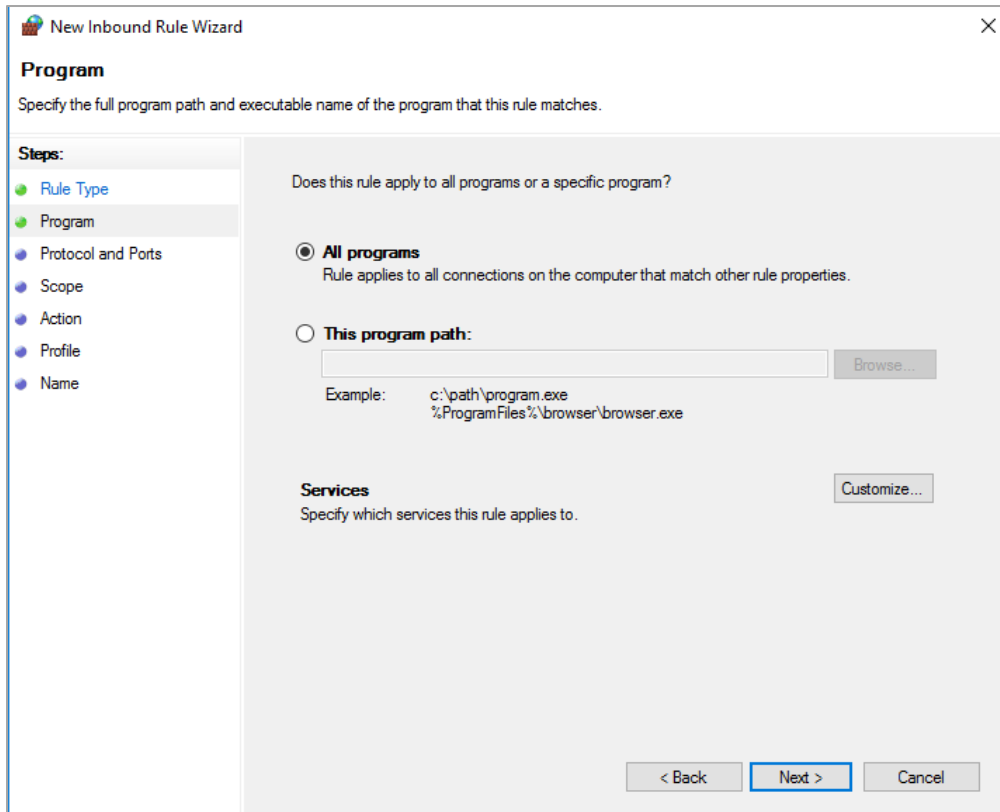
The simplest solution is to disable windows firewall completely, under Properties. If this isn't possible, continue with the following steps to open specific ports.



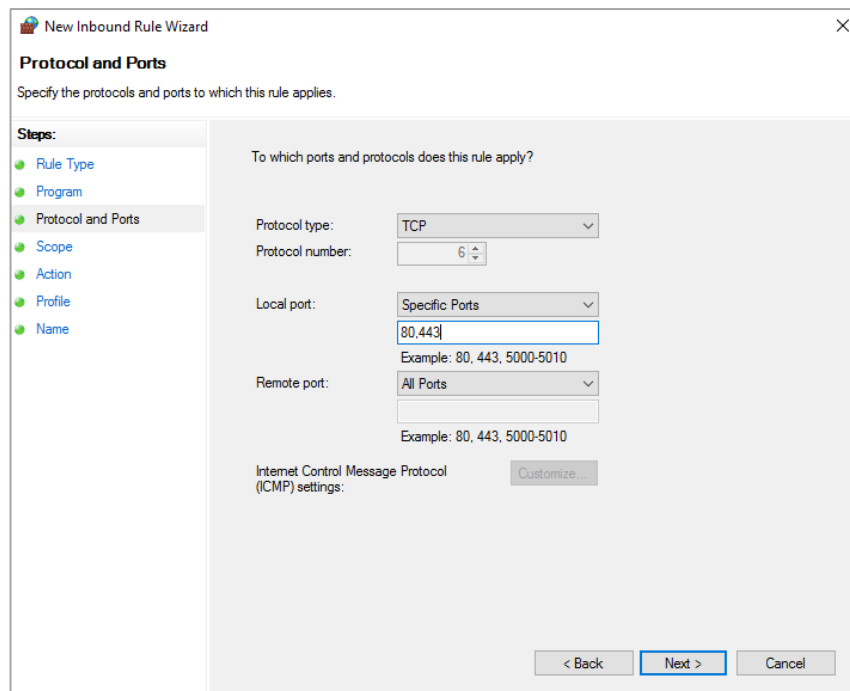
1. Click on 'Inbound Rules' in the left panel, then click on 'New Rule' in the right panel. Choose 'Custom' and go to next.



2. Choose 'All programs' and go to next.



- 'Protocol type:' should be 'TCP' and 'Local port:' should be set to 'Specific Ports'. In the field you should enter **80, 443**. This will allow you to access the Hub and QMC.



- Press 'Next' until you reach 'Name'. Ensure that 'Allow the connection' is selected Under Action'.

New Inbound Rule Wizard [X]

Scope
Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

Any IP address

These IP addresses:

Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

Any IP address

These IP addresses:

Action
Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

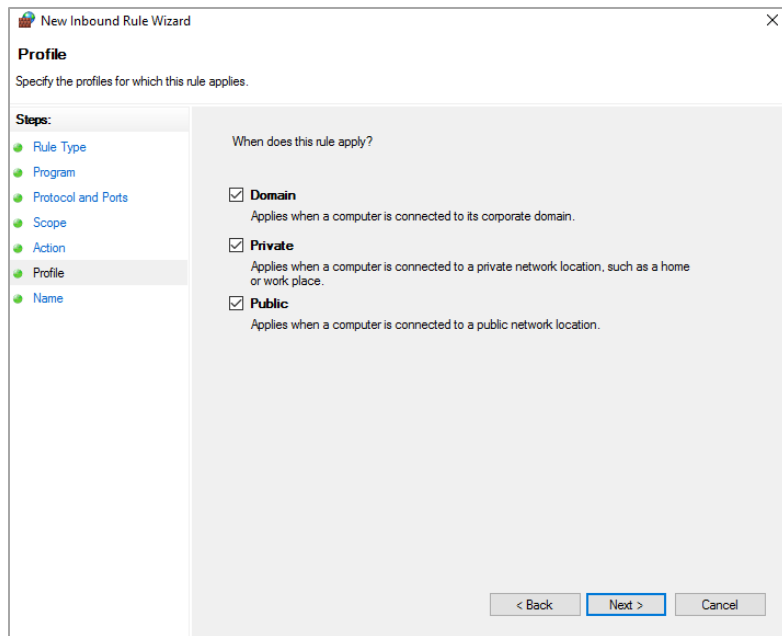
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

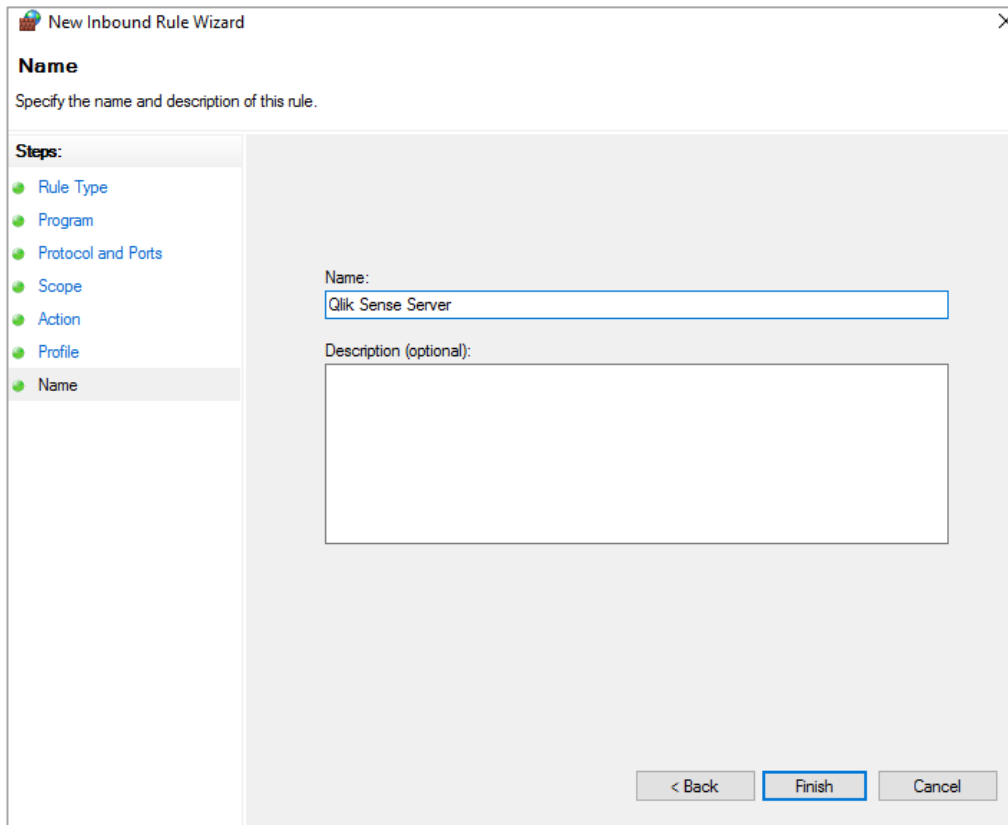
Allow the connection
This includes connections that are protected with IPsec as well as those are not.

Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Block the connection



5. Ensure that all options are ticked and click 'Next'.



6. Give the rule a name such as 'Qlik Sense Server' and then click 'Finish'. This will now allow traffic on those ports through the firewall to the operating system.
7. Close Windows Firewall.

APPENDIX VI - IE Enhanced Security Configuration

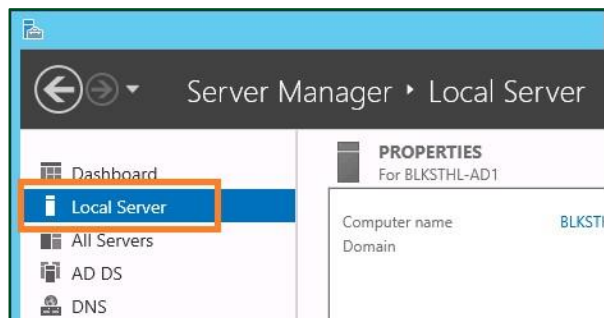
This section details how to disable IE Enhanced Security Configuration on Windows Server 2012 and 2016. It is important to disable this in the case the customer will be accessing and using “Web File” data as a data source. IE ESC blocks that traffic.

Windows 2012 & 2016

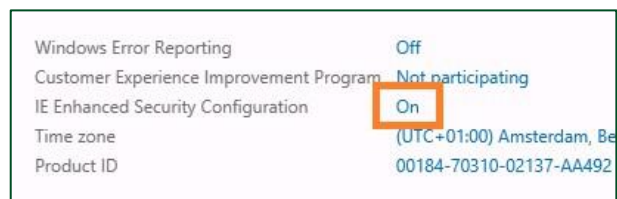
- On the taskbar, click **Server Manager**



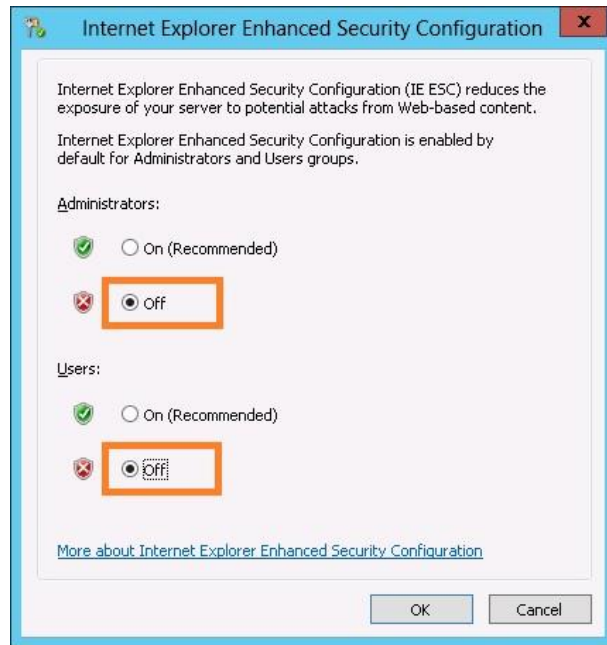
- Click “**Local Server**”



- Next to IE Enhanced Security Configuration, click “**On**”



- Next to Administrators, click “Off”
- Next to Users, click “Off”
- Click “OK”



APPENDIX VII - Client Provided Browser Certificate

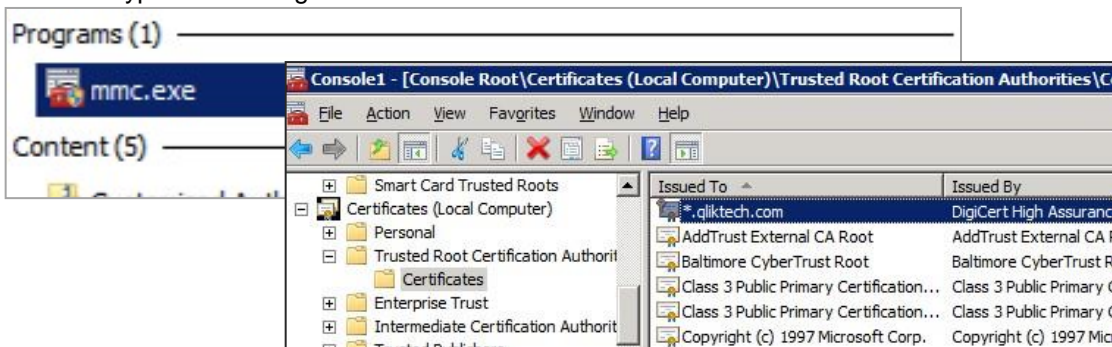
This section details how to import a client provided browser certificate into Qlik Sense.

Generate Certificate Signing Request for Trusted Certificate

If you don't already have a certificate from a Trusted Certificate Authority, you may use these instructions to help generate the CSR. <https://community.qlik.com/docs/DOC-15740>

Import Certificate to Windows Certificate Store

- Click **Start** > type **MMC** > Right Click > Run as Administrator...



- Click **File** > **Add / Remove Snap In...**

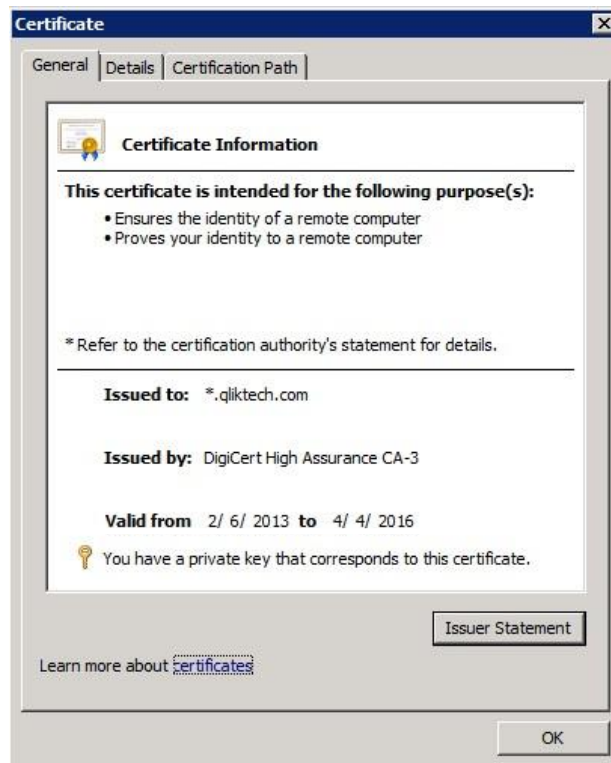
- Click **Certificates** > Click **Add** > choose **My User Account**
- Click **Certificates** > **Add** > choose **Computer Account** > choose **Local Computer**
- Navigate to each folder listed below and import the customer provided certificate
 - Certificates - Current User > Trusted Root Certification Authorities > Certificates
 - Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates
 - Certificates (Local Computer) > Personal > Certificates

Validate Existence of Private Key

- Double click on the imported certificate to view its properties.

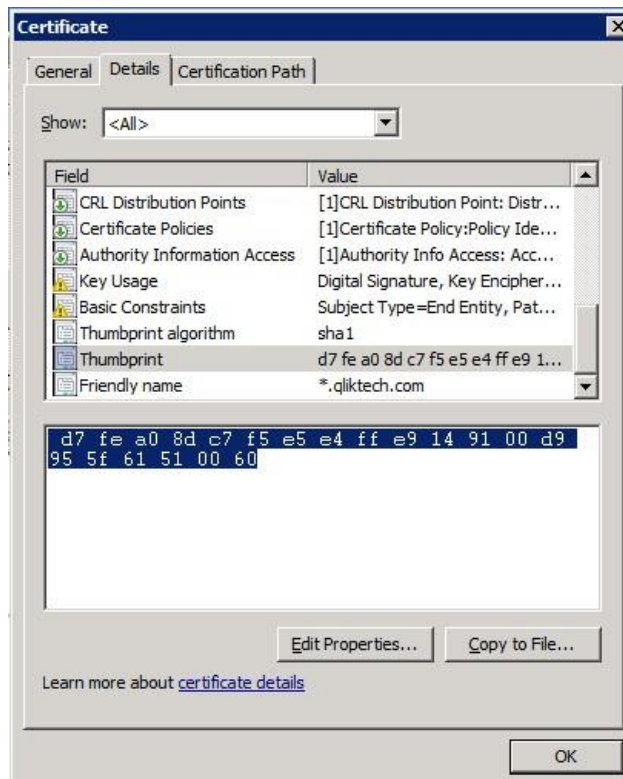


- Validate the private key exists with this certificate. If not, ask the person who provided you the certificate.

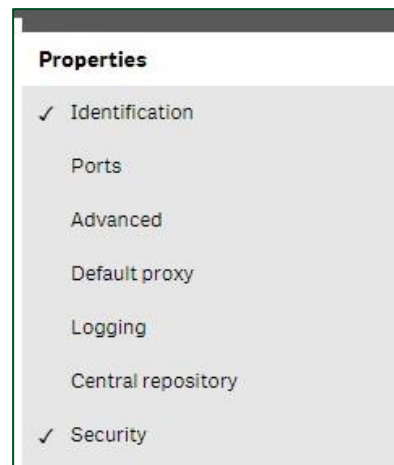


Import Certificate Thumbprint to Qlik Sense Proxy

- Navigate to the **Details** tab and copy the **Thumbprint** value. Make sure to copy all leading and trailing spaces.



- Open **QMC > Proxies > Central Proxy > Edit**
- On the right hand side of the screen, click **Security** to enable additional properties.



- Paste the browser thumbprint, including all spaces.



- Click **Apply** to restart the Proxy.

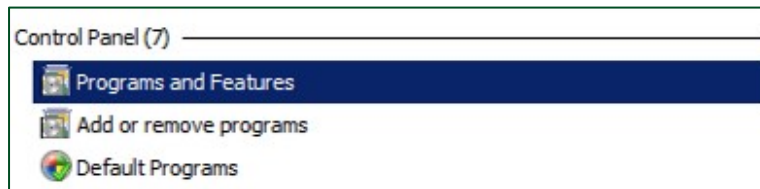


As a precaution, also enable HTTP traffic (see Proxy Setup section) if you haven't already. This will ensure that if this process has issues there is still a way to access the QMC.

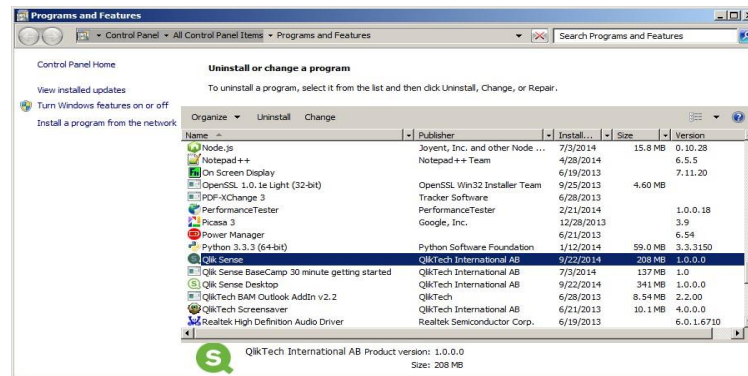
APPENDIX VIII - Qlik Sense Uninstall

This section describes how to perform a clean uninstall of Qlik Sense.

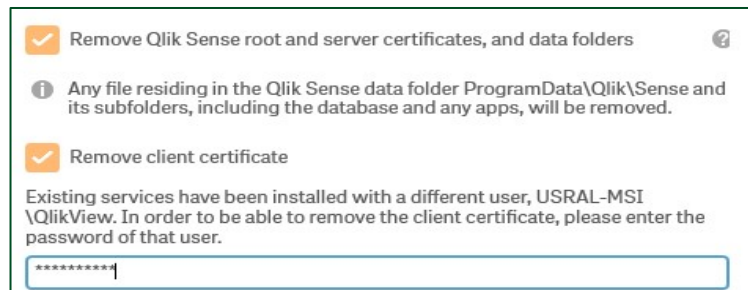
- Click **Start** > type **Programs and Features** and run **Programs and Features**



- Find **Qlik Sense** in the list and click **Uninstall**



- Check the two checkboxes to remove data and certificates.
- Enter the password of the service account running the Qlik Sense services.
- Note: This WILL delete everything. Backup apps first if you need to.



APPENDIX IX - Known Conflicts

There are known port conflicts with IIS, Skype, VMWare Workstation, Tableau and SQL Server. All of which may use port 443. Check whether this software is installed and disable the port or software.



[https://technet.microsoft.com/en-us/library/jj635851\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj635851(v=ws.11).aspx)



<https://support.skype.com/en/faq/FA148/which-ports-need-to-be-open-to-use-skypefor-windows-desktop>



<https://www.computersnyou.com/266/how-to-solve-vmware-is-using-port-443/>



<http://www.tableausoftware.com/manually-uninstalling>



Microsoft
SQL Server 2008 R2

<http://sqlmag.com/sql-server/sql-server-tcp-and-udp-ports>

Get permission to disable the windows services or uninstall the offending software.

APPENDIX X - Troubleshooting

Log Files

Log files are found in *C:\ProgramData\Qlik\Sense\Log*. In Particular, *Repository\System* and *\Trace*, and *Proxy\System* and *\Trace* are valuable to review if you have issues.

Connection Lost

If you experience a “Connection Lost” or a blank error message when opening hub, make sure you are using a URL that matches the way you installed.

- o IP address - <https://10.1.123.234/hub> o machine name – <https://WIN-Q3N0L8VHHHG>

Review the section [Proxy Setup](#).

HTTP 500 Error

If the QMC and Hub do not come up and the proxy shows a HTTP 500 error, it is likely certificate related. Check the proxy logs under *C:\ProgramData\Qlik\Sense\Log\Proxy\System*. A message about refusing connection to <https://localhost:4242> is indicative of a certificate issue. Shutdown the services and uninstall the certificates as described in the [Uninstall](#) section. Then start the services. If that doesn't work, perform a complete uninstall and reinstall.

Could not start services in a timely manner

If the windows services fail to start, stating that the services did not start in a ‘timely manner’, it is possible to extend the timeout period:

- Click Start, click Run, type `regedit`, and then click OK.
- Locate and then click the following registry subkey:
 - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control`
- In the right pane, locate the `ServicesPipeTimeout` entry.
- ****Note****: If the `ServicesPipeTimeout` entry does not exist, you must create it. To do this, follow these steps:
 - On the Edit menu, point to New, and then click `DWORD Value`.
 - Type `ServicesPipeTimeout`, and then press `ENTER`.
- Right-click `ServicesPipeTimeout`, and then click `Modify`.
- Click `Decimal`, type `60000`, and then click `OK`.
 - This value represents the time in milliseconds before a service times out.
- Restart the computer.