



# Qlik Alerting

Qlik Alerting®

November 2024

Copyright © 1993-2024 QlikTech International AB. All rights reserved.



---

<b>1 Qlik Alerting</b>	<b>6</b>
<b>2 Administration</b>	<b>7</b>
2.1 Syncing users from Qlik Sense	7
2.2 Qlik Alerting licensing	7
Equivalent privileges for alternative Qlik Sense license models	8
2.3 Filter users from Qlik Sense	8
Supported fields and related operators	8
Supported operators	9
Example queries	9
2.4 Assigning administrator rights to a user	10
2.5 Assigning user roles	10
2.6 Assigning user privileges	10
Steps to assign a user privilege	11
2.7 Enabling access for a user	11
Send a password reset email to a user	12
2.8 Disabling access for a user	12
2.9 Configuring Qlik Sense compatibility in Qlik Alerting	12
Enabling compatibility with QSEoW November 2024 and later versions	13
2.10 Using trusted SSL certificates with Qlik Alerting	13
Steps to add a trusted SSL certificate for Qlik Alerting	13
Additional steps to add SSL for Android devices	14
Managing HSTS settings for an SSL connection	14
Additional security configuration options	14
Force HTTP only with no redirect to HTTPS	15
2.11 Changing the ports for Qlik Alerting web access	16
2.12 Backup and restore the MongoDB database	16
Steps to backup	16
Steps to restore	17
2.13 Password encryption and strength	17
<b>3 Installation</b>	<b>18</b>
3.1 Installation prerequisites	18
Minimum requirements	18
Install NodeJS	19
Install MongoDB	20
Firewall settings	22
Exporting Qlik Sense certificates	22
3.2 Services and ports	23
Qlik Alerting services	23
Qlik Alerting default ports	24
3.3 Downloading installation files	25
3.4 Qlik Alerting installation	26
Validate that your Qlik Sense license includes the Qlik Alerting attribute	26
Install Qlik Alerting	26
Qlik Sense connection configuration	27
Qlik Alerting config settings	28
Email server configuration	29

---

Select an administration user .....	30
Additional step if ports were changed in Qlik Alerting settings step .....	31
Configuring single sign-on from Qlik Sense Enterprise on Windows to Qlik Alerting .....	31
3.5 Upgrade an existing version .....	35
Supported versions for upgrades .....	35
Upgrade steps .....	36
Additional information for upgrades from versions up to and including November 2020 .....	36
Troubleshooting .....	37
3.6 Database migration across servers .....	37
<b>4 Managing alerts .....</b>	<b>38</b>
4.1 Data alerts .....	38
4.2 System alerts .....	38
4.3 Broadcast notifications .....	38
4.4 Broadcast notifications .....	38
How to create a broadcast notification .....	39
4.5 Data alerts .....	40
Creating an alert .....	40
Building a data table .....	40
Condition section .....	41
Schedule section .....	45
Distribution section .....	46
Notification section .....	47
Data alert types .....	47
Managing custom notifications .....	50
Sharing an alert record .....	55
4.6 System alerts .....	56
How to create a system alert .....	56
<b>5 Mobile apps .....</b>	<b>59</b>
5.1 Who can access the Qlik Alerting mobile apps .....	59
5.2 Setting up the Qlik Alerting mobile app .....	59
5.3 Signing out from the Qlik Alerting mobile app .....	60
5.4 Navigating in the app .....	60
Settings Options .....	60
On the main alerts screen .....	61
5.5 Troubleshooting .....	62
<b>6 Qlik Sense extension .....</b>	<b>63</b>
6.1 Installing the Qlik Sense extension .....	63
Setting up a dedicated virtual proxy .....	63
6.2 The user flow of creating an alert in the extension .....	65
6.3 Default options purposefully designed in the extension .....	68
Setting up the Qlik Alerting extension on a sheet in a dashboard .....	68
6.4 Updating the default values for the extension .....	69
6.5 Troubleshooting .....	69
6.6 URL redirection support .....	70
Problem use case .....	70

## Contents

---

Configurations on Qlik Sense hub and Qlik Alerting .....	72
Configure the proxy servers .....	73
Troubleshooting for Chrome browser .....	78

# 1 Qlik Alerting

Qlik Alerting provides enterprise alerting for your Qlik Sense deployment. It offers self-service capabilities for users to create their own alerts on the data they have access to in Qlik Sense. It also provides the capability for users, often power users, to create and manage alerts for others with managed shared and broadcast alerts.

## 2 Administration

### 2.1 Syncing users from Qlik Sense

To simplify user setup, Qlik Alerting syncs users from the linked Qlik Sense installation during the initial registration process. Qlik Alerting also periodically scans the Qlik Sense user list, user licenses, and license details to remain in sync. This scan occurs every 30 minutes on completion of the previous check.

The sync process works in batches and may take a few minutes if you have a large number of users.

A Qlik Alerting admin user can also manually activate the sync process.

#### Do the following:

1. Navigate to **Admin > User Management > Users**.



*You must be logged in as an administrator to view this menu.*

2. Click **Sync with Qlik** at the top right of the table.



*This process may take a number of minutes as it schedules within the next minute and then processes the two phases as per the initial and periodic sync process.*

### 2.2 Qlik Alerting licensing

Qlik Alerting has a site-based license that will read the license details from Qlik Sense which should have the Qlik Alerting attributes as part of the license details. If you have purchased Qlik Alerting recently and this is your first install please ensure your Qlik Sense site has been updated with the revised license details as this is a prerequisite for installing.

Access privileges in Qlik Alerting are governed by the user's licensed access to Qlik Sense. The table below outlines how licenses in Qlik Sense translate to Qlik Alerting access.

Qlik Alerting licenses

#### Qlik license type

#### Qlik Alerting access and defaults

Professional

- User can create their own alerts and distribute to groups or individuals (through Broadcast and Managed Shared alerts).
- Can receive any distributed alert from other users.
- Default setup will allow advanced features such as distribution to others and share alerts but these privileges can be removed by an Admin.

### Qlik license type

### Qlik Alerting access and defaults

	<ul style="list-style-type: none"> <li>• Default setup will not allow system alerts or broadcast notifications but these permissions can be switched on by the admin for specific users through the privileges area.</li> </ul>
Analyzer	<ul style="list-style-type: none"> <li>• Standard user who can create their own alerts but is not able to distribute to groups or individuals.</li> <li>• Can receive any distributed alert from other users.</li> <li>• Will not be allowed access to any additional privileges.</li> </ul>
Capacity Analyzer	Recipient by email only, no access to web portal nor mobile app.
No license access	Recipient by email only, no access to web portal nor mobile app.



*If a user has been assigned both a Professional and Analyzer license, their experience from session to session might not be consistent. For example, sometimes, they might only receive the Qlik Alerting access associated with the Analyzer license type. To resolve this issue, consider removing the Analyzer license from a user.*

## Equivalent privileges for alternative Qlik Sense license models

- Token-based license sites will treat anyone with User Access pass or Login Access Pass as an equivalent to a Professional license.
- Core-based license sites will treat all users as an equivalent to a Professional license.

## 2.3 Filter users from Qlik Sense

You can limit the list of users that are synced across from Qlik Sense by adding a query string in the data source configuration. To understand how you are going to query the user list you can look at filters in the Qlik Management Console. Users table area as the filter query will behave in the same way as these column level filters.

### Supported fields and related operators

Qlik Alerting user sync filter fields and operators

Field name	field identifier for query	Supported operators
User directory	userDirectory	eq, ne, so
User Id	userId	eq, ne, so
Name	name	eq, ne, so
Admin roles	roles	eq,



Field name	field identifier for query	Supported operators
Tags	tags.name	eq, so
Custom properties	customProperties.value	eq, so
Created	createdDate	gt, lt
Last Modified	modifiedDate	gt, lt

### Supported operators

- eq : equal
- ne : not equal
- so : substring of
- gt : greater than
- lt : less than

Combine queries with

- and
- or

### Example queries

The following queries are examples that show how to construct both simple and more complex filter strings:

- Filter users by a single user directory.  
userDirectory eq 'exampleCompanyDomain'
- Filter users by a tag name.  
tags.name eq 'exampleTagName'
- Filter users by user directory and user id (for example where a user id is repeated across multiple domains and you just want to allow a few select users for testing).  
userDirectory eq 'exampleCompanyDomain' and (userId eq 'exampleUser1' or userId eq 'exampleUser2')
- Filter users by user directory with additional users from other user directories identified with a tag.  
userDirectory eq 'exampleCompanyDomain' or tags.name so 'exampleTagName'
- Filter users using a custom property value that is assigned to each user.  
customProperties.value eq 'exampleCustomPropertyName'
- Filter users by a user directory and only those whom have been created since 2020-01-01  
userDirectory eq 'exampleCompanyDomain' and createdDate gt '2020-01-01'

Points to consider:

- Values should be entered in single quotes.
- Filter values are case insensitive.

- Be sure to check which operators are relevant for each filter field, using an unsupported approach may provide unexpected results.

### 2.4 Assigning administrator rights to a user

---

You will need to always have at least one administrator user at any one time. There is no limit on how many administrator users you can assign.

**Do the following:**

1. Navigate to **Admin > User Management > Users**.
2. Use the search object to find the user you wish to make an administrator and highlight that row.
3. Click on the ... button and select edit.
4. Change the **user / administrator** radio selection to **administrator**.
5. Click **Save**.

### 2.5 Assigning user roles

---

There are two different types of user roles in Qlik Alerting: user and administrator. An administrator will have access to all functionality to be able to manage all aspects of the Qlik Alerting site.

### 2.6 Assigning user privileges

---

Professional level users can be given additional functionality through the assignment of user privileges. Only professional level users will be shown in the assigner user lists for privileges as other users cannot be assigned additional privileges. Administrator role users are also excluded from this list as they have access to all privileges as part of their user role.

The following user privileges are available:

User privilege categories

User privilege	Description
System Alerts	Allows a professional Qlik Sense licensed user access to system alerts functionality to create and receive system alert notifications.
Distribution Setting	Allows a professional Qlik Sense licensed user access to create broadcast and managed shared alerts which are sent to users with either a standard or a broadcast license.
Broadcast Notification	Allows a professional Qlik Sense licensed user access to create and manage broadcast notifications. These are manually created notification messages that can be sent to a user group.

Share Alerts	Allows a professional Qlik Sense licensed user to be able to share alert records they have created with other named professional or analyzer licensed users who are enabled in Qlik Alerting. This functionality makes a copy of the alert record that the recipient will take ownership of when they accept.
--------------	---

### Steps to assign a user privilege

#### Do the following:

1. Navigate to **Admin > User Management > User Privileges**. (You will need to be logged in as an administrator to view this menu.)

You will see a table that identifies the user privilege types available with a count to help you see what has been assigned.

2. Click the edit link of the user privilege type to which you wish to assign users.

The next page will show you two lists of users, on the left those who have not been assigned this privilege and on the right those who are already assigned.

3. Select those users you wish to move, use the search to find users easily.
4. Click the direction arrows to move them from one list to the other.
5. Click **Update**.

## 2.7 Enabling access for a user

---

A user will automatically be enabled to use Qlik Alerting based on their license allocation rights in Qlik Sense. You can disable their access as identified below. However, any user who wishes to create and/or to receive an alert will require an email address to be stored against their user record in Qlik Alerting. The email can come from one of two sources; the Qlik Sense user sync if the email address is an attribute stored against the user in Qlik Sense (i.e. it comes from the user directory connector) or the email can be entered and saved directly in Qlik Alerting.



*For a user to receive alerts on their mobile device they will need to create a password for Qlik Alerting and email is required for this step.*

To enter a user's email address do the following:

1. Navigate to **Admin > User Management > Users** (you will need to be logged in as an administrator in Qlik Alerting to see this page).
2. Search for the user you wish to add an email for.
3. Click on the ... menu on the user and select **Edit**.
4. Enter the email address in the **Email ID** field.
5. Click **Save**.

The user should now be able to receive email notifications, if they have an appropriate license in Qlik Sense, and can request to set their password from the Qlik Alerting login page.

### Send a password reset email to a user

An administrator can trigger an email to a user to allow them to set/reset their password from that email link. Do the following:

1. Navigate to **Admin > User Management > Users** (you will need to be logged in as an administrator in Qlik Alerting to see this page).
2. Find the user to send a password set/reset email to.
3. Click on the ... menu and select Reset password and confirm.

Multiple users can be selected to set/reset their passwords using the Reset password button at the top of the table.



*The password reset email that is sent has a one time use token that is active for 30 minutes. If the link is not accessed within 30 minutes, the password reset must be requested again, or you must select the **forgot password** option.*

## 2.8 Disabling access for a user

---

Disable the user in the **Admin > User Management > Users** area. Click the enabled switch against the user to turn off the users access.



*If the user has an Administrator role assigned, they will still be able to log in if they do not have a Qlik Sense named license but they will not receive triggered alerts. Other users will not be able to log on if they do not have a license in Qlik Sense.*

## 2.9 Configuring Qlik Sense compatibility in Qlik Alerting

---

The `websocketEnabled` flag in Qlik Alerting controls compatibility with different versions of Qlik Sense Enterprise on Windows (QSEoW) by managing the security requirements for WebSocket connections. This setting is essential for supporting newer versions, which require enhanced security.

- **False** (default): When `websocketEnabled` is set to false, Qlik Alerting does not support QSEoW November 2024 or later versions because they require Extended CSRF protection for WebSocket requests.
- **True**: When `websocketEnabled` is set to true, Qlik Alerting enables Extended CSRF protection, making it compatible with QSEoW November 2024 and later versions.

### Enabling compatibility with QSEoW November 2024 and later versions

1. Locate the configuration file. The `websocketEnabled` flag is located in the `default.json` file at:  
`C:\Program Files\Qlik Alerting\qlik-connector\config\default.json`
2. Open the file in a text editor and find the line:  
`"websocketEnabled": false`
3. Change it to:  
`"websocketEnabled": true`
4. Save the file and restart Qlik Alerting.

## 2.10 Using trusted SSL certificates with Qlik Alerting

---

The Qlik Alerting install ships with a default self-signed certificate to secure the connection between the desktop of the user and the hosted application. This is a secure approach that enables HTTPS connections but will result in error messages in browsers, such as “The site’s security certificate is not trusted” (Chrome) or “This Connection is Untrusted” (Firefox).

This also has an effect on the way the Qlik Alerting Extension will work in Qlik Sense as this can cause cross-domain errors which require the user to click on a message that allows the browser to ‘run unsafe scripts’ (not an optimal user experience).

### Steps to add a trusted SSL certificate for Qlik Alerting

#### Do the following:

1. Access the Qlik Alerting server via remote desktop.
2. Navigate to the `C:\Program Files\Qlik Alerting\config\certificates` folder.
3. Backup the `server.pem` and `server_key.pem` certificate files, so you can rollback the change if necessary.



*If you have been using a previous version of Qlik Alerting or Ping Alerting and have `client.pem` and `client_key.pem` certificates, you can simply rename them. Replace `client` with `server`.*



*Pass phrases for SSL certificates are not supported at this time.*

4. Replace the certificate files with your equivalent `server.pem` and `server_key.pem` certificate files.
5. Restart the Qlik Alerting Gateway service.

### Additional steps to add SSL for Android devices

The Android OS does not always fully recognize the SSL certificate for use by the Qlik Alerting mobile app.

Do the following:

1. Access the Qlik Alerting server via remote desktop.
2. Navigate to the `C:\Program Files\Qlik Alerting\config\certificates` folder.
3. Add the `*CA.crt` file for your SSL certificate, you will need to rename the file to be `CA.crt` so remove any additional naming on the file itself.
4. Restart the Qlik Alerting Gateway service.

### Managing HSTS settings for an SSL connection

By default Qlik Alerting is set as securely as possible and we have HSTS headers enabled. This means that if you have connected to the site as HTTP or HTTPS you will be forced to connect (by the browser) as HTTPS the next time you connect. This has caused some issues with connections from the extension and mobile app where the environments are not fully secured with 3rd party trusted certificates. The `HstsMaxAge` setting can be managed to disable this behaviour, follow the steps below.

**Do the following:**

1. Access the Qlik Alerting server via remote desktop.
2. Navigate to the `C:\Program Files\Qlik Alerting\config` folder.
3. Update the `default.json` file to include the following `hstsMaxAge` object before the gateway object:

```
{
  "hstsMaxAge": 31536000,
  "gateway": {
    "ip": "localhost",
    "httpPort": 4551,
    "httpsPort": 4552,
    "https": true
  },
  ...
}
```
4. If you have added other custom configuration changes (such as a connection to an external MongoDB instance) you may have multiple other attributes above the gateway object.
5. Restart the Qlik Alerting Gateway service to pick up the new settings.

### Additional security configuration options

Additional configuration options are available for organizations who wish to manage security tightly or wish to be specific about which security features to apply:

- Allow or block HTTP access.
- Allow or block TLS 1.2 (default), TLS 1.1, or TLS 1.0.
- Add additional security headers to manage CORS access and other security restrictions.

To access these settings do the following:

1. Access the Qlik Alerting server via remote desktop.
2. Navigate to the `C:\Program Files\Qlik Alerting\config` folder.
3. Update the default.json file to include the required object and key:value settings before the gateway object:

```
{
  "allowInsecure": {
    "http": false,
    "TLSv1": false,
    "TLSv1_1": false,
    "TLSv1_2": true
  },
  "customHeaders": {},
  "gateway": {
    "ip": "localhost",
    "httpPort": 4551,
    "httpsPort": 4552,
    "https": true
  },
  ...
}
```

4. If you have added other custom configuration changes (such as a connection to an external MongoDB instance) you may have multiple other attributes above the gateway object.
5. Restart the Qlik Alerting Gateway service to pick up the new settings.

### Force HTTP only with no redirect to HTTPS



*This is an unsecured approach and not recommended for production environments.*

Do the following:

1. Access the Qlik Alerting server via remote desktop.
2. Navigate to the `C:\Program Files\Qlik Alerting\config` folder.
3. Update the default.json file to include the required "allowInsecure" object with the "http": true setting before the gateway object.
4. Update the https key in the gateway object to false.

```
{
  "allowInsecure": {
    "http": true
  },
  "gateway": {
    "ip": "localhost",
    "httpPort": 4551,
    "httpsPort": 4552,
    "https": false
  },
  ...
}
```

5. If you have added other custom configuration changes (such as a connection to an external MongoDB instance) you may have multiple other attributes above the gateway object.
6. Restart the Qlik Alerting Gateway service to pick up the new settings.

## 2.11 Changing the ports for Qlik Alerting web access

---

If you wish to change the default ports from 4551 for HTTP and 4552 for HTTPS you must make this change in two places. For example, if you are running Qlik Alerting on a stand alone server with no other programs reserving these ports, you may wish to use ports 80 (HTTP) and 443 (HTTPS), which makes it easy for a user as they do not have to enter these default ports in the URL each time.

### Do the following:

1. Update the settings in the web UI.
  - a. In the Qlik Alerting web portal, navigate to **Admin > Config**.
  - b. Update the HTTP and HTTPS ports to those you would like to change to, for example 80 (HTTP) and 443 (HTTPS).
  - c. Click **Save**.
2. Update the config file for the services.
  - a. On the server, navigate to *C:\Program Files\Qlik Alerting\config*.
  - b. Open the *default.json* file.
  - c. On line 4, edit "httpPort": 4551; changing the 4551 value to your HTTP port entered in the Qlik Alerting settings step, for example port 80.
  - d. On line 5, edit "httpsPort": 4552; changing the 4552 value to your HTTPS port entered in the Qlik Alerting settings step, for example port 443.

```
{
  "gateway": {
    "ip": "localhost",
    "httpPort": 80,
    "httpsPort": 443,
    "https": true
  },
  ...
```
  - e. Restart the Qlik Alerting Gateway service.
3. You should now be able to access Qlik Alerting through these new ports.
4. If you have used the Qlik Sense extension in any app, you will need to reset the port setting in each of these instances.

## 2.12 Backup and restore the MongoDB database

---

You will want to periodically backup the MongoDB database as this serves as the core of Qlik Alerting. It is recommended that you backup the database before each install.

### Steps to backup

1. RDP onto the server as an administrator user.
2. Open a command window as an administrator.



3. Enter the following to change directory:

```
cd "C:\Program Files\MongoDB\Server\4.2\bin"
```



*If you are using a newer version of MongoDB, or it is located in a different location such as a D:\ drive, then please adjust this appropriately.*

4. Enter the following command, where *Backup Name* is the identifier for your backup:

```
mongodump --db=qlikalerting --out="Backup Name"
```

5. This will create a new folder in the *C:\Program Files\MongoDB\Server\4.2\bin* folder called "Backup Name" and will export all of the data from the database into JSON format files.
6. Zip this new folder and store where you require.

### Steps to restore

1. RDP onto the server as an administrator user.
2. Open a command window as an administrator.
3. Enter the following to change directory:

```
cd "C:\Program Files\MongoDB\Server\4.2\bin"
```



*If you are using a newer version of MongoDB, or it is located in a different location such as a D:\ drive, then please adjust this appropriately.*

4. Move the backup to a location that is easy to identify and unzip the file so the folder is located here, for example *D:\backups\Backup Name*.
5. Enter the following command, where *Backup Name* is the identifier for your backup:  

```
mongorestore "D:\backups\Backup Name"
```
6. You will now have restored the qlikalerting database in MongoDB.

## 2.13 Password encryption and strength

---

The Qlik Alerting platform uses Crypto-js for password hashing. The application uses the SHA-512 algorithm.

User passwords do not expire. The current password security requirements are as follows:

- At least one uppercase character
- At least one lowercase character
- At least one integer
- Password must contain a minimum of eight characters

## 3 Installation

Installing Qlik Alerting for Qlik Sense Enterprise on Windows is unbundled to make the install as flexible as possible. We have not bundled the NodeJS nor MongoDB database components into the installer to ensure that you can setup the process as you need to for your organization. For example, you may have an enterprise version of MongoDB running on another server and wish to re-use that resource rather than install another instance locally for Qlik Alerting.

The main prerequisites for an installation are:

- A Windows server that meets the minimum requirements as identified in the prerequisites page.
- An install of MongoDB, locally or on another server.
- Administrator access to the server to update firewall settings.
- Administrator access to the server to install Qlik Alerting.
- A Qlik Sense Enterprise on Windows site with a license key that includes the Qlik Alerting license attribute.

Follow the steps in [Installation prerequisites \(page 18\)](#) to ensure you are prepared to install Qlik Alerting.

Once these prerequisites are complete you can install Qlik Alerting and go through the setup process as documented in [Qlik Alerting installation \(page 26\)](#).

### 3.1 Installation prerequisites

#### Minimum requirements

You can install Qlik Alerting on the same server as Qlik Sense, or you can install it on its own server. To follow Qlik's best practices, it is recommended to use dedicated hardware to run Qlik Sense. For Qlik Alerting, ensure you meet the minimum hardware requirements.

Hardware and software requirements

<b>Platforms</b>	Microsoft Windows Server 2016 Microsoft Windows Server 2019 Microsoft Windows Server 2022
<b>Processors (CPUs)</b>	Multi-Core x64 compatible processors
<b>Memory</b>	8 GB RAM minimum
<b>Disk Space</b>	32 GB minimum
<b>Mobile App Android</b>	Android 12 or later
<b>Mobile App iOS</b>	iOS 16 or later

### Qlik Sense Enterprise on Windows requirements

Qlik Alerting uses the stable standard APIs from Qlik Sense Enterprise on Windows. While Qlik Alerting might work on older versions of Qlik Sense Enterprise on Windows, as far back as version 3.1 (from 2016), we highly recommend that you keep your Qlik Sense and Qlik Alerting installations up to date to make the most of the new functionality and to be covered by the Qlik support policies.

The minimum recommended version of Qlik Sense Enterprise on Windows is August 2021 for basic authentication and May 2023 for SSO authentication.

### Install NodeJS



*Qlik does not support the NodeJS product that is required to use Qlik Alerting, and any support should be directed to your NodeJS provider. Qlik does support the Qlik Alerting software that is installed as part of the installation package.*

NodeJS is the core engine of Qlik Alerting.



#### Do the following:

1. Download NodeJS for Windows from the  [Nodes.js® web site](https://nodejs.org/).

- **NodeJs v20.17.0** is supported.

Select the appropriate Windows installer for your system.

Direct download links:

-  [node-v20.17.0-x64.msi](#)
-  [node-v20.17.0-x86.msi](#)

2. Run the installer (the .msi file you downloaded in the previous step).
3. Follow the prompts in the installer.
  - a. Accept the license agreement.
  - b. Click **Next** several times.
  - c. Accept all the default installation settings.

You can make sure you have Node and NPM installed by running the following simple commands to see what version of each is installed.

#### Test Node

##### Do the following:

- Open the Command window, PowerShell, or a similar command line tool, and run:

```
node -v
```

This should print a version number. You will see something like v10.19.0.

#### Test NPM

##### Do the following:

- Open the Command window, PowerShell, or a similar command line tool, and run:

```
npm -v
```

This should print NPM's version number. You will see something like 6.13.4.

### Install MongoDB



*Qlik does not support the MongoDB product that is required to use Qlik Alerting, and any support should be directed to your MongoDB provider. Qlik does support the Qlik Alerting software that is installed as part of the installation package.*

MongoDB is the only database required for Qlik Alerting. Redis is no longer required as both the repository and the persistent cache/queue are now managed by MongoDB.



#### Do the following:

1. Download  [MongoDB](#) for Windows.

- **MongDB 5.0 and 6.0**

Supported on Windows Server 2016 and 2019.

Direct download links:

-  [mongodb-windows-x86\\_64-5.0.28-signed.msi](#)
-  [mongodb-windows-x86\\_64-6.0.17-signed.msi](#)

- **MongDB 7.0 and later**

Supported on Windows Server 2019 and 2022.

Direct download link:

-  [mongodb-windows-x86\\_64-7.0.14-signed.msi](#)

An .msi file will be downloaded on your server.

2. Double-click the file to run the installer.
3. Click **Next** when the MongoDB installation window pops up.
4. Accept the MongoDB user agreement and click **Next**.
5. When the setup asks you to choose the **Setup type**, choose *Complete*.
6. Accept the default **Service Configuration** settings and click **Next**.
7. Click **Install** to begin the installation.
8. Click **Finish** once the MongoDB installation is complete.

#### Alternative MongoDB options

You are able to use a previous install of MongoDB as your host for the Qlik Alerting repository if required. You will need to manage the firewalls between the two servers to ensure the Qlik Alerting server can access the MongoDB host server and port and secure the connection appropriately. You will also need to manage the authorization appropriately.

To change the config settings for the connection to MongoDB navigate to the main config file `C:\Program Files\Qlik Alerting\config\default.json` and do the following:

- Open the default.json file in a text editor.
- Update the default.json file to include the following mongodb object before the gateway object:

```
{
  "mongodb": {
    "database": "qlikalerting",
    "ip": "127.0.0.1",
    "port": 27017,
    "auth": false,
    "authDatabase": null,
    "user": null,
    "password": null,
    "connectionString": null
  },
  "gateway": {
    "ip": "localhost",
    "httpPort": 4551,
    "httpsPort": 4552,
    "https": true
  },
  ...
}
```

- Restart the Qlik Alerting Repository and Qlik Alerting Queuer services to pick up the new settings.
- The settings above are the default settings for a locally installed default instance of MongoDB. To update the settings to your external or cloud instance of MongoDB change the attributes based on the explanation below:

- "database": "qlikalerting"

The database in which all of the Qlik Alerting collections will be stored. This should be left as qlikalerting for simplicity.

- "ip": "localhost"

The IP or DNS of the MongoDB server to which you want to connect.

- "port": 27017

The port to connect to the database, default for Mongo is 27017.

- "auth": false

Change to true if you need to authenticate against the Mongo DB instance.

- "authDatabase": null

Identify the database required for authentication as this may be different to the qlikalerting database.

- "user": null

Enter the user for the connection.

- "password": null

Enter the password for the user to connect.

- "connectionString": null

Leave null if above is completed. If you are using the connection string, only the database field will be required in addition to the connection string.

### Supported setups

- To connect to a standalone database (single database node) you can use the specific connection details or the connectionString.
- To connect to MongoDB Atlas (cloud), a replica set or a shared cluster you should use the connectionString.

For information on how to construct your connection string, see your MongoDB admin or read more at [docs.mongodb.com](https://docs.mongodb.com).

### Firewall settings

There are ports that are required to be opened in order to enable communication between Qlik Alerting and Qlik Sense.



*For mobile messaging to work, Qlik Alerting requires direct internet access.*

You will need to open one or both of the following ports on the Qlik Alerting server:

- 4551 (HTTP)
- 4552 (HTTPS)

If you plan to update Qlik Alerting to use nonstandard ports (such as 443 for HTTPS rather than 4552) then please ensure the desired port is open.

You will need to open the following ports on the Qlik Sense central node (and separate proxy server if necessary):

- 443 (HTTPS access to Qlik Sense Proxy)
- 4242 (Qlik Sense Repository Service API listen port)
- 4243 (Qlik REST API listen port)
- 9200 (Qlik Licensing Service)

### Exporting Qlik Sense certificates

In order for Qlik Alerting to connect to Qlik Sense we require certificates to be exported from Qlik Sense for the server on which the Qlik Alerting server is installed.

#### Do the following:

1. Go to the Qlik Management Console (QMC) on your Qlik Sense Server.
2. Click **Start > Certificates**.
3. Enter your **Machine name**. This will be the IP or machine name of the server.
4. Enter a **Certificate password**.
5. Select the **Include secret key** check box.

6. Select *Platform independent PEM-format* for **Export file format for certificates**.
7. Click **Export Certificates**.

You will need to access the Server OS to retrieve these certificates from the relevant folder. The default folder is `C:\ProgramData\Qlik\Sense\Repository\Exported Certificates`.

Copy these certificates to a location that can be accessed by the Qlik Alerting Server when going through the initial setup or data source process.

For more information, see [Exporting certificates through the QMC](#).

## 3.2 Services and ports

---

The Qlik Alerting services run as Microsoft Windows services, which you can deploy on a single server. PoC and testing environments can however be installed on the same server as Qlik Sense.

### Qlik Alerting services

The Qlik Alerting architecture runs as a number of individual services. All Qlik Alerting services are prefixed with *Qlik Alerting* in the windows installer to ensure they are ordered consistently in the windows services views.

Qlik Alerting services

Service name	Description
<b>Gateway</b>	The Gateway service manages access and routes to all Qlik Alerting services. It ensures the simple management of any changes between front end and back end components.
<b>Scheduler</b>	The Scheduler service manages any event that is triggered based on a time-based schedule. It identifies the next time that any Qlik Sense reload task scan is due, the next time any alert record based on a schedule, or the next daily digest runtime. The Scheduler adds records to the database to act as a queue for future events.
<b>Queuer</b>	The Queuer service manages tasks that have been triggered but have not yet been picked up by the Worker for action. It is the backlog of work items to be processed. This service checks the database to add any scheduled events that are due but also receives queue requests from the Worker which will add additional work tasks to the queue during and on completion of other work tasks.


<b>Worker</b>	<p>The Worker service is the orchestrator of all the different tasks that are required to run the different processes in Qlik Alerting. It picks up the next task from the Queue and process it and therefore it orchestrates many different tasks. For example:</p> <ul style="list-style-type: none"> <li>• It checks reload tasks in Qlik Sense, identifies alerts with on-reload triggers of the apps that have reloaded, and adds those alerts into the Queue.</li> <li>• It sends a retry request to the queue if a process fails.</li> <li>• It processes data alert scans, gets the data from Qlik Sense and checks these against the conditions set for the alert that sends the task to the Notification Hub if an alert notification is to be sent.</li> </ul>
<b>Connector Hub</b>	<p>The Connector Hub service is a connector gateway that ensures that all core actions are consistent and resolves these requests to the relevant connector type. It also manages a queue in the database that ensures large spikes in requests are managed effectively.</p>
<b>Qlik Connector</b>	<p>The Qlik Connector service manages all access to Qlik Sense, including user session management and all other calls made to Qlik Sense to access metadata and application data.</p>
<b>Condition</b>	<p>The Condition service offers the validation engine where alert details and data from the scan are checked.</p>
<b>Notification Hub</b>	<p>The Notification Hub service manages actions when alert notifications are triggered. It manages requests to ensure that the relevant notification services receives information to send different types of notifications. . It also manages a queue in the database that ensures large spikes in requests are managed effectively.</p>
<b>Email Messenger</b>	<p>The Email Messenger manages email notifications sent through the identified mail server. It manages the authentication to the mail server, and the formatting of the mail information.</p>
<b>Mobile Messenger</b>	<p>The Mobile Messenger manages push notification to mobile devices so alert messages are sent directly to the notifications window on the mobile device. It also passes encrypted alert data to a real-time firebase database for the device to retrieve when the mobile app is opened, or when a message is received, and triggers the record to be grabbed.</p>
<b>Repository</b>	<p>The Repository service manages traffic from different services through to the dependent databases. This allows graceful management of the traffic to and from the database.</p>

### Qlik Alerting default ports

The following tables are an overview of the ports used in a Qlik Alerting architecture.



## Default ports

Service name	Default port setup
<b>Gateway</b>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  All traffic from external systems connects through this service. </div> 4551 (HTTP) 4552 (HTTPS)
<b>Scheduler</b>	4562 (HTTPS)
<b>Queuer</b>	4561 (HTTPS)
<b>Worker</b>	4563 (HTTPS)
<b>Connector Hub</b>	4565 (HTTPS)
<b>Qlik Connector</b>	4566 (HTTPS)
<b>Condition</b>	4564 (HTTPS)
<b>Notification Hub</b>	4567 (HTTPS)
<b>Email Messenger</b>	4568 (HTTPS)
<b>Mobile Messenger</b>	4569 (HTTPS)
<b>Repository</b>	4560 (HTTPS)

## Other components default ports

## Other components

Service name	Default port setup
<b>MongoDB</b>	27017 (TCP/IP)
<b>Redis</b>	6379 (TCP/IP)

### 3.3 Downloading installation files

The Qlik Download Site provides the files you need to install and upgrade Qlik products. You can find the site in Qlik Community under Support > Product News > Product Downloads.

Do the following:

1. Go to [Product Downloads](#).
2. Select **Qlik Data Analytics** or **Qlik Data Integration**, and then select your product.
3. Use the filters to narrow your list of possible downloads.
4. Click a link in the **Download Link** column in the **Download Assets** table to start the download.

## 3.4 Qlik Alerting installation



Ensure you have installed NodeJS and MongoDB as per the [Installation prerequisites \(page 18\)](#) instructions.


### Validate that your Qlik Sense license includes the Qlik Alerting attribute

Qlik Alerting uses an integrated license module with Qlik Sense. As the data source is setup, Qlik Alerting will read the licensing attributes from the Qlik Sense license data. There should be a Qlik Alerting attribute in this data that will provide all of the details required. In order to check that your license key includes the Qlik Alerting attribute, do the following:

1. In the Qlik Sense QMC navigate to **License management > Site license**.
2. Check the license details.
  - a. If you have a token-based license you should:
    - i. Expand the LEF access section.
    - ii. Validate that the QLIK\_ALERTING attribute is present in the license details.
    - iii. If no QLIK\_ALERTING license attribute can be found, you may need to re-enter and re-validate your license.
  - b. For serial license keys you will need to:
    - i. Retrieve the license Key, for example, 1234 0000 0000 1234.
    - ii. Go to [lef1.qliktech.com](https://lef1.qliktech.com) and enter this license key without spaces.
    - iii. Click on captcha and click the request LEF.
    - iv. Validate that the QLIK\_ALERTING attribute is present in the license details.
    - v. If no QLIK\_ALERTING license attribute can be found, you may need to wait for the license to refresh.

### Install Qlik Alerting

#### Do the following:

1. Check that the MongoDB service is running in the Windows services window or that your server has access to the external MongoDB instance.
2. Download the Qlik Alerting installer and save it to you hard drive ready for installation. This is accessible from  [Product Downloads](#).  
See: [Downloading installation files \(page 25\)](#)
3. Right-click the *Qlik Alerting Installer.exe* file, and then click **Run as Administrator**.
4. Click **Yes** if you get the **User Account Control** message.
5. Accept the license agreement and click **Next**.
6. Once the installation is finished, open Windows services and check to ensure that all the Qlik Alerting services are running. If any of these are not running, start through this window.

Access Qlik Alerting through the browser on the server, use `http://localhost:4551` or `https://localhost:4552` for the initial setup. You can also access the server from your desktop browser if you have setup the appropriate firewall and server DNS details.

### Qlik Sense connection configuration

#### Do the following:

1. Enter the following details for your Qlik Sense site.
  - **Qlik Sense hostname** is the IP or DNS of the Qlik Sense Server. (This should be an allow-listed value in the Qlik Sense Virtual Proxy is the URL which you use to access the server from any desktop.)
  - **Qlik Sense Service listen port HTTPS** is the HTTPS connection port for Qlik Sense. This will normally be the default value of 443 but if this has been customized you can change the value here. You can see if this and the following Qlik Ports have been customized in the Qlik Management Console (QMC) in the settings for the proxy you will be connection to.
  - **Qlik REST API listen port** will default to 4243 as per the standard install of Qlik Sense.
  - **Qlik Repository API listen port** will default to 4242 as per the standard install of Qlik Sense.
  - **Connect as user directory** is the Qlik Sense directory that the above user is assigned to.
  - **Connect as user id** is the Qlik Sense UserID that you will use to test the connection and run some of the background connection tasks.



*Ensure this user is a root admin in Qlik Sense or a user who can access all users, tasks, and apps. This user must also have a valid license in Qlik Sense.*

- **Filter for user fetch** (optional) allows the limiting of the users that will sync across from Qlik Sense. See [Filter users from Qlik Sense \(page 8\)](#) for details on the options and syntax to use.
- **Virtual proxy prefix** (optional) will remain blank by default. Qlik Alerting connects using the Windows authentication pattern. In most cases the 'Central Proxy (Default)' virtual proxy setup will work in this way so you can leave this field blank. If you have a different authentication setup, or wish to connect to a different virtual proxy, enter the Prefix for the virtual proxy in this field.
- **Session cookie header name** will default to X-Qlik-Session. This is the standard setup of the default virtual proxy. If you are connecting to different virtual proxy, this value will be changed (as it is distinct for each virtual proxy). Check the virtual proxy in the QMC to identify the value to enter here. It is common to use X-Qlik-Session-`<Prefix>` but this is not mandatory.

- **Alias hostname** allows you to enter a different URL for user access to the server and is used in all Qlik Sense links in emails and mobile notifications.
  - Ensure that this is the URL that users use to access the Qlik Sense environment from their browsers.
  - If users access with a different virtual proxy to the data connection above, add this virtual proxy to the URL, for example, qlik sense . company . com / okta where okta is the user access virtual proxy prefix.
  - If you are using the Qlik Alerting extension and connecting to it with a proxy or reverse proxy, enter the server address in the **Reverse proxy URL redirection** field.
- **Authentication** specifies the authentication pattern. To enable single sign-on authentication using Qlik Sense Enterprise on Windows credentials, select **SSO**. Then add the authentication URL in the **Authentication URL** field.

For information on how to set up single sign-on authentication, see [Configuring single sign-on from Qlik Sense Enterprise on Windows to Qlik Alerting \(page 31\)](#).

2. On the right hand side use the buttons to upload your certificates that have been exported from Qlik Sense, you need only the *client.pem* and *client\_key.pem* files.

See [Exporting Qlik Sense certificates \(page 22\)](#) for instructions on how to obtain the certificates from Qlik Sense.



*Ensure you have recently updated certificates from Qlik Sense as these exported certificates can be invalid after a Qlik Sense Enterprise upgrade. The Qlik Sense Enterprise February 2020 release was a release which requires all exported certificates to be regenerated.*

3. Click **Test Connection**. You should see a message saying connection successful.
4. Click **Save** to save your configuration settings.



*During this connection process the Qlik Alerting license attribute will be retrieved from Qlik Sense and all users will sync across (for the first time).*

### Qlik Alerting config settings

Enter the following details in order to ensure that all of the settings for the Qlik Alerting host server are correct.

#### Do the following:

1. Enter the **Qlik Alerting Host Server Name**. This should be the public IP address or fully qualified domain name (DNS) of the server on which you are installing Qlik Alerting. This is used in the generation of the email links, so it should be the external address which you would normally access from your desktop browser.
2. Check the **HTTP and HTTPS Ports**.

The default ports for Qlik Alerting are 4551 and 4552 but you can change those here if necessary. Be sure to open the firewall for your custom ports if you choose to change them. For example, if Qlik Alerting is installed on a stand alone machine the default ports can be changed to 80 (HTTP) and 443 (HTTPS) removing the need for users to specify the port when accessing Qlik Alerting in their browser.



*If you do change the port settings there is an additional step where you must manually configure the ports in a config file on the server once you have completed this process.*

### Email server configuration

Follow the steps below to configure the email server. This is required, even if you do not wish to receive alerts on email, as all password management etc is managed through email.

#### Do the following:

1. Enter your mail server details:
  - Address, e.g. smtp.domain.com
  - Port No.
  - Secured: SSL / TLS / None



*You may need to check the instructions below even when you have selected **None**, as later NodeJS versions require specific overrides of TLS versions. [Node.js](#) version 11.40 added the `tls.DEFAULT_MIN_VERSION` attribute, which is set to version 1.2. If the mail server you want to connect to uses TLS 1.1 or earlier, you need to override the default setting. See [Allow less secure TLS connections to your mail server \(page 30\)](#) for instructions on how to change the default version.*

- Authentication Method: Basic or Anonymous
  - User name, this is typically the email for the account but can be an ID if required (see Test email address below if an ID is used)
  - Password, this can be left blank if not required by your mail server.
  - Default sender, the email address the user will see the email has been sent by which can also include the user name, for example you can enter "Qlik Alerting" <noreply@qlikalerting.com>
  - Test email address, this is required if you are using an ID in the Username field as the test connection validation will attempt to send an email to either the test email address or the username.
2. Click **Test Connection**. You will see a message pop-up at the bottom of the screen and should receive an automated email message to the email account entered.
  3. Click **Save** to save your configurations settings.

To edit these settings outside of the registration process, go to **Admin > Channels**.



Ensure you have the correct firewall settings for Qlik Alerting to communicate with your mail server. To review the logs to see the error returned for the failed connection go to the `C:\ProgramData\QlikAlerting\email-messenger` folder and open the most recently updated file.

### Allow less secure TLS connections to your mail server

We have encountered some environments where the connection to the mail server requires an additional setting to enable NodeJS to allow less secure connections. If you have done everything you think necessary to connect to your mail server and there is still an issue please check with your mail server administrator the TLS version that the mail server requires. To update this setting do the following:

1. Access the Qlik Alerting server via remote desktop.
2. Navigate to the `C:\Program Files\Qlik Alerting\config` folder.
3. Update the `default.json` file to include a new key `"tlsMinVersion": 1.1` before the gateway object. The values here can be 1.0 or 1.1 depending on the setup of the mail server and network architecture. The default value is 1.2 at this time.
4. Update the `https` key in the gateway object to `false`.

```
{
  "tlsMinVersion": 1.1,
  "gateway": {
    "ip": "localhost",
    "httpPort": 4551,
    "httpsPort": 4552,
    "https": false
  },
  ...
}
```

5. If you have added other custom configuration changes (such as a connection to an external MongoDB instance) you may have multiple other attributes above the gateway object.
6. Restart the Qlik Alerting email messenger service to pick up the new settings.

### Select an administration user

In order to manage the Qlik Alerting site an administration user must be present in the Qlik Alerting repository. Enter the `domain\username` of the administration user to search for the correct user.

If no email address is present for this selected admin user you will be prompted to add an email to ensure that you can set the password when first logging on.



This can occur when there are no emails stored in Qlik Sense.

Qlik Alerting will send you an email directly with a set password link. Click on this to set your password.



If for some reason you cannot find this email then go to the logon page <https://QlikAlertingServer:4552>, click the forgotten password link, enter your username and click **Recover Password**.

### Additional step if ports were changed in Qlik Alerting settings step



This step is only required if the ports have been changed from the default 4551/4552 ports.

#### Do the following:


1. On the server navigate to `C:\Program Files\Qlik Alerting\config`.
2. Open the `default.json` file in a text editor.
3. In the gateway object, on line 4 by default, edit `"httpPort": 4551`; changing the 4551 value to your HTTP port entered in the Qlik Alerting settings step, for example port 80.
4. On line 5, edit `"httpsPort": 4552`; changing the 4552 value to your HTTPS port entered in the Qlik Alerting settings step, for example port 443.

```
{  
  "gateway": {  
    "ip": "localhost",  
    "httpPort": 80,  
    "httpsPort": 443,  
    "https": true  
  },  
}
```

5. Restart the Qlik Alerting Gateway service.

## Configuring single sign-on from Qlik Sense Enterprise on Windows to Qlik Alerting

Configure single sign-on (SSO) to allow users to authenticate to Qlik Alerting using Qlik Sense Enterprise on Windows credentials. With SSO, you don't need any other authentication within Qlik Alerting.

When you have configured external product sign-on to Qlik Alerting, users with permission will see a new menu item with  in their user profile menu in the Qlik Sense hub. When the users click the button, they are redirected to the configured sign-on URI path, where they are authenticated. Once successfully authenticated, the users are taken to the Qlik Alerting start page.

To set up SSO authentication to Qlik Alerting, you need to configure external product sign-on in the QMC with Qlik Alerting as the external product. Upload an SSO script in the QMC to create an authentication URL, and then add the URL in the Qlik Alerting configuration.

#### Prerequisites

- Qlik Sense Enterprise on Windows May 2023 or later.
- Qlik Alerting July 2023 or later.




SSO between Qlik Alerting and Qlik Sense Windows requires a direct connection to the Qlik Sense central node in multi-node deployments. This means load balancers or other configurations that redirect traffic should not be used for this connection.

### Configuring SSO authentication in the Qlik Management Console

You need **RootAdmin**, **ContentAdmin**, or **DeploymentAdmin** role to configure external product sign-on.

Do the following:

1. Open the QMC: *https://<QPS server name>/qmc*
2. Select **External product sign-on** on the QMC start page or from the **Start**▼ drop-down menu .
3. Enter a name.
4. For **Product** select Qlik Alerting.
5. Enter the path to the Qlik Alerting login URI: *https://<alerting\_server>:4552/api/users/authQXSession*
6. Enter the path to the Qlik Alerting start page: *https://<alerting\_server>:4552/#/loginQXSession*
7. Enter a **Menu label**.

Qlik Sense hub users with permission see  in their profile menu to access Qlik Alerting. The **Menu label** text is the label for that icon.

8. Click **Apply**, and then click **Save**.


When you have configured external product sign-on, you upload an SSO script to the content library.

1. Select **Content libraries** on the QMC start page or from the **Start**▼ drop-down menu .
2. Select the Default record and click **Edit**.
3. Under **Associated items**, click **Contents**.
4. Click **Upload**.
5. In the **Upload static content** dialog, click **Choose Files**, navigate to *%Program Files%\Qlik Alerting\setup* on the Qlik Alerting server and select the *qaw\_sso.html* file.
6. Click **Upload**. When the file is uploaded to the content library, you can see it under **Contents**.
7. Copy the **URL path** for the uploaded file. For example, */content/Default/qaw\_sso.html*.
8. Build the authentication URL from the copied URL path as *https://<qliksense\_server>/<your\_URL\_path>*. For example, *https://<qliksense\_server>/content/Default/qaw\_sso.html*.



9. Save the authentication URL somewhere. You will need it in the next step when you configure Qlik Alerting.

### Configuring access for users

Configure external product sign-on access for users who should have access to Qlik Alerting. Users with access will have a menu item with a bell icon  in the Qlik Sense hub that takes them to Qlik Alerting sign-on.



In addition to the access, users must also:


- Have Analyzer or Professional entitlement in Qlik Sense.
- Be included in the list of users in Qlik Alerting who are synced across from Qlik Sense. This list of users is defined by You configure **Filter for user fetch** in the **Sources** settings.

Users with **HubAdmin** role in Qlik Sense have external product sign-on access by default. For other users, you need to create a security rule in the Qlik Management Console to provide access.

The following example, shows how to create a security rule that gives access to all users in a specific user directory.

### Example: Creating a security rule for external product sign-on

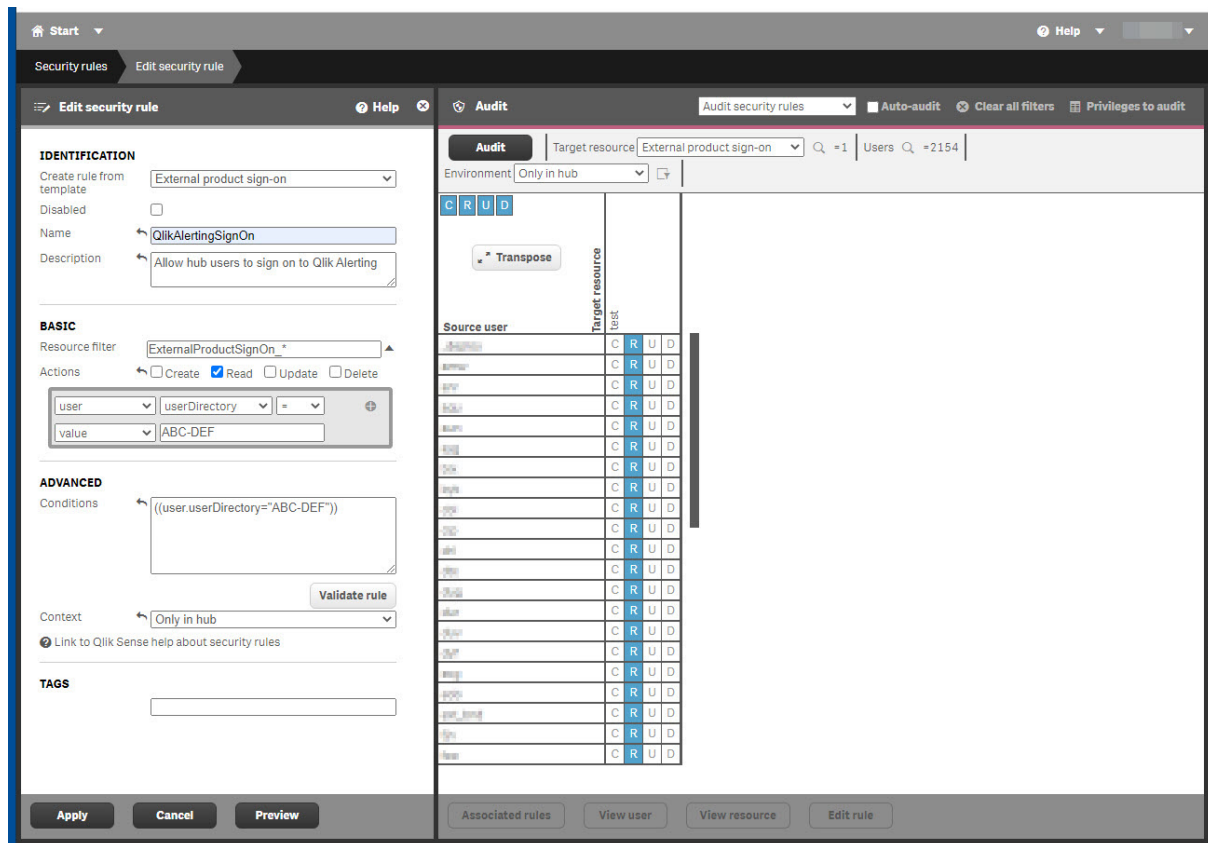
1. Open the QMC: `https://<QPS server name>/qmc`
2. Select **Security rules** on the QMC start page or from the **Start**  drop-down menu.
3. Click  **Create new** in the action bar.
4. From the **Create rule from template** list, select **External product sign-on**.
5. Enter a name, for example, *QlikAlertingSignOn*.
6. Leave **Resources filter** as *ExternalProductSignOn\_\**.
7. For **Actions**, select **Read**. Select the user condition properties **user**, **userDirectory**, **=**, and **value**. For value, enter the name of the user directory, in this example *ABC-DEF*.

The **Conditions** field under **Advanced** will show `((user.userDirectory="ABC-DEF"))`. You need to have the same condition here as in **Filter for user fetch** in Qlik Alerting. Having the same condition ensures that the users synced in Qlik Alerting are the same users that have been allowed access to Qlik Alerting from the Qlik Sense hub. Otherwise, a user might see the Qlik Alerting icon  in the hub without being able to access Qlik Alerting.

8. For **Context**, select **Only in hub**.
9. Click **Preview** to view the access rights that your rule will create and the users that they apply to.
10. Click **Apply** to create and save the rule.

**Successfully added** is displayed at the bottom of the page.

### Configuration of security rule that gives hub users SSO access to Qlik Alerting



Next, configure SSO authentication in Qlik Alerting.

#### Configuring SSO authentication in Qlik Alerting

When you have configured SSO authentication in the Qlik Management Console, you need to set it up in Qlik Alerting.

Do the following:

1. Open Qlik Alerting: [https://<alerting\\_server>:4552/](https://<alerting_server>:4552/)
2. Log in using administrator credentials.
3. Go to **Admin > Sources**.
4. On the Qlik source, click **•••**, and then select **Edit**.
5. For **Filter for user fetch**, enter `userDirectory eq 'ABC-DEF'`.

This is the same condition as in the security rule in the Qlik Management Console.

6. Under **Authentication**, select **SSO**.
7. The **Authentication URL** field is now enabled for editing. Enter your authentication URL that you saved from the configuration in the QMC content library. For example, [https://<qliksense\\_server>/content/Default/qaw\\_sso.html](https://<qliksense_server>/content/Default/qaw_sso.html).


8. Click **Test connection**. A dialog opens with details on the configuration.
9. Verify the entered details, and then click **Save**.

### Logging in to Qlik Alerting

Once you have enabled single-sign on, you have multiple ways to log in to Qlik Alerting.

#### Logging in to Qlik Alerting from the Qlik Sense hub

Do the following:

1. Go to `https://<qliksense_server>/hub/` and click your user profile icon.
2. Click the  icon.

You are redirected to the Qlik Alerting start page.

#### Logging in to Qlik Alerting from the Qlik Sense extension

When you have created an alert in the Qlik Sense extension, you can navigate to Qlik Alerting without entering credentials.

Do the following:

- In the **Create alert** dialog, click **Detailed view**.

You are redirected to the Qlik Alerting start page.

#### Logging in to Qlik Alerting from an email alert

If you have received an email alert from Qlik Alerting, you can log in from a link in the email.

Do the following:

- Click the link in the email.

You are redirected to the default browser. If you have an active Qlik Sense or Qlik Alerting session, you are taken directly to the Qlik Alerting start page. Otherwise, you're asked to enter your Qlik Sense credentials. After successful login, you are redirected to Qlik Alerting.

#### Logging in to Qlik Alerting by entering the URL in a browser

Do the following:

- Enter the Qlik Alerting URL in a browser: `https://<alerting_server>:4552/`

If you have an active Qlik Sense or Qlik Alerting session, you are taken directly to the Qlik Alerting start page. Otherwise, you are asked to enter your Qlik Sense credentials. After successful login you are redirected to Qlik Alerting.

## 3.5 Upgrade an existing version


---

### Supported versions for upgrades

Minimum version for direct upgrade is Qlik Alerting October 2021.

### Upgrade steps

#### Do the following:

1. Backup the MongoDB database named qlikalerting. For details, see [Backup and restore the MongoDB database \(page 16\)](#).
2. Backup any SSL certificates. If you have added these they will be found in the `C:\Program Files\Qlik Alerting/config/certificates` folder.
3. Download the Qlik Alerting installer from  [Product Downloads](#).  
See: [Downloading installation files \(page 25\)](#)

4. Right-click on the download and select **Run as administrator**.
5. Follow the steps to accept license agreement and install.

The install process will recognize the existing qlikalerting database and perform any database migration tasks required.

6. Once complete, check that all Qlik Alerting services are running, there are 10 services in this version.
7. In your browser, navigate to `https://localhost:4552` to check that everything is working.
  - If you need to replace the SSL certificates, follow the instructions in [Using trusted SSL certificates with Qlik Alerting \(page 13\)](#).
  - If you need to reset the ports to nonstandard (i.e. not 4551/4552) ports, then follow the instructions in [Changing the ports for Qlik Alerting web access \(page 16\)](#).

### Additional information for upgrades from versions up to and including November 2020

Releases from February 2021 have removed the requirement for the Redis database as MongoDB is now used for the activities that were previously managed in Redis. If you upgrade with the default settings the upgraded version of Qlik Alerting will automatically use MongoDB and Redis can be removed.

#### **Remove Redis from the Qlik Alerting server (based on the default install configuration from versions to November 2020)**

Do the following:

1. Remove the Windows service for Redis.
  - a. Open a new command window with run as administrator privileges on the Qlik Alerting server, and run the following commands.
  - b. Stop the Redis service:  
`net stop redis`
  - c. Delete the Redis service.  
`sc delete redis`
2. You can now delete the `c:\redis` folder.

### Troubleshooting

#### **The upgrade installs fully but not all of the services are visible in the Windows Services.**

We have identified some unusual instances where the ports are not released which blocks the setup of the new service. We have included a quick utility to support the clearing of the ports. Do the following:

1. Navigate to the **C:\Program Files\Qlik Alerting\setup\port-clearing** folder.
2. Right click on the **portclearall.bat** file and select run as administrator. If you have changed any of the standard ports you should make the changes to this .bat file directly.  
The cmd window will return information for each port, when the port was locked it will show a success message, when the port is clear already it will return a clear line.
3. Repeat step 2 until all ports show with blank line results.
4. Re-run the installer which will now reinstall the services correctly.

## 3.6 Database migration across servers

---

Follow the steps below to migrate your database to a new server.

1. Copy the Qlik Alerting database from the current server.
2. Perform a database dump operation to transfer the copied database content to the new server.



*Keep the same database version.*

3. Install Qlik Alerting on the new server. Copy the Qlik Alerting configuration from the previous server.

Once completed, you'll be able to use Alerting on the new server in the same way as on the previous one.

# 4 Managing alerts

There are three main types of alerts in Qlik Alerting; data alerts, system alerts and broadcast notifications. All users with access to the Qlik Alerting web portal will have access to data alerts but only Admin users will have access to system alerts and broadcast notifications.

## 4.1 Data alerts

---

Set alerts on the data in your Qlik Sense applications with simple or complex conditions that ensure you can create alerts to be notified exactly when you need to be. This includes a complex rules engine which allows multiple conditions, comparing with the history of previous scans and/or comparing with the data in the application, with the power to set conditions in steps to enable filtering by measures and other features that cannot be done directly in Qlik Sense.

## 4.2 System alerts

---

Set notifications to let users know when applications have reloaded, failed or are simply taking more time than expected. This is a powerful tool to enable owners of applications to ensure things are up-to-date. Be notified of problems as they happen rather than get surprised when users let them know that their applications are not updated.

## 4.3 Broadcast notifications

---

Keep your users up-to-date with the latest news with formatted notifications which can be sent directly and/or repeated on a schedule. Use them to notify of system downtime, new applications, user group reminders and any other business that people need to know about. All the notifications you have sent can be re-activated and edited to send again making it simple to re-purpose your old notifications.

## 4.4 Broadcast notifications

---

Broadcast notifications allow an Admin to send a formatted HTML message to user groups and/or users in Qlik Alerting. These messages can be sent directly once completed or set to send on a schedule. For example an Admin could wish to send out a reminder message for downtime on key systems using Qlik Alerting broadcast notifications, these messages could be sent every morning at 9 am for the week before the downtime to ensure that everyone is aware of what is happening.

### How to create a broadcast notification

#### Create a broadcast notification

##### Do the following:

1. Click **Alerts** from the top menu bar.
2. Click **Broadcast Notifications** at the top of the table to switch to the broadcast notifications view and see a list of all the broadcast notification records you own.
3. Click **Create** at the bottom of the table to create a new notification.

#### Notification section

##### Do the following:

1. Enter an **Alert Name** and **Alert Description**.
2. Enter a **subject/notification** line for the broadcast notification.
3. Enter the body of the message in the window. This window is expecting HTML but you can write plain text if your message is short and does not need formatting.
4. Click on the preview button to see the rendered HTML.

#### Schedule section

In this section the triggering of the alert scan is setup; this can be:

- Select the type of **Trigger** you would like to set; on reload or on schedule.

#### Trigger Now (default)

This will trigger the alert once as it is saved. The alert can be triggered again manually by highlighting the notification in the **My Alerts** table and clicking on the trigger button.

#### On Schedule

When you select on schedule you will see the server time is presented. All times you enter into this schedule area will be set based on this server time which may be different to your local time.

##### Do the following:

1. Enter a **Scan Since** date and time. This may be left blank if you wish the alert to start immediately.
2. Enter a **Scan Until** date and time. This may be left blank if you do not wish to set an end date at this time.
3. You can select one of **Days of Week** or **Days of Month**. This allows you to select on which days of the week or which days of the month the alert scan will trigger. For example you could set it to be only for working days of the week. Leaving these selections blank will automatically select all days of the week and all days of the month.
4. For **Schedule Alert By**, select **Interval** or **Times**.
  - **Interval:**
    - a. Set the start time and end time for the alert scan to trigger for a day on which it is scheduled. This allows you to manage your alerts so you do not get notified of changes outside of working hours.

- b. Set the interval in hours and minutes. The alert scan will trigger at the start time and then each interval from this time.
- **Times:**
    - a. Enter the time on which you would like the alert scan to trigger.
    - b. Click **Add Scan Time** to add the time record.



*You may enter more than one time on which it should trigger during the day.*

## 4.5 Data alerts

---

Data alerts allow a Qlik Alerting user to create a variety of alerts which will check their data in a Qlik Sense application. This check is performed as a user session which impersonates the user ensuring all application and data access security is respected. Alerts can be created on a schedule or when an application reload completes through a reload task in Qlik.

### Creating an alert

#### Do the following:

1. Click **My Alerts** from the top menu bar to see a list of all the alert records you own.
2. Click **Create** at the bottom of the table to create a new alert.

### Building a data table

In this section you will be building the table of data from which you wish to create your alert.

#### General

#### Do the following:

1. Enter an Alert Name.
2. Enter an Alert Description (optional).
3. Select the Qlik Sense Application.

#### Add measures

Select the different measures that you want to use in creating your alert. This may be one or multiple measures depending on the conditions that are required, for example the condition may be based off a different measure(s) than the one presented in the notifications. The standard notification templates will present the first 4 columns in your data table. You can add more but these will not show in the standard templates.

#### Do the following:

1. Select a measure. This will either be a measure from the list of master items or you can select a custom measure and you should complete the expression and label for this measure.
2. Select the **Format** for this measure when presented in the notification.
3. Click **Add Measure** and the measure will be shown in a table just below and in the preview.



4. Repeat this process to add additional measures.



*Measures can be removed by clicking the delete icon next to the measure in the list.*

### **Drill to Dimension (optional)**

The drill to dimension option allows the selection of a dimension to allow checking conditions across a table of data. Each row in the table will be evaluated to see if it meets the conditions or not.

#### **Do the following:**

- Select a dimension or field from the list that is displayed in the **Dimension** dropdown. You can search by typing into the entry box.

### **Filters**

Bookmarks OR filters on fields are supported, but the use of both at the same time is not supported.

#### **Do the following:**

1. From the filters dropdown you can select an existing bookmark or a custom filter.
2. If you have selected a custom filter do the following:
  - a. Select the filter field.
  - b. Select the **Values** in that filter field. Search for the values to simplify creating the value list by typing into the space.
  - c. Click **Add Filter**.
  - d. Repeat this process to add more field and filter values.

### **Preview Table Sort**

You can manage the sort order of the data table in the user interface, which also sets the sort order for the notification tables.

- Sort By - choose the column you wish to sort by.
- Sort Ascending - choose whether the sort order is ascending or descending.

## Condition section

The conditions section allows you to create up to 10 conditions from the measures and dimensions you have selected in the data table section. There are simple and complex condition types available with standard numeric and text string condition options. You can set multiple conditions and use the **Rules** area to organize those conditions to get the exact result you require with AND / OR and step options.

### **Condition types**

There are a number of condition types which you can choose from which range from simple to those which offer some complexity. The main condition types are:

- Manual Value - Compare the row value for the measure or dimension selected to a fixed value that you enter against the condition. This can be numeric (for measures) or text-based (for dimensions).

- Measure - Compare the row value for the measure or dimension selected to a second column from the data table you have created.
- Previous Scans - Compare the row value for the measure or dimension selected to a previous scanned value (for measures and dimensions) or to an aggregation of previous scanned values (for measures only) such as the average of the last 10 scanned values.
- Set - Compare the row value for the measure selected to the rest of the values in the column with some simple (average, min, max) and advanced (percentile, standard deviation) aggregation options.

### Setting a condition

#### Do the following:

1. Select a **Column** from the data table you have created. This can be a measure or the dimension column.
2. Select the **Operator** you want to use to compare the selected column value.

#### Numeric Operators

- Greater Than (>)
- Greater Than Or Equal To (>=)
- Less Than (<)
- Less Than Or Equal To (<=)
- Equal To (=)

#### Text String Operators

- Includes
  - Starts With
  - Ends With
3. Select the **Type** of the condition, once selected additional fields will show.

#### Numeric Operators

- Manual Value
  - Value - enter the fixed value that you will compare your selected column value against.
- Measure
  - Compare with - Select another column from your data table.
  - Offset - Enter a value that you wish to offset the returned value by. This can be both a number or a percentage but both should be entered in numbers (i.e. 50% = 50)
  - Is percent - Select this check box if the number you have entered is a percentage.
- Previous Scans (the history that has been stored from the previous scans for this alert held in the Qlik Alerting repository)
  - Scans - Select the number of previous scans. If you select 1 you will be checked versus the last time Qlik Alerting checked this alert. If you select a number

greater than 1 you will need to set an aggregation type.

- Aggregation
  - Average - for example, compare the current value with the average of the last 10 scanned values.
    - Offset
    - Is percent
  - Min - for example, compare the current value with the minimum of the last 10 scanned values.
    - Offset
    - Is percent
  - Max - for example, compare the current value with the maximum of the last 10 scanned values.
- Set (the returned dataset in the data table)

### Aggregation

- Average - the average of the values in the set of the selected column
  - Offset
  - Is percent
- Min - the minimum of the values in the set of the selected column
  - Offset
  - Is percent
- Max - the maximum of the values in the set of the selected column
  - Offset
  - Is percent
- Quartile
  - Quartile - Enter a value between 1 and 4 which indicates the upper boundary of the quartile. I.e. 1 is the 25th percentile value, 2 the 50th percentile value, 3 the 75th percentile value and 4 the 100th percentile value.
- Percentile
  - Percentile - Enter the value of the percentile, i.e. 90 is the 90th percentile value so your condition might be <measure> is greater than the 90th percentile value of the measure set
- Standard Deviation
  - Standard Deviation - Enter the number of standard deviations, i.e. -2 for a condition which looks for less than the lower bound of the 2nd standard deviations from the mean of the set, 1.5 for a condition which looks for all values above the upper bound of 1.5 standard deviations from the mean of the set in the selected column.

### Text String Operators

- Manual Value
  - Value - enter the fixed value that you will compare your selected column value against.
- Previous Scans
  - Scans - Will default to 1 as you can only compare with the last scanned value for text string operations

4. You can add further conditions by clicking **Add Condition**.

### Setting the rules

The rules entry option allows you to apply the conditions you have created in a way that is as flexible as possible. Each condition you have created will have an identifier (A, B, C, ..). You can also add layers to your rules (rule steps) which allow you to create very complex rule conditions where, for example, you can use the first step to filter values by a measure and the second steps to look for the outlier values (i.e. standard deviation).



*By default the **Rules** section will only show the first condition (A) and you will need to enter in the additional rule references (B, C, ..) and syntax.*

### Rules syntax

The following operators are permitted.



*Use lower case for the **and** and **or** operators when you write a rule. For example, (A and B) or C.*

- **and** - use *and* to create a rule where both conditions should be true for the record to be present, for example, *A and B*.
- **or** - use *or* to create a rule where either of the conditions can be true for the record to be present, for example, *A or B*.
- **()** - Use parenthesis to group certain rules so that you can combine *and* and *or* in the same rule, for example, *(A and B) or C*.
- **!** - Use an exclamation mark to add a NOT function to the rule, for example, *(A or B) and !C*. An example where this would be used is where you have a condition that is set to equal the previous scanned value, but you want to set it to not equal, you could use the **!** option to ensure the rule return catered for this.

There is a validation check for the rules which presents as a tick (when the rule syntax is valid) or as an exclamation mark (when the rule syntax is invalid).

### Rule steps

To allow for a much greater range of capability in condition setting there is a capability to set rules in groupings (sets) which will apply in order. This can be used to allow filtering by measure values before looking for outlier values which is something we cannot do in a single step, and that is not possible in Qlik Sense without writing complex (and inefficient) expressions.

To demonstrate how this works we can use a simple example. As a regional sales manager I want to know my worst performing 10% of stores in terms of gross margin %, however I only want to see the results from those stores that have sales over a certain level, say \$50,000. In this example:

- Use rule step 1 to apply a Manual Value condition where the sales value is greater than 50000.
- Use rule step 2 to apply a Set condition with a Percentile aggregation where the value is less than or equal to the 10th percentile value of the dataset that is output from step 1 (i.e. filtered to remove those with sales values less than 50000).

Click **Add Rule Step** to add new steps.

### Calculate conditions

Click the **Validate Conditions** button in the preview area to review the output of the conditions and rules you have created. This will present a table and a summary of the number of records returned as true in the current set of data.



*If you are using a previous condition, there will be no history available when you create the alert. It will automatically allow this condition type to be true. This allows you to test any other conditions you have. On save, the first history values will be captured and from then on the previous history will be respected as a condition.*

### Schedule section

In this section the triggering of the alert scan is setup; this can be

- Select the type of trigger you would like to set; **On Reload** or **On Schedule**.

#### On Reload (default)

An on reload trigger will trigger the scan process after each successful reload of the Qlik Sense application. A reload is typically when the data changes in a Qlik Sense application (excluding direct connect setups) so is the primary means of triggers for Qlik Sense applications. A scheduled reload allows you to set time-based reload options.

#### On Schedule

When you select on schedule you will see the server time is presented. All times you enter into this schedule area will be set based on this server time which may be different to your local time.

#### Do the following:

1. Enter a **Scan Since** date and time.  
This may be left blank if you wish the alert to start immediately.
2. Enter a **Scan Until** date and time.  
This may be left blank if you do not wish to set an end date at this time.
3. You can select one of **Days of Week** or **Days of Month**. This allows you to select on which days of the week or which days of the month the alert scan will trigger. For example you could set it to be only for working days of the week. Leaving these selections blank will automatically select all days of the week and all days of the month.

4. For **Schedule Alert By**, select **Interval** or **Times**.

**Interval:**

- a. Set the start time and end time for the alert scan to trigger for a day on which it is scheduled. This allows you to manage your alerts so you do not get notified of changes in out of work hours.
- b. Set the interval in hours and minutes. The alert scan will trigger at the start time and then each interval from this time.

**Times:**

- a. Enter the time on which you would like the alert scan to trigger.
- b. Click **Add Scan Time** to add the time record.



*You may enter more than one time on which it should trigger during the day.*

## Distribution section

### Channels

Select the delivery channel(s) you wish to receive the alert notifications through, you may choose one or more channels from the following:

- Email
- Mobile (sending to all a users registered mobile devices - up to 5)

### Notification frequency

This functionality allows you to ensure you are not sent notifications over and over again simply because the application has been reloaded in Qlik Sense for other purposes. These settings allow you to choose a frequency of being notified that will control how many times in a period you are notified. Options are:

- Every time [default]
- Only the first each Hour
- Only the first each Day
- Only the first each Week
- Only the first each Month
- Only Once (and never again)

### Advanced

The advanced option is governed by the distribution setting privilege which is assigned by the administrator. This allows a user to distribute the alert to others in the Qlik Alerting user list.

### Do the following:

1. Use the advanced switch to show the advanced distribution settings.
2. Select the type of distribution you would like.
  - Broadcast - takes the result of the data query using your Qlik data access and shares this result with all users.
  - Managed Shared - takes each recipient in turn and queries Qlik with their user (assuming section access and app security is in place) and sends each user the result of the queries based on their data access.
3. Select the recipients or groups using the assigner windows.
4. Preview the users who are currently assigned for the alert



*The preview also allows you to see which users have unsubscribed from the alert.*

## Notification section

### Link back to the Qlik Sense app

Select the relevant Sheet in the selected application. This is used in generating the URL with filters that will be sent in the alert notifications. The first sheet will be selected by default so you do not need to make any changes if you do not need to.

### Customize notification

You can choose to customize the notification text. This includes the email subject and mobile push notification message and the body of the email which can be adapted. You will need knowledge of HTML and CSS to manipulate the body template.

Review the detailed instructions in [Managing custom notifications \(page 50\)](#).

You can skip this section if you do not want to change the default notification (recommended). The default templates present tables up to the first 4 columns for alerts with a dimension and multiple measures.

### Do the following:

1. To modify the notification setting, click on the **Customize Notification switch**.
2. On the **Notification Subject** line you can enter text or construct a free text plus variable string.
3. You can import a template into the email message body area using the options above the text area and the templates you can download (see [Managing custom notifications \(page 50\)](#)). It is important to note that HTML can behave differently in different email clients so we have created our templates to be as consistent as possible. This does mean they are more complicated so you will need reasonable knowledge of HTML and CSS to manage this.
4. Click **Preview** to check that your HTML is formatting correctly.

## Data alert types

### Distribution settings - Broadcast alerts

A broadcast alert allows a user to send triggered notifications from their alerts to one or multiple users or user groups.

### How it works

A recipient of a broadcast alert will receive a notification when the conditions for that alert are met. Qlik Alerting will query the data based on the credentials of the owner of the alert and share that result with the many recipients. This makes it distinct to a managed shared alert which queries Qlik Sense for each recipient.

### Who can create a broadcast alert

Broadcast alerts are managed as part of the distribution user privilege. Users will need to have this privilege assigned to them to be able to create broadcast and managed shared alerts.

### Who can receive a broadcast alert

Anyone can receive a broadcast alert. Recipients do not need to have a license in Qlik Sense.

### Recipients can unsubscribe from a broadcast alert

Anyone can receive a broadcast alert, even those without a license. Recipients of a broadcast alert will be able to unsubscribe from the alert using the link on the email (a link for the mobile application will be added in the near future). The owner of the alert will be able to see which users have unsubscribed or are not receiving the alert due to licensing restrictions in Qlik Alerting. An unsubscribed user can be resubscribed by the owner of the alert through a link in the **Edit Alert** view.

### Distribution settings - Managed shared alerts

Managed shared alerts allow for a user, who is assigned the distribution user privilege, to share an alert with one or multiple other users. This type of sharing of an alert ensures that ownership of the alert remains with the creator so any changes will be reflected in the triggered notifications that a user receives.

### How it works

A recipient of a managed shared alert will receive a notification when the conditions for that alert are met. Qlik Alerting will query Qlik Sense for each and every recipient assigned to the managed shared alert respecting all security for that user through security rules and section access. This makes it distinct to a broadcast alert which sends a single Qlik Sense query response (based on the alert owner's credentials) to all recipients.

### Who can create a managed shared alert

Managed shared alerts are managed as part of the distribution user privilege. Users will need to have this privilege assigned to them to be able to create managed shared alerts.

### Who can receive a managed shared alert

To receive a managed shared alert created by another user, the recipient must be a licensed Qlik Sense user or have access to the specific app through analyzer capacity or user access rules. This lets Qlik Alerting query Qlik Sense on behalf of the recipient user with their credentials and security settings.

### Recipients can unsubscribe from a managed shared alert

Recipients of a managed shared alert will be able to unsubscribe from the alert using the link on the email (a link for the mobile application will be added in the near future). The owner of the alert will



be able to see which users have unsubscribed or are not receiving the alert due to licensing restrictions on either Qlik Sense or Qlik Alerting. An unsubscribed user can be resubscribed by the owner of the alert through a link in the **Edit Alert** view.

### Drill into dimension alerts

A drill into dimension alert allows a user to check the measure against the selected condition(s) across an array of data through one alert. The output of this alert will be the subset of the dimension values that meet the condition as a list with the measure value. This allows you to know directly where the problem with this measure might be, which store, product line, etc. Drill into dimension alerts can also be sent as managed shared alerts or broadcast alerts to other users if required.

For example, if you select 'country' as the drill to dimension in a sales margin % alert the measure will be returned as an array with country as the dimension and the sales margin % for each country.

### Who can create a drill into dimension alert

All users of Qlik Alerting can create a drill into dimension alert through the Qlik Alerting web portal or the Qlik Alerting extension. There is no specific user privilege to restrict functionality to this type of alert as it is considered a critical part of getting quicker insight into your data.

### Email notifications for data alerts

Email notifications are sent when a data alert is created or triggered. If the data in the alert exceeds the maximum number of rows, which is set to 100 rows by default, an attachment named *Data.csv* will be included in the email. The file attachment is sent to all recipients who have been added to the data alert.

The attached file contains the data values from the selection in the alert. The content of the email body remains the same regardless of whether an attachment is included or not.

### Adjusting the maximum number of rows

If necessary, you can customize the maximum number of rows allowed in the data alert. The default value is 100.

Do the following:

1. Locate the file *C:\Program Files\Qlik Alerting\email-messenger\config\default.json*.
2. Open the file and locate the `maxRows` parameter. Here is an example snippet of the configuration file:

```
email-messenger": {
  "ip": "localhost",
  "port": 9021,
  "https": false,
  "uses": {
    "run": {
      "interval": 200,
      "defaultStart": true,
      "maxConcurrent": 5,
      "maxDaily": 1000000
    },
    "maxRows": 100,
    "tlsMinVersion": 1.2
  }
}
```

```
    }
  }
```

3. Change the value of `maxRows` to your desired number of rows.
4. Save and close the file.
5. To apply the new configuration, restart the email-messenger service.

### Managing custom notifications

To customize the email body you will need to be able to understand and manipulate the HTML. You can import one of the templates as a starting point and these will help you understand the approach to the layout of the template. There is a reason for the structure we have used as each email client renders HTML differently so nesting the tables is the best approach to ensure it is consistent in each client. Of course, you are welcome to use whatever structure you require but we would suggest you test on multiple email clients to ensure it is consistent.

#### Custom notification / subject line

The custom notification/subject is the push notification message for the mobile and the subject line in an email. This enables you to target the message with enough information to act without having to open the body of the record. To give you an idea of how to use this field we have provided the following examples.

In the table below we provide some examples of how you can construct your notification message with simple text and/or using the dynamic variables:

Dynamic variable example uses

Example	Notification/Subject code example
Plain text	ALERT : You're about to run out of stock
Using the alert name	ALERT : {{alertName}}
Single alert example	ALERT : {{measures.0}} is {{conditions}} !
Drill to dimension alert example	ALERT : {{nRows}} {{dimensions.0}} with {{measures.0}} {{conditions}} !

See the [Dynamic text variables \(page 51\)](#) section below for a full list of those that can be used in the notification messages and the email message body.

#### Email body requirements and examples

There is one key requirement when you are using a custom email body message. You must include the full HTML code syntax structure as outlined below for the email to construct correctly. Use the preview button to review your code to see the structure you have created.

```
<!DOCTYPE HTML >
<html lang="en">
<head> .... </head>
<body> .... </body>
</html>
```

### Importing example templates


If you have the option of importing an HTML template file into the custom editor so you have a starting example to adapt. You can use one of the following template files, which are copies of the standard templates that are included in the Qlik Alerting installation, to load into this editor.

- Download the [Standard single measure notification template](#).
- Download the [Drill to dimension notification template](#).

### Dynamic text variables

The following are a list of text variables that can be called in the notification/subject and/or body of your customized notification. There are also more complex looping elements you can use which are covered in the next section.

Dynamic text variables

Variable label	Variable code	Description
Recipient Name	{{firstName}}	Provides the name of the user to whom the triggered notification will be sent. This can be the owner of the alert, the broadcast alert recipient or the managed shared alert recipient.
Alert ID	{{alertId}}	Provides the Alert ID (GUID) which is used in the unsubscribe URL link. This is not normally presented but may be useful for debugging purposes.
Alert Name	{{alertName}}	Provides the name of the alert record.
Alert Triggered Timestamp	{{timestamp}}	Provides the timestamp when the alert was triggered in Qlik Alerting.
Alert Measure	{{measures.0}}	Provides the measure name that is scanned for the alert. This can be either the master item label or the entered label for advanced Qlik expressions.
Alert Measure Current Value	{{values}}	Provides the current value of the measure at the time of the scan.  <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <i>This variable does not exist for drill to dimension alerts.</i> </div>
Alert Condition	{{conditions}}	Provides the conditions that the scan will check against to trigger the email. This is shown as a string.
Unsubscribe from Alert URL	{{unsubscribe}}	Provides the URL which can be clicked on to unsubscribe to the alert. Allowing users to opt out of an alert if they do not feel it adds value for them.
Qlik Alerting login URL	{{qlikAlertingLink}}	Provides the URL which can be used as a link to go straight to the Qlik Alerting login screen on the web portal.

Variable label	Variable code	Description
Qlik Sense Application Name	{{appName}}	Provides the name of the Qlik Sense application which the alert will scan.
Qlik Sense Application ID	{{appId}}	Provides the ID of the Qlik Sense application which the alert will scan.
Qlik Sense Application URL Link (with filters)	{{appLink}}	Provides a URL link to the Qlik Sense application which includes the filters and sheet reference as setup in the alert (or derived by the Qlik Alerting extension for Qlik Sense).
Qlik Sense Server	{{qlikLink}}	Provides the URL which can be used as a link to go straight to the Qlik Alerting login screen on the web portal.

### Looping elements

There are two types of loops that are used in our default templates. These are used for filters, and the arrays of values associated with them, and for the drill to dimension results.

#### Example: Filter table

This loop example shows all fields that have filters assigned to them (the `#query.filters` loop) and the values assigned to them (the `#values` loop):

```
<table style="color:#494848; font-size:13px; line-height:1.8; table-layout:auto; width:100%;">
  <tr style="background-color: #fff">
    <td style="width:40%"><strong>Field</strong></td>
    <td><strong>Selections</strong></td>
  </tr>
  {{#query.filters}}
    <tr style="border-bottom:1px solid #dfdfdf;">
      <td>{{field}}</td>
      <td>
        <table style="padding:0px; font-size:13px; width:100%">
          {{#values}}
            <tr>
              <td>{{.}}</td>
            </tr>
          {{/values}}
        </table>
      </td>
    </tr>
  {{/query.filters}}
</table>
```

#### Example: Drill to dimension results

There is one loop in this example as it is returned as one array of data, the `#dimensionvalues` loop:

```
<table style="color:#494848; font-size:13px; line-height:1.8; table-layout:auto; width:100%;">
  <tr style="background-color: #fff">
    <td><strong>{{dimensions.0}}</strong></td>
    <td><strong>{{measures.0}}</strong></td>
  </tr>
</table>
```

```
</tr>
  {{#dimensionValues}}
    <tr>
      <td>{{qText}}</td>
      <td>{{qNum}}</td>
    </tr>
  {{/dimensionValues}}
</table>
```

### Embedding web images into emails

A common request, particularly if you are sending alert emails to external organizations, is to be able to embed a logo or other images into the body of the alert. The answer is of course “Yes, you can!”

To add this functionality you can change the HTML and add an `<img>` tag as per the example below.

```
<table width="100%">
  <tr>
    <td align="center" style="padding:10px 25px;">
      <div style="text-align:right">
        
      </div>
    </td>
  </tr>
</table>
```

### Right to left language support

The email templates can be adapted to provide right-to-left language support for Arabic, Aramaic, Azeri, Dhivehi/Maldivian, Hebrew, Kurdish (Sorani), Persian/Farsi and Urdu. In order to enable this you must change the `<style>` code at the start of the template. There are two places that you will need to adjust to ensure the template works in right to left format. You will of course need to change the text, the labels and be using an application that is built using the language of your choice.

### Example: Default left-to-right CSS

```
<style type="text/css">
  div {
    direction: ltr;
    text-align: left;
    vertical-align: top;
    font-family: Tahoma, Ubuntu, Helvetica, Arial, sans-serif;
  }

  table, th, td {
    direction: ltr;
    text-align: left;
    border-collapse: collapse;
    mso-table-lspace: 0pt;
    mso-table-rspace: 0pt;
    word-break:break-word;
    vertical-align:top;
  }
</style>
```

### Example: Changes for right-to-left CSS

```
<style type="text/css">
  div {
    direction: rtl;
    text-align: right;
    vertical-align: top;
    font-family: Tahoma, Ubuntu, Helvetica, Arial, sans-serif;
  }

  table, th, td {
    direction: rtl;
    text-align: right;
    border-collapse: collapse;
    mso-table-lspace: 0pt;
    mso-table-rspace: 0pt;
    word-break: break-word;
    vertical-align: top;
  }
</style>
```

### Updating default email templates

The default email templates are shipped with the Qlik Alerting installer. However, it is possible for an organization to edit these base templates so that the default emails (and those templates that are imported into the custom editor) are customized for your organization.

Important:

- You will need to have remote desktop access to the Qlik Alerting server, or to the *C:/Program Files* drive folder on this server.
- You must have edit rights to the files in this location.
- These changes will need to be migrated when you upgrade Qlik Alerting. You will need to make copies of them and then replace the new templates that will be copied as part of the upgrade. Ensure that you check if any variables have been updated as you may need to make some changes to your templates over time.

### Do the following:

1. Navigate to the *C:/Program Files/Qlik Alerting/email-messenger/templates* folder (default install path).
2. Make a backup copy of the file you wish to edit.
3. Edit the .hjs files in any text editor, change the language type when viewing the file to HTML to make it simpler to read.
4. Save and test by creating and triggering an alert.

### Which files relate to which emails

Email types and templates		
Email type	Created email template	Triggered email template
Single measure data alert	dataCreate.hjs	data.hjs
Drill to dimension data alert	dimensionCreate.hjs	dimension.hjs
System alert	systemCreate.hjs	system.hjs

### Sharing an alert record

A user can share the alert they have created with another user. This creates a copy of their alert record which is then assigned to the recipient user whom, having accepted the alert, takes full control of the alert record.

#### Who can share an alert

Professional users who are assigned the 'Share alerts' user privilege will have access to the share alert functionality. Any Professional or Analyzer user will be able to receive a shared alert.

#### How to share alert records

##### Do the following:

1. Navigate to the **Alerts** view where your alerts are listed.
2. Select the alert or alerts that you wish to share using the check boxes on the left-hand side.
3. Click **Share**.
4. Select one or more users to share the alert with.
5. Click **Share**.

You will see a pop-up confirming that the alert has been shared.



*If the alert is disabled, it will copy as a disabled alert for the recipient when they accept it.*

#### How to receive shared alert records

You will receive an email which allows you to click on an accept or reject link directly.

You can also review the alerts shared with you in the web portal.

##### Do the following:

1. Click on the user icon.
2. Select **Suggestions**.  
You will see a list of suggestions which will include the shared alert records.
3. Click **Accept** to copy the alert to your 'Alerts' list or reject if you do not. If you reject, the record will be deleted.
4. You can now control the alert record, set the trigger and edit the details as you wish.



*Any distribution recipients will be removed during the share process to ensure other users do not receive the same alert from many different places. You will need to reset the recipients if you wish to distribute this alert.*

## 4.6 System alerts

System alerts check the status of reload tasks in Qlik Sense and provide early warning when things are not working as intended (failed reloads) or confirmation that things are on track (successful reloads).

You can set your alert to work off specific reload tasks or all reload tasks. If you use the all option then they will automatically cover any new reload tasks added to the Qlik Management Console (QMC). So you never need to miss a failed reload.

### How to create a system alert

To create a system alert, do the following:

1. Click **Alerts** from the top menu bar.
2. Click **System Alerts** at the top of the table to switch to the system alerts view and see a list of all the system alert records you own.
3. Click **Create** at the bottom of the table to create a new alert.

#### System section

Do the following:

1. Enter the **Alert Name** and **Alert Description**.
2. Select the **Reload Tasks** that this alert will monitor. There are two options to enable you to select the reload tasks:
  - a. Choose **Select tasks manually** to pick from the list of reload tasks, you can use the search box to find the tasks you want to select.
  - b. Choose **Select tasks by rule** to identify tasks dynamically so that any new task that is created can also be evaluated against your rule.
    - a. Select the **Operator** for your rule
      - **All** - will notify when any task meets the event type condition.
      - **Includes** - A string search operator that allows you to pick any task with the string in the task name.
      - **Starts with** - A string search operator that picks any task where the task name starts with the entered string.
      - **Ends with** - A string search operator that picks any task where the task name ends with the entered string.



*The table shows the tasks that would meet the conditions as per the rule at that point in time. New Tasks will also be evaluated as they are created.*

3. Select one or more **Event Triggers** from the following:
  - **Finished Successfully** – status 7 – When a reload task completes as expected.
  - **Finished Failed** – status 8 – When a reload task has completed but the process has failed.



- **Aborted Manually** – status 6 – When the reload task has been aborted or is in the process of being aborted.
- **Aborted By System** – status 9, 10, 11, 12 – When the reload task has been stopped by the Qlik Sense system without input from any user or admin.
- **In Progress** – status 1, 2, 3, 4, 5 – Identify when a task takes longer than a specified time in seconds to get an early warning of a possible failure or delay to reports being ready.
  - For in progress an input field will show that requires an input for a number of seconds to set the threshold following which the alert will trigger for a task. This will default to 180 seconds (3 minutes) but can be changed as required.

### Qlik Sense reload task status codes and descriptions

Code	Description
null	Never started
1	Triggered
2	Started
3	Queued
4	Abort initiated
5	Aborting
6	Aborted
7	Success
8	Failed
9	Skipped
10	Retrying
11	Error
12	Reset

### Distribution section

Do the following:

1. Select the delivery **Channels** you would like to receive the alert on; options are email and mobile.
2. Select the **Frequency** which you would like notifications to be sent. This will limit how many times you are notified of a triggered alert during the time period. The options are:
  - Every time [default]
  - Only the first each Hour
  - Only the first each Day
  - Only the first each Week

- Only the first each Month
  - Only Once
3. Click on the switch if you wish to distribute the alert notifications with other users. For system alerts this will always be a broadcast alert type.



*This section will only show for users with the appropriate privileges to distribute alerts.*

- Select the recipients directly, and/or
  - Select the user groups.
  - Use the preview button to check on the list of users at that point in time (as users in groups may change over time).
4. Click **Save**.

## 5 Mobile apps

Qlik Alerting applications are available for both iOS and Android devices. Click on App Store or Google play and search for Qlik Alerting to download.



*You need Qlik Alerting July 2023 or later to use mobile apps over iOS or Android.*

When you first open the app you will be asked to allow access to enable notifications, please accept this.

### 5.1 Who can access the Qlik Alerting mobile apps

To sign on and receive notifications through the Mobile app you will need to have access to the Qlik Alerting web portal. Professional and analyzer users in Qlik Sense who are enabled in Qlik Alerting will have access to both the mobile app and the Qlik Alerting web portal.

### 5.2 Setting up the Qlik Alerting mobile app

Once you have downloaded the app, on either Android or iOS, you need to connect the app to the Qlik Alerting server which will typically be behind a firewall and not accessible to the public. You can test this by accessing the Qlik Alerting web portal through the browser on your device. If you can see the login page for Qlik Alerting you can continue. If you cannot try connecting to the network through a VPN or by connecting to the wireless network in your office which is part of the network.

#### **Do the following:**

1. Ensure that you can access the Qlik Alerting web server.
2. Open the app and be sure to allow access to enable notifications (on opening the first time only).
3. You have two options to authenticate your device:
  - Use the QR reader (where you have access to a computer where you can open the Qlik Alerting web portal at the same time).
    - a. Open the Qlik Alerting web portal and sign in.
    - b. Go to the avatar, click and select user devices.
    - c. You will see a set of 5 cards which represent the devices you can attach. Click on the '+' icon to add a device.
    - d. On the mobile app use the QR reader option on the logon screen to read the QR code and you will be logged on automatically.

- Manually enter credentials.
  - a. Open the mobile app and select the 'login with email and password' option.
  - b. Select the connection approach HTTP or HTTPS.
  - c. Enter the IP or DNS of the Qlik Alerting server (as you login with the Qlik Alerting web portal).
  - d. Enter the port number, defaults are 4551 (http) and 4552 (https) but these can be changed.
  - e. Enter your username or your email (as you would when logging on to the Qlik Alerting web portal).
  - f. Enter your password (as you would when logging on to the Qlik Alerting web portal).

When you log in to the Qlik Alerting server through the mobile device a token is passed across to Qlik Alerting so that it can identify the device when sending a notification.

### 5.3 Signing out from the Qlik Alerting mobile app

---

This is simpler when you can access the Qlik Alerting web server as you did when you logged on with the app initially. You may need to be connected to your work wireless network or have your work VPN enabled where this server is protected by your organization's firewall.

#### **Do the following:**

1. In the app select the menu icon in the top left corner.
2. Select the sign out option.

If the app could not contact the Qlik Alerting server when you sign out you will need to take the following steps.

1. Log on to the Qlik Alerting web portal.
2. Go to the avatar, click and select user devices.
3. Identify the device that you have signed out of.
4. Remove the device.

### 5.4 Navigating in the app

---

Here are some quick tips to get around the Qlik Alerting mobile apps.

#### Settings Options

##### **Refresh Alerts**

Click on this option to refresh the list of your alerts at any time. Perhaps you removed an alert card by mistake and wish to reinstate it or it can be a good check that you have the latest information to

work from. You will see a message saying the refresh may take some time as it sends a request back to the Qlik Alerting server that you are connected to. However, the wait time is typically only a few seconds.

### **Delete History**

Click on this option to clear all history from the device. This will remove all triggered and scan history from all of the alerts but will leave the alert card placeholders showing on your device. If you wish to clear off of this information you can uninstall and reinstall the app being careful to read the signing out section above.

### **Clean up after...**

Click on this option to select from a number of options that determine how long history records will remain stored on the device. The default is 14 days but you can select from 7, 14, 30 or 90 days.

## **On the main alerts screen**

### **Filters and search**

There are two options to find the alert to get to the detail stored in the app.

- Filters - Use the filter icon on the top-right of the window to choose from the different alert types; data, system or notifications. This can help you quickly scroll through the records of interest to you.
- Search - you can search across all the alert types to find the application, measure, alert name you need. This allows you to navigate with ease to the record you want to check.

### **Alert card menu**

Tap and hold on the alert card on the main screen to get an additional menu to manage your data at the alert record level. This menu allows you to:

- Mark as read - Mark all triggered notifications for that alert as read and remove the unread indicator from the alert card.
- Clear history - you can clear the history of triggered notifications for that alert only.
- Remove alert - you can choose to remove the alert from your mobile app until the next alert notification comes in.

### **Alert Summary**

If you tap on an alert card you will be taken to a summary screen which shows two sections (for data alerts); a summary of the last 10 scans for that alert - showing the most recent history of triggered and not triggered (or counts of triggered with drill to dimension alerts), and the recent triggered notifications.

### **Alert Triggered Summary and Triggered Details**

Tap and hold on the triggered notification card to see a submenu which will allow you to mark the record as read.

Tap on the triggered notification card to see the details of the alert. Once in the alert details view you can swipe left and right to scroll through the history of triggered alerts for that alert record.

### 5.5 Troubleshooting

---

A user cannot sign on to the Qlik Alerting server with the mobile application

- Check the user is able to access the Qlik Alerting server through the browser on the device. They may need to be signed into the company VPN or the ports may need to be opened to allow access to the Qlik Alerting server from the device.
- You may have certificate issues if you are not using an SSL certificate from a trusted authority which will be blocked from connecting to the Qlik Alerting server using https. The QR reader approach to sign in, and the manual approach using https will result in a network error message.
  - On Android devices there may be an additional block by the OS where the SSL certificate is seen as not fully trusted and an additional setup step is required on the Qlik Alerting server. See [Using trusted SSL certificates with Qlik Alerting \(page 13\)](#) for more details.
- If you have signed out from a different Qlik Alerting server and now cannot connect to the new server please close the app fully (including from background) and retry.

## 6 Qlik Sense extension

The Qlik Sense extension for Qlik Alerting allows users to quickly create an alert directly from the dashboard. The extension needs to be placed on the dashboard sheet by the developer and presents as a button that will fit in one default grid square of space in the dashboard.

### 6.1 Installing the Qlik Sense extension

---

The extension is bundled with the Qlik Alerting installation files.

The zip file for the extension can be retrieved from the server where Qlik Alerting is installed in the *C:\Program Files\Qlik Alerting\* folder.

**Do the following:**

1. In the Qlik Management Console (QMC), and with a user with appropriate access, navigate to the extensions section.
2. If you already have an existing extension for Qlik Alerting installed then remove this.
3. Import the Qlik Alerting extension zip file.
4. If you had any config changes to manage the default values, or would like to make them, then follow the instructions below.

#### Setting up a dedicated virtual proxy

If Qlik Alerting and Qlik Sense are installed in the same domain but on different machines, you will need to set up a virtual proxy to use the extension. This will allow you to share the session across the specified domain.

**Setting up a virtual proxy in the Qlik Management Console**

**Do the following:**

1. In the Qlik Management Console, click **Virtual proxies** under **Configure system**.
2. Click **Add new**.
3. Under **Identification**, set **Prefix** as *qawextension*.
4. Specify *X-Qlik-Session-qawextension* as the **Session cookie header name**.
5. Under **Authentication**, for **Windows authentication pattern**, type *Windows*.
6. Under **Load balancing**, specify *Central* as the **Server node**.
7. In the **Session cookie domain** field, specify your premises domain (if Qlik Alerting and Qlik Sense are installed on the same domain).

For example, if your Qlik Sense machine is *sub.subdomain.maindomain.com* and your Qlik Alerting machine is *sub2.subdomain.maindomain.com*, then your **Session cookie domain** should be *subdomain.maindomain.com*.

8. Click **Apply**.

## Creating a virtual proxy in the Qlik Management Console

**IDENTIFICATION**

Description: This is dedicated Virtual Proxy for Qlik Alerting Extension

Prefix: qawextension

Session inactivity timeout (minutes): 10

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

**AUTHENTICATION**

Anonymous access mode: No anonymous user

Authentication method: Ticket

Windows authentication pattern: Windows

Authentication module redirect URI:

**LOAD BALANCING**

**Load balancing nodes**

Server node: Central

**ADVANCED**

Extended security environment:

Session cookie domain: qliktech.com

Has secure attribute (https):

SameSite attribute (https): Lax

Has secure attribute (http):

SameSite attribute (http): No attribute

Additional response headers:

Next, set up your Qlik Alerting with the virtual proxy.

### Setting up Qlik Alerting with the virtual proxy

#### Do the following:

If you are registering for Qlik Alerting for the first time, you will be redirected on launching to the registration page. In this case, start the following procedure at step 1.

If you have already installed Qlik Alerting and want to make changes to your Qlik Sense configuration. In this case, you can start the following procedure at step 4.

1. Log in to Qlik Alerting using your admin credentials.
2. Navigate to the **Admin** menu and click **Sources**.
3. Click **Edit source** for your source.
4. Specify the same virtual proxy settings that you set earlier to share the session cookie across the specified domain:
  1. Prefix is *qawextension*.
  2. Specify the **Session cookie header name** as *X-Qlik-Session-extension*.
  3. Click **Apply**.



### Using the Qlik Alerting extension in Qlik Sense

#### Do the following:

1. Log in to Qlik Sense using your normal URL without virtual proxy.
2. Open the sheet in which you have an extension.
3. Enter your Qlik Alerting server details.

Once you enter the Qlik Alerting details, the following steps are performed:

1. The Qlik Alerting extension creates the new session for the same user with the proxy server.
2. The Qlik Alerting extension fetches the new session created by the proxy server and passes this session ID to the Qlik Alerting gateway.
3. The Qlik Alerting gateway takes care of authentication of the user against the proxy server session by the Qlik Alerting extension.
4. When the authentication is completed, Qlik Alerting sends a JWT token and end the proxy server session created by the Qlik Alerting extension.

You can use the Qlik Alerting extension for this session as long as the JWT is available. If JWT is not available, the Qlik Alerting extension will follow steps 1 to 4.

## 6.2 The user flow of creating an alert in the extension

---

1. When a user accesses a sheet with the Qlik Alerting extension, the extension will automatically authenticate against the Qlik Alerting server with the user's Qlik Sense credentials. When this check is confirmed, the **Alert** button will appear.
2. If the user is authorized to access Qlik Alerting, they will be guided through the process of creating an alert.

#### Do the following:

- a. Enter a **name** and a **description** (optional) for the alert.
- b. Select your **Data**.
  - i. Either select a measure (or measures as you can select multiple) directly from the master item list which allows access to all master item measures in the application.

OR use the **filter by object** button to look for a measure from an object (which does not need to be a master item).

- Select the object by clicking on the overlay.

The list of measures and dimensions will now reflect the data from the object only

- Press clear to remove this filter.

- ii. You may select another object to see a different set of measures as you wish, and you can select measures from different objects.
  - iii. Press the **Add** button once you have decided which measure to select and it will present in a table below, repeat to add another measure.
  - iv. Select a **dimension** (optional) for the alert if you wish to analyze the data across the values of a dimension field.
  - v. Click **Next**.
- c. Select your **Conditions**.
- i. Complete the relevant fields.
    - Column - this allows you to choose either one of the measures or the dimension.
    - Operator - select the operator to evaluate; greater than, less than etc.
    - Type - select the type of comparison you wish to make and dependent on these you will have additional fields to enter:
      - Manual - choose to enter a manual value against which to evaluate the selected column.
        - Value - enter a manual value, 100 or 0.01 for 1%.
      - Measure - choose to enter a second column against which to evaluate the selected column.
        - Compare - select another column from the data you have selected to compare the first column with.
        - Offset - you can provide an offset to the value to manage the sensitivity of the alert e.g. 5.
        - Is percent - check if the offset you have entered is to be seen as a percentage e.g. 5%.
      - Previous Scans - choose to compare the column value against the last, or aggregation of a set of previous, values.
        - Scans - Enter the number of previous scans that you wish to compare with.
        - Aggregation - If you have entered a number other than the 'last scan' then you will need to choose an aggregation option; Average, Min or Max.
        - Offset - you can provide an offset to the value to manage the sensitivity of the alert e.g. 5.
        - Is percent - check if the offset you have entered is to be seen as a percentage e.g. 5%.
      - Set - choose to compare the column row value against an aggregation of all the values in the current data set.
        - Aggregation - Enter the aggregation you want to perform across the set of values; Average, Min, Max, Percentile or Standard Deviation.

- For percentile enter the number for the percentage (e.g. 90 equals the 90th percentile value).
  - For standard deviation enter the number of standard deviations, e.g. a condition of less than 2 standard deviations should have an entry -2 as you will be looking for the value lower than the lower boundary of 2 standard deviations from the mean. A condition of greater than 1.5 standard deviations should have an entry of 1.5 as you will be looking for those values greater than the upper bound of 1.5 standard deviations from the mean.
  - Offset - you can provide an offset to the value to manage the sensitivity of the alert e.g. 5. This option is not provided for the percentile or standard deviation aggregation options.
  - Is percent - check if the offset you have entered is to be seen as a percentage e.g. 5%. This option is not provided for the percentile or standard deviation aggregation options.
- ii. Click **Next**.
- d. Review **default** selections.

You can change a number of default options here.

- Selections / Bookmarks - you can select a number of options:
    - Retain the current selections in the app (which will be saved as a bookmark).
    - Choose none to remove any selections and filters for the alert.
    - Choose from an existing bookmark from your list of accessible bookmarks.
  - Trigger - this is set to on reload and can be changed in the Qlik Alerting web portal a link to which will be provided at the close step.
  - Frequency - you can limit the number of notifications you receive even if the alert scans more times than this. For example the app may reload every 5 minutes, but you only want to be notified every hour, then select 'only the first each hour'.
  - Channels - this will default to all (meaning both email and mobile app if you have one setup). You can select to limit this to email or mobile only as you wish.
- e. Click **Create Alert**.
- You will receive confirmation of the alert creation with a link to open in the Qlik Alerting web portal if you wish to make further changes or review.
- f. Click **Close**.

## 6.3 Default options purposefully designed in the extension

---

To ensure the process is as simple as possible for end users we have used default values for some of the settings of an alert in the Qlik extension. These can be easily updated in the alert record after creation using the URL link provided at the end of the create alert process.

The following are the default options purposefully designed into the extension:

- Filters are set as a bookmark on the current selections at the time of creating the bookmark. However, you can update this selection to an existing bookmark in the final review stage of the creation process.
- The schedule of the alert is set to on reload as this is by far the most common choice for users.
- Distribution settings (broadcast or managed shared alert settings) are not managed in the extension.

All other details can be updated through the Qlik Alerting web portal. A link to the web portal is provided from the confirmation screen when an alert is created.

### Setting up the Qlik Alerting extension on a sheet in a dashboard

#### Do the following:

1. Navigate to the dashboard and sheet where you wish to place the extension.
2. In the **Edit** view of the dashboard sheet, either as the developer or as a **My Sheet** for a user, you can access the extensions from the **Custom Objects > Extensions** options selections on the left hand menu.
3. Place the Qlik Alerting extension, drag and drop from the extensions library, onto the grid and into the desired position.
4. Bring up the properties for the extension. Click the extension and the properties will appear on the right hand side of the screen.
5. In the admin settings section, update the **contact email for support** email address so users are guided to whom they should contact in your organization if there is a problem with their connection to Qlik Alerting, such as the Qlik Sense user does not have a license in Qlik Alerting.
6. In the Qlik Alerting server settings section, update the details of the Qlik Sense server:
  - a. Update the **Qlik Alerting DNS/IP** with server name (FQDN) or IP of the Qlik Alerting server. This will be the address with which you can open the Qlik Alerting web portal in a web browser. Do not specify *http://* or *https://* nor the port in this field.
  - b. Update the **Port** with the correct port as specified during the setup of the Qlik Alerting server. This is the port that is part of the address you use to open the Qlik Alerting web portal in a web browser.
  - c. Check the **HTTPS** box to force only secure connections through HTTPS.

- d. If you have a proxy or reverse proxy server that redirects to the Qlik Alerting server, select the **Reverse proxy redirection** option and enter in the Qlik Alerting DNS/IP field the proxy server address without specifying the protocol or port.

### 6.4 Updating the default values for the extension

---

If you are an admin on your Qlik Sense site, and are comfortable with the extension editor in the dev hub, you can adjust the default values in the extension for all users who subsequently place the extension on their dashboards (removing the steps above for the user).

Follow the simple steps below but note you will need to repeat these steps each time you update the extension. Row references may change slightly but the order will remain the same.

#### Do the following:

1. Open the Qlik Alerting extension in the Qlik Sense Dev Hub
2. Navigate to the `js|definition.js` file.
3. On row 17 the `defaultValue` entry for the **Qlik Alerting DNS/IP** can be updated to your Qlik Alerting server.
4. On row 23, the `defaultValue` entry for the **Port** field can be updated with the correct port number for connections to your Qlik Alerting server.
5. On row 29, the `defaultValue` entry for **HTTPS** should be set to `false` if you wish to allow HTTP connections or `true` to force an HTTPS connection (this will be linked to the port you have chosen).
6. Save the `definition.js` file, refresh your browser connection to Qlik Sense and the next time you drag the extension onto a dashboard sheet the new default values will appear.



*This does not change the values entered in any previously placed instances of the extension. It will only affect newly placed versions of the extension.*

### 6.5 Troubleshooting

---

#### The alert button doesn't activate but I am a licensed user in Qlik Alerting?

This can be caused by a browser security exception. Check if the following options can be used to resolve this issue:

- Check your browser to see if it is blocking 'unsafe scripts'. On Google Chrome this shows as a shield icon in the right hand side of the URL bar. Click on this and allow click allow unsafe scripts.
- Qlik Alerting validates that the extension is being used on the same domain as the Qlik Sense source.
- To setup Qlik Alerting to use a trusted certificate should remove this security exception, see [Using trusted SSL certificates with Qlik Alerting \(page 13\)](#) for more details.

- You could also set the extension to run as HTTP (clear the HTTPS check box in the extension object settings), and access your Qlik Sense dashboard using HTTP.



*You may need to downgrade the HSTS security settings to revert back to HTTP, see [Administration \(page 7\)](#) for more details.*

- Ensure you run Internet Explorer with compatibility mode turned off.

### 6.6 URL redirection support

---

This topic provides an end-to-end example of using an NGINX reverse proxy or an IIS server with a redirection URL to the Qlik Alerting server.

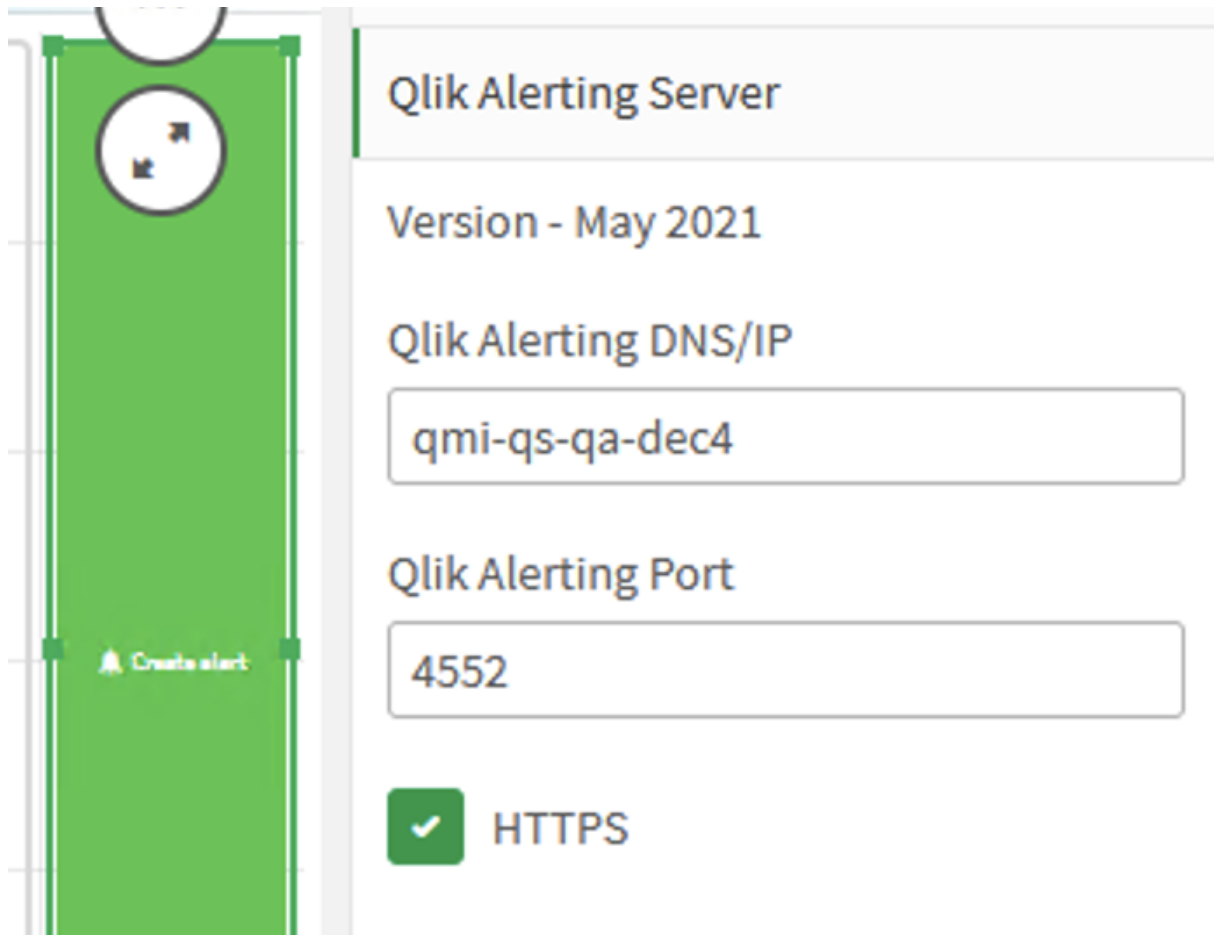


*To follow this example or to implement it in a production environment you need to have the Qlik Alerting October 2021 version or later.*

#### Problem use case

The expected behavior of the Qlik Alerting extension when added to a sheet is to display the server information in the extension, as shown in the image below.

### Qlik Alerting extension



This works only if the Qlik Sense and Qlik Alerting are on the same network. If the Qlik Alerting server is outside of the network, you must set up a reverse proxy to redirect the request coming from outside of the network to the Qlik Alerting server. For example, if the Qlik Alerting proxy server **QMI-WN-BL-2263** is outside the network, then the extension will fail, as shown below.

Failed Qlik Alerting extension

The screenshot shows the configuration interface for the Qlik Alerting extension. On the left, a configuration card is highlighted with a green border. A red error message is displayed on the card: "Check your URL matches the field Alias hostname in Qlik Alerting/Sc". Two circular callouts point to the error message and a menu icon. On the right, the configuration fields are: "Qlik Alerting Server" (empty), "Version - May 2021", "Qlik Alerting DNS/IP" (QMI-WN-BL-2263), "Qlik Alerting Port" (4552), and a checked "HTTPS" checkbox.



*It fails because the URL is different from the one set during the Qlik Alerting registration process, and because the proxy server configuration allows this extension to redirect to the original server.*

## Configurations on Qlik Sense hub and Qlik Alerting

The solution is to configure the extension, the Qlik Alerting server, and the proxy server. The following instructions show how to implement an IIS server and an NGINX server to act as a reverse proxy.

### Qlik Alerting registration process

- During the registration process (or on the sources tab for servers with the product already installed), enter the URL from the redirection proxy server. Do not include the protocol or port information. This provides a security check to match the value the customer is trying to configure on the extension.

Reverse proxy URL redirection

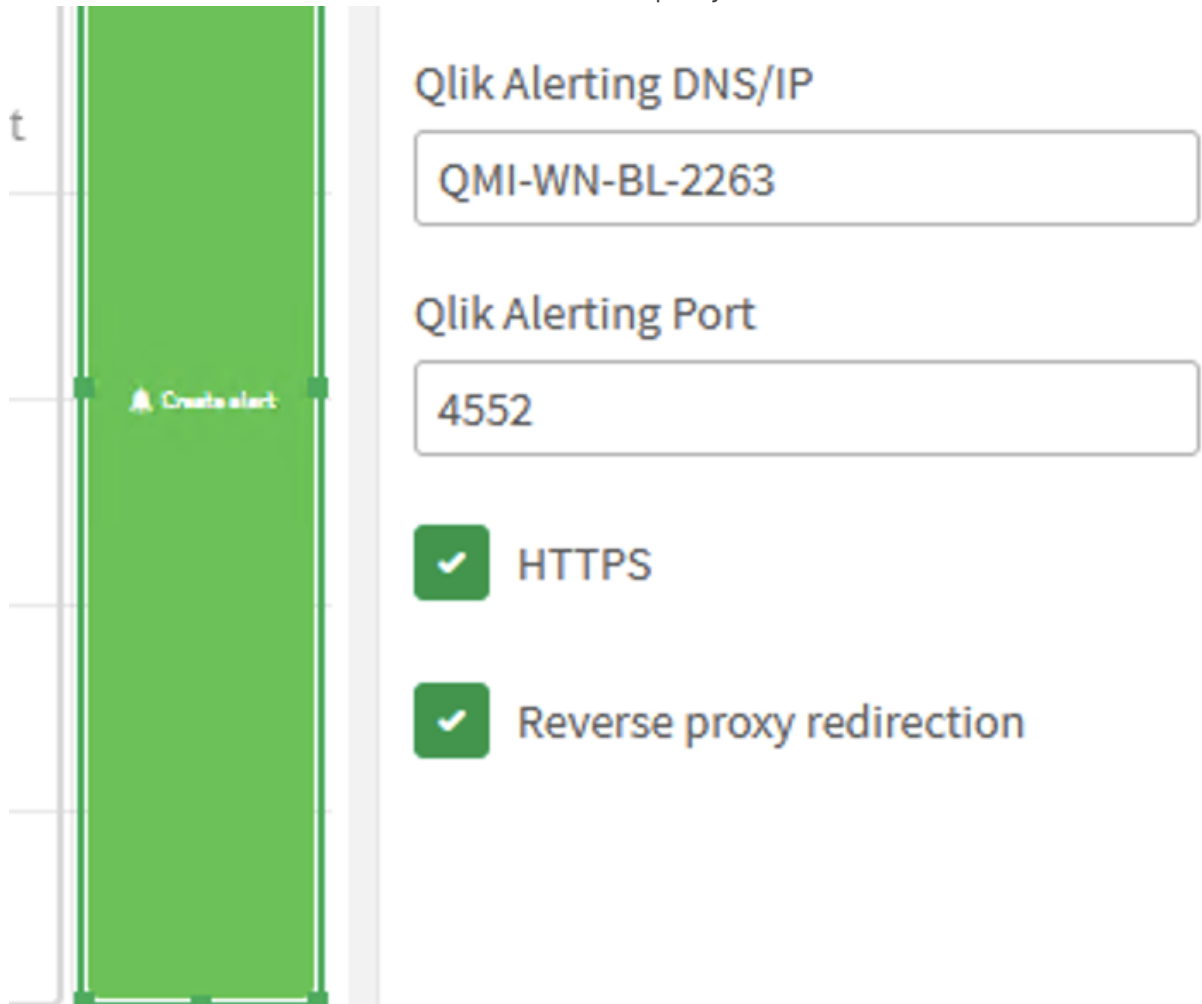
QMI-WN-BL-2263

URL from a reverse proxy, e.g redirectionurl.rdlund.qliktech.com



### Configure the Qlik Sense extension

- In the extension configuration window, enter the Qlik Alerting DNS name and port number.
- Select **HTTPS**.
- Select **Reverse proxy redirection**. This option tells Qlik Alerting that this is a redirection URL, and it should be checked with the one in the reverse proxy URL redirection field.



Qlik Alerting DNS/IP

QMI-WN-BL-2263

Qlik Alerting Port

4552

HTTPS

Reverse proxy redirection



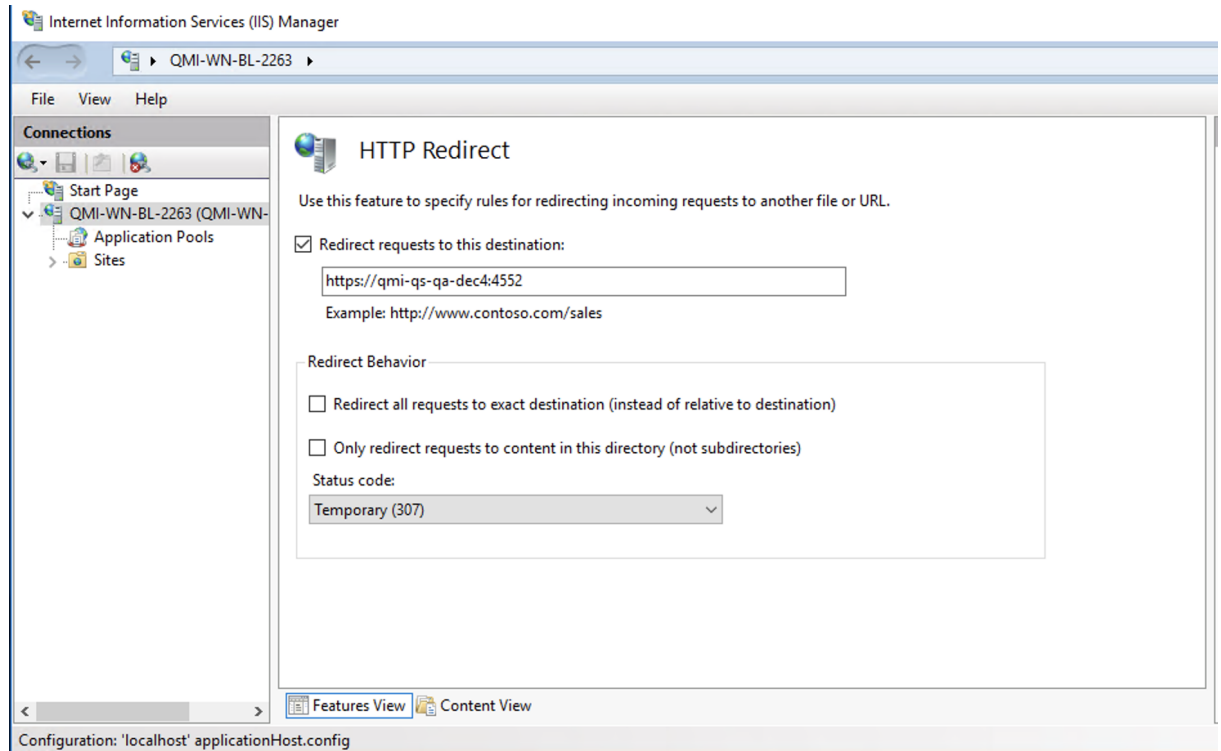
When this is configured, the extension lets you create an alert.

### Configure the proxy servers

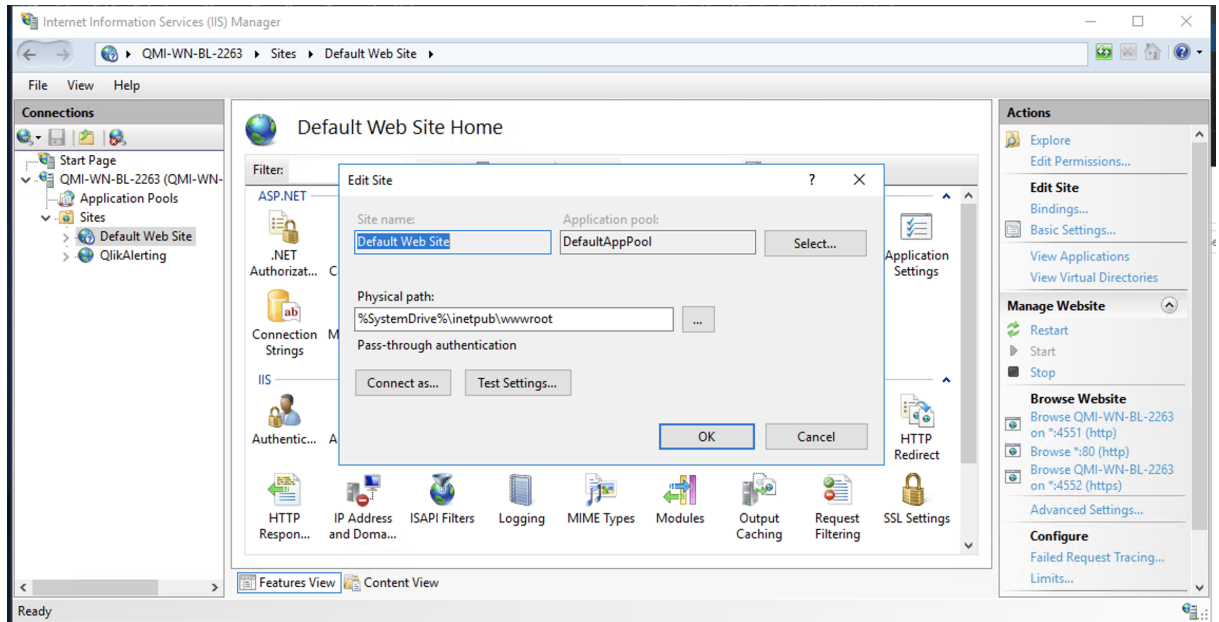
This section covers the configuration instructions for two servers: IIS server and NGINX reverse proxy server.

#### IIS server

1. On the IIS Manager, set the status code to 307. Every request to the IIS server that redirects to the original Qlik Alerting server must return a 307 code (which means temporary redirection). This allows the extension connect properly with the alerting server in the request.



2. Download CORS: <https://www.iis.net/downloads/microsoft/iis-cors-module>  
You need to enable CORS for IIS.
3. Once CORS is downloaded, return to the IIS Manager.
4. From the left-side pane, go to **Default Web Site**.
5. On the right-side pane, click **Actions > Edit site > Basic settings**.
6. In the **Physical path** field, verify the path to the `wwwroot` folder. `C:\inetpub\wwwroot` is the default IIS location.




7. Go to this folder and open the *web.config* file.

When you open that file, by default, looks like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <httpsRedirect enabled="true" childOnly="true" />
  </system.webServer>
</configuration>
```

8. Modify this file to look like this:

 *Where origin is the Qlik Alerting server.*

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <directoryBrowse enabled="true" />
    <cors enabled="true" failUnlistedOrigins="true">
      <add origin="https://qmi-qs-qa-dec4"
        allowCredentials="true"
        maxAge="120">
        <allowHeaders allowAllRequestedHeaders="true">
          <add header="header1" />
          <add header="header2" />
        </allowHeaders>
        <allowMethods>
          <add method="OPTIONS" />
        </allowMethods>
      </add>
    </cors>
  </system.webServer>
</configuration>
```

```
</system.webServer>
</configuration>
```

9. Save this file and restart the IIS server.

Enter the redirection address and port on the extension. If the configuration is correct, and there are no firewall restrictions or other internal security measures, the button should pop up and you can create an alert.

### NGINX reverse proxy

Lets say we have the same server as before with the address `https://QMI-WN-BL-2263`, and we want to use this server as a reverse proxy with NGINX to redirect all the request to the original Qlik Alerting server using the port 443.

Every NGINX server has the configuration file to set the properties for the http or https server we are running, it should be located under the root NGINX folder where you have installed it, under the name `nginx.conf`, to be able to handle the redirections properly and bypass the CORS issue, we have to set the following properties:

1. Open the `nginx.conf` file.

You need to allow requests on the extension.

2. Set the `add_header` to the following:

```
add_header 'Access-Control-Allow-Origin' $scheme://<OriginalServer>
add_header 'Access-Control-Allow-Headers'
'token,isreverseproxy,reverseproxyurl,Content-Type,Range';
```



*Where `<OriginalServer>` is either your Qlik Sense server or the Qlik Alerting server. If you get a message on the console that the origin doesn't match, try the other.*

3. Set the request method to 'options' to make a preflight request to the redirection server to check for CORS. Add the following:

```
if ($request_method = 'OPTIONS') {
    return 200;
}
```

4. Add a redirection for requests with a 307 code to the Qlik Alerting server.

```
return 307 $scheme://qmi-qs-qa-dec4:4552:port$request_uri;
```

The entire config file should look like this:

```
#user nobody;
worker_processes 1;

#error_log logs/error.log;
#error_log logs/error.log notice;
#error_log logs/error.log info;

#pid logs/nginx.pid;
```

```
events {
    worker_connections 1024;
}

http {
    include mime.types;
    default_type application/octet-stream;

    #access_log logs/access.log main;

    sendfile on;
    #tcp_nopush on;

    #keepalive_timeout 0;
    keepalive_timeout 65;

    #gzip on;

    server {
        listen 80;
        server_name localhost;

        #charset koi8-r;

        #access_log logs/host.access.log main;

        location / {
            root html;
            index index.html index.htm;
        }

        #error_page 404 /404.html;

        # redirect server error pages to the static page /50x.html
        #
        error_page 500 502 503 504 /50x.html;
        location = /50x.html {
            root html;
        }

    }

    # HTTPS server

    server {
        listen 443 ssl;
        server_name QMI-WN-BL-2263;

        ssl_certificate cert.pem;
        ssl_certificate_key cert.key;

        ssl_session_cache shared:SSL:1m;
    }
}
```

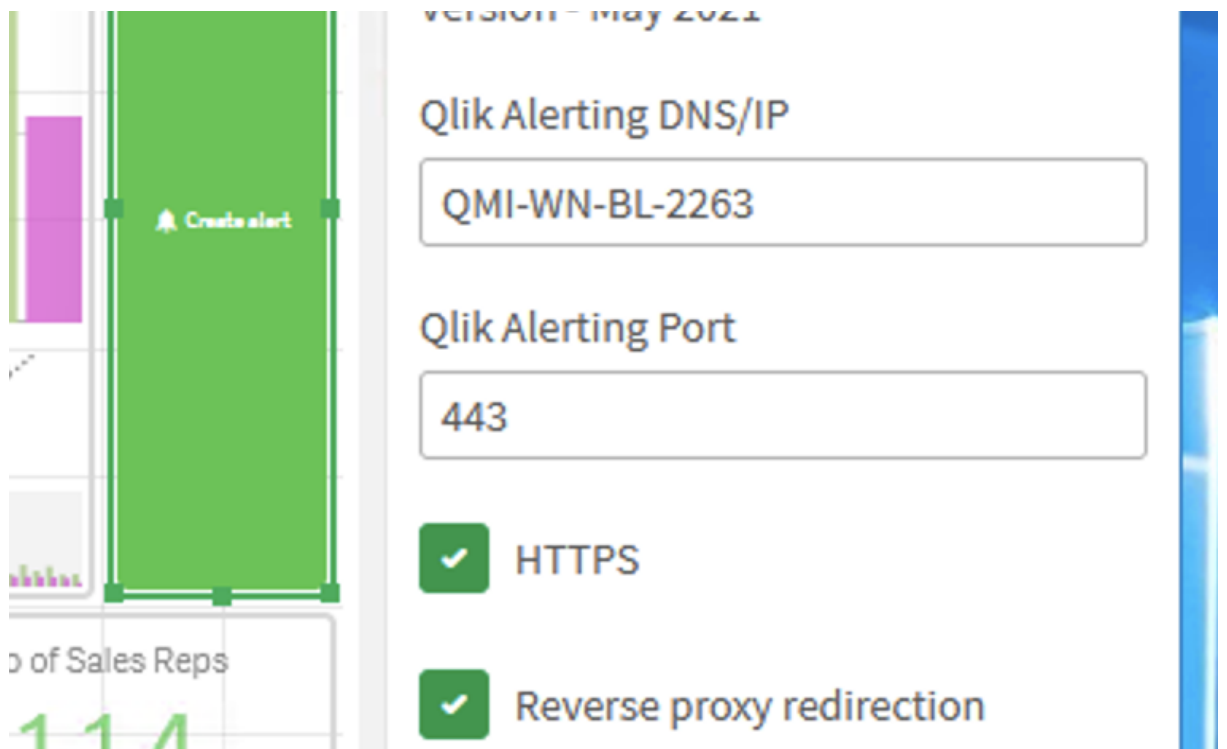
```

ssl_session_timeout 5m;

ssl_ciphers HIGH:!aNULL:!MD5;
ssl_prefer_server_ciphers on;
add_header 'Access-Control-Allow-Origin' add_header 'Access-Control-Allow-
Headers' 'token,isreverseproxy,reverseproxyurl,Content-Type,Tange';
if ($request_method = 'OPTIONS') {
    return 200;
}
location / {
    root html;
    index index.html index.htm;
}
#redirecting
return 307 $scheme://qmi-qs-qa-dec4:4552$request_uri;
}
}

```

- Restart the NGINX server.
- Return to the extension to verify the redirection. The button should appear and you should be able to create alerts.



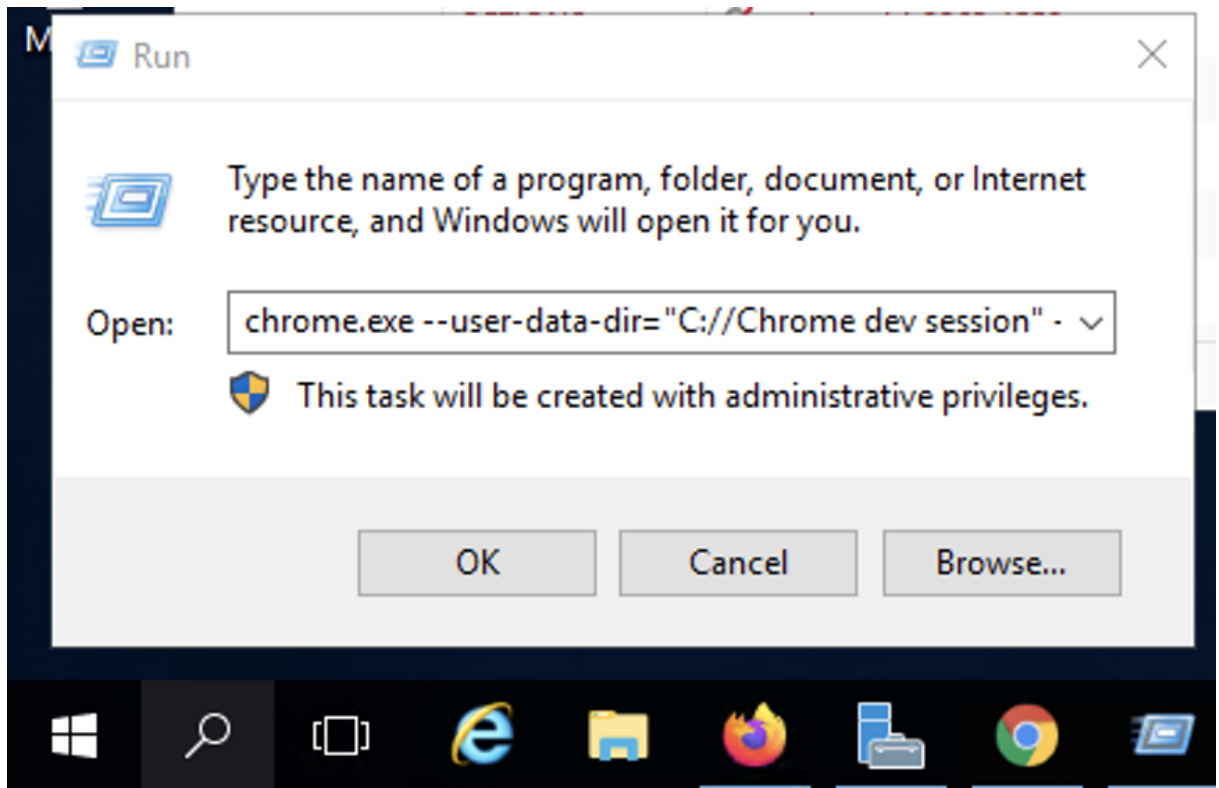
### Troubleshooting for Chrome browser

Requests that are directed through different servers are hard to debug when they fail. For example, with CORS, you can check your network tab to see when request fail.

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
	OPTIONS	qmi-wn-bl-2263:4552	extension	xhr		CORS Failed	0 B	1201 ms
	OPTIONS	qmi-wn-bl-2263:4552	extension	xhr		CORS Failed	0 B	1651 ms

To determine where the requests fail:

1. Go to the Windows search menu, type "Run".
2. In the Run window, enter: `chrome.exe --user-data-dir="C://Chrome dev session" --disable-web-security`



3. This starts a browser with the flag `--insecure` and you will be able to check if you have a CORS issue or something else that is blocking your request between servers.