Contents

1 Qlik Alerting ................................................................................................................ 5

2 Administration ............................................................................................................. 6
  2.1 Syncing users from Qlik Sense .............................................................................. 6
  2.2 Assigning administrator rights to a user .............................................................. 6
  2.3 Assigning user licenses ....................................................................................... 6
  2.4 Assigning user privileges ...................................................................................... 7
    Steps to assign a user privilege ................................................................................ 7
  2.5 Disabling access for a user ................................................................................... 8
  2.6 Updating a Qlik Alerting license ......................................................................... 8
  2.7 Using trusted SSL certificates with Qlik Alerting .................................................. 8
    Steps to add a trusted SSL certificate for Qlik Alerting ........................................ 9
  2.8 Changing the ports for Qlik Alerting web access ................................................ 9
  2.9 Backup and restore the MongoDB database .......................................................... 10
    Steps to backup ........................................................................................................ 10
    Steps to restore ......................................................................................................... 10

3 Installation .................................................................................................................. 11
  3.1 Installation prerequisites ....................................................................................... 11
    Minimum hardware requirements ............................................................................ 11
    Install NodeJS ......................................................................................................... 11
    Install MongoDB .................................................................................................... 12
    Install Redis ............................................................................................................ 13
    Firewall settings ..................................................................................................... 14
    Exporting Qlik Sense certificates ............................................................................ 15
  3.2 Qlik Alerting installation ....................................................................................... 15
    Install Qlik Alerting ............................................................................................... 15
    License setup ........................................................................................................... 16
    Qlik Alerting settings ............................................................................................. 16
    Email server configuration ...................................................................................... 16
    Qlik Sense connection configuration ..................................................................... 17
    Select an administration user ................................................................................ 17
    Additional step if ports were changed in Qlik Alerting settings step .................... 19
  3.3 Upgrade an existing version ................................................................................... 19
    Supported versions for upgrades ............................................................................ 19
    Upgrade steps .......................................................................................................... 19

4 Managing alerts ......................................................................................................... 21
  4.1 Data alerts .............................................................................................................. 21
  4.2 System alerts .......................................................................................................... 21
  4.3 Broadcast notifications ........................................................................................... 21
  4.4 Broadcast notifications ........................................................................................... 21
    How to create a broadcast notification .................................................................... 21
  4.5 Data alerts .............................................................................................................. 23
    How to create a data alert ....................................................................................... 23
    Data alert types ....................................................................................................... 30
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 make the setup of users as simple as possible Qlik Alerting imports users from the linked Qlik Sense installation. This process is automatically completed when you first install the product and connect to the datasource. To manually activate the sync process you can follow the simple steps below.

Do the following:

1. Navigate to Admin > User Management > Users. (You will need to be logged in as an administrator or the super admin to view this menu.)
2. Click Sync Qlik Sense Users at the bottom left of the table.

   This process may take a number of seconds if you have a large number of users.

2.2 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 edit button on the bottom toolbar.
4. Change the user role dropdown and select administrator.
5. Click Save.

2.3 Assigning user licenses

Do the following:

1. Navigate to Admin > License Allocation. (You will need to be logged in as an administrator or the super admin to view this menu.)

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

2. Click the edit (pencil) icon of the license type you wish to assign users to.

   The next page will show you two lists of users: on the left those who have not been assigned this license type and on the right those who are already assigned.
2. Select those users you wish to move. Use the search to find users easily.
3. Click on the direction arrows to move them from one list to the other.
4. Click Update.
5. Continue to assign users to other license types as required.

A user does not need to be assigned to both a broadcast and standard license. A standard license user can receive broadcast alerts as part of their license.

2.4 Assigning user privileges

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. Users can be given additional functionality through the assignment of user privileges.

The following user privileges are available:

<table>
<thead>
<tr>
<th>User privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>systemAlerts</td>
<td>Allows the user access to system alerts functionality to create and receive system alert notifications.</td>
</tr>
<tr>
<td>broadcastAlerts</td>
<td>Allows the user access to create broadcast and managed shared alerts which are sent to users with either a standard or a broadcast license.</td>
</tr>
<tr>
<td>broadcastNotification</td>
<td>Allows the user access to create and manage broadcast notifications. These are manually created notification messages that can be sent to a user group.</td>
</tr>
<tr>
<td>shareAlerts</td>
<td>Allows the user to be able to share alert records they have created with other users. This functionality makes a copy of the alert record that the recipient will take ownership of when they accept.</td>
</tr>
</tbody>
</table>

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 or the super admin 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 (pencil) icon of the user privilege type you wish to assign users to.
   
   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**.

6. Continue to assign users to other license types as required.

---

**A user does not need to be assigned to both a broadcast and a standard licenses. A standard license user can receive broadcast alerts as part of their license.**

### 2.5 Disabling access for a user

You can disable access in two ways:

- Remove the license allocation in **Admin > User Management > License Allocation**.
- Disable the user in the **Admin > User Management > Users table**.

---

**If the user has an Administrator role they will still be able to login even though these settings are removed, although they will not receive alert notifications.**

Remove the Administrator user role, and reset to user, for any disabled users.

### 2.6 Updating a Qlik Alerting license

In order to use Qlik Alerting you will need a valid license key. When you initially purchased your licenses, or when you received a renewal of your licenses, you will have received an email from Qlik which included your license details, a license key, a control number and a license JSON file (attachment).

Do the following:

1. Navigate to **Admin > License Management**. (You will need to be logged in as an administrator or the super admin to view this menu.)
2. Enter the **License key**.
3. Enter the **Control number**.
4. Enter the **Registered email**. This is the email that the license email was sent to.
5. Upload the license file `<organisationName>.json` that was attached to the license email.
6. Click **Update**.

### 2.7 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 affect 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 to 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`.
   - In Qlik Alerting April 2020 there is no support for pass phrases for SSL certificates.

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

**2.8 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.
   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.

2.9 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\4.0\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\4.0\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\4.0\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.
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, MongoDB or Redis 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.
- An install of Redis, locally or on another server.
- Administrator access to the server to update firewall settings.
- Administrator access to the server to install Qlik Alerting.

Follow the steps in Installation prerequisites (page 11) 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 15)

3.1 Installation prerequisites

Minimum hardware requirements

Qlik Alerting can be installed on the same server as Qlik Sense, however it is recommended that Qlik Alerting is installed on its own server separate to the Qlik Sense server. This is to follow Qlik’s best practices of having dedicated hardware for Qlik Sense. Here are the minimum hardware requirements for Qlik Alerting:

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Microsoft Windows Server 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Microsoft Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2016</td>
</tr>
<tr>
<td>Processors (CPUs)</td>
<td>Multi-Core x64 compatible processors</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB RAM minimum</td>
</tr>
<tr>
<td>Disk Space</td>
<td>32 GB minimum</td>
</tr>
<tr>
<td>Qlik Alerting Mobile App Android Support</td>
<td>Version 4.4 or above</td>
</tr>
<tr>
<td>Qlik Alerting Mobile App iOS Support</td>
<td>iOS 10.3.x or above</td>
</tr>
</tbody>
</table>

Install NodeJS

NodeJS is the core engine of Qlik Alerting.

Do the following:
1. Download the latest v.10 version for Windows from the Nodes.js® web site. Select the node-v10.xx.x-x64.msi option for the Windows installer.

As of February 6, 2020, the latest version is 10.19.0 and the Windows 64-bit installer can be downloaded directly here.

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.

4. Restart your computer.

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:

1. Open the Command window, PowerShell, or a similar command line tool.
2. Type node -v.

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

**Test NPM**

Do the following:

1. Open the Command window, PowerShell, or a similar command line tool.
2. Type npm -v.

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

**Install MongoDB**

MongoDB is the main repository database for Qlik Alerting.

Do the following:

1. Download MongoDB version 4.0.4 for Windows.

   An .msi file similar to mongodb-win32-x86_64-2008plus-ssl-4.0.4-signed.msi will be downloaded in your system.
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.

Change the Qlik Alerting config for the server connection for MongoDB navigate to the Queuer config file C:\Program Files\Qlik Alerting\repository\config\production.json and update the details in both the data and logs objects:

- "ip": "ip or dns of the MongoDB server" (default is localhost)
- "port": 27017 (default is 27017)
- "database": "qlikalerting"
- "config": {}

Install Redis

Qlik Alerting uses the Redis database as a persistent cache which ensures no alerts are missed, even when there is downtime on the server.

Do the following:

1. Download the Windows installer version of Redis.

   This install process uses version 3 of Redis which is not the most recent but Redis is not natively supported on Windows Server. We are building out a number of infrastructure options with Docker and Kubernetes which will allow us to manage this process better in the very near future.

2. Extract the downloaded redis64-latest.zip files.
   a. Right-click the zip file.
   b. Select Extract All.
   c. Enter your chosen location, for example, C:\Redis.

3. Initiate Redis for the first time.
   a. Navigate to the folder where you have extracted the files to, from this point on this will show as C:\Redis.
   b. Right-click the C:\Redis\redis-server.exe file and run as administrator.
      This will open a command window and the final line will show you the port on which Redis is running, port 6379.
   c. Do not close this window at this time, Redis is running through the command line so closing it will close Redis. We will create the service shortly.

4. Validate Redis connectivity.
Installation

a. Right-click the C:\Redis\redis-cli.exe file and run as administrator.
   This will open a command window.

b. Type ping and press Enter.
   Redis should return the text ‘PONG’.

c. Close all command windows before the next step.

5. Setup Windows service for Redis.

a. Open a new command window with run as administrator privileges.

b. Change directory to the Redis folder.
   - Type cd c:|Redis (or the path to your Redis folder) and press Enter.

c. Create the Redis service.
   i. Type (or copy and paste) redis-server --service-install redis.windows.conf --loglevel verbose --service-name redis and press Enter.
   ii. Type net start redis and press Enter to start the service.

d. Update the recovery settings for this service so it restarts if something happens to cause it to stop (such as Windows updates etc).
   - Type (or copy and paste) sc failure "redis" actions= restart/5000/restart/5000/restart/5000 reset= 86400 and press Enter.

   Alternatively you can make these changes through the Windows services GUI.

6. You can now close all of the command line windows as Redis is now running as a Windows service.

Alternative Redis options

You can setup and manage Redis in a number of different ways assuming you have the ability to support these in your environment. This will allow you to run the latest version of Redis.

- If you are using Microsoft Windows Server 2019 or later, you can install Redis natively in a Linux container through the Windows subsystem for Linux (WSL) functionality. A standard install of Redis on a QSL distribution will use the same IP and ports, so there are no configuration changes required in Qlik Alerting.

- You can also choose to use a separate Linux server to host your Redis server. You will need to manage the firewalls between the two servers to ensure that the Qlik Alerting server can access the Redis server. To change the Qlik Alerting configuration for the server connection for Redis, navigate to the Queuer configuration file C:|Program Files|Qlik Alerting|queuer\config\production.json and update the Redis object details:
  - "ip": "ip or dns of redis server" (default is localhost)
  - "port": 6379 (default is 6379)
  - "user": ""
  - "password": ""

Firewall settings

There are ports that are required to be opened in order to enable communication between Qlik Alerting and Qlik Sense.
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 4551) 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)

**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 Qlik Alerting installation

*Ensure you have installed NodeJS, MongoDB and Redis as per the Installation prerequisites (page 11) instructions.*

**Install Qlik Alerting**

Do the following:
3 Installation

1. Check that the MongoDB and Redis services are running in the Windows services window.
2. Download the Qlik Alerting installer and save it to your hard drive ready for installation. This is accessible from the Qlik Download Site.
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.

License setup
You should have received an email from QlikAlertingLicense@qlik.com which has all of the information required.

1. Download the .json file that is attached to that email.
2. Enter the license key and control number from the email into the form.
3. Enter the email address which originally received the license email (this is part of the validation and it must match).
4. Upload the .json file downloaded from the email into the form.
5. Click Validate to confirm the license details.

Qlik Alerting 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. Go to Admin > Delivery Channels.

2. You will see a table of delivery channels.
   - If a record exists, select the Company Mail record and click the pencil icon on the right to edit the record.
   - If no record exists in this table, click Create New.

3. Enter your mail server details:
   - Authentication Method (Basic, Anonymous, or NTLM)
   - SMTP Address
   - Port No.
   - Secured: None / TLS / SSL
   - Email User Name
   - Password
   - Default Sender ID

4. Click Test Connection. You will see a message popup at the bottom of the screen and should receive an automated email message to the email account entered.

5. Click Save to save your configurations settings.

Ensure you have the correct firewall settings for Qlik Alerting to communicate with your mail server.

Qlik Sense connection configuration

Do the following:

1. Enter the following details for your Qlik Sense site.
   - **Host Name** is the IP or DNS of the Qlik Sense Server (this should be a whitelisted value in the Qlik Sense Virtual Proxy and 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 Service API Listen Port** will default to 4242 as per the standard install of Qlik Sense.
   - **Connect as username** 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 whom can access all users, tasks and apps.

   - **User Directory** is the Qlik Sense directory that the above user is assigned to.
3 Installation

- **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). Please 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 Host Name for Email URL** allows you to enter a slightly different URL for access to the server. In most circumstances repeat the *Host Name* entry here. Where the hostname is an internal only connection due to network restrictions you will need to enter the external DNS or IP to ensure links from emails etc can work.

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 15)* 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.

5. You no longer need to restart the services.

   **During this connection process the Qlik Sense users will sync across to Qlik Alerting (for the first time).**

**Select an administration user**

In order to manage the Qlik Alerting site an administration user must be present. The Users will have synced during the preceding Qlik Sense connection step so now we should enter the domain\username of the administration user. This will be validated against the user list to ensure it is correct.

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.

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 the go to the logon page https:\\QlikAlertingServer:4552, click the forgotten password link, enter your username and click Recover Password.**
3 Installation

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.
3. 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.
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.
5. Restart the Qlik Alerting Gateway service.

3.3 Upgrade an existing version

Supported versions for upgrades

This release of Qlik Alerting has a number of significant backend changes over previous versions. As a result you will need to upgrade to a minimum version of 2019.03.02.26. Please contact support for access to this installer.

Upgrade steps

To upgrade to the April 2020 version of Qlik Alerting we will need to follow a slightly different process to normal, as there are some backend changes that are required.

Do the following:

1. Backup the MongoDB database. This will be either pingalerting or qlikalerting, depending on the version installed. For details, see Backup and restore the MongoDB database (page 10).
2. Backup any SSL certificates, if you have added these to your site.
   * For the 2019.03.02.26 version, these will be found in the C:\Ping Alerting\client\trusted_certificate folder.
   * If you are on a later version than 2019.03.02.26, these will be found in the C:\Program Files\Qlik Alerting/gateway/config/certificates/self or C:/Ping Alerting/gateway/config/certificates/self folders.
3. Uninstall Ping Alerting using the Add or remove programs option or by right-clicking C:/Ping Alerting/unins000.exe and selecting Run as administrator.
4. Download the Qlik Alerting installer from the Qlik Downloads site.
5. Right-click on the download and select Run as administrator.
6. Follow the steps to accept license agreement and install.

   The install process will recognize the existing pingalerting/qlkalerting database and perform any database migration tasks required.
7. Once complete, check that all Qlik Alerting services are running.

8. 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 8) as the location for these has changed.
   - 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 9).
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 is 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 and 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 **My 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**

> Any references to scan in the below details are to be seen as triggered. This notification will trigger each time as there is no data and condition to validate.

Do the following:

1. Enter a **Scan From** 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. **Days of Week**. Allows you to select on which days of the week the alert scan will trigger. For example you could set it to be only for working days of the week. Leaving this selection field blank will automatically select all days of the week.

4. **Days of Month**. Allows you to select the day of the month on which the alert scan will trigger, for example, the third day of each month for financial reporting purposes.

> These selections are an either/or selection and will work independently. If you select the first day of the month and a Monday for day of the week the alert scan will trigger on each Monday and on the first day of the month (regardless of which day of the week this is).
4 Managing alerts

5. 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.*

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.

**How to create a data alert**

**Create new 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.

**Data Table section**

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

Do the following:

- Enter an **Alert Name** and **Alert Description** (optional) at the top of the screen.

**Data Source**

Do the following:

1. Select the Qlik Sense **Application**.
2. 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.

**Measure**

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.
Do the following:

1. Select a measure from the list of master item measures or create an expression using the Custom Measure switch.
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 this selection area.
4. Repeat this process to add additional measures.

Measures can be removed by clicking the X next to the measure in the list.

5. If no dimension or filters are required, click the refresh table button to review the values of the measure selected.

Drill to Dimension (optional)

The drill to dimension option allows the selection of a dimension to allow the checking of 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.

Filters

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

Do the following:

1. Select a Bookmark from the application. This will show a list of the bookmarks that the logged on user can see in the application.

   OR

   Select a Filter Field from the list available.

2. Select the Values in that filter field. Search for the values to simplify creating the value list by typing into the space.

3. Click Add Filter.

4. Repeat this process to add more field and filter values

5. Click on the refresh table button to review the table of data that will be the base of your alert conditions and notifications.

Condition section

The conditions section allows you to create multiple conditions from the measures and dimension 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:
4 Managing alerts

- 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.
4 Managing alerts

- **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)*

**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**.
4 Managing alerts

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 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 Calculate Conditions 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.

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
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. Days of Week. Allows you to select on which days of the week the alert scan will trigger. For example you could set it to be only for working days of the week. Leaving this selection field blank will automatically select all days of the week.
4. Days of Month. Allows you to select the day of the month on which the alert scan will trigger, for example, the 3rd day of each month for financial reporting purposes.

   These selections are an either/or selection and will work independently. If you select the first day of the month and a Monday for day of the week the alert scan will trigger on each Monday and on the first day of the month (regardless of which day of the week this is).

5. 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:
4 Managing alerts

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)

**Notification section**
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 31)*.

You can skip this section if you do not want to change the default notification (recommended).

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 31)*). 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 other users or user groups

How does it work
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 broadcast alert 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
Recipients need to have either a Qlik Alerting broadcast license or a full standard Qlik Alerting license. These recipients do not need to be users in Qlik.

Recipients can unsubscribe from a broadcast alert
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 this 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 does it work
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 broadcast alert 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 needs to be a licensed Qlik Alerting user with a standard Qlik Alerting license, they also need to have access as a user to Qlik Sense. This allows Qlik Alerting to 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.

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.

Drill into dimension alerts can also be sent as managed shared alerts or broadcast alerts to other users if required.

**Who can create a drill into dimension alert**

All standard 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.

**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:

<table>
<thead>
<tr>
<th>Example</th>
<th>Notification/Subject code example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain text</td>
<td>&quot;ALERT : You're about to run out of stock&quot;</td>
</tr>
<tr>
<td>Using the alert name</td>
<td>&quot;ALERT : &quot; + {{alertName}}</td>
</tr>
<tr>
<td>Single alert example</td>
<td>&quot;ALERT : &quot; + {{measures.0}} + &quot; is &quot; + {{conditions}} + &quot;!&quot;</td>
</tr>
<tr>
<td>Drill to dimension alert example</td>
<td>&quot;ALERT : &quot; + {{nRows}} + &quot; &quot; + {{dimensions.0}} + &quot; with &quot; + {{measures.0}} + &quot; t &quot; + {{conditions}} + &quot;!&quot;</td>
</tr>
</tbody>
</table>

See the Dynamic text variables (page 32) 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.

```html
<!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.

<table>
<thead>
<tr>
<th>Variable label</th>
<th>Variable code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipient Name</td>
<td>{{firstName}}</td>
<td>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.</td>
</tr>
<tr>
<td>Alert ID</td>
<td>{{alertId}}</td>
<td>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.</td>
</tr>
<tr>
<td>Alert Name</td>
<td>{{alertName}}</td>
<td>Provides the name of the alert record.</td>
</tr>
<tr>
<td>Alert Triggered Timestamp</td>
<td>{{timestamp}}</td>
<td>Provides the timestamp when the alert was triggered in Qlik Alerting.</td>
</tr>
<tr>
<td>Alert Measure</td>
<td>{{measures.0}}</td>
<td>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.</td>
</tr>
<tr>
<td>Alert Measure Current Value</td>
<td>{{value}}</td>
<td>Provides the current value of the measure at the time of the scan.</td>
</tr>
</tbody>
</table>

*This variable does not exist for drill to dimension alerts.*
### 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%">Field</td>
    <td>Selections</td>
  </tr>
  {{#query.filters}}
  <tr style="border-bottom:1px solid #dfdfdf;">
    <td>{{field}}</td>
    <td>{{#values}}
      <table style="padding:0px; font-size:13px; width:100%">
        <tr>
          <td>{{.}}</td>
        </tr>
      </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:

```html
<table style="color:#494848; font-size:13px; line-height:1.8; table-layout:auto; width:100%;">
  <tr style="background-color: #fff">
    <td style="text-align: center" style="padding:10px 25px;">&lt;strong&gt;</td>
    <td>&lt;strong&gt;{{dimensions.0}}&lt;/strong&gt;</td>
    <td>&lt;strong&gt;{{measures.0}}&lt;/strong&gt;</td>
  </tr>
  {{#dimensionValues}}
    <tr>
      <td>&lt;qText&gt;</td>
      <td>&lt;qNum&gt;</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.

```html
<table width="100%">
  <tr>
    <td align="center" style="padding:10px 25px;">&lt;img src="https://qlik.imgix.net/us/-/media/images/qlik/global/qlik-logo-2x.png?h=94&w=308&la=en&hash=91b8028a0c9f991cf3864e421063d492988bd58575" alt="Qlik Logo" height="64">&lt;/img&gt;</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

```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;
  }
</style>
```
Example: Changes for right-to-left CSS

```html
<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

<table>
<thead>
<tr>
<th>Email type</th>
<th>Created email template</th>
<th>Triggered email template</th>
</tr>
</thead>
</table>

Qlik Alerting - Qlik Alerting, April 2020
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

Create a system alert

Do the following:

1. Click My 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. You can select one, multiple or all reload tasks. Use the search box to easily find your task as this list can be long. This list may also take a second or two to refresh if you have a large number of reload tasks as it is returning this list directly from Qlik Sense.

   If you select all the list will capture all tasks that exist at this point in time.

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 Process For > n Hours n Minutes** – status 1, 2, 3, 4, 5 – Identify when a task takes longer than a specified time to get an early warning of a possible failure or delay to reports being ready.

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.

   a. Select the recipients directly, and/or
   b. Select the user groups.
   c. Use the preview button to check on the list of users at that point in time (as users in groups may change over time).

   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.

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 and therefore be a licensed Qlik Alerting user. This means both Professional and Analyzer users in Qlik Sense can be assigned licenses in Qlik Alerting and will be able to sign up and use the mobile app.

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.
5 Mobile apps

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.
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 an config changes to manage the default values, or would like to make them, then follow the instructions below.

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
6  Qlik Sense extension

 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.

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.

   ![](image)

   *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.
- To setup Qlik Alerting to use a trusted certificate should remove this security exception, see Using trusted SSL certificates with Qlik Alerting (page 8) 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.