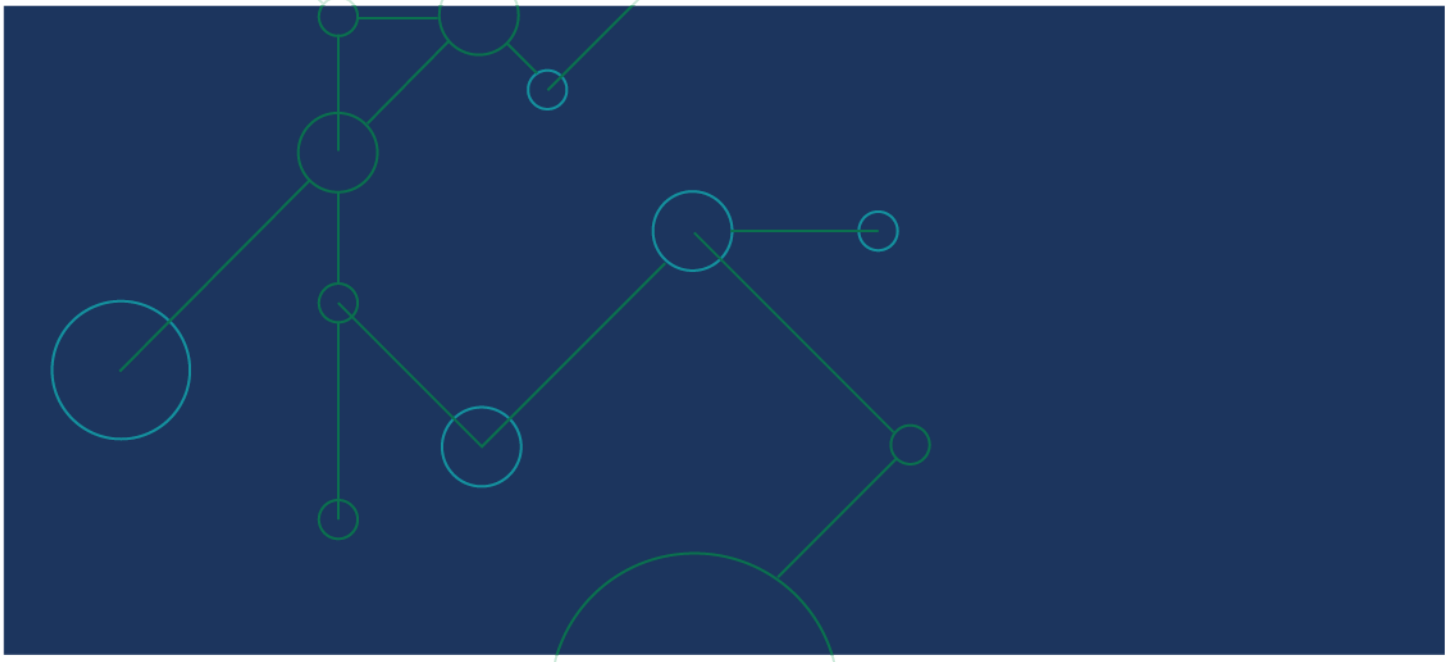
Technical Overview | August 2022

The Qlik Cloud® Platform



Contents

Qlik Cloud Overview

Qlik is a leader in data and analytics with a core mission to provide software that ensures organizations can work smarter and use data as a competitive edge. Qlik Cloud is a powerful end-to-end solution for data and analytics services. Our platform empowers curiosity-driven exploration offering everyone – at any skill level- the ability to use data to make transformative change for their organization.

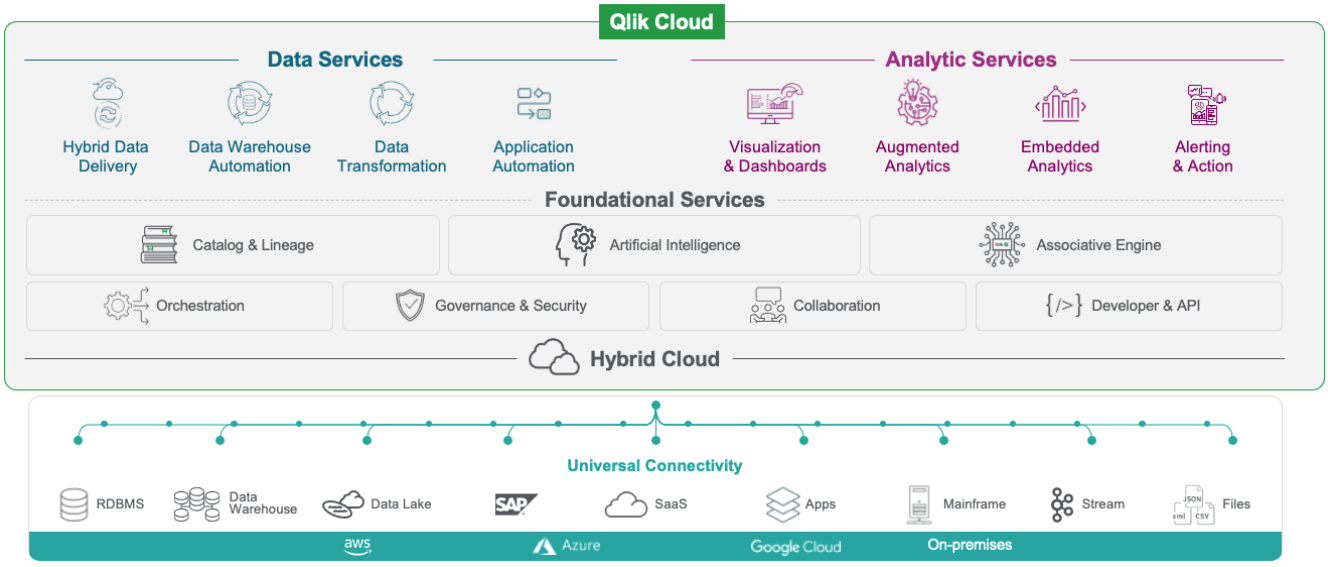
Through several Data focused services, the Qlik Cloud platform supports a full range of users and use-cases across the lifecycle from data integration to insight generation including Change Data Capture & Data Cataloging, Application Automation, self-service analytics & dashboards, conversational analytics, custom and embedded analytics and alerting.

This document highlights key aspects of the Qlik Cloud platform including architecture, security, governance, and reliability. It is designed to complement the technical documents for the Qlik solutions that run on the Qlik Cloud platform.

Architecture

Architecture Overview

All of Qlik's SaaS offerings and services, known collectively as the Qlik Active Intelligence Platform, run on the Qlik Cloud platform. The platform provides the underlying compute, storage security and governance features to provide services to our customers. The Qlik Active Intelligence Platform enables the creation of the analytics data pipeline. Powered by Qlik Cloud and a rich set of foundational services, it provides all the Data Services and Analytics Services you need to transform raw data into informed action



A Customer's instance of the Qlik Cloud platform is called a tenant and is logically separated from other tenants by using unique encryption keys. Access to the platform is controlled by the customer's configured Identity provider and any access to functions within the platform are based on the entitlements the customer has assigned across roles and users. A number of services are available on the Qlik Cloud platform:

- Analytics services – Provides a complete third-generation Analytics solution including Qlik Sense Enterprise SaaS
- Data Services – provide the ability to manage your data assets and provide change data capture to provide real-time access to your data as well as Application Automation to automate integrations between cloud applications.

Qlik Cloud Analytics Services

Incorporating our premier offering of analytics services, Qlik Sense sets the benchmark for third-generation analytics platforms, empowering everyone in your organization to make data-driven decisions. Built on our unique Associative Engine, it supports a full range of users and use-cases across the lifecycle from data to insight: self-service analytics, interactive dashboards, conversational analytics, custom and embedded analytics, mobile analytics, reporting and alerting. It augments and enhances human intuition with AI-powered insight suggestions, automation, and natural language interaction.

Qlik Cloud Data Services

Qlik Cloud data services is Qlik's hosted and managed data Integration Platform as a Service (iPaaS). Our vision is to provide a broad variety of data integration services aimed at helping you move from passive to active BI.

Hybrid Data Delivery is an enterprise grade integration service. The Hybrid Data Delivery service continuously streams data in near real-time from on-premises systems such as relational databases, mainframes, and SAP systems, to your Qlik Cloud tenant, or to your cloud data warehouse. QVDs created by the services are automatically updated whenever the source data changes and are ready for consumption by analytics apps without the need for scripting.

Qlik Application Automation is an integration platform to build integrations and automation flows between cloud applications. Closely integrated with the other Qlik Cloud services, Qlik Application Automation is able to build workflows between your cloud applications using a no-code approach by connecting data sources, applying conditions, calling webhooks, adding loops, scheduling runs, and setting up triggers. For example, a webhook in your CRM system could initial a reload or your sales performance Qlik Sense application.

Focus on your needs, not infrastructure

One of Qlik's goals is to reduce the cost and effort customers spend managing infrastructure and increasing the time they have for gaining insights from their data. When running on-premise deployments, customers need to factor in several costs which are not directly related to solving business problems such as:

- Infrastructure capital and operational costs
- Operating system management and software licensing
- Staffing costs for infrastructure administrators

With the Qlik Cloud platform, our customers can focus on solving business problems rather than administering their environment. This both reduces the total cost of ownership and the time it takes to get to actionable insights on your data – what Qlik refers to as *minutes to insight*.

Zero-Downtime Deployment for updates

Another significant effort involved with on-premises software deployments, and even many SaaS offerings, is the need for customers to test and certify product implementations, migrations and/or upgrades, which can include side by side SaaS environments. Instead of requiring such time intensive efforts, Qlik utilizes the concept of zero-downtime deployments for our Qlik Cloud platform infrastructure.

Qlik's zero downtime deployments for the Qlik Cloud platform allows a customer's tenant to be upgraded or modified without affecting customers' usage. Qlik's work on the platform is transparent to customers. For more information on Qlik's cloud native architecture and how zero-downtime deployments works, please see the section *Qlik and Cloud Native*.

Internationalization & Localization

The Qlik Cloud platform is a Unicode-enabled service and is compatible with data stored in any language. The user interface and supporting documentation are available in English, German, Spanish, French, Italian, Japanese, Dutch, Brazilian Portuguese, Russian, Swedish, Simplified Chinese, Polish, Turkish, Korean, and Traditional Chinese.

Users can define their locale in their profile settings. The user-defined app creation locale enables creators to inherit locale for script variables for formatting e.g. money format, decimal separators, month/day names.

Tenants, user roles & entitlements

Tenants

Each customer creates an instance of Qlik Sense Enterprise SaaS called a “tenant”. Subscriptions for Qlik Cloud include a single tenant, however, customers who require a multi-tenant environment may add additional tenants to their subscription A tenant can host either Analytics and Data services or any combination for which a customer has been entitled.

Roles & Entitlements

Access to features and entitlements within a tenant are controlled by the roles assigned to users and groups. Roles in combination with the user’s assigned entitlements will establish what the user(s) are able to do. User entitlements are based on the professional licenses agreed upon contractually for the tenant’s user types (ex. Company A purchased 1,000 Qlik Sense Professional licenses and 5,000 Qlik Sense Analyzer licenses).

Some roles are specific to the relevant service (e.g. analytics) and are not covered here. The platform wide roles are:

- **User** – This role is given to anyone who has access to a tenant. It is implied rather than specifically granted. It may be further broken-down entitlement (e.g. for Analytics; Professional, Analyzer, etc)

- **Developer** – The developer role is allowed more developer and creation type features such as the ability to create API keys. API keys are used for programmatic access to the tenant and for certain Qlik tools such as Qlik DataTransfer.

- **Tenant Admin** – The tenant admin role is provided full access to the management console for the management of all administrative aspects of a customer’s tenant. There is always a minimum of one tenant admin per tenant

- **Service Account Owner** - While not a role within the tenant, each tenant has a service account owner who controls initial setup, multi-factor authentication and billing. The service account owner is the initial tenant admin.

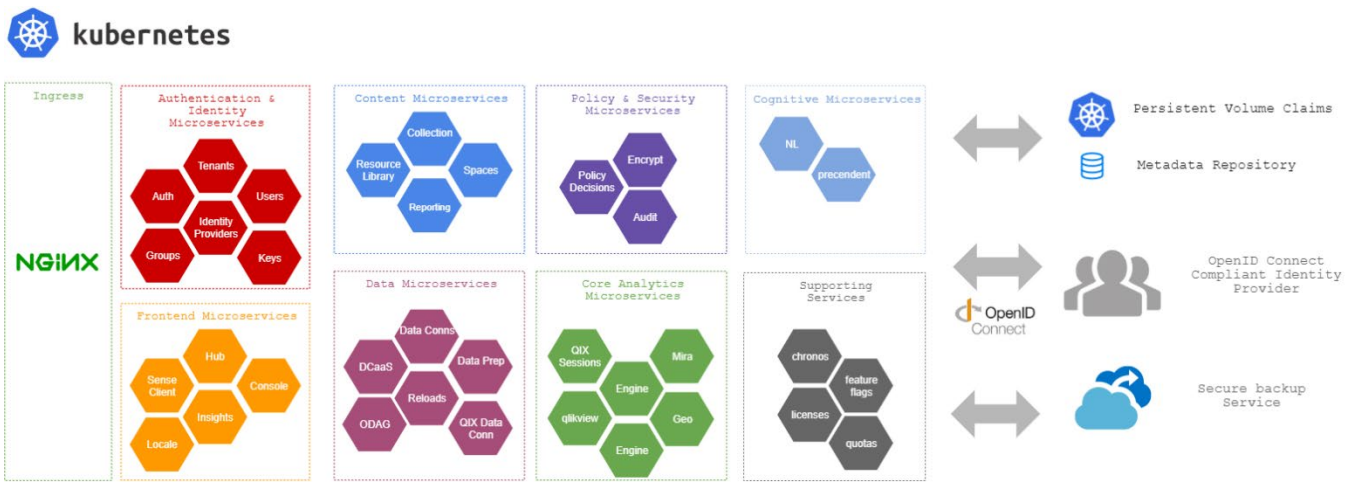
Qlik's cloud native platform and Kubernetes stack

To provide customers with a highly scalable, highly available cloud platform and service, Qlik could not simply just shift our on-premise products and move them to the cloud. Qlik Cloud is built upon a micro-services architecture, with the various components of the platform designed from the ground up to build a powerful, enterprise-ready cloud native solution. Qlik's container-based micro-services architecture allows each component to scale as needed rather than adding more servers as traditionally done on on-premises solutions.

A key feature of this platform is the ability to horizontally scale up as workloads increase and scale back down as they reduce; a key component used in the Qlik Cloud platform to ensure consistent performance for our customers - regardless of the number of users on the platform. Automated monitoring and the dynamic adjustment of resources allows all components of the platform to run with optimal resources whenever workloads change.

Another key aspect of cloud native apps is the concept of zero-downtime deployment. The Qlik Cloud platform has been designed to support zero-downtime deployment due to Qlik being able to upgrade the platform without outages.

Qlik utilizes Docker and Kubernetes to manage the scaling dependencies of the platform. A reference diagram for our Kubernetes deployment is shown below.



Some of the key technologies used in the Qlik Cloud platform are:

Kubernetes – Kubernetes provides automated container deployment, scaling, and management. For more information see *https://kubernetes.io/*

Docker – Docker provides containers where Qlik micro-services run. Containers are a standardized unit of software that allows developers to isolate their code from its environment, solving the “it works on my machine” headache. See *https://www.docker.com/why-docker*

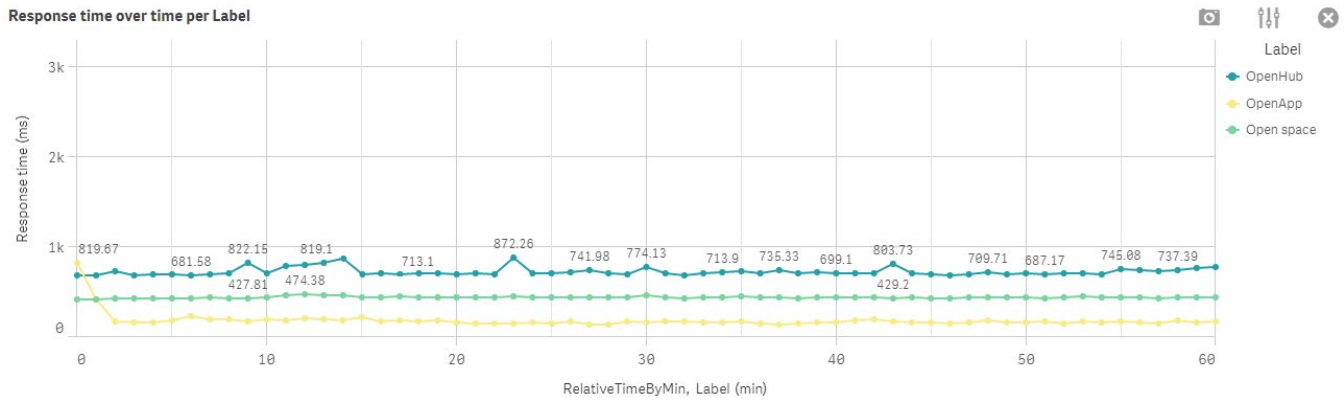
NGINX Ingress Controller – NGINX Ingress Controller provides the web interface and internal load balancing for Qlik Sense Enterprise SaaS tenants. NGINX is an HTTP and reverse proxy server, a load balancing server, and a generic TCP/UDP proxy server. See *https://www.nginx.com/products/nginx/kubernetes-ingress-controller/*

MongoDB - MongoDB is a cross-platform document-oriented database. It is used as the metadata repository within Qlik Sense Enterprise SaaS *https://www.mongodb.com/*

Predictable performance at scale

To ensure the best possible end user experience, Qlik continuously observes anonymized samples of the performance and scalability across individual tenants. Several different configurations are tested to make sure that the tenants can cope with the expected use cases and loads. Some of the parameters tested include:

- User ramp-up (that is, the number of users accessing the tenant per time unit)
- User type - e.g., consumer or creator
- Number of concurrent users
- Number and size of applications, data alerts, automation tasks, etc.
- Number, frequency and size of concurrent application and data loads



In this example, we tested 10,000 users per hour who were accessing 100 (out of 1600 available) different apps with an average data volume of 1.6 million rows. As shown above, response times for opening the Qlik Sense Hub, opening spaces, and opening individual apps were all under a second for all users.

A Sustainable architecture

Deploying physical hardware for IT systems create a significant carbon footprint for an organization. Data Centers account for nearly 1% of global electricity uses[1]. Companies moving resources to a public cloud provider will benefit somewhat from the efficiency gains from colocation and resource optimization provided. A recent survey conducted showed over half of the organizations using public cloud have an average CPU utilization of between 20-40%[2]; meaning that between 60-80% of the assigned resources are unused but still active. These servers continue to use significant amounts of power to operate. These same inefficiencies are true to on-premises deployed hardware, without the benefits from economies of scale a cloud provider has.

The Qlik Cloud platform provides significant benefits to organizations looking to reduce their carbon footprint further. The benefits come from three main areas:

Shared Services. The Qlik Cloud platform makes use of shared resources across a Qlik Cloud region, which would otherwise need to be duplicated for each customer deployment in a traditional client managed environment. We also benefit here from the regional nature of Qlik Cloud supporting multiple time zones. This means that peak times in one area are offset by the other time zones in that region. This significantly reduces resource usage further.

just in time resourcing

Qlik cloud uses intelligent queue management to minimize resources used at peak times. Instead of initiating all jobs at the exact time they are scheduled, at peak times Qlik Cloud may delay starting a job for a moment to avoid the need to provision excessive resources. This significantly reduces resource usage for application reloads, which make up approximately 1/3 of all resource usage in the Qlik Cloud platform.

Kubernetes auto-scaling. The Qlik Associative & cognitive engines respectively consist of the majority of resource usage in a Qlik Deployment. In a client managed environment, these resources need to be statically assigned, and sized for peak periods of the customers business cycle. This might mean that for large parts of the month they are significantly under-utilized. Qlik Cloud however is based on a Kubernetes architecture which auto-scales these resources to meet demand as needed and frees up these resources when demand eases.

[1] Source: https://www.iea.org/reports/data-centres-and-data-transmission-networks
[2] source: https://devops.com/granulate-issues-findings-from-state-of-cloud-computing-survey-highlighting-underutilization-of-it-infrastructure/

While Qlik does not capture detailed resource usage at a customer level all, of these factors combined lead to a significant reduction in resources used of a client-managed deployment of Qlik software.

Our cloud provider

The majority of services Qlik uses to run the Qlik Cloud platform are provided by Amazon Web Services (AWS). Amazon share Qlik's commitment to reducing their carbon footprint and working towards powering their operations with 100% renewable energy by 2025[3]. As of April 2022, Amazon was the world's leading corporate buyer of renewable energy.

As well as focusing on renewable energy, Amazon is also focused on minimizing the energy it uses. A study conducted by 451 Research show that AWS's infrastructure is 3.6 times more energy efficient than the median of U.S. enterprise data centers surveyed[4].

[3] Source: https://sustainability.aboutamazon.com/environment/the-cloud?energyType=true
[4] source: https://sustainability.aboutamazon.com/environment/the-cloud/cloud-efficiency

Standards & Compliance

Compliance & privacy

When moving workloads to a SaaS platform it is vital to know that data will be secure and that the service provider is following open and audited processes for security controls. Qlik Sense Enterprise SaaS has been built from a secure by design framework as a secure platform. Qlik also works with external parties to meet the applicable industry standards and/or that the best practice controls are in place.

ISO 27001

Qlik is ISO 27001 certified, meeting the international standards for implementing an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes the legal, physical, and technical controls involved in an organization's information risk management processes.

SOC 1 Type 2

Qlik Cloud is AICPA SSAE18 SOC 1 Type II Compliant. Qlik has successfully completed a SOC 1 Type 2 assessment which provides an evaluation on the suitability of the design and operating effectiveness of Qlik's internal controls, reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting.

SOC 2 – Type 2

Qlik Cloud is SOC 2 Type 2 compliant. SOC 2 is a rigorous examination by an independent accounting firm based on the AICPA Trust Services Principles and provides an evaluation of the design and operating effectiveness of Qlik's internal controls.

SOC 3

Building on SOC 2, Qlik has successfully completed a SOC 3 Assessment, which is a general use report attesting to Qlik's compliance to the AICPA Trust Services Principles.

TISAX

QlikTech Inc. is a TISAX participant and has completed a TISAX Assessment.

TISAX was developed by the Association of the German Automotive Industry (VDA) in partnership with an association of European automotive manufacturers, called the European Network Exchange (ENX). TISAX is a registered trademark and governed by ENX Association. The ENX Association governs TISAX on behalf of the German VDA. *https://enx.com/tisax*

HIPAA/HITRUST

Qlik supports customers with their HIPAA regulatory requirements via the HITRUST CSF certification. Qlik requires it mandatory for Customer Managed Keys (enhanced encryption) and a Business Associate Agreement (BAA) to be signed with Qlik prior to loading Personal Health Information into Qlik Cloud.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a United States federal statute governing the flow of healthcare information and provides federal regulatory standards that outline the lawful use and disclosure of protected health information in the United States.

HITRUST (Health Information Trust) is an independent testing organization. The HITRUST CSF (common security framework) is a framework that an organization can use to meet the legal requirements of HIPAA. HITRUST offers measurable criteria and objectives for applying appropriate administrative, technical, and physical safeguards that are also covered by HIPAA.

For the latest information on Qlik's external certifications and compliance, visit our Trust page.

Data Location

Any customer data that is inputted into the tenant, including any data within backup/recovery and disaster recovery systems, is maintained within the Qlik Cloud services region(s)chosen when creating their tenant. The customer controls whether data is transferred out of region, and none of the data the customer has inputted into the tenant is transferred out unless the customer elects to do so, for example by allowing access to a user in another region. Copies of backups are stored with a secondary provider within the same region.

Data privacy and GDPR

Qlik has built comprehensive internal processes to ensure Qlik's compliance with applicable privacy (including GDPR) requirements. Qlik is committed to protecting the data of Qlik customers and partners

and communicating in an open and transparent manner. Customers may store their personal data in Qlik Cloud, per our online terms. When doing so, Qlik would be classified as a Data Processor in terms of that data under relevant privacy laws, including the GDPR. For more information visit our *Privacy page*.

Data separation, storage & transport

Qlik Cloud is a multi-tenant platform. As a multi-tenant platform, it is critical that each customer's data is separated from others. Accordingly, each tenant has a uniquely generated set of encryption keys that Qlik or optionally the customer manages . Each tenant's keys are separate from keys Qlik uses to secure service to service communication. The following encryption is used within the Qlik cloud platform:

- In transit - TLS 1.2 encryption
- At rest - AES-256 encryption
- Within the platform – (upon authentication with the customer's designated IDP) uses signed JSON Web Tokens (JWTs) to ensure integrity, authenticity & non-repudiation

User access to the tenant is granted by the customer through the Identity Provider and permissions are controlled via the customer's administration portal.

Customer Managed keys

Qlik Cloud provides the ability for customers to use their own master keys from external Key Management Services to encrypt their data stored on Qlik Cloud. This capability will allow customers to encrypt their per tenant data with their own key. This capability Supports customers who have additional encryption requirements due to regulatory, data privacy, or data sovereignty requirements. Currently Qlik supports the AWS Key management System. Other key management systems will be evaluated in the future.

Content Deletion

"Content" is the customer-provided data and other information within the Qlik Cloud tenant. The creation and removal of content that resides in the tenant is controlled solely by the customer and any content can be deleted by the customer at any time. Backups are removed after a period of time in accordance with Qlik's internal data retention policies.

Customer-provided data is stored as encrypted QVD or QVF files in the underlying Kubernetes storage solution used by Qlik Cloud. When a customer deletes an App in Qlik Cloud, the service deletes the file

on the underlying Kubernetes storage solution. Qlik Cloud relies on the Kubernetes storage solution file system to execute the delete in the underlying block storage.

Qlik leverages both Amazon AWS and Google for backups to maintain copies of Content for 30 days before that Content is deleted from the supporting file systems. Qlik Cloud leverages Google Cloud Platform backups with Remote Sync and Amazon Simple Storage Service (S3) to copy Content for backup purposes.

Qlik Cloud platform security

Monitored for security 24/7

Qlik Cloud is monitored by Qlik's Site Reliability Engineering (SRE) team. All security logs are centrally processed by the SRE team, and all incidents are handled in accordance with Qlik's incident response program.

Security best practices

In order to ensure a strong, secure foundation, Qlik shares security responsibilities with AWS. These cloud computing services are used by Qlik for internal purposes as well as Qlik's clients for their own cloud deployments. See the section on Compliance & Privacy for more information.

Qlik Cloud relies on cloud infrastructure for secure physical access, redundant (fault tolerant) infrastructure, and scalability. Our cloud partner's network design and monitoring mitigate common types of network security issues such as Distributed Denial of Service (DDoS), Man in the Middle (MITM), IP Spoofing, Port Scanning, or packet sniffing.

Qlik's approach to security builds on our cloud partner's layers of security. Qlik has network and endpoint monitoring controls in place, including intrusion detection and process monitoring. At the Web layer, Qlik utilizes a web application firewall to detect and prevent attacks. Access to Qlik Cloud leverages multi-factor authentication and role-based access control.

Qlik performs regular vulnerability testing both at the network and endpoint level. Vulnerability remediation is incorporated into the continuous deployment methodology in Qlik Cloud. These tests are conducted by an independent 3rd party and include but are not limited to:

- OWASP top 10
- SANS top 20

Approach to vulnerability management

Qlik's software development process incorporates a Secure By Design approach to software delivery. A significant contributor to that process is our approach to vulnerability management. Qlik maintains a modern vulnerability management remediation policy that includes:

- Leveraging vulnerability severity ratings based on industry standard Common Vulnerability Scoring System (CVSS) to judge the severity of security issues. (Scale of 1-10 with 10 being most severe)
- A policy related to vulnerabilities identified during development and the release of software with known vulnerabilities including remediation windows
- A policy related to vulnerabilities identified in Qlik Cloud platform updates including remediation windows
- Customer notification policies for vulnerabilities
- Third party software security and remediation policy
- Tooling and processes covering Threat Modeling, Dynamic and Static Code Scanning, Penetration Testing, and Third Party Software components.

Security & Governance

Authentication and authorization

Identity and access management

Identity Providers (IDP) have become a standard way to manage authentication and authorization information for organizations. Qlik supports integration with a variety of Identity Providers by supporting the Open ID Connect protocol (OIDC).

Protocol based - OpenID Connect (OIDC) has become the de facto standard for single sign-on and identity provision on the Internet. OIDC has been designed to work in cloud and provides a solution for both user and machine authentication.

Control the credentials - When using an Identity Provider with Qlik, Qlik does not know customer logins and passwords. The login process is managed by customer's Identity Provider and the customer decides what information to provide to Qlik Sense Enterprise SaaS. This information could be a short name or code that does not identity the individual. Also, Qlik Sense Enterprise SaaS can utilize Identity Provider groups for controlling access permissions.

Control access – If a user's access in the customer's Identity Provider is removed or changed, the user will automatically be prevented from accessing Qlik Sense Enterprise SaaS or the corresponding changes are automatically applied.

Through OIDC support, the Qlik Cloud platform supports all the major identity providers including Okta, Auth0, Azure AD & ADFS.

Qlik Account

For customers that do not have an Identity Provider available externally or require an in-product solution that does not need to be managed, Qlik provides Qlik Account as a bundled Identity Provider option available as part of the Qlik Cloud platform at no extra cost. This allows customers to invite users by email to sign up for a Qlik Account which can then be used to log into the the Qlik Cloud platform.

While Qlik Account simplifies implementation for some customers, it requires a separate user name and password for Qlik Sense Enterprise SaaS. It is possible for customers to change from Qlik Account to their own Identity Provider if they desire to do so.

Multi-factor authentication

The Qlik Cloud platform supports multi-factor authentication for tenant administrators using Qlik Account or from the customer's identity solution. Qlik multi-factor authentication can also be configured for all users using Qlik Account or the customer's IDP.

Secure By Design – How Qlik Builds a Secure Platform

Qlik incorporates security during the software development life cycle by adhering to the Qlik Security Model, which has been developed by the Qlik Software Security Office. The Qlik Security Model is an internal process that ensures that all software development is done with a security focus. The model is a result of sourcing best practices from several existing well renowned secure software development processes and adapting them to fit the needs of Qlik. The model has five phases that span the entire lifecycle of software development:

Analysis & Design: This phase of the processes includes system and feature level threat modeling. When a product is designed, the team considers each feature and determines the possible threats for this feature. Countermeasures are put in place to mitigate each threat.

Develop: Qlik uses industry-leading static code analysis tools to identify issues on both the code specific to new features and the end-to-end code. After deployment, the static code analysis tool runs the report on a regular basis. The automated reports are supplemented with manual security testing processes. If manual verification confirms a security issue exists, then it is addressed prior to deployment.

Assemble: Test cases are created from a security perspective and executed during the development process. Testing includes system level, feature level, penetration level and fuzzing. Test cases consider the end-to-end new product release to identify any security issues within the new product. Specific tests are conducted on code that contains the new features within the product. An independent third-party security company regularly audits the products through penetration testing.

Deploy: The Software Security Office is involved in the deployment phase through its vulnerability management process. Working with external security companies, customers, and partners to identify vulnerabilities within the deployed code, the team will assess any reported vulnerability and determine appropriate action.

Evolve: All results from the activities that are a part of the security model are reviewed by the Software Security Office. The goal is to identify areas of improvements, and adjustments are made to the model accordingly

Governance

Monitor activity in the tenant

The Qlik Cloud platform's management console contains several tools to assist with the governance of a customer's Qlik Cloud tenant. The event viewer shows what user and system-initiated activities have taken place and provides an audit trail for major activities such as user logins, apps created, apps exported, reloading of apps and apps deleted. Within a Qlik Cloud platform tenant, activity is also made available to the customer via APIs. This activity can be downloaded to the customer's security information and event management solution.

Integrate into existing governance solutions

As well as documenting the audit trail though the Qlik Cloud platform's management console, The Qlik Cloud platform provides Application Programmable Interfaces that allow viewing (but not modifying or removing) tenant activity. Customers can integrate The Qlik Cloud tenant's audit trail into an existing security monitoring system or build a new audit application within Qlik Sense Enterprise SaaS via the APIs. For more information, read about our *Qlik Sense audit service* in our help documentation.

API governance policy

Qlik's API strategy follows an API governance policy to communicate additions, changes, and deprecations to Qlik's API portfolio. Qlik R&D follows API guidelines for marking API stability, standardizing references on specifications (e.g. OpenAPI for ReST APIs), and handling API deprecations.

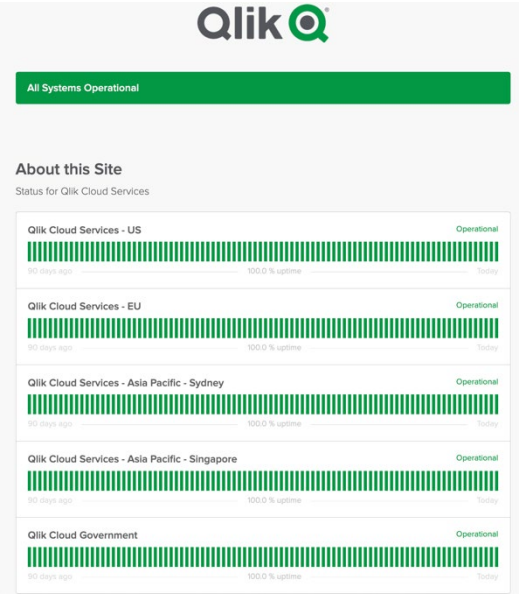
The main objective of the API strategy is to provide open and transparent guidance to customers and partners who rely upon Qlik APIs to extend the platform.

Qlik R&D has developed a patent-pending API governance framework that collects information from commits made by the development teams to help make APIs discoverable and maintainable. This helps the team deliver enhancements to the platform continuously and ensures API consumers outside the organization are accessing components of the highest caliber. For more information regarding Qlik's API governance policy please visit *https://qlik.dev/basics/api-governance*.

Reliability

Open and transparent

Qlik makes data on uptime and incidents publicly available, so customers and prospective customers can see and understand the current status and reliability of the Qlik Cloud platform on which Qlik's SaaS offerings run. This information is available at *https://status.qlikcloud.com/*.



Customers can see the overall uptime of the platform as well as look into specific issues that have occurred to see details on the impact.

Global presence

Support multiple regions throughout the world

Upon the creation of a Qlik Cloud tenant, customers choose the region in which their tenant is based: United States, Ireland, Australia or Singapore. Customers can therefore select a region to suit their business requirements.

Adaptable high availability infrastructure

The Qlik Cloud platform runs on AWS' mature, highly available, fault-tolerant infrastructure stack and deployed across multiple data centers in multiple regions. Further, the platform is built using a microservice based architecture running on Kubernetes and is designed from the ground up around scalability and fault tolerance. This allows the platform to instantly adapt to any changes and patches, minimizing any potential downtime for the platform.

Disaster recovery / backup and recovery

Qlik's SRE team performs disaster recovery tests regularly. As part of these tests, the team builds an entire new Qlik Cloud region. The disaster recovery test is only deemed successful once the new region is brought up, 100% of the replicated data is recovered and tenants are fully utilizable from the last backup/replication period.

Data and platform information on Qlik Cloud related to customer tenant configuration and metadata, is stored in a manner that allows for replication to secondary regions. Customer data files are backed up daily.

Site Reliability Engineering

Spotlight – The Site Reliability Engineering process at Qlik

Based on Google's Service Reliability Hierarchy, Qlik's SRE team focuses on the following areas:

Monitoring - Our SRE team ensures every service delivered to production can communicate to Qlik how its performing, so that our SRE team is aware of problems as they may arise.

Incident Response – The SRE team prepares the appropriate response plan for the problem. The various options available to the SRE team are documented in service specific playbooks and highlight the best way to deal with a service that is operating in a less than optimal manner.

Postmortems and Root Cause Analysis - When the SRE team is alerted that a service has been degraded in production, the SRE team need to ensure the underlying problem is fixed as quickly as possible. A postmortem is a documented record of an incident, its impact, the actions taken to minimize or resolve it, the root cause, and the follow up actions to prevent the incident from reoccurring. In many cases, one of the outcomes of the postmortem process is to add an additional automated test to the continuous delivery pipeline to ensure that functional issues do not reoccur.

Capacity Planning – The SRE team participates in the ongoing designs of new services and the impacts that new features / modifications may have on existing services. These include:

- how services scale up to handle increased traffic load
- how services scale down to seamlessly accommodate reduced capacity
- what are the optimal size and performance characteristics of infrastructure
- which services require auto-scaling

Development - The SRE team continually innovates around performance and scalability of the platform. Some examples include:

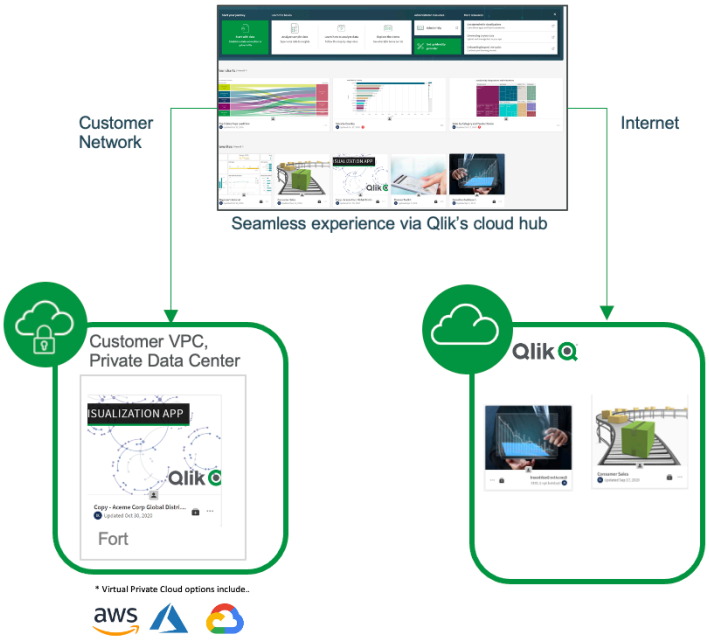
- Continual enhancement of measurement and monitoring tools
- Continual improvements to and expansions of automation capabilities

Measurement – Internal metrics (such as service level indicators and service level objectives) are used by the SRE team to continuously monitor the performance of the environment

Qlik Forts for Hybrid deployments

Overview

In some cases, it's not possible to host all data on Qlik's cloud platform. Some regions have regulations that mandate certain data may not leave that region. In other cases, corporate polices or latency concerns may lead customers to keep their data on-premises. This usually only applies to a subset of a customer's data; yet, in these cases customers have been forced to choose between a resource-intensive, client-managed solution or a complex multi-cloud solution. Qlik Forts are a new hybrid capability that enable organizations to easily maintain data location requirements as part of a SaaS deployment.



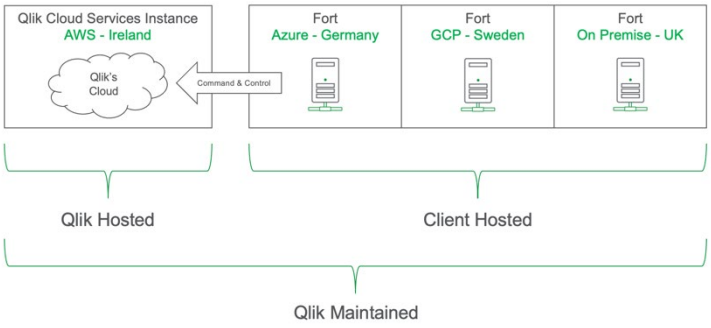
A Qlik Fort is a hybrid service that securely extends Qlik Sense SaaS capabilities near your data landscape, regardless of location whether on premises or in a public cloud. Qlik Forts enable businesses to benefit from the convenience of SaaS as well as the flexibility of a hybrid deployment that supports data security, privacy preferences, and investments in existing data infrastructures. With Qlik Forts, organizations can deploy Qlik Sense SaaS next to their on-premises data, virtually in any region or cloud. Qlik Forts works with Qlik Cloud as a single solution. Users get a seamless experience and single point of entry, so access to analytics and insights can easily scale across the organization. Forts currently supports Qlik Sense applications with other content support on the Forts roadmap.

Qlik has identified key use-cases we see as suitable and Qlik Forts provides a solution where a customer has sensitive data in some parts of their business that cannot be moved to Qlik Cloud due to regulations or its business preferences. By deploying a Fort near this data, it is possible to meet this

need without having to forgo a SaaS solution for other data. Qlik Forts also provides a solution for multinational organizations with global users that need to restrict usage of some apps to certain locations and users. A Qlik Fort can be deployed where the data and users are located to maintain data locality requirements and reduce latency and data movement costs. Apps that are used globally would still be deployed to Qlik Cloud.

Architecture

Qlik Forts are provided as a virtual machine image which can run in customers' virtualization platforms on-premises or on Azure, AWS, or GCP Platforms. Forts are accessed via Qlik Sense Enterprise SaaS, which handles the authentication and authorization. When a user opens an application hosted in a Fort, the user is securely redirected to that Fort and the application is opened there. The redirection happens from the user's browser and the Fort validates the user has been authenticated by Qlik Sense Enterprise SaaS which prevents users accessing the fort directly. When using Qlik Forts to connect to your private data sources, Forts does not send the data from those sources or the credentials for those data sources to any Qlik-hosted or 3rd party services.



Qlik Forts are based on the same cloud-native, containerized architecture as Qlik Sense Enterprise SaaS. The complexity of managing the Fort is handled by Qlik and we ensure the Fort is always up to date with the latest updates and patches. A service built into each Fort checks with Qlik regularly to pick up these updates and applies them in the background. No incoming connections from the internet are required from Qlik Cloud to a Fort. The Fort regularly contacts Qlik Cloud to exchange metadata about the Fort (such as its availability, if an application has been reloaded, etc.).

Customers can choose to deploy one or many Forts. Each Fort operates independently, and easily configurable in different physical locations around the world. When adding a Fort into a Customer's Qlik Sense Enterprise SaaS tenant, a customer assigns one or more spaces to the Fort. Any content created in those spaces is created in the Fort.

When a user selects an app in a space designated to a Fort, it triggers a browser redirect on the client. Therefore, it is possible for the Fort to sit inside a customer's private network and not be accessible from outside. Users need to on the private network to access apps located in Forts.

Security

Security was one of the key design goals for Qlik Forts. No ingress is required from Qlik Cloud to the Fort, avoiding the need to open up firewall ports. The Fort does not even require a public IP address assuming the customer does not want to open access to the Fort outside of their network. All data connection details are stored within the Fort and not sent to Qlik. When loading from a data source in the same private network as the Fort, all access is from the Fort, not Qlik Cloud. If a customer creates QVDs from an application running in a Fort, those QVDs are kept local to a Fort and cannot be accessed from outside that Fort. Within the fort, all service-to-service communication is authenticated.

Integrating and embedding with the Qlik Cloud Platform

Many of Qlik's Systems Integrators, OEMs, partners, and customers wish to be build solutions and portals for their internal and/or external customers leveraging Qlik Analytics or Data Integration technologies. Qlik allows a flexible set of deployment options to support this, based on the core concept of 1 Qlik Cloud tenant per external customer organization. This could mean deploying a single tenant for an enterprise, or multiple tenants for Qlik partners who themselves provide embedding of Qlik technology to their end customers.

Irrespective of deployment size, Qlik provides APIs to support platform orchestration and embedding to meet your organization's needs. Qlik supports several approaches and techniques to support this, based on one or many Qlik Cloud tenants. Qlik Cloud is built on an API first philosophy, so it is easy to implement and manage multiple tenants as part of a wider solution. Qlik Cloud's APIs allow provisioning, configuration, and hydration of Qlik Cloud tenants to serve automated deployment pipelines alongside your software and customer lifecycles.

Working with multiple Qlik Cloud tenants

Qlik Cloud is a shared platform with each customer having one or more tenants of their own. These tenants are not integrated with each other or a sub-tenant of a larger tenant. They are connected through the license as well as the integration the customer builds. This means the tenants can operate independently and are secured with unique encryptions keys ensuring end customers of the solution's data in protected from other end customers.

Deployment of tenants and the content of tenants can be fully automated using the Qlik Cloud APIs.

Tenant creation & deletion

Tenants can be created using Qlik Cloud's REST APIs, or with our developer tooling (such as Qlik-cli or the platform SDK).. When using the CLI or API methods, oAuth credentials provided through My Qlik can be used to authenticate with Qlik Cloud. By connecting to the registration endpoint for your region (e.g. *https://register.eu.qlikcloud.com/*) you can create tenants, e.g.

```
qlik tenant create --licenseKey "my-key" –json
```

Tenant deletion is not currently available through a public API however this is currently a roadmap item.

Tenant Hydration

Hydration is the process of populating a new tenant with the spaces, applications and configuration needed to meet the use-cases needed. It is possible to configure your tenant using APIs. This includes configuring the identity provider, spaces, connections and apps. It is possible to configure most aspects of a tenant required to provide users a ready to consume tenant without any manual intervention.

Tenant administration

When administering many tenants, it is inefficient to switch between many management consoles for administrative tasks. Using Qlik's APIs or the Qlik cli, it is possible to perform administrative tasks such as license and permissions management as well as monitoring tasks such as viewing audit information and integrating these tasks into a multiple tenant workflow. Qlik's monitoring applications are currently being updated to support multi-tenant environments.

Tenant administration features are designed to be used by the managing organization only. End-users should not be given direct access to admin roles or the management console as user license assignments will be visible for the whole license rather than just that tenant. If access to administrative features is to be provided to end customers, this should be implemented in the end solution with appropriate restrictions in place.

Architecting a multiple tenant solution

When working with multiple tenants, there are different architectures that can be used for the solution. The two main architectures are covered here.

Source to Target Architecture

In this model data connections are set up in a source tenant and applications reloads all occur there. Applications are then distributed to the target tenants once reloaded. This provides the advantage of centralizing integration with data sources, scheduling and testing in one location. The main downside of this approach as it increases the latency of application reloads so is not suitable for all use-cases.

Satellite architecture

In this model data connections, reloads and schedules are managed in the target tenants used by the end customers of the solution. The advantage of this approach is it can provide much lower latency in terms of reloads and in cases where the solution provides one tenant per customer, provides a physical

separation of customer data. The disadvantage of this approach is it increases the administrative load (although automation can minimize this).

Coordinated orchestration architecture

In this model, the orchestration tenant will connect to data sources via data gateway, which then fills S3 buckets with data processed from on-premise data sources. It then triggers the reloads of apps in the target tenants, which each reload their apps directly from the S3 buckets fed from the orchestration tenant.

Building a solution on the Qlik Cloud platform

Building a solution based on the Qlik Cloud platform may involve several techniques including:

- web solutions
    - Rendering visualizations from the Qlik Sense client on websites
    - Connect to the Qlik Associative Engine and create custom analytics
    - Create custom administration pages to for example trigger reloads
- Embedding analytics
- iFrames

Building a solution is an advance topic and the details are beyond the scope of this document. For more details on this, including an in-depth exploration of the alternatives with examples, see the *Qlik Developer Portal*.

Authentication approaches

API keys

An API key is a token representing a user in the Qlik Sense Enterprise tenant. Anyone may interact with the platform programmatically using the API key. The token contains the user context, respecting the access control privileges the user has in the tenant. API keys use cases include qlik-cli (command line interface), making requests through scripts, or a machine-to-machine backend solution(s).

When using OAuth clients generated via My Qlik (relevant in multiple tenant environments), API keys generated via these clients will run as a tenant administrator, known as a “bot user”.

Interactive Login

Typically, use of an interactive identity provider (and therefore interactive login) is not recommended for embedding use cases. This is because it’s difficult to ensure that the user isn’t prompted multiple times to log in – for example, once when they access the page containing the embedded content, and again when the embedded content starts to load.

However, if you wish to use this method to authenticate users in web apps, there are REST endpoints which help you to evaluate if the browser has an active Qlik Sense SaaS session. If no session exists, then use a redirect to the tenant's sign-in URL.

Web apps embedding Qlik Sense objects or data, also known as mashups in our client-managed offerings, require a web integration ID in the tenant's configuration. Web integration IDs are a security feature of Qlik Sense Enterprise SaaS for handling Cross-Origin Resource Sharing (CORS) of embedded Qlik Sense Enterprise SaaS content.

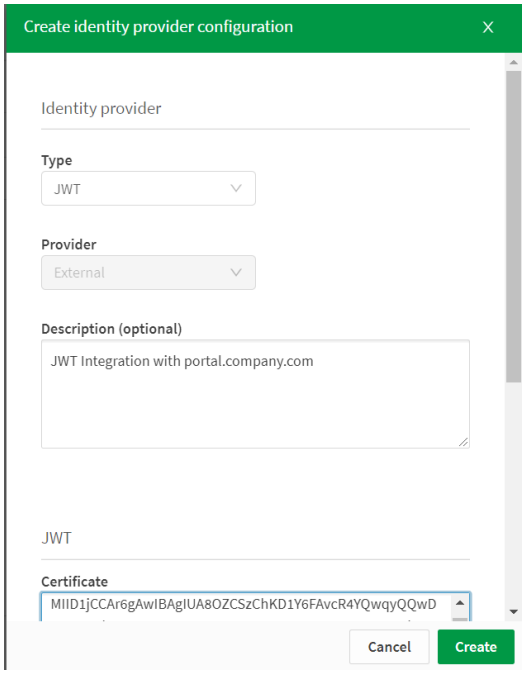
In addition, web apps with content embedded in them require a cross-site request forgery (CSRF) token supplied in the URI referencing Qlik Sense Enterprise SaaS APIs and the Qlik Associative Engine.

OAuth 2.0

OAuth is a standard security protocol for authorization and delegation. It allows third party applications to access API resources without disclosing the end-user credentials.

Qlik Sense SaaS supports OAuth 2.0 Authorization Code flow. The OAuth client can obtain an authorization code and exchange it with an access token that can be used to access Qlik Sense SaaS APIs.

JSON Web Tokens (JWT)



JSON Web Tokens, digitally signed, are commonly referred to as a “JWT.” A JWT is a standard for transmitting information between software applications in the form of a JSON object, verified and trusted using a public / private key pair. JWTs two primary use cases are authorization and information exchange. Qlik Sense Enterprise SaaS reads JWTs from external identity providers during the authentication phase. Qlik Sense Enterprise SaaS creates an internal JWT post authentication for use during a session.

The external JWT authorization option in Qlik Sense Enterprise SaaS enables client applications to directly send a custom JWT, bypassing the interactive sign-in to the Qlik tenant. The user is then authorized to access Qlik Sense Enterprise SaaS. The JWT capability enables customers to provide seamless integrations between their applications and Qlik Sense Enterprise SaaS.

Applications connecting to Qlik Sense Enterprise SaaS with JWTs require the same web integration ID and cross-site request forgery prevention as all integrations within the platform.

Tools and resources

Developer Portal

The Qlik Developer portal (*Qlik.dev*) - is a central location for developers to find the information they need to develop with Qlik products including Qlik Sense Enterprise SaaS and featuring developer documentation, API references, tutorials, and more

Qlik-cli

Qlik-cli is a command line interface for automating management activities in Qlik Sense Enterprise SaaS. This is available at https://qlik.dev/libraries-and-tools/qlik-cli.

Qlik's Platform SDK

Qlik's Platform SDK (software development kit) is a python module that allows developers to leverage the APIs of the Qlik Cloud platform from the comfort of python. The SDK provides access to both the REST and RPC clients to access all the APIs available for the Qlik Cloud Platform.

For more information on the Platform SDK see: *https://pypi.org/project/qlik-sdk/*

Summary

The Qlik Cloud platform is designed to provide our customers with a platform to securely move their analytic and data workloads to the cloud. Built on Cloud Native technologies, Qlik Cloud has been designed to automatically scale to meet the workloads of the modern enterprise and provides Qlik customers a platform that can consolidate their data and analytics solutions in a single hub.

With a global presence and a strong focus on security and availability, the Qlik Cloud platform provides a safe and secure platform for our global customers. With the ability to choose where the tenant is hosted, customers can ensure their data is close to their location and in a geography that meets their business requirements.

Qlik understands that our customers often want to integrate and embed their analytics and visualizations into their own portals and systems. Therefore, Qlik has and continues to invest in providing integration approaches and supported open sources libraries and tools to make this easier for our customers. With comprehensive APIs and Qlik's developer portal providing resources and examples, Qlik is committed to assisting our customers make Qlik Cloud a part of their own solutions.

For existing Qlik Client-Managed customers, Qlik Cloud has the capability to facilitate the transition to SaaS. Customers can choose to continue reloading apps on- premises, move some apps to Qlik Sense Enterprise SaaS or use Qlik Data integration tools to access their data sources on-premises while moving consumption to the cloud. Qlik Data Services provide a near real-time solution for bringing your data into the Qlik Cloud platform. Qlik Application Automation allows you to integrate your Qlik Cloud based solutions with 3rd party cloud-based solutions. Integrated identity providers and flexible deployment and subscription options make this easy to manage and minimizes costs during the transition.

About Qlik

Qlik's vision is a data-literate world, where everyone can use data and analytics to improve decision-making and solve their most challenging problems. Qlik offers real-time data integration and analytics solutions, powered by Qlik Cloud, to close the gaps between data, insights and action. By transforming data into Active Intelligence, businesses can drive better decisions, improve revenue and profitability, and optimize customer relationships. Qlik serves more than 38,000 active customers in over 100 countries.

qlik.com