QLIK EVALUATION GUIDES

The Qlik Cloud® Platform

Published: March 2024

Contents

1 Qlik Cloud overview

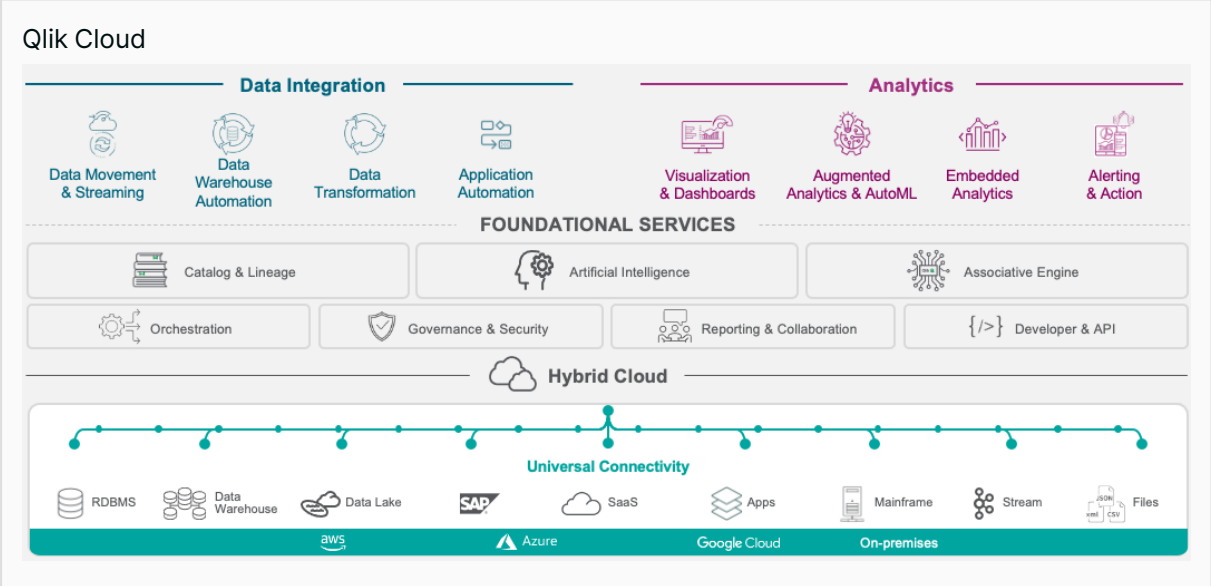
Qlik is a leader in data and analytics with a core mission to provide solutions that ensure organizations can work smarter and use data as a competitive edge. Qlik Cloud is a powerful end-to-end solution for data and analytics services. Our platform empowers curiosity-driven exploration offering everyone – 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. These services include change data capture, transformation, data cataloging, application automation, self-service analytics and 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.

1.1 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 delivers 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 integration 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. It 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 is based on the entitlements the customer has assigned across roles and users. A number of services are available on the Qlik Cloud platform:

- Analytics – provides a complete third-generation analytics solution including Qlik Sense Enterprise SaaS
- Data Integration – provides the ability to manage your data assets and utilize change data capture to provide real-time access to your data, as well as application automation to automate integrations between cloud applications.

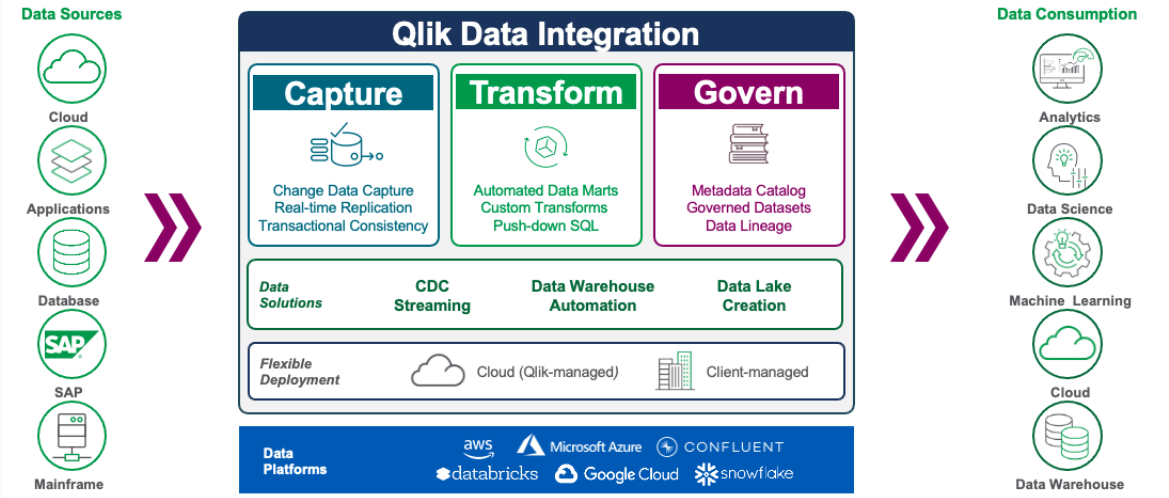
Qlik Cloud Analytics

Incorporating our premier offering Qlik Sense, Qlik Cloud Analytics 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 Integration

Qlik Cloud Data Integration 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. Qlik Cloud Data Integration is architected for real-time data capture, transformation, and analytics-ready data delivery leveraging a variety of methods in our unique change data capture approach.

Qlik Cloud Data Integration



Real-time data movement

Replicate data from on-premises or cloud sources into Qlik Cloud and other leading cloud data platforms. Automatically and continuously ingest data without the need for job scheduling or scripting. Your data is updated without manual intervention to drive insights and actions of important business moments.

Data transformation

Quickly turn raw transaction records into consumption-ready data via auto-generated, push-down SQL. Our no-code interface helps you create reusable transformation pipelines that intelligently conform data to dimensional models or custom formats.

Qlik Application Automation

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 initialize a reload of your sales performance Qlik Sense application.

2 Qlik Cloud platform

The Qlik Cloud platform is designed to provide our customers with a platform to securely move their analytics and data workloads to the cloud. Built on cloud-native technologies, Qlik Cloud automatically scales to meet the workloads of the modern enterprise and provides Qlik customers a platform to consolidate their data and analytics solutions in a single hub.

With a global presence and a strong focus on security and availability, Qlik Cloud provides a safe and secure platform for our global customers. With the ability to choose where their 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 continues to invest in providing integration approaches and supported open-source 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 help 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 third party cloud-based solutions. Integrated identity providers and flexible deployment and subscription options make this easy to manage and minimize costs during the transition.

2.1 Qlik Cloud Government

Qlik Cloud Government is an implementation of Qlik Cloud which is only available for the U.S. public sector. Qlik Cloud Government has differences from Qlik's commercial Qlik Cloud offering due to the security protocols required by the US public sector (**FedRAMP** Moderate Impact Level (IL) and Department of Defense (DoD) IL 2).

Qlik Cloud Government has also achieved **StateRAMP** (State Risk and Authorization Management Program) Moderate Authorized status. StateRAMP simplifies security for U.S. state, local, and higher education organizations by providing a standardized approach to security authorizations for cloud service providers.

In addition to **FedRAMP** and **StateRAMP**, Qlik Cloud Government also holds the following certifications:

- **Department of Defense** : Qlik Cloud Government has achieved the Department of Defense (DoD) IL 2.

- **TX-RAMP** – Level 2 - supporting confidential agency data determined to be at the moderate or high impact level.
- **ITAR** - Qlik Cloud Government supports compliance with the United States International Traffic in Arms Regulations(ITAR) around the handling of software and technical data controlled on the United States Munitions List (USML).
- **DISA** - Qlik Cloud Government has successfully met the standards for Impact Level (IL) 2 set by DISA (The Defense Information Systems Agency) a U.S. Government Organization that has created and maintains security guidelines for computer systems or networks connected to the DoD (Department of Defense).

Wherever possible, Qlik keeps both platform offerings in sync for product features and capabilities. For details on the differences between Qlik Cloud Government and our other Qlik Cloud offerings, see Qlik Cloud Government Overview .

2.2 Platform architecture

Qlik Cloud is a single-solution modern data stack with capabilities to move enterprise data from on-premises and cloud sources to Qlik's hosted self-service analytics solutions and other analytics environments. The foundation for these solutions is the Qlik Cloud platform Architecture. Qlik Cloud uses a cloud-native approach Based on CNCF's approach and related technologies to provide efficient and highly available services to our customers.

Focus on your needs, not infrastructure

Qlik wants to reduce the cost and effort that customers spend managing infrastructure and increase 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 reduces both 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 upgrades, which can include side-by-side SaaS environments. Instead of requiring such time-intensive efforts, Qlik uses the concept of zero-downtime deployments for our Qlik Cloud platform infrastructure.

Qlik's zero downtime deployments for the Qlik Cloud platform allow 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, see the *Qlik's cloud-native platform and Kubernetes stack* section below.

Internationalization and localization

The Qlik Cloud platform is a Unicode-enabled service that 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 such as money format, decimal separators, and month/day names.

Tenants, user roles and entitlements

Tenants

Each customer creates an instance of Qlik Cloud 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 Qlik Cloud Analytics and Data Integration, or any combination to which a customer has been entitled.

Roles and entitlements

Access to features and entitlements within a tenant is controlled by the roles assigned to users and groups. Roles, in combination with the user's assigned entitlement, establish what the user can do.

User entitlements are based on the user types available and they are assigned in the subscription the customer has purchased. This could be analyzer or professional in user-based subscriptions (for example, Company A purchased 1,000 Qlik Sense professional licenses and 5,000 Qlik Sense analyzer licenses), or basic or full in capacity-based subscriptions.

Some roles are specific to the relevant service (such as Analytics) and are not covered here. The platform-wide roles are:

- **User** – The user role is given to anyone who has access to a tenant. It is implied rather than specifically granted. It may be further broken downn by entitlement (for Analytics; professional, analyzer, and so on).
- **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 has 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 decrease; 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 applications 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 uses Docker and Kubernetes to manage the scaling dependencies of the platform. A reference diagram for our Kubernetes deployment is shown below.

Kubernetes deployment reference diagram

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 Kubernetes.

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 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 NGINX Ingress Controller.

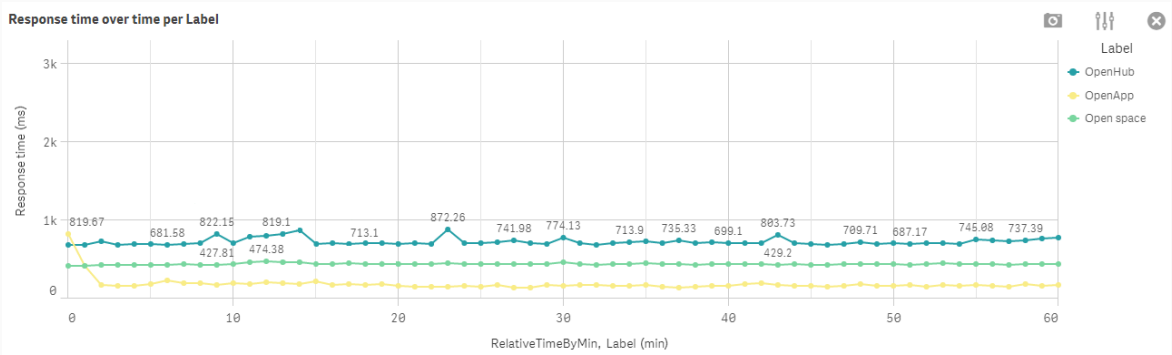
MongoDB - MongoDB is a cross-platform document-oriented database. It is used as the metadata repository within Qlik Sense Enterprise SaaS. See MongoDB.

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, such as 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

Response time in Qlik Sense hub



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 (see Data Centers and Data Transmission Networks). 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% (see Granulate Issues Findings from State of Cloud Computing Survey Highlighting Underutilization of IT Infrastructure); meaning that 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 for 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 and 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 customer's 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.

While Qlik does not capture detailed resource usage at a customer level, all of these factors combine to lead to a significant reduction in resources used for 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 (see Sustainability in the Cloud). 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 the AWS infrastructure is 3.6 times more energy efficient than the median of U.S. enterprise data centers surveyed.

2.3 Standards and compliance

Compliance and 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 Cloud has been built from a secure-by-design framework as a secure platform. Qlik also works with external parties to meet the applicable industry and Government standards and/or to ensure that best practice controls are in place.

Qlik Cloud government, our dedicated offering for the U.S. Public sector, is covered by a different set of standards as required by the government sector. Details on these are covered here: Qlik Cloud Government Compliance.

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

ISO: the International Organization for Standardization

ISO is an independent international organization committed to creating standards based on best practice. ISO bring together experts to understand and document better and safer ways to operate and publicized these though standards. Organizations can undertake certification to show their adherence to ISO standards.

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.

ISO 27017:2015

Qlik meets the standards of ISO 27017 an information management security specification for information management systems (ISMS) covering cloud security controls for cloud service providers. ISO 27017 is an extension to the ISO 27001 ISMS framework.

ISO 27018:2019

Qlik meets the standards of ISO 27018, an information management security specification for information management systems (ISMS) covering cloud privacy requirements and security controls for cloud service providers. ISO 27018 is an extension to the ISO 27001 ISMS framework

SOC: The System and Organization Controls framework

The System and Organization Controls (SOC) framework was created by AICPA, the American Institute of Certified Public Accountants. SOC is a standard for controls that protects information. Implementing SOC frameworks involve two phases:

- Implementing and maintaining SOC controls (SOC Compliance)
- External review process to verify and document and organization's compliance (SOC Certification)

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. It 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.

Global and industry specific standards and compliance

HIPAA/HITRUST

Qlik supports customers with their HIPAA regulatory requirements via the HITRUST CSF certification. Qlik requires it as mandatory for Customer Managed Keys (enhanced encryption) to be configured 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. Qlik has successfully completed a SOC2 Type 2 + HITRUST attestation for HIPAA compliance.

IRAP

IRAP is an assessment process required by Australian Government bodies wishing to use Cloud services. Qlik has been assessed by an independent Information Security Registered Assessors Program (IRAP) assessor against the Australian Government Information Security Manual (ISM) Controls produced by the Australian Signals Directorate (ASD). The assessment examined the security controls of Qlik Cloud and provides assurance that Qlik has met the controls required by the ASD.

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.

General Data Protection Regulation (GDPR) & Data privacy

The General Data Protection Regulation ((EU) 2016/679, abbreviated GDPR) is a European Union regulation on information privacy. 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, see our Privacy page.

Data separation, storage, and transport

Qlik Cloud is a multi-tenant platform. As a multi-tenant platform, it is critical that each customer's data is separated from the others. Accordingly, each tenant has a uniquely generated set of encryption keys that Qlik manages, or optionally that the customer manages (known as customer managed keys — see the following section). Each tenant's keys are separate from the keys that 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, and 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.

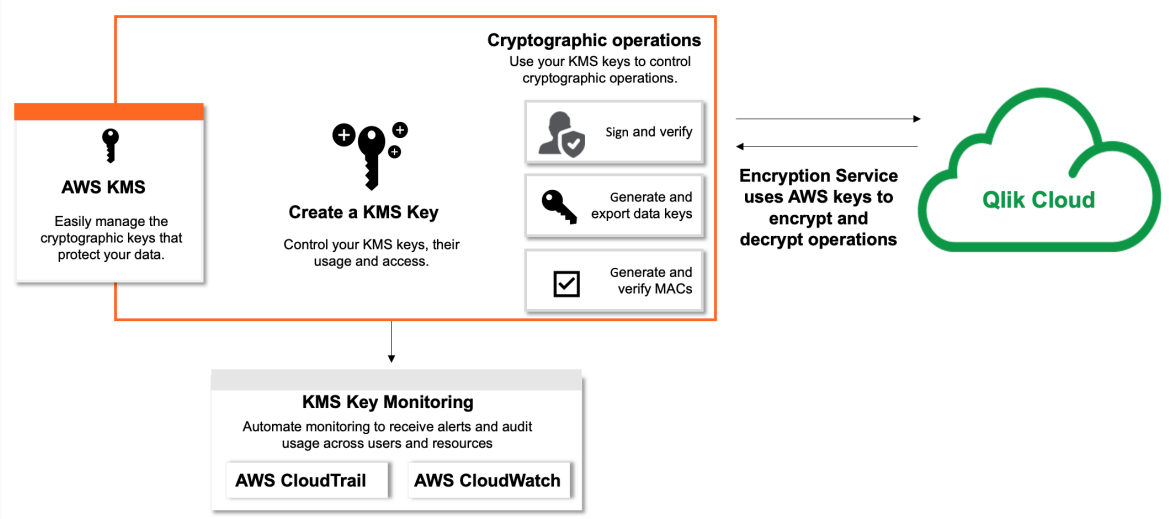
Data location

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.

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 that is stored on Qlik Cloud. This capability allows 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.

How Qlik Cloud uses Customer managed keys with AWS



Customer-managed keys provide the ability to move existing Qlik Cloud tenants from Qlik-managed to customer-managed keys, and also to revert from customer-managed keys to Qlik-managed Keys, or to switch between AWS KMS keys. Qlik also supports managing customer-managed keys through Qlik App Automation for both standard and OEM Qlik Cloud tenants. For customers who wish to manage this using their own solution, Qlik provides public APIs for key management.

The Customer Managed Keys feature supports Multi-Region Keys to provide Disaster Recovery in the event of failover of a region. This requires a multi-region key to be used as the customer managed key. The AWS Key management service does not support changing a single region key to a multi-region key, however Qlik Cloud does support switching keys, so this would be required should you wish to migrate to multi-region keys.

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 simple storage remote sync and Amazon 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. For more information, see the section above on Compliance and privacy.

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, and 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 uses 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 third 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

2.4 Security and 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 OpenID 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 the customer's identity provider, and the customer decides what information to provide to Qlik Cloud. This information could be a short name or code that does not identify the individual. Also, Qlik Cloud can use 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 and 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. This bundled identity provider option available as part of the Qlik Cloud platform at no extra cost. It 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 lifecycle 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, and 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 and 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 that is 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, see Reviewing system events 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.

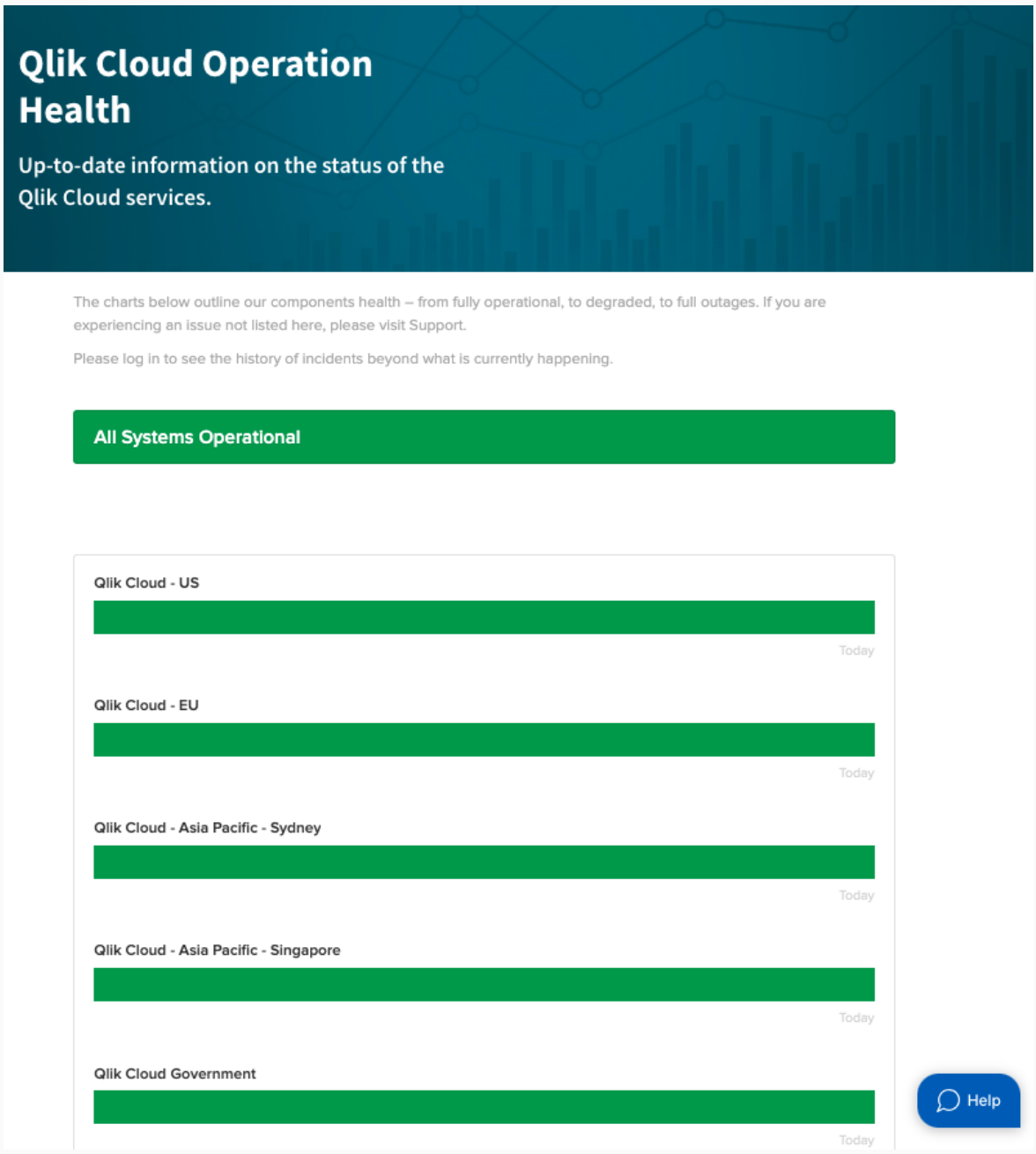
Qlik R&D has developed a patent-pending API governance framework that collects information from commits made by the development teams to help make APIs discoverable and maintainable. This helps the team deliver enhancements to the platform continuously and ensures API consumers outside the organization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

2.5 Reliability

Open and transparent

Qlik makes data on uptime and incidents publicly available so that 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 Qlik Cloud Operational Health.

Qlik Cloud status



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

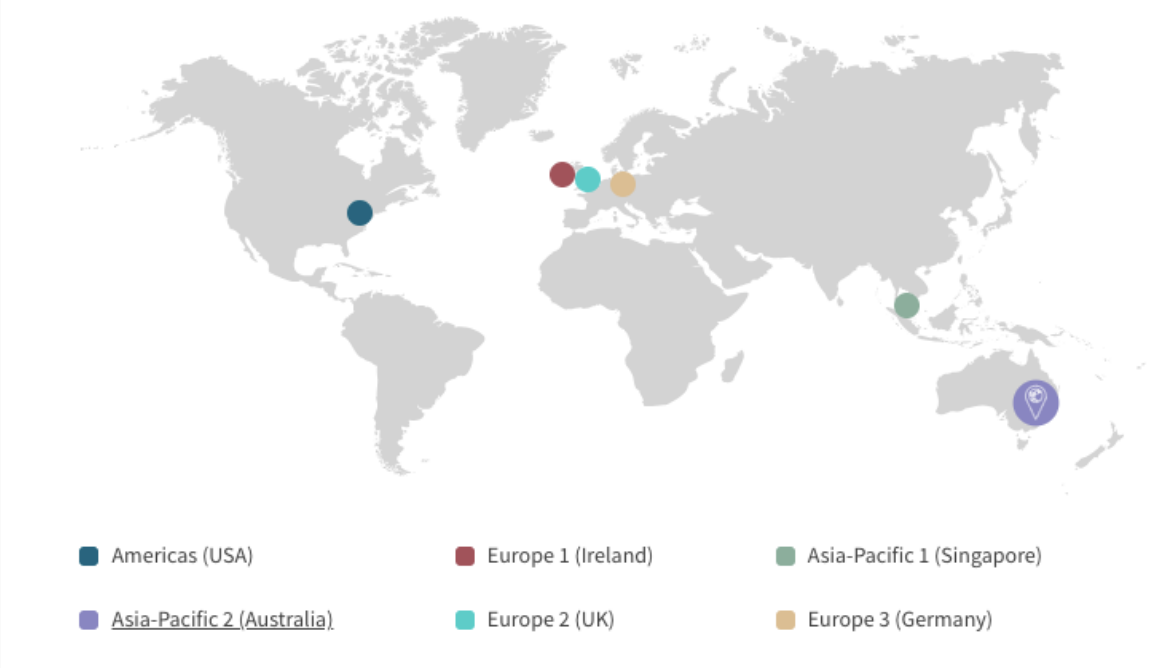
Support multiple regions throughout the world

Upon the creation of a Qlik Cloud tenant, customers choose the region in which their tenant is based:

- Australia
- Frankfurt
- Ireland
- London
- Singapore
- United States

Customers can therefore select a region to suit their business requirements. Qlik regularly reviews customer demand for new regions. Qlik plans to introduce a new region in 2024 in Tokyo.

Qlik Cloud Regions



Adaptable high-availability infrastructure

The Qlik Cloud platform runs on AWS' mature, highly available, fault-tolerant infrastructure stack, and is 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 that every service delivered to production can communicate to Qlik about how it is 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 needs to ensure that 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 and 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

2.6 Integrating and embedding

Many of Qlik's systems integrators, OEMs, partners, and customers want to build solutions and portals for their internal and/or external customers that leverage Qlik Cloud Analytics or Qlik Cloud Data Integration technologies. Qlik allows a flexible set of deployment options to support this, based on the core concept of one 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.

Qlik is currently designing ways for OEM partners to change the branding and customize certain styling elements to enable Qlik Cloud to look and feel like the OEM solution, without having to build unique user interfaces.

The initial release allows OEMs to use an API to set a custom logo, as well as remove the Qlik brand from several high-visibility areas across the product. This eliminates the need for many OEMs to recreate UI elements of Qlik Cloud to build their solution.

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 encryption 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 and 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, for example:

```
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 needed use cases. 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.

QlikWorld behind the curtain - how Qlik is able to create tenants on-demand for attendees

Qlik holds our annual conference, QlikWorld, each year. Thousands of customers and partners attend to learn more about Qlik product innovations and to get hands-on experience in our technical workshops.

In the years before Qlik Cloud, providing environments for QlikWorld attendees to learn about our products was an extremely resource- and time-intensive process. In just a few days, Qlik's Global Enablement team would set up hundreds of laptops with virtual machines for attendees to use. These would be loaded with VM images for all the workshops offered and would need to be reset after each session. This process meant we needed to schedule costly downtime between each session, and a team of people would need to be on hand the minute a session ended to have it ready for the next session.

However QlikWorld 2023 was very different thanks to our platform as a service investments in our APIs, along with connectors for tenant provisioning in Qlik Application Automation. When an attendee registered for a workshop, an automation would run, creating a tenant for them, configuring it, and pre-populating it with any required applications, data files, and other content used in the workshop. This would all happen in less than 15 seconds after the user had registered, with no manual intervention and the user receiving a link to the new tenant immediately in their inbox. Similar techniques were used for workshops where a shared tenant was used.

Qlik was able to save approximately 80% of the staffing costs and 25% of the time required compared to how this was done at the previous in-person QlikWorld. As an added bonus, attendees no longer lost access to their workshop environment the minute the session ended, allowing them to revisit the workshop environment later if desired.

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 is that 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 that 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 that 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 is difficult to ensure that the user is not 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.

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. Qlik Sense SaaS supports 2 Authorization grant types:

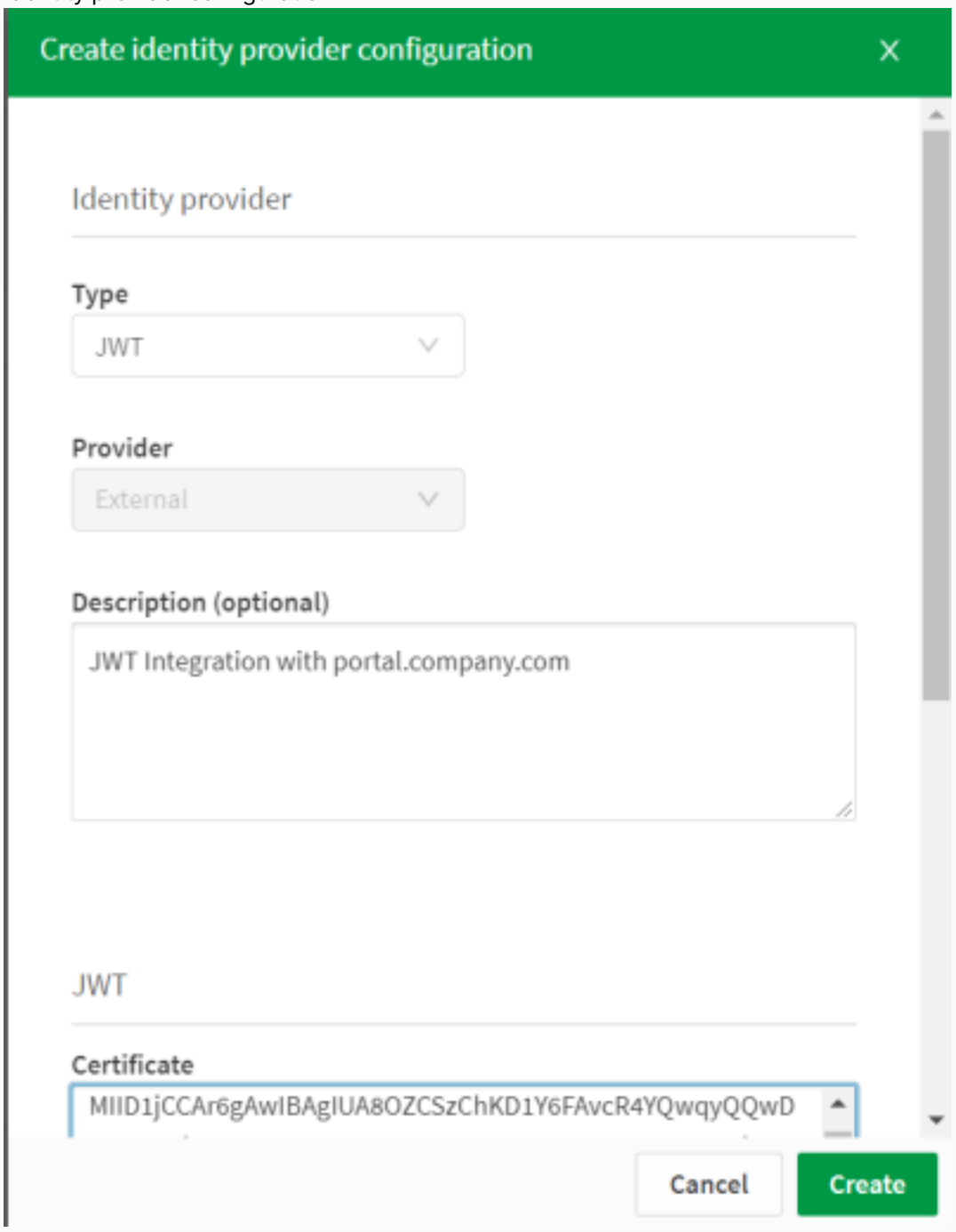
- Authorization code flow
- Authorization Code Flow with Proof Key for Code Exchange (PKCE).

OAuth scopes provide a way to limit the amount of access that is granted to OAuth client apps. For example, an access token issued to a client app may be granted full access to protected resources, or just read access. Each scope grants a different level of access.

For more information on OAuth, see Creating and managing OAuth clients.

JSON web tokens (JWT)

Identity provider configuration



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. The two primary use cases for JWTs 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) 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. For more information in the Qlik Developer Portal, see 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: Qlik SDK.

3 About Qlik Evaluation Guides

The content provided herein is provided for informational purposes. Due to Qlik Cloud's continuous release process, at times the content herein may differ from actual platform functionality. Please refer to Qlik Cloud Help for the product documentation for Qlik Cloud.

Any statement about future plans or intentions for the Qlik Cloud platform contained herein is not a commitment to deliver those features or functionalities, as the development, release, and timing of any features or functionality described for Qlik's products remain at our sole discretion.

For additional information regarding Qlik Cloud, please see Qlik Cloud or contact your Qlik representative.

3.1 Document history

This content has been developed to assist customers and prospective customers to understand and evaluate the Qlik Cloud platform and its related services. Traditionally this content has been published in document format only as a PDF; however, it is now primarily published as web content with PDF files available if required.

Over its history, this content has been known by the following names:

- Qlik Technical papers
- Qlik White papers
- Qlik Technical overview

This documentation supersedes the above documents.

3.2 Changelog

The PDF documents are generated from the evaluation guides at Qlik Help . The changelog for this evaluation guide is shown below.

Changelog — Qlik Cloud platform evaluation guide

February 2024

February updates

- updates to certifications including IRAP
- Customer managed keys DR

October 2023

October updates

- Customer-managed keys in *Standards and compliance*
- StateRamp in *Qlik Cloud platform*

- Minor updates

August 2023

August updates

- New cloud regions added

July 2023

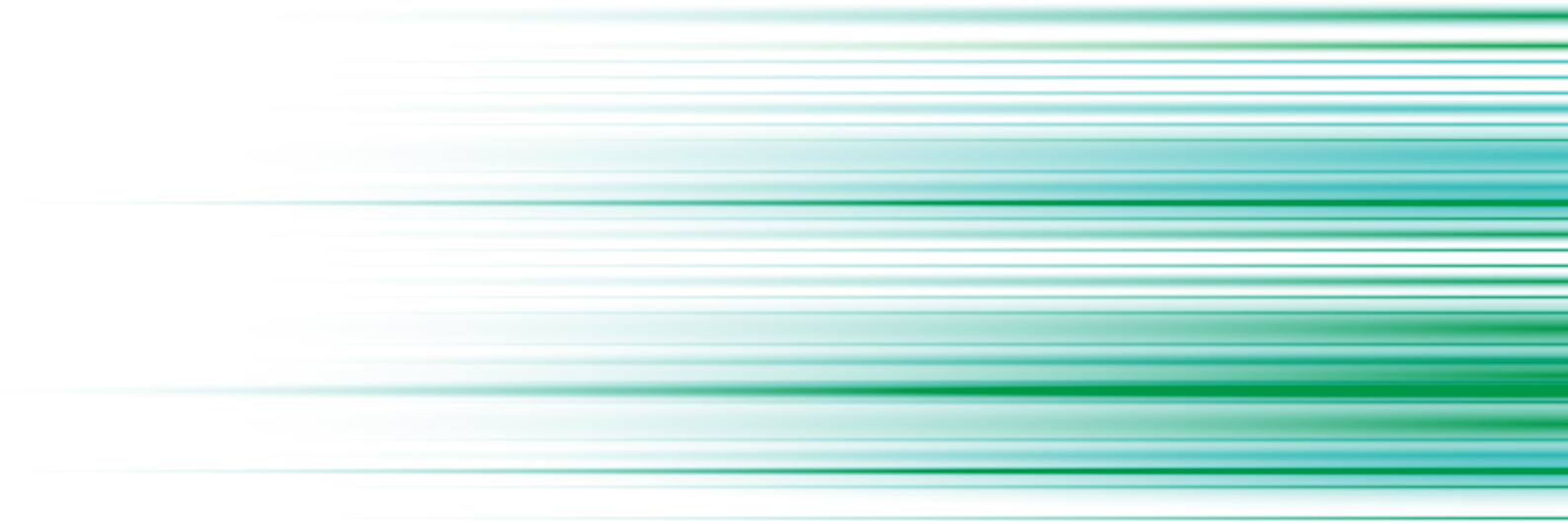
Initial release to help.qlik.com

Migration from static PDF to online content with PDF files auto-generated

Feb 2023

Final legacy version

Last version published as a static document only.



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. Our cloud-based Qlik Active Intelligence Platform® delivers end-to-end, real-time data integration and analytics cloud solutions 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 does business in more than 100 countries and serves over 38,000 active customers around the world.

qlik.com