

Qlik Sense® Enterprise SaaS - Government (US)

Contents

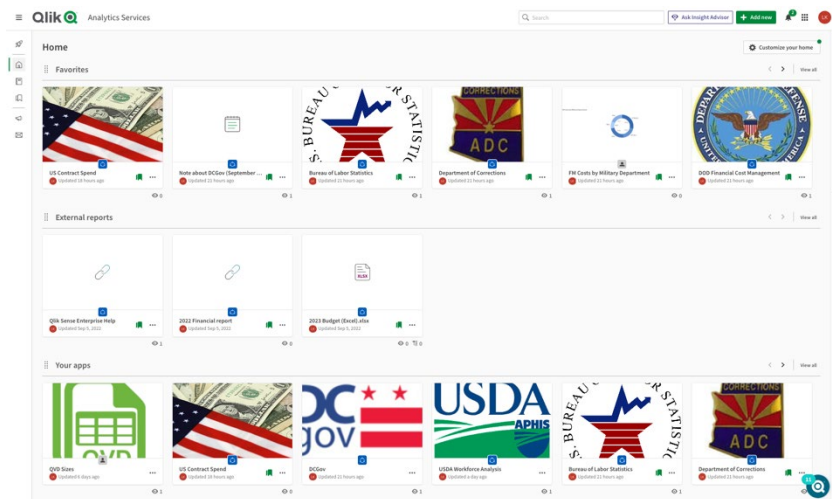
- Qlik Sense Enterprise SaaS - Government (US) Overview 2
 - A single platform for analytics 2
 - Associative, in-memory apps 2
 - Notifications and Alerts 4
 - Conversational analytics 4
 - Tenants, user roles & entitlements 5
 - Enterprise data at scale 7
 - Focus on analytics, not infrastructure 8
 - Integrating on-premises data with Qlik Sense Enterprise SaaS – Government (US) 10
 - Internationalization & Localization 11
- Reliability 12
 - Open and transparent 12
 - Adaptable high availability infrastructure 12
 - Site Reliability Engineering 13
- Security and Governance Model 13
 - Authentication and authorization 13
 - Governance 14
- Standards-Based Security & Compliance 16
 - Compliance & privacy 16
 - Qlik Sense Enterprise SaaS platform security 18
- Architecture 20
 - Qlik’s cloud native platform and Kubernetes stack 20
 - Predictable performance at scale 21
- Integrating and Expanding Qlik Sense Enterprise SaaS – Government (US) 22
 - Integration approaches 22
 - API governance policy 24
 - Qlik Reporting Service 25
 - Qlik Open Source 25
 - Tools and resources 25
- Summary 26

Qlik Sense Enterprise SaaS - Government (US) Overview

As part of Qlik’s cloud first strategy we have developed our own cloud service, Qlik Sense Enterprise SaaS - Government (US), which will serve multiple editions to support our customers like for Qlik Sense Enterprise SaaS - (US) which has been designed for the U.S. Public Sector. We manage cloud editions of our product portfolio to deliver them to customers as software-as-a-service (SaaS) offerings. Qlik Sense Enterprise SaaS is our premium cloud solution and gives organizations world-class analytics without the complexities of installing and managing their own deployment. Qlik has introduced *Qlik Sense Enterprise SaaS - Government (US)*, a version of Qlik Cloud and Qlik Sense Enterprise SaaS, focused on the U.S. Public Sector market. Qlik Sense Enterprise SaaS - Government (US) runs on our Qlik Cloud Government platform.

A single platform for analytics

The microservice-based architecture behind Qlik Sense Enterprise SaaS – Government (US) allows the hosting of Qlik Sense applications (apps) in a customer’s Qlik Sense Enterprise SaaS Government (US) tenant. In addition to hosting Qlik Sense apps, Qlik Sense Enterprise SaaS Government – (US) provides the ability to add links to other types of reports and assets such as documentation, providing a single portal for your users to consume all your analytics and reporting assets.



Associative, in-memory apps

Qlik Sense couples in-memory data storage technology with an Associative Engine that lets you analyze and freely navigate data intuitively. In its second generation, the proven Qlik Associative Engine allows users to easily explore data and create visualizations based on data from multiple data sources simultaneously. These sources range from Excel® and Access® to databases such as Oracle® and SQL Server to big data sources such as Databricks® and Redshift®.

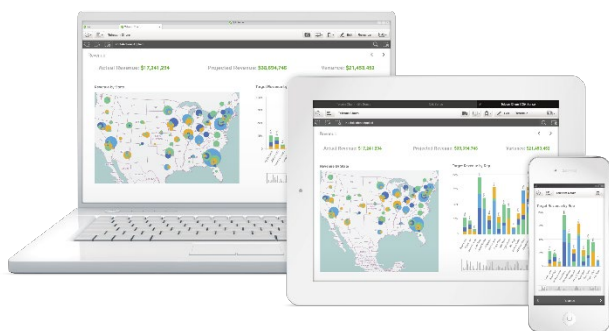
Qlik Sense uses columnar, in-memory storage. Unique entries are only stored once in-memory, and

relationships among data elements are represented as pointers. This allows for significant data compression, more data in RAM, and faster response times for your users.

In some big data scenarios, data should remain at the source, which is why Qlik uses a built-in technique called On-Demand Application Generation. Data sources can be queried based on your users' selections, yet still provide an associative experience to your user. Qlik's Dynamic Views feature expands this capability further for the biggest data sources available.

User Interfaces

Access to the Qlik Sense Enterprise SaaS – Government (US) environment is through a zero-footprint web browser interface (known as the Qlik Sense Hub). The Qlik Sense web browser interface makes all aspects of development, drag-and-drop content creation, and consumption possible. Qlik Sense features a responsive design methodology to automatically display and resize visualizations with the appropriate layout and information to fit the device — whether it is a browser on a laptop or desktop, tablet, or smartphone. Built with current standards of HTML5, CSS3, JavaScript®, and web sockets, Qlik Sense enables you to build



and consume apps on any device.

In addition to the web-based interface, Qlik Sense supports conversational analytics which integrates with major chat platforms such as Slack and MS Teams and data alerting capabilities to allow users to subscribe to and be notified of key changes to their data.

THE ASSOCIATIVE DIFFERENCE®

Relational databases and queries were designed in the 1980s for transactional systems, not modern analytics. Query-based tools leave data behind and limit your users to restricted linear exploration, resulting in blind spots and lost opportunities.

Qlik Sense runs on the unique Qlik Associative Engine, enabling users of all skill levels to explore their data freely without limitations. The Qlik Associative Engine brings together unlimited combinations of data — both big and small — without leaving any data behind. It offers unprecedented freedom of exploration through interactive selection and search, instantly recalculating all analytics and revealing associations to your user in green (selected), white (associated), and gray (unrelated). By keeping all visualizations in context together and retaining both associated and unrelated values in the analysis, the Qlik Associative Engine helps your users discover hidden insights that query-based tools would miss.

The Qlik Associative Engine is purpose-built for highly scalable, dynamic calculation and association on massive data volumes for large numbers of users. This unique technology is our primary advantage, with more than 25 years of innovation and investment.

Notifications and Alerts

Notification capabilities allow users to configure Qlik Sense Enterprise SaaS – Government (US) system-based events. These events include status of application reloads, and your users' status in Spaces. Users have control over their notification subscriptions, managing which channel (e-mail or web) they would like to receive them, as well as for opting to unsubscribe at any time.

Alerting capabilities allow users to configure alerts based on customer-defined business criteria relating to data in an application. Alerts are triggered to users during an application reload and can be set up to use a combination of dimensions and measures within an application. Alerts will apply the criteria solely to the data the user has permissions to access and may be delivered to the configured channel of choice (web or e-mail). All users of Qlik Sense Enterprise SaaS-Government (US) can create personal alerts. Users with a Professional role assignment can add other users as recipients to their alerts, provided that all recipients must have access to the application to receive the alert. Qlik Sense Enterprise SaaS-Government (US) allows users to track alert history. This information is protected by FIPS compliant encryption and securely stored within Qlik Cloud Government.

All notifications and alerts can be configured to send through these channels:

Email. Emails are sent using customer provided SMTP settings defined in the Administration Console and utilizing the Transport Layer Security (TLS) security settings from the customer's SMTP service. The same SMTP setting is shared across all features integrated with e-mail capabilities in Qlik Sense Enterprise SaaS – Government (US).

Web. Web notifications and alerts are delivered to the Qlik Sense web client browser over a secure HTTPS connection using FIPS compliant TLS 1.2 with signed digital certificates.

Conversational analytics

Insight Advisor Chat is a chat-based interface for conversational analytics. Insight Advisor Chat lets you search for insights in any app you can access. Insight Advisor Chat returns apps that contain relevant results. When you select an app, Insight Advisor Chat provides a text response or visualization. Insight Advisor Chat may suggest further analyses for your query that create different visualizations. You can also ask follow-up queries, such as in a particular country or for a particular year, and Insight Advisor Chat provides new results.

You can phrase your search queries for facts, comparisons, and rankings. Facts are statements such as *What are my open obligation of funds* or *Show expenses over time for FY2021*. You can ask for a

comparison by adding vs or compare to your query. For example, “*Compare budget to expenses over time*”. You can ask for rankings by adding top to your query. For example, “*Show me top 10 agencies by spend for FY2021*”.

Insight Advisor can analyze an app to see how fields are used to create charts. The Qlik Precedents Service examines the use of data fields and master items in charts. This teaches precedents for making aggregations, dimensions, and measures for the data model of the app. In unpublished apps, Insights can use precedents learned from published apps and from user feedback in the app.

The Qlik Sense Natural Language (NL) Query API lets you embed augmented analytics capabilities into your own software such as integration into an existing chatbot platform. You can use the NL Query API to query a selected app or multiple apps. The API responds with text or a visualization.

Tenants, user roles & entitlements

Tenants

Each customer creates an instance of Qlik Sense Enterprise SaaS Government (US) called a “tenant”. Each Qlik Sense Enterprise SaaS Government (US) customer has their own tenant. Multiple tenants are not available.

Roles

There are many roles that users can have in Qlik Sense Enterprise SaaS-Government (US) tenants. The roles combined with the entitlements establish what access users have within a tenant. Roles can be assigned to groups or to individual users.

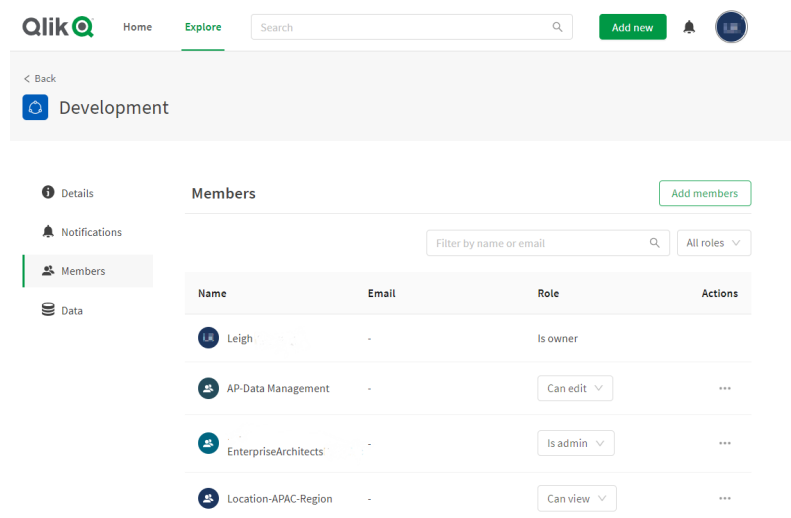
- **User** – This role is given to anyone who has access to a tenant. It is implied rather than specifically granted. It is further broken down by license type:
 - Professional - Professional access is for users who need access to all features within Qlik Sense Enterprise SaaS -Government (US). It is charged on a per user basis.
 - Analyzer - Analyzer access is for users who consume content created by others. It is charged on a per user basis.
 - Analyzer Capacity - Analyzer access is for users who consume content created by others. It is charged based on usage rather than at a per user fee.

- **Developer** – The developer role allows the user to create API keys. API keys are used for programmatic access to the tenant and for certain external tools.
- **Tenant Admin** – The tenant admin role provides full access to the management console for management of all administrative aspects of a customer’s tenant. There is always a minimum of one tenant admin.
- **Analytics Admin** – The Analytics Admin role is a partial administrator. A user with this role has access to the Using the Management Console but only to the areas of governance and content.
- **SharedSpaceCreator** - A user with this role can create shared spaces.
- **ManagedSpaceCreator** - A user with this role can create managed spaces.

Spaces

Spaces are areas of the Qlik Sense Hub used to both develop and control access to apps, data files and data connections. There are three types of spaces:

- **Personal spaces** - Private work areas for each user in the Qlik Sense Hub.
- **Shared spaces** - Areas used to develop apps collaboratively and share them with other users in the space. A group of users may use a shared space for the private development and consumption of their own apps.
- **Managed spaces** - Governed sections of the Qlik Sense Hub that are used for providing access to apps with strict access control both for the app and the app data.



Data Files & Data Connections in spaces – Data Files and Data Connections, just like Apps, can also be stored and reused across the three space types.

Access to shared and managed spaces can be assigned either directly to users or to groups. It is considered best practice to use groups and manage group membership in the Identity Provider rather

than directly assign access to individual users. Various levels of access can be assigned, so it is possible that a user can have different access permissions to different spaces.

Enterprise data at scale

Tenant resources

Each Qlik Sense Enterprise SaaS – Government (US) tenant provides fully expandable storage¹ and with a standard Qlik Sense Enterprise SaaS – Government (US) subscription, each Qlik Sense app can consume up to 5 gigabytes of memory. Qlik Sense Enterprise SaaS – Government (US) scales to meet the demand that is required on system resources with no requirements on users to configure any of the infrastructure.

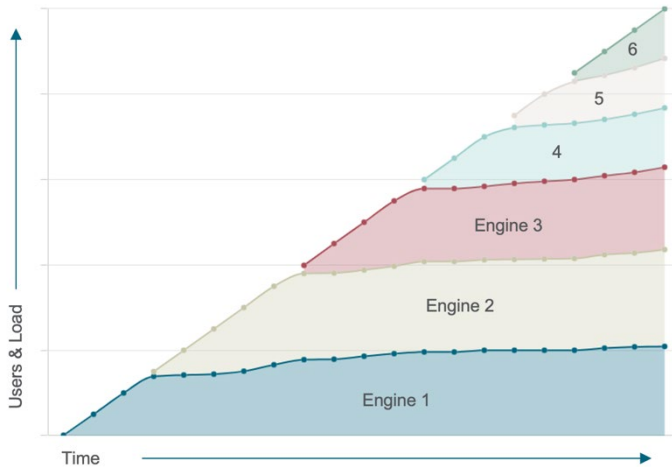
Dedicated Capacity

Certain use cases may require apps that use more than 5 gigabytes of memory. Qlik provides a Dedicated Capacity option for applications larger than 5 gigabytes in memory. For Qlik Sense Enterprise SaaS – Government (US) Dedicated Capacity is part of the standard offering, with the option to purchase more Dedicated Capacity if required.

In addition, Qlik Sense Enterprise SaaS – Government (US) supports integration with enterprise storage solutions such as AWS S3 and Azure storage to enable access to your own storage assets. Please see the section [Integrate on-premises Data with SaaS](#) for more details.

¹ Subject to the Qlik Sense Enterprise license metrics

Automatic scaling to meet user load



When using on-premises deployments of Qlik Sense, customers are required to estimate and size infrastructure for their peak usage. This is a complex process and often customers either under or over resource for peak usage times, leading to poor performance or unnecessary cost. Often these resources are only need for very short periods to deal with daily or weekly peaks.

In Qlik Sense Enterprise SaaS – Government (US) standard tier customers pay per user, not per engine. Therefore, this extra cost is eliminated. More importantly, user satisfaction is higher as dealing with increased load is instantaneous, not subject to delays of procurement, installation, and configuration of infrastructure.

When a user accesses an application in Qlik Sense Enterprise SaaS – Government (US), we initially check if the application is already open on one or more engines. If it is not, or these engines are already under heavy load, Qlik responds in turn by providing additional compute engines dynamically and opening another copy of the application. This autoscaling requires no configuration, management or extra expense from the customer and is transparent to the user. When the resources are not needed, Qlik will reduce the number of copies of the application open.

Focus on analytics, 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-premises deployments, customers need to factor in several costs which are not directly related to solving business problems such as:

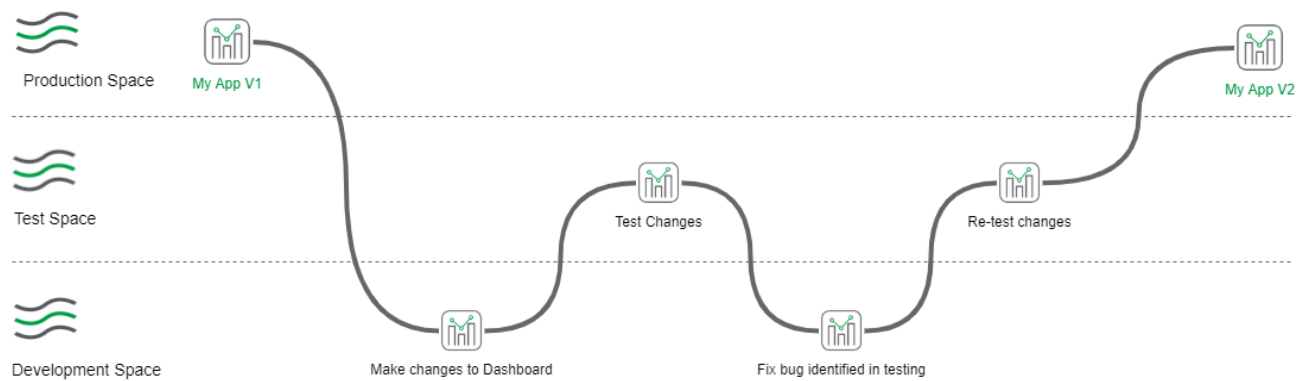
- Infrastructure capital and operational costs
- Operating system management and software licensing
- Staffing costs for infrastructure administrators

With Qlik Sense Enterprise SaaS – Government (US), our customers can focus on solving business problems rather than administering their analytics environment. This both reduces the total cost of

ownership of analytics and the time it takes to get to actionable analytics – what Qlik refers to as *minutes to insight*.

Move apps through a development lifecycle, not development servers

In a traditional BI environment apps would be developed on a development server. Once development was complete, they would be moved to a test server. Issues found in testing would mean several iterations of this process until the application could be deployed to production, requiring a lot of resources and infrastructure to manage. With Qlik Sense Enterprise SaaS – Government (US), apps are stored in discrete spaces. Each space has its own security settings, data connections and file storage. Customers can create as many development, test and production spaces as needed to suit their software development life cycle. This approach allows much greater flexibility, agility, and reduced infrastructure expense than with a traditional on-premises setup.



In the above example, users consume the app in the production space. When a change to the app is requested, a copy is made in the development space and is published to the test space when ready for app testers to review it. Several cycles may occur until the app is ready to be released to production. To facilitate these flows, each space has its own data connections and file storage, so that an app will load the appropriate data for the applicable life-cycle phase.

Qlik Sense Enterprise – Government (US) 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 Sense Enterprise SaaS-Government (US) infrastructure.

Qlik's zero downtime deployments for Qlik Sense Enterprise SaaS- Government (US) allows upgrades and modifications 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](#).

Integrating on-premises data with Qlik Sense Enterprise SaaS – Government (US)

Qlik understands that while many organizations are moving their systems to the cloud, there will always be some systems such as mainframes, that remain on-premises. Additionally, some customers that choose to migrate some systems to private clouds that are not directly accessible from public SaaS environments. Consequently, Qlik provides several solutions to integrate on-premises and private data sources with Qlik Sense Enterprise SaaS – Government (US).

Qlik Data Integration Portfolio*

Qlik's Data Integration portfolio is a bundled solution with components such as Qlik Catalog, Qlik Replicate® and Qlik Compose™ for Data Lakes and Data Warehouses, all providing the ability to publish data from a wide breadth of data source end points to cloud storage locations, such as S3 buckets & Cloud data warehouses. These can then be used by Qlik Sense Enterprise SaaS to load apps. Data Integration products which can be used with Qlik Sense Enterprise SaaS Government include:

- Qlik Replicate* - Universal data replication and real-time data ingestion²
- Qlik Enterprise Manager* - Centrally manage your data pipelines³

*This product is not included with Qlik Cloud Government. Customers are fully responsible to ensure that this product meets their requirements in all respects. For more information on Qlik's Data Integration Platform see: <https://www.qlik.com/us/products/data-integration-products>

API and script-based data integration

It is possible to move applications to and from the Qlik Sense Enterprise SaaS- Government (US) platform using either our APIs directly, or via the Qlik-cli tool. Applications can be created programmatically, imported, published, and reloaded. They can also export with or without data, and many other operations.

² FIPS Compliance due Q4 2021

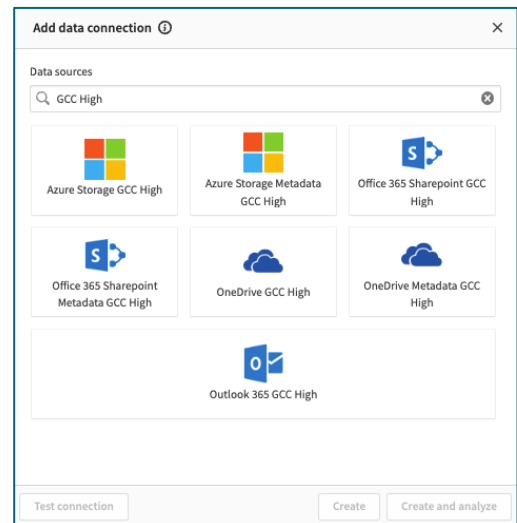
³ FIPS Compliance due Q4 2021

Qlik Data Transfer

Qlik Data Transfer is a lightweight Windows application that lets you upload data from on-premises data sources to Qlik Sense. Customers can choose to use Qlik Data Transfer as part of their implementation of Qlik Sense Enterprise SaaS - Government (US). This tool supports encrypted communications but is not FIPS compliant. Qlik Data Transfer is not available to download from Qlik Sense Enterprise SaaS - Government (US), but it can be downloaded from the [Qlik Download Site](#).

Government Cloud Connectors

For a Government deployment of Qlik Cloud, there is often a need to connect to data sources in other FedRAMP certified cloud providers. Qlik provides connectors to data sources in these 3rd party FedRAMP cloud deployments.

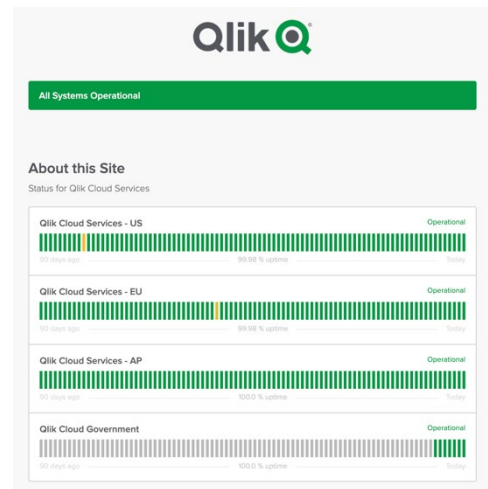


Reliability

Open and transparent

Qlik makes data on uptime and incidents publicly available, so customers and prospective customers can see understand the current status and reliability of Qlik Sense Enterprise SaaS – Government (US) This information is available at <https://status.qlikcloud.com>. If further information is needed or request the SLA, please contact [here](#).

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.



Adaptable high availability infrastructure

The Qlik Sense Enterprise SaaS – Government (US) platform runs in an Amazon GovCloud region. 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 and minimizes any potential downtime for the platform.

Disaster recovery / backup and recovery

Qlik’s Site Reliability Engineering (SRE) team performs disaster recovery tests regularly. As part of these tests, the team builds an entirely new Qlik Sense Enterprise SaaS – Government (US) 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 Sense Enterprise SaaS – Government (US) 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

Security and Governance Model

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 – Government (US) . This information could be a short name or code that does not identify the individual. Also, Qlik Sense Enterprise SaaS – Government (US) 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 – Government (US) or the corresponding changes are automatically applied.

Through OIDC support, Qlik Sense Enterprise SaaS – Government (US) supports all the major identity providers including Okta, Auth0, Azure AD & ADFS.

Qlik Sense Enterprise SaaS – Government (US) supports Government mandated multi-factor authentication via PIV (Personal Identity Verification) / CAC (Common Access Card) for tenant administrators and end users via the customer's identity solution.

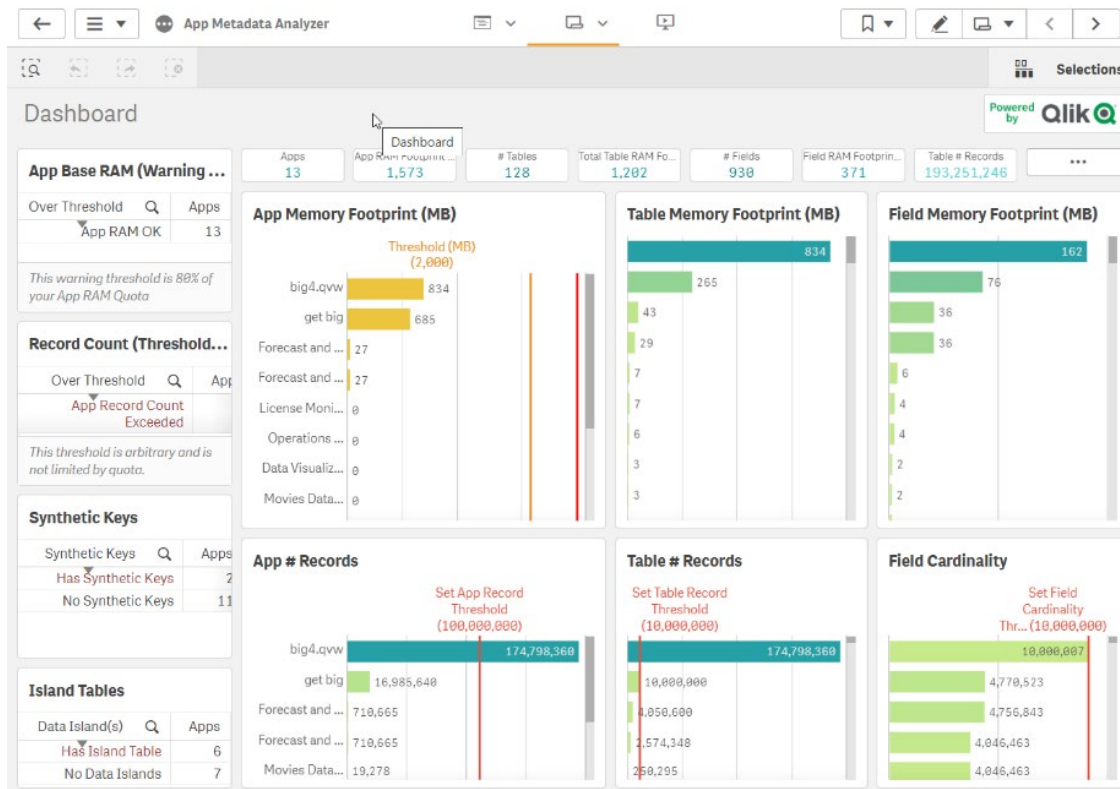
Section access

Section Access is used to control the security of an application. It uses the data model to define authorization at the data level and allows restricted access to data at row and column levels. For more information, read about [Section Access](#) in our help documentation.

Governance

Understanding tenant governance

Qlik provides the App Analyzer for Qlik Sense Enterprise SaaS – Government (US) to provide governance information into customer's tenant. This app looks at key performance characteristics of apps such as memory usage, cardinality, and the data model.



Monitor activity in the tenant

The Qlik Sense Enterprise SaaS – Government (US) management console contains several tools to assist with the governance of the Qlik Sense Enterprise SaaS – Government (US) 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 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 through the management console, provides Application Programmable Interfaces that allow viewing (but not modifying or removing) tenant activity. Customers can integrate the Qlik Sense Enterprise SaaS Government (US) 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.

Govern and improve your Qlik Sense Applications with the App Evaluation service

The App Evaluation service helps users manage their Qlik Sense Enterprise SaaS – Government (US) instance from a performance perspective. The service captures key metrics on Qlik Sense Enterprise SaaS – Government (US) applications, including increases in application size and length of time to open applications. Further, the service provides feedback on possible reasons for changes, allowing customers to address these issues.

The screenshot displays the 'Evaluation details' window for a Qlik Sense application. It features a 'Results' tab and a 'Breakdown' section. The performance metrics are as follows:

Metric	Value
Time to open	3.5 s
Peak size	453 MB
Data model size	314 MB
Total rows in app	85 rows
Public sheets in app	4 sheets
Public objects in app	35 objects

Below the metrics, a warning box indicates: 'Performance evaluation completed with warnings'. It lists two specific warnings:

- The calculation condition was unfulfilled
- This app utilizes section access, which means different users will see different results

At the bottom of the window, there are three buttons: 'Help', 'Download log', and 'Done'.

Standards-Based Security & 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 – Government (US) has been built from the ground up as a secure platform and Qlik has worked with external parties to ensure that the applicable industry standard and/or best practice controls are in place.

FedRAMP

The US government provides a standardized approach to security authorizations for Cloud Service Offerings; the Federal Risk and Authorization Management Program (FedRAMP). The Qlik Sense Enterprise SaaS- Government (US) platform has achieved FedRAMP authorization at the at the Moderate Impact Level (IL) and Department of Defense (DoD) Impact Level (IL) 2. Details of this are available on the [FedRAMP Marketplace](#).

For the latest information on Qlik’s external certifications and compliance, visit our [Trust page](#).

Data sovereignty

Customers' data, including any data within backup/recovery and disaster recovery systems, is maintained within the Qlik Sense Enterprise SaaS – Government (US) region. Nothing is transferred out of region unless the customer does so. Copies of backups are stored at a secondary location 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. For more information visit our [Privacy page](#).

Data separation & storage

Qlik Sense Enterprise SaaS – Government (US) is a multi-tenant platform. As a multi-tenant platform, it is crucial that each customer's data is separated from other customers. Each tenant has a uniquely generated set of encryption keys that Qlik manages for that customer. Each tenant's keys are separate from keys Qlik uses to secure service to service communication. The encryption used within the Qlik Sense Enterprise SaaS - Government (US) platform is FIPS Compliant.

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

Content Deletion

"Content" is the customer-provided data and other information within the Qlik Sense Enterprise SaaS tenant. The creation and removal of content that resides in the tenant is controlled by the customer. 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 Sense Enterprise SaaS – Government (US). When a customer deletes an App in their tenant, the service deletes the file on the underlying Kubernetes storage solution. QCS relies on the Kubernetes storage solution file system to execute the delete in the underlying block storage.

Qlik leverages Amazon AWS for backups to maintain copies of Content for 30 days before that Content ages out and is deleted from the supporting file systems. QCG leverages the Amazon GovCloud platform for backups and Amazon Simple Storage Service (S3) to copy Content for backup purposes.

Qlik Sense Enterprise SaaS platform security

Monitored for security 24/7

Qlik Sense Enterprise SaaS – Government (US) is monitored by Qlik's 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

To ensure a strong, secure foundation, Qlik shares security responsibilities with AWS GovCloud, our valued partner for cloud infrastructure. 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 Sense Enterprise SaaS- Government (US) relies on cloud infrastructure for secure physical access, redundant (fault tolerant) infrastructure, and scalability. Our AWS GovCloud'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 AWS GovCloud'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 QCG 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 Sense Enterprise SaaS- Government (US).

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 Sense Enterprise SaaS – Government (US) 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.

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

Architecture

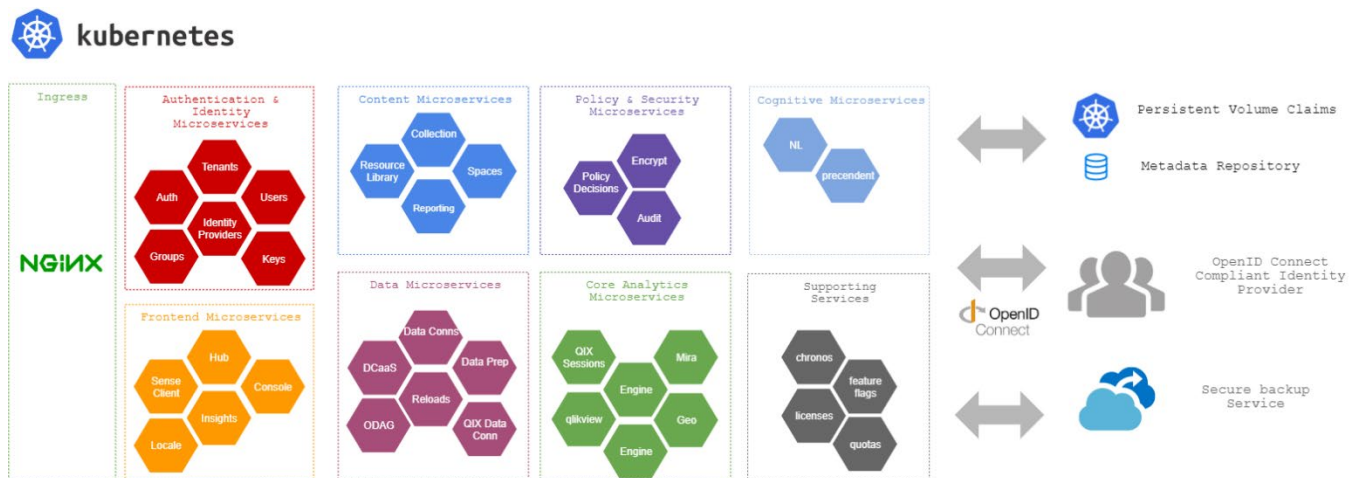
Qlik's cloud native platform and Kubernetes stack

In order to design a highly-scalable, highly-available cloud platform and service, Qlik could not simply shift our Windows products and move them to the cloud. Qlik Sense Enterprise SaaS – Government (US) is based on a micro-services architecture, and the various components of the platform have been built from the ground up to build a 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, which is used in to ensure consistent performance for our customers regardless of the number of users on the platform. Automated monitoring and adjustment of resources allows all components of the platform to have the right resources at the right time.

Another key aspect of Cloud Native apps is the concept of zero-downtime deployment. Qlik Sense Enterprise SaaS – Government (US) has been designed to support zero-downtime deployment. Qlik is able to upgrade key components of 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 Qlik Sense Enterprise SaaS – Government (US) 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>

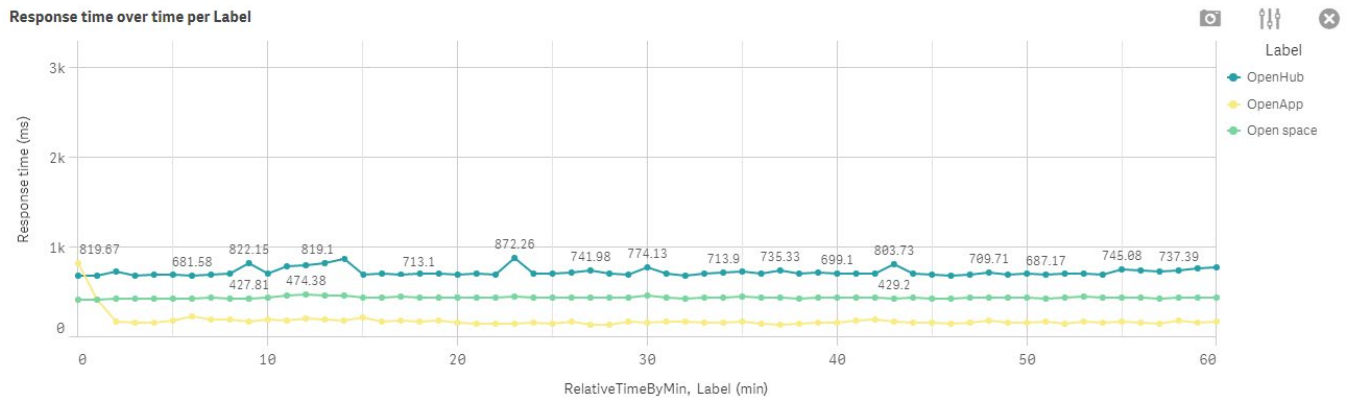
NGINX Ingress Controller – NGINX Ingress Controller provides the web interface and internal load balancing for tenants. NGINX is an HTTP and reverse proxy server, a load balancing server, and a generic TCP/UDP proxy server. See <https://www.nginx.com/products/nginx/kubernetes-ingress-controller/>

MongoDB - MongoDB is a cross-platform document-oriented database and is used as metadata repository <https://www.mongodb.com/>

Predictable performance at scale

To ensure the best possible end user experience, Qlik continuously takes anonymized samples of the performance and scalability of 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 apps
- Number, frequency, and size of concurrent reloads



In this example, we tested 10,000 users per hour 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.

Integrating and Expanding Qlik Sense Enterprise SaaS – Government (US)

Integration approaches

Qlik Sense Enterprise SaaS – Government (US) supports several options for integrating Qlik hosted apps into customer’s own environment. For detailed information on the options available see <https://qlik.dev/basics/authentication-options>

API keys

An API key is a token representing a user in the 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.

Interactive Login

To authenticate users in web apps, use multiple REST endpoints to evaluate if the browser has an active Qlik Sense SaaS session. Then use a redirect to the tenant's sign-in URL.

Web apps embedding Qlik Sense objects or data, also known as mashups, require a web integration id in the tenant's configuration. Web integration ids are a security feature of Qlik Sense Enterprise SaaS – Government (US) for handling Cross-Origin Resource Sharing (CORS) of embedded Qlik Sense application 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 – Government (US) APIs and the Qlik Associative Engine.

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 have two primary use cases, authorization, and information exchange. Qlik Sense Enterprise SaaS – Government (US) reads JWTs from external identity providers during the authentication phase. Qlik Sense Enterprise SaaS – Government (US) creates an internal JWT post authentication for use during a session.

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

Applications connecting to Qlik Sense Enterprise SaaS – Government (US) with JWTs require the same web integration id and cross-site request forgery prevention as all integrations. with the platform.

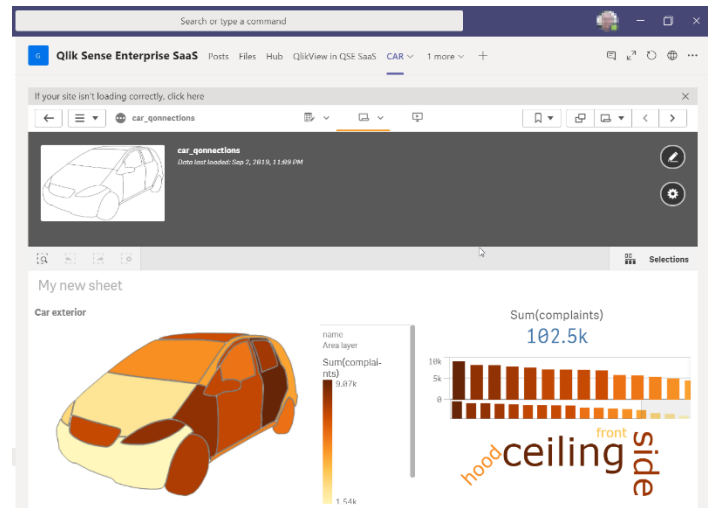
The screenshot shows a 'Create identity provider configuration' dialog box. It contains the following fields and options:

- Identity provider**: A text input field.
- Type**: A dropdown menu with 'JWT' selected.
- Provider**: A dropdown menu with 'External' selected.
- Description (optional)**: A text area containing 'JWT Integration with portal.company.com'.
- JWT**: A text input field.
- Certificate**: A text area containing the certificate string 'MIID1jCCAr6gAwIBAgIU80ZCSzChKD1Y6FAvcR4YQwqyQQwD'.

At the bottom right, there are 'Cancel' and 'Create' buttons.

Embedding

Qlik Sense Enterprise SaaS – Government (US) apps support embedding in another web portal, or within a tool such as a third-party client. Read more about how to [create mashups and web apps](#) on our help site. Qlik also provides pre-built examples that customers can use to get started on embedding their Qlik apps and visualizations into their mashups and web apps. These examples are available on GitHub here: <https://github.com/qlik-oss/web-integration-examples>



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>.

Qlik Reporting Service

To meet the need for certain types of flexibility in reporting, Qlik has introduced the Qlik Reporting Service.

The Qlik Reporting Service is an API that provides the ability to develop multi-page reports that can be distributed to users outside of Qlik Sense Enterprise SaaS – Government (US). Reports can be integrated into a customer's own applications. Reports are created as PDF documents. All Qlik sense Enterprise SaaS customers are entitled to create up to 100 reports as part of their SaaS subscription.

Qlik Open Source

In addition to API governance, Qlik R&D delivers libraries to accelerate development, testing, and integrating of the Qlik Sense Enterprise SaaS platform through Qlik Open Source (<https://github.com/qlik-oss>). A number of these first-party libraries are used in the platform itself, such as:

- **Nebula.js** - a collection of JavaScript libraries, visualizations and CLIs that helps developers build and integrate visualizations on top of the Qlik Associative Engine
- **Enigma.js & Enigma.go** - JavaScript & go lang libraries for consuming the Qlik Associative Engine
- **Gopherciser** - a load testing tool for Qlik Sense Enterprise SaaS

For more information on Qlik Open Source see <https://github.com/qlik-oss/open-source>.

Tools and resources

Developer Portal (<https://qlik.dev>) - is a central location for developers to find the information they need to develop with Qlik products including Qlik Sense Enterprise SaaS –Government (US), including developer documentation, API references, tutorials, etc.

Qlik-cli - is a command line interface for automating management activities in Qlik Sense Enterprise SaaS –Government (US). Customers can choose to use Qlik – cli as part of their implementation of Qlik Sense Enterprise SaaS - Government (US). This tool supports encrypted communications but is not FIPS compliant. This is available at <https://qlik.dev/libraries-and-tools/qlik-cli>.

Summary

Qlik Sense Enterprise SaaS- Government (US) is designed to provide our customers in the U.S. Public Sector with a platform to securely move their analytic workloads to the cloud. Built on Cloud Native technologies, the Qlik Sense Enterprise SaaS – Government (US) platform has been designed to automatically scale to meet the workloads of the modern enterprise and provides Qlik customers a platform that can consolidate Qlik Sense and other BI apps in a single hub.

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 supporting 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 Sense Enterprise SaaS-Government (US) a part of their own solutions.



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](https://www.qlik.com)

© 2022 QlikTech International AB. All rights reserved. All company and/or product names may be trade names, trademarks and/or registered trademarks of the respective owners with which they are associated.