White Paper

Qlik® Sense security overview

September, 2015

Platform

Qlik® Sense is an analytics platform powered by an associative, in-memory analytics engine. Based on users' selections, calculations are computed at runtime against data stored in-memory. Results are returned to users via a zero footprint web interface delivered on desktops, laptops, mobile devices, and through embedded analytics. Qlik Sense offers a highly interactive, associative experience in which users can freely navigate through data with little to no constraint in their analysis path.

Overview

Qlik® Sense provides self-service visualization that is scalable, secure, and governable. To ensure platform security, Qlik® Sense leverages internal and external resources to manage access, authentication, authorization, and data governance on four levels.

- **Network security:** All communication between Qlik® Sense services and web clients use web protocols using Transport Layer Security (TLS). TLS uses digital certificates to encrypt information exchanged between services, servers, and clients. Encrypted information flows through tunnels requiring two certificates to secure the connection; a server certificate to identify the correct server and a client certificate to allow the client to communicate with the identified server.
- **Server security:** The operating system security system controls access to certificates, storage, memory, and CPU resources. Qlik® Sense uses these controls to protect the platform by only allowing authorized users and processes access to required resources.[1]
- **Process security:** Qlik® Sense goes through a rigorous testing process during development to mitigate security risks and handle unanticipated events. Additional testing verifies Qlik® Sense is able to stand up against known security threats toward the software.
- **App security:** Attribute based access control provides a comprehensive framework to govern user capabilities within the platform. Row and column level data reduction through section access dynamically manages the data users view and select in applications.

[1] For more information about Qlik Sense architecture, review the Qlik Sense Architectural Overview.

Authentication

Qlik® Sense Proxy

All authentication in a Qlik® Sense deployment is managed by the Qlik® Sense Proxy Service (QPS), including clients connecting to the Hub or the Qlik® Management Console (QMC). Qlik® Sense requires an external identity provider to verify an individual user's identity. Upon verification, Qlik® Sense transfers the user to Hub or QMC using TLS and certificate authentication in the following methods:

- **Ticket API** transfers the user and user's attributes using a one-time ticket. For example, Windows authentication with Qlik® Sense invokes the ticket API after verification with the domain.
- **Session API** where an external module transfers a web session identifying the user to Qlik® Sense.
- **HTTP Headers** in solutions with trusted systems that transfer user information using this method.
- **SAML** integration with Qlik® Sense acts as a service provider (SP) integrating with an identity provider (IdP).
- **Anonymous** users can be configured to access Qlik® Sense.

Qlik Sense - three step authentication

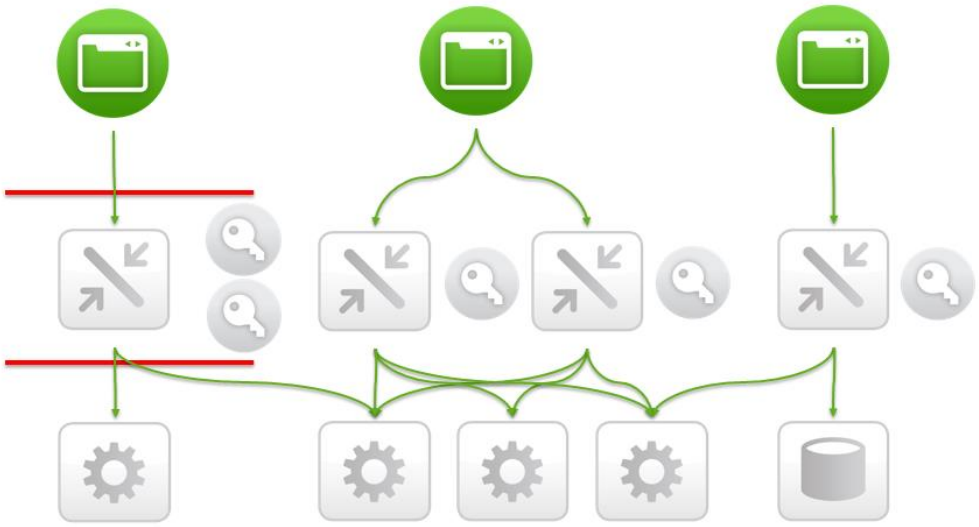
1. Authentication module gets the user identity and credentials.

2. Authentication module requests an external system to verify the user identity using the credentials.

3. User transferred to Qlik® Sense using the Ticket API, Session API, HTTP headers, or SAML.

Virtual Proxies

Each QPS in a Qlik® Sense deployment uses virtual proxies to support authentication. Virtual Proxies allow one proxy to support multiple authentication schemes, perform session management, and load balancing across multi-node deployments. Virtual proxies may link to one or many QPS nodes to direct traffic, load balance between engines, or provide specific access to administrative layers of a deployment. In the figure below, the leftmost virtual proxy is in a DMZ, and connects to two engines. Other proxies with virtual proxies connect to several engines depending on virtual proxy configuration and load balancing.

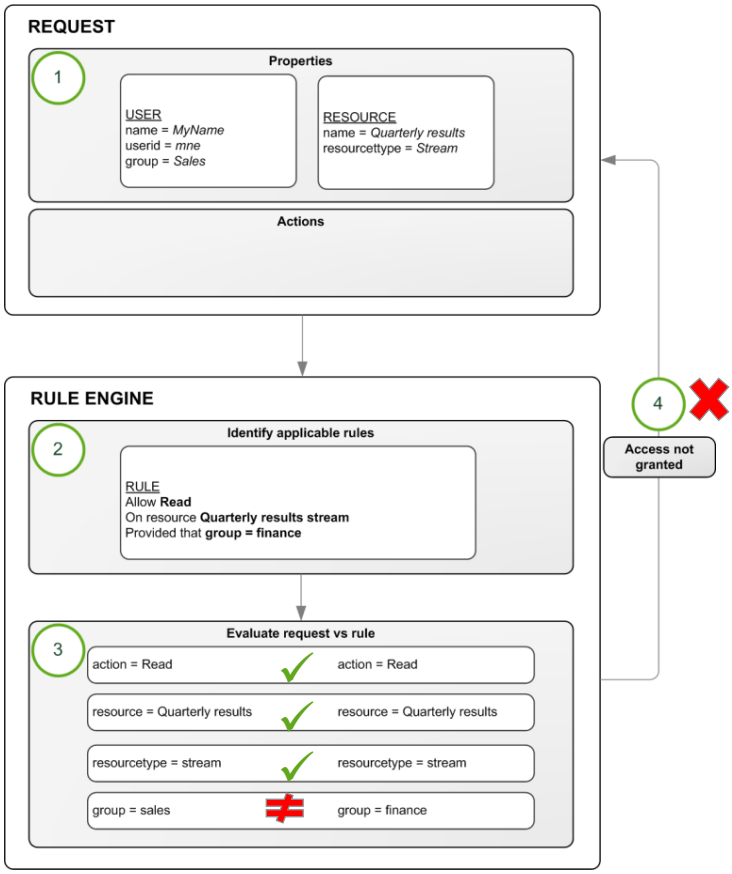


Authorization

After a user authenticates and gains access to Qlik® Sense, authorization through an attribute based access control (ABAC)[2] model enforces application visibility and self-service capabilities within applications.

Attribute Based Access Control (ABAC)

In Qlik® Sense, ABAC is defined as an access control method where **user** requests to perform **actions** on **resources** are granted based on assigned attributes of the **user**, assigned attributes of the **resource**, **environment** conditions, and a set of **security rules** that are specified in terms of those attributes and conditions. Attributes from Active Directory, LDAP, and databases are loaded into Qlik Sense. In addition, attributes may be defined and managed directly within Qlik Sense as well.



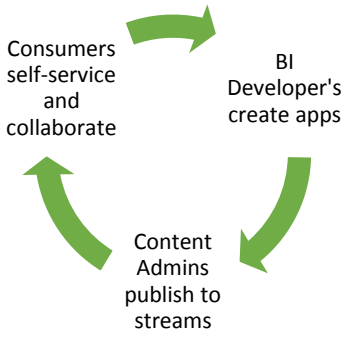
Security Rules

Qlik® Sense security rules define user capabilities on Qlik® Sense resources provided a condition. Access is provided if at least one rule returns true based on attributes like the roles or groups of the user and resources.

Security rules control access to application streams in the hub, capabilities within applications (sheet, story, bookmark creation), and administrative capabilities in the QMC (publish apps, set stream access, create and run tasks).

The security rules framework comes with several predefined rules enabling administrators to scale security across users leveraging existing roles and groups in the enterprise.

In a roles based enterprise, BI authors are responsible for app creation and have data access. Content Admins do not create, but publish applications to streams aimed at groups of consumers. Consumers have the ability to extend their own analysis with sheets and stories within an application; sharing new found insights with their teammates without compromising the integrity of the core application. All of these capabilities and corresponding rules are delivered out of the box with Qlik® Sense.



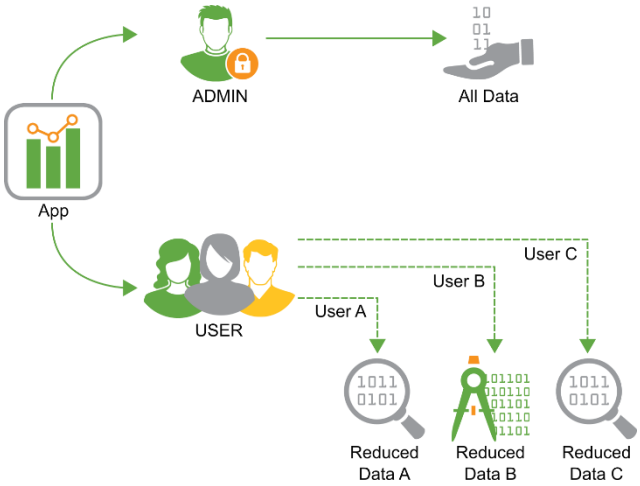
[2] ABAC is a special publication of the National Institute of Standards and Technology (NIST) catalogued as NIST Special Publication 800-162.

Data Reduction

Data reduction in Qlik® Sense determines what data users and groups are allowed to see when they enter a Qlik® Sense application. In Qlik® Sense, data reduction is known as section access.

Section Access

Section access performs row and column level security in a Qlik® Sense application. With section access, a single Qlik® Sense application may hold data for multiple users or groups. Through the authentication and authorization process, user information is sent into the application to dynamically reduce the data so that users access only the data they are allowed to view. Section access may use attributes and fields from external databases, directories, lookup tables, or created tables to enforce user visibility to data.



Dynamic Data Reduction

Section access reduces data in an application dynamically by associating section access data with the business data loaded into the application with a single defined relationship. Using common field names, rows of data are excluded from the user during application interaction. In addition, columns of data may be hidden from view by specifying field names to omit for each user.

Attributes and Fields

	A	B	C	D	E
1	ACCESS	USERID	GROUP	TERRITORYCODE	OMIT
2	USER	112ADAMS\QVRO	*	AFG	Population
3	USER	112ADAMS\QVRO	*	ALB	Population
4	ADMIN	SENSE20\Administrator	*	*	
5	USER	112ADAMS\QVPU	*	BRA	Population

App Data

Territories

- TERRITORYCODE
- Territory
- OICA region
- Region color
- Trading bloc
- ISO 3166-1 alpha-2
- Calling code
- Area (km2)
- Population
- GDP (US$ current)
- Currency name
- Currency code
- Capital city
- BBC country profile
- CIA World Factbook article
- Wikipedia country article

Result

Admin Sees

Territory code
AFG
ALB
BRA

QVRO Sees

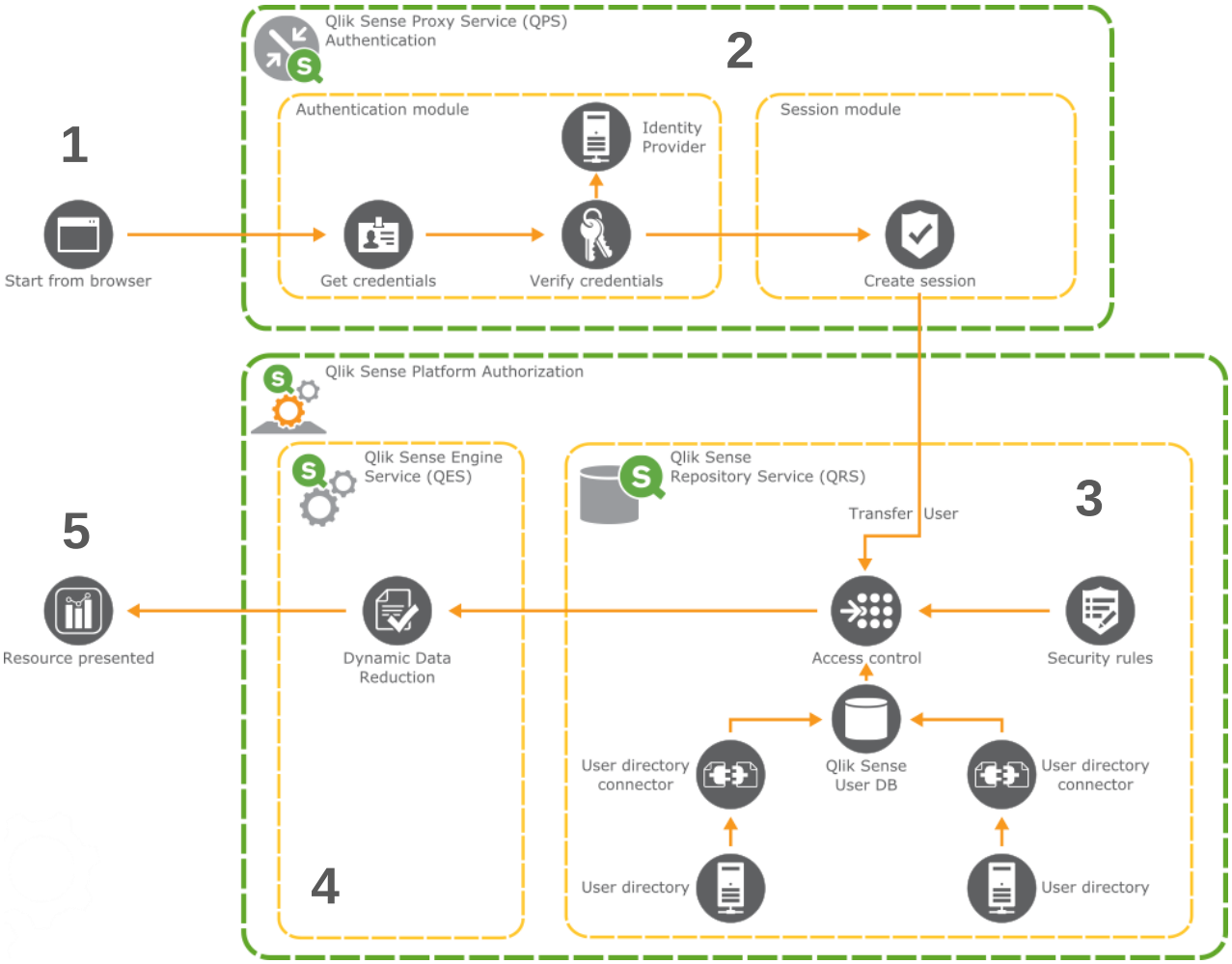
Territory code
AFG
ALB

QVPU Sees

Territory code
BRA

Qlik Sense Security User Access Workflow

Combining authentication, authorization, and data reduction is a seamless experience for a user accessing Qlik® Sense.

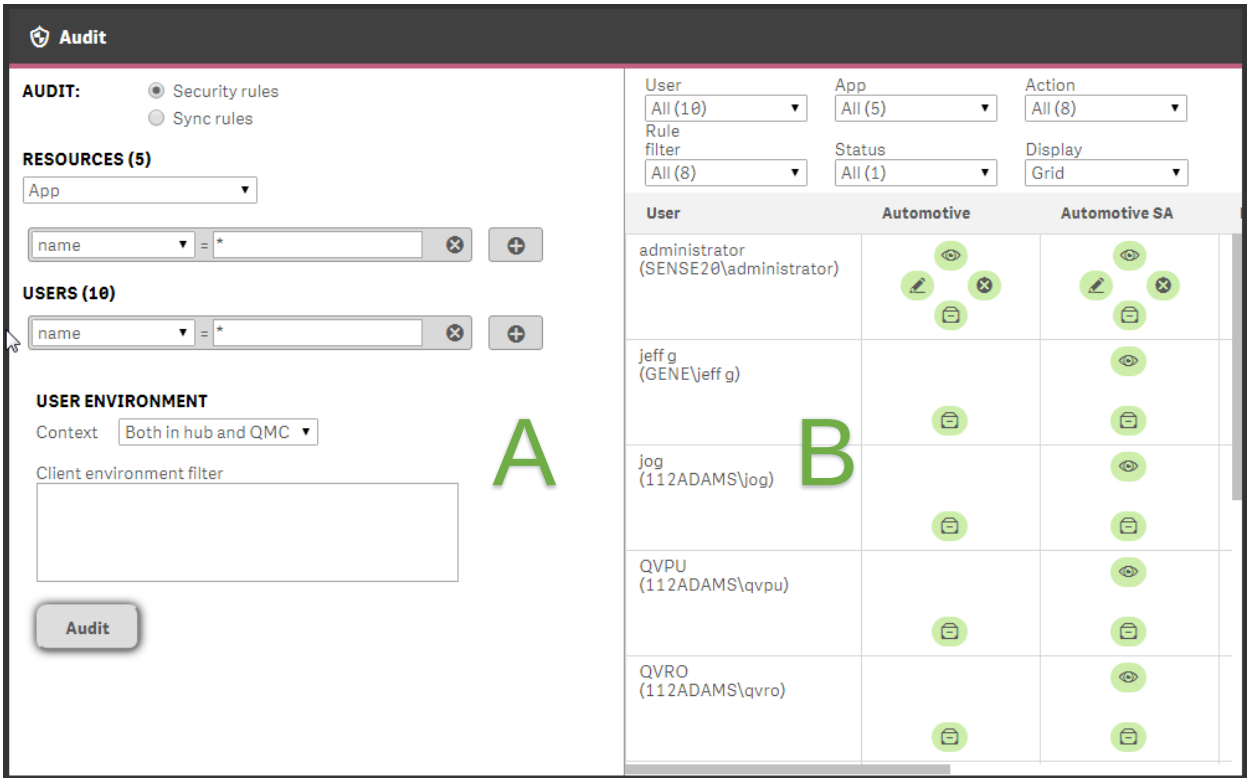


1. A user makes a request for Qlik® Sense content.
2. The Qlik® Sense proxy service authenticates the user and creates a session cookie in the browser.
3. The session cookie identifies the user to Qlik® Sense and synchronizes with a user directory to import attributes. At the same time the rules engine authorizes the user to Qlik® Sense content using the attribute based access control model.
4. The session state for the user is created in the engine. The engine performs dynamic data reduction using section access.
5. The engine sends content through a web socket connection to the client to render Qlik® Sense content.

Auditing

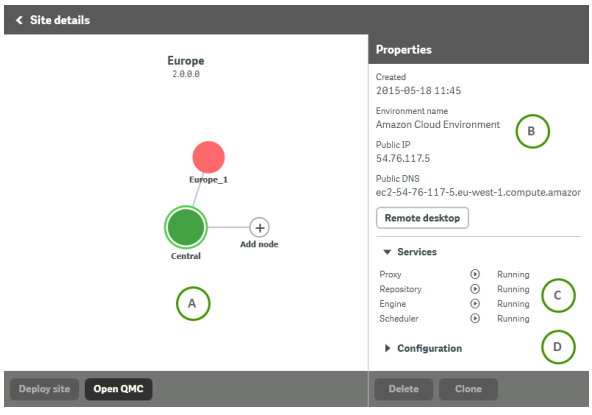
Governance is critical in enterprise business intelligence. Qlik® Sense delivers auditing, monitoring and logging using the QMC, applications, and log files to inform administrators and mitigate risks in deployments.

- **Audit** security rules using the Audit tab built into the Qlik® Management Console.

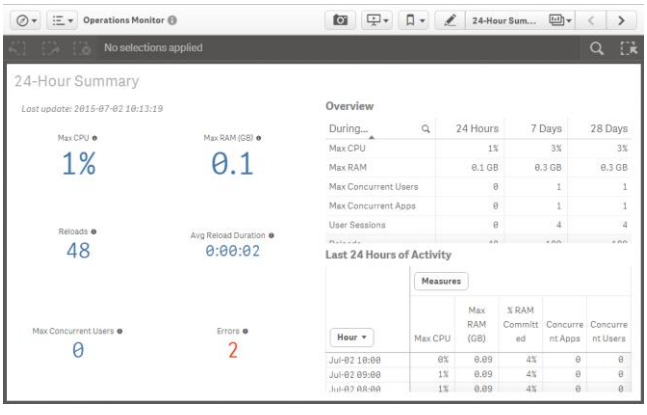


Using the Query view (A) and the Results view (B), administrators can evaluate user access control for applications. Administrators can use inline auditing when creating security rules for streams, content libraries, and data connections to preview access control based on rules they write.

- **Monitor** Qlik® Sense using the Operations Monitor and License Monitor applications. These applications present information related to uptime, sessions, resource utilization, change logging, and license compliance and management. The Qlik® Deployment Console enables administrators to monitor multi-node deployments and visually assess the health of the infrastructure.



Qlik Deployment Console



Qlik Operations Monitor

- **Logging** to text files runs in the background in a Qlik® Sense. All services include audit, system, and trace logs for deployment monitoring and management.

Summary

Qlik® Sense security provides comprehensive security at multiple levels to ensure only permissible users have access to allowable data via a secure connection.

- **Authentication** handled by the Qlik® Sense Proxy Service (QPS) using certificates for authentication and Transport Layer Security (TLS) to encrypt network traffic.
- **Authorization** between Qlik® Sense nodes using TLS and certificates, an attributed based access control (ABAC) system for managing user access and content, and presenting specific data for users via section access.
- **Auditing** the Qlik® Sense platform tracking changes in the repository database, comprehensive audit and security logging, monitoring applications, and tools for auditing access and managing multi-node deployments.
- **Confidentiality** by encrypting network connections with TLS and authenticating using certificates, leveraging the operating system file system and server access controls to protect content on Qlik® Sense nodes, protecting memory using operating system controls, securing application access at the resource level, encrypting sensitive information (e.g. passwords and data connection strings), and protecting app data using data reduction.
- **Integrity** through operating system controls like the file system to protect data at rest, encrypt sensitive information, and prevent data write back to the source system.

To learn more, visit Qlik®.com.