CAC Authentication and Qlik Sense on Windows

Considerations when Integrating with CAC Authentication

TABLE OF CONTENTS

Summary 2

Introduction 2

Common Authentication Solutions 3

Ticketing 3

Session 3

Header 4

SAML 4

JSON Web Token (JWT) 5

Common Scenarios 5

SiteMinder 5

Oracle Access Manager (OAM) 5

Internet Information Services (IIS) 5

Active Directory Federation Services (ADFS) with EAMS-A as a Claims Provider 6

Custom Ticketing and/or Header 6

Appendix 7

Appendix A - Enabling Smart Card Logon for Microsoft Windows Server 2012 Using DoD Public Key Infrastructure (PKI) 7

Appendix B - Contributors 7

Summary

- Qlik Sense relies on external identity providers (IdP) to authenticate users.
- The most common forms of authentication are ticketing and header authentication.
- Session, Security Assertion Markup Language (SAML) and JSON Web Token (JWT) authentication are also supported.

Introduction

Qlik Sense always asks an external system to verify who the user is and if the user can prove it. The interaction between Qlik Sense and the external identity provider is handled by authentication modules. For CAC authentication, it is most common to use the ticketing module or header authentication. Qlik Sense itself does not perform CAC authentication or integrate directly with the PKI, but rather should be setup to receive the credentials from the successfully authenticated user. Qlik Sense distinguishes a user by the unique combination of UserDirectory and UserId. If there is middleware between your authentication mechanism and Qlik Sense, these values can be passed through.

Authentication solutions

Qlik Sense authentication can be managed with any of the following solutions:

- Ticket
- Session
- Header
- SAML
- JWT

For more on Qlik Sense authentication methods, please see

https://help.qlik.com/en-US/sense/September2018/Subsystems/PlanningQlikSenseDeployments/Content/Sense_Deployment/Server-Security-Authentication-Solutions.htm

An example of such middleware could be a NodeJS applet that leverages Qlik Sense's ticketing module. This applet would receive the credentials from your authentication mechanism, and then build the request to Qlik Sense's ticketing module with said user's credentials. Another example could be header authentication against Oracle OAM over a reverse proxy – the user first authenticates against OAM, and then OAM passes along the headers with the user's credentials that Qlik Sense ingests.

For more on Qlik Sense authentication methods, please see: https://help.qlik.com/en-US/sense-admin/May2021/Subsystems/DeployAdministerQSE/Content/Sense_DeployAdminister/QSEoW/Administer_QSEoW/Managing_QSEoW/authentication-methods.htm

Common Authentication Solutions

Ticketing

Ticket authentication with Qlik Sense is similar to a normal ticket. The user receives a ticket after having been verified. The user then brings the ticket to Qlik Sense and, if the ticket is valid, is authenticated.

For more information on ticketing, please see:

https://help.qlik.com/en-US/sense/September2018/Subsystems/PlanningQlikSenseDeployments/Content/Sense_Deployment/Server-Security-Authentication-Solutions-Ticket-Solution.htm

For a step-by-step guide for enabling CAC with Qlik using ticketing, please see:

https://community.qlik.com/t5/Qlik-Community-Help-Documents/CAC-Authentication-Setup-Step-by-Step-Guide/ta-p/1508082

For some example Node.js code using ticketing in Qlik Sense, please see: https://developer.qlik.com/garden/56728f52d1e497241ae697fc

For information on how to request a ticket using the Qlik Proxy Service REST endpoint, please see: https://help.qlik.com/en-US/sense-developer/May2021/Subsystems/ProxyServiceAPI/Content/Sense_ProxyServiceAPI/ProxyServiceAPI-ProxyServiceAPI-Authentication-Ticket-Add.htm

Session

The session solution allows the Qlik Sense Proxy Service (QPS) to use a session from an external system to validate who the user is. Although this is not a common scenario that is deployed with CAC authentication, it is possible to authenticate a user using a session from an external system.

For information on session authentication, please see:

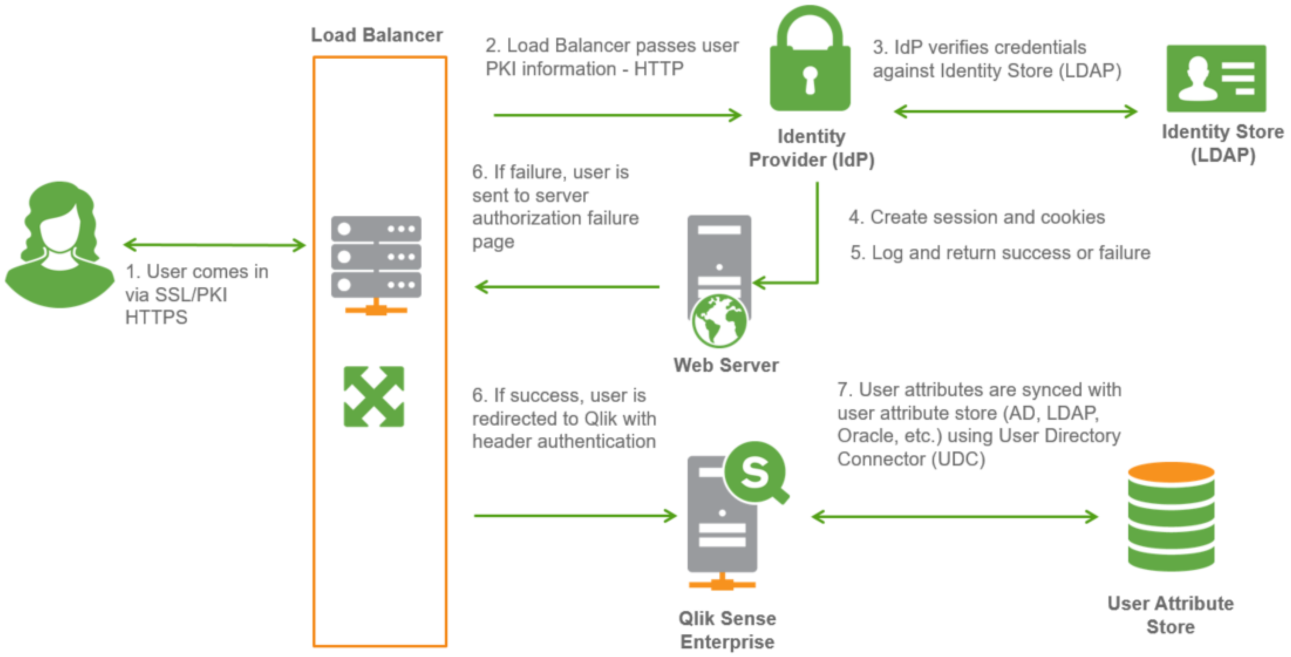
https://help.qlik.com/en-US/sense/September2018/Subsystems/PlanningQlikSenseDeployments/Content/Sense_Deployment/Server-Security-Authentication-Solutions-Session-Solution.htm

Header

The Virtual Proxy concept allows you to set up multiple authentication methods for a single environment. When using header authentication, traditional authentication is bypassed and instead the passed parameters in the HTTP header are used to identify the current authorized user. This makes this an ideal method to use in a trusted system where an existing identity management system has already identified the given user as an authorized user to access Qlik Sense.

For information and steps on setting up header authentication, please see the link below. Please note that this example is using a dynamic user directory, but it could also be set up with a static user directory: https://community.qlik.com/docs/DOC-20385

Example diagram


Load Balancer
2. Load Balancer passes user PKI information - HTTP
3. IdP verifies credentials against Identity Store (LDAP)
Identity Provider (IdP)
Identity Store (LDAP)
6. If failure, user is sent to server authorization failure page
4. Create session and cookies
5. Log and return success or failure
1. User comes in via SSL/PKI HTTPS
Web Server
6. If success, user is redirected to Qlik with header authentication
7. User attributes are synced with user attribute store (AD, LDAP, Oracle, etc.) using User Directory Connector (UDC)
Qlik Sense Enterprise
User Attribute Store

SAML

The Security Assertion Markup Language (SAML) is a data format for authentication and authorization. One of the key benefits of SAML is that it enables single sign-on (SSO), and thereby minimizes the number of times a user must log on to cloud applications and websites.

For information on SAML, please see: https://help.qlik.com/en-US/sense-admin/May2021/Subsystems/DeployAdministerQSE/Content/Sense_DeployAdminister/QSEoW/Administer_QSEoW/Managing_QSEoW/SAML-authentication.htm

For information on configuring SAML with different Identity Providers (IdP), please see: https://community.qlik.com/blogs/qlikviewdesignblog/2015/12/02/qlik-sense-saml-a-standardized-approach-to-authentication

JSON Web Token (JWT)

JSON Web Token (JWT) is an open standard for secure transmission of information between two parties as a JavaScript Object Notation (JSON) object. JWT is used for authentication and authorization. Because JWT enables single sign-on (SSO), it minimizes the number of times a user has to log on to cloud applications and websites.

For information on JWT, please see: https://help.qlik.com/en-US/sense-admin/May2021/Subsystems/DeployAdministerQSE/Content/Sense_DeployAdminister/QSEoW/Administer_QSEoW/Managing_QSEoW/JWT-authentication.htm

Common Scenarios

SiteMinder

Qlik Sense can be integrated with SiteMinder, a centralized Web access management system that enables user authentication and single sign-on, policy-based authorization, identity federation, and auditing of access to Web applications and portals.

For an example of using SiteMinder with header authentication, please see: https://community.qlik.com/docs/DOC-20383

Oracle Access Manager (OAM)

Qlik Sense can be integrated with Oracle Access Manager (OAM), a solution for web access management and user identity administration, using Apache or another reverse proxy as middleware. Header authentication is the most common authentication method being used in this scenario. OAM can also be used with SAML.

For example, code of using Apache as the reverse proxy with OAM, please see: https://community.qlik.com/docs/DOC-20431

Internet Information Services (IIS)

Internet Information Services (IIS), a general-purpose web server, can be leveraged as a reverse proxy with Qlik Sense.

For an example of setting up IIS as a reverse proxy with Qlik Sense, please see: https://community.qlik.com/docs/DOC-20406

Active Directory Federation Services (ADFS) with EAMS-A as a Claims Provider

Enterprise Access Management Service (EAMS-A), an identity and access management solution for Army applications, can act as a claims provider for Active Directory Federation Services (ADFS). Qlik Sense can then be configured with ADFS via a SAML virtual proxy.

For more information on configuring SAML for use with ADFS, please see: https://community.qlik.com/docs/DOC-16400

Custom Ticketing and/or Header

In many scenarios a custom solution is often preferred. For more detail on Qlik's authentication solutions, please see above for documentation.

Appendix

Appendix A - Enabling Smart Card Logon for Microsoft Windows Server 2012 Using DoD Public Key Infrastructure (PKI)

A reference guide for Enabling Smart Card Logon for Microsoft Windows Server 2012 Using DoD Public Key Infrastructure (PKI): https://community.qlik.com/docs/DOC-20566

Appendix B - Contributors

A special thanks to the following partners and customers for contributing to this guide:

- NuWave Solutions
- Integrated Data Services (IDS)
- CALIBRE
- VerticalApps
- K2 Technology Consulting
- US Army Corps of Engineers (USACE)
- Army Contracting Command (ACC)

Qlik® LEAD WITH DATA™

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 provides an end-to-end, real-time data integration and analytics cloud platform 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 50,000 customers around the world.

qlik.com