Securing / Hardening a Qlik Sense Server

Created by Levi Turner, last modified just a moment ago

(forked from Rikard's Hardening a Qlik Sense Server)

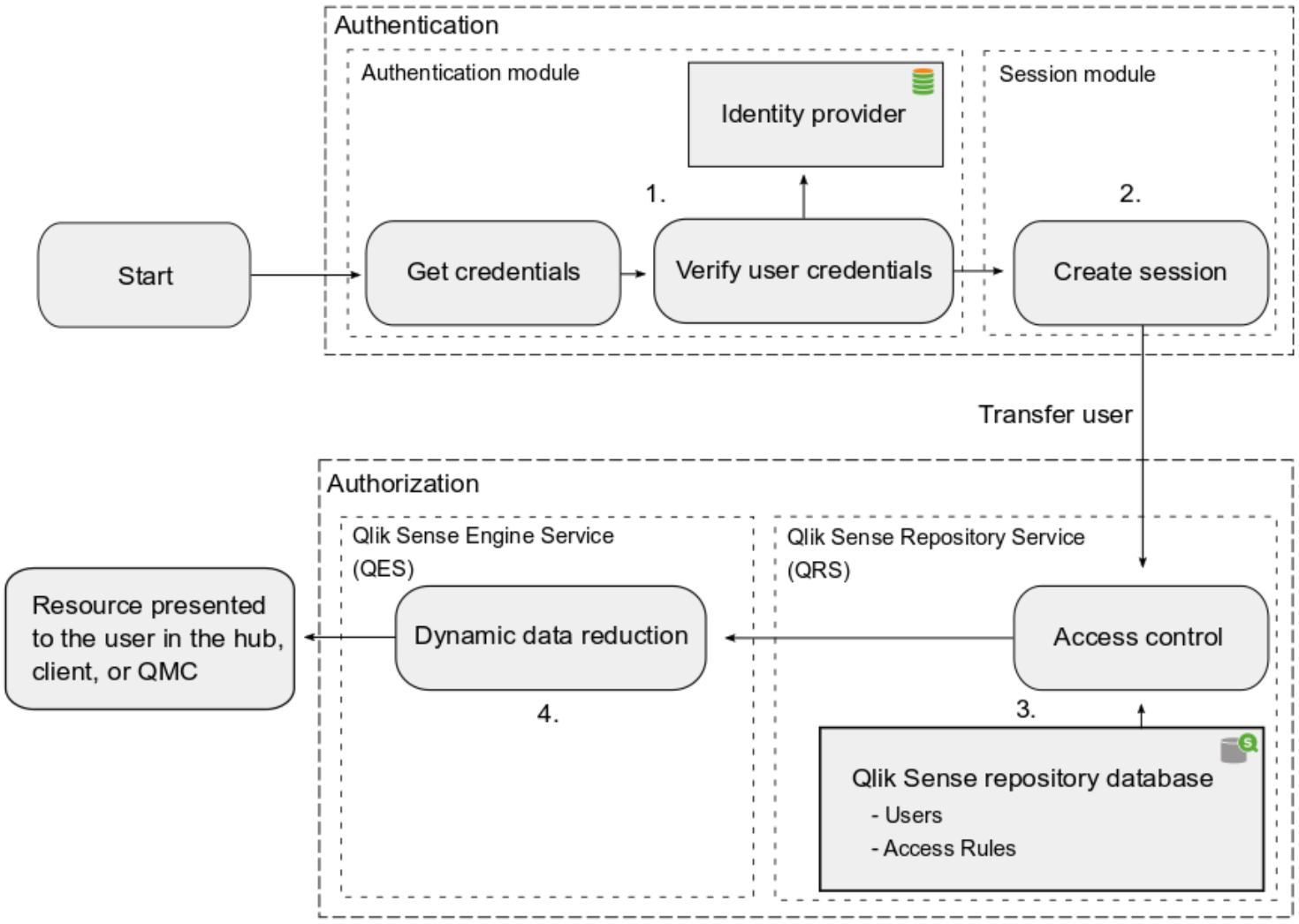
Overview

When it comes to a security approach inside of Qlik Sense Enterprise for Windows, there are four discrete areas which need to be covered:

1. Authentication
2. Authorization
3. Operating System level hardening
4. Generalized Web Server best practices
5. Network Appliances / Applications
6. Qlik specific guidance for external audiences

Some of these (e.g. 3 & 4) can interact with each other, but since they involve independent remediation we will address them separately.

The Qlik Sense Enterprise for Windows specific portions can be illustrated like so:

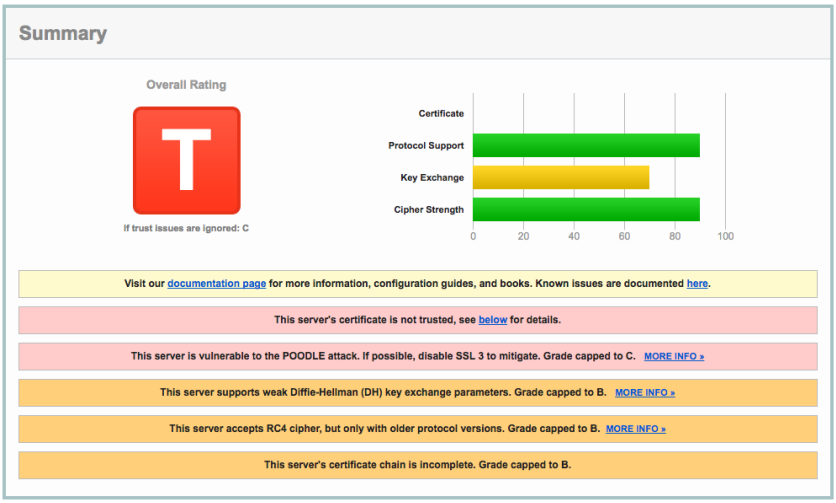


(source)

With Qlik products we rely almost entirely on other vendors, in example Microsoft for it's Windows Server platforms.

A default Windows Server 2012 R2 / 2016 / 2019 installation with a default Qlik Sense Enterprise for Windows installation is nothing to write home about regarding security. By using external tools like the reputable SSL Labs Server Test for doing analysis of the certificate and configuration we can get an idea about how secure the server is. It's not everything, but it's a good starting point for sure.

So, how do we get from this awkward default rating, to something we can actually leave the customer with? Ultimately we would like to aim for an A+ or at least an A rating.



⚠ **Note:** This guide is not a replacement for analysis or guidance from an organization's security team. The aspects of a Qlik Sense Enterprise for Windows deployment which may raise red flags can vary wildly between organization. So close collaboration with the organization's security teams(s) is encourage.

Authentication

As of modern versions of Qlik Sense Enterprise for Windows (June 2017 and newer), the following authentication methods are supported:

- Windows
- Kerberos
- Header
- Ticketing
- SAML
- JWT
- Anonymous

We cannot specify which authentication method is appropriate for each deployment. For an in-depth analysis, do review the use case and involve the relevant teams inside of Qlik (Enterprise Architecture, Consulting Services, etc) or with a partner organization. That being said, SAML is the most attractive option if available. Use of SAML allows for an organization to leverage potentially sophisticated authentication options available at the Identity Provider (IdP) like NotOnOrAfter and/or NotBefore on the SAML assertion, Multi-factor authentication (MFA), or geographic restrictions. Many of these style of features could be engineered for integration with another authentication mechanism like Ticketing, but re-use of existing investments in identity management is encouraged.

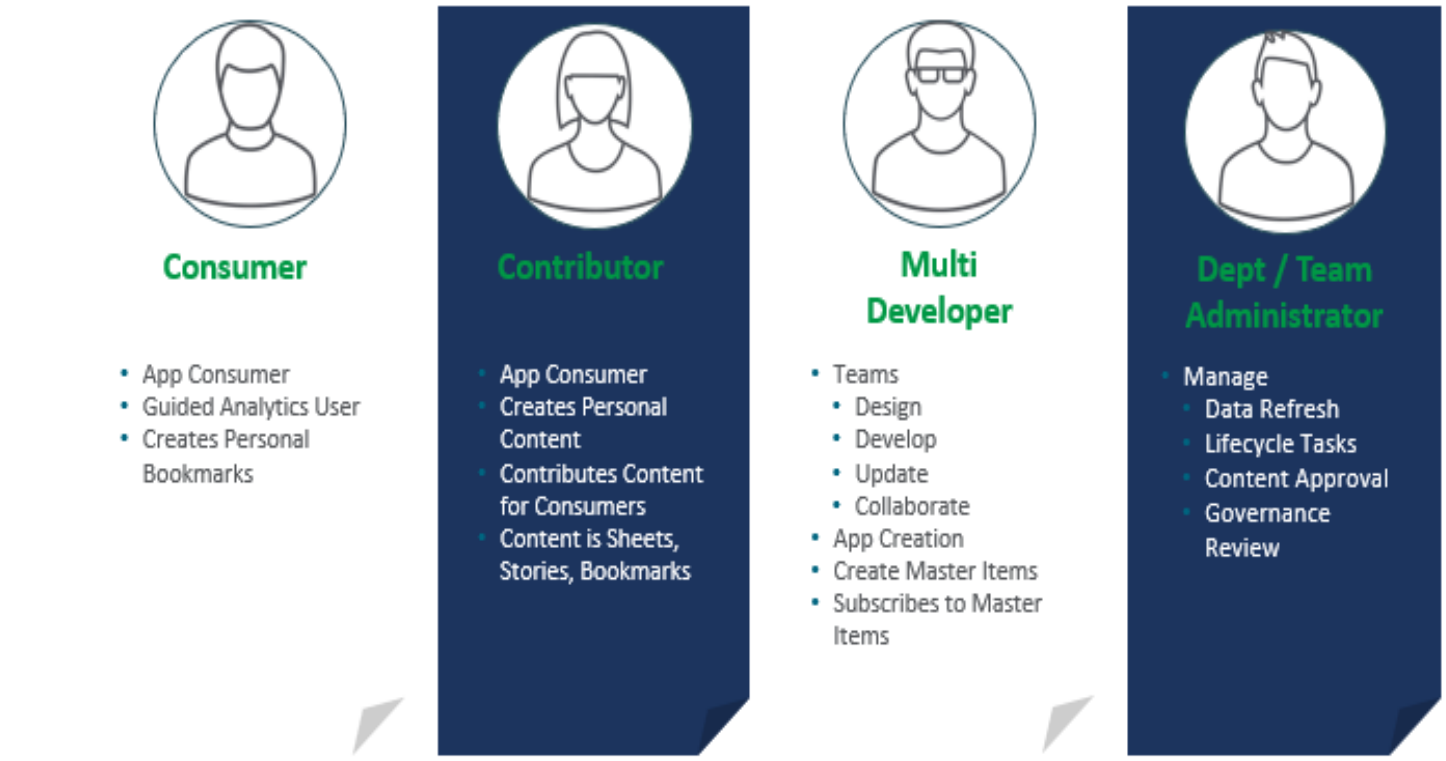
Authorization

Qlik Sense Enterprise for Windows offers two levels of authorization inside of its product: attribute-based access control (also called security rules) and row level data reduction (called section access).

Security Rules

Pages / Levi Turner's Home

This guide will not do an exhaustive review of security rules, but the high-level recommendation is to begin thinking of your users based on the capabilities that you intend to provide them. For example:



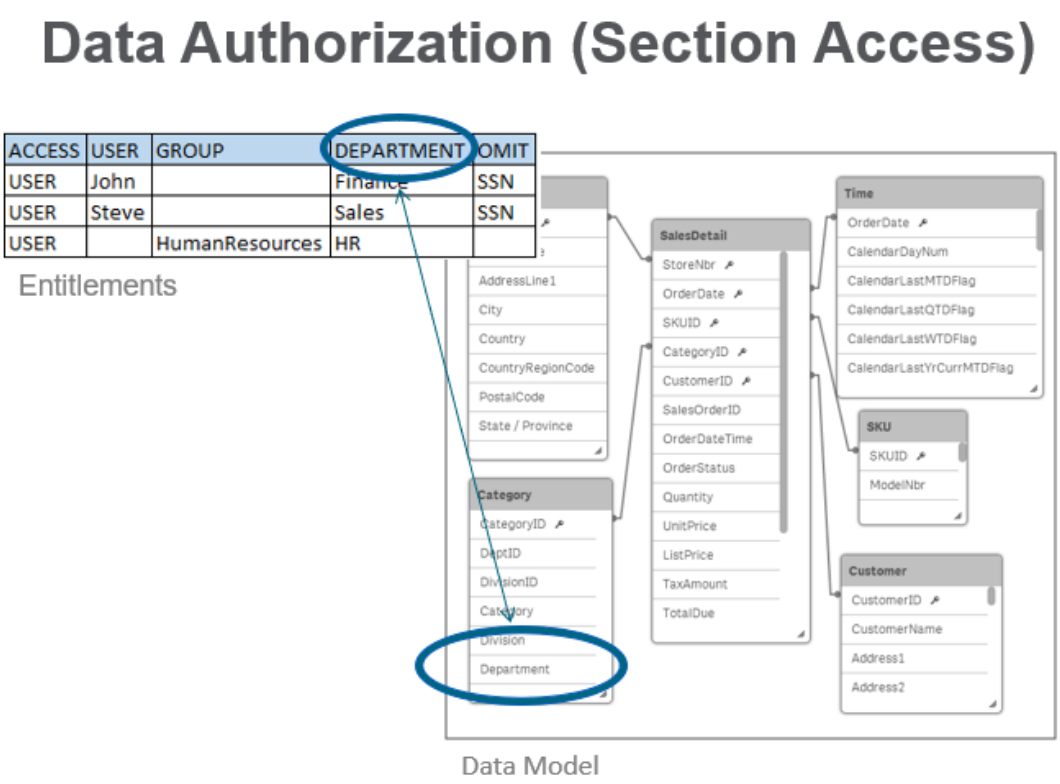
With this back-drop, a security rule framework can be designed, either by the customer by referencing the documentation and available assets or by engaging with a Qlik Consultant or Partner for guidance.

For guidance on security rules:

- Help.qlik.com
- A primer video

Section Access

This guide likewise will not exhaustively review section access. The gist of section access it that is allows a developer to define which rows each individual should be entitled to inside of an application with a shared data model:



Review available documentation for further guidance.

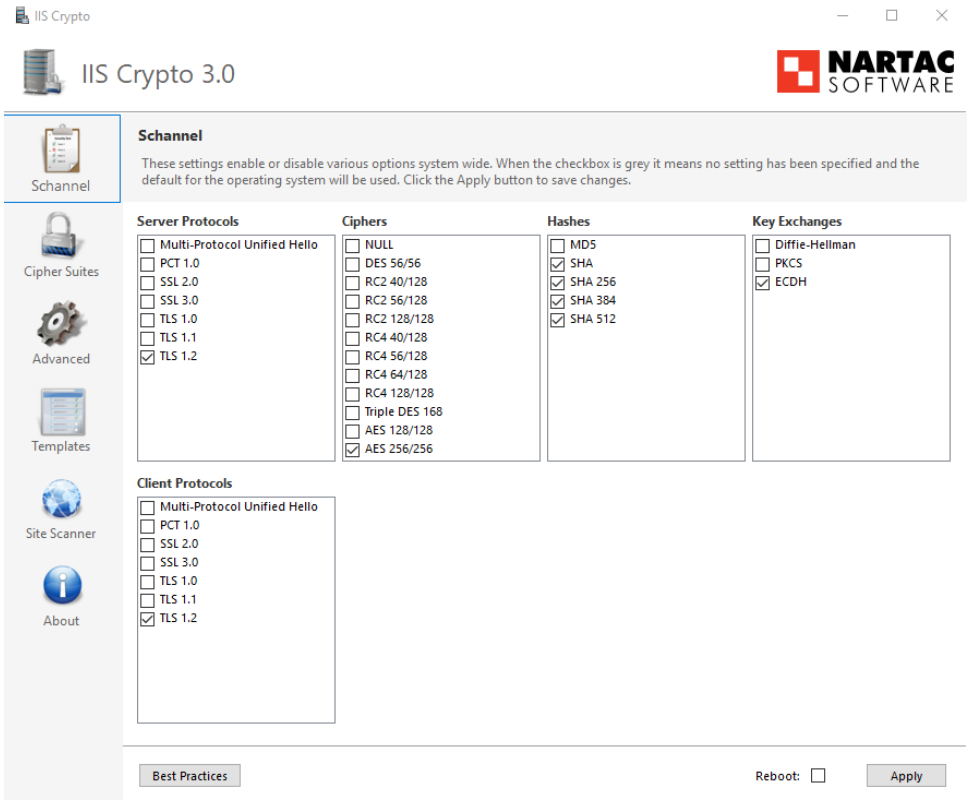
Operating System Hardening

Qlik Sense Enterprise for Windows inherits the available protocols, cipher suites, key exchanges, etc which are enabled on the Windows Server Operating Qlik Sense.

Step 1: Disabling protocols

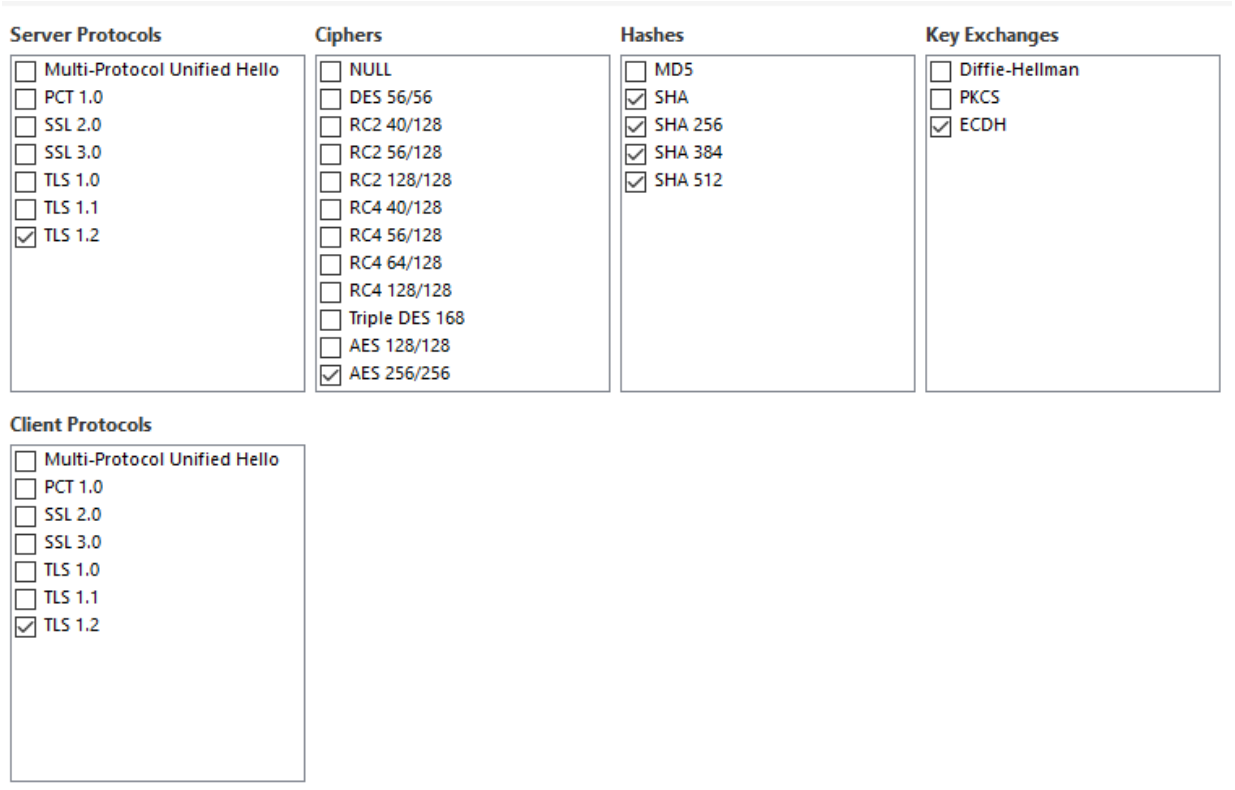
By default in Windows a lot of protocols are enabled by default, among others the quite heavily bashed and insecure SSLv3 causing the Poodle vulnerability (hysteria) a few years ago. We should disable protocols, ciphers, hashes and key exchanges that are considered deprecated or not secure enough these days. There are many ways of doing this, but for simplicity, understanding and a good overview IIS Crypto 3.0 is a good tool for this purpose. This tool is an easy tool for non security personnel to interact with the underlying Windows registry values. Each organization is encouraged to reach out internally to determine whether there are organizationally vetted scripts or hardening procedures for Windows Servers available. They are usually written in PowerShell like this script.

IIS Crypto also has a "Best Practice" button that can be quite handy. The problem with this is that things change, what was considered "safe" a while ago is not necessarily considered so today. This is also the reason why this work is never really done or finished. It's best practice to regularly scan servers for potential vulnerabilities. It's in the customers interest, and it's in our interest.



The selections we want to keep is as in the screenshot above.

1. For protocols we can now disable the deprecated TLS versions and only keep TLS 1.2.
2. For ciphers let's only keep AES 256 here.
3. Hashes remains the same as above, we only disable MD5.
4. For Key Exchanges we only keep ECDH.



When the settings are applied the server needs to be restarted for the changes to take effect everywhere.

Pages / Levi Turner's Home

Step 2: Firewalls

Firewalls should of course be closed, there's not much more to say about it really. For a publicly available server on the Internet **ONLY** port 443 needs to be open. For a multi-node architecture, refer to the documentation corresponding to the build of Qlik Sense Enterprise for Windows that you are installing to ensure coverage for needed ports between nodes.

Step 3: Service Account Permission

Local Admin Rights

Qlik Sense Enterprise for Windows does not require local administrator rights in order to function. This can be an attractive option inside some organization. This will require additional configuration, so do review available documentation for guidance. For most organizations, local administrator rights allow for an easier deployment but it not required.

Group Managed Service Accounts (gMSA)

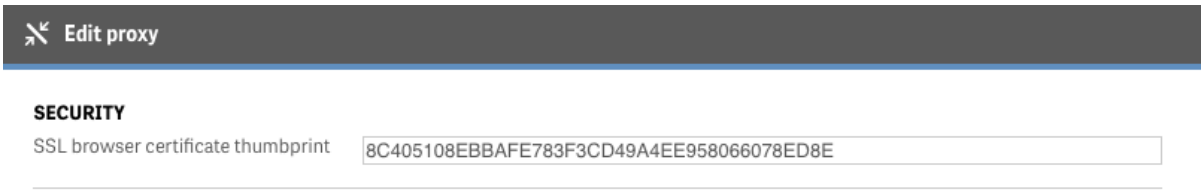
While Qlik Sense Enterprise for Windows does not officially support Group Managed Service Accounts, it can operate using one. The initial barrier is that the installer requires a service account and password to be entered during installation. A domain or local account could be substituted for the install stages only to be swapped out in the Windows Services applet (services.msc) after installation. Some functionality may require work-arounds (e.g. A User Directory Connection to Active Directory).

Generalized Web Server best practices

The Proxy Service bundled with Qlik Sense Enterprise for Windows is simply a web-server. This means applying general practice guidance but in the context of Qlik's web server.

Step 1: A proper certificate

The first thing we need is a of course a proper certificate to enable the customer to actually use HTTPS. The self-signed certificate we ship the product with in a default installation is not aimed for production use! If the customer does not have or want to use a proper certificate and the environment is entirely internal, feel free to enable HTTP and use that instead. If the server is publicly available on the Internet, a proper certificate should be used, HTTP should be disabled and HTTPS the only way to access the server.



As of July 2019, Qlik Sense Enterprise for Windows supported SHA1 and SHA2 certificates. If SHA384 or SHA512 certificates are needed, then a network application or appliance can be configured in front of Qlik Sense which offloads to Qlik Sense.

Optional: HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement which any web application can support through the use of a special response header. When a supported browser receives this header that browser will prevent any communication sent over HTTP in the future and will redirect all traffic over HTTPS instead. This sounds like a very nice idea and something that we might want. You need to be cautious about this though as you might block HTTP access to certain pages that actually requires it or needs to be excluded from this. The response header can be configured in different ways, here are some examples:

Pages / Levi Turner's Home

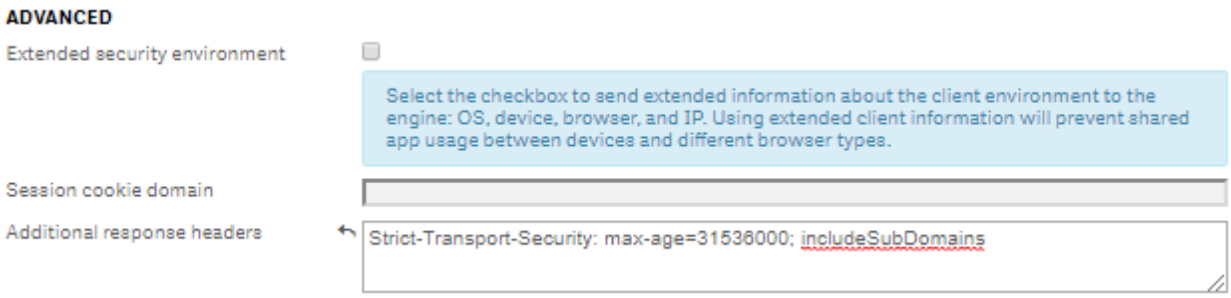
```
Strict-Transport-Security: max-age=31536000
```

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

When testing this, make sure to set a short max-date in case you make a mistake, when you have tested that it works as it should you can increase the value to like 1 year (max-age: 31536000) or 6 months (max-age: 15768000). Max-age is defined in seconds. As you can see the difference between these examples is the *includeSubDomain* directive which would block just about everything in the domain, so better be careful with it and confirm with the customers IT/security department before using it.

There is also a possibility to send a *preload* directive but then you **really** need to know what you're doing, read more about that here before enabling it, and again please advise with customer IT/security department.

In Qlik Sense we add any additional HTTP response headers we want to use in the Virtual Proxy configuration.

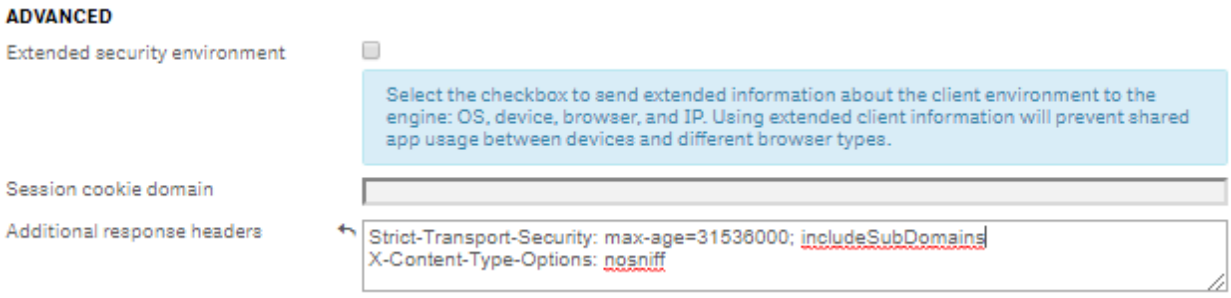


Optional: X-Content-Type-Options

The X-Content-Type-Options response HTTP header is a marker used by the server to indicate that the MIME types advertised in the Content-Type headers should not be changed and be followed. This allows to opt-out of MIME type sniffing. Here is an example of the header:

```
X-Content-Type-Options: nosniff
```

Like with the HSTS header, add it to a new line in the Advanced section of the Virtual Proxy that you seek to harden:



Optional: Additional HTTP Response Headers

There are numerous HTTP response headers that can be used in attempting to secure a server. Above are two of the most important ones, and in this section I will briefly cover a few others.

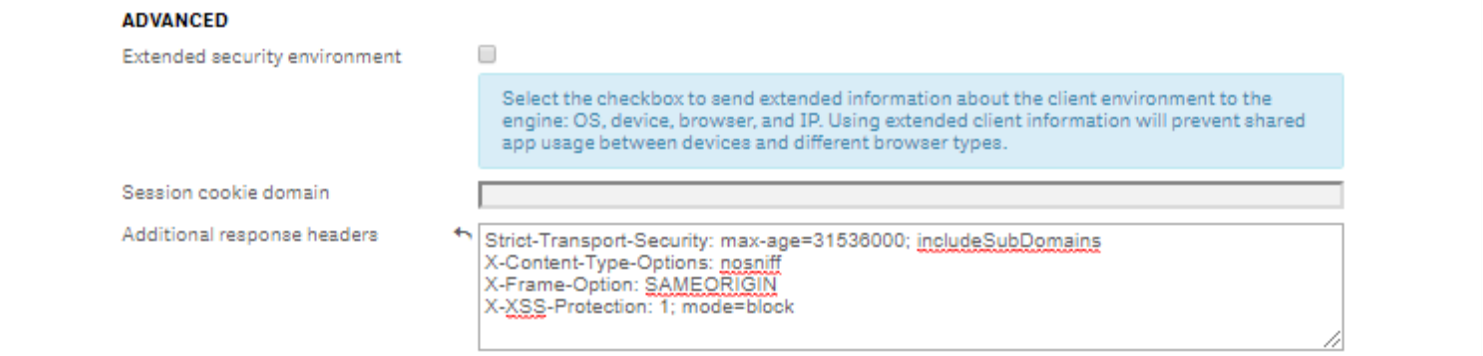
When trying different security headers I would recommend creating a new Virtual Proxy as "backup" in case you mess up, which is very easy to do when trying to lockdown something. Without an alternative way of accessing QMC it might become necessary to poke around directly in the PostgreSQL database in order to get things working again. Virtual Proxy configurations are located in the table *VirtualProxyConfigs* and the field for the response headers is called *AdditionalResponseHeaders*.

X-Frame-Options will prevent that someone puts our site in an iFrame from somewhere else, this is useful to improve security against Clickjacking where you are fooled into clicking somewhere you shouldn't.

```
X-Frame-Options: SAMEORIGIN
```

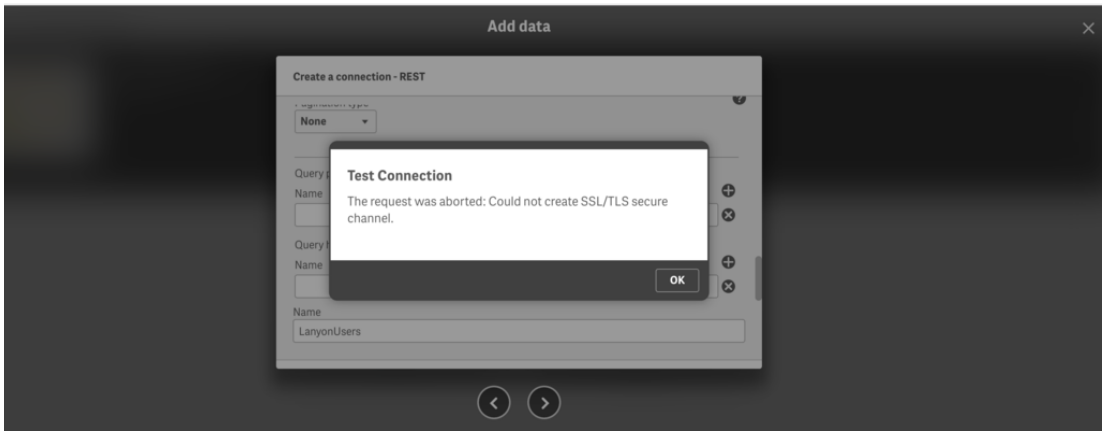
X-XSS-Protection improves security against some types of XSS (cross-site scripting) attacks.

```
X-XSS-Protection: 1; mode=block
```



Be Aware

If you lock down the servers very hard, you might want to be aware of certain situations that could occur if for example trying to load data from external sources, if a REST API on another server for example is not as tightly secured as your server they might end up in communication problems with each other, as you have actually disabled any common protocols and ciphers between the servers.



Network Appliances / Applications

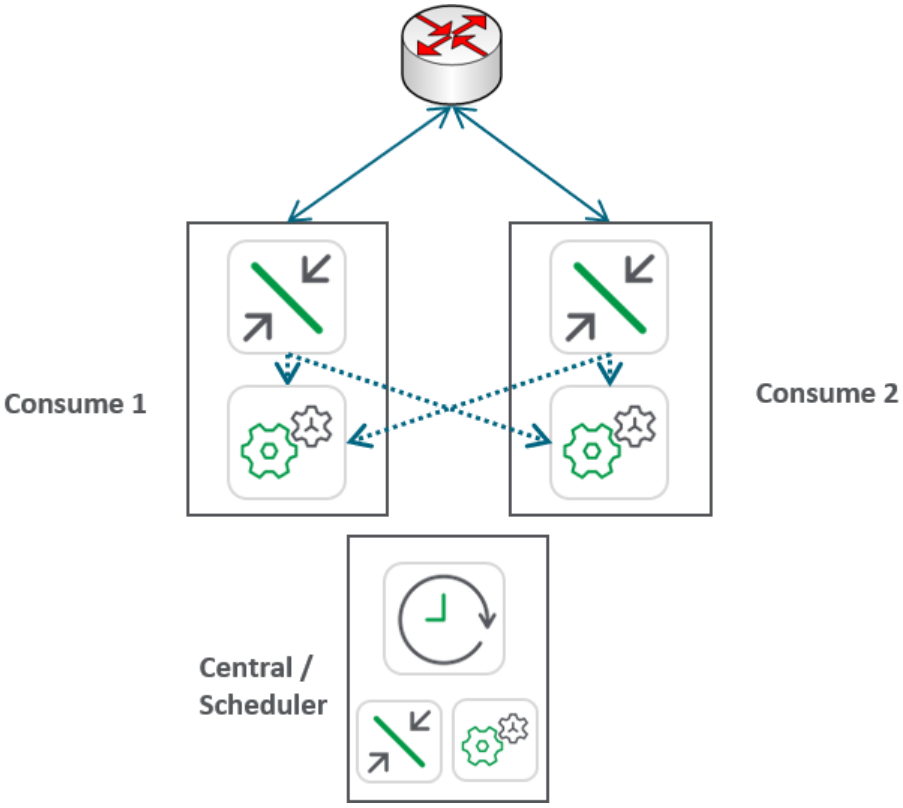
Qlik Sense Enterprise on Windows has no known incompatibilities with network applications or appliances (i.e. load balancers, reverse proxies, web application firewalls) provided that those devices support:

1. WebSockets
2. Sticky Sessions / Persistent connections between the device and a given Qlik Sense Proxy node

(1) is a hard requirement for Qlik Sense Enterprise as the delivery of the data inside of an application is through a WebSocket tunnel between the end user and the server. Most modern devices support WebSockets, either out of the box or with some additional configuration.

For (2), this is needed due to the Qlik Sense Proxy service being stateful. Session states are not shared between Qlik Sense [illegible] in a simple architecture:

Pages / Levi Turner's Home

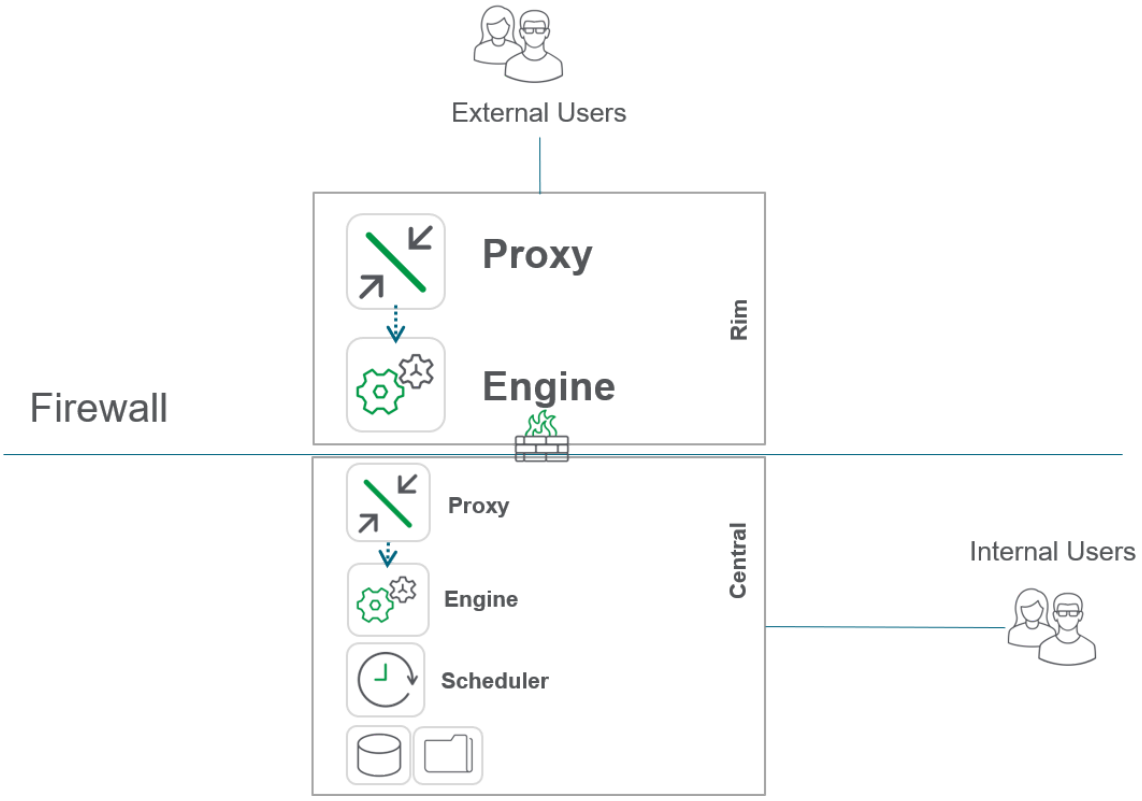


Upon accessing the Qlik Sense site through the network appliance / application, they are routed to a Proxy Service on either Consume 1 or Consume 2. After successfully authenticating, the user's session needs to remain on Proxy Service which initially handled the request in order to ensure that the user does not need to re-authenticate.

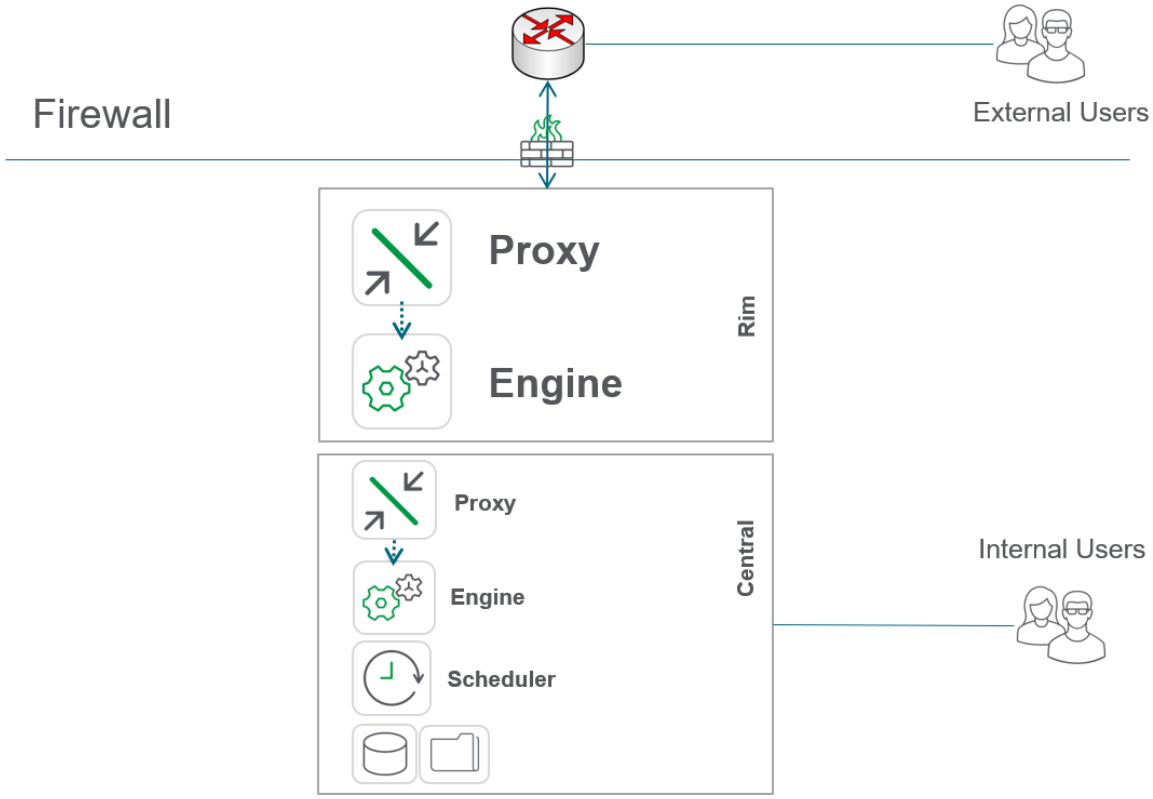
The precise configuration for (1) and (2) in this section varies by device so this guide will not instruct on the mechanics here. Consultant with the team(s) inside of an organization who support the device or devices is encouraged.

Qlik Specific Guidelines for External Audiences

When designing an architecture to support external audiences, network appliances or applications to route users inside of an organization's firewall is encouraged. This is needed due to each Qlik Sense node needing access to a common SMB share which hosts Qlik Sense applications, associated web files used in Qlik apps (e.g. thumbnail images, extensions), and is the location which log files are archived at. Using this example architecture as a reference of how many applications would be architected:



This design would require the SMB share which is hosted on the Central node to be exposed to the Rim node which lives in the DMZ, in addition to a number of ports used by Qlik Sense Enterprise on Windows. This requirement is not encouraged from the Qlik side due to security implications of SMB traffic being allowed through an edge device entering a network. An alternative architecture which is conducive to the requirements of Qlik Sense Enterprise while also segregating consumption of applications for an external audience would be as follows:



These architecture diagrams are not intended to be recommendations for all use cases so consultation with your Qlik account team or partner is encouraged.