WHITE PAPER

Qlik Sense in US Federal Environments

Considerations necessary for a successful implementation

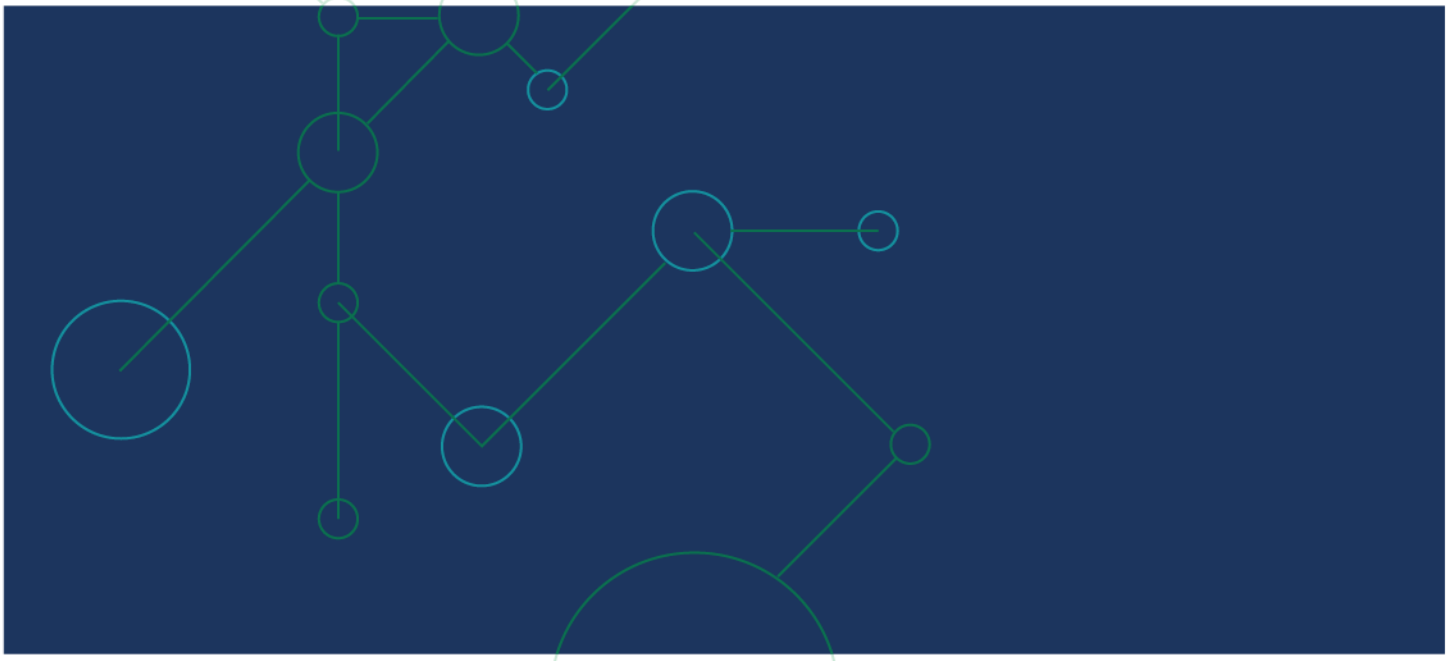


TABLE OF CONTENTS

Summary and Introduction 2

Antivirus Exclusions 3

Qlik Sense and FIPS 3

Hardening a Qlik Sense Server 8

CAC Implementation 8

Qlik Accessibility and 508 Compliance 8

Authority to Operate (ATO) 9

Reporting a Security Vulnerability 9

Qlik and FedRAMP 9

SUMMARY

- US Federal Customers have specific requirements for running Qlik Sense in their environments
- Considerations are listed out and provided as links to articles written about handling these issues

INTRODUCTION

At Qlik, we have seen that our US Federal customers consistently have many of the same requirements when it comes to installing and operating Qlik Sense in a Federal environment. This document is designed to provide references for these considerations and how to handle each.

A brief overview is provided for each topic, along with links to relevant materials for further detail. Together, these should help guide customers along the path of successfully installing and implementing Qlik Sense in US Federal environments.

Antivirus Exclusions

To eliminate the chance that antivirus and anti-malware will cause corruption or lock up files in the Qlik environment, or cause issues during an installation/upgrade/patch, some folders should be excluded from live scanning.

Additional impact of virus scans locking Qlik related files can result in loading and refresh failures as well as performance issues.

- Antivirus exceptions for Qlik Sense - McAfee, Symantec & other antivirus exclusions absolutely required: https://support.qlik.com/articles/Basic/Antivirus-exceptions-for-Qlik-Sense-McAfee-Symantec-Other-Anti-Virus-exclusions-absolutely-required
- Qlik Sense folder and files to exclude from antivirus scanning: https://support.qlik.com/articles/Basic/Qlik-Sense-Folder-And-Files-To-Exclude-From-Anti-Virus-Scanning

Qlik Sense and FIPS

This section will describe how to successfully implement Qlik Sense Enterprise in an environment with the FIPS security policy enabled.

What is the FIPS Security policy on Windows?

The FIPS security policy in Windows forces the use of only FIPS-validated (FIPS 140) cryptographic algorithms - both by disabling cipher suites available to the OS and by restricting the algorithms available to Windows frameworks like .NET.

Why does the FIPS Security policy interact with Qlik Sense?

When the FIPS security policy is enabled, the .NET framework, which Qlik Sense utilizes for several of its key services, can only use algorithm implementations which are certified by NIST to be FIPS 140 compliant.

Qlik Sense only uses FIPS compliant modules for encryption. Qlik Sense uses non-approved algorithms only for non-cryptographic operations. For example, checking the hash of a file for changes.

Should you run Qlik Sense in an environment with FIPS?

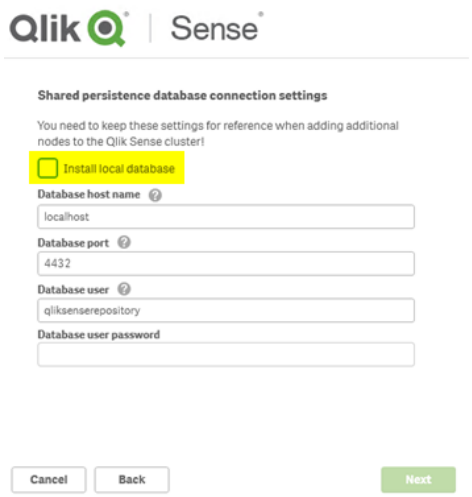
The answer to this question is yes, if FIPS is required. Qlik Sense can operate in an environment where FIPS is enabled, albeit requiring additional configuration. The key question for an administrator of a Qlik Sense site is whether FIPS is required due to regulatory or compliance factors for the organization. If FIPS is not required, then it is recommended to turn off FIPS due to the complexity and vigilance needed to configure Qlik Sense to operate in a FIPS environment. If FIPS is required, then continue reading for guidance on how to successfully configure Qlik Sense to interact with FIPS.

Microsoft's Statement about FIPS

In June 2019, Microsoft released a statement that they are no longer recommending FIPS Mode anymore. You can read that statement here: https://techcommunity.microsoft.com/t5/microsoft-security-baselines/why-we-8217-re-not-recommending-8220-fips-mode-8221-anymore/ba-p/701037

Installation

During the initial installation of a Central node for Qlik Sense, there is toggle option which specifies whether the Central node will install a local database or connect to a remote database:



If this toggle is selected, then the installation will proceed normally without issues.
After installation, the Qlik Sense Repository Service will fail to initialize successfully. To resolve this roadblock, you will need to edit the configuration files for the following Qlik Sense Services:

- Qlik Sense Printing Service
- Qlik Sense Proxy Service
- Qlik Sense Repository Service
- Qlik Sense Scheduler Service

1. Determine the installation path for Qlik Sense
    - The default installation path is C:\Program Files\Qlik\Sense
2. Open Notepad (or your preferred text editor) with administrative rights
3. Open each .config file for the services listed above
    - Default paths:
        i. C:\Program Files\Qlik\Sense\Printing\Printing.exe.config
        ii. C:\Program Files\Qlik\Sense\Proxy\Proxy.exe.config
        iii. C:\Program Files\Qlik\Sense\Repository\Repository.exe.config
        iv. C:\Program Files\Qlik\Sense\Scheduler\Scheduler.exe.config
4. Edit the config file to include a key to disable FIPS policy checking (outlined below)
5. Save the config file
6. Restart Qlik Sense Services

While the specific structure of each config file will vary between service and potentially between versions of Qlik Sense, there is a high-level schema:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <runtime>
  <appSettings>
    Some Stuff
  </appSettings>
    Some other stuff
  </runtime>
</configuration>
```

The administrator will need to add an additional key (`<enforceFIPSPolicy enabled="false"/>`) before the closing runtime tag (`</runtime>`) like so:

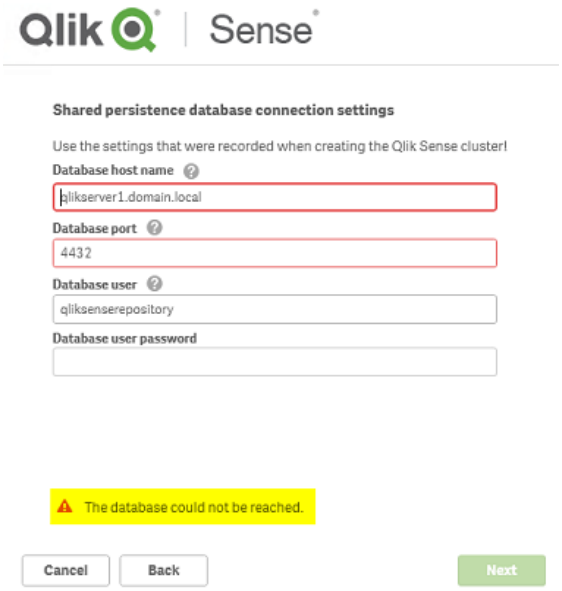
```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <runtime>
  <appSettings>
    Some Stuff
  </appSettings>
    Some other stuff
  <enforceFIPSPolicy enabled="false"/>
  </runtime>
</configuration>
```

If there is no runtime tag present, then write an open tag, add the `enforceFIPSPolicy` key and close the tag like so:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    Some stuff
  </appSettings>
  Some other stuff
  <runtime>
    <enforceFIPSPolicy enabled="false"/>
  </runtime>
</configuration>
```

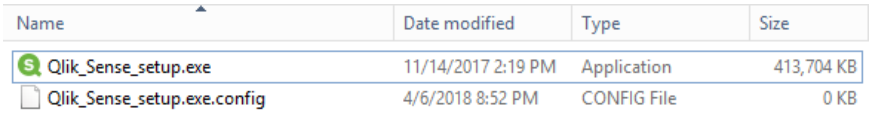
Installation against a remote PostgreSQL database

During install of Qlik Sense, there is a toggle option which allows an administrator to install Qlik Sense against a remote database. This configuration can be used when installing a Central or RIM node. When using this configuration option in a FIPS environment, the installer will be unable to validate the remote database.

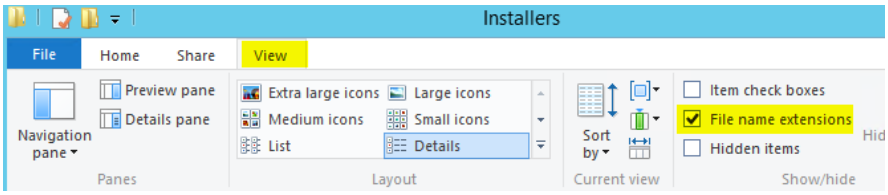


This is due to a dependency in the installer which does not support FIPS. To successfully install Qlik Sense against a remote database, the following needs to be done:

1. Close the installer
2. Create a text file in the same directory as the installer EXE
3. Rename the file to have the same name as the EXE with a file extension of .config like so:



- **Note**: By default, Windows Server 2012 and 2016 hide file name extensions, so be sure to enable file name extension display to ensure that the newly named file is named appropriately:



4. Open the file
5. Save the file with this structure:

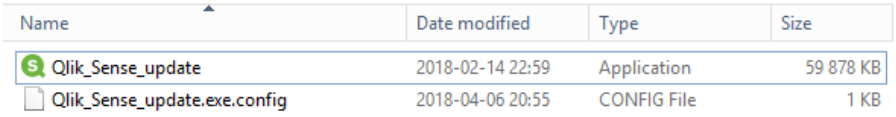
```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <runtime>
        <enforceFIPSPolicy enabled="false" />
    </runtime>
</configuration>
```

6. Launch the installer again and proceed through the configuration options

Update / Patch Process

The process for applying update or patch packages is a slight variation of the process of installing Qlik Sense against a remote Repository database:

1. Create a text file in the same directory as the update EXE
2. Rename the file to have the same name as the EXE with a file extension of .config like so:



- **Note**: By default, Windows Server 2012 and 2016 hide file name extensions, so be sure to enable file name extension display option to ensure that the newly named file is named appropriately

3. Open the file
4. Save the file with this structure:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <runtime>
        <enforceFIPSPolicy enabled="false" />
    </runtime>
</configuration>
```

5. Launch the installer

Upgrade Process

The process for upgrading Qlik Sense to a different version is the same as the initial setup process. Do note that the changes to the config files which were made initially to the Qlik Sense Printing, Qlik Sense Proxy, Qlik Sense Repository, and Qlik Sense Scheduler services may be removed so an administrator will need to repeat the changes to the .config files for those services.

Hardening a Qlik Sense Server

Server hardening is the process of using a set of disciplines and techniques to improve the security of a server, which is usually necessary in a Federal server deployment. There are many considerations for doing this effectively in Qlik Sense, and these are called out in this support article: https://support.qlik.com/articles/000089479

CAC Implementation

A common requirement for DoD customers is integration with Common Access Card (CAC) authentication. Qlik can integrate with CAC and nearly all DoD customers have implemented this type of configuration. Below are links to guides on how to set up CAC authentication in your environment:

- https://community.qlik.com/t5/Qlik-Sense-Documents-Videos/CAC-Authentication-Setup-Step-by-Step-Guide/ta-p/1508082
- https://community.qlik.com/t5/Qlik-Sense-Documents-Videos/CAC-Authentication-and-Qlik-Sense-pdf/ta-p/1492691

Qlik Accessibility / 508 Compliance

Over the past several years, Qlik has worked hard to make Qlik Sense more accessible to those with impairments. You can read about Qlik and Accessibility here: https://www.qlik.com/us/trust/accessibility.

Additionally, you can watch a video on some of the ways Qlik has made our product accessible to those who need it here: https://community.qlik.com/t5/Qlik-Design-Blog/Qlik-Sense-Accessibility/ba-p/1476193

Authority to Operate (ATO)

Qlik Sense Enterprise is listed on the Air Force Network Integration Center (AFNIC) Evaluated Products List. Qlik Sense Enterprise also has an Authority to Operate (ATO) with the Army, Navy, Air Force, Marine Corps, and other Intelligence and Defense Agencies: https://www.qlik.com/us/trust

DOD STIG ATOs

Security Technical Implementation Guide (STIG) is a set of DOD IA controls, security regulations, and best practices for securing an IA or IA-enabled system (operating system, network, application software, etc.). STIG provides guidance for such actions as mitigating insider threats, containing applications, preventing lateral movements, and securing information system credentials.

Qlik Sense Enterprise on Windows has gone through STIG assessments by several programs within the DOD. For more details on which programs have done this, contact your program ISO.

Reporting a Security Vulnerability

Qlik takes product security seriously. A dedicated team of security experts work on continuously testing, hardening, and securing all Qlik products. Should you need to report a suspected security vulnerability, please follow the instructions here: https://support.qlik.com/articles/000019159

Qlik and FedRAMP

Qlik currently has a commercial offering for a cloud product called Qlik Sense SaaS. Qlik is currently pursuing FedRAMP certification for this offering to provide our Federal customers a full SaaS experience. However, Qlik Sense Enterprise on Windows, Qlik's customer managed version of Qlik Sense, can operate in a FedRAMP cloud environment. There are currently over 25 customers that are running Qlik Sense Enterprise on Windows in a FedRAMP IaaS environment under their own agency ATO.

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

Qlik LEAD WITH DATA