

SECURITY OVERVIEW

This White Paper provides a comprehensive understanding of the formidable security measures integrated into Mail & Deploy software. Encompassing essential principles, proactive threat mitigation, compliance adherence, user authentication, and continuous monitoring, this document outlines a strategic and thorough approach to safeguard against evolving threats. It mirrors Mail & Deploy's unwavering commitment to transparency, accountability, and excellence in guaranteeing the confidentiality, integrity, and availability of our customers' critical data.



TABLE OF CONTENT

About Mail & Deploy	1
Introduction	2
Security Overview	3
Access to Mail & Deploy	4
Access to Data	7
Report Execution and Distribution	9
Component Communication	11
Report Development	12
Report Storage	12
Conclusion	13

ABOUT MAIL & DEPLOY

Mail & Deploy serves as a third-party component seamlessly integrated into the Qlik platform, specializing in the efficient distribution of meticulously crafted reports in universally compatible formats. These reports are generated by extracting data from applications deployed with QlikView, Qlik Sense, or Qlik Sense Cloud.

Empowering users with versatile functionality, Mail & Deploy facilitates scheduled deliveries of reports to designated recipients. Additionally, it offers interactive options for on-demand retrieval by users. This can be achieved through Mail & Deploy extensions tailored for Qlik Sense or via a personalized login within the Mail & Deploy Hub, ensuring a flexible and user-centric reporting experience.

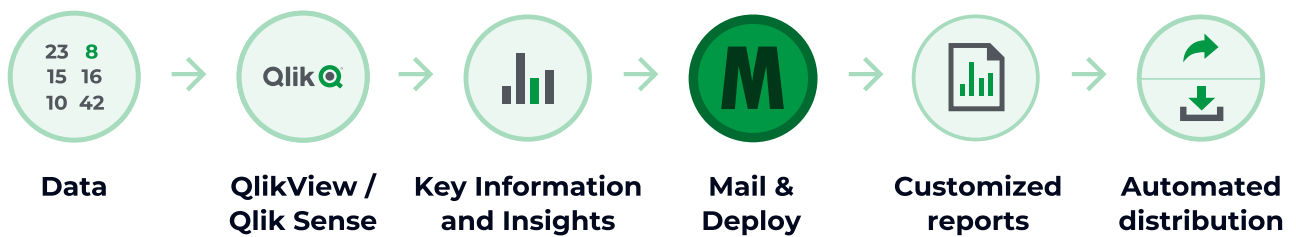


Figure I: Mail & Deploy platform

INTRODUCTION

Mail & Deploy stands as a robust software component, ensuring security through the utilization of third-party security frameworks in conjunction with the inherent Qlik security framework embedded within QlikView, Qlik Sense, and Qlik Cloud. Its comprehensive capabilities span access management, authentication, authorization, and meticulous data governance.

- Functioning as a Windows-based reporting suite, Mail & Deploy adheres to standard security protocols, enabling centralized control and streamlined provisioning of access to reports.
- User authentication within Mail & Deploy occurs seamlessly through web clients, with the flexibility of selecting from various authentication providers, including Windows, Azure AD, OIDC-identity providers, or the built-in Mail & Deploy authentication. For user management, Mail & Deploy facilitates external management through LDAP and other third-party repositories, ensuring synchronization at scheduled intervals.
- User roles and permissions are intricately defined within Mail & Deploy, delineating each user's capabilities based on specific user types and permissions.
- Reports are generated securely by establishing connections to QlikView, Qlik Sense, and Qlik Cloud applications, employing secure channels for data retrieval. Authentication to QlikView and Qlik Sense is handled through a Windows-based service account, while an API Key is employed for connectivity to Qlik Cloud.
- Customization is at the forefront, as Mail & Deploy Reports offer dynamic filtering options for individual recipients. Centralized management of reports is facilitated, with editing performed through the Mail & Deploy designer, necessitating a secure live connection to the Mail & Deploy Server, ensuring the integrity and confidentiality of the reporting process.

SECURITY OVERVIEW

Network Security:

Mail & Deploy prioritizes the security of its communication channels, employing web protocols with Transport Layer Security (TLS) to ensure the confidentiality and integrity of all exchanges between Mail & Deploy services and web clients. TLS relies on digital certificates to encrypt information, offering a robust layer of protection for data transmitted among services, servers, and clients.

Server Security:

The security architecture of the operating system plays a pivotal role in safeguarding Mail & Deploy. Access controls are implemented meticulously to regulate entry to certificates, file-based storage, memory, and CPU resources. By strictly permitting authorized users and processes access to necessary resources, Mail & Deploy fortifies its suite against potential threats.

Process Security:

Mail & Deploy undergoes a thorough and rigorous testing phase during development to pre-emptively address security vulnerabilities and effectively handle unforeseen events. Continuous testing further validates Mail & Deploy's resilience against well-known security threats, ensuring the software's robustness and reliability.

Qlik App Data Security:

Mail & Deploy aligns closely with the access control settings defined in QlikView, Qlik Sense, and Qlik Cloud to govern its ability to extract data from Qlik applications and distribute it to recipients. This meticulous alignment ensures that Mail & Deploy adheres strictly to user entitlements, granting access only to the data that users are authorized to view. This approach reinforces data security and confidentiality throughout the entire reporting process.

ACCESS TO MAIL & DEPLOY

Users gain access to the Mail & Deploy Management Console and Mail & Deploy Hub through secure sessions established with the Mail & Deploy web engine over HTTPS. This web engine, an exclusive HTTP server running on the Mail & Deploy server, ensures a secure environment for user interactions.

User authentication within the Mail & Deploy web engine is carried out seamlessly through Windows, Azure AD, or OIDC-Identity providers. The versatility of Mail & Deploy is underscored by its support for multiple security providers concurrently. Configuration of these security providers occurs within the Mail & Deploy Management Console, administered by an administrative user.

For OIDC-Identity providers, predefined settings for the certificate, header, and payload are essential in the Mail & Deploy Web Console. Users opting for this authentication method need to provide their own certificate for configuration.

Prior to accessing the Mail & Deploy Web Engine, users must be defined within the Mail & Deploy Management Console or synced from an external user repository. Additionally, users must be associated with at least one Mail & Deploy User Role, dictating their access levels within Mail & Deploy.

User synchronization is a seamless process, supporting various formats such as XML, CSV, LDAP, and Azure AD. This synchronization can be scheduled or externally triggered, ensuring updates to Mail & Deploy User Types and Permissions align with the latest user data. This meticulous approach not only bolsters security but also streamlines user management in Mail & Deploy.

Mail & Deploy User Types

The three default User Types are: Administrators, Standard Users and API Users.

An administrator can grant permissions to fine tune which Mail & Deploy users can access and/or customize the level of capability on specific components of the applications and access to administrative features.

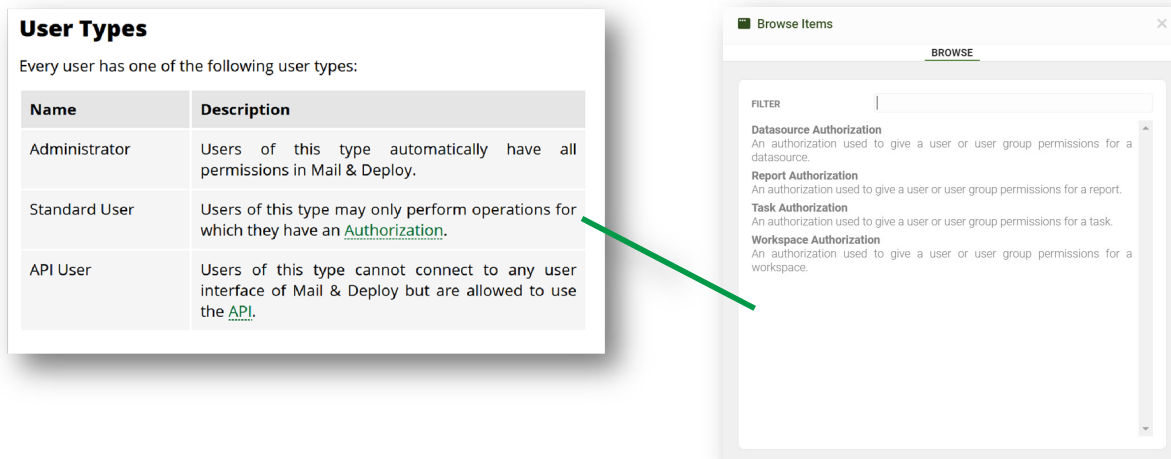


Figure II: Mail & Deploy User Types

Mail & Deploy Permissions

Prior to using Mail & Deploy Management Console or Mail & Deploy Hub, each user (except Admins) must be granted permissions.

Permissions define:

- Access to user definitions and administrative features
- Access to Data sources
- Access to Mail & Deploy workspaces
- Access to Mail & Deploy reports
- Access to Mail & Deploy tasks
- Actions (level of access per application component)

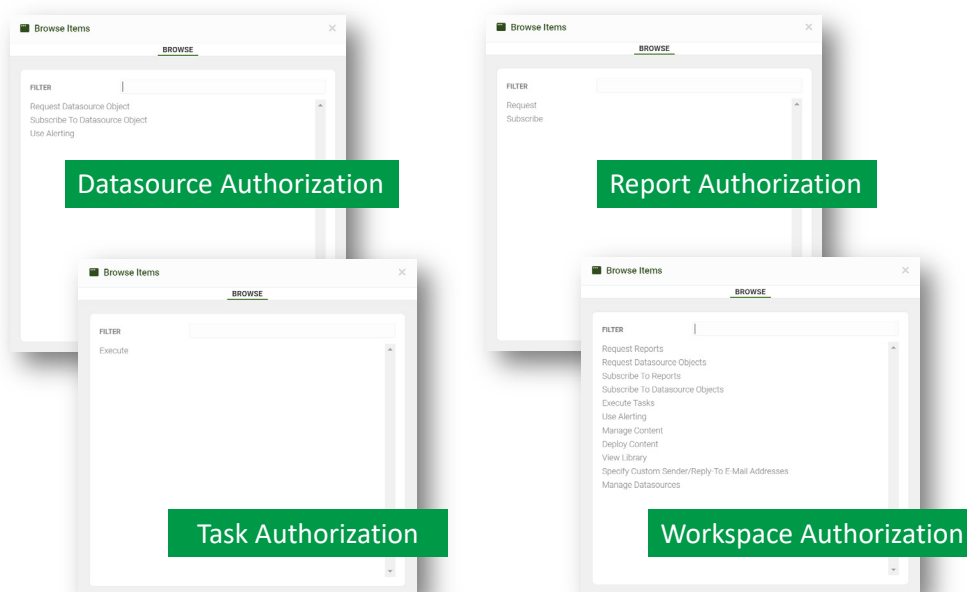


Figure III: Mail & Deploy Permissions

Mail & Deploy Workspaces

Workspaces are the main logical unit of organization for Mail & Deploy content.

A Mail & Deploy Workspace contains:

- Datasources
- Reports
- Tasks
- Alerts
- Subscriptions
- Value Tables
- Deployments
- Authorizations

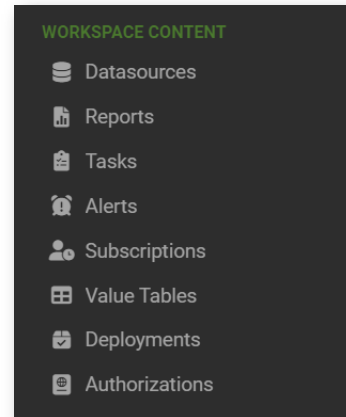


Figure IV: Mail & Deploy Workspace

It gives details about the connection to QlikView, Qlik Sense, Qlik Cloud and other Databases, their Apps/QVW's, Report definitions, Task definitions, Value Tables and more.

By securing access to Mail & Deploy Workspaces, Mail & Deploy user types govern the access to all content as well as the level of interactions that are permitted to administrators, developers and users.

Here are some examples of how User Types control access and use cases:

Target Type ^	Target	Resource Type	Resource	Permission(s)
User Group	Regional Mgrs	Report	01 Regional Sales Report	Request, Subscribe
User Group	Sales Rep	Report	02 Sales Rep Analysis Report	Request, Subscribe
User Group	Regional Mgrs	Workspace	M&D Demo - Qlik Tour	View Library
User Group	Sales Rep	Workspace	M&D Demo - Qlik Tour	View Library
User Group	Development	Workspace	M&D Demo - Qlik Tour	Manage Content

Figure V: Mail & Deploy Access Control

When a user logs into the Mail & Deploy Management console, the user's authenticated identity is used to lookup the security role memberships and establish what a use can and cannot do.

The following diagram illustrates the security flow of how administrators, developers and interactive users of Mail & Deploy access Mail & Deploy respositories.

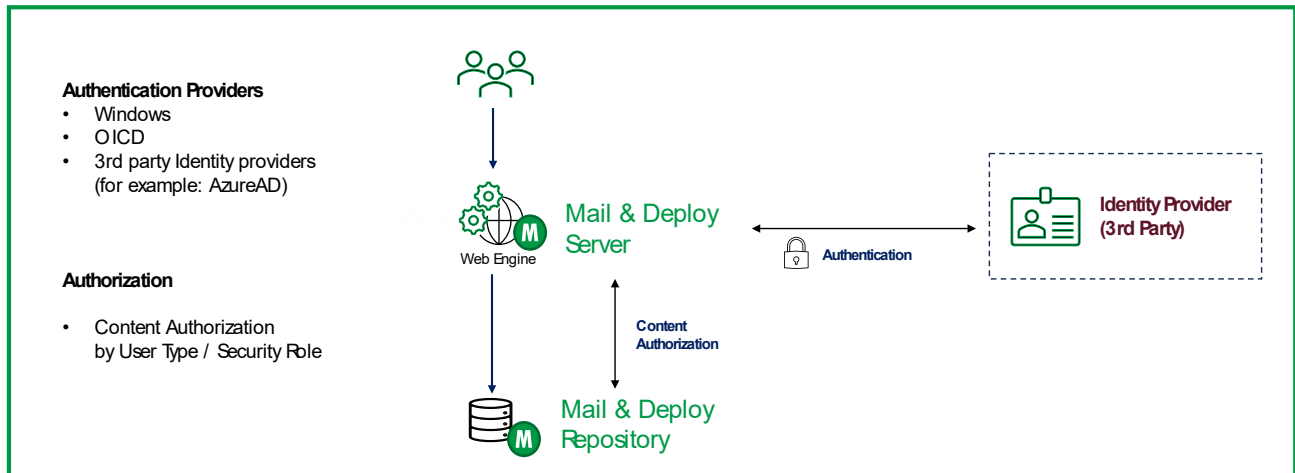


Figure VI: Mail & Deploy Authentication & Authorization Flow

ACCESS TO DATA

Mail & Deploy relies exclusively on data sourced from Qlik applications or SQL databases for its reports. Leveraging QlikView, Qlik Sense, and Qlik Cloud, Mail & Deploy ensures the extraction and delivery of data to end users while adhering to the existing security controls.

There are various connection types to client-managed Qlik Sense and QlikView applications from Mail & Deploy.

In all instances, explicit access must be granted to the Mail & Deploy Server service account through the security controls of QlikView and Qlik Sense. The windows service account running the Mail & Deploy Server authenticates to QlikView and Qlik Sense using the windows authentication provider integrated into both platforms.

When connecting to Qlik Sense, Mail & Deploy utilizes HTTP/HTTPS and communicates with a Qlik Sense virtual proxy. The virtual proxy must support windows authentication, and Mail & Deploy must be installed within the same windows domain as Qlik Sense.

Qlik Sense Connection

When connecting to Qlik Sense, Mail & Deploy utilizes HTTP/HTTPS and communicates with a Qlik Sense virtual proxy. The virtual proxy must support windows authentication, and Mail & Deploy must be installed within the same windows domain as Qlik Sense.

QlikView Connection

In the case of QlikView, Mail & Deploy establishes a connection to a QlikView Server or QlikView cluster over QVP using a local installation of QlikView Desktop on the server hosting the Mail & Deploy Web Engine. For QlikView local connections, the Mail & Deploy Web Engine service account must be granted windows file access privileges to open the QlikView QVW file via a UNC path.

It's important to note that, for all QlikView connections, the local copy of QlikView Desktop must be licensed for use by the windows service account managing the Mail & Deploy Server.

This meticulous approach ensures seamless connectivity and data retrieval while maintaining the necessary security measures in each Qlik environment.

Authorization and Authentication

The Mail & Deploy service account must be authorized to open the QlikView or Qlik Sense application as well as the application objects that reside within the application.

With QlikView, authorization to consume an application is granted through access control lists defined in the QlikView Management Console.

With Qlik Sense, authorization is granted through security rules defined in the Qlik Sense Management Console.

Once authenticated to QlikView or Qlik Sense, the Mail & Deploy service account has the delegation authority to use another identity for authorization purposes to retrieve metadata and data within the Qlik application.

Mail & Deploy administrators may configure extra filters to control which data is used to produce a report for any given recipient. Extra filtering is applied dynamically in the Qlik application at runtime when Mail & Deploy extracts data for the purposes of report generation.

Mail & Deploy administrators also have the option of defining a password on the generated report output file.

Mail & Deploy supports the generation of passwords for both “read” and “write” access to the resulting output file to protect the data once it is in a portable format such as a PDF file.

Access to data is therefore controlled by:

- Authentication to the Qlik platform hosting the application
- Authorization to use the Qlik application by the Mail & Deploy Server Service account
- “Extra Filters” that apply to Mail & Deploy recipient
- Optionally, a password on the generated report output file

REPORT EXECUTION & DISTRIBUTION

Developers as well as users of Mail & Deploy Extensions for Qlik Sense and Mail & Deploy Hub can initiate report execution at any time.

At runtime, the level of data authorization and filtering is evaluated through the following security flow:

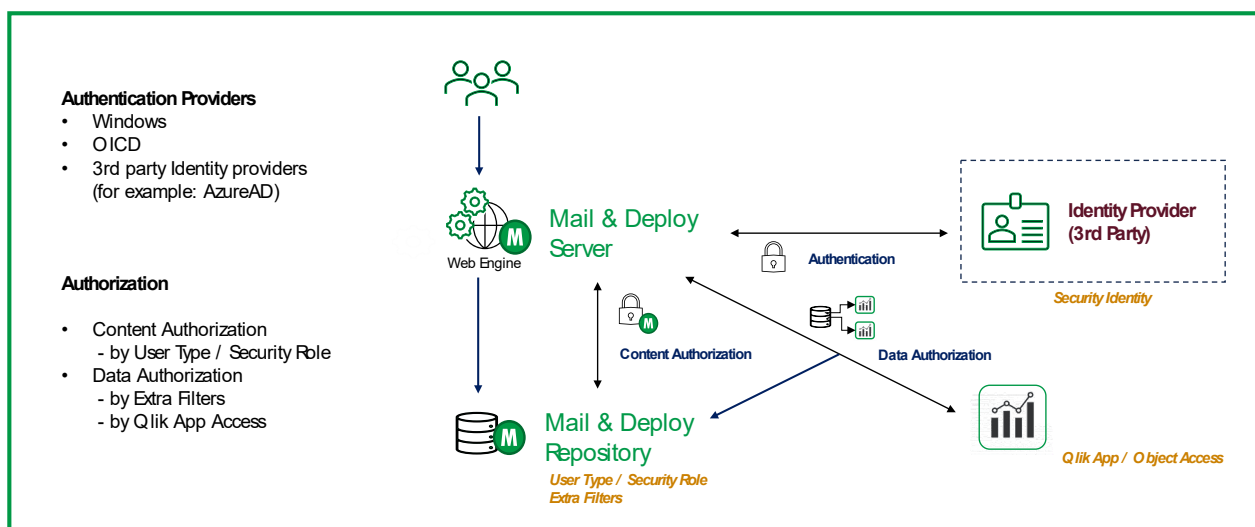


Figure VII: Mail & Deploy Security Flow for Mail & Deploy Extensions and Mail & Deploy Hub

When recipients receive reports passively, user may receive the report through multiple sharing channels including email, mobile, file server, FTP, Microsoft SharePoint/Teams, Dropbox, AWS S3, Google Drive or directly via the Mail & Deploy Hub.

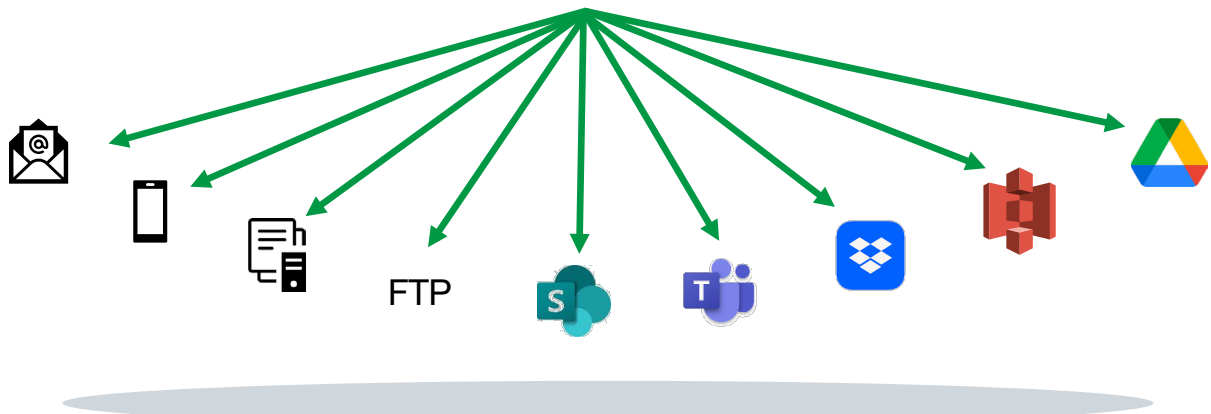


Figure VIII: Mail & Deploy Distribution Channels

For all distribution methods, the security flow to generate the report per recipient is as follows:

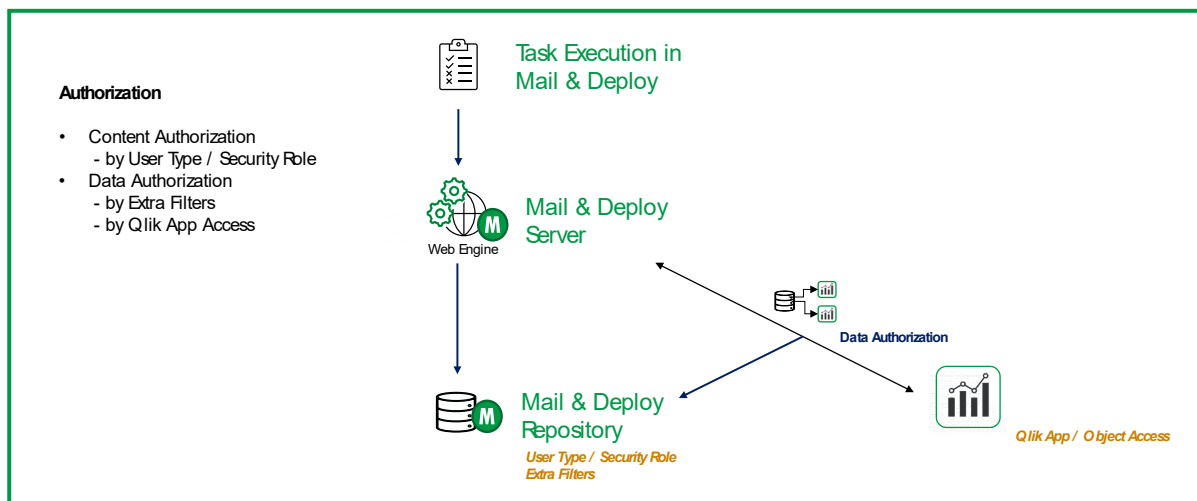


Figure IX: Mail & Deploy Distribution Channels

Secure Email Distribution

Mail & Deploy optionally distributes reports to recipients through email and a SMTP server. When doing so the report may be attached as a file, or, in the case of an HTML formatted report, embedded in the body of the email. As stated previously, attachments can be password protected.

With respect to transmission, Mail & Deploy offers the ability to communicate with the SMTP server through TLS or SSL depending on the requirements of the SMTP server.

COMPONENT COMMUNICATION

The Mail & Deploy internal components communicate over the channels and ports shown below.

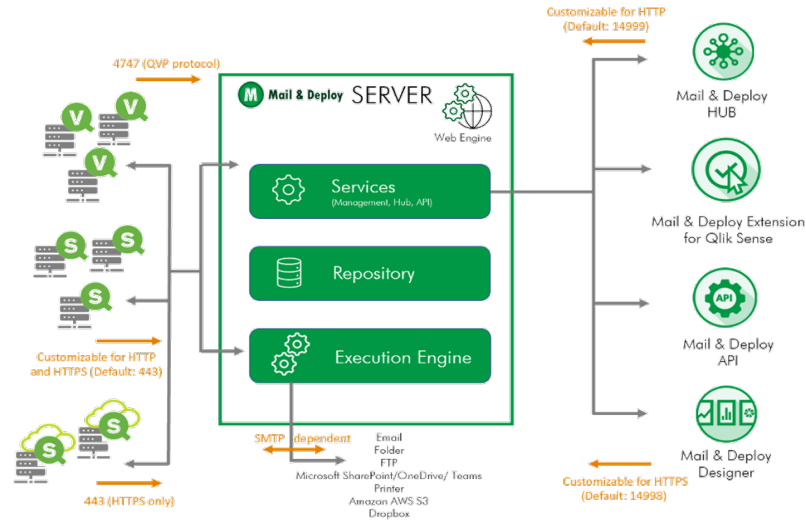


Figure X: Mail & Deploy On-Prem Port Diagram

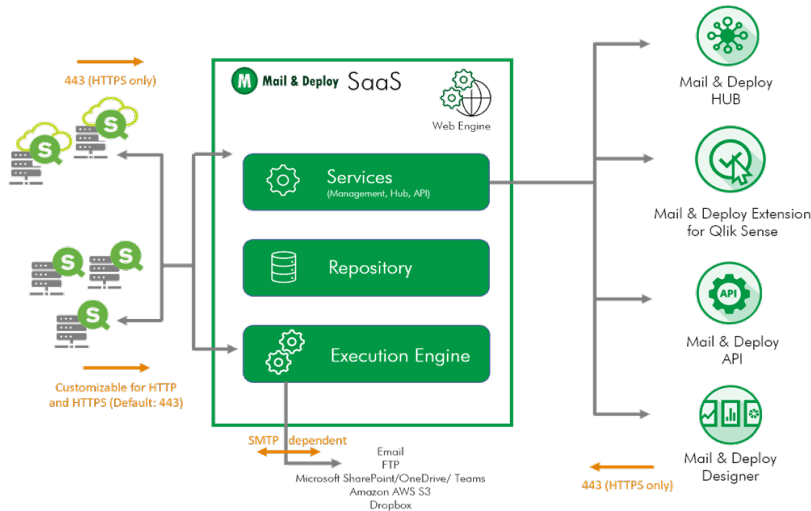


Figure XI: Mail & Deploy SaaS Port Diagram

Mail & Deploy Repository

The Mail & Deploy repository stores all Mail & Deploy application metadata. The application metadata includes users, connections to Qlik applications, SQL Servers, templates, tasks and system configuration details, etc.

Mail & Deploy Server

The central component of any installation is Mail & Deploy Server which is a windows services that:

- Runs under the Service Account
- Hosts the Repository (which is the central database that contains all data managed by Mail & Deploy)
- Performs all executions (such as Task executions).
- Provides Services that can expose a user interface for Users to connect or an API to connect to

For a full list of product versions that are shipped and supported with Mail & Deploy please refer to the system requirements at community.mail-and-deploy.com.

REPORT DEVELOPMENT

Mail & Deploy report development unfolds through the dedicated desktop application, the Mail & Deploy Designer. Within a Mail & Deploy site, all reports are centrally stored on the Mail & Deploy server. The Mail & Deploy Designer is initiated exclusively when a developer chooses to edit a report, ensuring a secure session through the Mail & Deploy Management Console.

To access and edit reports, developers undergo a secure login process via a browser to the Mail & Deploy Web Engine. The requisite privileges are granted based on their Mail & Deploy user roles.

Communication between the Mail & Deploy Designer and Mail & Deploy Web Engine transpires over HTTPS, prioritizing security in data transmission. Notably, while HTTPS is supported, the acceptance of HTTP is restricted, reinforcing our commitment to robust security practices.

REPORT STORAGE

Mail & Deploy securely stores essential components such as application metadata, report templates, and queue information on the Mail & Deploy Server.

When utilizing the Mail & Deploy Hub or the Mail & Deploy extensions for Qlik Sense, the Mail & Deploy Server efficiently manages the storage of published reports.

For Mail & Deploy extensions for Qlik Sense, these reports are stored on a disk location; however, with Mail & Deploy extensions for Qlik Sense, you have the flexibility to opt for report delivery via email. Notably, Mail & Deploy Hub reports are centrally stored in the repository.

Reports generated through Mail & Deploy extensions for Qlik Sense can be either downloaded to the local computer of the Qlik Sense user or sent via email. Hub reports, on the other hand, persist for a configurable period as defined by the administrator.

Similar to an email inbox, a dedicated copy of the report is maintained for each Hub recipient in their individual library.

For reports published to hard drive folders, Mail & Deploy offers the flexibility to publish them to configurable locations of choice, enhancing the user’s control over data management.

Mail & Deploy Distribution	Storage Location
Email	<not stored>
Folder	Folder Location of Choice
Mail & Deploy Hub	Central Mail & Deploy Repository
Mail & Deploy Extension for Qlik Sense	Local Disk Location
FTP	Folder Location of Choice
Microsoft SharePoint/Teams	Folder Location of Choice
Dropbox	Folder Location of Choice
Box	Folder Location of Choice
AWS S3	Folder Location of Choice
Google Shared Drive	Folder Location of Choice

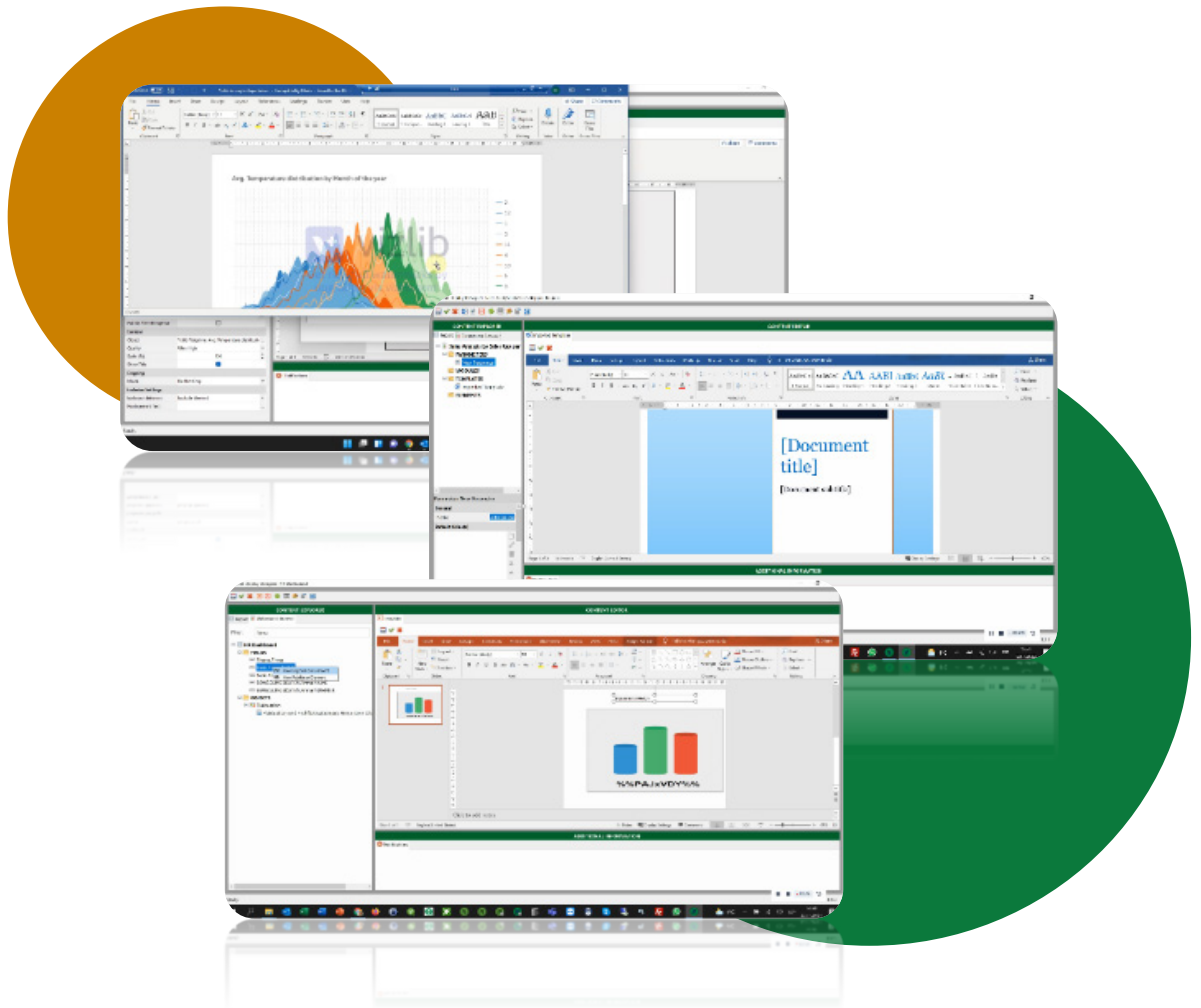
Figure XII: Storage Location

CONCLUSION

Mail & Deploy stands as a secure and adaptable solution, seamlessly expanding the capabilities of the Qlik Enterprise platform. It empowers customers to effortlessly introduce both interactive and passive reporting, catering to named recipients with data sourced from Qlik applications.

By aligning itself seamlessly with the security framework governing data access within Qlik applications, Mail & Deploy not only ensures a robust level of security but also offers additional options to precisely fine-tune the delivery of trusted data to users.

Utilizing standard network, platform, and web protocols, Mail & Deploy guarantees a secure deployment within an enterprise environment. This commitment to industry standards underscores the reliability and stability of Mail & Deploy, making it a trusted solution for businesses relying on Qlik for their data reporting needs.



About Mail & Deploy

Mail & Deploy, a distinguished product of MaD Reporting GmbH, has solidified its standing as a prominent figure in the Qlik® reporting landscape. As a recognized Qlik® Technology Partner, MaD Reporting GmbH has been at the forefront of Qlik® reporting evolution since 2008, introducing a proven alternative to Qlik® NPrinting.

This robust reporting suite, Mail & Deploy, emerges as a flexible and intelligent solution, providing Qlik® users across the globe with a unified and enriched reporting experience tailored for Qlik Sense® SaaS, Qlik Sense®, and QlikView®. Boasting advanced features and unparalleled power, this unified platform is available in both on-premise and SaaS configurations, ensuring adaptability to diverse business needs.

The global impact of MaD Reporting GmbH extends through a network of over 70 Qlik®-certified resell partners. With a track record of delivering exceptional value, Mail & Deploy has reached over 100,000 decision-makers across 200 enterprises, spanning more than 30 countries and encompassing various industry verticals.

Mail & Deploy is not just a reporting tool; it stands as a beacon of innovation, reliability, and global influence in the dynamic realm of Qlik® reporting solutions. The journey with Mail & Deploy is a testament to a commitment to excellence, ensuring businesses harness the full potential of their Qlik® platforms.

www.mail-and-deploy.com | info@mail-and-deploy.com

© 2008-2024 MaD Reporting GmbH. All rights reserved. Mail & Deploy® is a trademark of MaD Reporting GmbH and has been registered in one or more countries. Other marks and logos mentioned herein are trademarks or registered trademarks of their respective owners.