YSOFT SAFEQ®

SECURING THE ENTERPRISE WORKFLOW ENVIRONMENT

CONTENTS

INTRODUCTION

Organizations spend vast amounts of resources to ensure that their IT infrastructure – including print infrastructure – is secure. And for good reason. Mitigating risk from external bad actors and intentional/unintentional internal actors can prevent significant financial and brand reputation loss. However, the effort is nearly wasted if the software and related systems running on the infrastructure is unsecured.

This white paper outlines how YSoft SafeQ 6 provides secure print services and print services infrastructure. It also outlines the detailed measures that Y Soft takes to ensure that its YSoft SafeQ software, hardware and communication pathways – the entire system – is secure and adheres to an organization's security governance. In fact, we strongly believe that security is a continuous joint effort between an organization's security/IT teams, the print device manufacturers and the software that manages enterprise document workflow activities.

Common Security Acronyms

CIA
Confidentiality, integrity, availability

AAA
Authentication, Authorization, Accounting

GDPR
General Data Protection Regulations (closely associated with privacy)

In this document, we'll look at YSoft SafeQ security through the lens of:

- **Users** (individual employees including print administrators and guests)
- **Infrastructure** (servers, client devices such workstations, laptops, smartphones and tablets)
- **The print device**, which may be a multifunction device (MFD) or single function device (SFD). Within this section we also address data in use, transit, and at rest

Finally, we outline Y Soft policies, processes and commitment that contribute to the security of our products.

USER SECURITY

As with any type of security, an organization must achieve the right balance between security levels and usability/employee productivity. YSoft SafeQ offers a variety of methods to secure devices and document workflows in order to meet the requirements of an organization's security governance.

SECURING THE DEVICE

The first step in securing a company's document workflow system is to secure access to the print devices. YSoft SafeQ offers a variety of ways for users to authenticate (prove their identity against a corporate directory) to access the print device. They include:

MFD/SFD:

- Single or two-factor using:
  - Identity cards and card readers that accurately (zero fault tolerance) read with a simple swipe
  - PIN / Expiring PINs / Guest PINs
  - Username/password
  - Biometric (fingerprint)
  - Single sign on

External Terminal:

- Smart cables
- Any of the single or two-factor methods described above

Mobile Terminal (mobile app):

- Authentication requires email ownership verification

Shared workstation:

- A client that can support multiple users from a single workstation

USER – WORKFLOW/DOCUMENT SECURITY

Once a user is correctly authenticated at the device, they may have access to print, copy, scan, or fax features. Alternatively, a user's authentication credentials may authorize them to use only some functions (or even only some Automated Scan Workflows) and **blocks others**. This is particularly useful when allowing **guest printing** while restricting access to scan and copy functions, for example.

In the printing context, securing sensitive or confidential documents is still a concern. **Pull-printing**, known as Print Roaming in SafeQ, solves this by holding a print job in a secure print queue until the user authenticates at any print device.

Printed or copied documents may also contain **watermarks** (with a GUID – globally unique ID, overlay image or some other configurable text). **Job routing proxies** may be used to force print jobs to segregated and protected servers by using a DMZ (demilitarized zone). These are examples of YSoft SafeQ Extensions that are available as additional options to meet a customer's security needs.

PRINT ADMINISTRATOR – ENFORCING THE SECURITY PRINT POLICY

YSoft SafeQ provides access to the YSoft SafeQ system for administrators through an online dashboard. Access to the dashboard is protected by entering domain credentials or use of single sign on.

The dashboard enables the print administrator to set up **user controls** within YSoft SafeQ which meet the organization's print governance policies. Many of the User—Workflow/Document Security features mentioned above are set by the print administrator. Through YSoft SafeQ's Rule-based Engine or a YSoft SafeQ Extension, other controls can be implemented:

- **Time restrictions** to limit device access
- **Role access** – permitting or restricting features
- **Tags** for flagging restricted jobs/devices
- **Location restrictions**, for example, per server, country or region
- **Print job delegation** (no more shared PINs)
- **Archiving:** copy, scan, print job, print job preview
- **Local printers reporting**

GDPR Compliance

YSoft SafeQ 6 provides print administrators tools to aid in GDPR compliance with a subject's rights concerning their personal data.

More information can be found in the eBook, GDPR Compliance Guide for YSoft SafeQ 6.

YSoft SafeQ ensures the security of document data from the time the user sends the print job to the time it prints at the device with end-to-end security by encrypting a document throughout its print job lifecycle. Similarly, this end-to-end security applies to scans where data is secure during capture, processing and delivery.

Another administrator tool for monitoring security is **Reporting**. Through YSoft SafeQ, all activity is tracked by recording the meta data associated with the activity. Reporting provides an audit trail for security purposes.

INFRASTRUCTURE SECURITY

YSoft SafeQ's building block architecture can be easily deployed on an organization's existing infrastructure and, as the organization's needs change or grow, YSoft SafeQ can easily adapt. It is important therefore, to look at infrastructure security and how YSoft SafeQ interacts and works with existing protocols and systems.

SERVER

As part of best practices, server certificates and their management are typically a responsibility of the organization. YSoft SafeQ uses the organization's certificates to secure communication between the server and other parts of the YSoft SafeQ communication system, other 3rd party systems and as part of encrypted communication to verify user identity through authentication.

Note: YSoft SafeQ can work with self-signed, hard-coded certificates but this is not recommended, and an organization uses this at their own risk.

Other systems may include Mail Servers (where TLS/SSL is used for login/password authentication); LDAP (LDAP over SSL) or other Identity Management; database connections (TLS for connection/domain accounts for MS SQL; and other subsystems such as Spool Controllers. YSoft SafeQ uses Microsoft EFS for spooling.

See the communications pathways diagram on page 9 for other possible communication pathways that are secured using encryption, firewalls on documented ports, and an organization's server certificates. This includes other parts of YSoft SafeQ that may be on different servers, for example, communication between YSoft SafeQ's Management Server tier and Site Services where the Spooler Controller or Wireless Printing Services may exist. YSoft SafeQ also supports 3rd party antivirus systems that may be in use with documented exceptions.

Additionally, a maintenance plan can be defined to fit the organization's Disaster Recovery protocols including Recover Time Objective (RTO) and Recovery Point Objective (RPO).

SERVICE ACCOUNTS, PASSWORDS

YSoft SafeQ stores highly sensitive data (e.g. passwords for service accounts) in databases or configuration files. Even though access to server storage is typically highly restricted, an additional encoding layer of protection might be desired to mitigate certain attacks.

When configured, the highly sensitive data, referred to as secrets, can be encrypted using the AES algorithm in CBC mode of operation and random IV (initialization vector). Encryption is non-deterministic by design so that the same secrets will result in different ciphertexts each time they are encrypted. Length of a secret is partially masked by PKCS5 padding. Ciphertext is then authenticated using the HMAC-SHA256 algorithm and a truncated authentication tag is concatenated to the output which is encoded to Base64. HMAC uses an independent key – every key in the key file contains both encryption and authentication key internally.

This approach is currently used for the most critical systems: database service accounts (if SQL login is used), identity management database (over LDAP protocol), and for the email server service account, when used. Y Soft is extending usage of this encrypted method to cover all systems.

YSOFT SAFEQ IN THE CLOUD

Some organizations choose to have YSoft SafeQ Management Server and/or Site Services tiers in a hosted cloud environment. While there are many benefits to this kind of deployment, organizations need to consider if data transfer or job processing adheres to their security and privacy governance and or local laws with respect to where these severs are located.

DATA IN TRANSIT; GETTING THE PRINT JOB INTO YSOFT SAFEQ SECURELY

Today's workforce is increasingly becoming mobile. Secure solutions are needed across the desktop workstation and a variety of mobile devices.

Standard Shared Print Queues – (SMB 3.0+ on Windows 8 and newer)

Windows shared queues from print servers are often used and YSoft SafeQ can support this through or add additional options:

- SMB 3.0+ (Windows 8 and newer)
- IPPS
- YSoft SafeQ 6 client (YSoft SafeQ 5 is available as an Extension)
- A combination of SMB 3.0+ or IPPS and a YSoft SafeQ client

Should a connection to YSoft SafeQ Site Services be lost, YSoft SafeQ can print in offline mode. The workstation client enables users to print to a previously used printer which is useful when high availability of print services is needed. When connection is restored, job reporting is updated.

Signed Certificates

When distributing YSoft SafeQ client software to workstations, trusted certificates should be used to sign the package, to ensure it is safe and not tampered with potentially harmful viruses. Y Soft can provide the certificates however, it is preferable that organizations use their own.

Mobile Print

Mobile devices now must be considered as part of the print infrastructure whether these smartphones and tablets are company supplied or BYOD. While convenient and efficient, they do present new entry points as potential risks. YSoft SafeQ supports secure mobile printing in a variety of ways.

A user can either connect to a web interface and, after identity verification, upload the document, or use email integration, where an email attachment is pulled from the email server via POP3, IMAP or EWS protocol. Both options are possible with SSL/TLS encryption.

Mobile Integration Gateway

Another way to send job data to the YSoft SafeQ server is through Y Soft's Mobile Integration Gateway component, which allows sending jobs from iOS or Android devices via IPPSSL protocol.

- Signed installer
- MSI: CA cert., driver cert. publisher deployment
- Needed from all platforms (Windows, Mac, Linux, Google Cloud, mobile)

MULTIFUNCTION DEVICE (MFD), SINGLE FUNCTION DEVICE

As noted in the Server section above, organizations should provide certificates for the servers print devices are connected to; these certificates are used by YSoft SafeQ to verify identity through authentication. YSoft SafeQ also supports use of WebDav over HTTPS.

- Server certificate verification (authentication)
- WebDav over HTTPS
- NFC authentication
- MFD certificate verification (Embedded Terminal push) when supported by the MFD
- IPP SSL protocol, also with MFD certificate verification
- Additional methods may be used proprietary to the MFD manufacturer

YSoft SafeQ does not store any data on the MFD hard drive.

DEVELOPMENT OF YSOFT SAFEQ – SECURITY AT Y SOFT CORPORATION

Y Soft is recognized within the industry as having a strong security posture in the development of YSoft SafeQ. YSoft SafeQ is designed with security in mind. Security specialists are part of development teams ensuring that regular consultations take place during product design and within code reviews. Security consultations include the following.

- Threat Modeling using dataflow diagrams and the Microsoft STRIDE approach in the design phase aiming to eliminate design flaws
- Daily static source code analysis on Java and .NET projects
- Daily checks on 3rd party libraries for known vulnerabilities
- Review and record of all communication endpoints
- Defect management process. Public submissions of security concerns are openly discussed, analyzed and fixed. Security concerns can be submitted to Y Soft here: https://www.ysoft.com/en/report-a-security-issue

Y Soft uses a variety of tools and services in its security reviews. An example of these are listed below and includes Security Code Scan – static code analyzer for .NET (GitHub) and DevAudit.

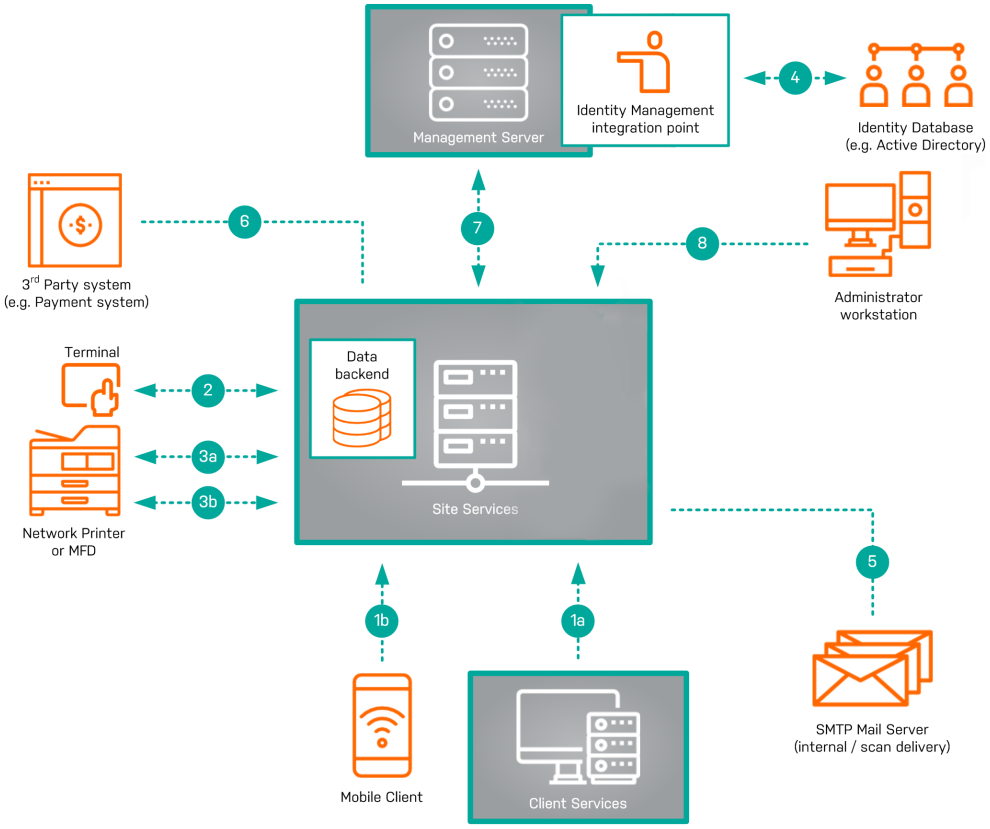


Figure 1.
YSoft SafeQ communication paths

1. Printing – communication from YSoft SafeQ when
   - **a.** A print job is sent from the client's workstation
   - **b.** A job is sent from a mobile client

2. MFD (multifunctional device) authentication — communication from the MFD's terminal/reader to YSoft SafeQ for the purposes of verifying a user's login credentials

3. Communication from YSoft SafeQ to the networked MFD:
   - **a.** A pull-print release of a print job
   - **b.** Authentication verification, authorization, and accounting

4. Integration with the identity management database or identity/authentication provider

5. Connection from YSoft SafeQ to an SMTP mail server or shared network folder for data delivery of digital scans

6. Integration with third-party applications or systems, for example, for delivery of digital scans to a cloud-based document repository

7. Inter-server communication. Depending on an organization's redundancy and fail-over requirements, multiple Client Services tiers or Management Server tiers can be in multiple remote locations. Inter-communications between the tiers at the various locations are required for print release job processing and the transfer of print job metadata for reporting purposes

8. Administrator access to the YSoft SafeQ Management interface

FREQUENTLY ASKED QUESTIONS

Where is data held in the processing of print jobs, scans and copies?

- **Print jobs** – When using Print Roaming, data is held in the Client Services and Site Services layers of YSoft SafeQ. If using Client Based Print Roaming, the print job is held at the client workstation and only print job metadata is communicated to the Client Services through to the Site Services and Management Server layer of YSoft SafeQ.

- **Scan to email, scan to file system and Automated Scan Workflows** – Data is temporarily held on the MFD hard drive and erased when the job is completed. If using scan to email, the email from the MFD to the client workstation can be delivered through encrypted communication. For even better security with end-to-end encryption, encrypted PDFs are supported. With Automated Scan Workflows, the digital scan is delivered to a predefined location through encrypted communication.

- **Copies** – Temporarily held on the MFD hard drive and erased when the job is completed.

Can you provide proof of data destruction on the MFD's hard drive?

Any data temporarily stored during scanning is immediately erased. The MFD service provider and the organization should have processes in place for securing the MFD hard drive during use, during servicing and in the event of decommissioning which includes destroying data on the hard drive. It should be noted, however, that the MFD's hard drive is outside of YSoft SafeQ's area of responsibility.

Can you provide compliancy with payment gateway systems?

YSoft SafeQ does not communicate directly with any payment gateway systems. In the case of the Credit and Billing module of YSoft SafeQ or the Payment Machine, YSoft SafeQ is only notified by the financial institution that payment and the amount has been received.

Can you securely integrate your reporting data into our web portal?

Web portals are typically secured via signed certificates, which are supported by YSoft SafeQ. YSoft SafeQ reporting data can be integrated with a web portal to show print, copy and scan data.

How can data be encrypted throughout its lifecycle?

With YSoft SafeQ, when using the spooling client, IPP over TLS protocol for encryption, authentication, and with integrity of the data transferred to the MFD, the data leaves the workstation only when the job is released. It is also possible for server-based Print Roaming to send the data from the workstation to the YSoft SafeQ server via an HTTPS channel. This is also the case for print data transfer between servers when Far Roaming is active. While at rest on the server or at the workstation, standard Microsoft EFS can be used for print data protection.

Can my organization view documents that have been printed by employees?
When using Print Roaming, an administrator with access to the file system can access the print streams for all jobs held at the YSoft SafeQ Management layer (jobs waiting to be printed, printed or marked as favorites). However, YSoft SafeQ can be configured to automatically delete print jobs after printing. If YSoft is running under a named service account and using Microsoft EFS, the administrator will have to know the service account's password to see the job. Any activity in the named service account is captured in the Windows audit logs. Additionally, Microsoft EFS enables segregation of duties – such as having enterprise administrators who can administer servers and applications without having access to print job data and enterprise administrators who have security clearance to access print job data.

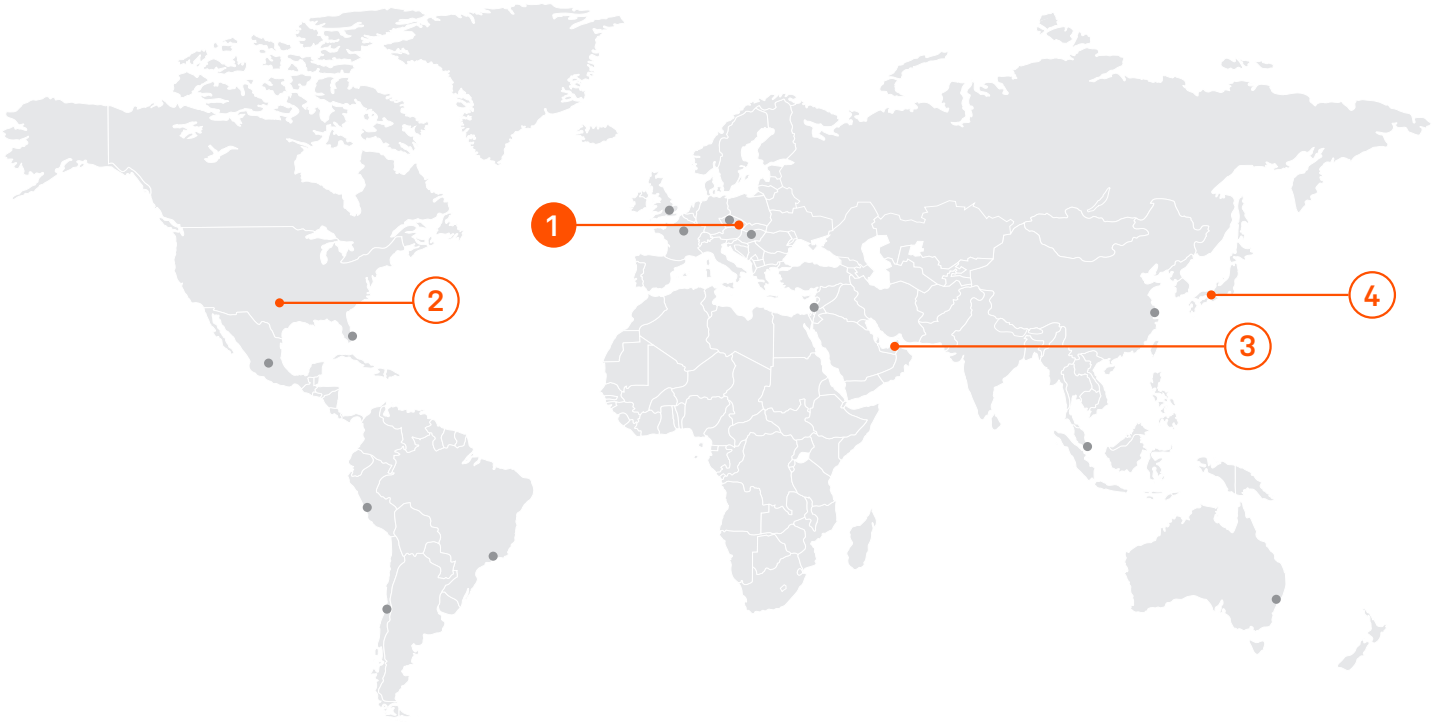
When using Client Based Print Roaming, only the print job's metadata is captured. To see the actual job, access to the workstation would be required.

Can users see what documents have been printed by others?
No.

How does YSoft SafeQ help organizations meet GDPR regulations?
Please review the detailed information in the GDPR Compliance Guide for YSoft SafeQ 6. In short, YSoft SafeQ enables administrators to address an individual's rights pertaining to the data the organization has (the Right to Access), to correct the data (the Right to Rectification), to prevent the processing of the data (the Right to Restrict Processing), and to delete the data (the Right to Erasure).

Can a person's personal identifying data be removed from the YSoft SafeQ system but remain anonymous for reporting purposes?
Yes. A delete query will remove a user's data from the YSoft SafeQ system without removing printing details for reporting purposes. The report will just show a blank user.

LOCATIONS



Company Headquarters	Regional Headquarters	
1 Y Soft Corporation, a.s. Technology Park, Technická 2948/13 616 00 Brno Czech Republic	2 North and Latin America Y Soft North America, Inc. 1452 Hughes Rd, Suite 110 Grapevine, TX 76051 3 Middle East Y Soft Middle East Office 410, 4th Floor, Alfa Building Dubai Internet City, Dubai	4 Asia Pacific Y Soft Japan, Ltd. KFM Building, 10th Floor 658-0032 Koyocho Higashinada Kobe, Hyogo Japan

For a complete list of more than sixteen countries and locations, please visit our website.

YSOFT
BUILD SMART BUSINESS

SFQ-SEC-WP-12-2019