

Kyocera Cloud Print and Scan Security White Paper



Version 20240312

Revision history

| Release Date | Revision | Chapter | Details |
|--------------|----------|--|---|
| 2021/05/17 | 1.0 | - | First release |
| 2021/05/18 | 1.1 | - | First official draft created |
| 2021/05/20 | | 3. Multitenancy | Added "Users not in KCPS system" in data access table. |
| | | Various | Used TLS in place of SSL/TLS and removed other references to SSL |
| | | 4. Encryption Algorithm for Sensitive Information | Removed this section. Moved information about KCPS encryption to the section Data Protection -> Encryption, and TLS to the section Data Protection -> HTTPS Protocol |
| | | 6.1.1 Access Control | Replaced users with operators to distinguish KCPS users for IT Ops/DevOps with access to cloud provider deployment. |
| 2021/06/28 | | 6.4 Security vulnerability testing | Added new section, updated Table of Contents |
| 2021/07/09 | | 4.3 Automatic logout | Added new section |
| 2022/01/04 | 1.2 | 4.3 Automatic logout | Updated section to mention that the automatic logout is now customizable for the Desktop client depending on specific RHQ deployment requirements. |
| | | 4.4 PIN Authentication | Added new section |
| | | 4.5 ID Card Authentication | Added new section |
| | | 6.4 Security vulnerability testing | Corrected timing of Security vulnerability test |
| | | 7. Device Authentication | Updated to add "PIN login" |
| 2022/06/05 | 1.3 | 5. Firewall Configuration | Updated TCP ports for Desktop client (5000/5001 -> 5570/5571) |
| | | 2. System Overview | Added SharePoint Online to supported third-party cloud storage |
| | | 4.5 ID Card Authentication | Updated text to indicate that registration of ID cards is now supported on the customer portal |
| | | 4.6 Azure Active Directory | New section detailing Azure AD support |
| 2022/08/01 | 1.3.2 | 5. Firewall Configuration | Updated source detail for port 5570 |

| | | | |
|------------|-------|---|--|
| | | 1.4 Regarding trademarks | Added new trademarks |
| | | 1.5 Important notice | Added new section |
| 2022/09/15 | | 1.4 Regarding trademarks | Corrected some trademarks |
| 2022/12/21 | 1.3.5 | 6.2.2 | Removed unnecessary explanations. |
| 2023/02/28 | 1.4.0 | 4.2 Password policy | Updated text on topic about password hashes |
| | | 4.7 3 rd Party Credentials and OAuth2 | Added new section to detail authentication flow and make it clear that KCPS does not keep credentials from 3 rd party services. |
| | | 6 Data Protection Technical Details | Renamed section from "Data Protection" to "Data Protection Technical Details" to specify that information in this section is for individuals with a technical background. |
| 2023/05/16 | 1.5.0 | 6.1.4 Information utilized by KCPS | Added folder locations of locally stored desktop client jobs for Windows and MacOS |
| 2023/11/9 | 1.7.0 | 2 System Overview | <ul style="list-style-type: none"> - Added Chrome extension as a client - Added detail for non-HyPAS for KCPS Desktop Client |
| | | 6.1.4 Information utilized by KCPS | Added entry for Chrome extension |
| | | 5. Firewall Configuration | Added items for KCPS Desktop Client (non-HyPAS) |
| 2024/01/12 | 1.8.0 | 4.6 Azure Active Directory | Replaced "Azure Active Directory" and "Azure AD" with "Microsoft Entra ID" |
| 2024/01/19 | | 3. Multitenancy | Updated Table 2-1 to add Print Manager role. Updated Table 2-1 to remove "License Info only" for "Device of customer org" for user types "Provider admin" and "Provider support" |
| 2024/02/05 | | 6.4 Security vulnerability testing | Update the schedule for security vulnerability testing |
| 2024/03/12 | 1.9.0 | 4.6.2 Google Workspace | Created new section "4.6. 3rd Party Authentication and Identity Servers" with sub-sections "4.6.1 Microsoft Entra ID" and "4.6.2 Google Workspace" |
| | | (Table 2-1) Access to organization and user data by user type | Changed "Log data" column heading to "Report" |
| 2024/04/08 | | 6.4. Direct Print / Scan from Box Storage | Added new section 6.4.Direct Print / Scan from Box Storage |

Contents

| | |
|---|-----------|
| 1. Introduction | 6 |
| 1.1. About this document | 6 |
| 1.2. Target reader | 6 |
| 1.3. Abbreviation | 6 |
| 1.4. Regarding trademarks | 6 |
| 1.5. Important notice | 6 |
| 2. System Overview | 7 |
| 3. Multitenancy | 9 |
| 4. User Identification and Authentication | 13 |
| 4.1. Account Lockout Policy | 13 |
| 4.2. Password Policy | 13 |
| 4.3. Automatic logout | 15 |
| 4.4. PIN Authentication | 15 |
| 4.5. ID Card Authentication | 15 |
| 4.6. 3 rd Party Authentication and Identity Servers | 15 |
| 4.6.1. 3rd Party Credentials and OAuth2 | 15 |
| 4.6.2. Microsoft Entra ID | 16 |
| 4.6.3. Google Workspace | 17 |
| 5. Firewall Configuration | 18 |
| 6. Data Protection Technical Details | 19 |
| 6.1. Protection of Stored Data | 19 |
| 6.1.1. Access Control | 19 |
| 6.1.2. Authentication | 19 |
| 6.1.3. Encryption | 19 |
| 6.1.4. Information utilized by KCPS | 20 |
| 6.1.5. Data Backup | 21 |
| 6.2. Protection of Communication Data | 21 |
| 6.2.1. User Access | 21 |
| 6.2.2. HTTPS protocol | 21 |
| 6.3. Secure communication between the KCPS server and databases | 22 |
| 6.4. Direct Print / Scan from Box Storage | 22 |
| 6.5. Security vulnerability testing | 22 |
| 7. Device Authentication | 23 |
| 8. AWS Security Technical Details | 24 |
| 9. Contact Information | 25 |

1. Introduction

1.1. About this document

This document describes Kyocera Cloud Print and Scan (KCPS) version 1.9.0

1.2. Target reader

This document is intended for staff members at the RHQ and sales companies of Kyocera Document Solutions group. For outside of the Kyocera Document Solutions group, such as channel partners or end users, it is expected that sales companies will create new official public documents based on the contents of this manual.

1.3. Abbreviation

- KCPS is the abbreviation for Kyocera Cloud Print and Scan.
- TA is the abbreviation for TA Triumph-Adler.
- TACPS is the abbreviation for TA Cloud Print and Scan.
- AWS is the abbreviation for Amazon Web Services.

1.4. Regarding trademarks

Box® and Box Enterprise® are registered trademarks of Box, Inc. and/or its affiliates.

Android®, Google Chrome®, Chromebook®, Google Drive™ and Google Workspace® are trademarks of Google LLC.

Macintosh®, macOS®, and iOS® are trademarks of Apple Inc., registered in the U.S. and other countries and regions.

Microsoft®, Windows®, Active Directory®, Microsoft Entra ID®, Microsoft Word, OneDrive®, OneDrive for Business®, SharePoint® and SharePoint Online® are registered trademarks of Microsoft Corporation in the U.S and/or other countries.

All other brand and product names herein are registered trademarks or trademarks of their respective companies.

1.5. Important notice

In the environment where multiple users share a single PC, there was timing when others can see, print or delete your print job while your desktop client is old version (v1.3.1 or lower).

It is highly recommended that you update to version 1.3.2 or later, which fixes the above issues.

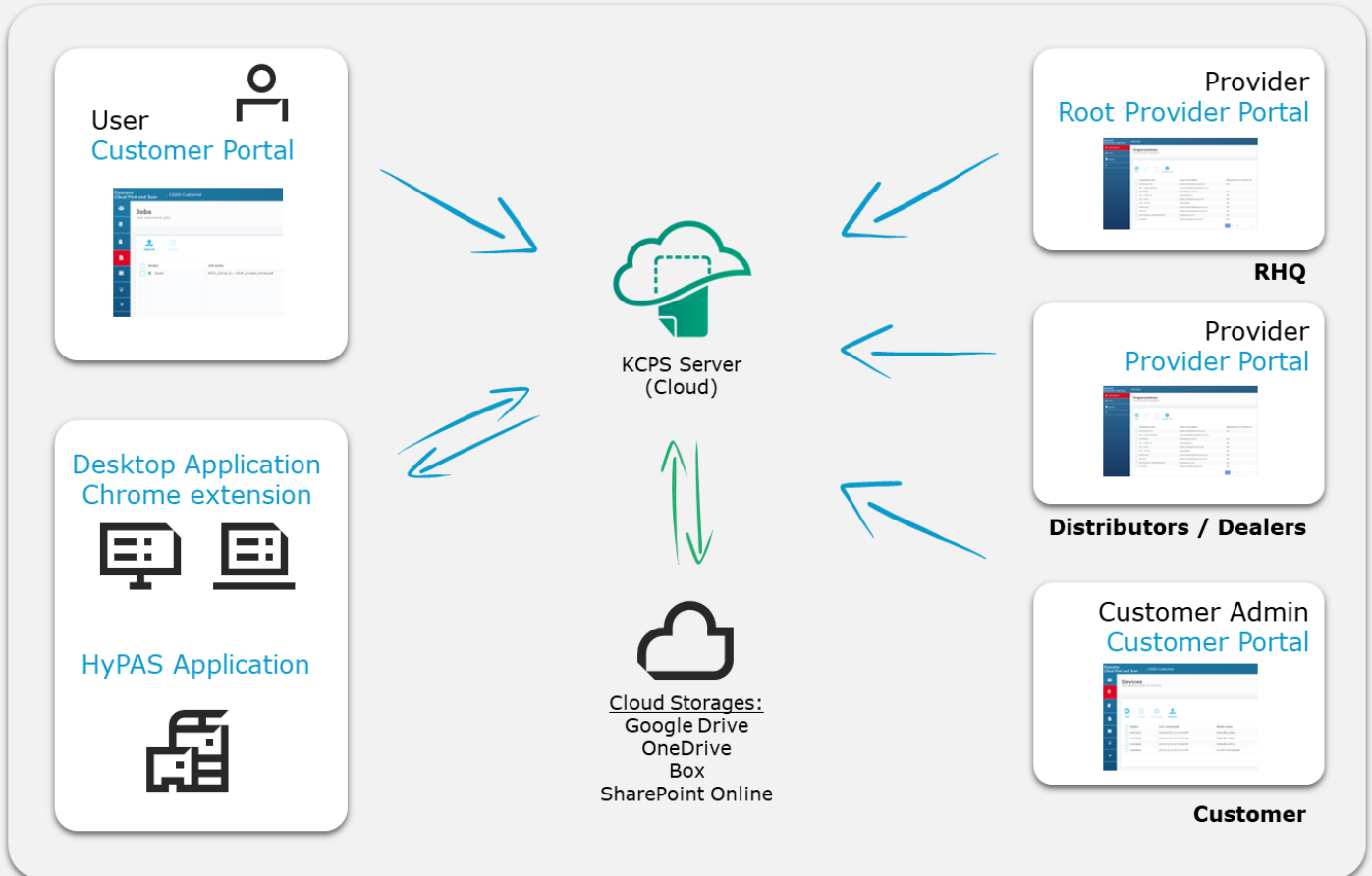
※KCPS desktop client does not support server OS, virtual desktop environments such as Citrix, and using KCPS desktop client as shared printer drivers is not supported.

2. System Overview

Kyocera Cloud Print and Scan (KCPS) is a cloud-based office printing and scanning solution that allows administrators to easily manage users, register Kyocera multi-functional printer (MFPs), and track print activities for their own organizations.

This white paper informs dealers and users about security measures in KCPS. Kyocera's priority is to provide secure protection of information assets that are handled by KCPS. These information assets are rigorously protected by the secure configuration and security features of KCPS.

KCPS consists of the following components:



Root provider portal: The root provider (RHQ) can access the **root provider portal** using a web browser. With this portal, RHQs can manage the URL links of the End User License Agreement (EULA), Privacy Statement, and the KCPS Desktop client package for their region. This portal also has an Organization tree for RHQs to view the hierarchy of all the organizations in their region.

Provider portal: The provider (RHQ, SC, Dealer) can access the **provider portal** using a web browser. They can add, edit, or delete organizations for child providers or for their customers.

Customer portal: The customer admin or customer user can access the **customer portal** using a web browser. The customer admin can add user accounts for their own organization and configure settings related to print limit and print policy.

Customer users can check their print job status and download scanned documents.

Desktop client: The Desktop client connects to the KCPS server. Customers can upload their print jobs. Depending on the spooling configuration (cloud spool or local spool), the print jobs are either stored in the desktop or stored in the KCPS server.

For non-HyPAS models, Desktop Client provides direct printing, a one-month print quota, and the print usage reports.

Chrome extension: The Chrome extension is provided specifically for Chromebook users to be able to upload their print jobs to KCPS Server from any of their applications on the Chromebook that supports the print function. The Chrome extension is published on and is available to be downloaded from the Chrome Web Store.

HyPAS application (MFP client): The HyPAS application must be installed for MFP to be used with KCPS systems. The HyPAS application connects to the KCPS server. Customers can release their print jobs that they uploaded using the Desktop client. Customers can also scan their documents using this application.

Cloud Storage: As third-party cloud storage, KCPS supports integrations with Google Drive, Box, OneDrive, and SharePoint Online. By linking your cloud storage account with your KCPS account, you can print from and send scanned data to your cloud storage.

KCPS was developed at Kyocera Document Solutions Development America (KDDA) which is certified to ISO 27001.

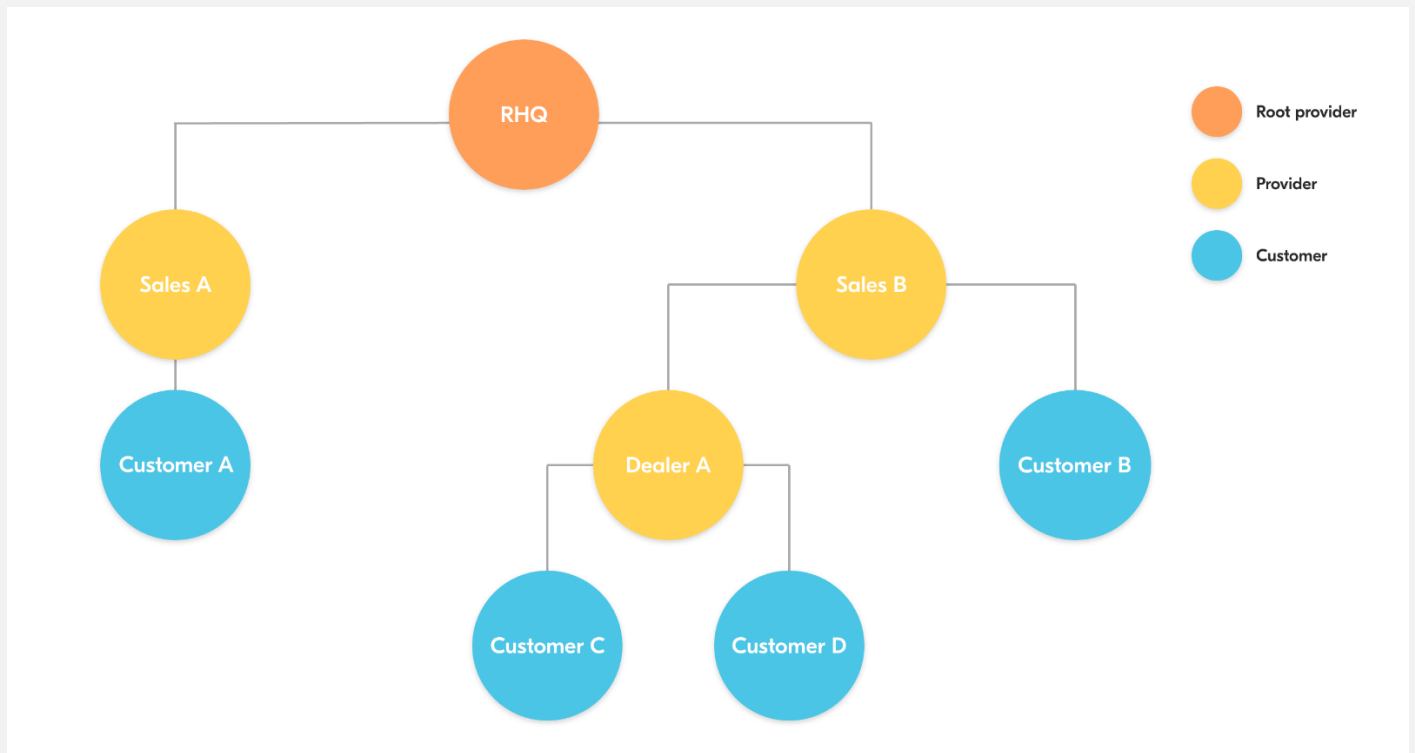


3. Multitenancy

KCPS uses multi-tenancy to accommodate multiple sales companies, dealers, and customer organizations. Each sales company, dealer, and customer are treated as one organization. Access control is enforced through a hierarchical tree structure. (Fig. 2-1)

Organizations are classified into two types: a provider organization and a customer organization. A provider organization is focused on managing one or more customer organizations. Provider organizations have auditing and reporting features while customer organizations would provide features directly related to office functions like printing and scanning.

The hierarchical structure is patterned after the common sales hierarchical structure used in Kyocera. An RHQ (regional headquarters) is the parent organization (root provider organization) with sales companies under the RHQ as children provider organizations. Customers of sales companies would be the customer organizations and leaf nodes in the hierarchical tree structure.



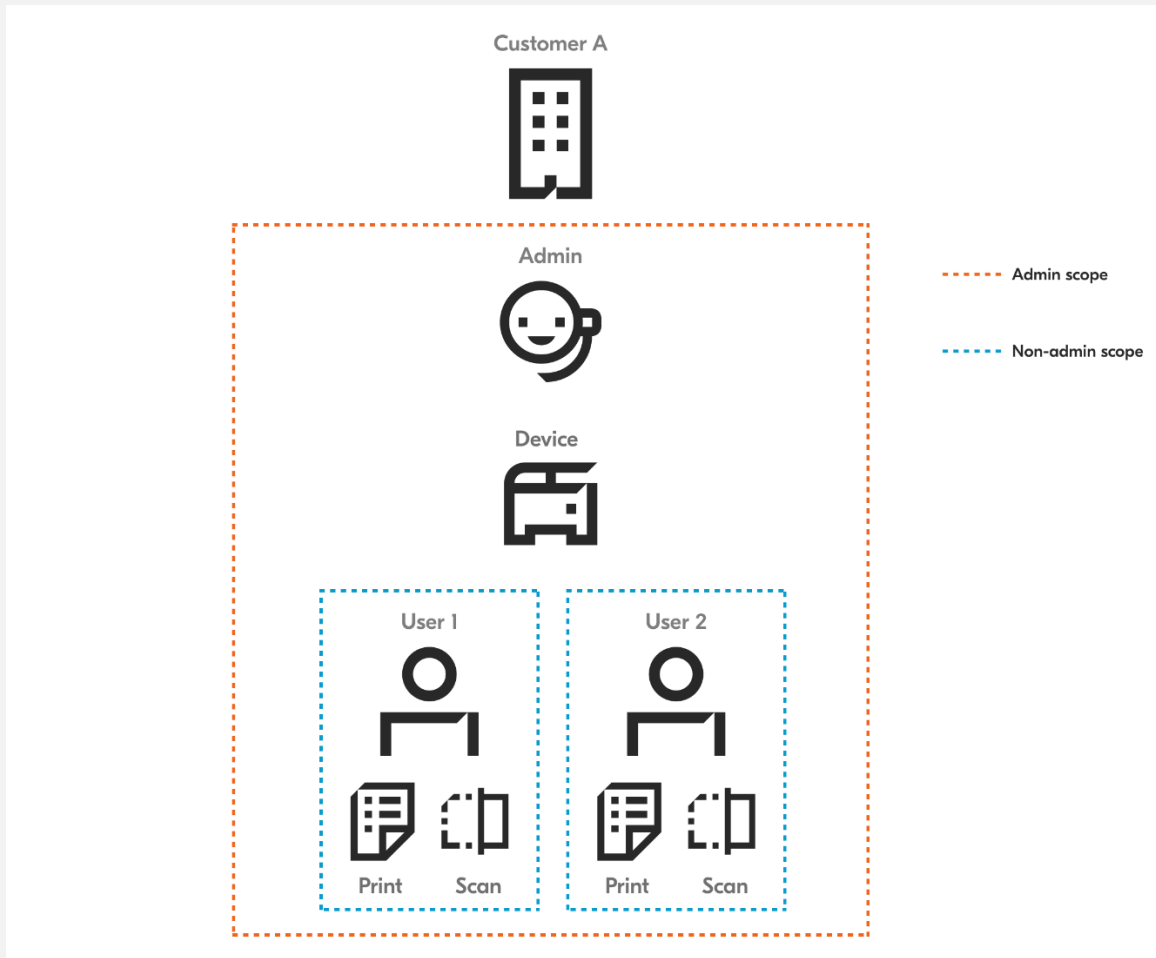
(Fig. 2-1) Hierarchical structure of KCPS Organizations

Any organization cannot view the data of another organization except for the parent organization. Data in customer organizations typically consists of user information, user’s job data (e.g. print and scan jobs, job information), devices associated with the customer organization, and logs (jobs/pages printed, pages scanned). Data is scoped and access to data is limited. (Table 2-1)

| User type | Users of customer organization | Devices of customer organization | Report (jobs/pages printed/scanned) | Customer job data (print and scan documents) |
|---------------------------------|---|----------------------------------|-------------------------------------|--|
| Provider admin | Inaccessible | Accessible | Inaccessible | Inaccessible |
| Provider support | Inaccessible | Accessible | Inaccessible | Inaccessible |
| Customer admin | Accessible | Accessible | Accessible | Accessible Can view own job data only |
| Print manager | Accessible Print quota settings only | Inaccessible | Inaccessible | Accessible Can view own job data only |
| Customer user | Inaccessible | Inaccessible | Inaccessible | Accessible Can view own job data only |
| Users not in KCPS system | Inaccessible | Inaccessible | Inaccessible | Inaccessible |

(Table 2-1) Access to organization and user data by user type

For instance, if User 1 and User 2 are both users in organization Customer A, User 1 can only see his own print and scan jobs and cannot see print and scan jobs of User 2. (Fig. 2-2)

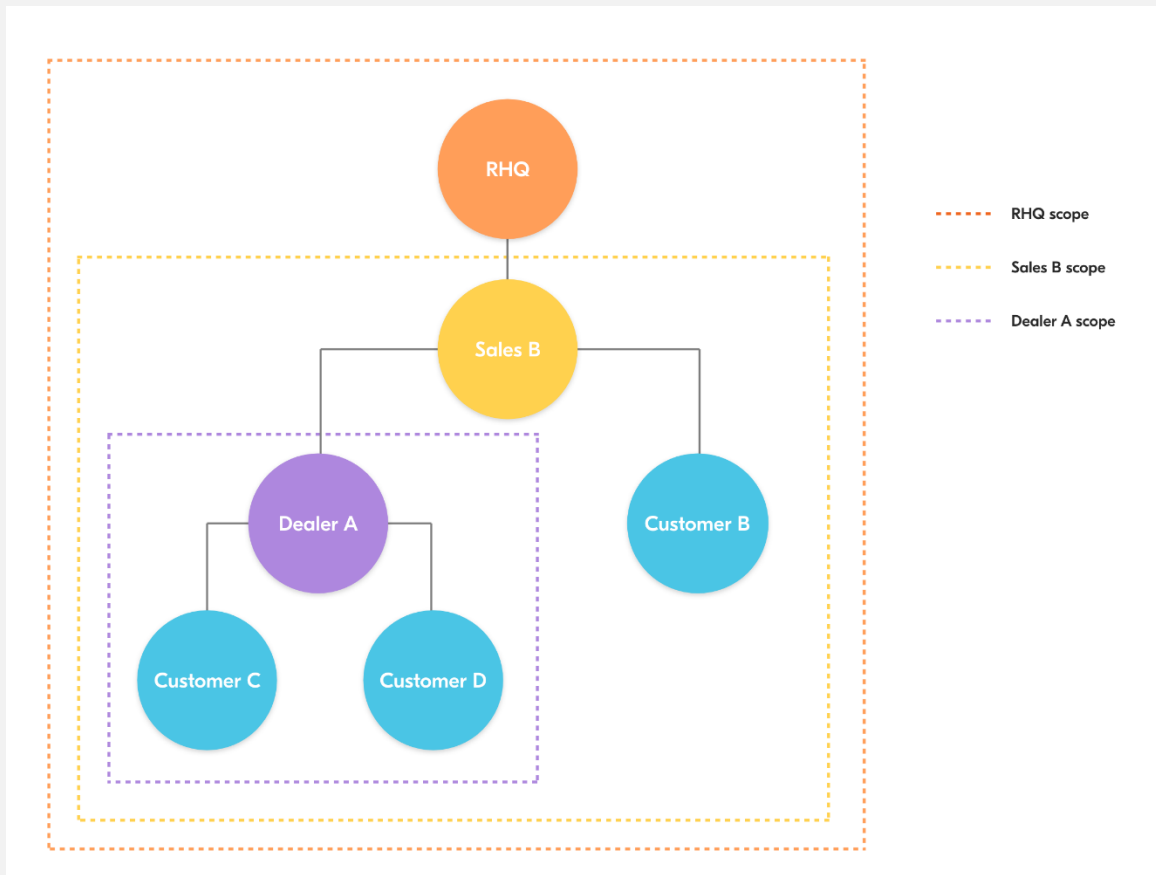


(Fig. 2-2) Access to user data for a customer organization

Additionally, User 1 and User 2 cannot see other users in organization Customer A from the customer portal, only Admin (who is an admin in Customer A) can see User 1 and User 2 (and himself, Admin) as users in the organization Customer A.

Finally, Admin cannot see print or scan jobs of other users, but Admin can see devices registered and associated to the organization Customer A.

Scopes are also present between root provider, provider and customer organizations. At the organization level, data that is tracked and shared are license-related information (e.g. how many devices a customer organization is allowed to register) to help with billing. (Fig. 2-3)



(Fig. 2-3) Access to license-related information for each organization

The visibility of this data goes upward to parent organizations. This means that RHQ can see the aggregated data of Customer B, C and D but will not be able to distinguish between these organizations. This is because the organization names are anonymized in the provider contract reports. Similarly, Sales B can see aggregated data of Customer C and Customer D and will not be able to distinguish between them.

It is worth noting that parent organizations can identify the organizations that they created, since they created those child organizations themselves (and set the organization name during creation of the organization). This means that Sales B can see data of Customer B separately and identify that data as separate from aggregated Customer C and Customer D. Similarly, Dealer A can see and distinguish data between Customer C and Customer D.

4. User Identification and Authentication

When accessing KCPS, the user must log in with an activated account. An unauthorized user cannot access KCPS. The following features are supported as security features for login:

4.1. Account Lockout Policy

The Account Lockout Policy protects KCPS from password cracking attacks. When a user fails to login a pre-determined number of times, the user account will be locked for a certain period.

As shown in the table below, when reaching the account lockout threshold for failed login attempts of three times, the account will be locked. The setting will unlock the account after 30 minutes.

| | |
|--|------------|
| Number of continuous failed login attempts | 3 attempts |
| Auto Unlock Time | 30 minutes |

4.2. Password Policy

A user needs to employ a strong password that is difficult to be analyzed and must be applicable to the KCPS Password Policy.

A password that does not meet the password policy is prohibited. This policy prevents users from setting simple passwords and guards against unauthorized access by a third party.

In addition to the password policy, another layer of security is not storing the password in the database; only the hash of the password is stored which prevents the user's password from being known in case a copy of the database has been leaked. Every time a user enters their credentials, the hash value of the password entered will be compared to the password hash value saved for that user.

The browser also masks all passwords in password input fields to prevent people in the vicinity of the user from casually reading the user's password from the screen.

The password length and complexity of password are defined in the table below.

| | |
|---------------------|--|
| Password Length | Between 8 to 64 characters |
| Password Complexity | Include at least one character from each category: <ul style="list-style-type: none">- numbers between 0 and 9- uppercase letters*- lowercase letters*- special symbols (!"#%&'()*+,-./:;<=>?@[]^_`{ }~) |

| | |
|--|---|
| | *Only English alphabet characters (no Unicode characters like umlaut, Japanese kanji/hiragana/katakana, etc.) |
|--|---|

4.3. Automatic logout

In order to prevent the case when a user has logged-in but has left their device un-attended, an automatic logout feature has been implemented to automatically log out the user upon detecting that their logged-in session has been idle after a certain period.

This automatic logout applies to all clients accessing the KCPS server; MFP/HyPAS, Desktop client, and web browser.

For the Desktop client, the automatic logout duration has been made to be customizable to cater to the specific needs of RHQs.

4.4. PIN Authentication

In order to cater to the ease of use of the KCPS HyPAS application, PIN authentication was implemented for easier login on the MFP. The PIN is a unique and randomly generated 6 digit number. In order to support security for the PIN authentication, the following features have been implemented:

- PINs are only generated by the KCPS system; i.e. user cannot specify their own PIN. The KCPS system makes sure that the randomly generated PINs are not duplicated among users
- New PINs can only be regenerated once every seven days; this prevents attempts for possible exhaustion of unique PINs

4.5. ID Card Authentication

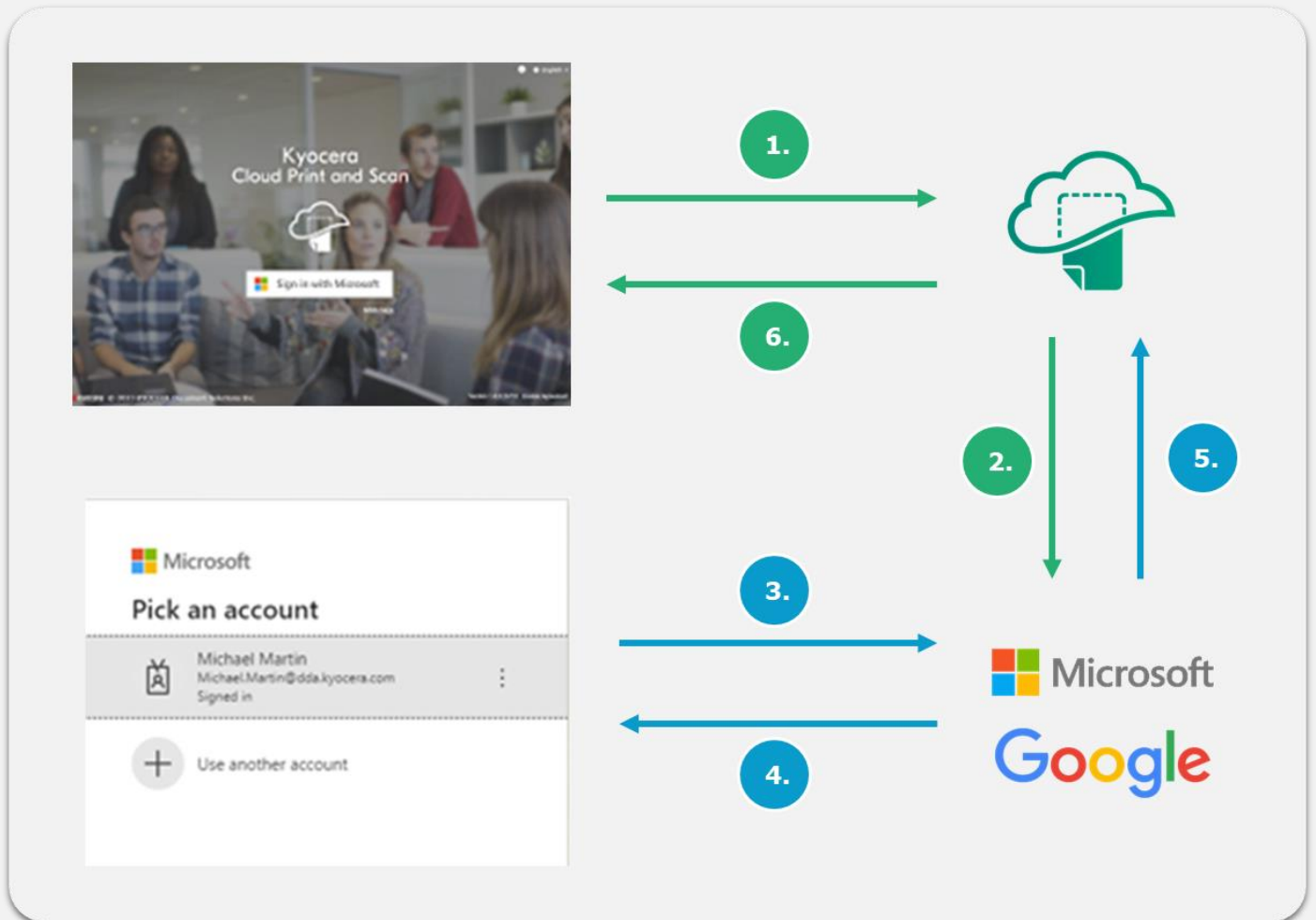
Support for ID card authentication has also been added as an alternative method for ease of logging onto the KCPS HyPAS application. Registration and management of ID cards (e.g. deletion of a previously registered ID card) is performed on the KCPS web application. Registration of ID cards can also be performed on the HyPAS application after a user authenticates in the HyPAS application.

4.6. 3rd Party Authentication and Identity Servers

Support for 3rd party Authentication and their corresponding identity servers is supported by KCPS.

4.6.1. 3rd Party Credentials and OAuth2

KCPS provides the facility to connect 3rd party storage and authenticating using Microsoft Entra ID or Google Workspace credentials instead of separate KCPS credentials. KCPS follows the industry standard for OAuth2 authentication flows.



1. User clicks on "Sign in with Microsoft".
2. KCPS calls Microsoft APIs to being the OAuth2 with Microsoft Entra ID credentials.
3. User is redirected to a login page that Microsoft controls.
 - Since this is a page that Microsoft controls, any additional authentication features that Microsoft supports will also be supported on this login page. (e.g. 2FA/MFA)
4. User follows the authentication prompts. (e.g. enters their username/email + password, performs 2FA/MFA)
5. Microsoft returns the result of authentication (whether successful or not) to KCPS.
6. Control is returned to KCPS and KCPS serves the appropriate page. (e.g. if authentication with Microsoft is successful, user is logged into KCPS)

This OAuth2 authentication flow is the same for other 3rd party service providers (e.g. storage providers that are supported like OneDrive, Google Drive, Box, and SharePoint). When authentication is initiated to link to these 3rd party service providers, a separate web page is loaded and authentication is performed on pages controlled by those 3rd party service providers.

KCPS will never have access to or a copy of the user credentials entered for 3rd party services.

4.6.2. Microsoft Entra ID

Microsoft Entra ID (formerly known as Azure Active Directory / Azure AD) is supported by the web application. Once the administrator configures a customer organization to use a specific Microsoft Entra ID instance, users that exist on that Microsoft Entra ID instance can login to the KCPS web

application and Desktop client using their Microsoft Entra ID credentials.

When a user successfully logs in to the KCPS web application or Desktop client using their Microsoft Entra ID credentials, a KCPS user is created pulling information from their Microsoft Entra ID identity (email, group info). This KCPS user is a separate KCPS identity on the KCPS web application. Some things are important to note in this regard:

- KCPS does not keep Microsoft Entra ID credentials; KCPS follows the OAuth2 authentication workflow and always routes to Microsoft Entra ID to verify credentials
- KCPS does not manage the Microsoft Entra ID user
 - o If the equivalent KCPS user is deleted on KCPS, the Microsoft Entra ID user is not deleted and still exists on Microsoft Entra ID
 - o If the Microsoft Entra ID user is deleted, the KCPS user will still exist on KCPS but will not be able to authenticate into KCPS with Microsoft Entra ID credentials because the Microsoft Entra ID user no longer exists

When Microsoft Entra ID is configured for the organization, a user will not be able to login to HyPAS using their Microsoft Entra ID credentials. ID card and PIN login are still available for the user to authenticate into the KCPS app on HyPAS.

4.6.3. Google Workspace

Google Workspace is supported by the web application. The cases described in the Microsoft Entra ID section are also supported for Google Workspace. In addition to those cases, Google Workspace also supports the following:

- Import of users from the Google Workspace; this process is manually initiated from the web portal.

5. Firewall Configuration

Required Ports:

| Source | Destination | Protocol | Port | Service |
|----------------------------|---------------------|----------|------|---|
| MFP / HyPAS | KCPS Server | TCP | 443 | HTTPS: Login and send job log and scan data to KCPS |
| KCPS Desktop Client | KCPS Server | TCP | 443 | HTTPS: Login and send job list to KCPS |
| Web Browser | KCPS Server | TCP | 443 | HTTPS: Access to the UI |
| KCPS Desktop Client | Printer/MFP | TCP | 443 | HTTP: IPP Printing (For non-HyPAS models) |
| KCPS Desktop Client | Printer/MFP | TCP | 631 | HTTPS: Secure IPP Printing (For non-HyPAS models) |
| KCPS Desktop Client | KCPS Desktop client | TCP | 5570 | HTTP: Used for internal / local communication only |
| MFP / HyPAS | KCPS Desktop client | TCP | 5571 | HTTPS: Get job list and job data |
| KCPS Desktop Client | KCPS Desktop Client | TCP | 5572 | HTTP: Used for internal / local communication only (For non-HyPAS models) |
| KCPS Desktop Client | Printer/MFP | TCP | 9091 | HTTPS: Get printer information (For non-HyPAS models) |

Please consult with your local IT to open these ports for KCPS communication.

6. Data Protection Technical Details

This chapter is intended for those with technical knowledge.

6.1. Protection of Stored Data

KCPS's information assets must be protected and not leaked or lost. KCPS implements security protection measures for stored information assets and a data recovery support through the features described below.

6.1.1. Access Control

KCPS's environment resources will be restricted to only individuals who will be maintaining/monitoring the environment (henceforth referred to as "operators", e.g. IT Ops, DevOps). Only operators with proper access control will have access to KCPS's AWS environment resources and as well as application data. Operators will be required to have proper RBAC (role-based access control) authorization.

6.1.2. Authentication

KCPS's database requires operator authentication to gain access to database data. Authentication credentials are configured during setup.

6.1.3. Encryption

KCPS uses the highest encryption standard supported by the Play Framework (2.6.6) and Silhouette (5.0.0) library version used: SHA-256 bit. Within the KCPS server, this encryption is specifically used for authentication (generating the authentication hash when a user makes a login attempt).

As described in Chapter 8 (AWS Security Technical Details), KCPS is hosted on the AWS platform. And MongoDB is used for the database.

AWS provides encryption at multiple levels to help secure your data, including encryption at rest, encryption in flight, and key management (using AWS Key Management), allowing AWS to support various encryption models.

Disks used by AWS Virtual Machines are protected by disk encryption. This protects both OS disk and data disks with full volume encryption. Disks are encrypted using 256-bit Advanced Encryption Standard (AES) and transparent to users.

Data at rest in KCPS's database is encrypted via MongoDB Atlas's provided encryption in their enterprise version. MongoDB utilizes by default 256-bit Advanced Encryption Standard in cipher Block Chaining mode (AES256-CBC), with other encryption options available. Encryption key used

by MongoDB can be taken from the cloud provider’s Key Management Service, with MongoDB automatic key rotation every 90 days. The encryption process is transparent to users.

Data stored via AWS S3 storage has default encryption provided. S3 encryption can utilize AWS managed keys or customer master keys stored within the key management service.

Data in transit is also encrypted.

6.1.4. Information utilized by KCPS

| KCPS Component | Information Assets (Used for the purpose of identification and communication within KCPS) |
|---------------------|---|
| KCPS Server | <ul style="list-style-type: none"> • Organization information (URLs of each portal, email addresses of admins of each organization, organization type, license information, data retention periods) • User information (first and last names, username, email address, authentication hashes, authentication tokens of linked cloud storage accounts) of each KCPS user • Device information (serial number, network information such as host name and IP address) of each KCPS device, used for device registration and report generation. • Device logging information (number of scans, other device operations) for the purposes of usage report compilation (to assist with billing) and for maintenance/troubleshooting. • Print and scan job information • Print jobs (if cloud spooling) and scan jobs • Usage reports (used for billing purposes) by user, user group, device, provider and customer organizations. |
| KCPS HyPAS | <ul style="list-style-type: none"> • Authentication tokens generated by KCPS Server to authenticate the device or logged-in KCPS user to send info to and receive info from KCPS server. • Documents (PDF/JPG) to print or scanned from the device • Metrics (jobs and pages printed and scanned) |
| KCPS Desktop client | <ul style="list-style-type: none"> • Proxy settings of the network where the desktop is connected to; used to facilitate communication between the KCPS Desktop client and the KCPS Server • Authentication tokens generated by KCPS Server to authenticate the device or logged-in KCPS user to send info to and receive info from KCPS server. • Documents (PDF) printed from applications using the Desktop client print queue. Local spooling stores the PDF print jobs locally on the desktop while Cloud spooling uploads the PDF print jobs to the KCPS Server. |

| | |
|-----------------------|---|
| | <ul style="list-style-type: none"> Documents (PDF) locally stored on the desktop are at the following folder locations: <ul style="list-style-type: none"> ➤ (Windows) C:\Users\<username>\AppData\Local\KCP</username> ➤ (Mac) /Users/Shared/Library/Kyocera Cloud Print and Scan Print job information (document name, number of pages, location for KCPS HyPAS to download the print job from). |
| KCPS Chrome extension | <ul style="list-style-type: none"> Authentication tokens generated by KCPS Server to authenticate the device or logged-in KCPS user to send info to and receive info from KCPS server. |

6.1.5. Data Backup

KCPS database backup on AWS is facilitated by MongoDB Atlas. MongoDB Atlas provides configurable cloud backup, which is managed by MongoDB. The current backup schedule is set to twice a day, kept for 7 days. Database restoration is also facilitated by MongoDB Atlas.

6.2. Protection of Communication Data

KCPS protects communication data regarding user access to use KCPS, and data communication to transfer data between KCPS and devices, respectively.

In order to protect KCPS communication data from masquerading, tapping or modifying the data, the communication data is encrypted, and KCPS components are mutually authenticated.

6.2.1. User Access

When a user accesses KCPS from an application (web application using a browser, Desktop client, or HyPAS application), an authenticated communication channel is established. KCPS user can access KCPS portal from the Web browser’s client UI regardless of the user role. When a user accesses KCPS portal, the user is always identified and authenticated. If this identification and authentication are successful, the user can access KCPS portal based on his/her role. KCPS portal protects the communication data through HTTPS.

6.2.2. HTTPS protocol

HTTPS works over underlying secure protocols (TLS) that encrypt all traffic between browsers and servers. TLS require a certificate with a private key, a public key, domain information, and a chain of signatures by certificate authorities.

In KCPS, TLS is used to secure and protect sensitive information that is shared between KCPS server and a browser, device, or database. This information includes:

- KCPS user credentials and passwords
- Device authentication information
- User data

- Job metrics (print and scan jobs, pages printed, color settings used, etc.)

6.3. Secure communication between the KCPS server and databases

KCPS on AWS will establish network connection to database using TLS encrypted network traffic. Database access is restricted to connections coming from Atlas's IP access list with the proper database authentication credentials.

6.4. Direct Print / Scan from Box Storage

To provide an additional data privacy and security for customers, when a customer links their Box storage to KCPS, printing from Box storage or scanning to Box storage (fax forwarding included) will bypass KCPS temporary storage and print directly from or scan directly to Box storage.

6.5. Security vulnerability testing

In order to keep the KCPS system up-to-date with the latest security measures the following schedule will be followed for security vulnerability assessment:

- Perform internal security vulnerability assessment for each software release build release.
- Periodic vulnerability assessment in accordance with server management regulation.
- If the configuration of the public server has changed significantly, such as an upgrade, perform vulnerability assessment as necessary.

7. Device Authentication

To protect sensitive information transmitted between KCPS and Kyocera devices, security is enforced through HTTP over TLS. By default, the TLS protocol is enabled as the default for device communication.

The following options can be set in device authentication:

- Simple login
- ID card login
- PIN login

8. AWS Security Technical Details

KCPS is hosted on the AWS platform. AWS meets the broad set of internationally recognized information security controls and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2 (see the detailed list of compliant standards in AWS Security Whitepaper).

The hosting environment is designed to utilize the AWS provided services and security features to help secure and monitor our application. The various features that are utilized include:

- Various AWS credential for login/access
- Security logs
- Instance isolation
- Firewalls/API access
- Secure HTTPS access points
- Network security (VPC isolation, Network Security groups, Network Access Control List, Internet Gateway, etc.),
- Storage
- Simple Notification Service monitoring CloudWatch application logs

KCPS is deployed to the following AWS regions:

- Tokyo (ap-northeast-1)
- Frankfurt (eu-central-1)
- North Virginia (us-east-1)

Refer to the [Introduction to AWS Security](#) and [AWS Security Documentation](#) for more details regarding global infrastructure and service-specific security.

KCPS uses MongoDB Atlas hosted on AWS for database storage. The hosted database cluster resides in the same region as the KCPS instance. This database cluster is configured as a 3-node replica set. MongoDB Atlas automatically deploys each node across availability zones within the region for redundancy and high availability.

Refer to [MongoDB Atlas AWS Reference document](#) for details regarding database cluster creation and deployment on AWS.

9. Contact Information

If you have any questions or comments, please contact us using the following information below.

<https://www.kyoceradocumentsolutions.co.uk/>

©2024 KYOCERA Document Solutions Inc.

KYOCERA Document Solutions (UK) Ltd.

75-77 London Road, Reading, RG1 5BS

Tel: 0118 931 1500 – Fax: 0018 931 1108



[Kyoceradocumentsolutions.co.uk](https://www.kyoceradocumentsolutions.co.uk)

KYOCERA Document Solutions does not warrant that any specifications mentioned will be error-free. Specifications are subject to change without notice. Information is correct at time of going to press. All other brand and product names may be registered trademarks or trademarks of their respective holders and are hereby acknowledged.