TA/UTAX Cloud Capture:

Security White Paper

Document Version: 01/2026

January 6, 2026

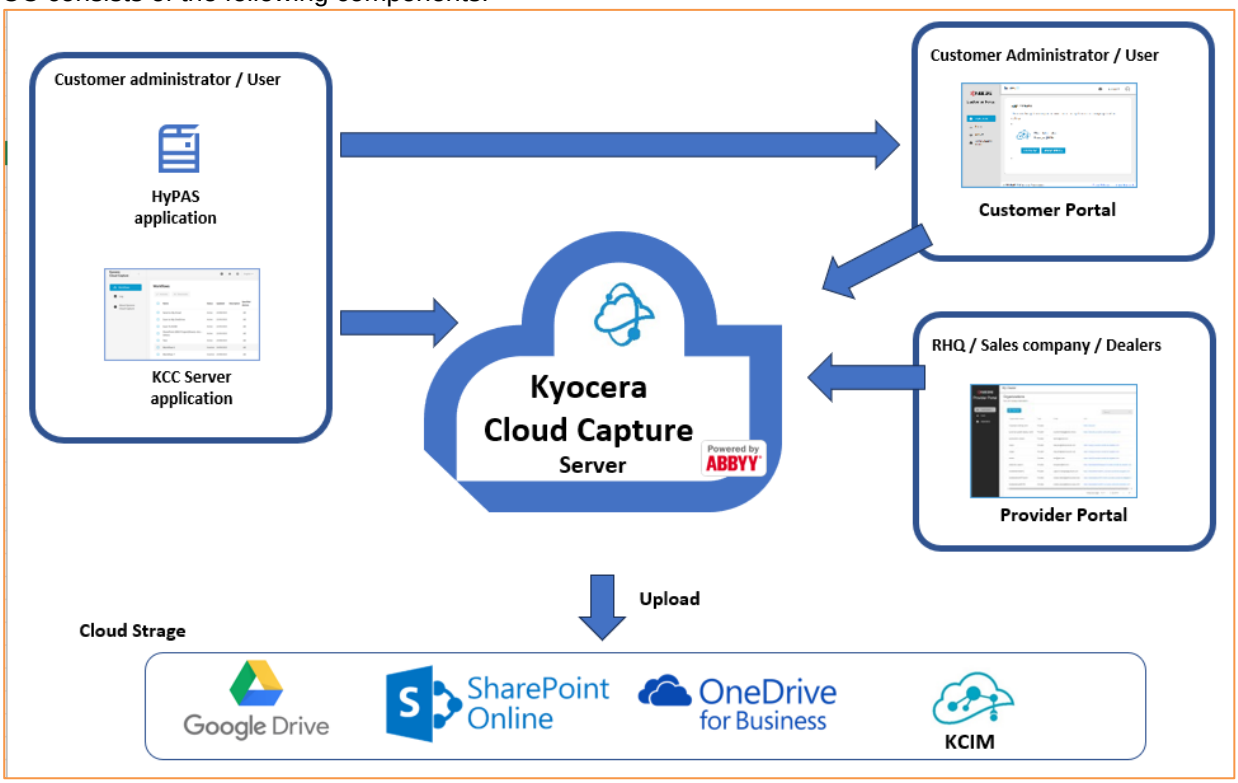
About this document

This document is confidential. For internal use only.
This document describes TA/UTAX Cloud Capture (CC)

1. Overview

Cloud Capture (CC) is a cloud-based capture solution that allows users easy connect the input data to the Digital Cloud Platform.
This white paper informs dealers and users about security measures in CC. The priority is to provide secure protection of information assets that are handled by CC. These information assets are rigorously protected by the secure configuration and security features of CC.

CC consists of the following components:



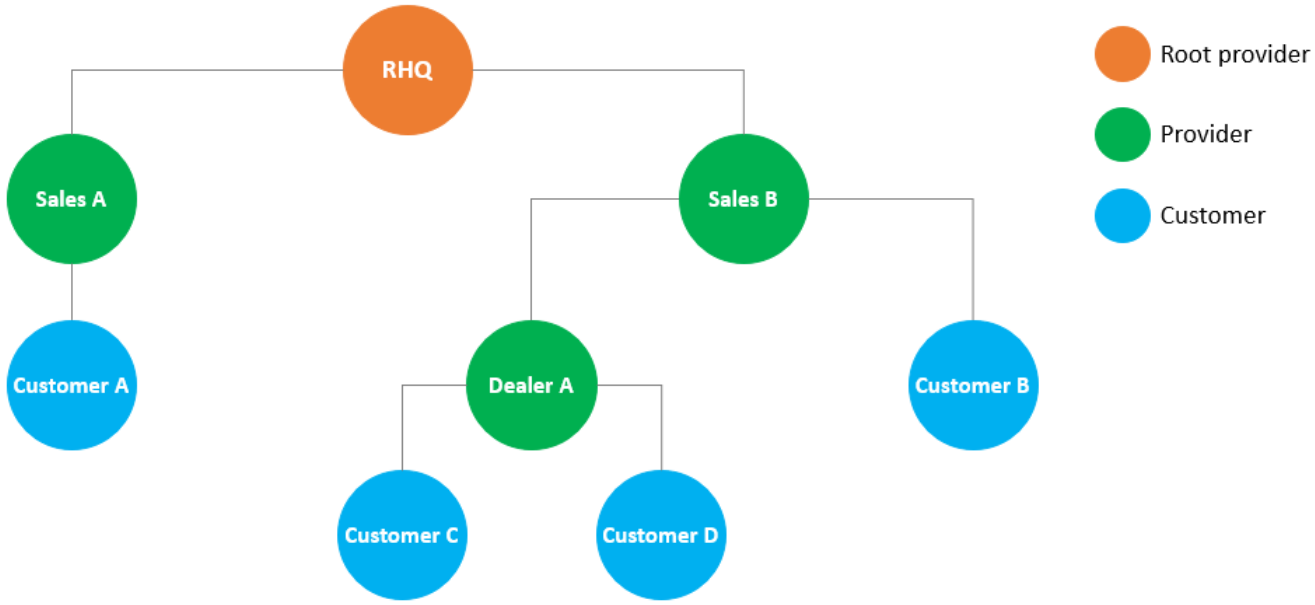
- **CC:** CC is a cloud capture system that provides customers with image processing, file format conversion, and indexing features.
- **Server application:** Customer administrators or customer user can access server application of CC using a web browser. Customer administrators can configure the scan workflow, view the logs, and download Admin Guide. Customer user can download User Guide.
- **HyPAS application:** The HyPAS application must be installed for MFP to upload documents from MFP to CC. The HyPAS application connects to CC. Customers can scan and upload their documents to CC using this application.
- **Digital Cloud Platform:** A platform built on the cloud that runs a cloud-based system that includes CC and the Customer Portal, Provider Portal, and Root Provider Portal.
- **Customer Portal:** The customer administrators or customer user can access the Customer Portal using a web browser. The customer administrators can add user accounts for their own organization and register MFPs. Customer users can register their user account with CC to establish a link between third-party cloud storage and CC and download the user guide.
- **Provider Portal:** The provider (SCs, Dealers, Distributors) can access the provider portal using a web browser. They can add, edit, or delete organizations for child providers or for their customers.
- **Root Provider Portal:** The root provider (RHQs) can access the root provider portal using a web browser. Features are same as the provider portal as of v1.0.

2. Multitenancy

CC and DCP 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 the document management feature.

The hierarchical structure is patterned after the common sales hierarchical structure. 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 terminal nodes in the hierarchical tree structure.



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

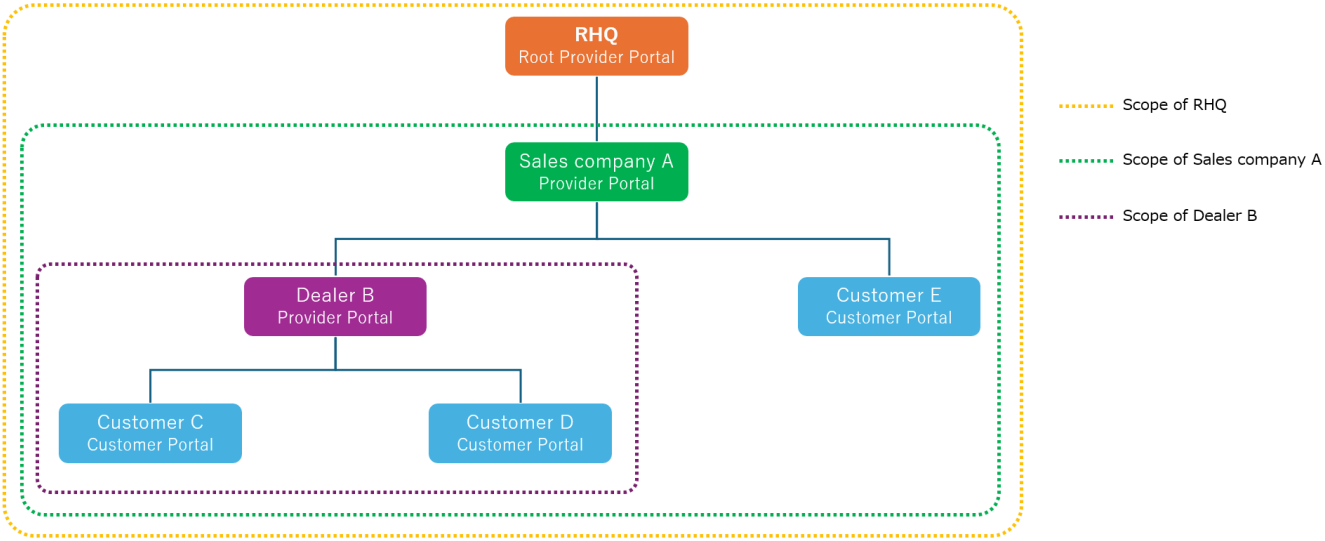
Any organization cannot view the data of another organization except for the parent organization.
The parent provider only can get usage counter information and the contact information of the organization representative from the customer. The usage count is the data related to the license information such as storage usage size and the subscription information.
Data is scoped and access to data is limited. (Table 2-1)

User type	Users of customer organization	Contract information (OCR count, document count and size)
Provider Admin/Support	Inaccessible	Accessible
Customer Admin	Accessible	Accessible
Customer user	Inaccessible	Accessible Can view contract information only

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

Scopes are formed between parent and child organizations, and are used for data inheritance and access management. At the organization level, when a child organization is created, its parent organization's document class definition data (document classes and attributes of the document classes) are inherited.

Also, the parent organization can manage the subscription information of the customer child organization (e.g. how many OCR pages) to help with billing. (Fig 2-3)



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

The direct visibility of this data is only between parent and child organization. But RHQ can retrieve the entire child organization's usage data. The provider portal can generate a report of subscription status of the entire organization hierarchy but the detail organization information will be anonymized.

3. Communication security between modules

Transport Layer Security (TLS) is a standard security technology for establishing an encrypted link between a server and a client. In CC and all DCP services, TLS is used to secure and protect sensitive information that is shared between CC and a browser, device, mobile or database. This information includes:

- CC/DCP user credentials and passwords
- User data
- Document information (document, OCR data, index data, metadata, etc)
- Document count metrics (OCR page counts, etc.)

No third party on the network can decrypt or tamper with the payload in transit.

3.1. Security between HyPAS application and CC server

The following table lists the TLS versions available when the HyPAS application is installed on CC-supported devices. For models with multiple supported TLS versions, the version used depends on the FW version. If the latest version of FW is installed, 1.3 is used.

	Project name	TA model	TLS version
A3 MFP	Tomcat 4	4063i 3263i	1.3/1.2
	Iris 2	6007ci 5007ci 4007ci 3207ci 2507ci	1.3/1.2
	Iris 2020	7008ci 6008ci 5008ci 4008ci 3508ci 2508ci	1.3/1.2
	Iris 2020 mono	7058i 6058i 5058i	1.3/1.2
	Iris 2 mono	6057i 5057i	1.3/1.2
	Zeus 4	9057i 8057i 7057i	1.2
	Mercury 4	8307ci 7307ci	1.2
	Iris 2024	7009ci 6009ci 5009ci 4009ci 3509ci 2509ci 7059i	1.3/1.2

		6059i 5059i	
	Athena	9515ci 8515ci 7515ci 10565i 9565i 8565i 7565i	1.3
	Matsuri 3	P-3241i MFP	1.3/1.2
A4 MFP	Perseus 2 High	352ci 402ci 502ci	1.3/1.2
	Polaris E Plus	P-6038i MFP P-6038if MFP	1.2
	Polaris Next HyPAS	P-4532i MFP P-6039i MFP P-5539i MFP P-4539i MFP	1.3/1.2
	Libra 2	P-4027iw MFP	1.3/1.2
	Virgo	P-C3563i MFP P-C3567i MFP P-C4063i MFP P-C4067i MFP 358ci 458ci	1.3/1.2

4. User Identification and Authentication

When accessing CC, the user must log in with an activated account. An unauthorized user cannot access CC. The following features are supported as security features for login.
CC uses OAuth 2.0 authentication method by Keycloak. For more information about Keycloak, see Chapter 5.

4.1. Account Lockout Policy

The Account Lockout Policy protects CC 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. The locked account also can be unlock by the admin manually. Password reset will unlock the account if the login attempt is coming from same browser (same tab_id) that requested password reset.

Number of continuous failed login attempts	3 attempts in 15 minutes
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 CC/DCP 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.

All authentication is securely processed based on OAuth 2.0 using Keycloak.

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: Upper case (A ~ Z) Lower case (a ~ z) Numbers (0 ~ 9) Symbols (!"#$%&'()*+,-./:;<=>?@[]^_`{|}~)

4.3. Username Policy

Username policy is put in place to verify if the value is a valid username. This prevents special characters which may be used in SQL injection[1]

Username Length	Between 4 to 64 characters
Prohibited characters	Symbols \ / : , ; * ? " < > | [ ] { } $ % ` & ( ) + =| ! # ' ~ ^ spaces

Note: Users who have created a username including spaces or ! # ' ~ ^ in version 1.0 may still login and

[1] Refer to SQL injection - Glossary | CSRC (nist.gov) for more detail information.

continue CC usage, however, it is recommended to update your login username. When updating your username, the new policy must be followed to save.

4.4. First name/Last name policy

A policy for first name/last name fields is in place to prevent certain special characters which may be used in SQL injection. The validator checks if the value is a valid person name as an additional barrier for attacks such as script injection.

Allowed symbols	-@.'`+:,

Note: Users who have created a first name/last name in version 1.0 which included any symbols other than the above mentioned, may continue CC usage, however, it is recommended to update your first name/last name fields to follow the new policies. When updating your first name/last name fields, the new policy must be followed to save.

4.5. PIN Authentication policy

PIN code authentication allows users to log in easily using a 6- or 8-digit numeric code they set. Administrators can configure the code length policy, with some regions requiring 8-digit codes only. This balances ease of use with security.

PIN code length	6 digit or 8 digit

4.6. IC Card Authentication policy

Supports IC card authentication to enhance user security. This prevents unauthorized access and ensures a highly secure usage environment. The authentication process is simple and fast, improving overall convenience.

4.7. Multi Factor Authentication policy

Email-based Multi-Factor Authentication (MFA) leverages users' existing email addresses, adding an extra security layer by requiring a verification code sent via email, reducing the risk of unauthorized access even if passwords are compromised. This method enhances user convenience as no special apps are needed.

Verification code expiration	5 minutes

4.8. Microsoft Entra ID

CC allows administrators to federate the system with their organization's Entra ID tenant. This allows you to synchronize user information from the Entra ID tenant to the DCP, and allow users to log in using their Entra ID account information.

When you log in, it uses an authentication method called OAuth 2.0, and a pop-up screen appears asking you to enter your Entra ID account information. This screen is managed on the Entra ID side, and if multi-factor authentication (MFA) is enabled on the Entra ID side, this is also done here. Note that MFA for Entra ID is managed separately from MFA settings in the Customer Portal and cannot be controlled by the Customer Portal.
As of version 1.7, Microsoft Entra ID authentication is available in the Customer Portal.

5. Firewall Configuration

To allow applications operated by customer administrators and customer users to access cloud servers on the Digital Cloud Platform, the firewall settings in the customer environment must be changed to allow communication on specific ports.

Required Ports:

Case	Connection source application (operating terminal)	Destination	Protocol	Port	Services
1	Hype's application（MFP client）	Cloud server（CC）	HTTPS/TCP	443	Get scan workflow, specify destination folder, upload scanned images
2	HyPAS application（MFP client）	Cloud server（Customer Portal）	HTTPS/TCP	443	Login, register devices
3	Server application（Web browser）	Cloud server（CC）	HTTPS/TCP	443	Set scan workflow settings, review logs, download guides
4	Customer Portal（Web browser）	Cloud server（Customer Portal）	HTTPS/TCP	443	Login, user / role / device management, download guides

*Cloud servers are exposed to the Internet through a load balancer, and the load balancer has a fixed IP address. This ensures stable and secure access control because the IP address to which services are accessed does not change.

IP addresses to allow
Register the static IP address of the load balancer provided by the service. Registering by IP address rather than domain name or URL avoids DNS resolution effects and caching issues.

How to obtain IP Addresses
You can check the IP address from the URL of the cloud server in the following ways:

- Use "ping" command
  Example:You can use "ping [host name]" at the command prompt or terminal displays the IP address of the responder.
- Use "nslookup" command
  Example:You can use "nslookup [host name]" to get the IP address from the DNS lookup result.

There are three types of IP addresses for each case. You can obtain each IP address from the following host names.

- Case 1, 2: Host name "device.dpio.kyocera.biz"
- Case 3: Host name of the URL of the screens other than the login screen
- Case 4: Host name in the URL of the login screen

Please register the three IP addresses obtained by these methods in the firewall.

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

6. Keycloak security features

The CC uses Keycloak as an identity/authentication management service that supports OAuth 2.0. Keycloak is an open source authentication management system that supports a variety of security features.

6.1. Threat model Mitigation

Keycloak mitigates the below possible security vulnerabilities as an authentication server.

- Password guess: brute force attacks
- Read-only User Attributes
- Clickjacking
- Cross-site request forgery (CSRF) Attacks
- Unspecific Redirect URIs

7. Protection of Stored Data

CC doesn't store user's data except workflow configuration that contains user's storage connection information. The CC uses the SharePoint connector, Google Drive connector, OneDrive connector, and KCIM connector to send document data to SharePoint Online, Google Drive, OneDrive, and KCIM specified in the workflow type. The customer admin has to accept consent form to give a permission for SharePoint connector and OneDrive connector to access the user's data. The user has to also accept a consent form that grants permissions to the Google Drive connector.

7.1.1. Access Control

The customer admin has to accept consent form to give a permission for SharePoint connector to access the user's data. SharePoint connector will not manipulate any data nor store user's data inside CC. The user has to also accept a consent form that grants permissions to the GoogleDrive connector. The GoogleDrive connector does not manipulate data and does not store user data in CC.

7.1.2. Authentication

CC user needs to authenticate to DCP to gain access to CC workflow definition and third party connectors.

7.1.3. Encryption

CC database uses AES256 algorithm for encryption.

7.1.4. Data Backup

Daily backup for database runs automatically. It is stored on Google Cloud Storage and encrypted by AES256.
Backup data resides outside the primary hosting environment and is stored and replicated to a secure external location for geographic redundancy and disaster recovery requirements. In addition, backup data is distributed and stored redundantly in multiple regions within the corresponding area. This enables data recovery in the event of a hosting environment failure or regional disaster. The backup data retention period is 7 days.

Geographic region	Backup region name	Backup Region Description
TA/UTAX	eu	Data centers in the European Union

7.2. Protection of Communication Data

CC protects communication data regarding user access to use CC, and data communication to transfer data between CC and devices, respectively.
In order to protect CC communication data from masquerading, tapping or modifying the data, the communication data is encrypted, and CC components are mutually authenticated.

7.2.1. User Access

When a user accesses CC from a web application using a browser, an authenticated communication channel is established. CC user can access CC web portal from the Web browser's client UI regardless of the user role. When a user accesses CC web portal, the user is always identified and authenticated. If this identification and authentication are successful, access token will be issued and the user can access CC web portal based on user's role. CC web portal protects the communication data through HTTPS.

7.2.2. Access token and refresh token

Once the authentication is successful, an access token and refresh token will be issued and user session will be maintained. User session will be used to access for all document operations. Access token will be used to access user management and contract management operations. The access token's life span is 15 minutes and can be refreshed using refresh token whenever any access of BE API after access token expired. UI will be logged out in case of 15 minutes inactivity.

7.2.3. HTTPS protocol

HTTPS works over underlying secure protocols (TLS 1.3/1.2) 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.

7.3. Secure communication between the CC server and databases

CC will establish network connection to database using TLS and AES 128 encrypted network traffic.

7.4. Security vulnerability testing

In order to keep the CC application 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.

8. Device (MFP/Mobile) Authentication

To protect sensitive information transmitted between CC and devices, security is enforced through HTTP over TLS. The used version of TLS is 1.3/1.2.
User must authenticate through CC authentication from the device application to establish the network connection between CC and the device.
The client authentication will be authenticate using user id and password, ID Card, or PIN code, and client-id and client-secret.

9. Google Cloud Platform Security Technical Details

CC is hosted on the Google Cloud Platform. GCP meets the broad set of internationally recognized information security controls and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1/2/3, GDPR, CCPA (see the detailed list of compliant standards in GCP Cloud Compliance, https://cloud.google.com/security/compliance).

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

- Various GCP 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

CC is deployed to the following GCP regions:

- Japan
- EU
- USA

CC uses managed storage and PostgreSQL Database hosted on GCP.
Hosting infrastructure compliance does not automatically apply to the hosted application (in this case, the CC application). This white paper clearly states the following facts:

- The CC application itself is not subject to independent third-party compliance testing apart from GCP compliance.
- We conduct technical vulnerability tests, such as vulnerability diagnosis and security scanning, but these are different in purpose and scope from third-party assessments of compliance.
- Compliance compliance of hosted applications is currently based on self-assessment.