Triumph-Adler
The Document Business
A KYOCERA GROUP COMPANY

IF IT WORX, IT'S
UTAX

TA/UTAX Cloud Capture:

Security White Paper

Document Version: 10/2024

October 01, 2024

About this document

This document is confidential. For internal use only.

This document describes TA/UTAX Cloud Capture (TA/UTAX CC)

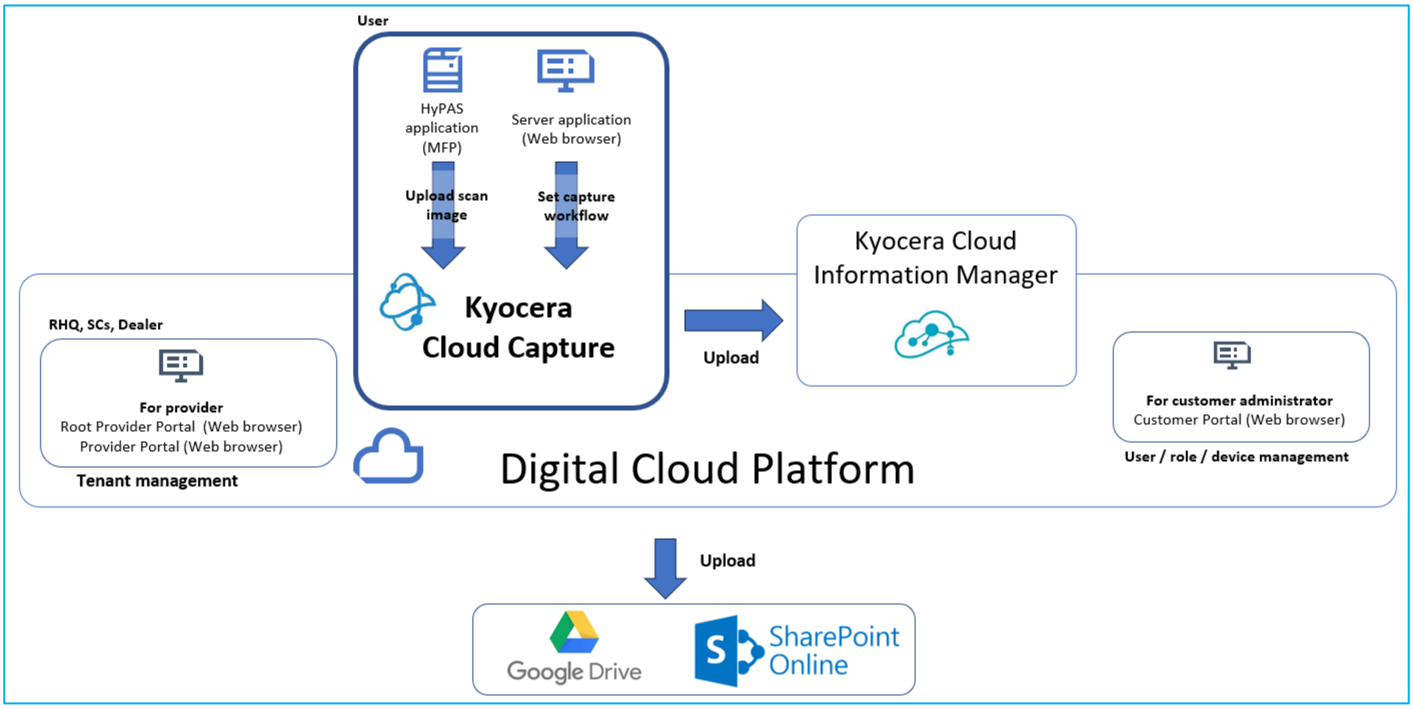
Target reader

This document is intended for staff members at the RHQ and sales companies of Kyocera Document Solutions group.

1. Overview

Cloud Capture (TA/UTAX 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 TA/UTAX CC. The priority is to provide secure protection of information assets that are handled by TA/UTAX CC. These information assets are rigorously protected by the secure configuration and security features of TA/UTAX CC.

TA/UTAX CC consists of the following components:


User
HyPAS application (MFP)
Server application (Web browser)
Upload scan image
Set capture workflow
Kyocera Cloud Capture
Upload
Kyocera Cloud Information Manager
RHQ, SCs, Dealer
For provider
Root Provider Portal (Web browser)
Provider Portal (Web browser)
Tenant management
Digital Cloud Platform
For customer administrator
Customer Portal (Web browser)
User / role / device management
Upload
Google Drive
SharePoint Online

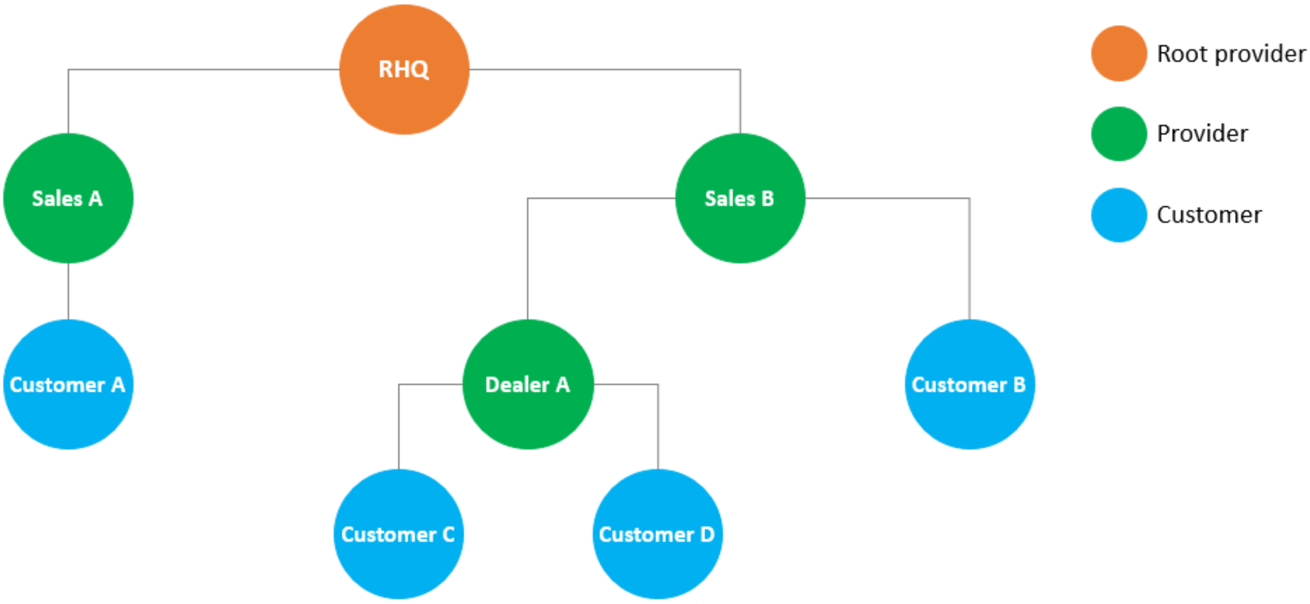
- **TA/UTAX CC:** TA/UTAX CC is a cloud capture system that provides customers with image processing, file format conversion, and indexing features.
- **Server application:** Customer administrators or customer user can access server application of TA/UTAX CC using a web browser. Customer administrators 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 TA/UTAX CC. The HyPAS application connects to TA/UTAX CC. Customers can scan and upload their documents to TA/UTAX CC using this application.
- **Digital Cloud Platform:** A platform built on the cloud that runs a cloud-based system that includes TA/UTAX 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 TA/UTAX CC to establish a link between third-party cloud storage and TA/UTAX 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

TA/UTAX 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

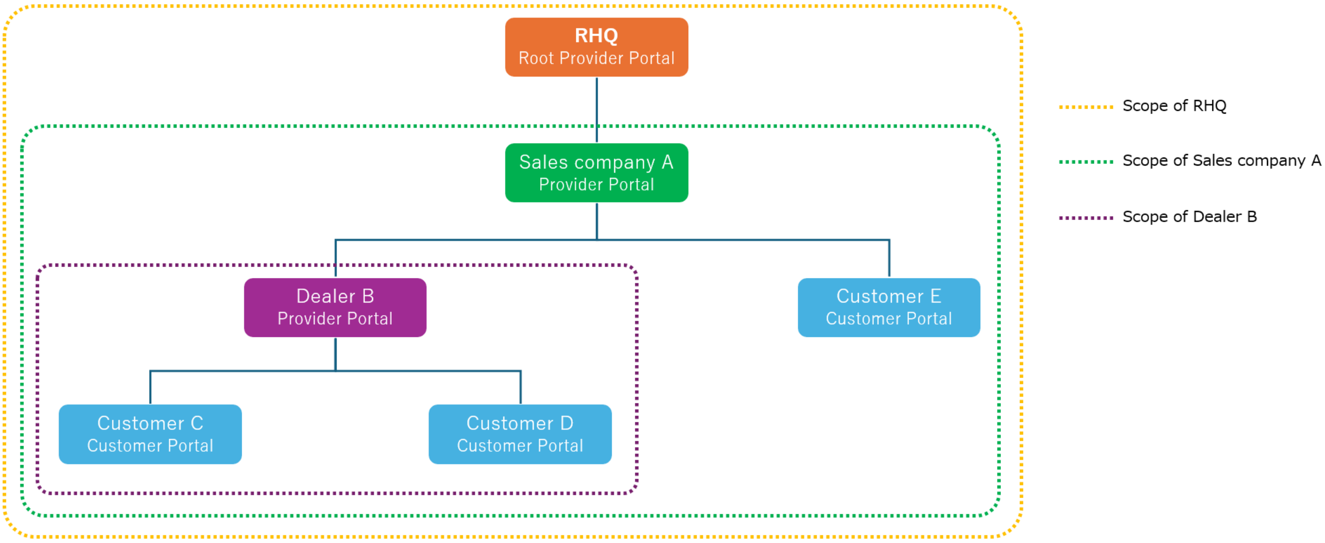
Any organization cannot view the data of another organization except for the parent organization.
The parent provider only can get usage counter information and the contact information of the organization representative from the customer. The usage count is the data related to the license information 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 TA/UTAX CC and all DCP services, TLS is used to secure and protect sensitive information that is shared between TA/UTAX CC and a browser, device, mobile or database. This information includes:

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

4. User Identification and Authentication

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

<table>
<tr><td>Password Length</td><td>Between 8 to 64 characters</td></tr>
<tr><td>Password Complexity</td><td>Include at least one character from each category:
Upper case (A ~ Z)
Lower case (a ~ z)
Numbers (0 ~ 9)
Symbols (!"#$%&'()*+,-./:;<=>?@[]^_`{|}~)</td></tr>
</table>

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]

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

Note: Users who have created a username including spaces or ! # ’ ~ ^ in version 1.0 may still login and continue TA/UTAX 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 TA/UTAX 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.

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

5. Keycloak security features

TA/UTAX CC/DCP uses Keycloak as an identity/authentication management service. Keycloak is an open source authentication management system that supports a variety of security features.

5.1. Keycloak features

Keycloak provides the following features:

- OAuth 2.0 support.
- Admin Console for central management of users, roles, role mappings, clients and configuration.
- Account Management console that allows users to centrally manage their account.
- Theme support - Customize all user facing pages to integrate with your applications and branding.
- Login flows - optional user self-registration, recover password, verify email, require password update, etc.
- Session management - Admins and users themselves can view and manage user sessions.
- Token mappers - Map user attributes, roles, etc. how you want into tokens and statements.
- CORS support - Client adapters have built-in support for CORS.
- Client adapters for JavaScript applications, WildFly, JBoss EAP, Fuse, Tomcat, Jetty, Spring, etc.

5.2. Threat model Mitigation

Keycloak mitigates the below possible security vulnerabilities as an authentication server. At this moment, TA/UTAX CC has brute force attacks protection is configured and plan to adopt more security features from Keycloak.

- IP restriction
- Port restriction
- Password guess: brute force attacks
- Read-only User Attributes
- Clickjacking
- SSL/HTTPS Requirement
- Cross-site request forgery (CSRF) Attacks
- Unspecific Redirect URIs
- FAPI compliance
- Compromised Access and Refresh Tokens
- Compromised Authorization Code
- Open redirectors
- Password database compromised
- Limiting Scope
- Limit Token Audience
- Limit Authentication Sessions

6. Data Protection

6.1. Protection of Stored Data

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

6.1.1. 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 TA/UTAX 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 TA/UTAX CC.

6.1.2. Authentication

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

6.1.3. Encryption

TA/UTAX CC database uses AES256 algorithm for encryption.

6.1.4. Data Backup

Daily backup for TA/UTAX CC database runs automatically. It is stored on Google Cloud Storage and encrypted by AES256. Google Cloud Storage are protected in two ways: geographic redundancy and incremental backups.
Geographic information is obtained by synchronously copying a stored storage object between data centers more than 100 miles away.
Geographic redundancy protect a stored storage objects from down of data center.

6.2. Protection of Communication Data

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

6.2.1. User Access

When a user accesses TA/UTAX CC from a web application using a browser, an authenticated communication channel is established. TA/UTAX CC user can access TA/UTAX CC web portal from the Web browser's client UI regardless of the user role. When a user accesses TA/UTAX 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 TA/UTAX CC web portal based on user's role. TA/UTAX CC web portal protects the communication data through HTTPS.

6.2.2. 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.

6.2.3. HTTPS protocol

HTTPS works over underlying secure protocols (TLS 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.

6.3. Secure communication between the TA/UTAX CC server and databases

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

6.4. Security vulnerability testing

In order to keep the TA/UTAX 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.

7. Device (MFP/Mobile) Authentication

To protect sensitive information transmitted between TA/UTAX CC and devices, security is enforced through HTTP over TLS. The used version of TLS is 1.2.
User must authenticate through TA/UTAX CC authentication from the device application to establish the network connection between TA/UTAX CC and the device.
The client authentication will be authenticate using user id, password, client-id and client-secret. Mobile and MFP have different client-id and client-secret.

8. Google Cloud Platform Security Technical Details

TA/UTAX 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

TA/UTAX CC is deployed to the following GCP regions:

- Japan
- EU
- USA

TA/UTAX CC uses managed storage and PostgreSQL Database hosted on GCP.