TA/UTAX Cloud Information Manager:

Security White Paper

Version 2.4

Document Version: 01/2024

January 16, 2024

About this document

This document is confidential. For internal use only.
This document describes TA/UTAX Cloud Information Manager (TA/UTAX CIM) version 2.4.

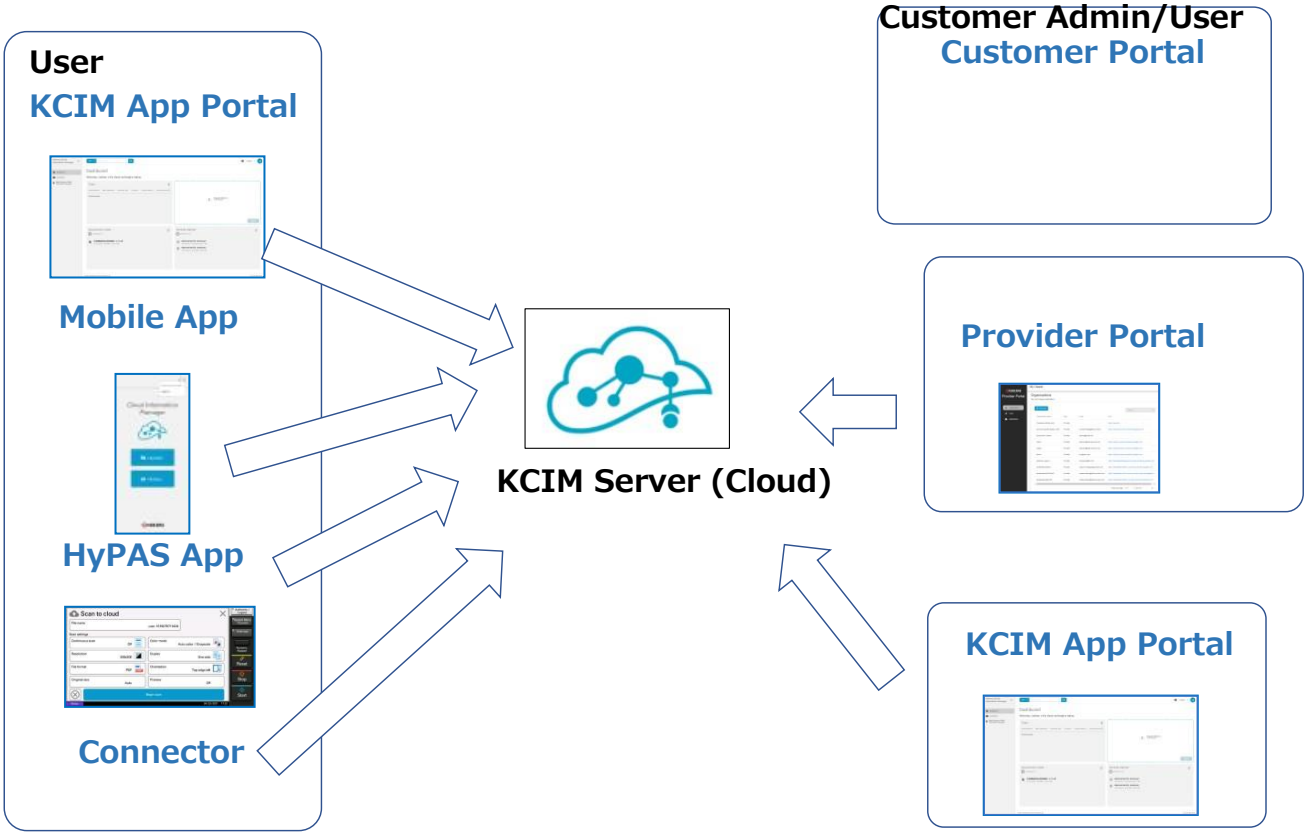
Target reader

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

1. Overview

TA/UTAX Cloud Information Manager (TA/UTAX CIM) is a cloud-based document management system that allows users easy to manage documents, scan, upload, index and store the documents.
This white paper informs dealers about security measures in TA/UTAX CIM. TA/UTAX's priority is to provide secure protection of information assets that are handled by TA/UTAX CIM. These information assets are rigorously protected by the secure configuration and security features of TA/UTAX CIM.

The system components are shown in the following architectural diagram:



The key components of the CIM system are described below:

CIM Server (Cloud): CIM Server is a cloud document management system that provides document management and user management features to customers.

Customer Portal: The customer portal is a one-stop portal where customer can manage common settings for CIM and other available solutions, as a common platform for supporting multiple applications. The customer admin or customer user can access this portal using a web browser. They can launch a landing page or application settings page within each application portal as well.

Provider portal: The provider portal is an application that supports CIM organization management, user management and document class management. The provider (RHQ, 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 direct customers.

CIM App portal: The customer admin or customer user can access the CIM App portal using a web browser. The customer admin can add user accounts for their own organization and configure access control of document classes. The customer user can upload, edit, delete and search documents.

HyPAS App (MFP client): The HyPAS application must be installed for Multi-Function Printer (MFP) to be able to use the CIM system. The HyPAS application connects to the CIM server. Customers can scan their documents in MFP and upload to the server.

Mobile application (iOS/Android): The mobile application connects to the TA/UTAX CIM server. The customer users can upload a photo and local file to TA/UTAX CIM server.

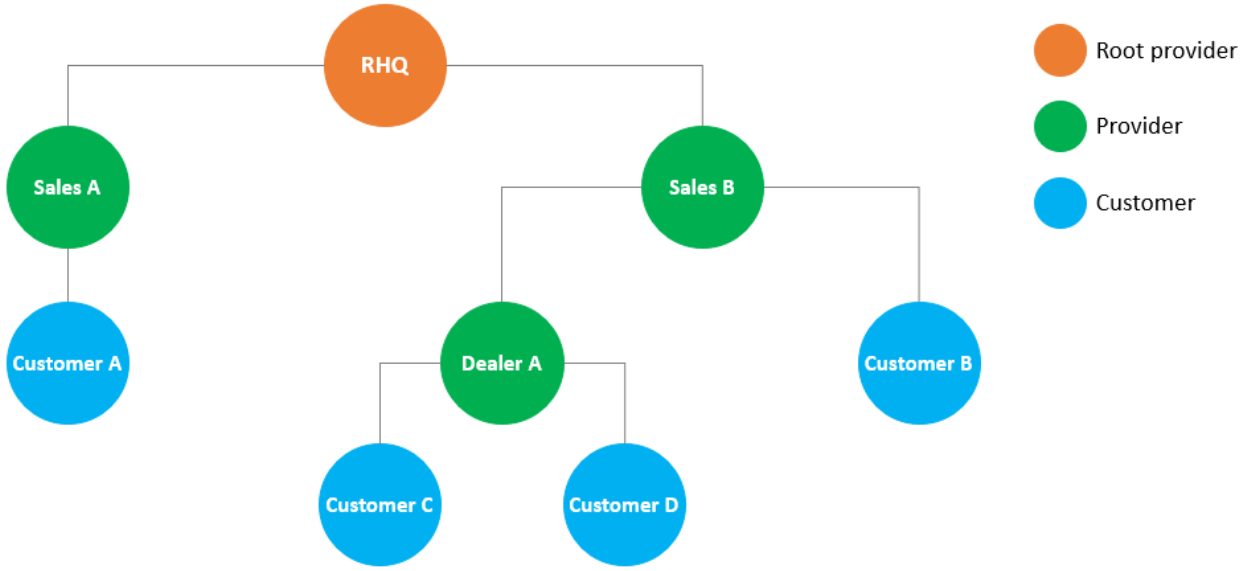
Connector: By developing a connector, CIM can integrate with other solutions, such as ScannerVision.

2. Multitenancy

TA/UTAX CIM 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 used in TA/UTAX. 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 TA/UTAX CIM Organizations

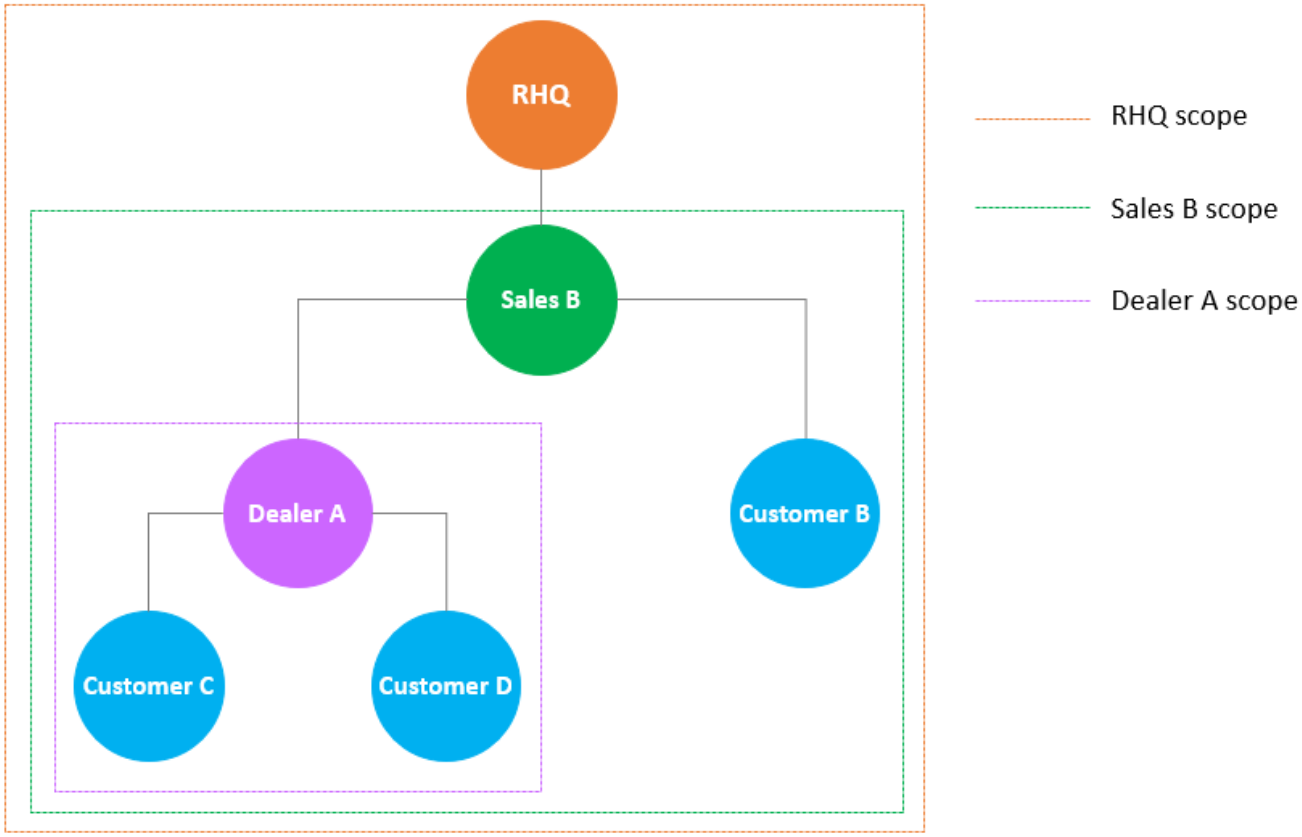
Any organization cannot view the data of another organization except for the parent organization.
The parent provider only can get usage counter information and the contact information of the organization representative from the customer. The usage count is the data related to the license information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

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

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

Scopes are present between parent and child organizations. At the organization level, parent/child organization can share the document class definition data (document classes and attributes of the document classes).

Also, the parent organization can manage the license-related information of the customer child organization (e.g. how many OCR pages, document size allowed) 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. TA/UTAX CIM's provider portal can generate OCR usage report of the entire organization hierarchy but the detail organization information will be anonymized.

3. Communication security between modules

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

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

4. User Identification and Authentication

When accessing TA/UTAX CIM, the user must log in with an activated account. An unauthorized user cannot access TA/UTAX CIM. The following features are supported as security features for login.
TA/UTAX CIM uses OAuth 2.0 authentication method by keycloak. Keycloak is a user authentication management software sponsored by RedHat.

4.1. Account Lockout Policy

The Account Lockout Policy protects TA/UTAX CIM 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 unlocked 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 CIM 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 (!"#$%&'()*+,-./:;<=>?@[]^_`{|}~)

5. Keycloak security features

TA/UTAX CIM uses keycloak as an identity/authentication management service. Keycloak is an open-source authentication management system yet, supports various 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.
- Not-before revocation policies per realm, application and user.
- 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 CIM 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 CIM's information assets must be protected and not leaked or lost. TA/UTAX implements security protection measures for stored information assets and a data recovery support through the features described below.

6.1.1. Access Control

Only individuals with proper access control will have access to all TA/UTAX CIM document information (document/content/metadata). Users will be required to have proper defined document access roles to access the specific document classes. Document access role is given per document class and controlled by the organization administrators in TA/UTAX CIM.

6.1.2. Authentication

TA/UTAX CIM database requires user authentication to gain access to database data. Authentication credentials are configured during initial release of the instance.

6.1.3. Encryption

TA/UTAX CIM database uses AES256 algorithm for encryption.

6.1.4. Data Backup

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

6.2.1. User Access

When a user accesses TA/UTAX CIM from a web application using a browser, an authenticated communication channel is established. TA/UTAX CIM user can access TA/UTAX CIM web portal from the Web browser's client UI regardless of the user role. When a user accesses TA/UTAX CIM 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 CIM web portal based on user's role. TA/UTAX CIM 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. SSL and 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 CIM server and databases

TA/UTAX CIM 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 CIM application up-to-date with the latest security measures the following schedule will be followed for security vulnerability assessment:

- Perform internal security vulnerability assessment at the time of software release
- A yearly assessment will be conducted by an external/3rd party vendor specializing in security vulnerability testing for web applications

7. Device (MFP/Mobile) Authentication

To protect sensitive information transmitted between TA/UTAX CIM and devices, security is enforced through HTTP over TLS. The used version of TLS is 1.2.
User must authenticate through TA/UTAX CIM authentication from the device application to establish the network connection between TA/UTAX CIM 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 CIM 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 CIM is deployed to the following GCP regions:

- Japan
- EU
- USA

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