IF IT WORX, IT'S UTAX

UTAX CLOUD PRINT AND SCAN SECURITY WHITEPAPER

utax.com

About UTAX Cloud Print and Scan

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

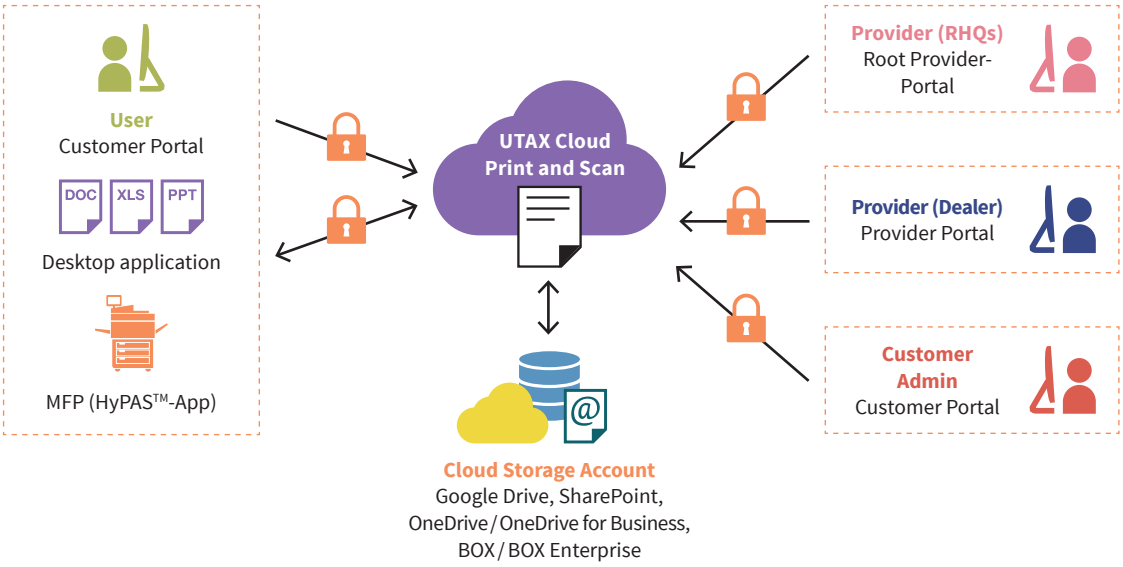
This white paper informs dealers and users about security measures in UCPS. UTAX's priority is to provide secure protection of information assets that are handled by UCPS. These information assets are rigorously protected by the secure configuration and security features of UCPS.

We hope you enjoy reading

Your UTAX team

CONTENT

1. The components of UTAX Cloud Print and Scan



(Fig. 1-1) UCPS 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 UCPS desktop application 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 application: The desktop application connects to the UCPS 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 UCPS 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 UCPS Server from any of their applications on the Chromebook that supports the print function. The Chrome extension is published on and available to be downloaded from the Chrome Web Store.

HyPAS™ application (MFP client): The HyPAS™ application connects to the UCPS server. Customers can release their print jobs that they uploaded using the UCPS desktop application. Customers can also scan their documents using this application.

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

bsi ISO/IEC 27001 Information Security Management CERTIFIED

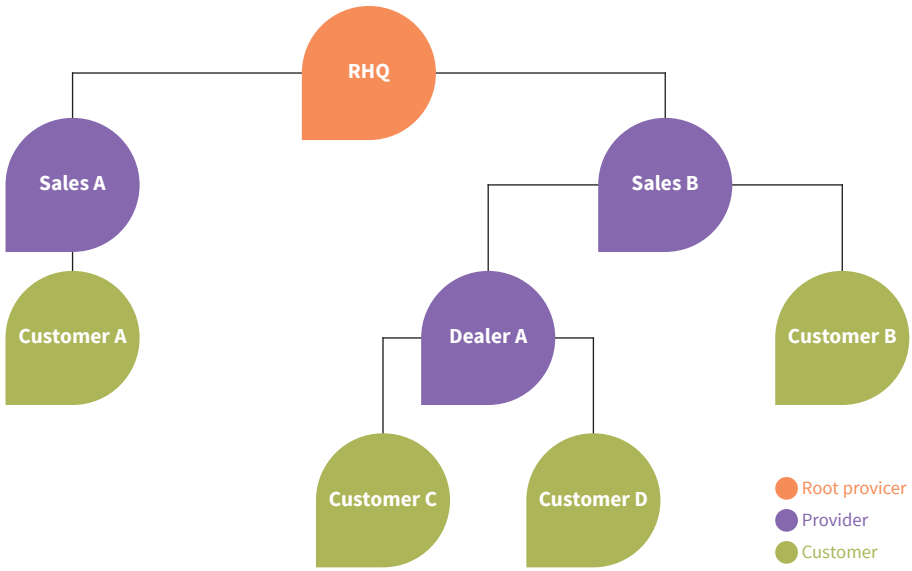
TACPS was developed by Kyocera Document Solutions (KDC) and Kyocera Document Solutions Development America (KDDA), which are certified to ISO 27001.

2. Multitenancy

UCPS uses multi-tenancy to accommodate multiple sales companies, dealers, and customer organizations. Each sales company, dealer, and customer is 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 at 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.



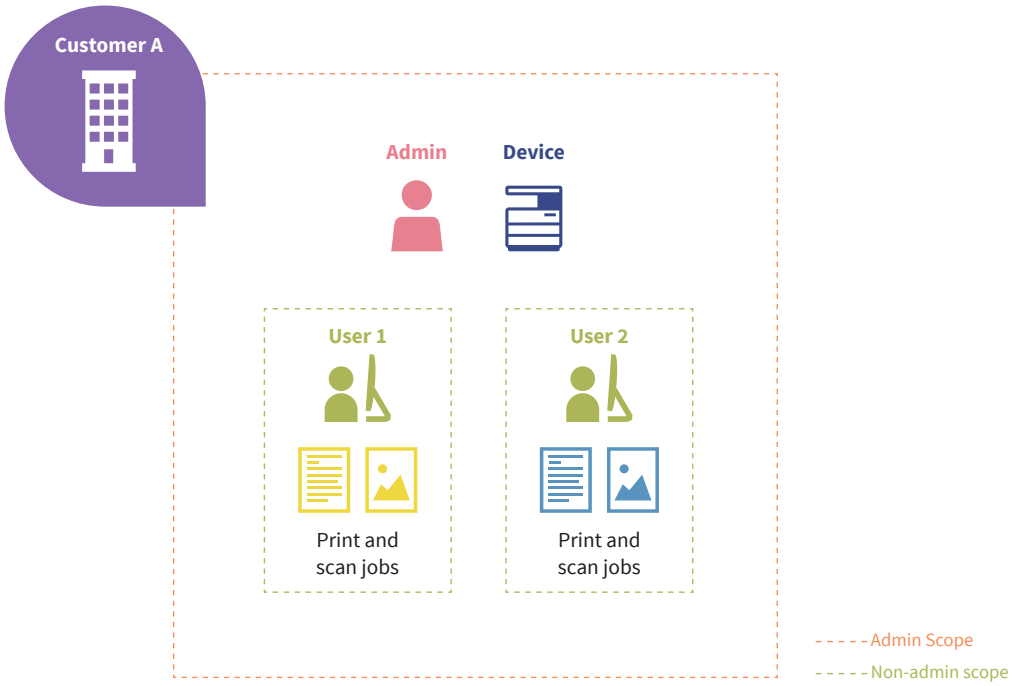
(Fig. 2-1) Hierarchical structure of UCPS Organizations

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 User report, User group report Device report	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	Accessible Can view own log data only	Accessible Can view own job data only
Guest 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

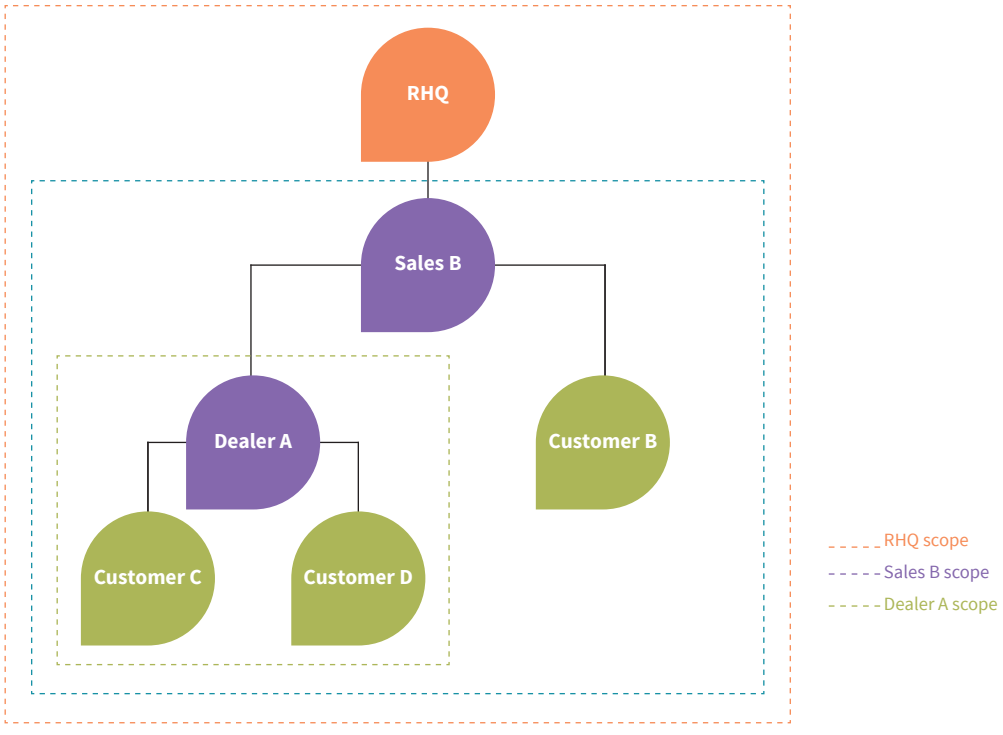
Additionally, User 1 and User 2 cannot see other users in organization Customer A from the customer portal, only Admin (who is an admin in Customer A) can see User 1 and User 2 (and himself, Admin) as users in the organization Customer A.

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).

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.



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

3. User Identification and Authentification

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

3.1. Account Lockout Policy

The Account Lockout Policy protects UCPS 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

3.2. Password Policy

A user needs to employ a strong password that is difficult to be analyzed and must be applicable to the UCPS 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 passwords in UCPS are hashed for storage and passwords transferred via a network can be encrypted when transmitted. The browser also masks all passwords.

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: • 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.)

3.3. 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 UCPS 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.

3.4. PIN Authentication

To simplify logging in to the UCPS HyPAS™ application, the solutions supports PIN authentication. In general, PIN authentication is useful for improving convenience, but it reduces the strength of security. Because each environment requires different levels of security, UCPS supports a PIN authentication feature that is adaptable to different environments.

- PIN code length can be selected from 4, 5, or 6 digits.
- Any PIN code can be specified
- Automatic generation of random PIN codes
- The PIN code is masked display like “****”.
- When the customer administrator displays the PIN code for a user, the configured PIN code is masked. However, the user's own PIN code is displayed unmasked.

3.5. ID Card Authentication

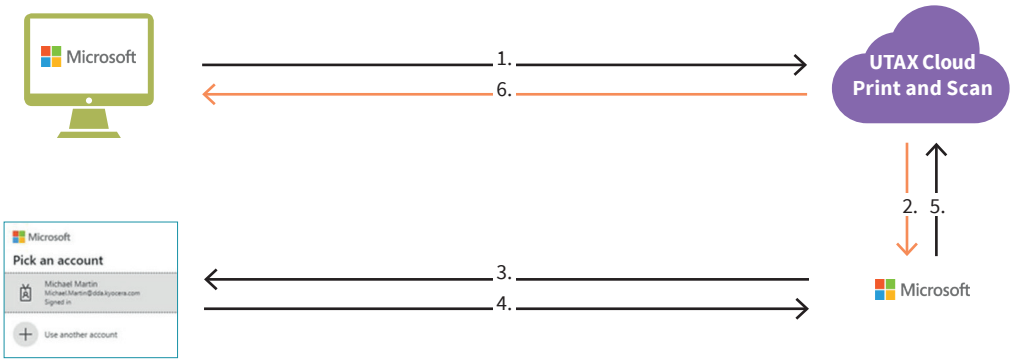
Support for ID card authentication has also been added as an alternative method for ease of logging onto the UCPS HyPAS™ application. Registration and management of ID cards is performed on the HyPAS™ application after a user authenticates in the HyPAS™ application. Management of ID cards (e.g. deletion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

3.6. 3rd Party Authentication and Identity

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

3.6.1. 3rd Party Credentials and OAuth2

UCPS provides the facility to connect 3rd party storage and authenticating using Azure AD credentials instead of separate UCPS credentials. UCPS follows the industry standard for OAuth2 authentication flows.



1. User clicks on “Sign in with Microsoft”.
2. UCPS calls Microsoft APIs to being the OAuth2 with Azure AD 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 UCPS.
6. Control is returned to UCPS and UCPS serves the appropriate page. (e.g. if authentication with Microsoft is successful, user is logged into UCPS)

This OAuth2 authentication flow is the same for other 3 rd 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 3 rd party service providers, a separate web page is loaded and authentication is performed on pages controlled by those 3 rd party service providers.

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

3.6.2. 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 UCPS web application and Desktop client using their Microsoft Entra ID credentials.

When a user successfully logs in to the UCPS web application or Desktop client using their Microsoft Entra ID credentials, a UCPS user is created pulling information from their Microsoft Entra ID identity (email, group info). This UCPS user is a separate UCPS identity on the UCPS web application.

Some things are important to note in this regard:

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

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 UCPS app on HyPAS.

3.6.3. 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.

4. Firewall Configuration

Required Ports:

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

*Print job data for cloud spooling is initiated by the MFP / HyPA™ so no special firewall inbound rules are necessary for port 443.
Please consult with your local IT to open these ports for UCPS communication.

UTAX places the highest priority on security.

5. Data Protection

5.1. Protection of Stored Data

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

5.1.1. Access Control

UCPS'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 individuals with proper access control will have access to UCPS's AWS environment resources and as well as application data. Operators will be required to have proper RBAC (role-based access control) authorization.

5.1.2. Authentication

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

5.1.3. Encryption

UCPS 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 UCPS server, this encryption is specifically used for authentication (generating the authentication hash when a user makes a login attempt).

As described in Chapter 7, UCPS is hosted on the Amazon 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 VMs 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 UCPS'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.

Data assets are tightly protected by UCPS security configuration and security features

5.1.4. Information ultilized by UCPS

UCPS Component	Information Assets (Used for the purpose of identification and communication within UCPS)
UCPS Server	• Organization information (URLs of each organization 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 UCPS user • Device information (serial number, network information such as host name and IP address) of each UCPS 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.
UCPS HyPAS™	• Authentication tokens generated by UCPS Server to authenticate the device or logged-in UCPS user to send info to and receive info from UCPS server. • Documents (PDF/JPG) to print or scanned from the device • Metrics (jobs and pages printed and scanned)
UCPS Desktop application	• Proxy settings of the network where the desktop is connected to; used to facilitate communication between the UCPS Desktop application and the UCPS Server • Authentication tokens generated by UCPS Server to authenticate the device or logged-in UCPS user to send info to and receive info from UCPS server. • Documents (PDF) printed from desktop applications using the UCPS Desktop application print queue. Local spooling stores the PDF print jobs locally on the desktop while Cloud spooling uploads the PDF print jobs to the UCPS Server. • Documents (PDF) locally stored on the desktop are at the following folder locations: - (Windows) C:\Users\<username>\AppData\Local\KCP - (Mac) /Users/Shared/Library/Cloud Print and Scan • Print job information (document name, number of pages, location for UCPS HyPAS™ to download the print job from).
UCPS Chrome extension	• Authentication tokens generated by CPS Server to authenticate the device or logged-in user to send info to and receive info from the server.

5.1.5. Data Backup

UCPS 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.

The deployment regions for TACPS and the database backup regions are as followed:

Geographical Region	AWS Region
Asia Pacific	ap-northeast-1(Tokio)
Asia Pacific (AU)	ap-southeast-2(Sydney)
Europe (EU)	eu-central-1(Frankfurt)
United States (US)	us-east-1(North Virginia)

5.2. Protection of Communication Data

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

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

5.2.1. User Access

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

5.2.2. 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 UCPS, TLS is used to secure and protect sensitive information that is shared between UCPS server and a browser, device, or database.

This information includes:

- UCPS user credentials and passwords
- Device authentication information
- User data
- Job metrics (print and scan jobs, pages printed, color settings used, etc.)

The UCPS environment can also be configured by the environment administrator to utilize a self-signed certificate. Steps would need to be followed in order to either create a self-sign certificate within the environment or upload a self-signed certificate to the environment.

Certificates through Cert-manager have a lifespan of 90 days and will automatically renew when it reaches expiration. Self-signed certificates will need to be managed by environment Administrator.

5.3. Secure communication between the UCPS server and databases

UCPS 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.

5.4. Direct Print / Scan from Box Storage

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

5.5. Security vulnerability testing

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

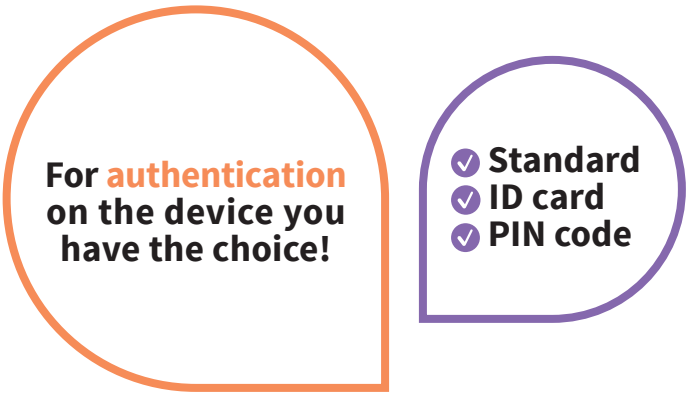
- Perform internal security vulnerability assessment at the time of software release
- Periodic vulnerability assessment in accordance with server management regulation.
- If the configuration of the public server has changed significantly, such as an upgrade, perform vulnerability assessment as necessary.

6. Device Authentication

To protect sensitive information transmitted between UCPS and UTAX 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:

- Simple login
- ID card login
- PIN login



7. Amazon AWS Security Technical Details

UCPS is hosted on the Amazon 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

UCPS is deployed to the following AWS regions:

- Tokyo (ap-northeast-1)
- Sydney (ap-southeast-2)
- 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.

UCPS uses MongoDB Atlas hosted on AWS for database storage. The hosted database cluster resides in the same region as the UCPS 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.

8. About UTAX

As a partner of high performing specialist retailers, UTAX paves the way for digital processes. Our expertise for office communication solutions and IT processes are up to date: with more than 60 years of experience, we offer everything that makes document management and project business easier.

As a registered trademark of TA Triumph-Adler GmbH, UTAX is distributed in Germany through a network of over 200 authorised dealers. Internationally, we operate in over 40 countries in the EMEA region.

Trust is the basis for a successful long-term partnership. We are always available and take care of our partners' needs as well as our own. Their success is also our success.

That way you can concentrate on your core business.

IF IT WORX, IT'S UTAX