TA CLOUD PRINT AND SCAN SECURITY WHITEPAPER

About TA Cloud Print and Scan

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

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

We hope you enjoy reading

Your TA Triumph-Adler team

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. TACPS desktop client does not support being used as a shared printer driver.

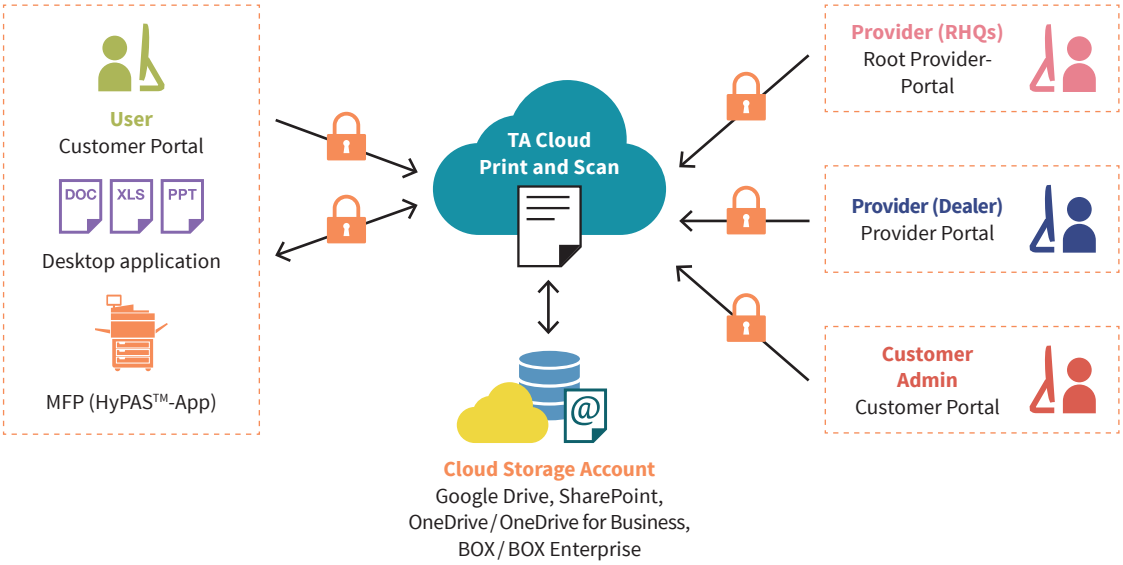
CONTENT

CONTENT

1. The components of TA Cloud Print and Scan

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

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



(Fig. 1-1) TACPS 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 TACPS 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 TACPS 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 TACPS 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 TACPS 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 TACPS server. Customers can release their print jobs that they uploaded using the TACPS desktop application. Customers can also scan their documents using this application.

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

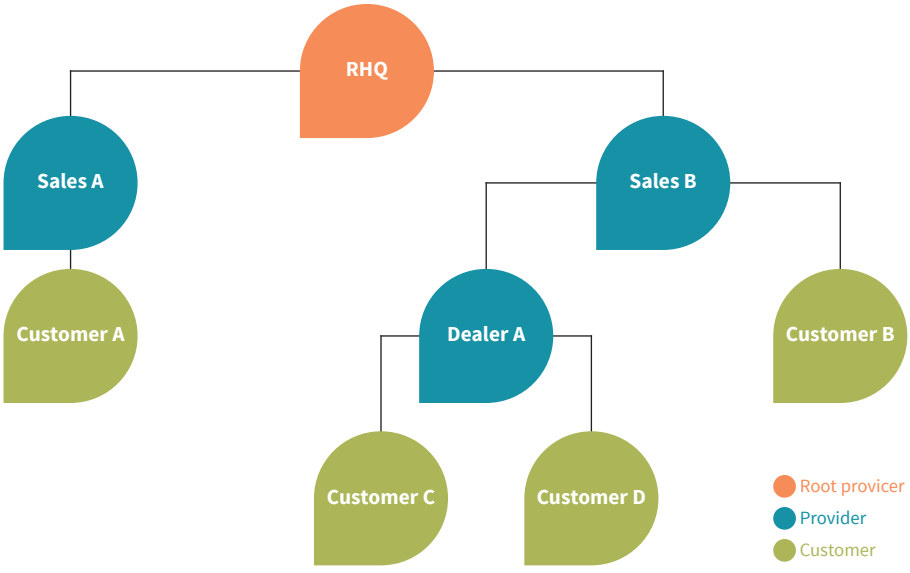
TACPS was developed by Kyocera Document Solutions (KDC) and Kyocera Document Solutions Development America (KDDA), which are certified to ISO 27001.

2. Multitenancy

TACPS 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 Triumph-Adler. 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 TACPS Organizations

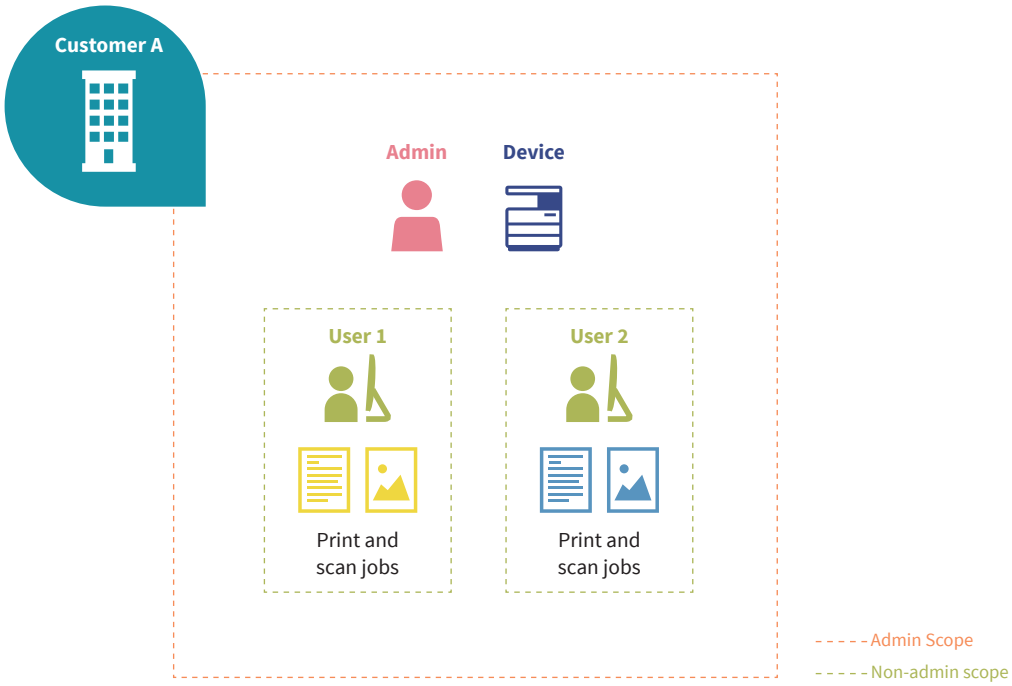
Any organization cannot view the data of another organization except for the parent organization. Data in customer organizations typically consists of user information, user's job data (e.g. print and scan jobs, job information), devices associated with the customer organization, and logs (jobs/pages 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

If access to the external admin API is granted to the customer administrator, the customer administrator will be able to access the list of users in the customer organization and the job log of the customer organization (including device information, executor ID, execution time, job type, and page count) through the API.

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

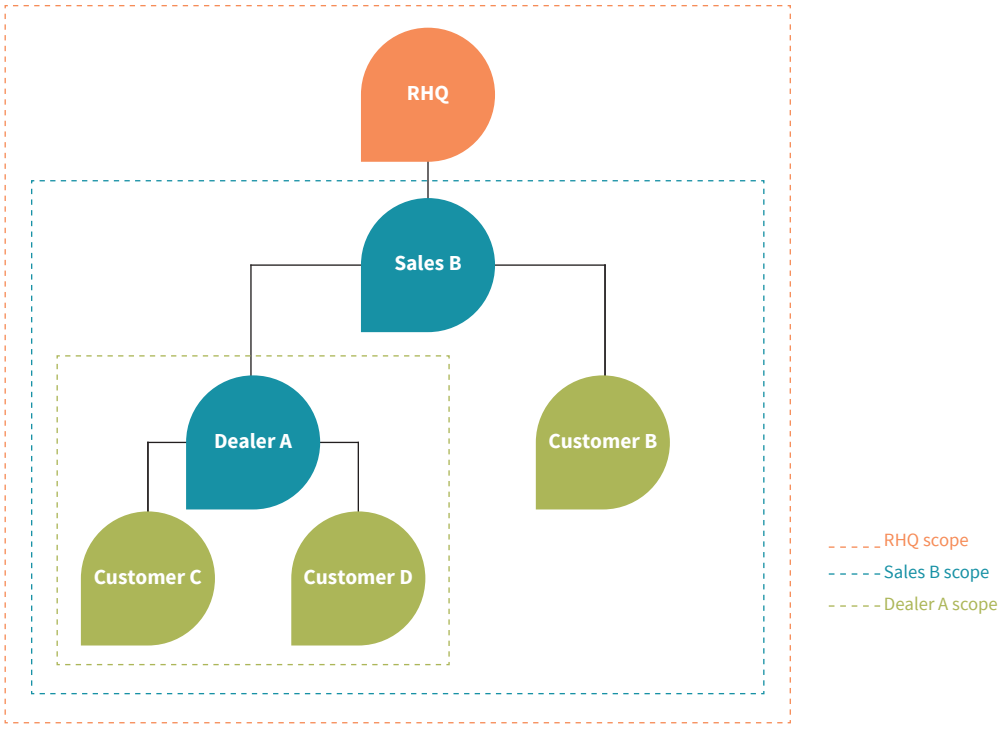
Additionally, User 1 and User 2 cannot see other users in organization Customer A from the customer portal, only Admin (who is an admin in Customer A) can see User 1 and User 2 (and himself, Admin) as users in the organization Customer A.

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. 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 CPS, TLS is used to secure and protect sensitive information that is shared between CPS and a browser, device, desktop client, mobile or database.

This information includes:

- CPS user credentials and passwords
- User data
- Job information (Print job, Scan job, etc)
- Document
- Document count metrics (Print page counts, Scan page counts, Quota, etc.)

This ensures that third parties on the network cannot decrypt or tamper with the payload during transmission.

3.1. Security Between HyPAS Applications and CPS Server

The table below lists the TLS versions available when a HyPAS application is installed on a model supported by CPS. Models that list multiple versions in the Supported TLS Version column use different TLS versions depending on the device's firmware version. If the latest version of the firmware is installed, the more secure version will be used.

3.1.1. A3 MFP

Product line	MFP	Support TLS version
Athena	9515ci 8515ci 7515ci 10565i 9565i 8565i 7565i	1.3
Iris	6006ci 5006ci 4006ci 3206ci 2506ci	1.2/1.0
Iris2	6007ci 5007ci 4007ci 3207ci 2507ci 6057i 5057i	1.3/1.2
Iris2020	7008ci 6008ci 5008ci 4008ci 3508ci 2508ci 7058i 6058i 5058i	1.3
IRIS2024	7009ci 6009ci 5009ci 4009ci 3509ci 2509ci 7059i 6059i 5059i	1.3
HANABI2	P-C3080i MFP P-C2480i MFP	1.2
MATSURI2	P-3240i MFP P-2540i MFP	1.2
MATSURI3	P-3241i MFP	1.3
Mercury4	8507ci 7507ci	1.2
Tomcat3	4062i 3262i	1.2
Tomcat4	4063i 3263i	1.3
Zeus4	9057i 8057i 7057i	1.2

3.1.2. A4 MFP

Project name	TA/UTAX brand	Support TLS version
Libra	P-4026iw MFP	1.2/1.0
Libra2	P-4027iw MFP	1.3
Mebius E-Model HyPAS MFP	P-C3062i MFP P-C3066i MFP P-C3562i MFP P-C3566i MFP	1.2
TASKalfa Mebius-E Plus	357ci	1.2
Perseus2	352ci 402ci 502ci	1.3/1.2
	302ci	1.2
Polaris E-Model	P-6036i MFP P-5536i MFP P-4531i MFP P-4536i MFP	1.2
Polaris E-Model 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
Virgo	P-C3563i MFP P-C3567i MFP P-C4063i MFP P-C4067i MFP 358ci 458ci	1.3

3.1.3. A4 Printer

Project name	TA/UTAX brand	Support TLS version
Virgo	P458ci	1.3

4. User Identification and Authentification

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

4.1. Account Lockout Policy

The Account Lockout Policy protects TACPS 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 setting will unlock the account after 30 minutes. This setting also applies in the event of a one-time passcode (OTP) authentication failure during multi-factor authentication (MFA).

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 TACPS 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: • 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. 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 vulnerabilities.

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

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 vulnerabilities. The validator checks if the value is a valid person name as an additional barrier for attacks such as script injection.

Username Length	Between 1 to 255 characters
Prohibited characters	Symbols \ / : , ; * ? " < > | [ ] { } $ % ` & ( ) + =

4.5. 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 TACPS 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.

4.6. PIN Authentication

To simplify logging in to the TACPS 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, TACPS supports a PIN authentication feature that is adaptable to different environments.

Selectable PIN code length	4-12 digits
Custom PIN code setting	Supported
Administrator setting arbitrary PIN codes for each user	Supported
Masked display of configured PIN codes (****)	• When a customer administrator views a user's PIN code, it is displayed in masked format. • User's own PIN code is displayed without masking.

4.7. ID Card Authentication

Support for ID card authentication has also been added as an alternative method for ease of logging onto the TACPS 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 TACPS web application. Registration of ID cards can also be performed on the HyPAS™ application after a user authenticates in the HyPAS™ application.

4.8. Multi Factor Authentication

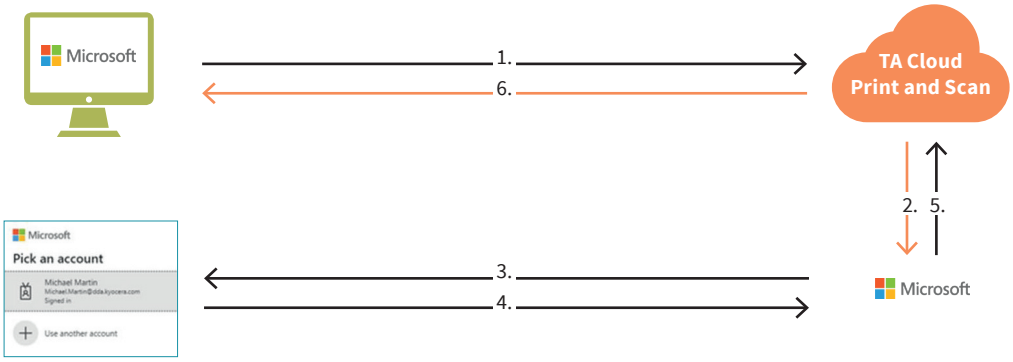
TACPS supports email-based multi-factor authentication (MFA). It sends a one-time passcode to the user's registered email address and requires its input. This significantly reduces the risk of unauthorized access even if the password is compromised. This OAuth2 authentication flow is the same for other 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. TACPS will never have access to or a copy of the user credentials entered for 3rd party services.

4.9. 3rd Party Authentication and Identity

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

4.9.1. 3rd Party Credentials and OAuth2

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



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

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.

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

4.9.2. 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 TACPS web application and Desktop client using their Microsoft Entra ID credentials.

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

Some things are important to note in this regard:

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

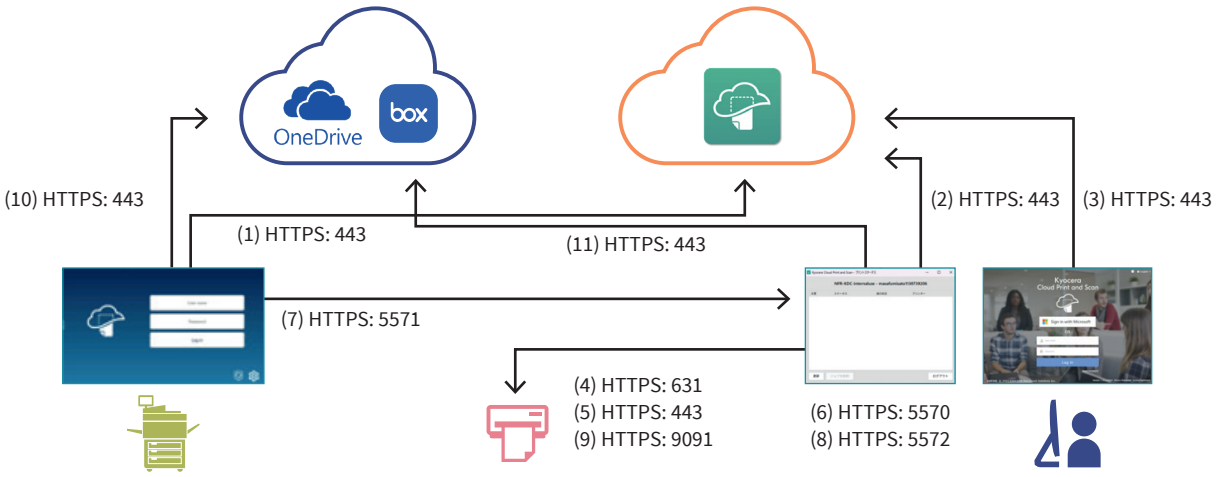
When Microsoft Entra ID is configured for the organization, a user will not be able to login to HyPAS using their Microsoft Entra ID credentials. ID card and PIN login are still available for the user to authenticate into the TACPS app on HyPAS.

4.9.3. 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. Ports and Communication Requirements

The ports used by TACPS are as follows. The label numbers in the diagram (e.g., (1), (2), …) correspond to the connection information listed in the table below.



Required Ports:

Source	Destination	Protocol	Port	Service
MFP / HyPAS™	TACPS Server	TCP	443	HTTPS: Login and send job log and scan data to TACPS *
TACPS Desktop Client	TACPS Server	TCP	443	HTTPS: Login and send job list to TACPS
Web Browser	TACPS Server	TCP	443	HTTPS: Access to the UI
TACPS Desktop Client	Printer/MFP	TCP	631	HTTP: IPP Printing (for non-HyPAS™ models)
TACPS Desktop Client	Printer/MFP	TCP	443	HTTPS: Secure IPP Printing (for non-HyPAS™ models)
TACPS Desktop Client	TACPS Desktop Client	TCP	5570	HTTP: Used for internal / local communication only
MFP / HyPAS™	TACPS-Desktop-Client	TCP	5571	HTTP: Get job list and job data
TACPS Desktop Client	TACPS-Desktop-Client	TCP	5572	HTTP: Used for internal / local communication only (for non-HyPAS™ models)
TACPS Desktop Client	Printer/MFP	TCP	9091	HTTPS: Get printer information (for non-HyPAS™ models)
TACPS HyPAS™ application	3rd parties cloud storage	TCP	443	HTTPS: Get print job data, Send scan data, and Fax forwarding
TACPS Desktop Client	3rd parties cloud storage	TCP	443	HTTPS: Send print job data (Only supports sending to OneDrive)

*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 TACPS communication.

6. Data Protection Technical Details

This chapter is intended for those with technical knowledge.

6.1. Protection of Stored Data

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

6.1.1. Access Control

TACPS'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 TACPS'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

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

6.1.3. Encryption

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

As described in Chapter 7, TACPS 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 TACPS'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 TACPS security configuration and security features

6.1.4. Information ultilized by TACPS

TACPS Component	Information Assets (Used for the purpose of identification and communication within TACPS)
TACPS 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 TACPS user • Device information (serial number, network information such as host name and IP address) of each TACPS 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.
TACPS HyPAS™	• Authentication tokens generated by TACPS Server to authenticate the device or logged-in TACPS user to send info to and receive info from TACPS server. • Documents (PDF/JPG) to print or scanned from the device • Metrics (jobs and pages printed and scanned)
TACPS Desktop application	• Proxy settings of the network where the desktop is connected to; used to facilitate communication between the TACPS Desktop application and the TACPS Server • Authentication tokens generated by TACPS Server to authenticate the device or logged-in TACPS user to send info to and receive info from TACPS server. • Documents (PDF) printed from desktop applications using the TACPS 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 TACPS 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 TACPS HyPAS™ to download the print job from).
TACPS 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.

6.1.5. Data Backup

TACPS 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)

6.2. Protection of Communication Data

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

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

6.2.1. User Access

When a user accesses TACPS from an application (web application using a browser, desktop application, or HyPAS™ application), an authenticated communication channel is established. TACPS user can access TACPS web portal from the Web browser's client UI regardless of the user role. When a user accesses TACPS web portal, the user is always identified and authenticated. If this identification and authentication are successful, the user can access TACPS web portal based on his/her role. TACPS web 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 TACPS, TLS is used to secure and protect sensitive information that is shared between TACPS server and a browser, device, or database.

This information includes:

- TACPS 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 TACPS server and databases

TACPS 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 Printing and Scanning from Box and OneDrive Storage

TACPS provides features that enhance the privacy and security of user data. Currently, the supported storage services are limited to Box and OneDrive; however, when a user links these storage services to TACPS, all printing and scanning (including fax forwarding) uploads are handled through direct interaction with the respective storage services. At no point is TACPS's temporary storage used in the process.

6.5. Security vulnerability testing

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

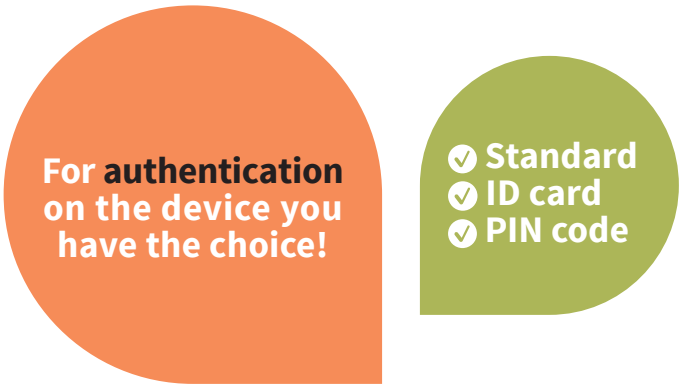
- Perform internal security vulnerability assessment at the time of software release
- Periodic vulnerability assessment in accordance with server management regulation.
- If the configuration of the public server has changed significantly, such as an upgrade, perform vulnerability assessment as necessary.

7. Device Authentication

To protect sensitive information transmitted between TACPS and Triumph-Adler 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



8. Amazon AWS Security Technical Details

TACPS 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

TACPS 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.

TACPS uses MongoDB Atlas hosted on AWS for database storage. The hosted database cluster resides in the same region as the TACPS 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. We are TA Triumph-Adler

Together we shape the world of work: TA Triumph-Adler supports small and medium-sized businesses in making collaboration easier, more effective and more secure.

We combine consulting, technology and service to create complete solutions for efficient document processes – from the initial consultation to rollout and ongoing support for the solution. TA Triumph-Adler offers everything from a single source and accompanies its customers throughout the entire process.

The history of TA Triumph-Adler began in the 19th century – not in the office, but with the production of bicycles. The company continued to develop steadily, moving into typewriters, calculators and office systems. Today, TA Triumph-Adler stands for intelligent document solutions that combine analogue and digital processes.

This allows employees to concentrate on what matters most, while TA Triumph-Adler works behind the scenes to ensure smooth, sustainable information flows.

Stay up to date and …

Unsere Themen bei LinkedIn

@ TA Triumph-Adler DACH

take a look at our world.

Folgen Sie uns auf Instagram

@ tatriumphadler

triumph-adler.com

02/2026