TA CLOUD PRINT AND SCAN SECURITY WHITEPAPER

HALLO

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

CONTENT

1. The components of TA Cloud Print and Scan 4

2. Multitenancy 6

3. User Identification and Authentification 10

3.1. Account Lockout Policy 10
3.2. Password Policy 10
3.3. Automatic logout 11
3.4. PIN Authentication 11
3.5. ID Card Authentication 12
3.6. Azure Active Directory 12
3.7. 3rd Party Credentials and OAuth2 13

4. Firewall Configuration 14

5. Data Protection Technical Details 15

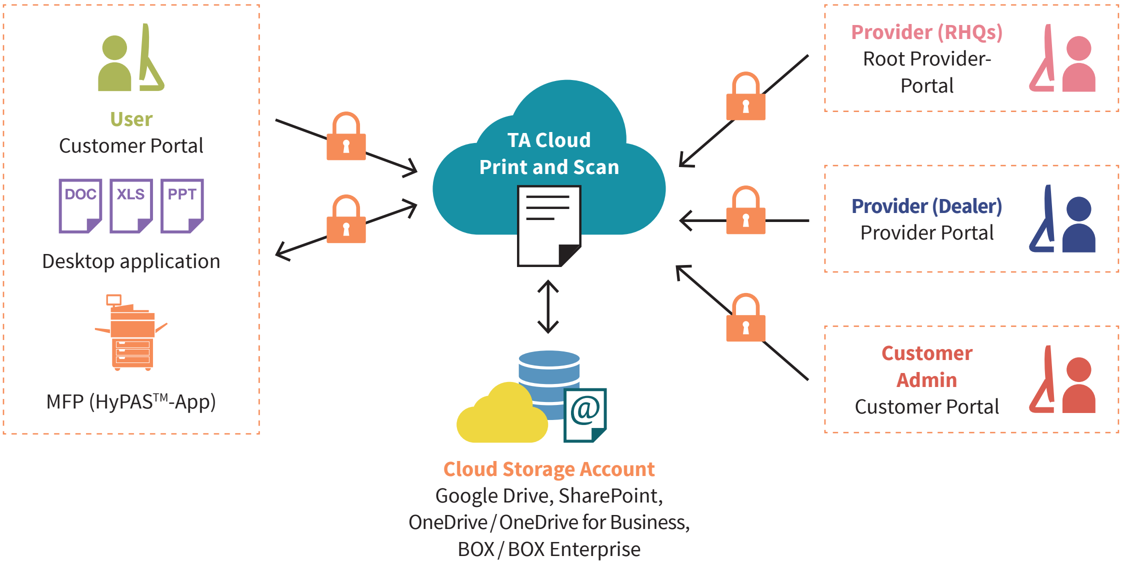
5.1. Protection of Stored Data 15
5.1.1. Access Control 15
5.1.2. Authentication 15
5.1.3. Encryption 15
5.1.4. Information ultilized by TACPS 17
5.1.5. Data Backup 17
5.2. Protection of Communication Data 18
5.2.1. User Access 18
5.2.2. HTTPS protocol 18
5.3. Secure communication between the TACPS server and databases 19
5.4. Security vulnerability testing 19

6. Device Authentication 20

7. Amazon AWS Security Technical Details 21

8. About TA Triumph-Adler 22

1. The components of TA Cloud Print and Scan



(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.

bsi
ISO/IEC
27001
Information Security
Management
CERTIFIED

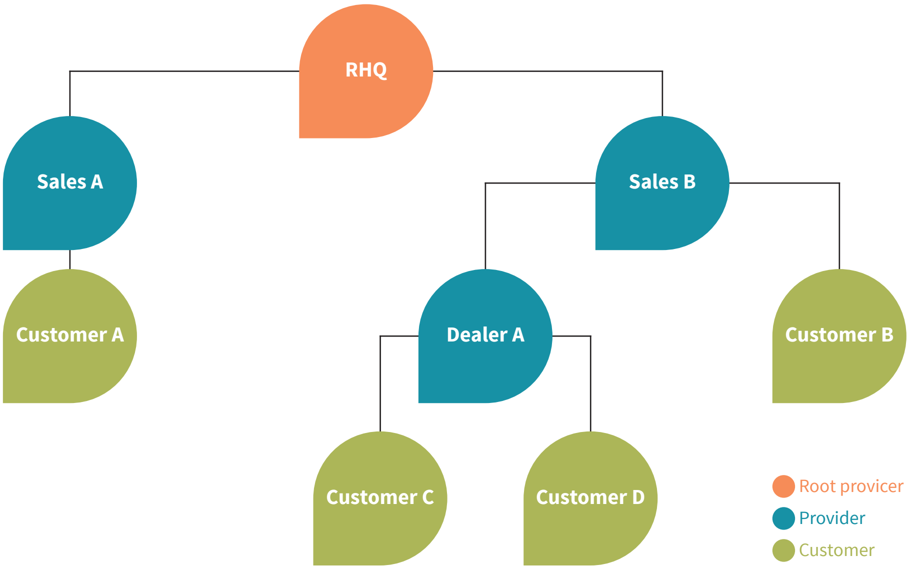
TACPS was developed at KYOCERA Document Solutions Development America (KDDA) which is certified to ISO 27001

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.



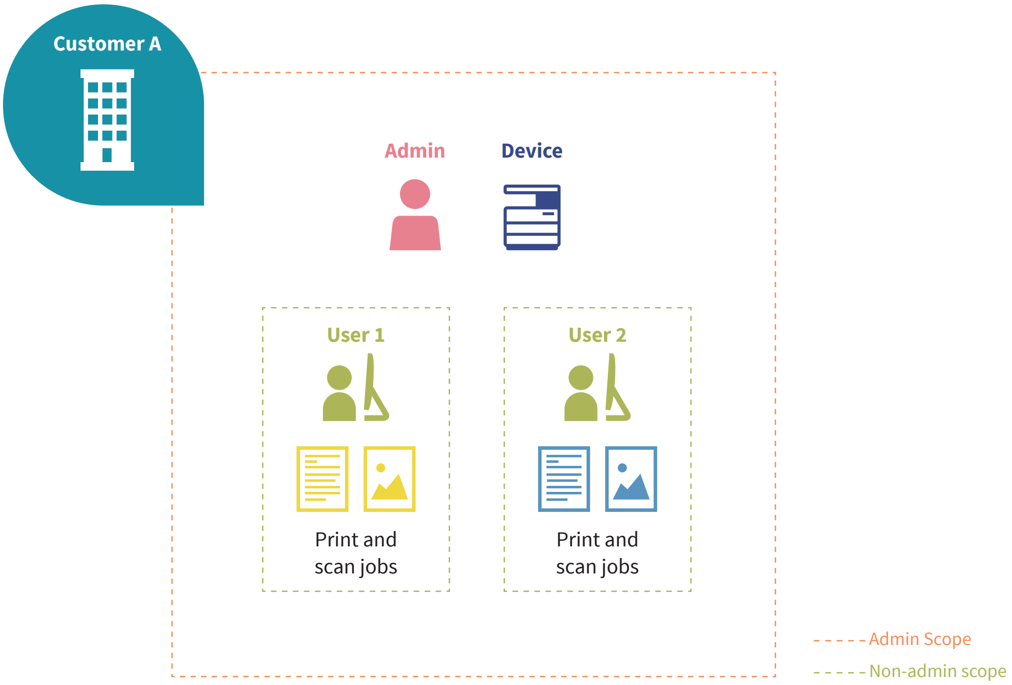
(Fig. 2-1) Hierarchical structure of TACPS Organizations

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	Log data (jobs/pages printed/ scanned)	Customer job data (print and scan documents)
Provider admin	Inaccessible	Accessible License info only	Inaccessible	Inaccessible
Provider support	Inaccessible	Accessible License info only	Inaccessible	Inaccessible
Customer admin	Accessible	Accessible	Accessible User report, User group report Device report	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
Users not in TACPS system User who is set to destination for reports by the administrator	Inaccessible	Inaccessible	Accessible Provider contracts report Customer contracts report Contract history report	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

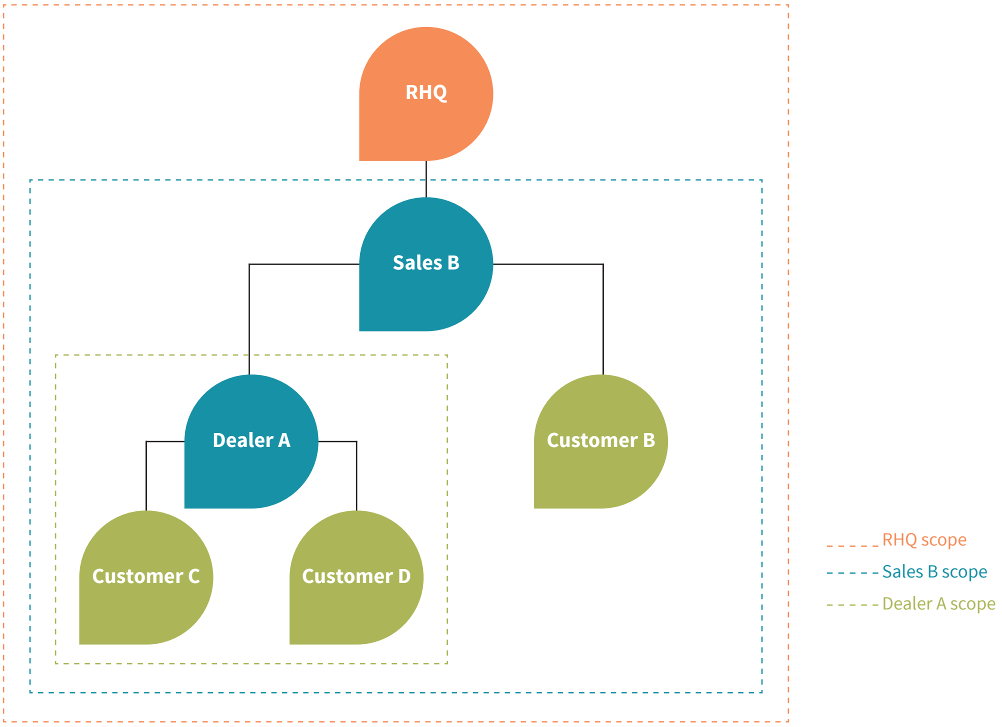
Additionally, User 1 and User 2 cannot see other users in organization Customer A from the customer portal, only Admin (who is an admin in Customer A) can see User 1 and User 2 (and himself, Admin) as users in the organization Customer A.

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 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.

3.1. 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.

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 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.)

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 TACPS server; MFP/HyPAS^{TM}, 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

In order to cater to the ease of use of the TACPS HyPAS^{TM} application, PIN authentication was implemented for easier login on the MFP. The PIN is a unique and randomly generated 6 digit number.

In order to support security for the PIN authentication, the following features have been implemented:

- PINs are only generated by the TACPS system; i.e. user cannot specify their own PIN. The TACPS system makes sure that the randomly generated PINs are not duplicated among users
- New PINs can only be regenerated once every seven days; this prevents attempts for possible exhaustion of unique PINs

3.5. ID Card Authentication

Support for ID card authentication has also been added as an alternative method for ease of logging onto the TACPS HyPAS^{TM} application. Registration and management of ID cards is performed on the HyPAS^{TM} application after a user authenticates in the HyPAS^{TM} 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^{TM} application after a user authenticates in the HyPAS^{TM} application.

3.6. Azure Active Directory

Azure Active Directory (Azure AD) is supported by the web application. Once the administrator configures a customer organization to use a specific Azure AD instance, users that exist on that Azure AD instance can login to the TACPS web application and Desktop client using their Azure AD credentials.

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

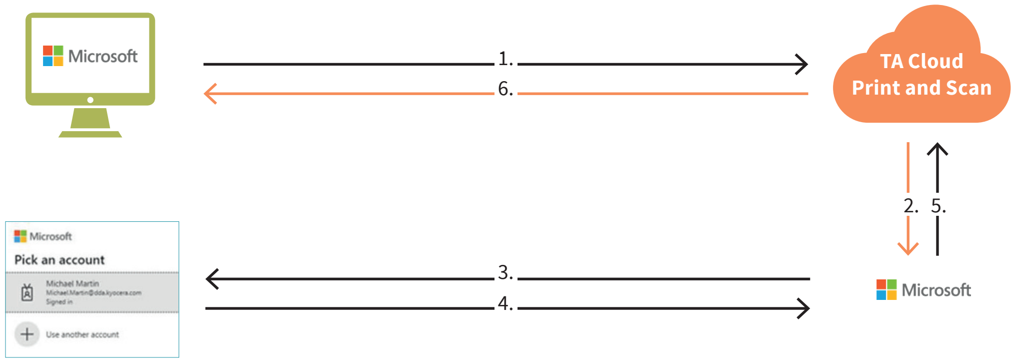
Some things are important to note in this regard:

- TACPS does not keep Azure AD credentials; TACPS follows the OAuth2 authentication workflow and always routes to Azure AD to verify credentials
- TACPS does not manage the Azure AD user TACPS verwaltet nicht den Azure-AD-Benutzer.
  - If the equivalent TACPS user is deleted on TACPS, the Azure AD user is not deleted and still exists on Azure AD
  - If the Azure AD user is deleted, the TACPS user will still exist on TACPS but will not be able to authenticate into TACPS with Azure AD credentials because the Azure AD user no longer exits

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

3.7. 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. Firewall Configuration

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	443	HTTP: IPP Printing (for non-HyPAS™ models)
TACPS Desktop Client	Printer/MFP	TCP	631	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)

TA Triumph-Adler places the highest priority on security.

5. Data Protection Technical Details

This chapter is intended for those with technical knowledge.

5.1. 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.

5.1.1. 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.

5.1.2. Authentication

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

5.1.3. 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

5.1.4. 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.

5.1.5. 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.

5.2. 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.

5.2.1. User Access

When a user accesses TACPS from an application (web application using a browser, desktop application, or HyPAS^{TM} 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.

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 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.)

5.3. 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.

5.4. 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
- A yearly assessment will be conducted by an external/3rd party vendor specializing in security vulnerability testing for web applications

6. 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

For **authentication** on the device you have the choice!

✓ Standard
✓ ID card
✓ PIN code

7. 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)
- 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.

8. About TA Triumph-Adler

TA Triumph-Adler is your guide to entering the world of the digital office. We can provide you with everything you need for the workplace of the future in a one-stop solution. We develop and deliver end-to-end managed document services that cover the entire document handling process in a networked and mobile office.

Having a dependable partner at your side allows you to tackle your transition to digital processes more courageously and successfully. TA Triumph-Adler is that partner.

Triumph and Adler have been familiar and illustrious names in offices since the 19th century. Formerly known mainly for typewriters, we are now prominent in the printers and copiers market. These days, we prefer to talk about MFPs, or multifunction printers, because our devices have long since been digitally upgraded with a wide range of optional extras.

Handling documents has been our core business for over 120 years, and we are now bringing this expertise into the digital era. We act as your go-to partner when it comes to archiving, managing and editing documents in digital form. Our services range from an entry-level archiving solution to a customised ECM system. If you want something more, just get in touch with us and we will deliver it!

That way you can concentrate on your core business.