ScanTrip Cloud Security White Paper

June 2023 Version 1.0

Table Of Contents

1. Introduction

Dispatcher ScanTrip Cloud is a cloud-based application that combines powerful document processing automation with the availability and accessibility of cloud architecture. Using Dispatcher ScanTrip Cloud, customers can manage their workflows, users, devices, and more from a single location that is accessible from anywhere.

Since customer information and business data are highly sensitive website transactions that take place, the security of this information and the site becomes of paramount importance. We are committed to protecting our customers by:

- Protecting user data
- Protecting proprietary information transmitted through the site
- Ensuring site integrity
- Preventing site imposters

Dispatcher ScanTrip Cloud implements rigorous security protocols in order to inspire trust and confidence in our customers. These policies complement the controls also provided by our hosting service, Amazon Web Services (AWS). An industry leader in cloud computing, AWS continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.

This White Paper outlines the security features provided by the Dispatcher ScanTrip Cloud.

1. Data Collection

Dispatcher ScanTrip Cloud collects the following information about your system:

- The values of your device security settings.
- Basic licensing information, such as your Dispatcher ScanTrip Cloud business plan, the license count, billing frequency, any descriptive name that you specified for your plan, etc.
- The unique identifier associated with your MarketPlace account.

In addition, Dispatcher ScanTrip Cloud collects the following **personally identifiable information (PII)**

PPI	Used For
MarketPlace email address*	Logging into the Dispatcher ScanTrip Cloud portal
First/last name*	Displaying on the User’s page of the Dispatcher ScanTrip Cloud portal
Phone Number*	2-Factor Authentication, if needed

*** See the Secure Account Creation section on page 8 for more information.**

2. Data Storage Security

For maximum security, Dispatcher ScanTrip Cloud stores collected data in an encrypted Amazon DynamoDB table, a fully-managed, durable database with built-in security features and backup and restore functions. This data is accessible to the Dispatcher ScanTrip Cloud Web and Device services, as well as a select number of specialized Konica Minolta system developers for support purposes only.

To provide an additional layer of data protection and ensure that data is secured from unauthorized access, this data is encrypted at rest by AES-256 using encryption keys stored in AWS. Data in transit is protected using Transport Layer Security (TLS) 1.3. MFP data is protected by TLS 1.2.

To provide the highest level of data durability, availability, and security in the AWS cloud, device admin passwords are stored in encrypted storage in an AWS S3 encrypted bucket and are not accessible to anyone except the user.

All Dispatcher ScanTrip Cloud identity data is stored in multi-region, load-balanced data centers located in the US (Virginia), Germany (Frankfurt), and Japan (Tokyo) to best manage network latency and address regulatory compliance. Content is backed up within each data center.

3. Communication

MFPs will be connected to the nearest AWS Content Delivery Network (CDN) entry point automatically. The following URLs and their subdomains must be accessible from the MFP (over HTTPS / Port 443):

https://scantripcloud.com

https://dispatcherScanTrip Cloud.com

https://konicaminoltamarketplace.com

4. Tenant Isolation

Strong tenant isolation security and control features are part of the Dispatcher ScanTrip Cloud system via AWS Identity and Access Management (IAM), which provides granular access restrictions to storage instances. With IAM, we are able to securely control who is authenticated (signed in) and authorized to use resources.

5. Data Retention

Dispatcher ScanTrip Cloud abides by a strict customer data retention policy to address specific concerns from our customers. Any backups of customer data taken to facilitate disaster recovery are automatically deleted after a 30 day period.

Data may be retained as long as the user is an active Dispatcher ScanTrip Cloud customer. Once a customer discontinues the service, data will be kept for 90 days before being automatically deleted. Customers may request all data associated with their use of the service to be deleted permanently at any time by contacting Konica Minolta.

6. Access Control

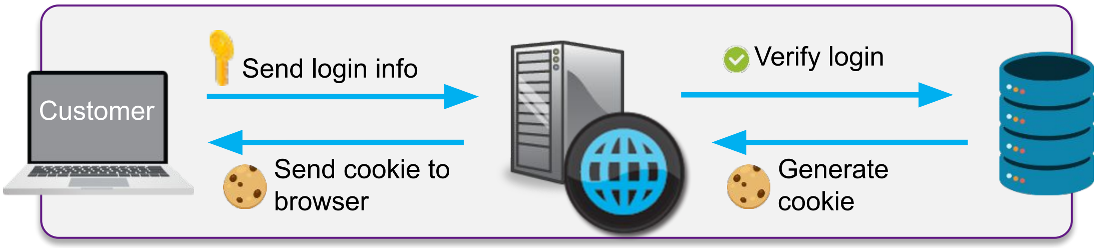
Access to production servers is limited to a select group of Konica Minolta personnel for the express purpose of customer support. If any Dispatcher ScanTrip Cloud customer data is used by Konica Minolta for any other purposes than customer support (e.g., to improve the service, etc.), it is used in an anonymized form.

1. Overview

Cookies are used to store information on web browsers and provide a seamless experience for users of the Dispatcher ScanTrip Cloud online portal. The use of cookies makes it possible for users to access the features and pages they are looking for within the site.

2. Purpose

Dispatcher ScanTrip Cloud cookies are primarily used for authentication purposes (verifying user accounts and determining when users are logged in). For example, cookies are used to keep users logged in as they navigate between Dispatcher ScanTrip Cloud pages so that the user does not have to keep logging into the Dispatcher ScanTrip Cloud portal.



Important Note: Users can access the Dispatcher ScanTrip Cloud portal using their MarketPlace credentials. As is the case with MarketPlace cookies, Dispatcher ScanTrip Cloud cookies are never used to store highly sensitive or critical information (e.g., user passwords, etc.)

3. Cookies Used

Cookie	Name	Purpose	Duration
Session	BMPSID	Identifies that the user is logged into MarketPlace	1 month
	Session	Identifies that the user is logged into ScanTrip Cloud	1 week
	Tenant Selector	Identifies the tenants the user has logged into	Capped by browser

Flag	Purpose
HTTPOnly	Protects session cookies from being stolen. This flag tells the web browser that the cookie can only be accessed through HTTP.
Secure	Protects cookie theft via man-in-the-middle attacks. This flag tells the web browser that the cookie can only be transmitted using a secure connection (SSL/HTTPS).

4. User Consent

As part of the European Union’s e-privacy directive that requires websites to receive user consent for the use of tracking technologies, a cookie notification appears at the bottom of the page of the Dispatcher ScanTrip Cloud Portal. This provides a way for users to give their consent over cookies usage.

5. Cookie Tracking

Dispatcher ScanTrip Cloud does not offer its content to any third parties.

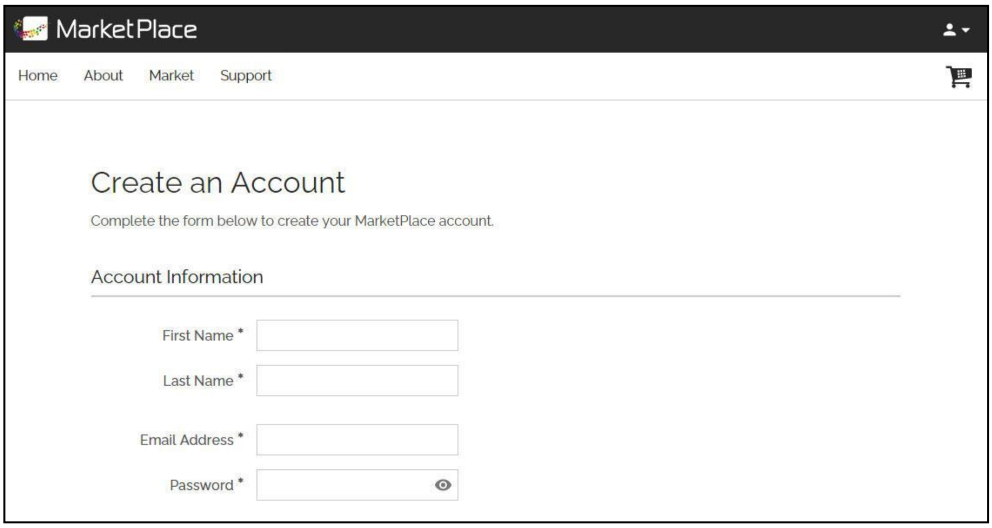
1. Overview

At least one user must create accounts on the Konica Minolta MarketPlace to obtain licenses for the Dispatcher ScanTrip Cloud agent and gain initial access the Dispatcher ScanTrip Cloud online portal (other methods of authentication can be configured later). To deliver these services, the MarketPlace collects limited user information when users create an account, such as email address, hash of the password, first and last name, and phone number. All handling of personal information follows Konica Minolta’s Privacy Policy.

2. Secure Account Creation

To ensure that the website login process and registration forms are secure, MarketPlace (and, by extension, Dispatcher ScanTrip Cloud) implements the following security best practices:

- **Secure login** - Logins happen over HTTPS to reduce the risk of the user's credentials being captured via a MiTM (Man in the Middle) attack.
- **Email Confirmation** - The user’s email address must be verified as part of the sign-up process.
- **Secure password reset** - To reduce automated attacks, CAPTCHA is used when requesting a password reset to ensure that requesters are real human beings.
- **Disposable email address prevention** – MarketPlace accounts cannot be created with disposable email addresses.



Create an Account

Complete the form below to create your MarketPlace account.

Account Information

First Name *

Last Name *

Email Address *

Password *

1. Overview

Dispatcher ScanTrip Cloud provides a variety of powerful user management features to ensure that admins have the granular control they need to manage who has access to specific components within the overall system. Dispatcher ScanTrip Cloud license owners/admins are able to invite other admins to join their Dispatcher ScanTrip Cloud plan via the online portal; as part of the invitation process, one or more access roles can be assigned. These roles can be easily modified at any time via the portal's Users page.

2. Access Roles

The following access roles are available to be assigned/modified:

- **Tenant Manager** - User can set up and view high-level reports for multiple tenants.
- **Tenant Admin** - User can add/edit/remove users, devices, workflows and view granular reports for a single tenant.
- **Tenant User** - User can view and use workflows.

VI. Operational Security

1. Overview

Operational security is a critical component to the overall security of Dispatcher ScanTrip Cloud. Possible threats are continuously identified, security holes and vulnerabilities are analyzed, with countermeasure policies put into place. With Dispatcher ScanTrip Cloud, we are committed to proactively preventing potential issues that may occur and have implemented a variety of operational best practices via AWS.

2. Monitoring

Dispatcher ScanTrip Cloud is continuously monitored and assessed to maintain the security, reliability, availability, and performance of the system.

3. Vulnerability Scans

The following types of vulnerability scanning are performed:

- **Web Application Security (WAS) Scans** – Scans are performed on Dispatcher ScanTrip Cloud at periodic intervals for each major release to detect any vulnerabilities, performing simulated attacks and analyzing the result. This ensures that:
  - There are no exploitable vulnerabilities if an unauthorized user attempts to access Dispatcher ScanTrip Cloud.
  - An authorized user cannot breach Dispatcher ScanTrip Cloud's security controls.

- **Source Code Diagnosis** – Source code diagnosis is performed after every code commit to discover vulnerabilities.

- **Dynamic Application Security Testing (DAST) Scans** - Scans are periodically performed on Dispatcher ScanTrip Cloud simulating an "outside-in" attack and analyzing the result. This ensures that:
  - There are no exploitable vulnerabilities if an unauthorized user attempts to access Dispatcher ScanTrip Cloud
  - Potential vulnerabilities are identified quickly

- **Static Application Security Testing (SAST) Scans*** - Scans are performed on the Dispatcher ScanTrip Cloud source code to identify potential vulnerabilities. This ensures that vulnerabilities can be identified and fixed before any code changes are made public, further securing Dispatcher ScanTrip Cloud.

*Will be implemented for public launch

1. Overview

As part of our commitment to provide a service that is both highly available and secure, we understand that informational security is mission-critical for our customers. That is why we have also put into place several stringent administrative security practices to ensure that data is always protected.

2. Multi-Factor Authentication

Multi-factor authentication is set up as part of our AWS service, requiring two forms of authentication to access the AWS developer console, project infrastructure, storage, etc.

3. Tracking

Requests for access to Dispatcher ScanTrip Cloud storage buckets are tracked via access logging, a critical feature for security and access audits.

4. Control

We also follow strict security measures regarding our development, staging, and production environments to prevent data breaches. Only Konica Minolta personnel with an approved development/administrative role may access the different environments:

- **Development** – This environment is used to conduct code development and develop new features without touching actual customer data. This environment is accessible to only a select number of Konica Minolta developers who are working on the project.
- **Staging** – This is our final testing ground before code is pushed into production, used to perform quality assurance evaluation, vulnerability testing and risk analysis, and integration testing. This environment is further restricted to a smaller group of Konica Minolta developers.
- **Production** – This is the “live” Dispatcher ScanTrip Cloud system, available to all end users. Access to this environment is extremely limited, available only to a few specific Konica Minolta development administrators.

1. Overview

The Dispatcher ScanTrip Cloud is protected from DDoS (Distributed Denial of Service) attacks via its hosting service, Amazon Web Services (AWS). AWS provides DDoS attack mitigation technology called AWS Shield for all of its customers to protect from common attacks, including SYN/ACK floods, Reflection attacks, and HTTP slow reads.

2. Quick Detection

AWS Shield provides always-on network flow monitoring, which inspects incoming traffic to AWS and uses a combination of traffic signatures, anomaly algorithms and other analysis techniques to detect malicious traffic in real-time.

3. Inline Attach Mitigation

Automated mitigation techniques are built into AWS Shield, providing protection against common infrastructure (Layer 3 and 4) attacks. Automatic mitigations are applied inline so there is no latency impact, and always-on detection and inline mitigation minimizes downtime. AWS Shield uses several techniques, such as deterministic packet filtering and priority-based traffic shaping, to automatically mitigate attacks without impact to the Dispatcher ScanTrip Cloud.

4. Vulnerability Scans

Vulnerability scans are administered on a regular basis to actively scan for security threats.

1. Who has access to my data?

Dispatcher ScanTrip Cloud resources in AWS are controlled via strictly-defined access control lists (ACL). Except for customer support and software development reasons, any access by Konica Minolta personnel must have the customer's written permission.

3. Where is my data hosted?

Customer data is hosted within three different data centers in the United States (Virginia), Germany (Frankfurt), and Japan (Tokyo).

4. Can I have by data hosted in a single data center?

We store customer data in multiple data centers to provide resilience and high availability.

5. Is Dispatcher ScanTrip Cloud PCI compliant?

Dispatcher ScanTrip Cloud is not a transaction processor or merchant in accordance with PCI terms. All purchasing transactions are handled via the Konica Minolta MarketPlace, which is PCI compliant.

6. Does Dispatcher ScanTrip Cloud comply with data privacy laws like GDPR?

Konica Minolta respects the privacy of our customers and is committed to protecting our customers' personal data to meet the highest standard regarding compliance. Our Global Personal Data Protection policy sets forth the basic principles of our data protection and security standards to ensure compliance with national and international data protection laws in force all over the world.

7. What happens to my data once I stop being a customer?

Once you have terminated your Dispatcher ScanTrip Cloud service, data is retained for 90 days. After that time, the data is logically wiped from the system.

10. What security measures have been put into place for access to the Dispatcher ScanTrip Cloud Portal?

Users log into Dispatcher ScanTrip Cloud via Single Sign-On authentication with MarketPlace. In addition, users cannot access a tenant on the portal unless they are members of that tenancy. Additional users must be invited to the tenant via an email with an invitation link. Invitation links cannot be used more than once and are set to expire after 7 days.

KONICA MINOLTA