RICOH CloudStream Security White Paper

Version 1.1.12

History

Version	Date	Details of Changes
1.0.0	November 1, 2023	First Edition
1.0.1	December 15, 2023	"Data Protection" - Changed the following items of "Data Type" not supported in MVP to red strikeout. ・PIN code ・Card authentication information (card name, card number) Also, deleted the following item. ・Embedded settings (e.g. Microsoft 365 tenant and client IDs)
1.0.2	February 20, 2024	"Communication Security" -Add description of default mail server to "Communication Diagram", "Data Flow", and "Email". "Data Protection" -Add region of AWS to "Data Storage Location". -Add mail sending loa and suppression list to "Data Type".
1.1.0	March 8, 2024	Published as DM+PrintScan integrated version. "Data Protection" -Add "Encryption Key Management" section.
1.1.1	October 30, 2024	Incorporate security white paper updates from a partner company (For PrintScan) "Appendix" -Added port 443 to "Data Flow (PrintScan)" in addition to existing PrintScan custom ports (e.g. 8443) See "Devices Connected to CloudStream Using HTTPS Default Port 443" for using port 443. See "Devices Connected to CloudStream Using Legacy Ports" for using ports other than 443 such as 8443. "Appendix" -Added information for PrintScan to "Communication from the customer environment to CloudStream" "Trademarks" -Add "Open Telekom Cloud" and "PostgreSQL"
1.1.2	December 6, 2024	"System Overview" |- "System Configuration" Add the Device Monitoring Service to the system configuration. "Communication Security" |- "Mutual Authentication" Add the Device Monitoring Service Update the DM Data Flow diagram. "Operations Security" |- "Vulnerability Support" Add explanation of frequency guidelines for vulnerability assessment. |- "Backup" Add explanation of redundancy and accessibility for backup data. "Appendix" |- "Data Flow (DM)" Add the protocols and ports of the Device Monitoring Service Add explanation about port 80 which DM Agent Deployment Tool uses when installing DM Agent. Add explanation about communication to proxy servers. |- "Data Flow (PrintScan) Add explanation about port 443 which Mobile App uses. Overall Reflect ETC review feedback
1.1.3	December 17, 2024	"Appendix" |- "Data Flow (DM)" Add port 80, which the DM Agent Deployment Tool must use when installing the DM Agent

		|- "Data Flow (PrintScan) Reflect port change (8443 -> 443) during SSO from DM to PrintScan.
1.1.4	February 4, 2025	Add about support for MFA authentication "System Overview" |- "System Configuration" Update configuration diagram "CloudStream Security Measures" |- "Data Protection" |- "User Authentication" Add about proxy servers for DM Agent/Deployment Tool "CloudStream Security Measures" |- "Communication Security" | |- "Communication Path" "Appendix" |- "Data Flow (DM)" Add about segmentation of production, test, staging, production environment and how to deploy. "CloudStream Security Measures" |- "Development Security" |- "Development Process" Add about change management and code review. "CloudStream Security Measures" |- "Development Security" |- "Change Management" New Specify the data center for the data to be deleted. "CloudStream Security Measures" |- "Data Protection" |- "Data Deletion" Vulnerability testing perspective added. "CloudStream Security Measures" |- "Operations Security" |- "Vulnerability Support" Description of Azure Monitor added. "CloudStream Security Measures" |- "Operations Security" |- "System Monitoring" Note about Azure activity logs added. "CloudStream Security Measures" |- "Cloud Service Provider's Access Control to Data" |- "Access Authority Management" Corrected the description of UK DC. "CloudStream Security Measures" |- "Data Protection" |- "Data Storage Location" Supported SNMP versions added "Appendix" |- "Data Flow (DM)"
1.1.5	April 30, 2025	Overall Correction Items - Removed description of Open Telekom Cloud Ireland DC added "CloudStream Security Measures" |- "Data Protection" |- "Data Storage Location" "Appendix" |- "Communication from the customer environment to CloudStream" PrintScan Cloud IP addresses added "CloudStream Security Measures" |- "Communication Security"

		|-- ”Permission Settings for Communication from the Customer Environment to CloudStream” FTP description added ”Appendix” |- ”Data Flow (DM)”
1.1.6	July 31, 2025	Extraction of items to be included in the security white paper from the RFP responses ”CloudStream Security Measures” |- ”Data Protection” | |- "User Authentication” | |- "Data Deletion” |- "Cloud Service Provider’s Access” | |- "Firewall” (*) Go to "Network Separation” and deleted. |- "Operations Security” | |- ”Backup” | |- "System Monitoring” (*) Part of the description is moved to ”Audit log”. | |- "Audit Log‟ (*) New |- ”Communication Security” | |- "Network Separation‟ (*) Moved from ”Firewall” and renamed. |- "Development Security” |- "Development Process” Added description about Open Telekom Cloud. ”CloudStream Security Measures” |- ”Data Protection” |- "Data Storage Location”
1.1.7	December 2, 2025	Adapted from a vendor-provided security white paper on vulnerability handling in PrintScan. “CloudStream Security Measures” |- “Operations Security” |- “Vulnerability Support” Added @Remote Center. “System Overview” |- “System Configuration” “CloudStream Security Measures” |- “Communication Security” |- “Communication Path” “Appendix” |- “Data Flow (DM)” Added note on deletion of data processed by OCR. ”CloudStream Security Measures” |- ”Data Protection” |- "Data Deletion” Added PrintScan Germany region. “Appendix” |- “Communication from the customer environment to CloudStream” Deleted notes of PMC “Appendix” |- “Data Flow (PrintScan)”

1.1.8	January 13, 2026	Deleted @Remote Center. “System Overview” |- “System Configuration” “CloudStream Security Measures” |- “Communication Security” |- “Communication Path” “Appendix” |- “Data Flow (DM)”
1.1.9	February 13, 2026	Modified the timing of data deletion. ”CloudStream Security Measures” |- ”Data Protection” |- "Data Deletion”
1.1.10	May 11, 2026	Added @Remote Center. “System Overview” |- “System Configuration” “CloudStream Security Measures” |- “Communication Security” |- “Communication Path” “Appendix” |- “Data Flow (DM)” Revised the terminology for data deletion targets (licenses → tenants) ”CloudStream Security Measures” |- ”Data Protection” |- "Data Deletion”
1.1.11	July 7, 2026	Update regarding temporary administrator accounts “CloudStream Security Measures” |- “Cloud Service Provider’s Access Control to Data” |- “Access Authority Management”
1.1.12	October 22, 2026	Added Software Server. “System Overview” |- “System Configuration” “CloudStream Security Measures” |- “Communication Security” |- “Communication Path” “Appendix” |- “Data Flow (DM)”

Contents

Introduction 8
Purpose 8
Target Audience 8
System Overview 9
System Configuration 9
Shared Responsibility Model 12
CloudStream Security Measures 14
Data Protection 14
Data Storage Location 14
Data Type 14
Data Encryption 17
Encryption Key Management 17
User Authentication 18
External Authentication Linkage 19
Account Management by the Customers 19
Data Deletion 20
Cloud Service Provider's Access Control to Data 20
Access Authority Management 20
Multi-tenant 21
Physical and Environmental Security 22
Physical Server 22
Operations Security 23
Vulnerability Support 23
Protection from DDoS Attack 24
Backup 24
Troubleshooting 25
System Monitoring 25

Audit Log 26
Internal Audit 26
Communication Security 26
Network Separation 26
Communication Path 27
Communication Encryption 29
Mutual Authentication 30
Permission Settings for Communication from the Customer Environment to CloudStream 30
Development Security 32
Development Process 32
Change Management 32
Supplier Relationships 33
Governance of outsourcing company 33
Information Security Incident Management 34
Incident Information Publication Method 34
Customer Support 34
Availability 34
Redundancy 34
Compliance 35
Privacy Policy 35
Zero Trust 36
Cloud Infrastructure 36
Edge Device 36
Trademarks 37
Appendix 38
ISO Comparative Table 38
Data Flow (DM) 38
Data Flow (PrintScan) 43

Devices Connected to CloudStream Using HTTPS Default Port 443 43
Devices Connected to CloudStream Using Legacy Ports 49
Communication from the customer environment to CloudStream 51

Introduction

Purpose

This document provides an overview of the security features and practices implemented in the RICOH CloudStream (hereinafter referred to as "CloudStream") solution. Information contained in this document is intended to assist customers in understanding how the security of the solution is ensured and how customers may leverage the security features of the solution to maintain the confidentiality, integrity, and availability of their data.

Ricoh Group, as a cloud service provider, is responsible for most of the information security measures and implements various security measures from many aspects. Each security measure is explained, based on the structure of ISO/IEC27017, the international standard for cloud security (Chapter 5 to Chapter 18). (Appendix/ISO Comparative Table)

Target Audience

The target audience for this document includes IT professionals, security professionals, and decision-makers responsible for selecting and implementing CloudStream solutions in their organizations. This document also provides insight into the security controls implemented to ensure compliance with relevant regulations and standards.

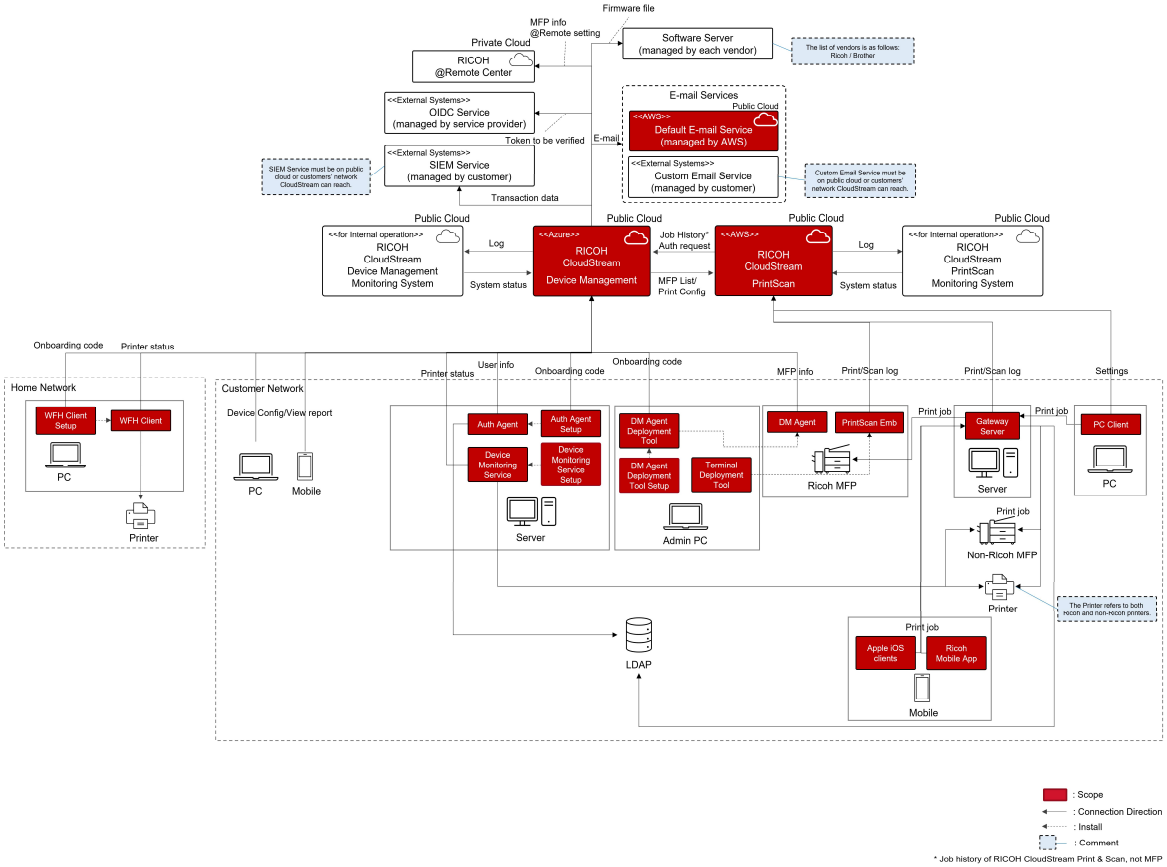
All information in this document is based on the current state of technology and best practices. The content of this document is subject to change as new threats may emerge and new security controls are implemented.

This document does not replace or supersede any contractual agreements or terms of service between RICOH and customers. It serves as a supplement to these documents to provide additional information and transparency into the security practices implemented in relation to RICOH CloudStream.

System Overview

System Configuration

The CloudStream system configuration is shown below.



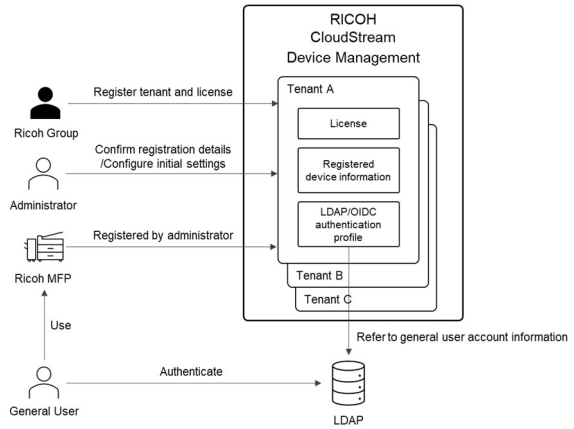
Elements	Description
RICOH CloudStream Device Management (hereinafter referred to as CloudStream DM)	Cloud service for device management
RICOH CloudStream PrintScan (hereinafter referred to as CloudStream PrintScan)	Cloud services for printing and scanning
RICOH CloudStream Device Management Monitoring System (hereinafter referred to as CloudStream DM Monitoring)	Cloud service for internal operations of the Ricoh Group that collects and monitors logs for CloudStream DM
RICOH CloudStream PrintScan Monitoring System (hereinafter referred to as CloudStream PrintScan Monitoring)	Cloud service for internal operations of the Ricoh Group and partner that collects and monitors logs for CloudStream PrintScan
Default E-mail Service (managed by AWS)	Default email server provided by CloudStream leveraging AWS fully managed service
Custom E-mail Service (managed by Customer)	Customer-owned any email server

SIEM Service (managed by customer)	Customer-owned SIEM services exclusively support Splunk Enterprise
DM Agent	MFP application to send device status and logs to the cloud, and receive and apply configuration settings to the device from the CloudStream cloud
DM Agent Deployment Tool	PC application for installing DM Agent on devices
DM Agent Deployment Tool Setup	Installer for the DM Agent Deployment Tool application
Auth Agent	Windows server application to acquire user information from an on-premises LDAP server and send it to the cloud
Auth Agent Setup	Installer for the Auth Agent application
WfH Client (Work from Home Client)	PC application to acquire printer information from printers used during telecommuting and send it to the cloud
WfH Client Setup	WfH Client installer
Device Monitoring Service	Windows server application to acquire device information from devices that do not support DM Agent and send it to the cloud
Device Monitoring Service Setup	Device Monitoring Service installer
PrintScan Emb	MFP application to receive print jobs from, and scan jobs to the cloud
Terminal Deployment Tool	PrintScan Emb Installer
PC Client	PC application to create and send print jobs to the Cloud or Gateway Server
Gateway Server	Linux server application to relay print jobs to devices and send print and scan data to the cloud
RICOH @Remote Center	RICOH's service to manage devices remotely
Software Server	Server that distributes firmware managed and provided by vendors

For details of DM and PrintScan, please refer to the table below.

DM	PrintScan
CloudStream DM (Figure 1) is a SaaS-type cloud service provided by Ricoh Group (*1), which provides the services to manage and configure customers' devices. By integrating with CloudStream PrintScan, it can also provide usage reports utilizing print and scan job histories. To use CloudStream DM, the customer's tenant must first have a CloudStream DM license, and a device registered. Tenants and licenses are provided to customers in advance by the Ricoh Group. The tenant's administrator confirms the tenant's registration details and performs the necessary initial settings such as device registration and authentication profile settings. The general users in the tenant authenticate	RICOH CloudStream PrintScan service (Figure 2) delivers cloud-based print, copy and scan services with optional edge components as per customer needs. Document storage and processing remains local to ensure that document integrity and privacy is maintained. Only the print job's selected metadata travels encrypted to the cloud for management and reporting purposes. CloudStream PrintScan (software) is embedded on multifunction devices (MFDs) and printers at the business location. There, it is either connected with Edge device, (hardware or virtual appliance) or directly to a

with the authentication server configured in the authentication profile and use the devices registered on CloudStream DM.



(*1) Please see the following website for Ricoh Group's company information.

https://www.ricoh.com/

The location of the head office is as follows.

3-6, Nakamagome 1-chome, Ohta-ku, Tokyo 143-8555 Japan

cloud instance. The edge device is responsible for processing jobs onsite. Though it does the work of a server, the Edge device, much like a network router, is self-contained and needs no customer maintenance. A Virtual Appliance operates in a comparable manner to the Edge hardware device but is run on a customer-supplied server or virtual machine.

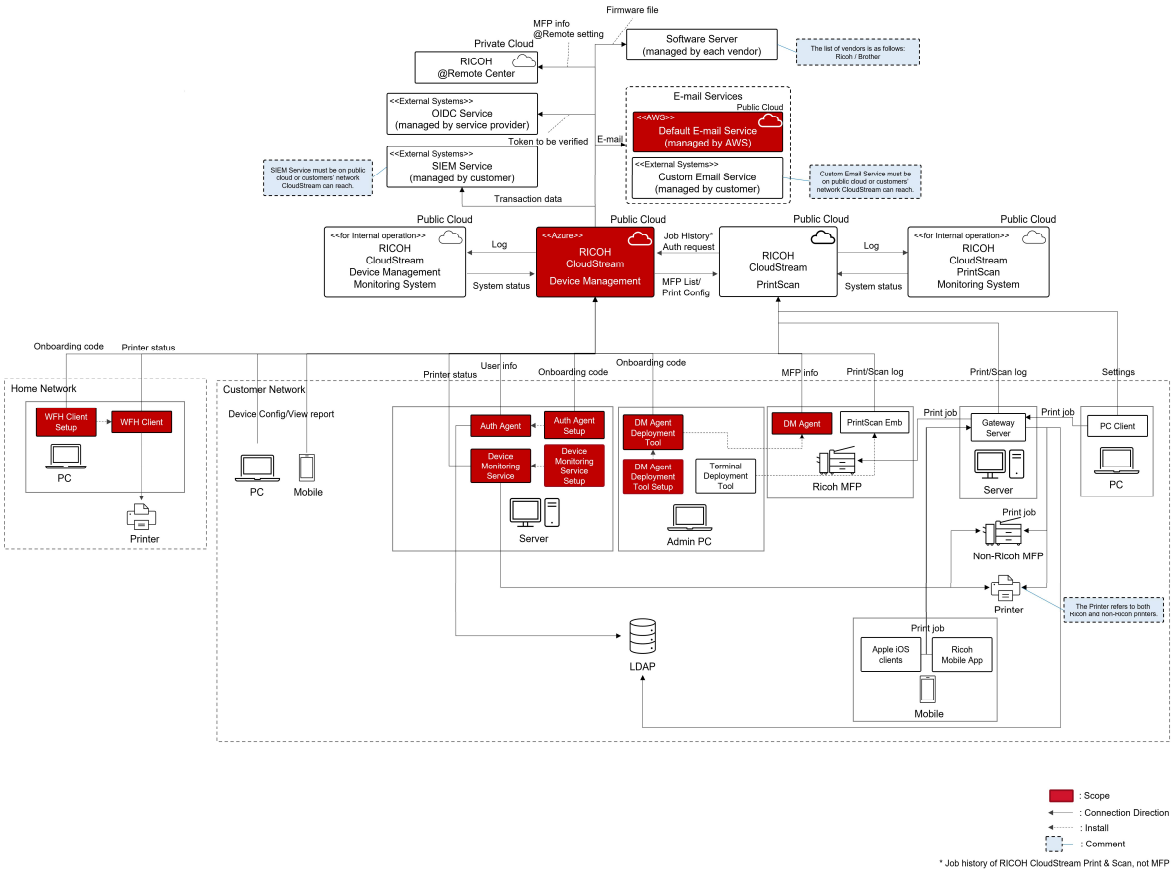


Figure 1. DM System Configuration

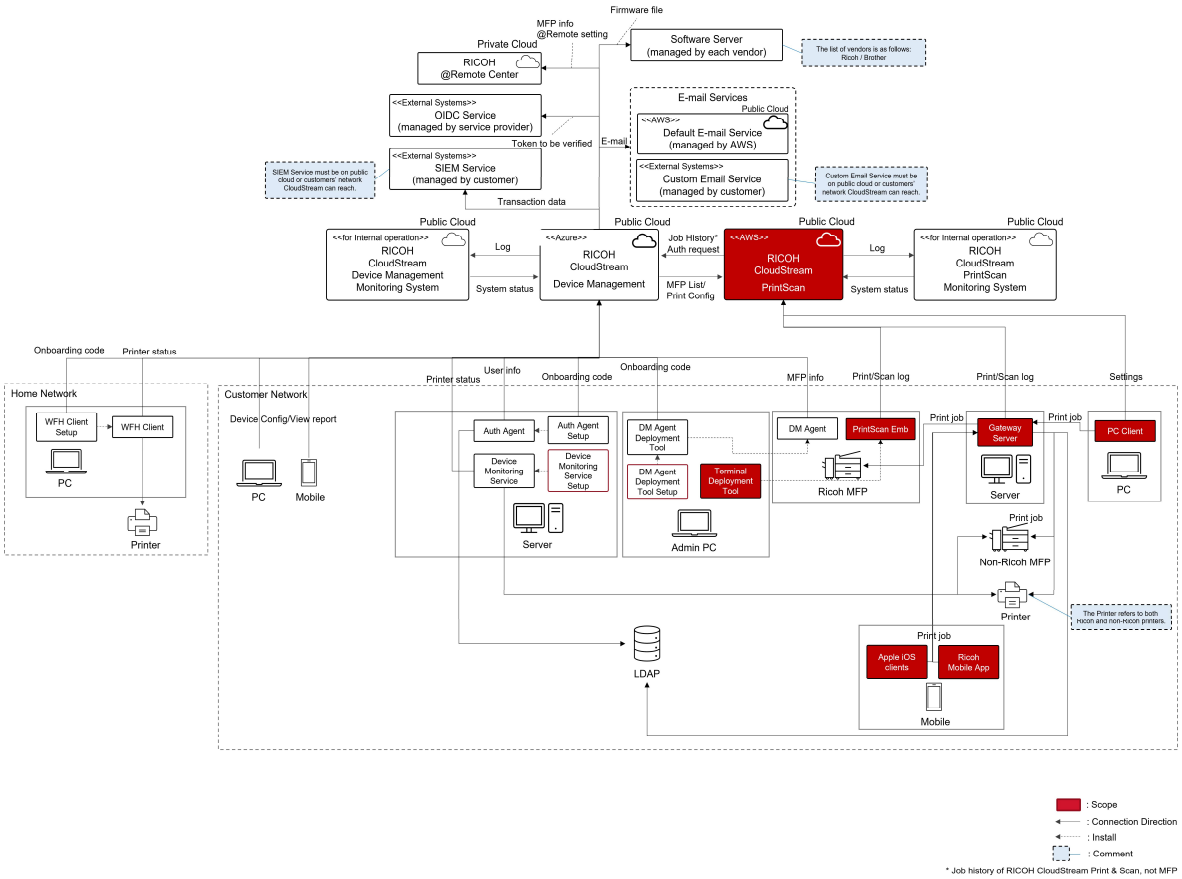


Figure 2. PrintScan System Configuration

Shared Responsibility Model

The use of cloud services is now essential for many organizations, and migrating from on-premises to cloud services has greatly improved operational efficiency and reduced costs. The following figure illustrates the difference in the scope of responsibility for information security measures between cloud services and on-premises.

In the case of on-premises, information security measures were closed within the organization because the organization owns the information system. On the other hand, in the case of cloud services, certain parts of the information system are shared rather than dedicated. Therefore, the cloud service provider is responsible for some information security measures. In the case of CloudStream, a cloud service, the Ricoh Group, which provides CloudStream, is responsible for some information security measures. However, information security measures on the side of service users continue to be important, and information security measures for cloud services can be achieved through the cooperation of both parties.

Responsibility	Cloud Service (CloudStream)	On-Premise
Information and data		
Devices (Mobile and PCs)		
Accounts and identities		
Identity and directory infrastructure		
Applications		
Network controls		
Operating system		
Physical hosts		
Physical network		
Physical datacenter		

: Customer

: Service Provider (Ricoh)

: Shared

CloudStream Security Measures

Data Protection

Cloud services entrust customers' data on the cloud service provider's side, so it is important to comprehend how cloud service providers protect data for risk countermeasures. In this section, it is described how for CloudStream to protect data.

Data Storage Location

CloudStream stores data in regional data centers according to the customer's location.

This improves the responsiveness of data access and enables the customer to comply with legal requirements such as GDPR.

<table>
<tr><th>DM</th><th>PrintScan</th></tr>
<tr><td>Data is stored in a location (data center) according to the customer's region.

CloudStream DM is careful about where data is stored, and uses multiple Azure/AWS data centers depending on the customer's region. Data is stored on servers in the following Azure/AWS data centers:

-For Customers in EMEA: Azure/AWS Europe Region
-For Customers in US and Latin America: Azure/AWS US Region
-For Customers in Canada: Azure/AWS Canada Region
-For Customers in Asia: Azure/AWS Australia Region</td><td>AWS product infrastructure for CloudStream PrintScan resides in the USA, Canada, The European Union, UK, Singapore, and Australia regions.

Open Telekom Cloud (OTC) infrastructure for CloudStream PrintScan resides in Germany.

[Mapping of customer regions and data center location (*1)]

• For customers in EMEA: Frankfurt, Germany
• For customers who select UK DC: United Kingdom
• For customers who select OTC DC: Germany
• For customers who used PMC: Ireland
• For customers in US/Latin America: North Verginia
• For customers in Canada: Montreal
• For customers in Asia Pacific: Singapore, Australia (*2)

(*1) This is a basic policy and may differ depend on the deal.

(*2) For now, it is implemented only in Australia initially.</td></tr>
</table>

Data Type

A list of data types stored in CloudStream is defined and disclosed. Appropriate handling methods are also defined for each data type.

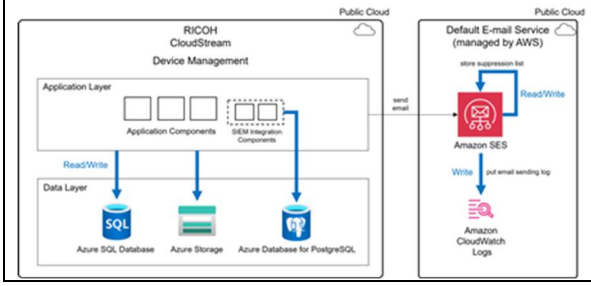
Therefore, it is possible to verify that the handling of data meets the customer’s security requirements.

<table>
<tr><th>DM</th><th>PrintScan</th></tr>
<tr><td><table>
<tr><th>Data Type</th><th>Data Acquisition Method</th><th>Storage Location</th></tr>
<tr><td>Full name</td><td>Input by the administrator,</td><td>Azure SQL Database</td></tr>
</table></td><td>Application metadata, configuration, job metadata, reporting and generic user information are stored in cloud provider’s managed SQL database.</td></tr>
</table>

	Provided by LDAP/OIDC external authentication services	
User name	Input by the administrator, Provided by LDAP/OIDC external authentication services	Azure SQL Database
Email Address	Input by the administrator, Provided by LDAP/OIDC external authentication services	Azure SQL Database
Admin Password	Input by the administrator	Azure SQL Database
Telephone number	Input by the administrator	Azure SQL Database
PIN code	Automatically generated by the system	Azure SQL Database
Card authentication information (card name, card number)	Input by the administrator	Azure SQL Database
Group name/department name to which the user belongs	Provided by LDAP external authentication services	Azure SQL Database
Customer tenant information (sales agent name, customer company name, contact email address, contact name, service URLs, license information)	Input by the administrator	Azure SQL Database
Device information (model name, vendor name, serial number, MAC address, operation status, counter)	Received from DM Agent installed on devices	Azure SQL Database
Device configuration	Input by the administrator	Azure SQL Database
Polling configuration	Input by the administrator	Azure SQL Database
Job history (Job history of RICOH CloudStream Print & Scan, not MFP)	Provided by CloudStream PrintScan	Azure SQL Database
Email server settings (SMTP address, port number, source	Input by the administrator	Azure SQL Database

email address, account name, password)		
SIEM transfer settings (host name, port number, authentication token)	Input by the administrator	Azure SQL Database Azure Database for PostgreSQL
Data storage policy that sets the storage period for the data	Input by the administrator	Azure SQL Database
Client certificate	Automatically generated by the system	Azure SQL Database
Authentication profiles of LDAP/OIDC	Input by the administrator	Azure SQL Database
Alert policy	Input by the administrator	Azure SQL Database
Alert policy log (alert time, destination email address, etc.)	Automatically logged when the administrator set alert policies and alert is executed	Azure SQL Database
Audit log (access date and time, user name accessed, etc.)	Automatically logged when used by the administrator or end user	Azure SQL Database
Authentication log (access date and time, authenticated user name, success or failure of authentication)	Automatically logged when used by the administrator or end user	Azure SQL Database
Report log	Automatically logged when executing a report task	Azure SQL Database
Report information	Automatically stored when executing a report task	Azure Storage
License information	Input by the administrator, Input by the operation team	Azure SQL Database
Access token and refresh token of the OIDC external authentication service	Issued by external services	Azure SQL Database
Suppression list (including email addresses)	Automatically generated by the system	Amazon SES

Email sending log (including email address and subject line)	Automatically generated by the system	Amazon CloudWatch Logs



Data Encryption

CloudStream encrypts data (e.g., AES-256) for storage to prevent information leakage.

User passwords in CloudStream are hashed, so anyone cannnot view the original password string.

DM	PrintScan
All data at rest are encrypted, and passwords are hashed for strict protection basically. CloudStream DM encrypts and saves data in the Azure SQL Database, Azure Storage, Amazon SES, and Amazon CloudWatch Logs (*1) (*2). The encryption algorithm is AES-256. (*1) Suppression list and email sending log are saved in Amazon SES and Amazon CloudWatch Logs respectively. The encryption is implemented according to the policy defined by AWS. https://aws.amazon.com/compliance/data-center/controls/?nc1=h_ls (*2) SIEM transfer settings are encrypted and saved in both Database and Azure Database for PostgreSQL. The encryption algorithm is AES-256.	RICOH leverages several technologies to ensure stored data is encrypted at rest. Platform data is stored using AES-256 encryption. User passwords are hashed following industry best practices and are encrypted at rest. To further safeguard data, RICOH leverages multiple technologies to ensure that stored data is encrypted at rest. Platform data is stored using AES-256 encryption, a robust and widely accepted standard for data security. User passwords are hashed according to industry best practices and are also encrypted at rest, providing an additional layer of security.

Encryption Key Management

Confidential information (e.g., keys used for encryption) handled by CloudStream is managed securely using the services of cloud infrastructure (AWS, Azure) trusted by external certification (ISO27001, SOC 2, NIST, FedRAMP).

DM	PrintScan
The server certification, its secret key, root certification, and other authentication information utilizing inside CloudStream DM are stored in Azure Key Vault for strict control.	Encryption keys for both in transit and at rest encryption are securely managed by the RICOH platform. TLS private keys for in transit encryption are managed through our content delivery partner, ensuring robust security and performance across geographically distributed networks. Volume and field level encryption

	keys for at rest encryption are stored in a hardened Key Management System (KMS). Keys are rotated at a frequency that is dependent upon the sensitivity of the data they are encrypting. (*1) AWS KMS to create and control keys used to encrypt. (https://aws.amazon.com/kms/)

User Authentication

CloudStream password policy configuration feature allows customers to customize the strength of their own passwords. This feature enables customers to configure password policies tailored to their specific security requirements.

CloudStream provides a range of user authentication features, including:
- Username and password authentication
- Authentication via card readers
- LDAP and OIDC support
- Single Sign-On (SSO)
- Multi-Factor Authentication (MFA)

These capabilities enable CloudStream to deliver a more secure and reliable environment for customers.

DM	PrintScan
CloudStream DM provides local authentication for locally managed administrator accounts. To keep passwords of the administrators more secure, we provide the function to configure a password policy for each tenant. Each tenant can configure the following items as a password policy. "Account Locked Threshold" is the number of times before the administrators fail to log in consecutively and the account is locked. If the account is locked, the administrators cannot log in until another administrators unlock the account on the Admin Accounts screen. - Maximum Password Age - Account Locked Threshold - Minimum Password Length - Character type of password (numeric, symbol, etc.) On the other hand, external authentication services supporting LDAP or OIDC manage the general users. Users authenticated via LDAP or OIDC can also be granted administrative privileges . MFA is enabled for accessing Microsoft Entra ID settings for CloudStream DM. Supported authentication methods are authenticator apps, software tokens (one-time passwords), and SMS. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks	The RICOH products allow users to login to their CloudStream PrintScan accounts using built-in login or Single Sign On (SSO). The built-in login enforces a uniform password policy which requires a minimum of 6 characters and a combination of lower- and uppercase letters, special characters, whitespace, and numbers. People who use RICOH's built-in login cannot decrease the default password length and have the ability to enforce more secure password policies if required. Customers who use an SSO provider can set up SSO-based login for their users. Instructions for setting up SSO are available in the CloudStream PrintScan documentation. Single Sign On users can configure a password policy in their SSO provider. More advanced SAML-based SSO integrated with any SAML-based IDP is available. MFA is enabled for accessing Microsoft Entra ID settings for CloudStream PrintScan cloud and PC Client. Supported authentication methods are authenticator apps, software tokens (one-time passwords), and SMS. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks

External Authentication Linkage

It is possible to integrate with external user management systems using standard protocols such as LDAP and OIDC.

This enables centralized user management, allowing for streamlined administration.

By implementing multi-factor authentication (MFA), a higher level of security can be achieved.

DM/PrintScan
CloudStream is built on modern authentication methods (OAuth 2.0) and utilizes Single sign-on (SSO) provided by external Identity Providers such as Microsoft Azure Active Directory. SSO allows you to authenticate users in your own systems without requiring them to enter additional login credentials to use the CloudStream. SSO is a session and user authentication service that permits a user to use one set of login credentials to access multiple applications. Customers who want to use CloudStream, we recommend them to use an external Identity Provider that manages the Internet identity of all their users. This approach allows admins to define the required level of user identity protection by enforcing multi-factor authentication. Another advantage is that users log in at browsers which they know (and consider secure) via Microsoft's authentication page, and CloudStream merely receives information on the results. User credentials are safely confirmed by their external Identity Provider and never shared with the service provider (CloudStream). The external Identity Provider provides CloudStream only basic user details such as their first name, last name, and username based on permissions and grants set in the Identity Provider. Whenever a user logs in, CloudStream refreshes the user details from the external Identity Provider – role membership changes, name changes and account deactivation/reactivation. Browser access to the management portal uses role-based access within the application, authenticated via SAML, OAUTH2 and OpenID Connect industry standards. At MFDs, CloudStream may authenticate a user's identity by verifying against a company's directory. The device connects to Active Directory using an LDAP (Lightweight Directory Access Protocol) connector on the Edge device synchronized to the cloud service via secured line. The product does not access any user passwords or other private data. For cloud directories (Azure AD (Active Directory), Google, …) standard OAUTH2 protocols are used.

Account Management by the Customers

As described in "User Authentication" above, CloudStream provides the feature to configure password policies.

DM	PrintScan
Information security measures for customers using CloudStream DM will continue to be important. We ask our customers to do the following: -Appropriate management of tenant accounts. (user registration, deletion, authorization, etc.) -The password assigned to each user shall be properly managed by the user themselves. -Set the password according to the email sent to the user at the time of user registration. -Appropriately manage the set password so that it is not known to other people. -Be careful about handling confidential information when using LDAP/OIDC to link with external authentication services.	The RICOH products allow for granular authorization rules. Customers are empowered to create and manage users of their portals and assign the privileges that are appropriate for their accounts and limit access to their data features. For more information about user roles, please see the CloudStream PrintScan documentation.

-Appropriately manage your devices. -Synchronize the time set of the customers' device with NTP etc. (The purpose is to ensure proper encrypted communication between your devices and CloudStream DM. All CloudStream DM servers are synchronized with NTP.). In addition, CloudStream DM provides a function to help you manage your password more securely. For more information, see Security Measures for Customers' Account.	

Data Deletion

In response to a deletion request from customers or periodic inventory, we will delete the tenant information.

The deletion process is operated in an integrated manner with DM and PrintScan.

DM	PrintScan
In response to a deletion request from the customer or periodic inventory, we will delete the tenant information from Azure/AWS.For periodic inventory, the tenant information will be deleted every six months after all licenses registered to the tenant have expired for more than three months. None of the customer's confidential information will not remain in our database servers. After deletion, the data becomes inaccessible. In addition, the handling of the data at the time of deletion is strictly controlled by Azure/AWS. Azure: https://learn.microsoft.com/en-US/azure/security/fundamentals/protection-customer-data AWS: https://aws.amazon.com/compliance/data-center/controls/?nc1=h_ls	In response to a customer deletion request or periodic inventory, we ensure that all tenant information is completely removed from our systems. We have established robust data deletion procedures that are compliant with regulatory requirements, including the General Data Protection Regulation (GDPR). Our systems are designed to ensure that once data is deleted, no residual data remains, thus maintaining the confidentiality and integrity of customer information. We temporarily store files used for OCR processing only during the processing period. Once the workflow is completed, all data is deleted, except for metadata retained for reporting purposes. Expired trial tenants will be deleted after 90 days, and production tenants will also be deleted after 90 days automatically.

Cloud Service Provider's Access Control to Data

The customer cannot manage the risk of unauthorized access to customer data entrusted to the cloud service provider from outside or inside the provider. Therefore, it is important for the cloud service provider to implement external and internal access control as a risk countermeasure. CloudStream implements external and internal access control as follows.

Access Authority Management

In the development and operation of CloudStream, we implement proper Role-Based Access Control (RBAC) for our employees. Access permissions granted to employees are limited to the minimum.

This prevents unintentional information leakage, data falsification, and loss.

DM	PrintScan
We use Azure RBAC to set access permissions for each account and each server so that we can control access to the minimum necessary. In addition, handling of access control is defined, such as periodic inventory of accounts. Ricoh Group may view the data only in the event of a failure or when responding to customer inquiries. Ricoh Group cannot view raw admin passwords because they are hashed, although Ricoh Group can view data only if required for incident or handling inquiries from customers. We may temporarily grant our employees access to a customer's tenant, strictly for the purpose of supporting service implementation, and only with the customer's explicit consent. Azure's activity logs feature records events related to the creation, modification, and deletion of CloudStream resources in an audit log. These events include actions such as starting and stopping virtual machines, configuration changes, and more. Access to the activity log is restricted to employees with the necessary permissions. Activity logs are monitored by Azure Monitor, which notifies system administrators when it detects suspicious activity. ● Azure Monitor System monitoring and collecting service logs and metrics to visualize activities.	Access to customer data is limited to authorized RICOH group or RICOH partner (dealer etc) who require it for their job. A very limited number of highly trained specialists responsible for application maintenance and management only in specific cases and on an as-needed basis have administrator access to the databases. Access to the data is logged to cloud provider's audit logs.

Multi-tenant

CloudStream is a multi-tenant service.

The data between tenants (customers) is logically separated.

DM	PrintScan
Like many other SaaS cloud services, CloudStream DM provides services to multiple tenants and operates in a multi-tenant environment. The data of each tenant is logically separated and it is not possible to refer to the information of other tenants.	For shared infrastructure customers, secured separation between tenants' User Directories are in place. RICOH provides a highly scalable, multi-tenant SaaS solution. The cloud-based application, in this case CloudStream PrintScan provides services to multiple businesses, each one

	considered a separate 'tenant.' In this multitenant scenario, data is logically separated and each tenant must have its own metadata identification, separation, and protection All above mentioned points apply Each tenant owns a unique security certificate associated with its metadata. The user interface accesses to authorized content exclusively. RICOH logically segments the data using portal IDs and associates that unique ID with all data and objects specific to a customer. Information is made available via the user interface to be produced for a specific RICOH portal, without the risk of cross-portal access or data pollution. Authorization rules are incorporated into the design architecture and validated on a continuous basis. Additionally, we log application authentication and associated changes and application availability.

Physical and Environmental Security

Physical Server

As physical servers, we use cloud infrastructure (AWS, Azure) data centers trusted by external certification (ISO27001, SOC 2, NIST, FedRAMP). Physical security is ensured by the cloud infrastructure provider.

Employees of Ricoh and partner companies do not have access to physical servers. In addition, the each physical security is ensured by Azure/AWS as follows.

Azure: https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

AWS: https://aws.amazon.com/compliance/data-center/controls/?nc1=h_ls

DM	PrintScan
Since cloud services store data on the side of the cloud service provider, the customer cannot manage the physical security of the storage location. Therefore, it is important for the operator to ensure the security of the storage location. CloudStream DM uses Azure and AWS data centers as data storage locations. Azure and AWS maintains an audited security program, as well as physical, environmental, and infrastructure security protections. Business continuity and disaster recovery plans have been independently validated as part of their(Azure and AWS) SOC 2 Type 2 and ISO 27001 certifications.	Because we leverage public cloud services for hosting, backup, and recovery, RICOH does not implement physical infrastructure or physical storage media within its products. RICOH does not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our products available to our customers. AWS maintains an audited security program, as well as physical, environmental, and infrastructure security protections. Business continuity and disaster recovery plans have been independently validated as part of their(AWS) SOC 2 Type 2 and ISO 27001 certifications.

Operations Security

It is important for cloud service providers to take various operational measures daily so that cloud services always maintain security. In accordance with Ricoh Group's established security processes, CloudStream routinely implements the following various measures.

Vulnerability Support

We regularly conduct vulnerability assessments using assessment tools to detect and address potential vulnerabilities at an early stage.

This prevents information leakage and system downtime due to attacks.

DM	PrintScan
We regularly conduct vulnerability assessment using multiple vulnerability assessment tools and confirm that there are no vulnerabilities including OWASP (Open Web Application Security Project) Top 10 in each release cycle, typically every three months We regularly collect vulnerability information and take measures according to Ricoh Group's internally established process. If a vulnerability that affects in CloudStream DM is discovered, Ricoh will provide information to customers via the website. To defend against malware intrusion, we do the following: -Detection of malware by Microsoft Defender for Cloud -Denial of unauthorized outbound requests by Azure Firewall	We use OWASP (Open Web Application Security Project) guidelines for software design, vulnerability assessment and threat modelling. Possible security implications are identified and marked during design phase, the code is tested using static and dynamic code tools and analysis. Features with security tags are tested by the QA team and only released if passed. RICOH manages a multi-layered approach to vulnerability scanning, using a variety of industry-recognized tools to ensure comprehensive coverage of our technology stack. Vulnerability scans are configured to scan for exploitable vulnerabilities on a daily basis. Continually running scans, using adaptive scanning inclusion lists, and continuously updating vulnerability detection signatures helps RICOH stay ahead of many security threats. According to our Software Security Development standard and our Security testing standard, industry best practices for secure SDLC including formal design reviews, code reviews, threat modelling and scanning of the code during development. We also bring in industry-recognized third parties to perform quarterly penetration tests. The goal of these programs is to iteratively identify flaws that present security risk and rapidly address any issues. Penetration tests are performed against the application layers and network layers of our technology stack addressing the OWASP Top 10 and other common Application Security Risk. Schedule of penetration testing is mandated by our Security Testing standard. The results from all Penetration tests are being evaluated, discussed, and prioritized according to the risk score with the Product Management team. Remediations are then planed and

	implemented. According to the ISO27001 risk assessment framework, all critical issues are also added to our Risk Treatment table. The content of the PEN Testing reports is highly sensitive information and considered confidential. In exceptional cases we might consider sharing a redacted version of our PEN Tests against a signed NDA (Non-Disclosure Agreement). We leverage different endpoint protection solutions to protect its systems. These enables us to have extensive visibility into anomalous system behaviour as well as to rapidly investigate and take appropriate action through either automated event triggers or manual containment of a system. Protecting our Cloud environment in AWS we use several AWS professional tools, including: ● Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. ● AWS Security Hub evaluates configuration items to assess whether the AWS resources comply with the desired configurations defined by the defined security standards.

Protection from DDoS Attack

CloudStream is secured by detecting and protecting DDoS attacks using the services of cloud infrastructure (AWS, Azure) trusted by external certification (ISO27001, SOC 2, NIST, FedRAMP).

DM	PrintScan
To counter to DDoS attacks, Azure DDoS Protection monitors external communications to detect and mitigate DDoS attacks.	To counter to DDoS attacks, AWS Shield Standard monitors external communications to detect and mitigate DDoS attacks.

Backup

The CloudStream database is regularly backed up.

This allows data to be restored in the unlikely event of database failure, etc.

DM	PrintScan
We store the data in zone redundancy and regularly back up the data in case of failures of database or storage, and erroneous operations.	Systems are backed up regularly with established schedules and frequencies. Several days' worth of backups are kept for any database in a way that ensures restoration can occur easily. Backups are monitored for successful execution, and alerts are generated

The regular backed-up data is stored in zone redundancy and is not accessible to users. Backup data is stored in the Azure SQL Database and Recovery Services vault.	in the event of any exceptions. Failure alerts are escalated, investigated, and resolved. Data is backed up daily to their local region. Additionally, backups are copied periodically to off-site locations in the event of a primary regional outage. Monitoring and alerting are in place for replication failures and triaged accordingly. During the restore tests, we use a checklist to determine all the items that need to be tested to confirm that the DR test was successful. All production data sets are stored on a highly available file storage facility like Amazon's S3. By default, all backups are encrypted and protected through access control restrictions on RICOH product infrastructure networks and access control lists on the file systems storing the backup files.

Troubleshooting

CloudStream logs the system for troubleshooting purposes. The logs are used to assist troubleshooting issues, and the logs can be viewed by Ricoh and partner company employees as needed.

However, confidential information such as passwords and document data are not output in the logs.

DM	PrintScan
We log application logs and access information to the system, but we do not log the user password.	Application logs for troubleshooting are collected in cloud provider's central log repository and available to support personnel on an as-needed basis. Logs do not expose any access/credentials related or document content information.

System Monitoring

An independent monitoring system is in operation to monitor the operational status of CloudStream.

This maintains the high response performance and availability of CloudStream.

DM	PrintScan
We monitor the operational status and performance of CloudStream hosted in Azure and AWS 24 hours a day, 365 days a year. The system will notify Ricoh Group when it detects a problem, and Ricoh will respond promptly.	Protecting our Cloud environment in AWS we use several AWS professional tools, including: ● AWS GuardDuty which is a threat detection service that continuously monitors for malicious activity and unauthorized behaviours to protect the AWS account. ● AWS IAM Access Analyzer helps us to identify the resources in the organization,

Additionally, we use Azure professional tools to protect CloudStream. Microsoft Defender for Cloud Threat detection service to protect the Azure account by monitoring for resource vulnerabilities and unauthorized network access, and assessing whether encryption settings and security configurations follow best practices	such as Amazon S3 buckets or IAM (Identity Access Management) roles, that are shared with an external entity. This lets us identify unintended access to our resources and data, which is a security risk. ● Additionally, we periodically monitor AWS Trusted advisor findings to keep best practices for cost management, high availability, security, and performance.

Audit Log

CloudStream keeps audit logs of the system. We also keep an audit log of customers' activities, which customers can use themselves.

DM	PrintScan
User activity on CloudStream and authentication results are available to customers as audit logs or authentication logs for their own monigtoing and review. The storage period can be set by the customer for up to five years. Also the system utilizes Azure Monitor to record internal system activity as audit logs. Activity logs are used for internal investigations when unauthorised activity is detected or suspected. These logs are stored for a period of 5 years.	The CloudStream PrintScan system records internal system activity as audit logs. These logs are reviewed to detect any signs of security anomalies or breaches. Audit logs are used internally to support investigation in the event of unauthorized activity, or when such activity is suspected. Print and scan activity on CloudStream PrintScan is available to customers on CloudStream DM for their own monitoring and review.

Internal Audit

Internal audits are conducted by Ricoh and its partners to ensure that security measures are properly implemented.

DM	PrintScan
We regularly conduct internal audits by Ricoh Group's department independent of CloudStream DM to confirm that CloudStream DM security measures are properly implemented. https://www.ricoh.com/security Furthermore, we conduct regular assessments to identify security risks in areas such as organizational management, security training, business continuity planning, and information asset management.	Internal audits are important for our Information Security Management System (ISMS), ensuring compliance with ISO 27001 and our internal security policies. These audits are regularly scheduled, meticulously planned, and conducted by independent, qualified auditors. In addition we have automated compliance control monitoring using Drata.

Communication Security

Network Separation

CloudStream is protected by network separation and network firewalls to prevent unauthorized access.

DM	PrintScan
CloudStream implements a multi-layered defense strategy for all connections. Azure servers that store customer data cannot be accessed directly from the Internet (must go through an endpoint within CloudStream DM). In addition, communication is restricted by a virtual firewall (Azure Network Security Group) to prevent unauthorized access. Network configurations are documented based on best practices and are reviewed at least once a year.	The RICOH product infrastructure enforces multiple layers of filtering and inspection of all connections throughout the platform. Network-level access control lists are implemented to prevent unauthorized network access to our internal product infrastructure. Firewalls are configured to deny network connections that are not explicitly authorized by default, and traffic monitoring is in place for detection of anomalous activity. Changes to our network security are actively monitored and controlled by standard change control processes. Firewall rulesets are reviewed on an annual basis to help ensure that only necessary connections are configured.

Communication Path

The direction, protocol (e.g., HTTPS), and type of data to be transferred are clearly indicated for communications within and between CloudStream and external entities.

This allows us to verify that the communications that occur when using CloudStream meet the customer's security requirements.

DM	PrintScan
Figure 3 shows communication direction between components and communication protocols for CloudStream DM. Additionaly, dta flow between components of CloudStream DM are shown in "Appendix/Data Flow (DM)". CloudStream DM communicates any hostname and port set by customers of email servers and LDAP authentication servers over TCP. In addition, communication over HTTPS (443/TCP) required to operate the system is used. As for communication from the customer environment to CloudStream DM, please refer "Appendix/Communication from the customer environment to CloudStream" CloudStream DM sends email to customers. CloudStream DM offers a default email server, and customers also have the option to utilize their own mail server.	Figure 4 shows communication direction between components and communication protocols for CloudStream PrintScan. Additionaly, data flow between components of CloudStream PrintScan are shown in "Appendix/Data Flow (PrintScan)" **Print Job Data in transit: Worksta tion to Edge device & Edge device to the multifunction printer.** Because the Edge device is secure in your trusted network, all print job data stays safely within your company's boundaries. Data is transferred via secured IPPS protocol for printers that support higher levels of data security. Support for legacy, unsecured protocols, such as LPR is also available, yet disabled by default. **Print Job Data in transit: Workstation to Cloud & Cloud to the multifunction printer.** Data is transferred via secured TCP or HTTPS protocol to cloud and downloaded by trusted multifunction printer using device authenticated HTTPS protocol from the cloud in

The source address varies based on customers' regions. Access to the default mail server is exclusively permitted from a fixed IP address within each CloudStream DM region.

Customer	Source Address
Customers in EMEA	mail.eu.cloudstream.ricoh.com
Customers in US and Latin America	mail.na.cloudstream.ricoh.com
Customers in Canada	mail.ca.cloudstream.ricoh.com
Customers in Asia	mail.ap.cloudstream.ricoh.com

context of user authenticated to the multifunction printer.

Scan Job Data in transit: Multifunction printer to Edge cloud

Scan data are transferred to the cloud services using device-authenticated (with context of specific user) WebDAV/S protocol.

Print job metadata: Edge device to cloud or multifunction printer to cloud

Print job metadata is used for reporting purposes. Reports provide insight and an audit of print services use. Metadata includes print and scan activity on printers or groups of printers, users or groups of users. It does not include the content of a document.

Please refer to "Gateway Server to Cloud Services" in Data Flow (PrintScan) for protocols.

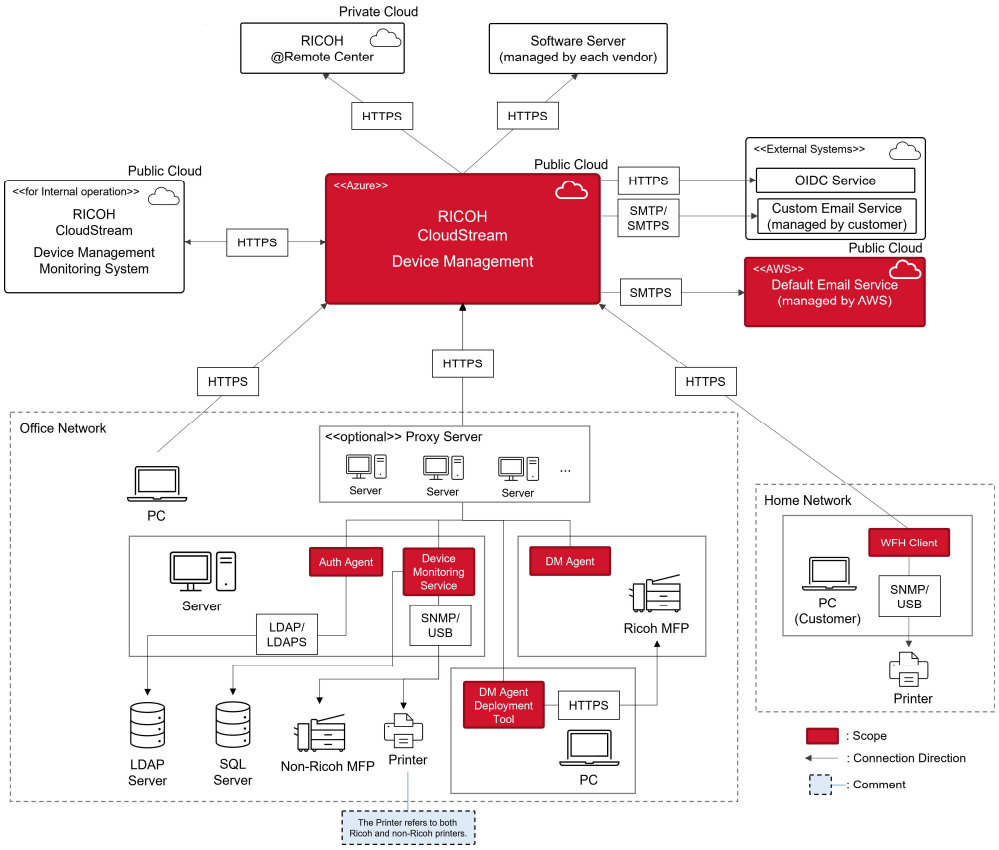


Figure 3. DM Data Flow

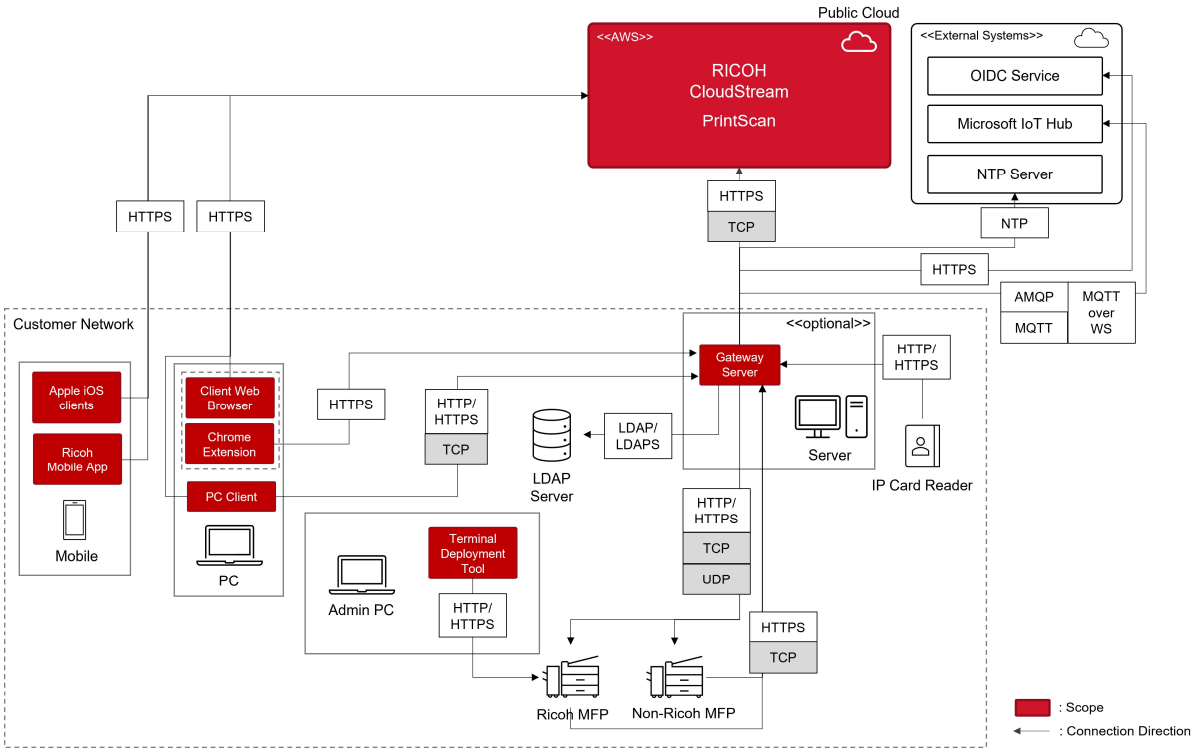


Figure 4. PrintScan Data Flow

Communication Encryption

CloudStream generally encrypts communications. We disclose supported protocols (TLS, IPv4, etc.) and public key lengths.

This prevents data eavesdropping and tampering, and it is possible to verify that the communications that occur when using CloudStream meet the customer's security requirements.

DM	PrintScan
All communication paths are encrypted with HTTPS, except for email (*). Note that IPv6 connections are not supported. We use public certification with ECC 256 bit published by third-party certificate authority as server certification. Supported TLS version and cipher suite are as follows: TLS Version ·TLSv1.2 ·TLSv1.3 Cipher Suite ·TLS_AES_256_GCM_SHA384 ·TLS_AES_128_GCM_SHA256 ·TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ·TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ·TLS_CHACHA20_POLY1305_SHA256	All sensitive interactions with the RICOH products, including API calls and authenticated sessions, are encrypted in transit using TLS version 1.3 and 2,048-bit keys or better. This ensures that data transmitted between clients and servers remains secure and protected from interception or tampering. Additionally, certain email features are designed with an extra level of both at-rest and in-transit encryption, enhancing the overall security posture of products by RICOH and its partners. These measures collectively ensure that sensitive information is consistently protected across all facets of data handling and storage. Secure portal communication between an administrator and the management portal using HTTPS, compatible with the version supported by the client.

(*) The default email server employs SMTPS for the encryption of email traffics. In case that customers use their own email server, customers can configure to use SMTPS or STARTTLS to send encrypted email traffic.	Browser access to the management portal is through HTTPS. Updates for edge devices are transferred via encrypted and device authenticated HTTPS communication.

Mutual Authentication

CloudStream's communication can verify through mutual authentication that both server and client are trusted.

This is important from a zero-trust perspective, preventing access from unauthorized clients.

DM	PrintScan
Communications from DM Agent, Auth Agent, WfH Client, and Device Monitoring Service to the cloud service are secured via mutual TLS authentication. Client certificates for mutual TLS authentication are securely distributed using an onboarding code to the client. An onboarding code is a unique number to control the client certificate. The administrator issues an onboarding code with an expiration date and set it to the client. That is how client certificates are securely distributed to the client.	All system services, components, Edge devices and deployed MFDs are mutually authenticated. Once secure cloud and edge environments are established, all services and devices (including optional authentication for MFDs – if supported by the MFD vendor) are performed using mTLS industry standard protocol.

Permission Settings for Communication from the Customer Environment to CloudStream

We provide connection information (fixed IP address, port, etc.) to CloudStream. See table below for details. IP addresses are subject to change.

By configuring this information in the firewall whitelist of the customer's environment, only communication with CloudStream will be permitted, enhancing the security of the customer's environment.

<table>
<tr><th>DM</th><th>PrintScan</th></tr>
<tr><td>IP addresses to communicate from customer environment to CloudStream DM or from CloudStream DM to the Internet are fixed. Customers can give access from the customers’ environment only to CloudStream DM by setting the fixed IP addresses to the whitelist of the customers’ firewall. Also, customers can give access only from CloudStream DM by allowing email servers or LDAP authentication servers to receive from the fixed IP addresses. The fixed IP address varies for each CloudStream DM region, and the IP address values are as follows:
<table>
<tr><th>CloudStream DM Region</th><th>IP Address</th></tr>
</table>
</td><td>A complete list of the ports and protocols that must be enabled on firewalls to ensure system functionality can be found in the CloudStream PrintScan documentations. The customer network is expected to allow access to ports and services outlined in the documentation over the Internet, including name resolution (DNS).

Inbound (from Internet to CloudStream cloud)
<table>
<tr><th>CloudStream PrintScan Region</th><th>IP Address</th></tr>
<tr><td>For customers in EMEA: Frankfurt, Germany</td><td>52.57.32.65</td></tr>
</table>
</td></tr>
</table>

For Customers in EMEA: Azure Europe Region	20.113.73.197
For Customers in US and Latin America: Azure US Region	20.252.6.56
For Customers in Canada: Azure Canada Region	20.220.243.35
For Customers in Asia: Azure Australia Region	20.227.2.98

	18.159.1.221 3.78.120.145
For customers who select UK DC: United Kingdom	3.8.221.201 52.56.154.204 18.135.59.42 18.130.67.94 (for Xerox devices only)
For customers who select Ireland DC: Ireland	52.50.253.210 18.202.147.163 52.19.122.66 52.30.117.6 (for Xerox devices only)
For customers in US/Latin America: North Verginia	23.21.249.252 54.225.106.109 54.205.27.251
For customers in Canada: Montreal	15.222.76.70 15.156.3.124 15.156.139.9
For customers in Asia Pacific: Singapore, Australia	54.153.223.24 13.237.129.18 13.238.29.243

Outbound (from CloudStream cloud to Internet)

CloudStream PrintScan Region	**IP Address**
For customers in EMEA: Frankfurt, Germany	3.66.14.128 18.184.95.83 18.199.47.109
For customers who select UK DC: United Kingdom	18.134.42.232 3.11.157.65 3.10.114.230
For customers who select Ireland DC: Ireland	176.34.88.154 54.217.150.104 54.155.19.247
For customers in US/Latin America: North Verginia	35.168.89.37 35.169.168.199 3.225.50.8
For customers in Canada: Montreal	15.222.53.82 3.98.69.134 15.156.114.171

	For customers in Asia Pacific: Singapore, Australia	13.236.170.166 3.106.171.162 13.237.17.215

Development Security

Development Process

We emphasize security not only in operation but also in development.

In developing CloudStream, Ricoh and its partners develop services in accordance with ISO and other international standards. Our development processes are documented and communicated to all CloudStream developers.

CloudStream is completely separate for production and development environments (development, testing and staging). Customer data is only used in the production environment for previously agreed uses.

DM	PrintScan
CloudStream DM applications, including source code and build artifacts, are securely stored in an Azure-provided repository. These applications are built and deployed to the cloud environment using CI/CD pipeline tools. The cloud infrastructure is segmented into distinct environments—development, testing, staging, and production—each managed under a secure software development lifecycle (SDLC) process. Cloud service providers must implement security measures not only in operation but also in development to maintain the security of their services. Ricoh Group develops our products in accordance with ISO/IEC27034-1 of international standard of security technology. https://www.ricoh.com/security Code reviews, testing, and merge approval are performed before deployment. Merge approvals are controlled by the repository owner. Once approved, the code undergoes building, unit testing, and deployment in CloudStream DM's Continuous Integration (CI) environment. Subsequently, the code is tested in the separated development and test environment before being released to production.	**Application/Edge Device Updates** Edge device application is managed by industry-standard tools and protocols and systems provided by cloud provider platform. Deployment is managed via tiered environment with separated development, testing, staging and production environment plus dedicated deployment plans per customer. Application components are stored in cloud provider's secured artifact repository and deployed to cloud instances and edge devices using automated and secured state-of-the-art tools (also provided by the cloud platform). All artifacts are created and deployed using secured development lifecycle process and managed by team of highly trained specialists responsible for application maintenance and management. Code reviews, testing (where applicable), and merge approval is performed before deployment. Approval is controlled by designated repository owners. Once approved, code is automatically submitted to CloudStream PrintScan's continuous integration environment where compilation, packaging and unit testing occur.

Change Management

CloudStream services are managed following the Infrastructure as Code (IaC) approach, incorporating a well-defined change management process.

DM	PrintScan
CloudStream DM applications and infrastructure are managed using images and configuration files. These assets are deployed and updated in the cloud environment through carefully managed configuration scripts, following a strict change management process. The applications and infrastructure are continuously monitored and secured by Microsoft Defender for Cloud (D4C). Any deprecated settings or vulnurabilities detected by D4C are promptly addressed through the established change management process.	Automation drives our ability to scale with the customers' needs. Server instances are tightly controlled from provisioning through deprovisioning, ensuring that deviations from configuration baselines are detected and reverted at a predefined cadence. If a production server deviates or drifts from the baseline configuration, it will be overwritten with the baseline configuration within 30 minutes. All server type configurations are embedded in images and configuration files. Server-level configuration management is handled using these images and configuration scripts when the server is built. Changes to the configuration and standard images are managed through a controlled change management process. Each instance type includes its own hardened configuration, depending on the deployment of the instance. Patch management is handled using automated configuration management tools or by removing server instances that are no longer compliant with the expected baseline and provisioning a replacement instance in its place. Rigorous and automated configuration management is baked into our day-to-day infrastructure processing.

Supplier Relationships

Even if the security of the cloud service and its organization is perfect, there is a risk that the supply chain (services used and contractors) will be attacked. It is common to use other companies' PaaS/IaaS as one of the services used in SaaS. CloudStream implements the following security measures for such supply chains.

Governance of outsourcing company

We use cloud infrastructure (AWS, Azure) trusted by external certification (ISO27001, SOC 2, NIST, FedRAMP).

The security of these outsourcing partners is guaranteed by the cloud infrastructure providers. (→Reference: AWS (*1), Azure (*2))

(*1) https://aws.amazon.com/jp/compliance/programs/

(*2) https://learn.microsoft.com/en-us/compliance/

DM	PrintScan
CloudStream DM uses Azure and AWS, a typical public cloud, as PaaS/IaaS. Azure and AWS are used worldwide and security is guaranteed as follows. Azure: https://learn.microsoft.com/en-us/compliance/ AWS: https://aws.amazon.com/compliance/	CloudStream PrintScan uses AWS, a typical public cloud, as PaaS/IaaS. AWS is used worldwide and their security is guaranteed as follows. AWS: https://aws.amazon.com/jp/compliance/

- Ricoh Group emphasizes information security of outsourcing companies and implements measures to protect information security. https://www.ricoh.com/security	

Information Security Incident Management

Incident Information Publication Method

CloudStream Device Management provide real-time service availability by a status dashboard. The status dashboard will be updated, and incident information will be posted in the event of service outage or when otherwise deemed necessary as an incident. Customers themselves can check the status of service operation and recovery by themselves.

Status Dashboard: https://cloudstream.status.ricoh.com

Ricoh will also notify you in advance of planned outages on the status dashboard.

In addition to posting notifications on the status dashboard, you can subscribe to receive emails when service outage information is posted.

Customer Support

If you discover CloudStream Device ManagementDM incident, please contact Ricoh Group customer support.

https://www.ricoh.com/contact

Availability

It is important to reliably provide services even when cloud service servers are affected by disasters (availability).

Redundancy

As a countermeasure against failures and disasters, we have redundant configurations of servers across multiple availability zones.

The redundant configurations are achieved by adopting services from cloud infrastructures (AWS, Azure) trusted by external certifications (ISO27001, SOC 2, NIST, FedRAMP).

DM	PrintScan
CloudStream DM has redundant servers in 3 different availability zones (*) in Azure. Our applications are deployed with a minimum of 2 server instances. This allows us to continue service delivery even if a failure or disaster occurs in a single availability zone. In addition, we distribute the load across multiple redundant servers to improve availability. (*) Redundant within a single availability zone just for transfer settings of the SIEM integration	Our solution has been set up using 3 different Availability Zones in each of the regions where the solution is deployed. This means that we have multiple servers connected in a cluster environment with failover into different physical locations. If one zone for whatever reason fails, other servers located in a physically different location will automatically take over, completely seamless to users.

	RICOH will make reasonable efforts to achieve an uptime of 99.9% (calendar month) for the Service. All RICOH product services are built with full redundancy. Server infrastructure is strategically distributed across multiple distinct availability zones and virtual private cloud networks within our infrastructure providers, and all web, application, and database components are deployed with a minimum of n+1 supporting server instances or containers. RICOH and its partners maintain a disaster recovery plan that is tested quarterly as a part of our ISO27001 controls. Our Recovery Point Objective is maximum 24 hours and SLO for Recovery Time Objective, RTO is 90 min.

Compliance

It is important to properly handle customer information entrusted to cloud services based on the laws and regulations of each country.

Privacy Policy

Ricoh Group has established a privacy policy and publishes it to customers on its website.

https://www.ricoh.com/privacy/group-privacy-policies

Zero Trust

Cloud Infrastructure

RICOH CloudStream uses software-defined infrastructures in Cloud and Edge (*) to provide auto-scaling and advanced networking and security.

(*) Edge Devices on which CloudStream application runs, such as MFP, Windows Server, and Linux Server, and PC.

In the view of Zero Trust approach, there are no trusted networks and zero implicit trust among services, instances, and clients. All system services, components, Edge devices and (optionally) deployed MFDs are mutually authenticated, and all communication is secured using industry-standard protocols, such as TLS (Transport Layer Security) 1.3.

Zero Trust is often perceived as a network level architectural decision. Yet we believe that the Zero Trust approach needs to be applied holistically.

The following network protocols are primarily used:

- ✓ HTTPS (HTTP over 1.3 with server authentication)
- ✓ HTTPS with mTLS (HTTP over 1.3 with mutual-TLS authentication)
- ✓ IPPS (IPP over HTTPS)

mTLS refers to TCP communication secured with mTLS (mTLS 1.3)

Communication happens in 3 tiers:

- ✓ Cloud: services exposed via publicly accessible endpoints (public cloud)
- ✓ Edge 2 Cloud: bi-directional communication from Edge devices to Cloud services.
- ✓ On Premise: Edge 2 Edge, Mobile Clients, and Desktop Clients

Edge Device

RICOH CloudStream uses software-defined infrastructures in Cloud and Edge (*) to provide auto-scaling and advanced networking and security.

(*) Edge Devices on which CloudStream application runs, such as MFP, Windows Server, and Linux Server, and PC.

- ✓ Trusted and Secure Device Identity - Each device provides trusted bond with its associated cloud tenant for management. Such identity is sufficient for establishing trust and unique identification of the device. This identity includes, but is not limited to, secure establishment and storage of encryption and digital signing keys in specialized secure enclave on your device.
- ✓ Mutual Service Authentication - Once secure cloud and edge environments are established, all services and devices (including optional authentication for MFDs – if supported by the MFD vendor) are performed using mTLS industry standard protocol.
- ✓ Cloud Manageability - All cloud and especially edge deployments are securely manageable from cloud, including seamless remote deployments and rolling / transitional updates and upgrades. Device 2 Cloud communication is secure, including mutual authentication.

Trademarks

- The product names of Microsoft Azure or other Microsoft products are trademarks of Microsoft Corporation in the U.S. and other countries.
- The product names of Amazon Web Services or other Amazon products are trademarks of Amazon.com, Inc. or its affiliates in the U.S. and other countries.
- The product names of PostgreSQL or other related products are trademarks of the PostgreSQL Community Association of Canada (PGCAC) in the U.S. and other countries.

Appendix

ISO Comparative Table

Chapter of ISO/IEC27017		Section of this document
Number	**Title**	
5	Group of policies for Information Security	Please refer to the following for the Ricoh Group's security.https://www.ricoh.com/security/products
6	Organization for Information Security	
7	Human Resource Security	
8	Asset Management	"Data Protection"
9	Access Control	"Cloud Service Provider's Access Control to Data"
10	Encryption	"Data Protection"
11	Physical and Environmental Security	"Physical and Environmental Security"
12	Operations Security	"Operations Security"
13	Communication Security	"Communication Security"
14	System Acquisition, development and maintenance	"Development Security"
15	Supplier Relationships	"Supplier Relationships"
16	Information Security Incident Management	"Information Security Incident Management"
17	Information Security Aspects of Business Continuity Management	"Availability"
18	Compliance	"Compliance"

Data Flow (DM)

Web UI

Client	Server	Functions	Request Data	Response Data	Protocol	Port
PC	CloudStream DM	Web UI	UI request File upload	UI response File download	HTTPS	443
Mobile	CloudStream DM	Web UI	UI request	UI response	HTTPS	443

			File upload	File download		

DM Agent Deployment Tool/DM Agent

Client	Server	Functions	Request Data	Response Data	Protocol	Port
DM Agent Deployment Tool	CloudStream DM	Get service URLs	-	Service URLs	HTTPS	443
DM Agent Deployment Tool	CloudStream DM	Generate client certificate	Onboarding code	Client certificate	HTTPS	443
DM Agent Deployment Tool	Printer	Install DM Agent	DM Agent application file	-	HTTPS	80(*)/443/51443
DM Agent Deployment Tool	Proxy server with basic authentication (optional)	Mediate communication to CloudStream DM	Same as each communication from DM Agent to CloudStream DM	Same as each communication from DM Agent to CloudStream DM	HTTP/HTTPS	Any port
DM Agent Deployment Tool	Printer	Get firmware information	-	Firmware information	FTP	21 (Control) / Any port (Data)
DM Agent Deployment Tool	Printer	Update firmware	Firmware	-	FTP	21(Control) / 20 (Data)
DM Agent	CloudStream DM	Get service URLs	-	Service URLs	HTTPS	443
DM Agent	CloudStream DM	Renew client certificate	Client certificate (current)	Client certificate (new)	HTTPS	443
DM Agent	CloudStream DM	Get polling configuration	-	Polling configuration	HTTPS	443
DM Agent	CloudStream DM	Get device management task	-	Device configuration Firmware Application	HTTPS	443
DM Agent	CloudStream DM	Post device management result	Device information Device configuration	-	HTTPS	443
DM Agent	Proxy server with basic authenticati	Mediate communication to	Same as each communica	Same as each communication from DM	HTTP/HTTPS	Any port

	on (optional)	CloudStream DM	tion from DM Agent to CloudStream DM	Agent to CloudStream DM		
DM Agent	Proxy server with Kerberos authentication (optional)	Mediate communication to CloudStream DM	Same as each communication from DM Agent to CloudStream DM	Same as each communication from DM Agent to CloudStream DM	UDP/TCP (Kerberos Authentication protocol)	Any port

(*) Port 80 is used only as a fallback if the installation of the DM Agent via port 443 fails.

WfH Client

Client	Server	Functions	Request Data	Response Data	Protocol	Port
WfH Client	CloudStream DM	Get service URLs	-	Service URLs	HTTPS	443
WfH Client	CloudStream DM	Generate client certificate	Onboarding code	Client certificate	HTTPS	443
WfH Client	CloudStream DM	Renew client certificate	Client certificate (current)	Client certificate (new)	HTTPS	443
WfH Client	CloudStream DM	Get polling configuration	-	Polling configuration	HTTPS	443
WfH Client	CloudStream DM	Post device information	Device information	-	HTTPS	443
WfH Client	Printer	Monitor device	-	Device information	SNMP/USB	161
WfH Client	CloudStream DM	Is WfH Device	device manufacturer, model, and serial number	True/False	HTTPS	443
WfH Client	CloudStream DM	Upload Logs	Trace logs of the service	-	HTTPS	443
WfH Client	CloudStream DM	Get Notifications	List of previously handled notifications	Notification information	HTTPS	443
WfH Client	Proxy server (optional)	Mediate communication to CloudStream DM	Same as each communication from WfH Client to CloudStream DM	Same as each communication from WfH Client to CloudStream DM	HTTP/HTTPS	Any port

Auth Agent

Client	Server	Functions	Request Data	Response Data	Protocol	Port
Auth Agent	CloudStream DM	Get service URLs	-	Service URLs	HTTPS	443
Auth Agent	CloudStream DM	Generate client certificate	Onboarding code	Client certificate	HTTPS	443
Auth Agent	CloudStream DM	Renew client certificate	Client certificate (current)	Client certificate (new)	HTTPS	443
Auth Agent	CloudStream DM	Get authentication request	-	User information	HTTPS	443
Auth Agent	CloudStream DM	Get authentication profiles	-	Authentication profile	HTTPS	443
Auth Agent	CloudStream DM	Post authentication result	-	User information	HTTPS	443
Auth Agent	Proxy server (optional)	Mediate communication to CloudStream DM	Same as each communication from Auth Agent to CloudStream DM	Same as each communication from Auth Agent to CloudStream DM	HTTP/HTTPS	Any port
Auth Agent	LDAP Server	Authenticate user	User information	User information	LDAP/LDAPS	Any port

Device Monitoring Service

Client	Server	Functions	Request Data	Response Data	Protocol	Port
Device Monitoring	CloudStream DM	Get service URLs	-	Service URLs	HTTPS	443
Device Monitoring	CloudStream DM	Generate client certificate	Onboarding code	Client certificate	HTTPS	443
Device Monitoring	CloudStream DM	Renew client certificate	Client certificate (current)	Client certificate (new)	HTTPS	443
Device Monitoring	CloudStream DM	Get polling configuration	-	Polling configuration	HTTPS	443
Device Monitoring	CloudStream DM	Post device information	Device information	-	HTTPS	443

Device Monitoring	Printer	Monitor device	-	Device information	SNMP (*)/USB	161
Device Monitoring	CloudStream DM	Is Device Monitoring Service Device	device manufacturer, model, and serial number	True/False	HTTPS	443
Device Monitoring	CloudStream DM	Upload Logs	Trace logs of the service	-	HTTPS	443
Device Monitoring	CloudStream DM	Get Notifications	List of previously handled notifications	Notification information	HTTPS	443
Device Monitoring	Proxy server (optional)	Mediate communication to CloudStream DM	Same as each communication from Device Monitoring to CloudStream DM	Same as each communication from Device Monitoring to CloudStream DM	HTTP/HTTPS	Any port
Device Monitoring	SQL Server	Monitored device		-	TCP	Any port (Default is 1433)

(*) SNMP v1/v2 and v3 are supported.

External Systems

Client	Server	Functions	Request Data	Response Data	Protocol	Port
CloudStream DM	OIDC ID Provider	Authenticate user	Authentication request	Authentication result	HTTPS	443
CloudStream DM	Custom SMTP Server	Email notification	SMTP credentials Email message Report file	-	SMTP/SMTPS	Any port
CloudStream DM	Amazon SES	Email notification	SMTP credentials Email message Report file	-	SMTPS	587
CloudStream DM	SIEM Service	SIEM integration	Transaction data	-	HTTPS	Any port

RICOH @Remote Center

Client	Server	Functions	Request Data	Response Data	Protocol	Port
CloudStream DM	@Remote Center	Post device information	Device information	-	HTTPS	443

Software Server

Client	Server	Functions	Request Data	Response Data	Protocol	Port
CloudStream DM	Software Server	Get device firmware files	-	Firmware files	HTTPS	443

CloudStream DM Monitoring

Client	Server	Functions	Request Data	Response Data	Protocol	Port
CloudStream DM	CloudStream DM Monitoring	Send service health metrics	Service health metrics	-	HTTPS	443
CloudStream DM Monitoring	CloudStream DM	Check service health status	-	Service health status	HTTPS	443

Data Flow (PrintScan)

Note: The information of data flow for PrintScan refers "Ports and Protocols"(https://manual.na.ps.cloudstream.ricoh.com/docs/requirements#Requirements-portsprotocolsPortsandProtocols). In case of any inconsistency, excess or deficiency, the "Ports and Protocols" shall take precedence.

Devices Connected to CloudStream Using HTTPS Default Port 443

Only Cloud Hosted

Web Administration UI

Client	Server	Description	Protocol	Port
Client Web browser	CloudStream PrintScan	HTTPS/SSL Web interface used for direct access or during SSO from DM.	TCP HTTPS	443

PC Client to CloudStream PrintScan

Client	Server	Description	Protocol	Port
PC Client Client IPP	CloudStream PrintScan	Authenticate users, retrieve printers, messaging exchange, send print jobs, and register as trusted endpoints. Replaces ports 2560, 7300, 7400, and 9631 on environments with standard port 443 support.	TCP HTTPS	443

Printer to CloudStream PrintScan

Client	Server	Description	Protocol	Port

Printer	CloudStream PrintScan	Connection from Cloud terminals running on MFP (e.g. HP Workpath Gen 2, KM IWS Gen 2, Ricoh Gen 2) and for sending scanned jobs (e.g. HP Workpath Gen 2, Ricoh Gen 2, KM IWS Gen 2). Replaces ports 7400, 8705, 8707, and 8711 on environments with standard port 443 support.	TCP HTTPS	443

CloudStream Chrome Extension to Gateway Server

Client	Server	Description	Protocol	Port
Chrome Extension	Gateway Server (API Service)	Chrome Extension communicate with API to authenticate users, retrieve printers and send jobs to CloudStream	TCP HTTPS	7300

Terminal Deployment Tool to Printer

Client	Server	Description	Protocol	Port
Terminal Deployment Tool	Printer	Connection for installing terminal over HTTPS	TCP HTTPS	443
Terminal Deployment Tool	Printer (Ricoh only)	Connection for installing terminal over HTTP	TCP HTTP	80
Terminal Deployment Tool	Printer (FUJIFILM BI only)	Connection for pushing configuration to FUJIFILM BI devices	TCP HTTPS	58070

PC Client to Printer (For PC Client in 'Local Storage' mode)

Client	Server	Description	Protocol	Port
PC Client Document Output Service	Printer	CloudStream document output service delivering print jobs to a physical printer	TCP	9100
PC Client Document Output Service	Printer	CloudStream document output service delivering print jobs to a physical printer via IPP/S	TCP HTTP	631
PC Client Document Output Service	Printer	CloudStream document output service delivering print jobs to a physical printer via IPP/S	TCP HTTPS	443

Legacy Mobile Print to Gateway Server

Client	Server	Description	Protocol	Port
Apple iOS clients	Gateway Server (Mobile Print Service)	AirPrint print jobs from Apple iOS devices (secure)	TCP HTTPS	7910

Ricoh Mobile App	Gateway Server (Mobile Print Service)	Authentication and document data from Apps (secure)	TCP HTTPS	9444

Mobile apps

Client	Server	Description	Protocol	Port
Ricoh Android / iOS Mobile App	Gateway Server (API Service)	Authentication and document data from Apps (secure)	TCP HTTPS	443
Ricoh Android / iOS Mobile App	Gateway Server (API Service)	Authentication and document data from Apps (secure) for cases when a connection to port 443 can't be established	TCP HTTPS	9444
Ricoh Android / iOS Mobile App	Gateway Server (Authentication Service)	OAuth authentication from Apps (secure) for cases when a connection to port 443 can't be established	TCP HTTPS	7400

With On-Premises Gateway

Gateway Server to CloudStream PrintScan

Client	Server	Description	Protocol	Port
Gateway Server	CloudStream PrintScan	Gateway Server communicating with CloudStream PrintScan for messaging exchange and server API. Replaces ports 2560 and 7300 on environments with standard port 443 support.	TCP HTTPS	443

Gateway Server to Printer – print operations

Client	Server	Description	Protocol	Port
Gateway Server (Document Output Service)	Printer	CloudStream document output service delivering print jobs to a physical printer	TCP	9100
Gateway Server (Document Output Service)	Printer	CloudStream document output service delivering print jobs to a physical printer via IPP/S	TCP HTTPS	631
Gateway Server (Document Output Service)	Printer	CloudStream document output service delivering print jobs to a physical printer via IPP/S	TCP HTTPS	443

Gateway Server to Printer/MFP – embedded deployment

Client	Server	Description	Protocol	Port
Gateway Server (Terminal Client Service)	Printer	SNMP management	UDP	161
Gateway Server (Terminal Client Service)	Printer	Deployment of the embedded client to the MFP (all brands)	TCP HTTPS	443
Gateway Server (Terminal Client Service)	Ricoh MFP	Deployment of the embedded client to Ricoh MFP	TCP HTTP	80
Gateway Server (Terminal Client Service)	Ricoh MFP	Deployment of the embedded client to Ricoh MFP	TCP HTTP	8080
Gateway Server (Terminal Client Service)	Canon MFP	Deployment of the embedded client to Canon MFP	TCP HTTP	8451
Gateway Server (Terminal Client Service)	Ricoh MFP	Deployment of the embedded client to Ricoh MFP	TCP HTTPS	51443
Gateway Server (Terminal Client Service)	Ricoh, Lexmark MFP	Deployment of the embedded client to Ricoh and Lexmark MFP	UDP	8710
Gateway Server (Terminal Client Service)	HP MFP	Deployment of the embedded client to HP MFP	TCP HTTP	80
Gateway Server (Terminal Client Service)	HP MFP	Deployment of the embedded client to HP MFP	TCP HTTP	7627
Gateway Server (Terminal Client Service)	Sharp MFP	Sharp OSA communication, only for Sharp devices with embedded client	TCP	10080
Gateway Server (Terminal Client Service)	KM MFP	Konica Minolta OpenAPI communication, only for KM devices with embedded client	TCP	50003

KM IWS Install Tool	KM MFP	default port for installing IWS from the IWS Install Tool	TCP	8091

Printer/MFP to Gateway Server

Client	Server	Description	Protocol	Port
Printer	Gateway Server (Terminal Client Service)	Connection from the embedded clients running on the Ricoh and Lexmark MFP	SSL	8700
Printer	Gateway Server (Terminal Client Service)	Connection from the embedded clients running on the MFDs (except Ricoh and Lexmark)	SSL	8703
Printer	Gateway Server (Terminal Client Service)	Connection from the embedded clients running on the MFDs (except Ricoh and Lexmark)	TCP	8704
Printer	Gateway Server (Terminal Client Service)	Connection from the embedded clients running on the HP and Konica Minolta MFP	TCP HTTPS	7301
Printer	Gateway Server (Terminal Client Service)	Connection from the embedded clients running on the MFP	TCP HTTP	7302
Printer	Gateway Server (Authentication Service)	Connection from the embedded clients to Authentication Service to register as trusted endpoints	TCP HTTPS	7400
Printer	Gateway Server (Terminal Client Service)	Connection from Equitrac server for embedded clients running on the MFP	TCP HTTPS	14080
Printer	Gateway Server (Terminal Client Service)	Connection from Equitrac server for embedded clients running on the MFP	TCP HTTP	14081
Printer	Gateway Server (Terminal Client Service)	Connection from the Ricoh SLNX Share embedded clients running on the MFP	TCP HTTPS	14082
Printer	Gateway Server (Terminal Client Service)	Connection from the Ricoh SLNX Share embedded clients running on the MFP	TCP HTTP	14083

Printer to Gateway Server

Client	Server	Description	Protocol	Port

Printer	Gateway Server (Terminal Client Service)	Connection from the embedded clients, HP Workpath Application and KM IWS, running on the MFP	TCP HTTPS	7301
Printer	Gateway Server (Authentication Service)	Connection from the embedded clients to CloudStream Authentication Service to register as trusted endpoints	TCP HTTPS	7400
Printer	Gateway Server (Mobile Print Service)	Connection from the embedded clients, HP Workpath Gen 1 Application and KM IWS Gen 1, running on the MFP	TCP HTTPS	9444

Gateway Server to Cloud Services

Client	Server	Description	Protocol	Port
Gateway Server	mcr.microsoft.com	Microsoft Container Registry	SSL	443
Gateway Server	*.data.mcr.microsoft.com	Data endpoint providing content delivery	SSL	443
Gateway Server	*.cdn.azcr.io	Deploy modules from the Marketplace to devices	SSL	443
Gateway Server	global.azure-devices-provisioning.net	Device Provisioning Service access	SSL	443
Gateway Server	*.azurecr.io	Personal and third-party container registries	SSL	443
Gateway Server	*.blob.core.windows.net	Download Azure Container Registry image deltas from blob storage	SSL	443
Gateway Server	*.azure-devices.net	IoT Hub access	AMQP MQTT AMQP over WS	5671 8883 443
Gateway Server	*.docker.io	Docker Hub access	SSL	443
Gateway Server	*.ricoh-pmc.com	Platform	SSL	443
Gateway Server	CloudStream PrintScan	Gateway Server communicating with CloudStream PrintScan for messaging exchange	TCP	443
Gateway Server	CloudStream PrintScan	Gateway Server communicating with CloudStream PrintScan server API	TCP HTTPS	443
Gateway Server	*.google.com	NTP server (time{1-12}.google.com) or any chosen NTP server	UDP NTP	443

Mobile device to Gateway Server

Client	Server	Description	Protocol	Port
Mobile device	Gateway Mobile Print Service	Needed for AirPrint via DNS-SD (makes only sense for Gateway Server)	UDP TCP	53
Mobile device	Gateway Mobile Print Service	Needed for AirPrint via DNS-SD (makes only sense for Gateway Server)	UDP TCP	8053

IP Card Reader to Gateway Server

Client	Server	Description	Protocol	Port
IP card reader	Gateway Server (API Service)	IP card reader communicate with API to authenticate users	TCP HTTPS	7300
IP card reader	Gateway Server (API Service)	IP card reader communicate with API to authenticate users	TCP HTTP	7303

Devices Connected to CloudStream Using Legacy Ports

Gateway Server to CloudStream PrintScan

Client	Sever	Description	Protocol	Port
Gateway Server	CloudStream PrintScan	Gateway Server communicating with CloudStream PrintScan for messaging exchange	TCP	2560
Gateway Server	CloudStream PrintScan	Gateway Server communicating with CloudStream PrintScan API	TCP HTTPS	7300

Web Administration UI

Client	Server	Description	Protocol	Port
Client Web browser	CloudStream PrintScan	HTTPS/SSL Web interface of the PMC solution	TCP HTTPS	8443

PC Client to Gateway Server

Client	Server	Description	Protocol	Port
PC Client	CloudStream PrintScan	PC Client in 'Local Storage' mode communicating with the CloudStream PrintScan for messaging exchange	TCP	2560
PC Client	Gateway Server (API Service)	PC Client communicate with API to authenticate users and retrieve printers	TCP HTTPS	7300

PC Client	Gateway Server (API Service)	Clients sending standard print jobs to server	TCP HTTPS	7300
PC Client	Gateway Server (Authentication Service)	PC Client communicate with Gateway Server (Authentication Service) to register as trusted endpoints	TCP HTTPS	7400
Client IPP	Gateway Server (IPP Service)	Clients sending IPP/http print jobs to server	TCP HTTP	8631
Client IPP	Gateway Server (IPP Service)	Clients sending IPPS/https print jobs to server	TCP HTTPS	9631

Printer to Gateway Server

Client	Server	Description	Protocol	Port
Printer	Gateway Server (Authentication Service)	Cloud terminal integration – communicate with Authentication Service to register as trusted endpoints	TCP HTTPS	7400
Printer	Gateway Server (Terminal Client Service)	Cloud terminal integration (SQTS) – connection from Cloud Terminals running on MFP (e.g. HP Workpath Gen2, KM IWS Gen 2, Ricoh Gen 2) and for sending scanned jobs (e.g., HP Workpath Gen 2, Ricoh Gen 2)	HTTPS	8705
Printer	Gateway Server (Terminal Client Service)	Cloud terminal integration – connection from Cloud terminals running on MFP	TCP	8706
Printer	Gateway Server (Terminal Client Service)	Cloud terminal integration – connection from Cloud terminals running on MFP which provide scan data using SwA protocol (mainly Fujifilm BI terminals)	TCP HTTPS	8707
Printer	Gateway Server (Terminal Client Service)	Cloud terminal integration – connection from Cloud terminals running on MFP which provide scan data using WebDAV protocol (KM IWS cloud terminals)	TCP HTTPS	8711

Gateway Server to Cloud Services

Client	Server	Description	Protocol	Port
Gateway Server	CloudStream PrintScan	Gateway Server communicating with CloudStream PrintScan for messaging exchange	TCP	2560
Gateway Server	CloudStream PrintScan	Gateway Server communicating with CloudStream PrintScan server API	TCP HTTPS	7300

Communication from the customer environment to CloudStream

DM

Function	Destination Host	Port	Protocol
Access from PC or device to CloudStream	*.na.cloudstream.ricoh.com *.eu.cloudstream.ricoh.com*.ap.cloudstream.ricoh.com *.ca.cloudstream.ricoh.com The "*" part depends on the using country and tenant.	443/TCP	HTTPS
Help Page	manual.na.cloudstream.ricoh.com	443/TCP	HTTPS

PrintScan

Function	Destination Host	Port	Protocol
Access from PC or device to CloudStream	*.na.ps.cloudstream.ricoh.com *.eu.ps.cloudstream.ricoh.com *.uk.ps.cloudstream.ricoh.com *.ie.ps.cloudstream.ricoh.com *.de.ps.cloudstream.ricoh.com *.ap.ps.cloudstream.ricoh.com *.ca.ps.cloudstream.ricoh.com The "*" part depends on the using country and tenant.	443/TCP (*1)	HTTPS
Help Page	manual.na.ps.cloudstream.ricoh.com	443/TCP	HTTPS

(*1) If you use legacy ports to communicate with CloudStream PrintScan, alternative ports will be utilized. For more information, please refer to the 'Devices Connected to CloudStream Using Legacy Ports' section.