EPSON
EXCEED YOUR VISION

Epson Cloud Solution PORT

Security Guideline

Contents

Security Initiatives

Security Policy

In line with the "Corporate Principles" based on the "Management Philosophy", Epson has defined the basic approach on information security and the matters to be observed in "Basic Policy on Information Security". Epson shall continue to be a company trusted by society, our customers, and our business partners by creating a governance and corporate culture that can be put into practice and each and every member of the group recognizes the importance of information security.

1. Epson recognizes all information (*) used in the corporate activities as an important management resource, and positions the information security initiatives as one of the important management activities.
   (*) Includes confidential business information such as customers' personal information, sales, products, technology, production, and know-how. Also includes information systems that store and utilize the aforementioned information.
2. Epson has stipulated a global information security policy to clarify the responsibility structure and promotion framework for information security and build a management system that can properly protect and manage information assets.
3. Epson is committed to earning the trust of customers and stakeholders and is striving to ensure business continuity by accurately grasping and managing the risks of information security related to corporate activities.
4. Epson will continue to educate and conduct awareness-raising activities for all our employees including executive-level employees, to establish information security for all group members.
5. Epson has established a compliance program to comply with information security laws, contracts, and other related laws and regulations, and shall strive to do so thoroughly.
6. As a management responsibility, Epson evaluates the information security management system and strives to improve it continuously.

Security Initiatives

For allowing our customers to use our products and services safely and securely, Epson has put the following security initiatives in place.

1. Epson considers the security of products and services to be the basis of quality.
   • We are creating products and services that take security into consideration during the product life cycle (from planning to end of customer use).
2. We are pro-actively providing security information to our customers and creating awareness about it.
3. Epson will continue to respond to vulnerabilities.
   • Epson carries out vulnerability tests by using industry standard tools and strives to provide products and services that are not vulnerable.
   • If an unknown or unfamiliar vulnerability is found, Epson will promptly analyze it and provide information and countermeasures for the same.

Data Center

At Epson, we use service providers that meet global security standards and criteria. Epson Cloud Solution PORT uses Amazon Web Services (Amazon Web Services; hereinafter referred to as "AWS").

Protection of Customer Data

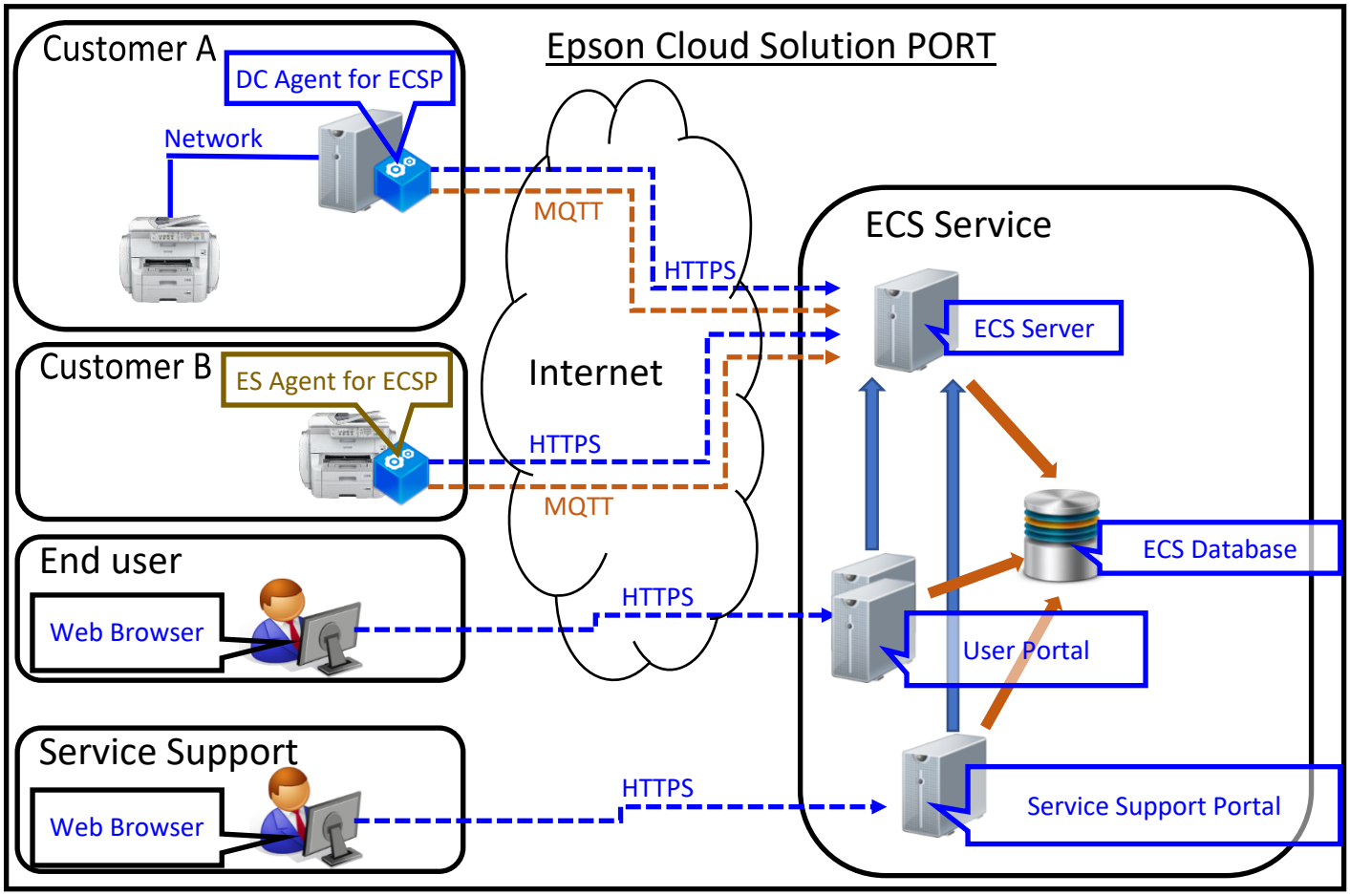
Epson is taking the following initiatives to ensure the security of the information received from our customers.

1. Communication between the device/PC and the server is encrypted. We protect our customers' data from wiretapping or tampering by a third party.
2. Epson utilizes customer data in the following combinations. Such use protects the customer data from an unauthorized access.
   • Handling of data by using a private cloud environment (Virtual Private Cloud)
3. We constantly monitor our servers for an unauthorized access. If found, we immediately respond to threats.
4. The privacy statement defines the policy on protection of personal information.
   This policy clarifies "Collected Information", "Purpose and Scope of Use", "Method of Managing Information", etc. and personal information collected will not be provided to a third party without the consent of the customer.
5. Access to your data is limited to those with special access right and all access to your data is recorded. This access right is periodically inventoried and maintained in an appropriate state.

Epson Cloud Solution PORT

Overview and Terminology

Epson Cloud Solution Port (hereinafter referred to as "ECS") manages Epson-made devices and provides various services. ECS is constituted by Epson DC Agent for Epson Cloud Solution Port (hereinafter referred to as "DC Agent for ECSP"), Epson ES Agent for Epson Cloud Solution Port (hereinafter referred to as "ES Agent for ECSP"), ECS Server, Website (User Portal, Service Support), and ECS Database. See the following for more details. Furthermore, this document provides information related to security of ECS.



DC Agent for ECSP is a Windows client application that collects device data from the specified network-connected devices and transmits the same to the ECS Server.

ES Agent for ECSP is a device firmware. It collects data of its own device and transmits the same to the ECS Server.

The ECS Server receives the data transmitted by the DC Agent for ECSP and the ES Agent for ECSP and stores the data in the ECS Database. User Portal and Service Support Portal are Web sites provided by the "Epson Cloud Solution PORT member service" and "Epson Remote Monitoring System" that allow authorized users to log in. The User Portal allows the user to view the data stored in the ECS Database. Moreover, the Service Support Portal allows the users to perform remote operation of the device by using the ECS Server. The user information is stored in the ECS Database.

Data Collection

Network Protocol

The DC Agent for ECSP collects device data by using the following network protocols and ports.

See Appendix for all network protocols and ports used by the DC Agent for ECSP.

DC Agent for ECSP

Protocol	Port	IN/OUT	Explanation
SNMP(UDP)	161	OUT	Collects data from the network-connected devices.
ENPC(UDP)	3289	OUT	Epson's proprietary printer control protocol.

*Ports used by the printer drivers are not mentioned.

Collected and Transmitted Data

The DC Agent for ECSP and the ES Agent for ECSP collect device data such as product name, serial number, status information, ink level, and job history, and transmits it to the ECS Server.

See "Appendix" for details on the device data transmitted by the DC Agent for ECSP and the ES Agent for ECSP.

Security

The DC Agent for ECSP collects device data from the specified devices. The target devices are identified based on a device list managed by the DC Agent for ECSP. No data is collected from an unspecified device and PC. The ES Agent for ECSP or the DC Agent for ECSP do not collect printing data.

Data Transmission

Network Protocol

The DC Agent for ECSP and the ES Agent for ECSP transmit the device data to the ECS Server by using the following network protocols and ports.

See the Appendix for the network protocols and ports used by the DC Agent for ECSP and the ES Agent for ECSP.

DC Agent for ECSP

Protocol	Port	IN/OUT	Explanation
HTTPS(TCP)	443	OUT	Transmits device data to the ECS Server

*Ports used by the printer drivers are not mentioned.

ES Agent for ECSP

Protocol	Port	IN/OUT	Explanation
HTTPS(TCP)	443	OUT	Transmits device data to the ECS Server

Data Format

The DC Agent for ECSP and the ES Agent for ECSP transmits the device data in JSON format, an industry standard data-exchange format.

Security

Data transmission via the Internet between the client (DC Agent for ECSP or ES Agent for ECSP) and the server (ECS Server) is protected by HTTPS connection.

See "SSL Section" in "Appendix" for more information on HTTPS.

Remote Operation

Network Protocol

The DC Agent for ECSP and the ES Agent for ECSP perform remote operations by using the following network protocols and ports.

See the Appendix for the list of network protocols and ports used by the DC Agent for ECSP and the ES Agent for ECSP.

DC Agent for ECSP /ES Agent for ECSP

Protocol	Port	IN/OUT	Explanation
HTTPS(TCP)	443	OUT	Downloads SSL Certificate of the ECS Server.
MQTT over SSL (TCP)	443	OUT	Receives remote operation command of the ECS Server.

*Ports used by the printer drivers are not mentioned.

Types of Remote Operation

The Service Support in-charge can perform the following remote operations:

- Acquisition of device status information and cumulative operation information
- Head cleaning
- Diagnostics (only for printers equipped with Diagnostics Function)

Target Devices

Remote operation of only the specific devices can be performed. Remote operation cannot be performed for devices that are not specified.

Security

The Support Service users having an ECS Service account can send remote operation command to the specified devices. Other users cannot perform any type of remote operation. A user can perform remote operations for the devices they are managing. A user cannot perform remote operation on or access other devices.

The flow of the remote operation is as follows:

(1) The Support Service in-charge selects the device and the type of remote operation via the ECS Service.
(2) The ECS Service sends a request to the ECS Server via a secured internal network of the data center.
(3) The ECS Server uses MQTT over SSL to send the remote operation command to the DC Agent for ECSP or the ES Agent for ECSP.

Data communication between the DC Agent for ECSP or the ES Agent for ECSP and the ECS Server via Internet is secure because it is encrypted by using HTTPS or MQTT over SSL.
See "SSL Section" in "Appendix" for more information on HTTPS and MQTT over SSL.

User Management

Network Protocol

The web browser accesses the ECS Service by using the following network protocols and ports.

Web Browser

Protocol	Port	IN/OUT	Explanation
HTTPS(TCP)	443	OUT	Accesses web services of the ECS Service.

User Information

Information of the users having access rights to the ECS Service is encrypted and saved securely in the database.

Security

The registered users can log on to the ECS Server. The logged-in user can view information on all devices for which they have access rights. The user cannot view the information of the devices for which they do not have access rights.
Moreover, the Support Service in-charge can perform remote operation of devices that they manage. Remote operation cannot be performed for devices for which the in-charge does not have access rights.

Data communication between the client (web browser) and the server (ECS Server) via Internet is secure because it is encrypted by using HTTPS. See the section on "SSL" in "Appendix" for more information on HTTPS.

Data Storage

Security

The ECS Server receives the data transmitted by DC Agent for ECSP and ES Agent for ECSP. The ECS Service receives user information such as user name and password, partner information, and client information. All the data is saved safely and securely in the database in AWS, based on the Epson's Privacy Policy and Security Policy.

Appendix

Transmitted Data

The device data transmitted from the DC Agent for ECSP or the ES Agent for ECSP to the ECS Server via HTTPS includes the following.

The type of device data collected on or transmitted to the ECS Server is differentiated by model, accessory, configuration, eject type, and usage status.

Category	**Data**
Agent	Agent ID
	Agent type
	Agent version
	Collection type
	Sent date
	OS
	OS Version
	OS product type
Device	Manufacturer name
	Model name
	Serial number
	Region code
	Country code
	Time
	Acquired date
	Firmware version

Category	**Data**
Device	Printer Status
	Error/warning code
	Status/Error/Warning history
	Operation panel setting
	Printer setting
	Maintenance setting
	Media setting
	Network setting
	Consumable parts information
	Cleaning history
	Maintenance history
	Cumulative ink usage
	Cumulative printing time
	Cumulative printing area
	Job history

Network Protocol and Ports Used

The network protocols and ports used by the DC Agent for ECSP and the ES Agent for ECSP are as follows:

ES Agent for ECSP

Protocol	Port	IN/OUT	Explanation
HTTPS(TCP)	443	OUT	Transmits device data to the ECS Server. Downloads SSL Certificate of the ECS Server.
MQTT over SSL (TCP)	443	OUT	Wait for remote operation command from the ECS Server.

DC Agent for ECSP

Protocol	Port	IN/OUT	Explanation
SNMP(UDP)	161	OUT	Collects data from the network-connected devices. Downloads SSL Certificate of the ECS Server.
HTTPS(TCP)	443	OUT	Transmits device data to the ECS Server.
MQTT over SSL (TCP)	443	OUT	Wait for remote operation command from the ECS Server.
ENPC(UDP)	3289	OUT	Epson's proprietary printer control protocol.

SSL

Only HTTPS or MQTT over SSL protocol is used for all the ECS data transmission via Internet. "S" at the end of HTTPS is an abbreviation for "Secure". HTTPS is often used to protect the confidential information entered during transactions such as online banking and online shopping. MQTT over SSL and HTTPS use SSL (Secure Socket Layer). SSL is a standard security technology for establishing an encrypted link between a server and a client. In the ECS model, the DC Agent for ECSP, the ES Agent for ECSP, or a web browser is a client, and the ECS Server or the ECS Service is a server.
All data transmissions by using HTTPS or MQTT over SSL are securely protected and guaranteed to be transmitted to the appropriate destination.

Trademark

- EPSON and EXCEED YOUR VISION are registered trademarks of Seiko Epson Corporation.
- Microsoft and Windows are registered trademarks of Microsoft Corporation in United States of America and other countries.
- Other product names are trademarks or registered trademarks of their respective holders.

© Seiko Epson Corporation 2020