EPSON
EXCEED YOUR VISION

Epson Projector Management Connected

Security White Paper

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. This service system 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.

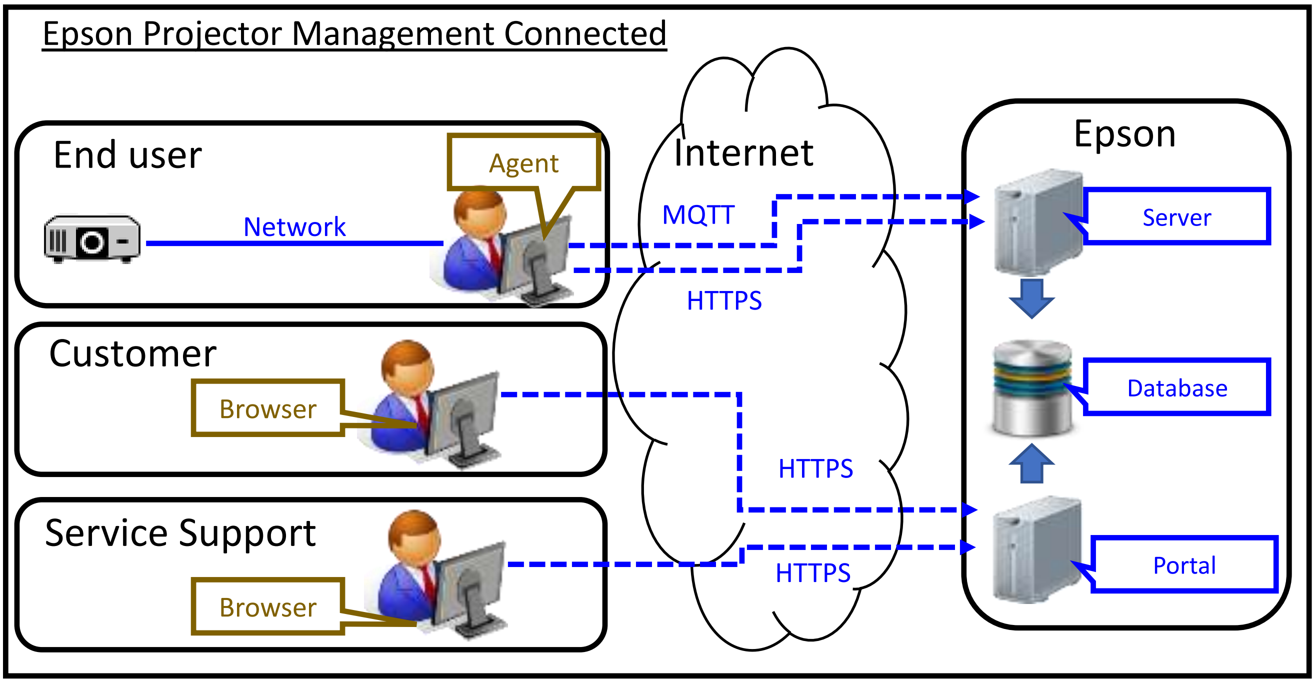
4. The privacy statement defines the policy on protection of personal information. This policy clarifies "Collected Information", "Purpose and Scope of Use", "Method of Managing Information", etc. and personal information collected will not be provided to a third party without the consent of the customer.

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 Projector Management Connected

Overview and terminology

Epson Projector Management Connected (hereinafter referred to as EPMC) helps you to manage Epson projector and provide a wide variety of services to your customers. This system consists of the EPMC Agent (hereinafter referred to as Agent), EPMC Server (hereinafter referred to as Server), Website (Portal), and EPMC Database (hereinafter referred to as Database). See the chart below for an overview. Furthermore, this document provides information related to security of EPMC.



The Agent is a Windows client application that collects projectors and peripherals data from the specified network connected devices and transmits the same to the Server.

The Server receives the data sent by the Agent and stores the data in the Database.

The Portal is the Web site provided by EPMC that allows authorized users to log in. It allows the user to view the data stored in the Database. Moreover, it allows the users to perform remote operation of the device by using the Server.

Data Collection

Network protocols

The following shows the network protocols and ports used by the Agent to collect device data.

Protocol	Port	IN/OUT	Description
TCP	3629	OUT	Collects device data from a network connected device.
HTTP	80	OUT	Collects device data from a network connected device.

See the Appendix for the complete list of network protocols and ports used by Agent.

Data collected

The Agent collects and transmits device data, such as the device status, serial number, usage, and error history. The Agent does not collect user’s data, such as the projected images or images from the embedded camera. See the Appendix for further information about the device data collected and transmitted by the Agent.

The Agent only uses the internet to collect device data from specified devices. You can check the target devices on the Agent screen. It does not collect any data from non-specified devices.

Data Transmission

Network protocols

The following shows the network protocols and ports used by the Agent to send device data to the Server.

Protocol	Port	IN/OUT	Description
MQTT	443	OUT	Sends device data to the Server.

See the Appendix for the complete list of network protocols and ports used by the Agent.

Data format

The Agent and Server send device data in the industry standard format, JSON.

Security

Any data transmitted over the Internet between the Agent and the Server is protected by TLS.

Remote Operation

Network protocols

The Agent performs remote operations by using the following network protocols and ports.

Protocol	Port	IN/OUT	Description
HTTPS(TCP)	443	OUT	Downloads SSL certificate of the Server.
MQTT	433	OUT	Waits for device control order from the Server.
TCP	3629	OUT	Controls the target device.

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

Type of Remote Operation

The user can perform the following remote operations:

- Collect device data
- Power On/Off
- A/V Mute On/Off
- Source Change
- Change some settings (Only Service Support)

Security

The Support Service users can send remote operation commands to the devices if specifically permitted by the end user.
A user can perform remote operations for the devices they are managing. A user cannot perform remote operation on or access other devices.

Data communication between the Agent and the Server via the Internet is secure because it is encrypted by using HTTPS or MQTT.
See "Appendix" for more information on HTTPS and MQTT.

Software Update

Network protocols

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

Protocol	Port	IN/OUT	Description
HTTPS(TCP)	443	OUT	Checks if a new version of the Agent is available on the Epson download server. Downloads the new version of the Agent from the Epson download server.

Security

Epson’s download server always provides the latest version of the Agent. The Agent checks if a new version of the Agent. When new version is available, the Agent installer is downloaded by HTTPS. Only once the Agent has confirmed that the file is the correct module provided by Epson, will the Agent run the update.

User Management

Network protocols

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

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

User Information

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

Security

The registered users can log on to the 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 only perform remote operation of devices if specifically permitted by the end user.   Remote operation cannot be performed for devices for which the Support Service in charge does not have access rights.

Data communication between the client (web browser) and the server (Server) via the 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 Server receives the data transmitted by the Agent. The Service receives user information such as username and password, partner information, and client information. All the data is saved safely and securely in the database in AWS, based on Epson's Privacy Policy and Security White Paper.

Appendix

Data transmissions

The following data can be transmitted from the Agent to the Server by MQTT.

The types of device data in the table above that are collected and transmitted to the Server depend on the model, accessories, configuration, agent version, and usage status.

Category	Data item
Agent	Information for the Agent: Agent code, version, identifier, connected device count.
	Settings for the PC installed the Agent: Locale, language.
	Logs relative to the Agent: System event when exceptions occur in Agent.
Device	Information for the device setting in the Agent: Display name, group name, comment.
	Information for the device: Serial number, firmware version, lens type, temperature limit.
	Logs for the device: Initial power-on date, lamp replace date, error/warning count, last light calibration time.
	Status for the device: Power, source, A/V mute, signal, light-up time, total operation time, luminance const remain time, temperature, fan revolution, luminance sensor.
	History for the device: Error, warning, usage, temperature, ac voltage.
	Settings for the device: Projector name, local time, IP address, color mode, schedule, luminance mode, luminance const level, volume.

Network protocols and ports

The following shows the complete list of network protocols and ports used by the Agent.

Protocol	Port	IN/OUT	Description
TCP	3629	OUT	Discovers devices using unicast. Collects device data from the connected devices. Controls the target device. Waits for the status change notification from connected devices.
HTTP	80	OUT	Collects device data from the connected devices.
HTTPS(TCP)	443	OUT	Downloads SSL certificate of the Server. Checks if a new version of the Agent is available on the Epson download server. Downloads the new version of the Agent from the Epson download server.
MQTT	443	OUT	Transmits device data to the Server. Waits for device control order from the Server.

HTTPS

HTTPS is the secure version of HTTP (Hypertext Transfer Protocol). The ‘S’ at the end of HTTPS stands for ‘Secure’. HTTPS is often used for online banking or shopping to establish a reliable link between a client and a server to protect confidential information. All the data transmitted using HTTPS is secure, protected, and guaranteed to be sent to the correct destinations.

MQTT

MQTT is a lightweight protocol suitable for sending and receiving short data frequently with many devices. Therefore, it is used in M2M and IoT. The Agent connects to the server using an X.509 client certificate over a secure TLS connection.

Network traffic

The amount of network traffic for a full data collection is roughly up to 100 KB per device, depending on the model, accessories, configuration, agent version, and usage status. The performance depends on the network environment.

Trademarks

- ❑ EPSON and EXCEED YOUR VISION are registered trademarks of Seiko Epson Corporation.
- ❑ Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.
- ❑ Other product names may be trademarks or registered trademarks of their respective owners.

© Seiko Epson Corporation