

Epson Cloud Solution PORT

安全准则

目录

安全举措.....3

安全政策	3
安全举措	3
数据中心	4
客户数据保护	4

Epson Cloud Solution PORT.....5

概述和术语	5
-------------	---

数据收集.....6

网络协议	6
收集和传输的数据.....	6
安全性	6

数据传输.....7

网络协议	7
数据格式	7
安全性	7

远程操作.....8

网络协议	8
远程操作的类型.....	8
目标设备	8
安全性	9

用户管理.....10

网络协议	10
用户信息	10
安全性	10

数据存储..... 11

安全性	11
-----------	----

附录..... 12

传输的数据	12
使用的网络协议和端口.....	13
SSL	14
商标	14

安全举措

安全政策

根据基于“管理理念”的“公司原则”，爱普生定义了信息安全的基本方法以及“信息安全基本政策”中要注意的事项。通过创建可以付诸实践的管理方法和企业文化，并让集团中的每个成员都认识到信息安全的重要性，爱普生将继续成为社会、客户以及业务合作伙伴所信任的公司。

1. 爱普生将公司活动中使用的所有信息（*）视为重要的管理资源，并将信息安全举措定位为重要的管理活动之一。
（*）包括如客户的个人信息、销售、产品、技术、生产和专有技术等机密商业信息。还包括存储和利用上述信息的信息系统。
2. 爱普生已经制定了一套全面的信息安全政策，用以明确信息安全的责任结构和推行框架，并建立可以妥善保护和管信息资产的管理系统。
3. 爱普生致力于赢得客户和利益相关方的信任，并努力通过准确地把握和管控与公司活动相关的信息安全风险来确保业务连续性。
4. 爱普生将继续为包括高管级别员工在内的所有员工开展教育和意识提升活动，以便为集团所有成员建立信息安全意识。
5. 爱普生制定了符合信息安全法律、合同和其他相关法律法规的合规计划，并将努力贯彻执行该计划。
6. 作为管理责任，爱普生还将评估信息安全管理系统并努力不断对其进行改进。

安全举措

为了使我们的客户安全可靠地使用我们的产品和服务，爱普生已制定了以下安全举措。

1. 爱普生认为产品和服务的安全性是质量的基础。
 - 我们正在创建在产品生命周期（从规划到用户使用结束）中考虑安全性的产品和服务。
2. 我们正在积极地向我们的客户提供安全信息，并提高关于安全信息的意识。
3. 爱普生将继续积极应对漏洞。
 - 爱普生使用行业标准工具进行漏洞测试，并努力提供不易受攻击的产品和服务。
 - 如果发现未知或不熟悉的漏洞，爱普生将立即对其进行分析并提供相应的信息和对策。

数据中心

在爱普生，我们使用符合全球安全标准和条件的服务提供商。Epson Cloud Solution PORT 基于不同区域使用的的网络服务列表如下。

中国以外的区域：亚马逊网络服务（亚马逊网络服务，以下称为“AWS”）。

中国：阿里巴巴云（阿里巴巴云，以下简称“阿里云”）

客户数据保护

爱普生正在采取以下措施，以确保从客户处收到的信息的安全性。

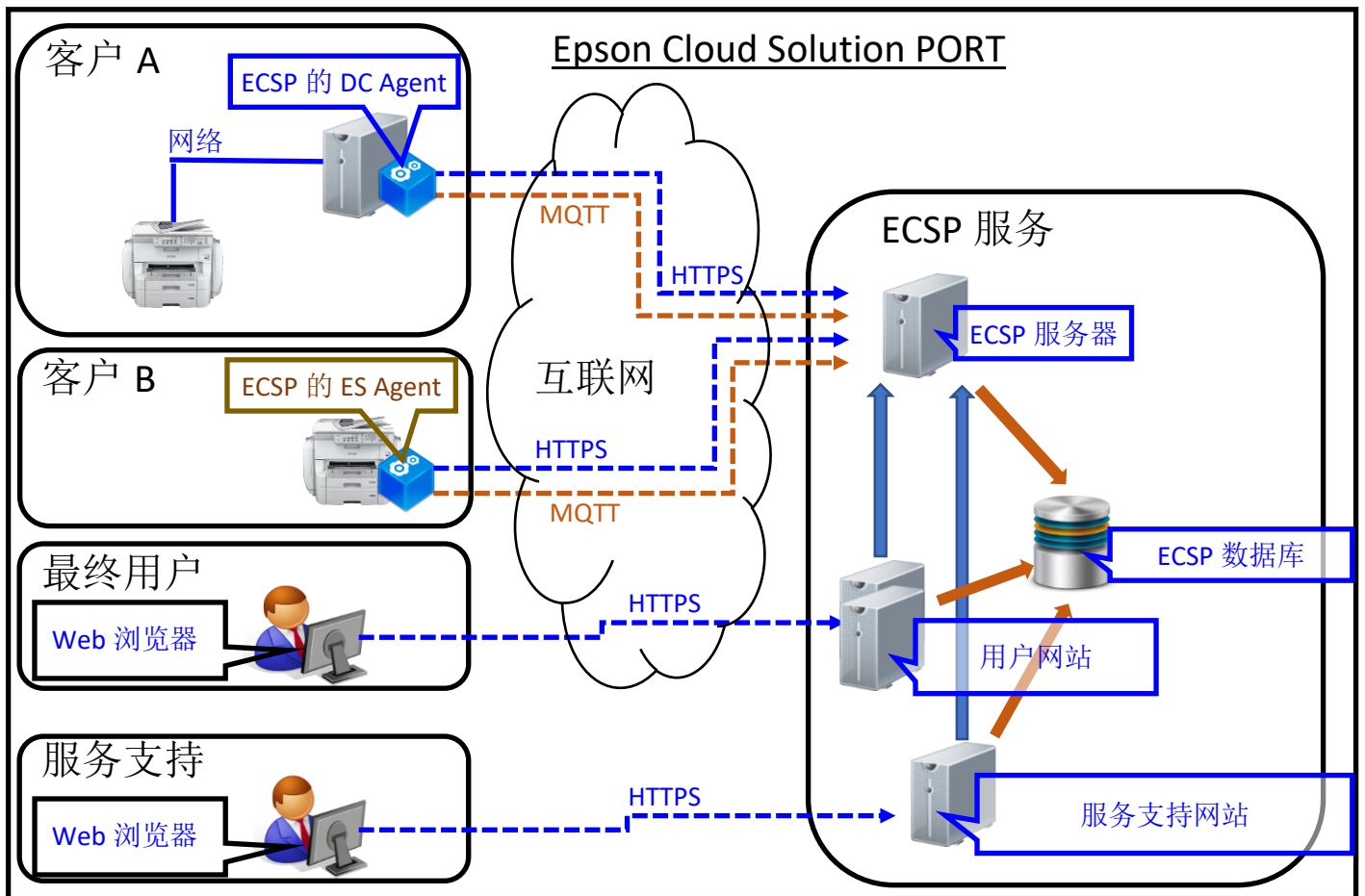
1. 设备/PC 和服务器之间的通信已加密。我们保护客户的数据免遭第三方的窃听或篡改。
2. 爱普生通过以下组合利用客户数据。此类使用可保护客户数据免受未经授权的访问。
 - 使用私有云环境（虚拟私有云）处理数据
3. 我们会持续监控我们的服务器是否存在未经授权的访问。如果发现，我们将立即对威胁作出反应。
4. 隐私声明定义了保护个人信息政策。

该政策阐明了“收集的信息”、“目的和使用范围”、“管理信息的方法”等内容，而且未经客户的同意，不会将收集的个人信息提供给第三方。
5. 只有具有特殊访问权限的用户才能访问您的数据，并且所有对您数据的访问都将被如实记录。该访问权限会定期进行盘点，并保持适当的状态。

Epson Cloud Solution PORT

概述和术语

Epson Cloud Solution PORT（以下称为“ECSP”）管理爱普生制造的设备并提供各种服务。ECSP 由 Epson Cloud Solution PORT 的爱普生 DC Agent（以下称为“ECSP 的 DC Agent”）、Epson Cloud Solution PORT 的爱普生 ES Agent（以下称为“ECSP 的 ES Agent”）、ECSP 服务器、网站（用户协议、服务支持）和 ECSP 数据库组成。有关更多详细信息，请参见以下内容。此外，本文档还提供了与 ECSP 安全性相关的信息。



ECSP 的 DC Agent 是一种 Windows 客户端应用程序，它从指定的网络连接设备收集设备数据，并将相同的数据传输到 ECSP 服务器。

ECSP 的 ES Agent 是一种设备固件。它收集自身设备的数据，并将相同的数据传输到 ECSP 服务器。

ECSP 服务器 接收 ECSP 的 DC Agent 和 ECSP 的 ES Agent 传输的数据，并将数据存储到 ECSP 数据库中。用户网站 和 服务支持网站 是由“Epson Cloud Solution PORT 会员服务”和“爱普生远程监控系统”提供的网站，允许授权用户登录访问。用户网站允许用户查看存储在 ECSP 数据库中的数据。此外，服务支持网站还允许用户使用 ECSP 服务器对设备执行远程操作。用户信息存储在 ECSP 数据库中。

数据收集

网络协议

ECSP 的 DC Agent 使用以下网络协议和端口收集设备数据。

有关 ECSP 的 DC Agent 使用的所有网络协议和端口，请参阅附录。

ECSP 的 DC Agent

协议	端口	输入/输出	描述
SNMP (UDP)	161	输出	从连网设备收集数据。
ENPC (UDP)	3289	输出	爱普生专有的打印机控制协议。

*未提及打印机驱动程序使用的端口。

收集和传输的数据

ECSP 的 DC Agent 和 ECSP 的 ES Agent 收集设备数据（如产品名称、序列号、状态信息、墨量和任务历史），并将其传输到 ECSP 服务器。

有关 ECSP 的 DC Agent 和 ECSP 的 ES Agent 所传输设备数据的详细信息，请参阅“附录”。

安全性

ECSP 的 DC Agent 从指定的设备收集设备数据。目标设备根据 ECSP 的 DC Agent 管理的设备列表进行识别。不会从未指定的设备和 PC 收集数据。ECSP 的 ES Agent 或 ECSP 的 DC Agent 不收集打印数据。

数据传输

网络协议

ECSP 的 DC Agent 和 ECSP 的 ES Agent 通过使用以下网络协议和端口将设备数据传输到 ECSP 服务器。

有关 ECSP 的 DC Agent 和 ECSP 的 ES Agent 所使用的网络协议和端口，请参阅附录。

ECSP 的 DC Agent

协议	端口	输入/输出	描述
HTTPS (TCP)	443	输出	将设备数据传输到 ECSP 服务器

*未提及打印机驱动程序使用的端口。

ECSP 的 ES Agent

协议	端口	输入/输出	描述
HTTPS (TCP)	443	输出	将设备数据传输到 ECSP 服务器

数据格式

ECSP 的 DC Agent 和 ECSP 的 ES Agent 使用 JSON 格式（行业标准的数据交换格式）传输设备数据。

安全性

客户端（ECSP 的 DC Agent 或 ECSP 的 ES Agent）与服务器（ECSP 服务器）之间的互联网数据传输受 HTTPS 连接保护。

有关 HTTPS 的详细信息，请参阅“附录”中的“SSL 部分”。

远程操作

网络协议

ECSP 的 DC Agent 和 ECSP 的 ES Agent 通过使用以下网络协议和端口执行远程操作。

有关 ECSP 的 DC Agent 和 ECSP 的 ES Agent 所使用的网络协议和端口列表，请参阅附录。

ECSP 的 DC Agent/ECSP 的 ES Agent

协议	端口	输入/输出	描述
HTTPS (TCP)	443	输出	下载 ECSP 服务器的 SSL 证书。
MQTT over SSL (TCP)	443	输出	接收 ECSP 服务器的远程操作命令。

*未提及打印机驱动程序使用的端口。

远程操作的类型

服务支持负责人可以执行以下远程操作：

- 获取设备状态信息和累积的操作信息
- 打印头清洗
- 诊断（仅适用于配备诊断功能的打印机）

目标设备

只能执行指定设备的远程操作。无法对未指定的设备执行远程操作。

安全性

具有 ECSP 服务帐户的支持服务用户可以将远程操作命令发送到指定的设备。其他用户不能执行任何类型的远程操作。用户可以对其所管理的设备执行远程操作。用户无法对其他设备执行远程操作或访问其他设备。

远程操作流程如下：

- (1) 支持服务负责人通过 ECSP 服务选择设备和远程操作的类型。
- (2) ECSP 服务通过数据中心的安全内部网络将请求发送到 ECSP 服务器。
- (3) ECSP 服务器使用 MQTT over SSL 将远程操作命令发送到 ECSP 的 DC Agent 或 ECSP 的 ES Agent。

ECSP 的 DC Agent 或 ECSP 的 ES Agent 与 ECSP 服务器之间通过互联网进行的数据通信是安全的，因为其是使用 HTTPS 或 MQTT over SSL 加密的。

有关 HTTPS 和 MQTT over SSL 的详细信息，请参阅“附录”中的“SSL 部分”。

用户管理

网络协议

Web 浏览器通过使用以下网络协议和端口来访问 ECSP 服务。

Web 浏览器

协议	端口	输入/输出	描述
HTTPS (TCP)	443	输出	访问 ECSP 服务的 Web 服务。

用户信息

对具有 ECSP 服务访问权限的用户信息进行加密，并安全地保存在数据库中。

安全性

注册用户可以登录 ECSP 服务器。登录的用户可以查看有关其具有访问权限的所有设备的信息。用户无法查看其没有访问权限的设备的信息。

此外，支持服务负责人可以对其管理的设备执行远程操作。对于负责人没有访问权限的设备，则无法执行远程操作。

客户端（Web 浏览器）和服务器（ECSP 服务器）之间通过互联网进行的数据通信是安全的，因为其是使用 HTTPS 加密的。有关 HTTPS 的详细信息，请参阅“附录”中的“SSL”部分。

数据存储

安全性

ECSP 服务器接收由 ECSP 的 DC Agent 和 ECSP 的 ES Agent 传输的数据。ECSP 服务会接收用户信息，例如：用户名和密码、合作伙伴信息和客户端信息。根据爱普生的隐私政策和安全政策，所有数据都会安全可靠地保存在服务提供商的数据库中。

附录

传输的数据

通过 HTTPS 从 ECSP 的 DC Agent 或 ECSP 的 ES Agent 发送到 ECSP 服务器的设备数据包括以下内容。

在 ECSP 服务器上收集或传输到 ECSP 服务器的设备数据类型按型号、配件、配置、出纸类型和使用状态进行区分。

类别	数据
代理	代理 ID
	代理类型
	代理版本
	收集类型
	发送日期
	操作系统
	操作系统版本
	操作系统产品类型
	设备
设备	制造商名称
	型号名称
	序列号
	区域代码
	国家代码
	时间
	获取日期
	固件版本

类别	数据
设备	打印机状态
	错误/警告代码
	状态/错误/警告历史记录
	操作面板设置
	打印机设置
	维护设置
	介质设置
	网络设置
	消耗部件信息
	清洗历史
	维护历史
	累计墨水使用量
	累计打印时间
	累计打印面积
	任务历史

使用的网络协议和端口

ECSP 的 DC Agent 和 ECSP 的 ES Agent 所使用的网络协议和端口如下：

ECSP 的 ES Agent

协议	端口	输入/输出	描述
HTTPS (TCP)	443	输出	将设备数据传输到 ECSP 服务器。 下载 ECSP 服务器的 SSL 证书。
MQTT over SSL (TCP)	443	输出	等待来自 ECSP 服务器的远程操作命令。

ECSP 的 DC Agent

协议	端口	输入/输出	描述
SNMP (UDP)	161	输出	从联网设备收集数据。下载 ECSP 服务器的 SSL 证书。
HTTPS (TCP)	443	输出	将设备数据传输到 ECSP 服务器。
MQTT over SSL (TCP)	443	输出	等待来自 ECSP 服务器的远程操作命令。
ENPC (UDP)	3289	输出	爱普生专有的打印机控制协议。

SSL

只有 HTTPS 或 MQTT over SSL 协议用于通过互联网传输的所有 ECSP 数据。HTTPS 末尾的“S”是“安全”的缩写。HTTPS 通常用于保护在交易（如网上银行和网上购物）期间输入的机密信息。MQTT over SSL 和 HTTPS 使用 SSL（安全套接字层）。SSL 是一种标准安全技术，用于在服务器和客户端之间建立加密链接。在 ECSP 模型中，ECSP 的 DC Agent、ECSP 的 ES Agent 或 Web 浏览器是客户端，ECSP 服务器或 ECSP 服务是服务器。使用 HTTPS 或 MQTT over SSL 进行的所有数据传输都得到安全保护，并保证传输到相应的目的地。

商标

- EPSON 和 EXCEED YOUR VISION 是精工爱普生株式会社的注册商标。
- Microsoft 和 Windows 是 Microsoft Corporation 在美国和其他国家/地区的注册商标。
- 其他产品名称是其各自所有者的商标或注册商标。

© Seiko Epson Corporation 2021