京瓷的多功能复合机（一体机）和打印机的安全最佳实践

版本 122024/2024年12月6日

目录

引言

概览

随着社会数字信息网络的快速发展，为连接到这些网络上的各种物联网设备提高了便利性。办公室使用的物联网设备可以处理各种类型的敏感信息。然而，物联网设备面临着近期先进且多样化的威胁，如未经授权通过网络访问物联网设备，以及在网络传输过程中对信息的窃听或篡改。多功能复合机和打印机（以下简称“产品”）也不例外。就像个人电脑一样，当客户使用该产品并将其连接到网络时，必须引起客户的关注。

京瓷办公信息系统（以下简称“京瓷”）致力于帮助应对组织在其环境中面临的安全挑战，包括联邦、州和地方政府；国防部；企业；以及医疗保健、教育和金融行业。我们通过安全的产品和服务来提高客户的信息安全和隐私性以及可靠性，并且符合国际法律要求和安全标准。

京瓷帮助我们的客户确保其安全政策被配置为他们的行业最佳实践。通过参考此文档，客户可以考虑其组织的安全态势。

目的

本文档的目的是向客户（即管理员）提出能够帮助客户配置适当安全设置的安全措施并增强工作场所中 Kyocera 产品的安全性的建议。京瓷为其产品向客户提供多种安全功能。我们建议在将安全设置应用于您的特定环境以及产品从安装和运行开始到报废阶段的整个生命周期时，尽可能多地使用本文档中所写的配置。为了确保产品最佳的性能和最有效的使用，请在设置产品提供的安全功能之前，仔细阅读本文档。如需了解其他配置的更多信息，请参阅操作指南。

目标对象

本文档的目标对象为：

- 管理员
- 其他客户

目标对象应了解以下内容：

在当前的网络安全环境下，客户（即组织）管理其终端设备（即产品）和资源以保护网络和信息资产是非常重要的。同样重要的是，客户(例如，管理员)应该教育他们组织的员工如何正确地使用与网络连接的产品。例如，用户授权管理[*1]应由组织明确确定并设置，以防止权限提升。因此，客户可以放心地在正确设置的安全环境中使用京瓷产品。

**1：参考京瓷多功能复合机和打印机的安全白皮书中描述的“用户授权管理”。*

NOTE

应该只有管理员才能够访问高级安全功能，如网络配置、系统配置、打印协议和端口。管理员应确定谁可以访问地址簿，谁可以添加、编辑或删除地址簿中的条目。管理员可以定义、强制执行和禁止进行各种安全设置。总体来说，管理员应该全面负责控制和管理产品，并确保不进行不当的操作。

版本声明

本文档中包含的信息可能会在未事先通知的情况下发生变化。其中可能包含不准确之处或打字错误。本文档的后续版本可能会纳入变更或改进。产品或软件的变更或改进将根据需要随时进行。

并非所有京瓷产品在每个市场都支持所有的安全功能和软件。某些安全功能和软件仅适用于特定的产品型号。客户可以通过查阅用户指南、操作指南，或联系您所在地区的京瓷销售公司来获取更多关于产品的信息。

局限性

这份文档旨在帮助您为用户的使用环境配置最低限度的安全设置。请注意，您需要独立评估文档中描述的信息，以及京瓷产品或服务的使用情况，特别是那些连接到您网络环境中的产品或服务。文档中的信息可能会在未提前通知的情况下发生变化。

文档中的信息是“按原样”提供的，无论是明示的还是暗示的都不附带任何形式的保证。尽管在编撰这些信息时已经谨慎处理，但京瓷不对本文中提供的信息的准确性、完整性或充分性，以及是否适用于特定目的，做出任何陈述或保证，并且不对任何错误或遗漏承担责任。京瓷产品和服务的唯一保证是随附的明示保证声明中所规定的。本文中的任何内容均不应被解释为构成额外的保证。

使用京瓷产品时的建议

本节解释了产品上的适当安全设置如何帮助用户确信能够以安全的方式保护其静止状态和传输过程中的关键数据/信息，包括可能存在的安全风险。

> *NOTE*
> *本文档中描述的以下设置仅作为常见工作场所中安全最佳实践的建议/推荐。在为用户环境中的京瓷产品进行配置之前，请确认推荐的设置。*

安装阶段

识别、认证和授权

管理员密码

我们强烈建议为每个用户环境设置合适的密码，以确保用户能够安全且便捷地使用京瓷产品。在出厂默认设置中，每台设备都设有一个独特的密码。然而，管理员密码应从其出厂默认值中进行更改。管理员密码应复杂且难以被猜出，并且不应与任何不需要访问权限的人共享。

如果未设置管理员密码，且产品保留其出厂默认设置，则存在设备设置和存储在产品中的网络设置被篡改或未经授权访问的风险。这可能导致敏感和个人信息泄露的可能性。

设置唯一的管理员密码有助于防止产品被未经授权的访问或使用。

例如)

<从产品的操作面板>

配置管理员（管理员）密码设置

1. 单击**部门管理/验证**>**用户登录设定**>**添加/编辑本地用户**。
2. 选择**管理员**。
3. 输入**登录密码**和**确认密码**。
4. 单击**登录**。

屏幕可能会因产品型号的不同而有所不同。

密码策略

应设置密码策略，并鼓励用户使用难以被猜测的强密码。

不符合密码策略的密码应被禁止使用，否则很容易被攻击者分析破解。

密码策略有助于防止用户设置简单的密码，并防止第三方未经授权的访问。

例如)

<来自该产品的操作面板>

1. 单击**部门管理/验证>验证安全性**。
2. 选择**密码策略设定**。
3. 切换到**开启>密码策略**。

屏幕可能会因产品型号的不同而有所不同。

例如)

<从Web连接>

配置密码策略设置

1. 单击**安全设定**>**设备安全**
2. 指定所需的设置，如红色框中所示的**密码策略设定**。
3. 单击**提交**。

用户帐户锁定策略

用户帐户锁定策略应设置为严格控制对产品的访问。

用户账户锁定策略会检测因输入错误密码而导致的连续失败登录尝试，当尝试次数超过预设的阈值时，会立即锁定用户账户一段时间。

用户账户锁定策略有助于防止针对产品的拒绝服务攻击（DoS）或暴力破解攻击。

例如)

<来自该产品的操作面板>

1. 单击**部门管理/验证>验证安全性**。
2. 选择**用户帐户锁定设定>锁定，锁定策略**。
3. 在锁定上，切换到**打开**。

屏幕可能会因产品型号的不同而有所不同。

例如)

<从Web连接>

配置用户帐户锁定策略设置

1. 单击**安全设定**>**设备安全**。
2. 指定所需的设定，如远程屏幕中所示的**用户帐户锁定设定**。
3. 单击**提交**。

产品管理界面

进入到产品管理界面的访问凭据（即管理员登录名和密码）应提前进行注册。

如果不对普通用户访问产品管理界面进行限制，这可能导致产品被未经授权地使用或更改设置。

京瓷提供了产品管理界面（例如 Command Center Remote extensions），该界面仅允许具有管理员权限的用户通过网络远程（通过网页浏览器）实时访问、检查和更改京瓷产品的各种设置，从而防止产品被未经授权的使用和更改设置。

例如)

<从Web连接>

配置基于web的管理员登录

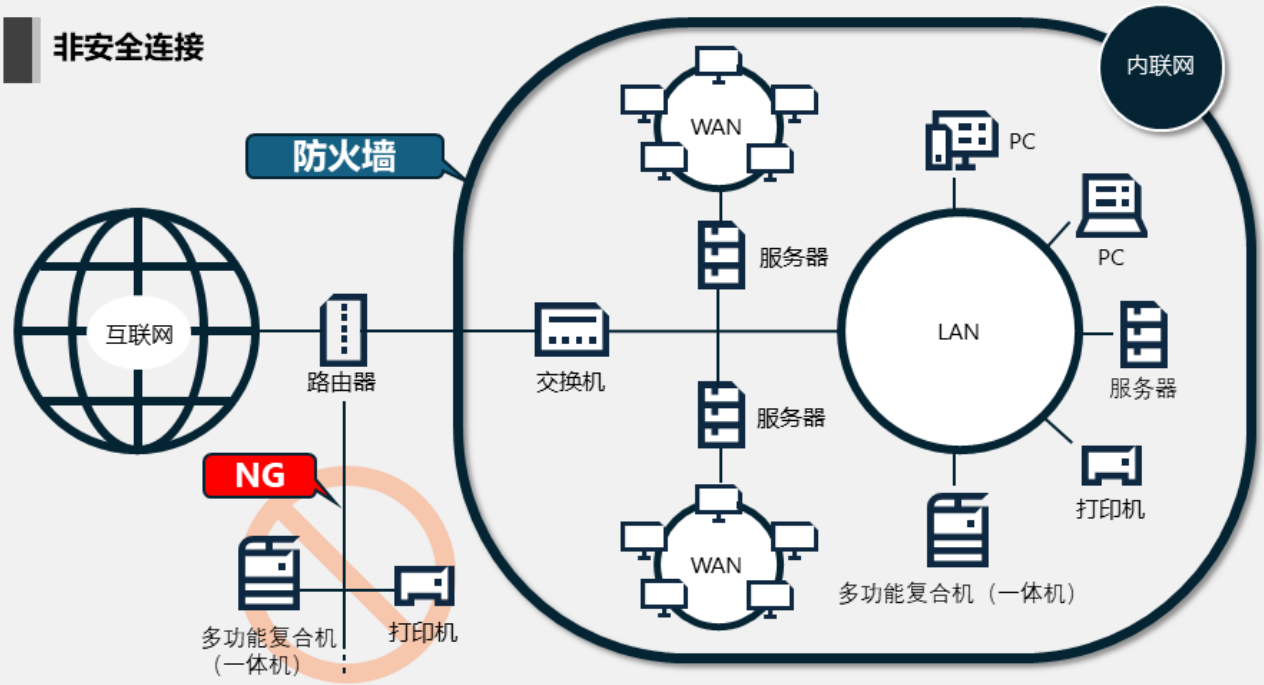
1. 单击远程屏幕右上角的**登录或管理员登录**，然后出现“管理员登录”屏幕。
2. 输入**用户名**和**密码**。
3. 单击**登录**。

网络安全性

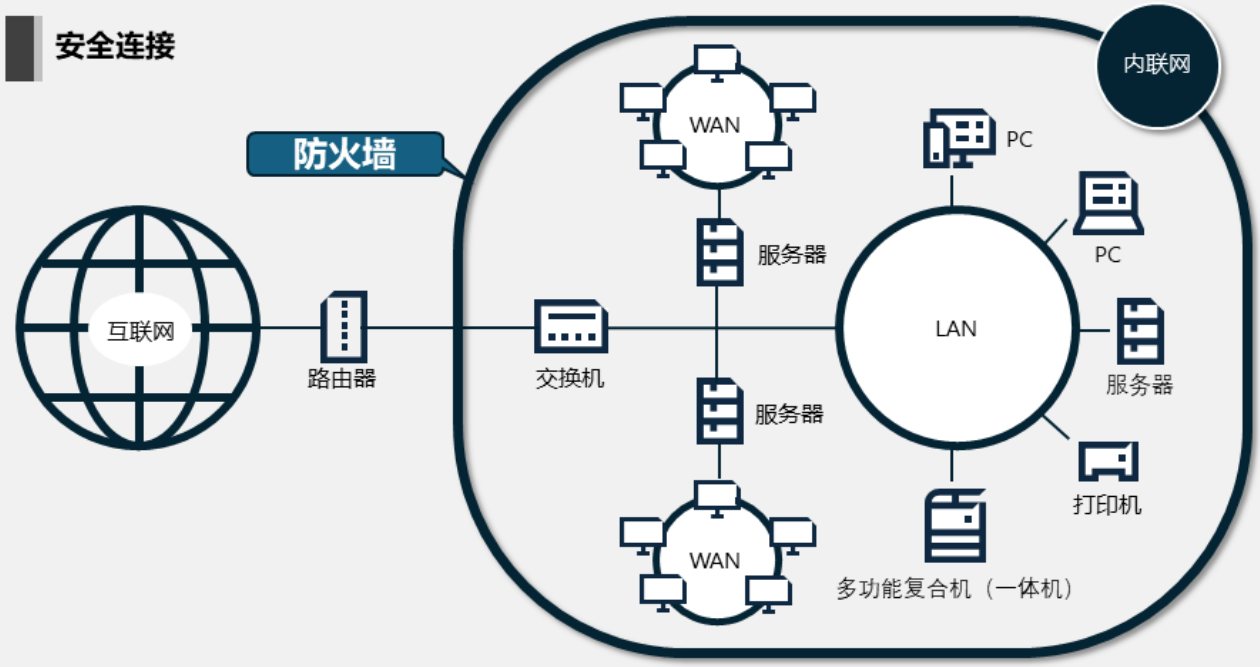
互联网联接

产品不应直接连接到互联网。应为产品分配一个本地IP地址，并将其连接到具有防火墙/路由器保护的内部网络（局域网LAN），与外部网络隔离。

如果产品直接连接到互联网，而没有防火墙/路由器来控制来自互联网的访问，那么产品将直接暴露在外部网络的攻击之下。换句话说，存储在产品中的数据（例如复印、打印和传真时的数据）以及通讯录条目等个人信息将被暴露，并可能被外部网络访问。这会导致产品被未经授权访问的风险，从而可能导致安全设置和发送目的地被篡改，以及数据泄露。



可由数目不详的用户从互联网（即从外部网络）访问



只有局域网合法用户访问（即内部用户）

以下数据应得到保护：

- 存储在产品上的硬盘/SSD中的数据
- 存储在产品内部的用户栏/作业栏/传真栏中的数据
- 注册在目的地列表上中的信息，例如地址簿和个人身份信息
- 存储在共享栏中的数据
- 设备设置
- 审核日志

NOTE

由于该产品是一个网络连接的设备，它应该限制网络访问，网络协议和端口的使用，并阻止恶意软件的入侵。

管理员应在根据产品需求设置启用/禁用FTP、HTTP、IPP、SMTP、RAW、SNMP等常见协议，以阻止不必要的连接。

此外，产品的使用应通过设置IP地址来限制，只允许/拒绝指定范围的IP地址（以及子网掩码组合）访问产品并发送/接收文档。

此外，该产品应使用诸如SSL/TLS和IPsec等加密协议来保护通过网络传输中的数据。

最后，京瓷获得了Wi-Fi CERTIFIED WPA3认证。

支持此功能的产品能够提供更强大的保护，防止未经授权的使用。这有助于防止像KRACK攻击和暴力破解攻击。

例如)

<从Web连接>

配置协议设置

1. 单击**网络设定>协议**。
2. 在远程屏幕中所示的任何协议中，指定所需的设置的**关闭/开启**。
3. 单击**提交**。

例如)

<从Web连接>

配置IP过滤器（IPv4）设定

1. 单击**网络设定**> TCP/IP。
2. 将IP过滤器（IPv4）设置为**开启**。
3. 在筛选类型中，选择**允许**或**拒绝**。
4. 如有必要，请将始终允许ICMP设置为**开启**。
5. 单击**设置**。

配置IP过滤器（IPv6）设定

1. 单击**网络设定**> TCP/IP。
2. 将IP过滤器（IPv6）设置为**开启**。
3. 在筛选类型中，选择**允许**或**拒绝**。
4. 如有必要，请将始终允许ICMP设置为**开启**。
5. 单击**设置**。

例如)

<从Web连接>

配置网络访问设置

1. 单击**安全设定**>**网络安全**。
2. 指定所需的设定，如**过滤/防火墙**、SNMPv1/v2c、SNMPv3、TLS、IEEE802.1X和IPSec。
3. 单击**提交**。

例如)

<从Web连接>

配置IP设置（有线网络）

1. 单击**网络设定**> TCP/IP。
2. 此屏幕包括以下配置项：DHCP、Auto-IP、IP地址、子网掩码、域名、DNS服务器、DNS搜索后缀、DNS over TLS、证书自动验证、Hash和WINS服务器。
3. 单击**提交**。

例如)

<从Web连接>

配置IPSec设置

1. 单击**网络设定**> TCP/IP。
2. 切换到**开启**以使用IPSec协议。
3. 指定所需的设置，如**确认有效期**、**限制**和**根证书**。
4. 单击**提交**。

NOTE

在京瓷，我们自行进行漏洞测试和渗透测试，以确保我们的产品没有漏洞，并由第三方执行渗透测试，以确保我们的产品没有漏洞。

但是，如果该产品直接连接到互联网上，客户将面临对该产品的安全风险。

TLS加密通信

当通过网页浏览器或网络打印访问产品时，应通过启用TLS协议对传输中的通信数据进行加密。还应检查通信目的地是否是合法的连接目标。TLS协议有助于防止数据被窃听和篡改，并使数据难以被分析。

如果TLS加密通信不受支持，这将导致设置信息和打印数据被篡改、泄露、窃听，信息被发送到未经授权的目标（即设备），以及产品被外部网络未经授权访问的风险。

根据每个组织环境对应的安全级别，可以设置更强版本的加密协议（例如，TLS 1.3）或加密算法（AES）。自签名证书和CSR证书支持安全且更高级别的TLS 1.3/SHA-2。

NOTE

使用可用的更强加密进行通信。

京瓷产品支持TLS加密协议，包括TLS1.0、1.1、1.2和1.3。这些功能的可用性取决于产品型号。

例如)

<从Web连接>

配置TLS

1. 单击**安全设定**>**网络安全**。
2. 指定所需的设置，如**TLS版本**（TLS1.0、TLS1.1、TLS1.2、TLS1.3），**有效加密**（ARCFOUR/DES/3DES/AES/AES-GCM/CHACHA20/POLY1305），Hash（SHA1/SHA2（256/384））,HTTP安全（仅HTTPS/HTTPS或HTTP）、IPP安全（仅IPP over TLS/IPP或IPP over TLS),Enhanced WSD 安全（仅保护（Enhanced WSD over TLS）/不保护（Enhanced WSD over TLS和Enhanced WSD）),eSCL安全（仅保护（eSCL over TLS）/不保护（eSCL over TLS和eSCL）),REST安全（仅保护（REST over TLS）/不保护（REST over TLS和REST））和**客户端设置**。
3. 单击**提交**。

例如）

<从Web连接>

配置电子邮件发送协议

1. 单击**网络设定>协议**。
2. 在SMTP（电子邮件发送）中，切换到**开启**。
3. 在SMTP安全中，选择**TLS**。
4. 在证书自动验证中，依次选中以下复选框：**有效期、服务器标识、链接**和**吊销**。
5. 在吊销检查类型中，从以下选项中选择： OCSP、CRL、CRL & OCSP。
6. 对于Hash中，请选择**SHA1**或**SHA2（256/384）**的方框。

NOTE

远程屏幕显示了一个实例，用于确认通信目的地是否为合法连接目标。

例如)

<从Web连接>

导入CA颁发的证书

1. 单击**安全设定**>**证书**。
2. 在输入证书中，选择**导入**设备证书文件。
3. 选择“**选择文件**”以浏览证书文件。
4. 选择**打开**。
5. 在导入设备证书后，单击“**提交**”。

NOTE

远程屏幕显示了各自证书的管理设置示例。

我们建议按照红框中标注的，为设备证书导入由CA颁发的证书。

存储数据保护

硬盘/SSD加密

应使用产品支持的所有加密功能，并启用支持的所有安全功能，以确保产品尽可能安全/强大。

在复印、打印、传真和扫描过程中获取的图像数据会存储在产品内部的硬盘驱动器（HDD）或固态硬盘（SSD）中。用户注册信息、设备设置和通讯录也存储在这些驱动器上。如果硬盘（HDD/SSD）被恶意人员从产品中移除，存储在硬盘上的数据/信息可能会被泄露。

通过启用硬盘（HDD/SSD）加密功能，存储在硬盘上的数据会受到加密保护。加密算法和密钥长度分别采用AES和256位，这些标准也用于保护政府文件。即使硬盘（HDD/SSD）被恶意人员从产品中移除，存储在硬盘上的敏感或机密数据也不会泄露。由于数据受到加密保护，即使将硬盘连接到PC解析工具，也无法解析数据。

NOTE

产品内置了一个加密模块，该加密模块由京瓷设计和实现。

设备管理

审计日志

强烈建议记录产品上所有活动（例如登录日志、设备日志和安全通信错误日志）的审计日志，以便为管理员提供可视化的记录，如产品或文档被访问和处理的时间和方式。换句话说，组织应通过SIEM监控产品安全日志，以便实时检测任何入侵行为。产品应能够无缝地通过syslog协议与SIEM进行通信。因此，SIEM服务器会根据分析结果向客户端通知外部攻击和威胁。

例如)

<从Web连接>

配置审计日志（系统日志）设置的设置

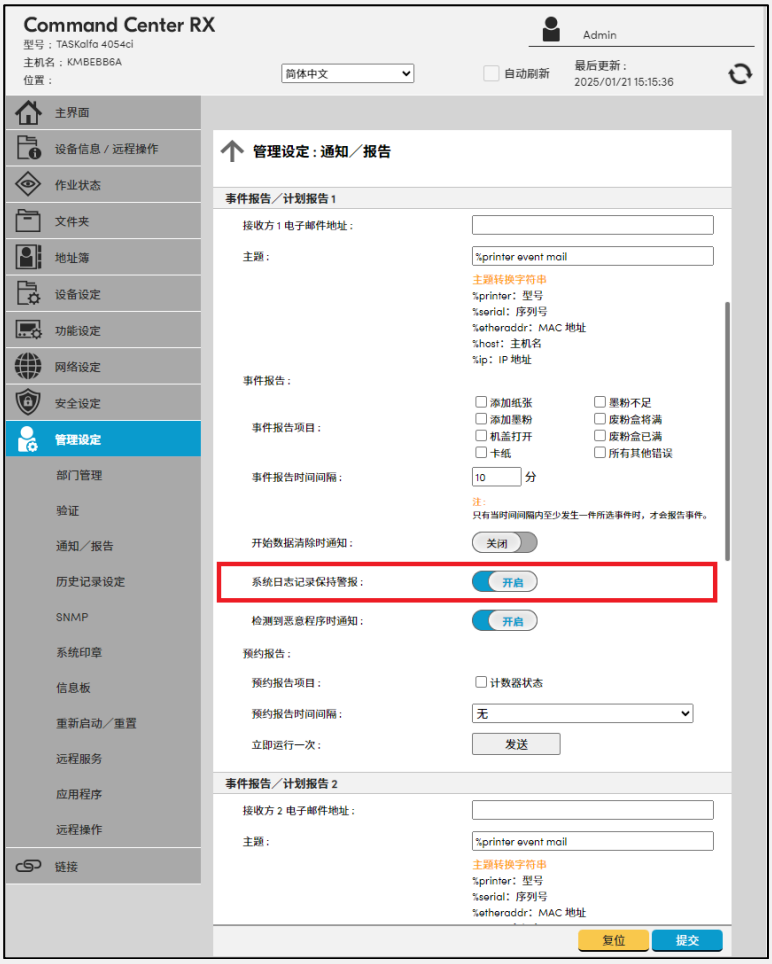
1. 单击**管理设定>历史记录设定**。
2. 显示**系统日志**的状态。
3. 在**目的服务器**中，输入目的服务器的地址。
4. 在**端口编号**中，输入系统日志的端口编号。
5. 在**实体**中，从下拉列表中选择获取日志的设施的数量。
6. 在**严重性**中，从下拉列表中选择已获取的日志的严重性。

例如)

<从Web连接>

配置审计日志（系统日志）设定

1. 单击**管理设定**>**通知/报告**。
2. 在**系统日志记录保持报警**中，切换到**开启**。
3. 单击**提交**。



作业状态/作业日志设定

用户（即管理员）应该检查产品是否安全使用，并检查是否有未经授权的访问，并应该更新产品设置，以控制谁可以访问定期访问和使用该产品。要确认这一点，应设置作业状态/作业日志。

这些日志提供了作业信息和传真传输日志，例如谁访问了该产品、发生了哪些错误以及功能是如何被使用的。

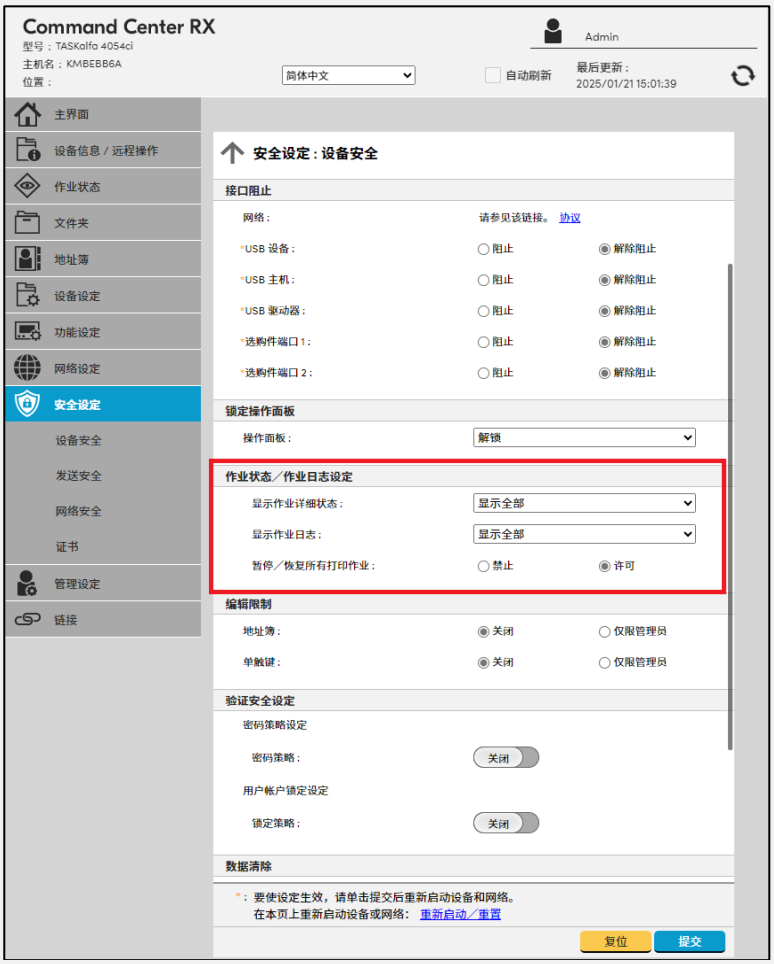
作业日志极大地遏制了恶意人员未经授权使用产品或导致数据泄露的行为，并且能够追踪对产品的未经授权的访问。

例如)

<从Web连接>

配置作业状态/作业日志设置

1. 单击**安全设定**>**设备安全**。
2. 在“**显示作业详细状态**”、“**显示作业日志**”中，从下拉列表中选择“**显示全部/仅我的作业/隐藏全部**”。在“**显示传真日志**”中，切换到“**显示所有/隐藏所有**”。在“**暂停/恢复所有打印作业**”中，切换到“**禁止/许可**”。
3. 单击**提交**。



接口阻止

应使用产品支持的安全特性，以确保产品尽可能的安全/强大。根据用户的安全政策，应禁止通过该产品的USB设备、USB主机、可选接口等接口进行访问。网络接口也应受到协议基础上的限制。

如果这些设置不当，则可能存在数据泄漏或未经授权访问产品上的数据的风险。

这些接口阻止设置可以防止数据通过USB闪存从USB接口泄漏，并防止病毒的传播。

例如)

<从Web连接>

配置接口阻止设定

1. 单击**安全设定**>**设备安全**
2. 在**USB设备**、**USB主机**、**USB驱动器**和**选购件端口**中，切换到“阻止/解除阻止”。若要配置详细的设置，请转到**网络设定**>**协议**。
3. 单击**提交**。

锁定操作面板

内部人员处理其组织的关键数据/信息的可能性相对较高。如果一些未经授权的内部人员对产品或其特定功能进行未经授权的使用，这可能会导致存储在产品上的关键数据/信息泄露。

因此，应限制在产品面板上的操作。部分锁定功能控制选项有三个领域：输入/输出、作业执行和纸张。此功能可以禁止系统菜单和作业取消操作。只有管理员可以设置这些选项。

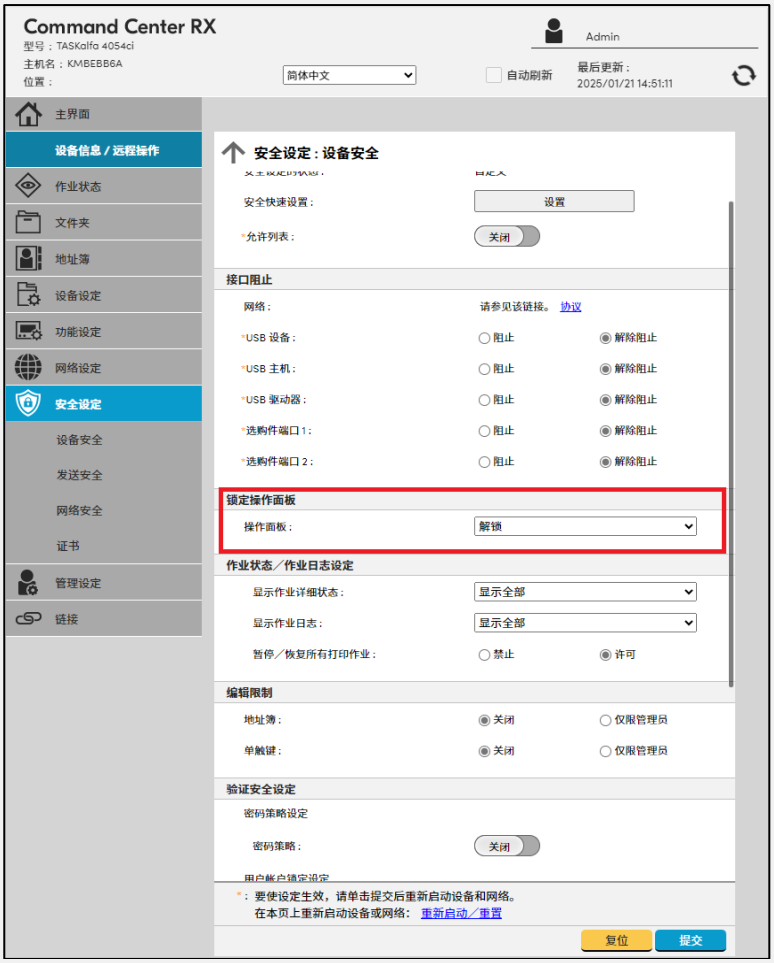
部分锁定功能可以防止对该产品进行未经授权的操作。

例如）

<从Web连接>

配置锁定操作面板设置

1. 单击**安全设定**>**设备安全**。
2. 在**操作面板**中，从下拉列表中选择**“锁定（部分锁定1/部分锁定2/部分锁定3）/解锁”**。
3. 单击**提交**。



在运行阶段

设备管理

产品软件管理

对于您的组织来说，保持京瓷产品的产品软件更新是非常重要的。为此，请定期访问京瓷办公信息系统（中国）网站，查看最新的安全相关信息。

如果您的设备仍然运行过时的软件版本，它可能会提供利用已知漏洞的产品的机会。用户应该通过运行最新的软件版本来维护您的产品的安全性和功能。

NOTE

*至于安全级别的增强，可以启用**允许列表**作为一种恶意软件预防措施。如果是一个不受信任的程序文件，则它不包含在，允许列表自动阻止程序运行。产品的操作面板显示了一个示例的安全设置，如红框所示。默认情况下，允许列表是关闭的。若要启用，，管理员可以从菜单中将“允许列表”切换到“开启”。*

屏幕可能会因产品型号的不同而有所不同。

NOTE

用户应始终应用最新的安全更新，不仅针对产品本身，也包括处理您宝贵信息资产的电脑和服务器，以保护这些用于您办公室组织的物联网设备免受攻击。

固件的真实性和完整性

我们强烈推荐使用数字签名的固件，安全启动和运行时完整性检查（RTIC）可用于您的京瓷产品，以验证固件的完整性和真实性。特别是，RTIC可以预期会更多当与安全启动功能一起使用时，可以作为一种有效的防止固件更改的安全措施。

对固件应用数字签名签名可验证固件有效性。当产品启动时，安全启动会利用数字签名验证固件是否经过认证/合法。即使固件被恶意人员篡改，也无法被执行。运行时完整性检查（RTIC）会在产品运行期间定期验证固件的有效性是否得以维持，且不会改变产品启动后部署在RAM中的固件。即使固件被恶意重写，也可以通过确认上传到产品的固件的哈希值和从签名创建的哈希值来检测，并作为系统错误发出警告。

有了这些恶意软件保护设置，固件不被改变，损害产品，被恶意第三方利用该产品作为跳脚石。

屏幕可能会因产品型号的不同而有所不同.

打印安全

走近式和认证打印作业

打印作业应保存在个人电脑中，直到用户通过产品操作面板输入其适当的密码。

如果打印好的文件长期留在产品托盘上，或者直到文件所有者走到产品前取出，可能会由第三方读取，以后可能会发现文件数据泄露。

京瓷在打印驱动程序中提供了个人打印功能。可以设置密码打印作业从PC发送的打印作业被保存在产品中，当用户到达产品旁时，需要输入正确的密码才能开始打印文档。这可以防止打印的文件被第三方阅读或取走。

例如)

<来自该产品的操作面板>

配置打印/存储的作业设置

1. 单击**作业文件夹>个人打印>存储的作业**。
2. 在密码字段中输入一个密码。
3. 单击**确定**。

屏幕可能因产品模式而有所不同.

发送安全

发送安全

该产品提供各种设置，以在发送前在屏幕上确认发送目的地（即地址编号）和主题。这有助于防止发送到错误的地址，并防止由于无意中将发送目的地添加到组而导致发送到意外目的地。

通过配置这些正确的设置，组织可以放心，文档只能发送给正确的所有者，而不会落入错误的人手中。这可以有效地防止未经授权的使用或错误的发送造成的错误的号码输入，即使是错误或错误。

例如)

<来自该产品的操作面板>

配置发送安全设置设置

1. 单击**功能设定>发送/存储>防止错误发送设定**
2. 切换到**打开**。

屏幕可能会因产品型号的不同而有所不同。

屏幕可能会因产品型号的不同而有所不同。

例如)

<从Web连接>

配置发送安全设定

1. 单击安全设定>发送安全。
2. 在**发送前检查目的地，新目的地的输入检查，选择时的目的地检查**，切换到**开/关**。在**新目的地输入，新目的地输入（传真），调用目的地，广播**中，切换到禁**止/许可**。
3. 单击**提交**。

在报废阶段

存储数据保护

数据清除

在产品租赁结束或寿命结束时，管理员设置并执行清除功能，以完全清理产品中保留的数据或任何残留数据，使用数据覆盖方法，SSD安全擦除（取决于产品型号）。产品设置可以恢复到出厂默认设置。

这可以防止关键的数据/信息恢复和数据/信息泄露到外部。

屏幕可能会因产品型号的不同而有所不同。

例如)

<从Web连接>

配置数据清除时间设定

1. 单击**安全设定**>**设备安全**。
2. 指定所需的设置，如**预约数据清除时间**和**数据清除后的设备使用**。
3. 单击**提交**。

京瓷办公信息系统（中国）有限公司

上海市黄浦区黄陂南路838弄2号3幢B座6层
电话：021-53011777
热线电话：400-601-6028