降低用于办公室的MFP (imageRUNNER ADVANCE DX/ imageRUNNER ADVANCE/imageRUNNER系列)和用于生产印刷的MFP (imagePRESS/imagePRESS Lite系列)未经授权访问风险的有用提示

重要 建议系统管理员阅读本手册。

本指引的概述和使用

目标

本指引提供了与用于办公室的佳能MFP (imageRUNNER ADVANCE DX/imageRUNNER ADVANCE/imageRUNNER系列)和用于生产印刷的MFP (imagePRESS/imagePRESS Lite系列)相关的附加信息，特别是那些可以采取的用于增强本设备安全操作的步骤。本文档将有助于您更好地了解设备功能并有助于使您确信设备会以安全、准确的方式对设备数据进行操作、存储或传送，包括与安全和网络基础设施相关的任何潜在影响。

建议您完整阅读本文档并采取与您的信息技术安全策略和做法相符的适当措施以增强贵组织的现有安全策略。由于安全要求因客户而异，因此最终需要您负责确保安全配置、修补程序和修改的实施、重新安装和测试全部都适合于您的环境并且是该环境所需的。

目标受众

本指引旨在供网络管理员、经销商和其他商业客户使用。为了最大限度地利用本指引，应了解下列内容：

- 网络环境
- 对部署在该网络上的应用程序所施加的所有限制
- 可用操作系统

本指引的限制

本指引旨在帮助您评估设备和网络环境的安全性，但无法成为所有潜在客户的完整信息源。本指引提出了一个假设的客户打印机环境；如果您的网络环境与假设环境不同，您的网络管理团队和您的经销商或授权的佳能服务提供商必须了解到这些不同并确定是否需要进行修改或采取额外的措施。
此外：

- 本指引仅描述了那些在应用程序中对一般网络环境(无论是整体网络、安全性还是其他客户资源)有明显影响的功能。
- 本指引的信息与上面指定的佳能设备相关。虽然该信息的大部分将在整个设备生命周期内保持不变，但其中一些数据是专门用于修订的并且将定期进行修订。IT组织应与他们的授权佳能服务提供商进行确认以确定其环境的适用部署。

感谢您购买佳能产品。本文档是用于保护多功能复印机/打印机(以下简称MFP，包括用于办公室的MFP (imageRUNNER ADVANCE DX/imageRUNNER ADVANCE/imageRUNNER系列)或用于生产印刷的MFP (imagePRESS/imagePRESS Lite系列))免受来自外部网络未经授权访问的指导手册概述。
建议系统管理员在使用前通读本文档。关于imagePRESS Server/ColorPASS/imagePASS/imagePRESS CR Server，请参见“保护打印机免受未经授权的访问”。

前言

近年来，MFP配备的功能数量逐步增加。除了诸如复印、传真和打印等常规功能之外，适用于经由网络使用多种类型协议访问MFP的用户的很多功能现在也可用。佳能MFP亦是如此，提供了各种方便的功能，诸如使用HTTP协议的远程用户界面功能和使用SMB/WebDAV协议的文件共享功能等。
本文档描述了在使用佳能MFP时针对防止外部网络未经授权访问的要点。

根据您所拥有机器的型号，可能不支持本文档中描述的功能。关于每个要点所需的MFP操作/设置以及是否支持各个功能的详细信息，请参见机器的用户手册。

防止外部网络未经授权访问的要点

1. 使用私有IP地址
2. 使用防火墙限制通信
3. 使用密码管理MFP信息
4. 限制远程用户界面的使用
5. 设置SSL(TLS)加密通信
6. 更新固件
7. 检测未经授权的固件修改
8. 使用审核日志
9. 根据安全策略管理MFP

注释

远程用户界面(UI)是预安装软件，可以让您使用Web浏览器访问机器的各项功能。例如，可以经由远程用户界面从计算机访问机器用于检查机器状态、执行作业以及指定各种设置。也可以通过连接到网络的计算机管理机器，而无需直接操作机器。可以通过将机器的IP地址输入Web浏览器来访问远程用户界面的门户页面。

使用远程用户界面的注意事项：

在Web浏览器中打开远程用户界面期间不要访问其他网站。此外，如果在使用远程用户界面更改设置期间或在更改设置已完成时需要离开计算机，请确保关闭Web浏览器。

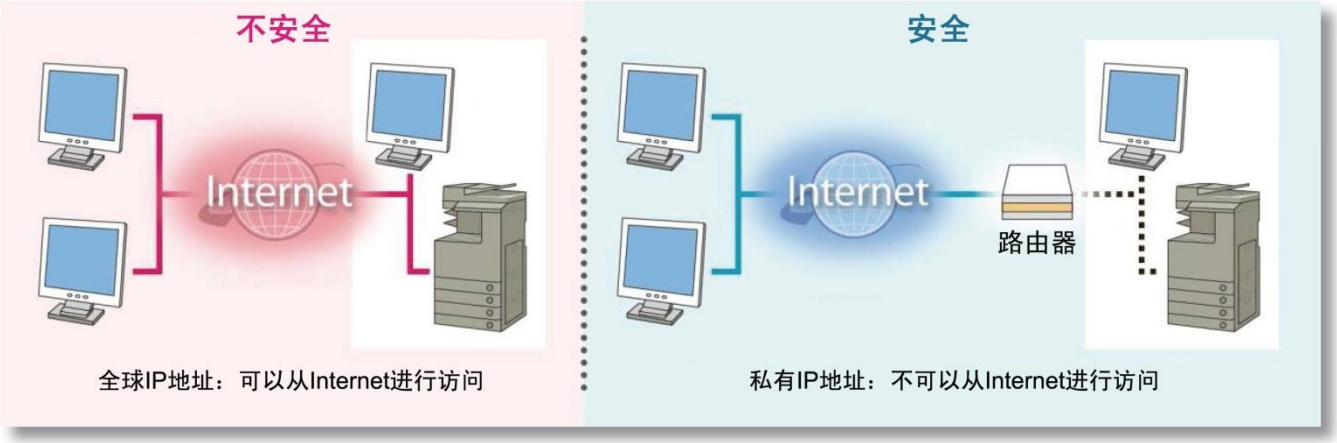
使用私有IP地址

IP地址是分配给网络上设备的数字代码。有两种IP地址类型：用于Internet连接的**“全球IP地址”**和用于诸如公司内联网等本地网络的**“私有IP地址”**。MFP被分配了一个全球IP地址时，Internet上的匿名用户就可以进行访问。这增加了由于第三方未经授权访问导致信息泄露的可能性。另一方面，对使用私有IP地址的MFP的访问限于仅在公司或其他局域网(LAN)使用的内联网上的授权用户。

原则上，在使用MFP时需分配一个私有IP地址。该私有IP地址必须属于下列范围之一。检查MFP是否具有私有IP地址。

私有IP地址范围

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255



注释

即使为MFP分配了全球IP地址，也可以通过诸如建立防火墙防止来自外部网络的访问等方式来限制未经授权访问的风险。为MFP设置全球IP地址时，请咨询公司的网络管理员。

▪ 检查IP地址的屏幕示例

机器的控制面板

机器的控制面板

* 屏幕根据机器的型号可能会有所不同。

使用防火墙限制通信

防火墙是一种不仅可以防止外部网络访问，还可以防止攻击和入侵本地网络的系统。防火墙可以通过限制指定的外部IP地址访问网络环境阻止来自外部网络具有潜在危险的未经授权访问。还可以使用佳能MFP中采用的功能筛选IP地址。

▪ 防火墙设置的屏幕示例

机器的控制面板

远程用户界面

* 屏幕根据机器的型号可能会有所不同。

使用密码管理MFP信息

即使MFP在未经授权的情况下被恶意第三方访问，通过密码保护也可以大大降低信息泄露的可能性。可以使用密码保护MFP上各种类型的数据。本小节提供了一些可以通过密码保护的功能和信息的示例。此外也可以在其他功能和信息上设置密码。可以根据需要在这些功能和信息上设置密码。

* 可以从机器的控制面板或远程用户界面设置密码。

▪ 密码输入的屏幕示例

机器的控制面板

用户登录的密码输入屏幕

机器的控制面板

系统管理员的密码输入屏幕

* 屏幕根据机器的型号可能会有所不同。

注释

虽然MFP受到了密码保护，但是管理密码对于安全措施至关重要。管理密码时应考虑下列几点：

- 确保更改默认密码。
- 避免使用别人容易猜出的密码。
- 不要让别人知道您的密码。

限制远程用户界面的使用

远程用户界面具有限制远程用户界面使用的功能。

- 使用远程用户界面需要进行一些设置，诸如更改系统管理员设置的默认PIN等。
- 可以限制一般用户访问远程用户界面。管理员和一般用户都需要PIN或密码。

▪ 启用/禁用远程用户界面的屏幕示例

机器的控制面板

机器的控制面板

* 屏幕根据机器的型号可能会有所不同。

▪ 远程用户界面登录屏幕的屏幕示例

根据机器和设置，显示的登录屏幕可能会与下面的屏幕有所不同。

登录屏幕1

无论是管理员还是一般用户，在访问远程用户界面时屏幕都会提示输入用户名和密码。

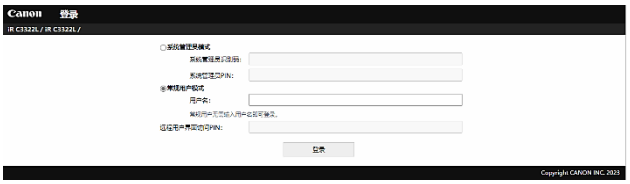
登录屏幕2

在访问远程用户界面时屏幕会提示管理员输入系统管理员ID和系统PIN，或提示一般用户输入PIN。

登录屏幕3

设置了部门ID管理时，在访问远程用户界面时屏幕会提示输入部门ID/PIN。

登录屏幕4



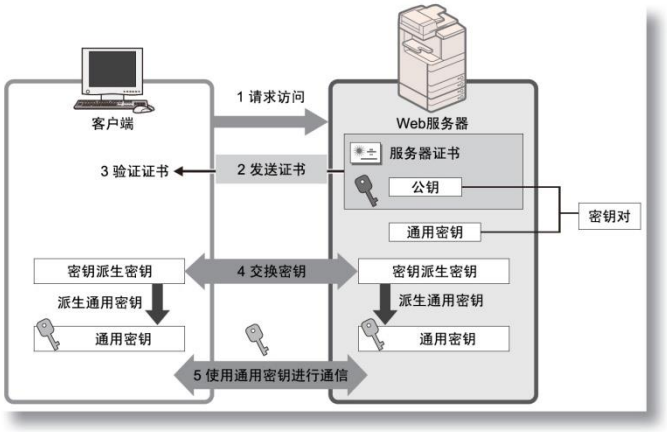
在未设置部门ID管理的情况下，在访问远程用户界面时屏幕会提示管理员输入系统管理员ID和系统PIN，或提示一般用户输入PIN。

设置SSL (TLS)加密通信

通过将服务器证书安装到MFP可以确保在经由Web浏览器访问MFP时与MFP的通信是安全的并通过SSL (TLS) 进行了加密。在使用SSL (TLS) 通信时会使用服务器证书和公钥生成仅可以由用户和MFP使用的通用密钥。这有助于防止经由外部网络进行未经授权的访问。

SSL (TLS) 通信的结构(右图)

1. 用户从其计算机访问机器时要求SSL (TLS) 的服务器证书。
2. 将证书从机器发送到用户的计算机。
3. 在用户的计算机上验证从机器接收的证书。
4. 在用户的计算机和机器之间交换密钥以建立通用密钥。
5. 现在，用户的计算机和机器都拥有通用密钥并可以使用该通用密钥发送/接收数据。



▪ SSL (TLS)设置的屏幕示例

机器的控制面板

远程用户界面

注释

建议在安全策略设置中启用[通信操作策略]以增强安全性。

* 关于[通信操作策略]的信息，请参见机器的用户手册。

更新固件

在新增功能或修复功能发生的问题时会更新固件。

可以将机器设置为定期检查是否有新固件并自动更新固件。

▪ 固件更新设置的屏幕示例

机器的控制面板

机器的控制面板

* 屏幕根据机器的型号可能会有所不同。

检测未经授权的固件修改

为了进一步增强固件的安全性，可以设置MFP以在MFP启动时以及在运行MFP期间检测固件修改。

▪ 固件修改检测设置的屏幕示例

机器的控制面板

* 屏幕根据机器的型号可能会有所不同。

使用审核日志

可以使用日志检查/分析机器的使用情况。日志会记录诸如操作日期/时间、用户名、操作类型、功能类型和操作结果等信息。

日志类型

- 用户认证日志
- 作业日志
- 传送日志
- 高级存储箱保存日志
- 存储箱操作日志
- 存储箱认证日志
- 高级存储箱操作日志
- 机器管理日志
- 网络认证日志
- 导出/导入全部日志
- 存储箱备份日志
- 应用程序/软件管理屏幕操作日志
- 安全策略日志
- 分组管理日志
- 系统维护日志
- 认证的打印日志
- 设置同步日志
- 用于审核日志管理的日志

日志检索方式

- 自动导出(自动导出到SMB服务器的指定文件夹)
- 手动导出(从远程用户界面导出)
- 连续发送(发送到Syslog/SIEM服务器)

▪ 日志设置的屏幕示例

远程用户界面

* 屏幕根据机器的型号可能会有所不同。

根据安全策略管理MFP

一些组织对安全策略进行了定义，包括用于信息安全的基本策略和安全措施标准。应在这些策略下操作诸如计算机和MFP等信息设备。

机器能够全面管理与安全策略相关的多个设置并且可以仅限于由负责信息安全的人员进行设置更改。

安全策略设置

[界面]

- 无线连接策略
  禁止无线连接以防止非指定的大量访问。
- USB策略
  禁止USB连接以防止未经授权的连接和数据检索。

[认证]

- 认证操作策略
  确保进行用户认证以避免未注册用户进行未经授权的操作。
- 密码操作策略
  严格限制密码操作方式。
- 密码设置策略
  通过设置所需的复杂性级别和有效期使第三方难以猜到用于用户认证的密码。
- 封锁策略
  在由于密码错误导致登录操作连续失败特定次数时在特定的时间段内阻止用户登录。

[密钥/证书]

通过阻止使用弱加密并对指定硬件内的用户密码和密钥进行加密来保护重要的数据。

[网络]

- 通信操作策略
  通过要求验证签名和证书启用更安全的通信。
- 端口使用策略
  通过关闭不使用的端口防止外部渗透。

[日志]

通过要求记录日志启用定期审核。

[作业]

- 打印策略
  防止由于打印导致的信息泄露。
- 发送/接收策略
  限制发送时的目标操作以及处理接收数据的方式。

[存储设备]

通过删除硬盘上不需要的数据防止信息泄露。

▪ 安全策略设置的屏幕示例

远程用户界面

* 屏幕根据机器的型号可能会有所不同。

USRM2-9642-01