



Pro C7100s/C7100sx

操作说明书
安全指南

目录

1. 开始使用

配置安全功能设置之前.....	9
使用本机之前.....	10
管理员和用户.....	11
管理员.....	12
配置管理员验证.....	13
指定管理员权限.....	14
注册和更改管理员.....	16
使用 Web Image Monitor 配置管理员验证.....	18
管理员登录方式.....	19
使用控制面板登录.....	19
使用 Web Image Monitor 登录.....	20
管理员注销方式.....	21
使用控制面板注销.....	21
使用 Web Image Monitor 注销.....	21
超级用户.....	22
重置管理员密码.....	22
更改超级用户.....	23

2. 配置用户验证

用户.....	25
关于用户验证.....	26
配置用户验证.....	27
用户代码验证.....	29
基本验证.....	31
指定基本验证.....	31
通讯簿中保存的验证信息.....	32
指定登录用户名和密码.....	33
指定登录详细信息.....	34
Windows 验证.....	35
指定 Windows 验证.....	36
安装 Internet 信息服务 (IIS) 和证书服务.....	40
创建服务器证书.....	42
LDAP 验证.....	43

打印机作业验证.....	48
打印机作业验证级别.....	48
打印机作业类型.....	48
“authfree” 命令.....	50
自动注册到通讯簿.....	51
自动注册的通讯簿项目.....	51
地址簿自动编入的数据保留设置.....	51
用户锁定功能.....	53
指定用户锁定功能.....	53
取消密码锁定.....	54
自动注销.....	55
使用外部设备进行验证.....	56
3. 限制机器的使用	
限制使用目的地列表.....	57
防止更改管理员设置.....	59
限制每个管理员可以更改的设置.....	59
禁止用户更改设置.....	59
指定菜单保护.....	60
复印功能.....	60
打印功能.....	60
扫描功能.....	60
防止用户注册/更改程序.....	61
限制可使用的功能.....	62
限制使用介质插槽.....	64
管理每个用户的打印容量.....	65
指定打印容量限制.....	66
指定默认的最大使用计数.....	67
指定每个用户的最大使用计数.....	68
检查每个用户的打印容量.....	69
对打印容量使用计数器列表进行打印.....	70
重置打印容量使用计数器.....	72
配置自动重置功能.....	73

4. 防止从机器中泄漏信息

保护通讯簿.....	75
指定通讯簿访问权限.....	75
对通讯簿中的数据进行加密.....	77
对机器上的数据进行加密.....	79
启用加密设置.....	81
备份加密密钥.....	82
更新加密密钥.....	83
取消数据加密.....	84
删除机器上的数据.....	86
自动清除内存.....	86
清除所有内存.....	90

5. 提升网络安全

访问控制.....	95
启用和禁用协议.....	96
使用控制面板启用和禁用协议.....	101
使用 Web Image Monitor 启用和禁用协议.....	102
指定网络安全等级.....	103
使用控制面板指定网络安全等级.....	103
使用 Web Image Monitor 指定网络安全等级.....	104
每种网络安全等级下的功能状态.....	104
通过设备证书保护通信路径.....	108
从控制面板创建并安装设备证书（自签证书）.....	108
从 Web Image Monitor 创建并安装设备证书（自签证书）.....	109
创建（证书机构颁发的）设备证书.....	110
安装（证书机构颁发的）设备证书.....	110
安装中间证书（由证书颁发机构颁发）.....	111
配置 SSL/TLS 设置.....	112
启用 SSL/TLS.....	113
SSL/TLS 的用户设置.....	114
设置 SSL/TLS 加密模式.....	114
为 SMTP 连接启用 SSL.....	115
配置 S/MIME.....	117

电子邮件加密.....	117
附加电子签名.....	119
检查证书的有效期限.....	121
配置带有电子签名的 PDF.....	122
配置 IPsec 设置.....	123
通过 IPsec 进行加密和验证.....	124
加密密钥自动交换设置.....	124
IPsec 设置.....	125
加密密钥自动交换设置配置流程.....	130
telnet 设置命令.....	133
配置 IEEE 802.1X 验证.....	139
安装站点证书.....	139
选择设备证书.....	140
为以太网设置 IEEE 802.1X 项.....	140
SNMPv3 加密.....	143
加密传送的密码.....	144
指定驱动程序加密密钥.....	144
指定 IPP 验证密码.....	145
Kerberos 验证加密设置.....	146

6. 防止文件泄漏

管理文件夹.....	149
删除文件夹.....	149
更改文件夹的密码.....	150
解除文件夹锁定.....	151
管理保存的文件.....	153
配置各个保存文件的访问权限.....	154
更改文件的所有者.....	156
配置各个用户对保存文件的访问权限.....	157
为保存的文件指定密码.....	159
解除对保存文件的锁定.....	160
管理锁定打印文件.....	162
删除锁定打印文件.....	162
更改锁定打印文件的密码.....	164

解除锁定打印文件的锁定.....	165
防止未经授权复印/复印数据安全性.....	167
启用图案打印.....	167
在纸张上打印用户信息.....	169
在打印机上强制保存要打印的文件.....	171

7. 管理机器

管理日志文件.....	173
使用 Web Image Monitor 管理日志文件.....	174
可以使用 Web Image Monitor 进行管理的日志.....	174
可下载日志的属性.....	179
指定日志收集设置.....	203
下载日志.....	204
可以保存在机器上的日志数.....	205
有关日志条目数达到最大值时的操作注意事项.....	206
打印机作业日志.....	208
删除所有日志.....	209
禁止向日志收集服务器传送日志.....	209
从机器中管理日志.....	210
指定日志收集设置.....	210
禁止向日志收集服务器传送日志.....	210
指定删除所有日志.....	211
通过日志收集服务器管理日志.....	211
为单个用户配置主页屏幕.....	212
有关使用用户自己的主页屏幕的警告.....	212
管理设备信息.....	214
导出设备信息.....	215
导入设备信息.....	216
定期导入设备信息.....	218
手动导入服务器的设备设置信息文件.....	219
故障排除.....	219
管理环保计数器.....	222
配置环保计数器.....	222
重置机器的环保计数器.....	223

重置用户的环保计数器.....	223
管理通讯簿.....	224
指定自动删除通讯簿数据.....	224
删除通讯簿中的所有数据.....	224
指定扩展安全功能.....	225
其他安全功能.....	231
扫描仪功能.....	231
系统状态.....	231
检查固件有效性.....	231
限制客户工程师操作.....	232
增强安全性的附加信息.....	233
可使用控制面板配置的设置.....	233
可使用 Web Image Monitor 配置的设置.....	234
IPsec 可用/不可用时配置的设置.....	236

8. 故障排除

如果显示信息.....	239
如果显示错误代码.....	240
基本验证.....	240
Windows 验证.....	241
LDAP 验证.....	245
如果无法操作机器.....	249

9. 设置的操作权限列表

如何读取.....	253
系统设置.....	254
纸盘纸张设置.....	263
编辑主页.....	264
为操作员调整设置.....	265
为技术熟练的操作员调整设置.....	266
复印机/文件服务器特性.....	267
打印机功能.....	274
打印特性.....	275
扫描仪特性.....	279
扩展功能设置.....	281

维护.....	282
Web Image Monitor: 显示环保计数器.....	283
Web Image Monitor: 作业.....	284
Web Image Monitor: 设备设置.....	285
Web Image Monitor: 打印机.....	295
Web Image Monitor: 扫描仪.....	299
Web Image Monitor: 接口.....	302
Web Image Monitor: 网络.....	303
Web Image Monitor: 安全.....	307
Web Image Monitor: @Remote.....	309
Web Image Monitor: 网页.....	310
Web Image Monitor: 扩展功能设置.....	311
Web Image Monitor: 地址簿.....	312
Web Image Monitor: 通讯簿集中管理.....	313
Web Image Monitor: 主电源关闭.....	314
Web Image Monitor: 重置打印机作业.....	315
Web Image Monitor: 重置该机器.....	316
Web Image Monitor: 设备主页管理.....	317
Web Image Monitor: 画面监控.....	318
Web Image Monitor: 每个用户的自定义画面.....	319
Web Image Monitor: 文件服务器.....	320
Web Image Monitor: 打印机: 打印作业.....	321
保存文件操作权限列表.....	322
通讯簿操作权限列表.....	324
索引	327

1. 开始使用

本章将介绍使用机器安全功能时需要注意的事项以及如何配置管理员设置。

配置安全功能设置之前

★重要信息

- 如果未配置安全设置，则机器中的数据容易受到攻击。
- 为了防止机器被盗或蓄意破坏，请在安全位置安装本机。
- 本机的购买者必须确保机器的使用人员也能恰当操作，并且与机器管理员或超级用户确定的操作一致。如果管理员或超级用户未进行必要的安全设置，则存在用户违反安全操作的风险。
- 在设置本机的安全功能以及确保用户执行适当的操作之前，管理员必须通读《安全指南》，尤其要特别注意“配置安全功能设置之前”一节。
- 管理员必须通知用户有关安全功能的正确用法。
- 如果已将本机连接到网络，则必须采用防火墙或类似措施来保护其运行环境。
- 为在通讯期间保护数据，请应用机器的通讯安全功能，并将其连接到支持安全功能（例如加密通讯）的设备。
- 管理员应定期检查机器的日志，以发现非法事件和异常事件。

使用本机之前

1

本节说明如何对传送的数据进行加密以及如何配置管理员帐户。如果要获得较高的安全性，请在使用机器前进行以下设置。

1. 打开机器电源。

有关打开主电源的详细信息，请参见《开始使用》中的“打开/关闭电源”。

2. 按[用户工具]键。



3. 按[系统设置]。

4. 按[接口设置]。

5. 指定 IPv4 地址。

有关如何指定 IPv4 地址的详细信息，请参见《连接机器/系统设置》中的“接口设置”。

6. 在[系统设置]中按[文件转送]。

7. 按下[管理员的电子邮件地址]，然后指定本机器管理员的电子邮件地址。

8. 从控制面板创建并安装设备证书。

有关如何安装设备证书的信息，请参见 p.108 “通过设备证书保护通信路径”。

输入在步骤 7 中指定的地址，作为设备证书的电子邮件地址。

9. 更改管理员的登录用户名和密码。

有关指定管理员登录用户名和密码的详细信息，请参见 p.16 “注册和更改管理员”。

10. 将本机连接到通用网络环境。

↓ 注

- 要启用更高的安全性，请参见 p.233 “增强安全性的附加信息”。

管理员和用户

本节介绍本手册中使用的术语：“管理员”、“超级用户”、“用户”和“所有者”。

管理员

本机有 4 种管理员：用户管理员、机器管理员、网络管理员和文件管理员。

他们的主要任务是指定操作机器的设置。其访问权限取决于管理员类型。管理员不能执行复印和打印等普通操作。

超级用户

只有一个超级用户。超级用户可以指定每个管理员的密码。对于普通操作，不需要超级用户，因为管理员可指定自己的密码。

用户

用户是指使用本机进行复印和打印等普通操作的人员。

所有者

在机器中复印机、打印机或其他功能下注册了文件的用户称为所有者。

管理员

1

管理员管理机器的用户访问及各种其他重要的功能和设置。

对限制访问和设置进行控制时，管理员在使用本机之前先选择本机管理员并启用验证功能。启用验证功能后，将需要提供登录用户名和密码才能使用机器。根据职能，本机的管理员角色分为 4 个类别：用户管理员、机器管理员、网络管理员和文件管理员。共享管理员任务可便于各位管理员执行任务，同时也可以防止未经授权的管理员操作。多个管理员角色可以分配给一个管理员，一个角色还可以由多个管理员共享。您还可以设置超级用户，该超级用户可以更改管理员的密码。

管理员不能使用复印和打印等功能。要使用这些功能，管理员必须以用户身份接受验证。

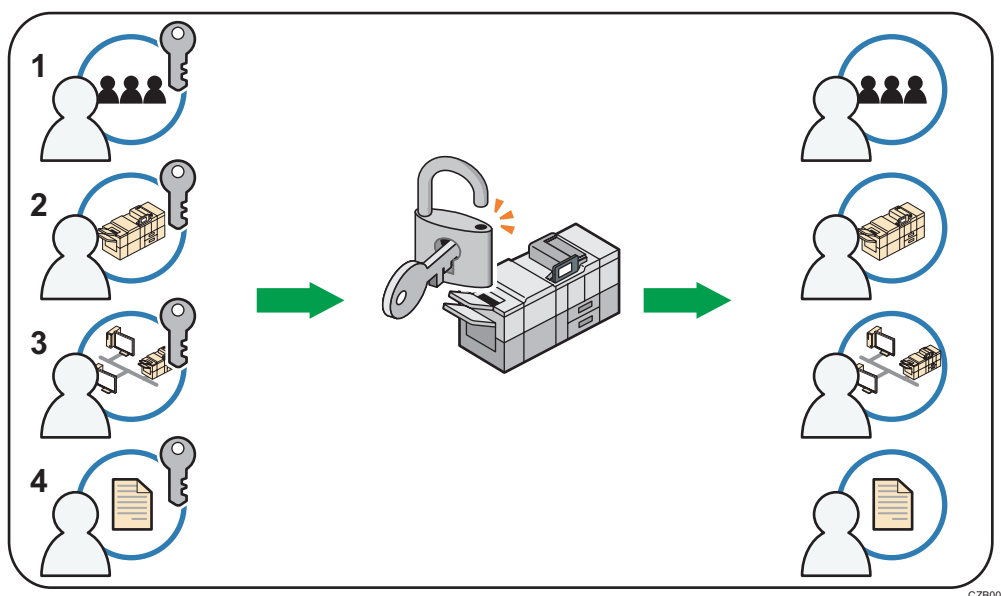
有关注册管理员的说明，请参见 p.16 “注册和更改管理员”，有关更改管理员密码的说明，请参见 p.22 “超级用户”。有关用户的详细信息，请参见 p.25 “用户”。

配置管理员验证

管理员验证需要登录用户名和密码，才可验证试图指定机器设置或从网络访问这些设置的管理员。注册管理员时，您不能使用已在通讯簿中注册的登录用户名。对管理员与对通讯簿中注册的用户的管理方式是不同的。由于系统不会对管理员执行 Windows 验证和 LDAP 验证，因此，即使由于网络问题而无法访问服务器，管理员仍然可以登录。每位管理员均以登录用户名来标识。如果将多个管理员权限授予同一个登录用户名，一位管理员就可以同时充当多种类型的管理员。有关注册管理员的说明，请参见 p.16 “注册和更改管理员”。

您可以为每位管理员指定登录用户名、密码和加密密码。加密密码用于对通过 SNMPv3 传送的数据进行加密。使用 SNMPv3 的应用程序（例如 Device Manager NX）也会用到它。管理员仅限于管理机器的设置和控制用户访问，因此他们无法使用诸如复印和打印之类的功能。要使用这些功能，管理员必须在通讯簿中注册为用户，然后接受验证。指定管理员验证，然后指定用户验证。有关指定验证的详细信息，请参见 p.27 “配置用户验证”。

各个管理员的角色



1. 用户管理员

管理通讯簿中的个人信息。

用户管理员可以注册/删除通讯簿中的用户或更改用户的个人信息。

在通讯簿中注册的用户也可以更改和删除其自身的信息。

如果用户忘记了自己的密码，用户管理员可以删除该密码，然后创建一个新密码，从而使该用户可以再次访问机器。

2. 机器管理员

主要负责管理机器的默认设置。您可以对机器进行设置，使每项功能的默认值只能由机器管理员来指定。通过进行此设置，可防止未经授权的用户更改设置并使机器可供其用户安全地使用。

3. 网络管理员

管理网络设置。您可以对机器进行设置，使 IP 地址和电子邮件的发送和接收设置之类的网络设置只能由网络管理员来指定。

进行此项设置可以防止未经授权的用户更改设置和禁用机器，从而确保网络的正常运行。

4. 文件管理员

管理保存文件的访问权限。可以指定一些密码，只允许具有权限的注册用户查看和编辑保存在文件服务器中的文档。通过此设置，可防止由于未经授权的用户查看和使用注册数据而造成数据泄漏和被篡改。

↓ 注

- 管理员验证也可以通过 Web Image Monitor 来指定。有关详细信息，请参见 Web Image Monitor 帮助。
- 无需指定管理员验证也可以指定用户代码验证。

指定管理员权限

要指定管理员验证，请将“管理员验证管理”设置为[开]。如果启用了此设置，则管理员只能配置分配给他们的设置。

要以管理员身份登录，请使用默认登录用户名和密码。

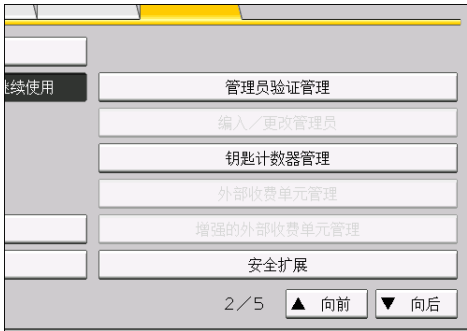
有关使用管理员验证登录和注销的详细信息，请参见 p.19 “管理员登录方式”和 p.21 “管理员注销方式”。

★ 重要信息

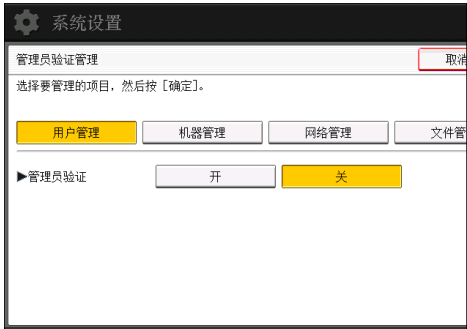
- 如果您启用了“管理员验证管理”，请确保不要忘记管理员登录用户名和密码。如果您忘记了管理员登录用户名或密码，则必须使用超级用户的权限来指定新密码。有关超级用户权限的详细信息，请参见 p.22 “超级用户”。

1. 按[用户工具]键。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[▼向后]。

5. 按[管理员验证管理]。



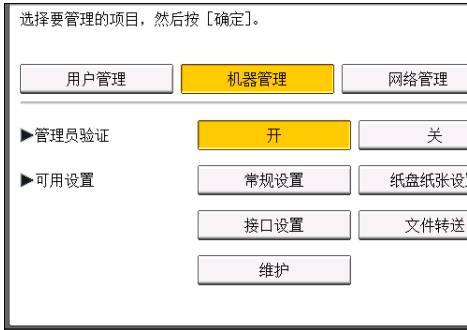
6. 按[用户管理]、[机器管理]、[网络管理]或[文件管理]键选择要管理的设置。



7. 将"管理员验证"设置为[开]。

出现“可用设置”。

8. 从“可用设置”中选择要管理的设置。



用户将无法使用选定的设置。

可用的设置取决于管理员类型。

要为多个类别指定管理员验证，请重复步骤 6 到步骤 8。

9. 按[确定]。

10. 按[用户工具]键。

注册和更改管理员

1

如果指定了管理员验证，建议一人只担任一种管理员角色。

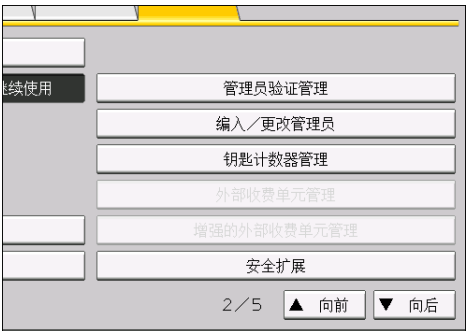
共享管理员任务可便于每位管理员执行任务，同时也可以防止未经授权的管理员操作。最多可以注册 4 个可授予管理员权限的登录用户名（管理员 1 到 4）。

管理员的权限只能由具有相关权限的管理员进行更改。

请务必分配所有管理员权限，以便每种管理员权限都至少与一个管理员相关联。

有关使用管理员验证登录和注销的详细信息，请参见 p.19 “管理员登录方式” 和 p.21 “管理员注销方式”。

1. 以管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[▼向后]。
5. 按[编入／更改管理员]。



6. 在与您要指定其权限的管理员对应的行中，按[管理员 1]、[管理员 2]、[管理员 3]或[管理员 4]，然后按[更改]。



每次向各位用户分配管理员权限时，请在每个类别下选择一个管理员，如下所示。

[illegible]

要合并多个管理员权限，请将多个管理员权限分配给一个管理员。

例如，要将机器管理员权限和用户管理员权限分配给[管理员 1]，请按机器管理员和用户管理员对应行中的[管理员 1]。

7. 按“登录用户名”所对应的[更改]。
8. 输入登录用户名，然后按[确定]。
9. 按“登录密码”所对应的[更改]。
10. 输入登录密码，然后按[确定]。
按照密码策略增强登录密码。
有关密码策略以及如何指定的详细信息，请参阅[密码策略](#)。
11. 再次输入登录密码进行确认，然后按[确定]。
12. 按"加密密码"所对应的[更改]。
13. 输入加密密码，然后按[确定]。
14. 再次输入加密密码进行确认，然后按[确定]。
15. 按两次[确定]。

此时会将您自动注销。

 注

- 有关可用于登录用户名和密码的字符，请参见 p.17 “可用于用户名和密码的字符”。

可用于用户名和密码的字符

以下字符可用于登录用户名和密码。名称和密码区分大小写。

- 大写字母: A 到 Z (26 个字符)
- 小写字母: a 到 z (26 个字符)
- 数字: 0 到 9 (10 个字符)
- 符号: (空格) ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ { | } ~ (33 个字符)

登录用户名

- 不能包含空格、冒号或引号。
- 不能留为空白。
- 最长可以有 32 个字符。
- 如果管理员的登录用户名最多为 8 个字符，则必须包含除数字字符（数字）外的其他字符。如果只包含数字，则必须使用 9 个或更多字符。

登录密码

- 管理员和超级用户的最大密码长度为 32 个字符；用户的最大密码长度为 128 个字符。
- 可用于密码的字符类型没有限制。出于安全考虑，建议创建密码时包含大小写字母、数字和符号。包含大量字符的密码不易被其他用户破解。
- 在[安全扩展]的[密码策略]中，可以指定包含大小写字母、数字和符号的密码，以及用于密码的最小字符数。有关指定密码策略的详细信息，请参见 p.225 “指定扩展安全功能”中的“密码策略”。

使用 Web Image Monitor 配置管理员验证

您可以使用 Web Image Monitor 登录机器和更改管理员设置。有关使用管理员验证登录和注销的详细信息，请参见 p.19 “管理员登录方式”和 p.21 “管理员注销方式”。

1. 以管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“设备设置”下，单击[管理员验证管理]或[编入/更改管理员]。
4. 根据需要更改设置。
5. 注销。

↓ 注

- 有关 Web Image Monitor 的详细信息，请参见 Web Image Monitor 帮助。

管理员登录方式

如果指定了管理员验证，请使用管理员的登录用户名和密码来登录。超级用户以相同方式登录。

有关管理员和超级用户的用户名和密码的信息，请向管理员咨询。

使用控制面板登录

1. 按[用户工具]键。
2. 按[登录/注销]键。

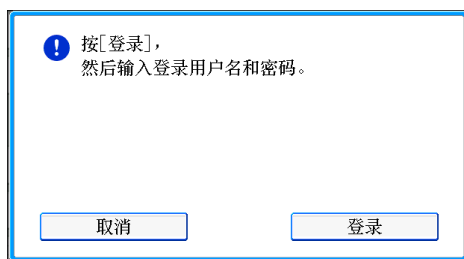


CWW226

出现登录屏幕。

也可以通过在用户工具菜单中按[登录]让登录屏幕显示出来。

3. 按[登录]。



4. 输入登录用户名，然后按[确定]。
5. 输入登录密码，然后按[确定]。

出现“验证中...请等待。”，然后显示初始设置屏幕。

注

- 如果已指定用户验证，将显示验证屏幕。要以管理员身份登录，请输入管理员的登录用户名和密码。

- 如果您使用管理员权限登录，则屏幕上会出现登录管理员的名称。当使用具有多个管理员权限的用户名登录时，将显示与该用户名关联的权限之一。
- 如果您试图从操作屏幕登录，则会出现“您没有使用此功能的权限。您仅可以管理员身份更改设置。”信息。按[用户工具]键以显示初始设置屏幕。

使用 Web Image Monitor 登录

1. 打开 Web 浏览器。

2. 在地址栏中输入“http://（机器的 IP 地址或主机名）/”。

输入 IPv4 地址时，字段不能以零开头。例如，如果地址为“192.168.001.010”，您必须将其输入为“192.168.1.10”才能连接到机器。

在中括号中输入 IPv6 地址，例如：[2001:db8::9abc]。

如果将“允许 SSL/TLS 通信”设置为[仅限密文]，请输入“http://（机器的 IP 地址或主机名）/”以访问机器。

3. 单击窗口右上角的[登录]。

4. 输入管理员的登录用户名和密码，然后单击[登录]。

↓ 注

- 通过保留登录用户名和密码，可将 Web 浏览器配置为自动完成登录对话框。此功能降低了安全性。为防止浏览器保留登录用户名和密码，请禁用浏览器的自动完成功能。

管理员注销方式

如果指定了管理员验证，请确保完成更改设置后再注销。超级用户以相同方式注销。

1

使用控制面板注销

1. 按[登录/注销]键，然后按[是]。

↓ 注

- 还可以按照以下步骤注销：
 - 按[节能]键。

使用 Web Image Monitor 注销

1. 单击窗口右上角的[注销]。

↓ 注

- 注销后删除 Web Image Monitor 中的高速缓存。

超级用户

超级用户可以删除管理员的密码并指定新密码。

如果管理员忘记或更改了密码，超级用户可以为管理员指定新的密码。如果您以超级用户的用户名和密码登录，则无法使用普通功能或指定系统设置。登录和注销的方式与管理员相同。请参见 p.19 “管理员登录方式”和 p.21 “管理员注销方式”。

★重要信息

- 切勿忘记超级用户的登录用户名和密码。如果忘记了这些用户名和密码，服务代表将不得不将机器恢复到其默认状态。这样将导致机器设置数据、计数器、日志及其他数据丢失。维修请求可能需要付费。

↓注

- 有关可用于登录用户名和密码的字符，请参见 p.17 “可用于用户名和密码的字符”。
- 不能为超级用户和管理员指定相同的登录用户名。
- 您可以使用 Web Image Monitor 以超级用户身份登录，并删除管理员密码或指定一个新密码。

重置管理员密码

1. 以超级用户身份从控制面板中登录。

有关如何登录的详细信息，请参见 p.19 “管理员登录方式”。

2. 按[系统设置]。

3. 按[管理员工具]。

4. 按[▼向后]。

5. 按[编入／更改管理员]。

6. 按想要重置的管理员所对应的[更改]。



7. 按“登录密码”所对应的[更改]。

8. 输入登录密码，然后按[确定]。

9. 再次输入登录密码进行确认，然后按[确定]。

10. 按两次[确定]。

此时会将您自动注销。

↓ 注

- 超级用户可更改管理员的登录密码，但不能更改其登录用户名。

更改超级用户

本节介绍如何更改超级用户的登录用户名和密码。

为此，您必须通过“管理员验证管理”下的设置启用用户管理员的权限。有关详细信息，请参见 p.14 “指定管理员权限”。

1. 以超级用户身份从控制面板中登录。

有关如何登录的详细信息，请参见 p.19 “管理员登录方式”。

2. 按[系统设置]。

3. 按[管理员工具]。

4. 按[▼向后]。

5. 按[编入/更改管理员]。

6. 在“主管”下，按[更改]。

7. 按“登录用户名”所对应的[更改]。

8. 输入登录用户名，然后按[确定]。

9. 按“登录密码”所对应的[更改]。

10. 输入登录密码，然后按[确定]。

11. 再次输入登录密码进行确认，然后按[确定]。

12. 按两次[确定]。

此时会将您自动注销。

2. 配置用户验证

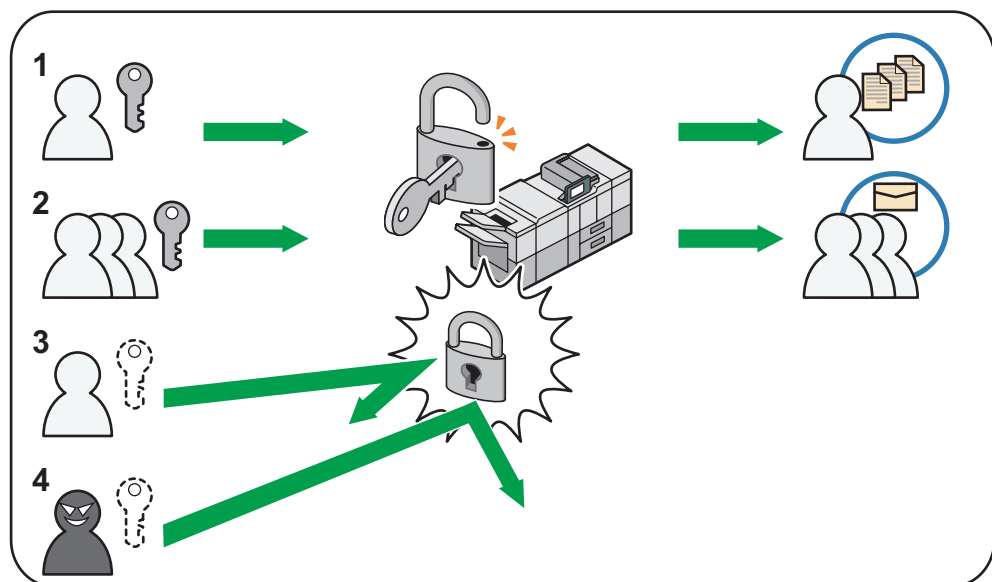
本章介绍如何指定用户验证并说明用户验证启用的功能。

用户

用户在机器上可以执行复印和打印等普通操作。系统使用机器通讯簿中的信息对用户进行管理，并且用户只能使用管理员允许其访问的功能。通过启用用户验证，可以只允许通讯簿中注册的人员使用机器。用户管理员可在通讯簿中对用户进行管理。有关管理员的详细信息，请参见 p.12 “管理员”。有关通讯簿中的用户注册的详细信息，请参见《连接机器/系统设置》中的“注册用户信息”或 Web Image Monitor 帮助。

关于用户验证

用户验证是一个系统，它要求提供登录用户名和密码，以便验证操作机器或通过网络访问机器的用户。



CZB010

1. 用户

用户在机器上可以执行复印和打印等普通操作。

2. 群组

群组在机器上执行复印和打印等普通操作。

3. 未经授权的用户

4. 未经授权的访问

配置用户验证

用户验证方法有 4 种：用户代码验证、基本验证、Windows 验证和 LDAP 验证。要使用用户验证，请从控制面板上选择一种验证方法，然后为该验证进行必需的设置。具体设置视验证方法而定。指定管理员验证，然后指定用户验证。

★重要信息

- 如果由于硬盘或网络故障而无法启用用户验证，则可以通过这种方式使用机器：通过管理员验证访问机器，然后禁用用户验证。例如，在您需要紧急使用机器时就可以这样做。
- 您不能同时使用多种验证方法。

用户验证配置流程

配置步骤	详细信息
配置管理员验证	p.14 “指定管理员权限” p.16 “注册和更改管理员”
配置用户验证	指定用户验证。 总共有 4 种类型的用户验证： • p.29 “用户代码验证” • p.31 “基本验证” • p.35 “Windows 验证” • p.43 “LDAP 验证”

用户验证方法

类型	详细信息
用户代码验证	使用八位数字用户代码进行验证。针对每个用户代码进行验证，而不是针对每个用户。 必须提前在机器的通讯簿中注册用户代码。
基本验证	使用机器的通讯簿进行验证。 必须提前在机器的通讯簿中注册用户。 可针对每个用户进行验证。
Windows 验证	在机器所在的同一网络中，使用 Windows 服务器的域控制器执行验证。 可针对每个用户进行验证。

类型	详细信息
LDAP 验证	在机器所在的同一网络中，使用 LDAP 服务器执行验证。 可针对每个用户进行验证。

在扫描仪模式下发送电子邮件以防止身份欺诈时，通过 Windows 或 LDAP 验证获得的用户电子邮件地址可用作发件人的固定地址（“发件人”）。

如果中途切换用户验证方法

- 如果使用不超过 8 位的用户代码帐户来进行用户代码验证，则即使验证方法已由用户代码验证切换为基本验证、Windows 验证或 LDAP 验证，该用户代码帐户也可继续用作登录用户名。此时，由于用户代码验证没有密码，因此登录密码设置为空白。
- 切换为外部验证方法（Windows 验证或 LDAP 验证）时，除非外部验证设备已提前注册了相应用户代码帐户，否则无法启用验证。但是，即使无法完成验证，用户代码帐户也会保存在机器的通讯簿中。
- 为安全起见，当从用户代码验证切换至其他验证方法时，建议您删除不用的帐户，或设置一个登录密码。有关删除帐户的详细信息，请参见《连接机器/系统设置》中的“删除注册名”。有关更改密码的详细信息，请参见 p.33 “指定登录用户名和密码”。

↓ 注

- 打开主电源后，扩展功能可能不会出现在用户验证管理菜单的用户验证项目列表中。如果发生这种情况，请稍等片刻，然后再次打开用户验证管理菜单。
- 用户验证也可通过 Web Image Monitor 来指定。有关详细信息，请参见 Web Image Monitor 帮助。

用户代码验证

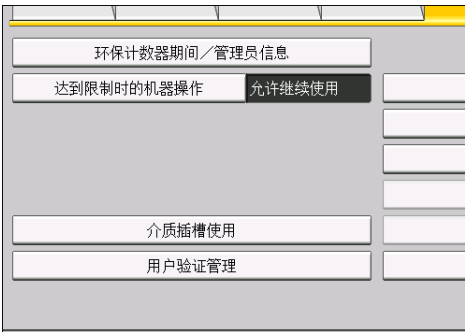
此验证方法是一种根据用户代码来限制对功能进行访问的验证方法。多个用户可以使用同一用户代码。

有关指定用户代码的详细信息，请参见《连接机器/系统设置》中的“注册用户代码”。

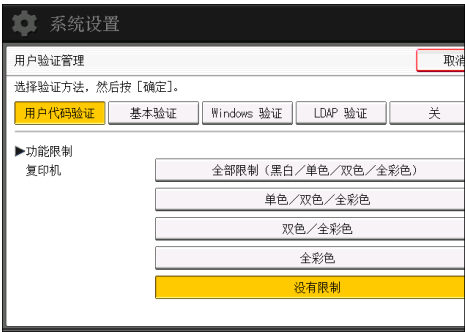
有关在打印机驱动程序或 TWAIN 驱动程序中指定用户代码的详细信息，请参见驱动程序帮助。

2

- 1. 以机器管理员身份从控制面板中登录。
- 2. 按[系统设置]。
- 3. 按[管理员工具]。
- 4. 按[▼向后]。
- 5. 按[用户验证管理]。



- 6. 选择[用户代码验证]。
- 如果您不想启用用户验证，请选择[关]。
- 7. 在“功能限制”中，选择要限制的功能。



如果没有显示您要选择的功能，请按[▼向后]。

选定的功能将执行用户代码验证。用户代码验证不会应用到没有选定的功能。

有关为个人或群组限制可用功能的详细信息，请参见 p.62 “限制可使用的功能”。

8. 要指定打印机作业验证，请在“功能限制”下为“打印机”选择[PC 控制]之外的项目。

如果项目未显示，请按[▼向后]。

如果您不想指定打印机作业验证，请转到步骤 14。

9. 按[▼向后]。

10. 选择“打印机作业验证”等级。

有关打印机作业验证级别的说明，请参见 p.48 “打印机作业验证”。

如果您选择了[全部]或[简单（全部）]，请转到步骤 14。

如果您选择了[简单（限制）]，请转到步骤 11。

11. 按“限制范围”对应的[更改]。

12. 指定将[简单（限制）]应用于“打印机作业验证”的范围。



您可以指定应用此设置的 IPv4 地址范围。

13. 按[退出]。

14. 按[确定]。

15. 按[登录/注销]键。

将出现确认信息。如果按[是]，将自动注销。

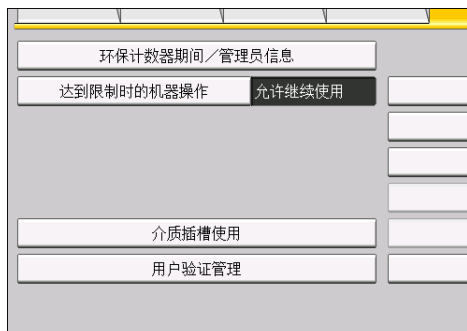
基本验证

使用机器的通讯簿验证每位用户时请指定此验证方法。使用基本验证时，不仅可以管理机器的可用功能，还可以限制对保存文件和通讯簿的访问。在基本验证下，管理员必须指定可供通讯簿中注册的每位用户使用的功能。有关如何限制功能的详细信息，请参见 p.32 “通讯簿中保存的验证信息”。

指定基本验证

配置机器之前，请确保在“管理员验证管理”下正确配置了管理员验证。

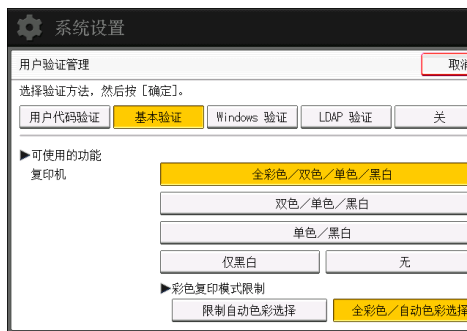
1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[▼向后]。
5. 按[用户验证管理]。



6. 选择[基本验证]。

如果您不想启用用户验证，请选择[关]。

7. 在“可使用的功能”中，选择要允许使用的机器功能。



如果没有显示您要选择的功能，请按[▼向后]。

在此处选择的功能将成为默认的基本验证设置，这些设置会分配给通讯簿中的所有新用户。

有关为个人或群组指定可使用的功能的详细信息，请参见 p.62 “限制可使用的功能”。

8. 按[▼向后]。

9. 选择“打印机作业验证”等级。

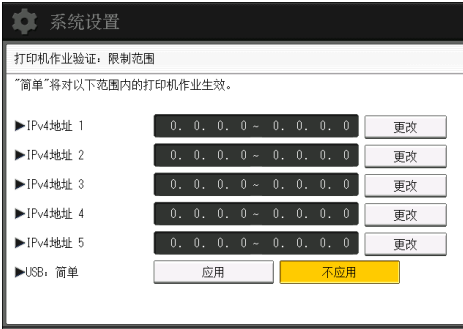
有关打印机作业验证级别的说明，请参见 p.48 “打印机作业验证”。

如果您选择了[全部]或[简单（全部）]，请转到步骤 13。

如果您选择了[简单（限制）]，请转到步骤 10。

10. 按“限制范围”对应的[更改]。

11. 指定将[简单（限制）]应用于“打印机作业验证”的范围。



您可以指定应用此设置的 IPv4 地址范围。

12. 按[退出]。

13. 按[确定]。

14. 按[登录/注销]键。

将出现确认信息。如果按[是]，将自动注销。

通讯簿中保存的验证信息

如果已启用用户验证，则可以为每个用户或用户组指定机器功能的访问限制和使用限制。指定通讯簿中每个用户条目所需的设置。有关可以限制的功能的详细信息，请参见 p.62 “限制可使用的功能”。

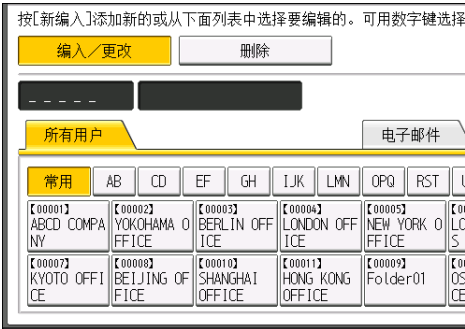
用户必须具有已在通讯簿中注册的帐户，才能在指定用户验证时使用机器。有关通讯簿中的用户注册的详细信息，请参见《连接机器/系统设置》中的“注册用户信息”。

用户验证也可通过 Web Image Monitor 来指定。有关详细信息，请参见 Web Image Monitor 帮助。

指定登录用户名和密码

在“通讯簿管理”中，指定要用于“用户验证管理”的登录用户名和密码。
有关可用于登录用户名和密码的字符，请参见 p.17 “可用于用户名和密码的字符”。

- 1. 以用户管理员身份从控制面板中登录。
- 2. 按[通讯簿管理]。
- 3. 选择用户。



- 4. 按[验证信息]。



- 5. 按“登录用户名”所对应的[更改]。
- 6. 输入登录用户名，然后按[确定]。
- 7. 按“登录密码”所对应的[更改]。
- 8. 输入登录密码，然后按[确定]。
- 9. 再次输入登录密码进行确认，然后按[确定]。
- 10. 按[确定]。
- 11. 按[退出]。
- 12. 注销。

指定登录详细信息

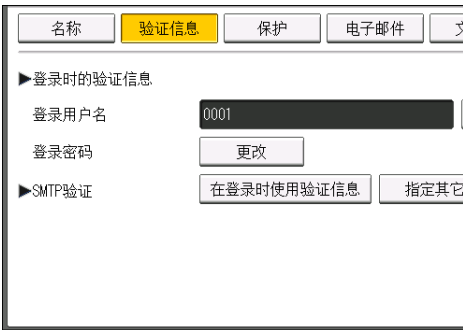
“通讯簿管理”中指定的登录用户名和密码可用作“SMTP 验证”、“文件夹验证”和“LDAP 验证”的登录信息。

如果您不想将“通讯簿管理”中指定的登录用户名和密码用于“SMTP 验证”、“文件夹验证”或“LDAP 验证”，请参见《连接机器/系统设置》中的“注册文件夹”和“注册 SMTP 和 LDAP 验证”。

★重要信息

- 将“在登录时使用验证信息”用于“SMTP 验证”、“文件夹验证”或“LDAP 验证”时，必须指定除“other”、“admin”、“supervisor”或“HIDE***”之外的用户名。符号“***”代表任意字符。

1. 以用户管理员身份从控制面板中登录。
2. 按[通讯簿管理]。
3. 选择用户。
4. 按[验证信息]。
5. 在“SMTP 验证”中选择[在登录时使用验证信息]。



对于文件夹验证，请在“文件夹验证”中选择[在登录时使用验证信息]。

对于 LDAP 验证，请在“LDAP 验证”中选择[在登录时使用验证信息]。

如果没有显示您要选择的功能，请按[▼向后]。

6. 按[确定]。
7. 按[退出]。
8. 注销。

Windows 验证

使用 Windows 域控制器验证在目录服务器上有自己帐户的用户时，请指定此验证方法。如果用户在目录服务器上没有自己的帐户，就无法对其进行验证。在 Windows 验证下，您可以为目录服务器中注册的每个群组指定访问限制。可将保存在目录服务器中的通讯簿注册到机器中，这样不必先使用机器在通讯簿中注册各项设置，就可进行用户验证。

您首次访问机器时，可使用所在群组可以使用的功能。如果未在组中注册，则可以使用“*默认群组”下的可用功能。要限制仅某些用户可使用的功能，请事先在通讯簿中进行设置。

要在 Windows 验证下自动注册用户信息，建议使用 SSL 对机器和域控制器之间的通信进行加密。为此，您必须创建域控制器的服务器证书。有关创建服务器证书的详细信息，请参见 p.42 “创建服务器证书”。

★重要信息

- 如果您使用 Windows 验证，则在目录服务器中注册的用户信息会自动在机器的通讯簿中注册。即使在机器上编辑了自动注册在机器通讯簿中的用户信息，执行验证时也会被目录服务器中的信息覆盖。
- 在其他域中管理的用户须接受用户验证，但他们无法获取用户名等项目。
- 如果同时设置了 Kerberos 验证和 SSL 加密，则无法获取电子邮件地址。
- 如果您在域控制器中创建了新用户，并且在配置密码时选择了“用户下次登录时须更改密码”，请首先登录到计算机并更改密码。
- 如果在本机上选择了 Kerberos 验证，但验证服务器仅支持 NTLM 验证，则验证方法会自动切换为 NTLM。
- 如果在 Windows 服务器上启用了“来宾”帐户，未在域控制器中注册的用户也会通过验证。启用此帐户后，用户将在通讯簿中注册，并可使用“*默认群组”下的可用功能。

Windows 验证可使用这两种验证方法中的一种执行：NTLM 或 Kerberos 验证。下面列出了这两种方法的执行要求：

NTLM 验证的操作要求

要指定 NTLM 验证，必须满足以下要求：

- 本机支持 NTLMv1 验证和 NTLMv2 验证。
- 在要使用的域中创建域控制器。
- 以下所列操作系统支持此功能。要在运行 Active Directory 时获取用户信息，请使用 LDAP。如果您使用的是 LDAP，我们建议您使用 SSL 来对机器和 LDAP 服务器之间的通信进行加密。只有在 LDAP 服务器支持 TLSv1 或 SSLv3 时，才能使用 SSL 进行加密。
 - Windows Server 2003/2003 R2
 - Windows Server 2008/2008 R2
 - Windows Server 2012/2012 R2

Kerberos 验证的操作要求

要指定 Kerberos 验证，必须满足以下要求：

- 在要使用的域中创建域控制器。
- 操作系统必须支持 KDC（密钥分发中心）。要在运行 Active Directory 时获取用户信息，请使用 LDAP。如果您使用的是 LDAP，我们建议您使用 SSL 来对机器和 LDAP 服务器之间的通信进行加密。只有在 LDAP 服务器支持 TLSv1 或 SSLv3 时，才能使用 SSL 进行加密。下面列出了兼容的操作系统：
 - Windows Server 2003/2003 R2
 - Windows Server 2008/2008 R2
 - Windows Server 2012/2012 R2

要在 Windows Server 2008 中使用 Kerberos 验证，请安装 Service Pack 2 或更高版本。

- 如果启用了 Kerberos 验证，则系统会对机器和 KDC 服务器之间的数据传输进行加密。有关指定加密传输的详细信息，请参见 p.146 “Kerberos 验证加密设置”。

注

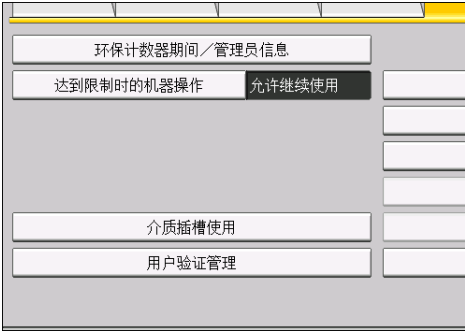
- 有关可用于登录用户名和密码的字符，请参见 p.17 “可用于用户名和密码的字符”。
- 随后访问机器时，您可使用所在群组及您个人可用的所有功能。
- 在多个群组中注册的用户可以使用这些群组的所有可用功能。
- 在 Windows 验证下，无需创建服务器证书，但希望使用 SSL 自动注册用户名等用户信息时除外。

指定 Windows 验证

配置机器之前，请确保在“管理员验证管理”下正确配置了管理员验证。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[▼向后]。

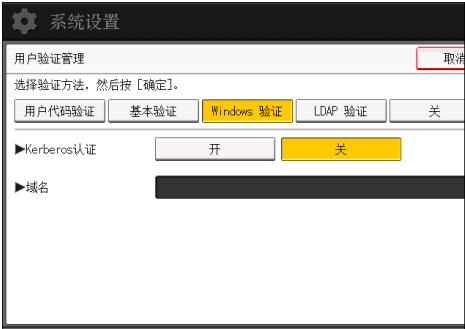
5. 按[用户验证管理]。



6. 选择[Windows 验证]。

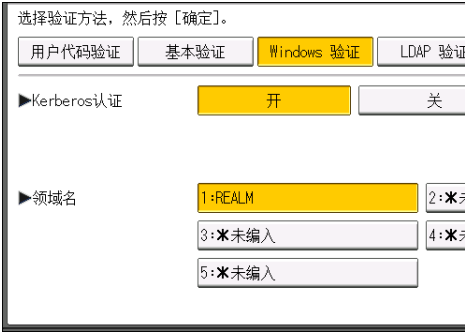
如果您不想启用用户验证，请选择[关]。

7. 如果想要使用 Kerberos 认证，请按[开]。



如果想要使用 NTLM 验证，请按[关]并转至步骤 9。

8. 选择 Kerberos 验证领域并转至步骤 10。



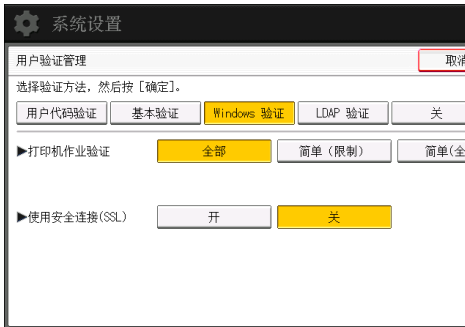
要启用 Kerberos 认证，必须预先注册领域。领域名必须以大写字母进行注册。有关注册领域的详细信息，请参见《连接机器/系统设置》中的“编入领域”。

最多可注册 5 个领域。

9. 按“域名”所对应的[更改]，输入要验证的域控制器名称，然后按[确定]。

10. 按[▼向后]。

11. 选择“打印机作业验证”等级。

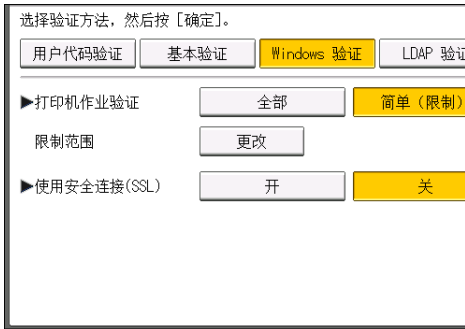


有关打印机作业验证等级的说明，请参见 p.48 “打印机作业验证”。

如果您选择了[全部]或[简单(全部)]，请转到步骤 15。

如果您选择了[简单(限制)]，请转到步骤 12。

12. 按[更改]。



13. 指定将[简单（限制）]应用于“打印机作业验证”的范围。



您可以指定应用此设置的 IPv4 地址范围。

14. 按[退出]。

15. 按“使用安全连接(SSL)”所对应的[开]。

如果没有为验证使用安全套接字层(SSL)，请按[关]。

如果您尚未注册全局群组，请转到步骤 22。

如果您已注册了全局群组，请转到步骤 16。

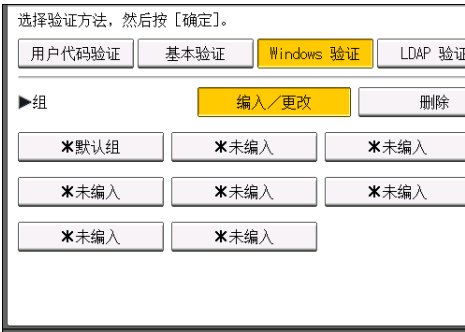
如果在 Windows 服务器下注册了全局群组，您可以限制每个全局群组的可用功能。

您需要事先在 Windows 服务器中创建全局群组，并在每个群组中注册要验证的用户。您还需要在机器中注册可供全局群组成员使用的功能。在机器中创建全局群组，方法是输入在 Windows 服务器中注册的全局群组名称。（请注意，群组名称区分大小写。）然后，指定各个群组可用的机器功能。

如果未指定全局群组，用户可以使用[*默认组]中指定的功能。如果指定了全局群组，未在全局群组中注册的用户可以使用[*默认组]中指定的功能。默认情况下，*默认群组成员可以使用所有功能。根据用户需要指定对可用功能的限制。

16. 按[▼向后]。

17. 在“群组”下按[编入／更改]，然后按[*未编入]。



18. 按“组名称”的[更改]，然后输入组名称。

19. 按[确定]。

20. 在“可使用的功能”中，选择您要允许使用机器的哪些功能。



如果没有显示您要选择的功能，请按[▼向后]。

Windows 验证将应用于选定的功能。

用户仅能使用选定的功能。

有关为个人或群组指定可使用的功能的详细信息，请参见 p.62 “限制可使用的功能”。

21. 按[确定]。

22. 按[确定]。

23. 按[登录/注销]键。

将出现确认信息。如果按[是]，将自动注销。

安装 Internet 信息服务 (IIS) 和证书服务

如果要机器自动获取在活动目录中注册的用户信息，则指定此设置。

建议您将 Internet 信息服务 (IIS) 和证书服务作为 Windows 组件进行安装。

安装组件，然后创建服务器证书。

如果它们未安装，请按如下方式进行安装：

Windows Server 2008 R2 下的安装

1. 在[开始]菜单中，指向[管理工具]，然后单击[服务管理器]。

2. 单击左列中的[角色]，然后在[操作]菜单中单击[添加角色]。

3. 单击[下一步>]。

4. 选择“Web 服务器 (IIS)”和“Active Directory 证书服务”复选框，然后单击[下一步>]。

如果出现确认信息，请单击[添加特性]。

5. 阅读内容信息，然后单击[下一步>]。

6. 确认已选择[证书授权机构]，然后单击[下一步>]。

7. 选择[企业]，然后单击[下一步>]。

8. 选择[根 CA]，然后单击[下一步>]。

9. 选择[新建私钥]，然后单击[下一步>]。

10. 选择加密服务提供程序、密钥长度和哈希算法，以创建新的私钥，然后单击[下一步>]。

11. 在“此 CA 的普通名称：”中，输入证书机构名称，然后单击[下一步>]。

12. 选择有效期，然后单击[下一步>]。

13. 将“证书数据库位置：”和“证书数据库日志位置：”设置为默认值，然后单击[下一步>]。

14. 阅读注意事项，然后单击[下一步>]。

15. 选择要使用的角色服务，然后单击[下一步>]。

16. 单击[安装]。
17. 完成安装以后，单击[关闭]。
18. 关闭[服务器管理器]。

Windows Server 2012 下的安装

2

1. 在“开始”屏幕上，单击[服务器管理器]。
2. 在[管理]菜单上，单击[添加角色和功能]。
3. 单击[下一步>]。
4. 选择[基于角色或基于功能的安装]，然后单击[下一步>]。
5. 选择服务器，然后单击[下一步>]。
6. 选择“Active Directory 证书服务”和“Web 服务器 (IIS)”复选框，然后单击[下一步>]。
如果出现确认信息，请单击[添加特性]。
7. 检查要安装的功能，然后单击[下一步>]。
8. 阅读内容信息，然后单击[下一步>]。
9. 确保在[Active Directory 证书服务]的[角色服务]区域中选定了[证书颁发机构]，然后单击[下一步>]。
10. 阅读内容信息，然后单击[下一步>]。
11. 检查要安装在[Web 服务器 (IIS)]下的角色服务，然后单击[下一步>]。
12. 单击[安装]。
13. 完成安装后，请单击服务器管理器的通知图标，然后单击[配置目标服务器上的 Active Directory 证书服务]。
14. 单击[下一步>]。
15. 在[角色服务]区域中单击[证书颁发机构]，然后单击[下一步>]。
16. 选择[企业 CA]，然后单击[下一步>]。
17. 选择[根 CA]，然后单击[下一步>]。
18. 选择[新建私钥]，然后单击[下一步>]。
19. 选择加密提供程序、密钥长度和哈希算法，以创建新的私钥，然后单击[下一步>]。
20. 在“此 CA 的普通名称:”中，输入证书机构名称，然后单击[下一步>]。
21. 选择有效期，然后单击[下一步>]。
22. 将“证书数据库位置:”和“证书数据库日志位置:”设置为默认值，然后单击[下一步>]。
23. 单击[配置]。
24. 如果出现“配置成功”信息，请单击[关闭]。

创建服务器证书

安装 Internet 信息服务 (IIS) 和证书服务 Windows 组件后，按如下方式创建服务器证书：

本文使用了 Windows Server 2008 R2 来说明具体的步骤。

2

1. 在[开始]菜单上，指向[管理工具]，然后单击[Internet 信息服务 (IIS) 管理器]。
在 Windows Server 2012 下，在“开始”屏幕上单击[Internet 信息服务 (IIS) 管理器]。
出现确认信息时，单击[是]。
2. 在左列中，单击服务器名称，然后双击[服务器证书]。
3. 在右列中，单击[创建证书请求...]。
4. 输入全部信息，然后单击[下一步]。
5. 在“加密服务提供者：”中，选择提供者，然后单击[下一步]。
6. 单击[...], 然后为证书请求指定文件名。
7. 指定保存文件的位置，然后单击[打开]。
8. 单击[完成]，关闭[Internet 信息服务 (IIS) 管理器]。

LDAP 验证

使用 LDAP 服务器验证在 LDAP 服务器上有自己帐户的用户时，请指定此验证方法。如果用户在 LDAP 服务器上没有自己的帐户，就无法对其进行验证。可将保存在 LDAP 服务器中的通讯簿注册到机器中，这样不必先使用机器在通讯簿中注册各项设置，就可进行用户验证。使用 LDAP 验证时，为防止密码信息以未加密形式在网络上发送，建议使用 SSL 对机器和 LDAP 服务器之间的通信进行加密。您可在 LDAP 服务器上指定是否启用 SSL。为此，必须创建 LDAP 服务器的服务器证书。有关创建服务器证书的详细信息，请参见 p.42 “创建服务器证书”。可以在 LDAP 服务器设置中指定 SSL 设置。

使用 Web Image Monitor，可以启用相关功能以检查 SSL 服务器是否可以信任。有关使用 Web Image Monitor 指定 LDAP 验证的详细信息，请参见 Web Image Monitor 帮助。

选择明文验证时，将会启用 LDAP 简化验证。可使用用户属性（例如 cn 或 uid）而非 DN 来执行简化验证。

要为 LDAP 验证启用 Kerberos，必须预先注册领域。领域必须以大写字母配置。有关注册领域的详细信息，请参见《连接机器/系统设置》中的“编入领域”。

★重要信息

- 如果您使用 LDAP 验证，则在 LDAP 服务器中注册的用户信息会自动在机器的通讯簿中注册。即使在机器上编辑自动注册在机器通讯簿中的用户信息，执行验证时也会被 LDAP 服务器中的信息覆盖。
- 在 LDAP 验证下，您无法为目录服务器中注册的组指定访问限制。
- 输入登录用户名或密码时，请勿使用日文、繁体中文、简体中文或韩文双字节字符。如果使用双字节字符，将无法使用 Web Image Monitor 进行验证。
- 如果同时设置了 Kerberos 验证和 SSL，则在 LDAP 验证中使用 Active Directory 时，系统将无法获取用户信息。
- 使用 LDAP 验证时，如果 LDAP 服务器设置中的“匿名验证”未设置为“禁止”，没有 LDAP 服务器帐户的用户可能仍可访问该服务器。
- 如果使用 Windows Active Directory 配置 LDAP 服务器，或许“匿名验证”可以使用。如果 Windows 验证可用，我们建议您使用它。

LDAP 验证的运行要求

要指定 LDAP 验证，必须满足以下要求：

- 请配置网络，以便机器可以检测到 LDAP 服务器。
- 使用 SSL 时，TLSv1 或 SSLv3 可在 LDAP 服务器上运行。
- 在机器上注册 LDAP 服务器。
- 要注册 LDAP 服务器，请指定以下设置：
 - 服务器名称
 - 搜索起始位置

- 端口号
- SSL 通信
- 验证
选择 Kerberos、DIGEST 或明文验证。

- 用户名
如果 LDAP 服务器支持“匿名验证”，则不必输入用户名。

- 密码
如果 LDAP 服务器支持“匿名验证”，则无需输入密码。

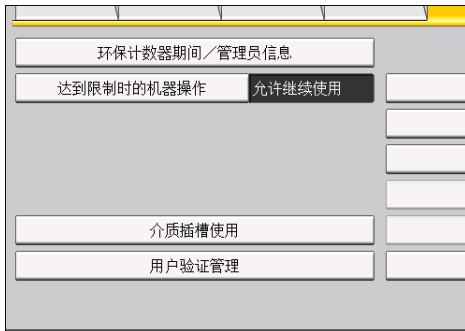
有关注册 LDAP 服务器的详细信息，请参见《连接机器/系统设置》中的“编入 LDAP 服务器”。

↓ 注

- 有关可用于登录用户名和密码的字符，请参见 p.17 “可用于用户名和密码的字符”。
- 在 LDAP 简单验证模式下，如果密码留空，则验证将失败。要使用空密码，请与服务代表联系。
- 未注册用户指定 LDAP 验证后首次访问机器时，该用户将在机器中进行注册，并且可以在 LDAP 验证过程中使用“可使用的功能”下提供的功能。要限制每位用户的可用功能，请在通讯簿中注册各个用户及相应的“可用功能”设置，或指定每位注册用户的“可用功能”。“可用功能”设置将在用户访问机器时启用。
- 如果启用了 Kerberos 验证，则系统会对机器和 KDC 服务器之间的数据传输进行加密。有关指定加密传输的详细信息，请参见 p.146 “Kerberos 验证加密设置”。

配置机器之前，请确保在“管理员验证管理”下正确配置了管理员验证。

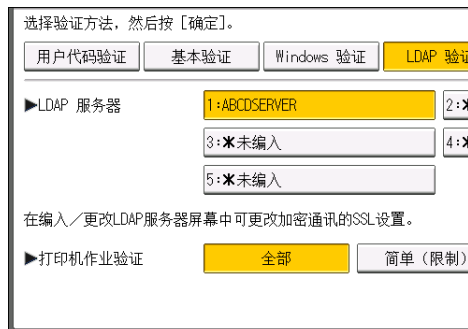
1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理工具]。
4. 按[▼向后]。
5. 按[用户验证管理]。



6. 选择[LDAP 验证]。

如果您不想启用用户验证，请选择[关]。

7. 选择要用于 LDAP 验证的 LDAP 服务器。



选择验证方法，然后按 [确定]。

用户代码验证 基本验证 Windows 验证 **LDAP 验证**

▶LDAP 服务器

1: ABCDSERVER 2: *

3: *未编入 4: *

5: *未编入

在编入/更改LDAP服务器屏幕中可更改加密通讯的SSL设置。

▶打印机作业验证

全部 简单(限制)

8. 选择“打印机作业验证”等级。

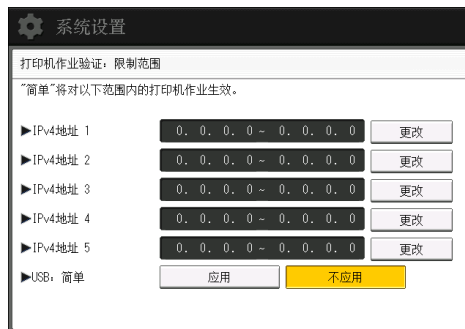
有关打印机作业验证级别的说明，请参见 p.48 “打印机作业验证”。

如果您选择了[全部]或[简单（全部）]，请转到步骤 12。

如果您选择了[简单（限制）]，请转到步骤 9。

9. 按“限制范围”对应的[更改]。

10. 指定将[简单（限制）]应用于“打印机作业验证”的范围。



系统设置

打印机作业验证 限制范围

“简单”将对以下范围内的打印机作业生效。

▶IPv4地址 1 0. 0. 0. 0 ~ 0. 0. 0. 0 更改

▶IPv4地址 2 0. 0. 0. 0 ~ 0. 0. 0. 0 更改

▶IPv4地址 3 0. 0. 0. 0 ~ 0. 0. 0. 0 更改

▶IPv4地址 4 0. 0. 0. 0 ~ 0. 0. 0. 0 更改

▶IPv4地址 5 0. 0. 0. 0 ~ 0. 0. 0. 0 更改

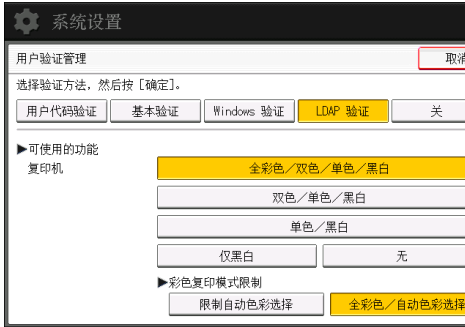
▶USB: 简单 应用 不应用

您可以指定应用此设置的 IPv4 地址范围。

11. 按[退出]。

12. 按[▼向后]。

13. 在“可使用的功能”中，选择要允许使用的机器功能。



如果没有显示您要选择的功能，请按[▼向后]。

LDAP 验证将应用于选定的功能。

用户仅能使用选定的功能。

有关为个人或群组指定可使用的功能的详细信息，请参见 p.62 “限制可使用的功能”。

14. 按[▼向后]。

15. 按“登录名属性”所对应的[更改]。

16. 输入登录名属性，然后按[确定]。

使用登录名属性作为搜索条件，以获取有关已通过验证用户的信息。您可以基于登录名属性创建搜索过滤器，再选择用户，然后从 LDAP 服务器中检索用户信息，以便该信息传送到机器的通讯簿中。

要指定多个登录属性，请用逗号（,）分隔各属性。搜索将返回满足一或两个属性的结果。

此外，如果在两个登录属性之间放置等号（=）（例如：cn=abcde、uid=xyz），搜索将仅返回匹配该属性的结果。指定明文验证时也可应用此搜索功能。

使用 DN 格式进行验证时，不需要注册登录属性。

选择用户名的方法视服务器环境而定。检查服务器环境并相应地输入用户名。

17. 按“唯一属性”所对应的[更改]。

18. 输入唯一属性，然后按[确定]。

在机器上指定唯一属性，以将 LDAP 服务器中的用户信息与机器中的用户信息进行匹配。通过执行此操作，如果 LDAP 服务器中注册用户与机器中注册用户的唯一属性匹配，则系统会将这两个实例视为相同用户处理。

您可输入诸如“序列号”或“用户识别名”之类的属性。此外，如果“cn”或“雇员号”是唯一的，也可以将其输入。如果不指定唯一属性，则系统将在机器中创建用户信息相同但登录用户名不同的帐户。

19. 按[确定]。

20. 按[登录/注销]键。

将出现确认信息。如果按[是]，将自动注销。

打印机作业验证

打印机作业验证是一种使用户验证能够应用于打印作业的功能。

PCL 和 PostScript3 驱动程序都支持用户验证。PostScript3 驱动程序仅支持用户代码验证。

打印机作业验证级别

“全部”的安全等级最高，之后是“简单（限制）”，最后是“简单（全部）”。

- 全部

选择此选项可验证所有打印作业和远程设置。

机器验证所有打印机作业和远程设置，并取消验证失败的作业和设置。

要在不支持验证的环境中进行打印，请选择[简单（全部）]或[简单（限制）]。

- 简单（限制）

选择此选项可限制[简单（全部）]的范围。

无论验证功能如何，您都可以打印指定的范围。验证将被应用于此范围以外的地址。

您可指定是否将[简单（全部）]应用于用户的 IPv4 地址。可从 Web Image Monitor 中配置 IPv6 地址的应用范围。

- 简单（全部）

如果想要使用机器无法识别的打印机驱动程序或设备进行打印，或者如果不需要经过验证进行打印的话，请选择此选项。

无验证信息的打印机作业和设置无需验证即可执行。

机器对具有验证信息的打印机作业和远程设置进行验证，并取消验证失败的作业和设置。

由于系统允许在不进行用户验证的情况下而直接打印，因此未经授权的用户可以使用机器。

打印机作业类型

视打印机作业验证级别和打印机作业类型的组合而定，机器可能无法正确打印。根据运行环境设置相应的组合。

禁用用户验证时，所有作业类型都可以进行打印。

打印机作业类型：在以下情况下，系统会指定打印机作业：

1. 在 PCL 打印机驱动程序或 PCL 通用驱动程序中选中了[用户验证]复选框。
2. 在 PCL 微型驱动程序*中选择了[用户验证]和[With Encryption]复选框。

* 验证功能无法与 IA-64 操作系统搭配使用。

3. 在 PCL 微型驱动程序中选中了[用户验证]复选框。
4. 没有在 PCL 打印机驱动程序或 PCL 微型驱动程序*中选中[用户验证]复选框。

* 验证功能无法与 IA-64 操作系统搭配使用。

5. 使用 PostScript 3 打印机驱动程序或 PS3 通用驱动程序输入了用户代码。

使用不支持验证的 PCL 打印机驱动程序进行恢复/并行打印时也是如此。

6. 没有使用 PostScript 3 打印机驱动程序或 PS3 通用驱动程序输入用户代码。使用不支持验证的 PCL 打印机驱动程序进行恢复/并行打印时也是如此。
7. 打印机作业或 PDF 文件从没有打印机驱动程序的主机发出，并通过 LPR 进行打印。
8. PDF 文件通过 ftp 打印。个人验证使用通过 ftp 登录时所用的用户 ID 和密码来执行。不过，用户 ID 和密码不会加密。

打印机作业验证级别和打印机作业类型

打印机作业验证：驱动程序加密密钥：密钥强度	简单（全部）：简单加密	简单（全部）：DES	简单（全部）：AES	全部：简单加密	全部：DES	全部：AES
打印机作业类型 1	C*1	C*1	C*1	C*1	C*1	C*1
打印机作业类型 2	C*1	C*1	X*1	C*1	C*1	X*1
打印机作业类型 3	B	X*1	X*1	B	X*1	X*1
打印机作业类型 4	X	X	X	X	X	X
打印机作业类型 5	A	A	A	B	B	B
打印机作业类型 6	A	A	A	X	X	X
打印机作业类型 7	A	A	A	X	X	X
打印机作业类型 8	B	B	B	B	B	B

*1 通过用户代码验证执行的打印分类为 B。

A: 无论用户验证为何, 都可进行打印。

B: 如果用户验证成功, 可进行打印。如果用户验证失败, 将重置打印作业。

C: 如果用户验证成功, 并且打印机驱动程序和机器的“驱动程序加密密钥”匹配, 则可以进行打印。

X: 无论用户验证为何, 都无法进行打印, 并且会重置打印作业。

↓ 注

- 有关“驱动程序加密密钥: 密钥强度”的详细信息, 请参见 p.225 “指定扩展安全功能”。

“authfree” 命令

如果在打印机作业验证下选择[简单 (限制)], 则 telnet authfree 命令可用来指定打印机作业验证的例外情况。

有关用于登录 telnet 的登录用户名和密码的信息, 请向管理员咨询。有关登录到 telnet 和使用 telnet 的详细信息, 请参见《连接机器/系统设置》中的“使用 telnet 进行远程维护”。

查看设置

```
msh> authfree
```

如果不指定打印作业验证排除, 不会显示验证排除控制。

IPv4 地址设置

```
msh> authfree "ID" range "start-address" "end-address"
```

IPv6 地址设置

```
msh> authfree "ID" range6 "start-address" "end-address"
```

IPv6 地址掩码设置

```
msh> authfree "ID" mask6 "base-address" "masklen"
```

验证排除控制初始化

```
msh> authfree flush
```

↓ 注

- 在 IPv4 和 IPv6 环境中, 最多可注册和选择 5 个访问范围。

自动注册到通讯簿

对于通过 Windows 或 LDAP 验证登录的用户，其个人信息将自动注册到通讯簿中。通过复制其他注册用户的信息，您可以指定任何其他信息。

自动注册的通讯簿项目

2

- 登录用户名
- 登录密码
- 注册号码
- 名称^{*1}
- 主要显示^{*1}
- 电子邮件地址^{*2}
- 保护文件
用户／组的权限^{*3}

*1 如果无法获取此信息，则在此字段中注册登录用户名。

*2 如果无法获取此信息，则不能自动注册。

*3 如果[地址簿自动编入的数据保留设置]设置为[保留数据]，则系统会优先使用它。

↓ 注

- 执行自动注册时，如果通讯簿中注册的数据量已达到限额，您可以自动删除旧的用户帐户。有关详细信息，请参见 p.224 “管理通讯簿”。

地址簿自动编入的数据保留设置

您可以从已注册用户那里复制没有自动注册到通讯簿中的信息，然后注册这些信息。

1. 以用户管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。

4. 按[地址簿自动编入的数据保留设置]。

	地址簿自动编入的数据保留设置
	自动删除通讯簿中的用户 关
	删除通讯簿中的所有数据
	显示/打印计数器
	显示/清除/打印每个用户的计数器
	显示/清除环保计数器
通讯簿	每个用户显示/清除环保计数器
1 / 5 ▲ 向前 ▼ 向后	

5. 按[保留数据]。

6. 使用数字键输入要应用指定设置的通讯簿注册号码，然后按[#]。

7. 按[确定]。

8. 按[登录/注销]键。

将出现确认信息。如果按[是]，将自动注销。

用户锁定功能

如果多次输入不正确的密码，用户锁定功能会阻止以同一登录用户名做进一步的登录尝试。即使已锁定的用户后来输入了正确的密码，验证仍将失败，并且机器将无法使用，直到锁定期结束或管理员或超级用户禁用锁定功能为止。

要使用锁定功能进行用户验证，必须将验证方法设置为基本验证。使用其他验证方法时，锁定功能仅保护超级用户和管理员帐户，而不保护一般用户帐户。

锁定设置项目

可以使用 Web Image Monitor 进行锁定功能设置。

设置项目	描述	设置值	默认设置
锁定	指定是否启用锁定功能。	- 有效 - 无效	无效
在锁定前尝试的次数	指定在应用锁定前允许进行的验证尝试次数。	1-10	5
锁定解除定时器	指定是否在指定时段结束后取消锁定。	- 有效 - 无效	无效
锁定用户的时间	指定多少分钟后取消锁定。	1-9999 分钟	60 分钟

锁定解除权限

具有解除锁定权限的管理员如下：

已锁定用户	解除锁定管理员
普通用户	用户管理员
用户管理员、网络管理员、文件管理员、机器管理员	超级用户
超级用户	机器管理员

指定用户锁定功能

1. 以机器管理员身份从 Web Image Monitor 登录。

2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[用户锁定策略]。
4. 将“锁定”设置为[有效]。
5. 在下拉菜单中，选择在应用锁定前允许进行的登录尝试次数。
6. 锁定以后，如果要在经过指定的时间后取消锁定，请将“锁定解除定时器”设置为[有效]。
7. 在“锁定用户的时间”字段中，输入多少分钟后禁用锁定。
8. 单击[确定]。
用户锁定策略已设置。
9. 注销。

取消密码锁定

1. 以用户管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[地址簿]。
3. 选择已锁定用户的帐户。
4. 单击[详细输入]，然后单击[更改]。
5. 在“验证信息”下，将“锁定”设置为[无效]。
6. 单击[确定]。
7. 注销。

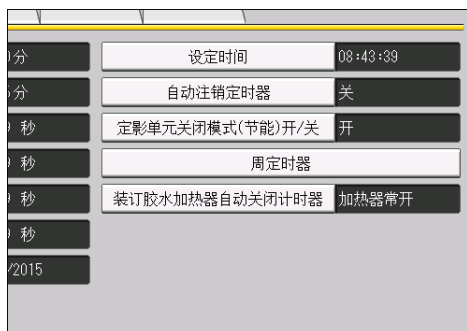
↓ 注

- 您可以通过以下方式取消管理员和超级用户密码锁定：关闭主电源，然后重新打开；或者，使用 Web Image Monitor 在[配置]下的[编入/更改管理员]中取消相关设置。

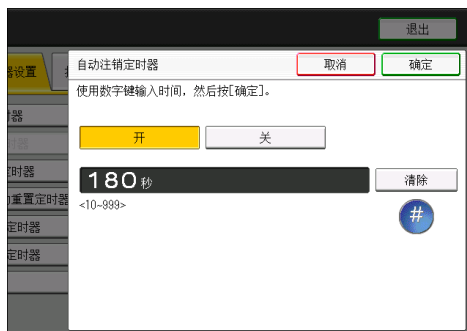
自动注销

登录后，如果您在给定时间内没有使用控制面板，机器会自动将您注销。此功能称为“自动注销”。指定执行“自动注销”前机器等待的时间。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[定时器设置]。
4. 按[自动注销定时器]。



5. 选择[开]。
- 如果您不想指定[自动注销定时器]，请选择[关]。
6. 使用数字键输入“10”到“999”（秒），然后按[#]。



如果操作有误，请按[清除]。

7. 按[确定]。
8. 按[登录/注销]键。

将出现确认信息。如果按[是]，将自动注销。

注

- 您可以在[网页]中指定 Web Image Monitor 的“自动注销”设置。有关详细信息，请参见 Web Image Monitor 的“帮助”。

使用外部设备进行验证

要使用外部设备进行验证，请参见设备手册。

有关详细信息，请联系您的销售代表。

3. 限制机器的使用

本章介绍如何限制用户使用机器。

限制使用目的地列表

在扫描仪功能下，您可以分别限制目的地列表的使用。

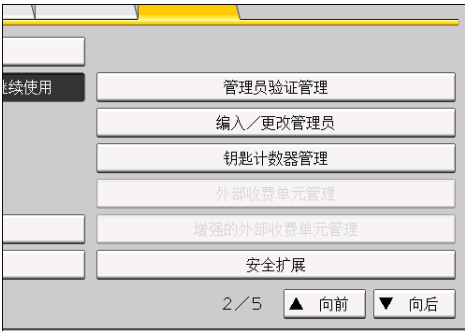
限制目的地的使用

您可以禁止向没有在通讯簿中注册的地址发送扫描文件。通过启用此项，可以禁止用户手动输入相关各方的电子邮件地址或文件夹目的地。

限制添加用户目的地

通过使用[编入地址]，您可以禁止将手动输入用于发送扫描文件的地址注册到通讯簿中。另外，使用此设置时，只有用户管理员可以在通讯簿中注册新用户，以及更改现有注册用户的密码和其他信息。此外，即使您将这些功能设置为[开]，注册为目的地的用户仍然可以更改其密码。只有用户管理员可以更改除密码以外的项目。

- 1. 以用户管理员身份从控制面板中登录。
- 2. 按[系统设置]。
- 3. 按[管理员工具]。
- 4. 按[▼向后]。
- 5. 按[安全扩展]。



- 6. 按[▼向后]。

7. 将“限制目的地的使用”或“限制添加用户目的地”设置为[开]。

选择项目。

▶限制目的地的使用	开 <input checked="" type="button" value="关"/>	▶验证当前作业
		登录权限
▶限制添加用户目的地	开 <input checked="" type="button" value="关"/>	<input checked="" type="button" value="关"/>
		▶密码策略
▶SNMPv1,v2设置	禁止 不禁止	更改

如果您将“限制目的地的使用”设置为[开]，则屏幕上不会出现“限制添加用户目的地”。

8. 按[确定]。

9. 按[登录/注销]键。

将出现确认信息。如果按[是]，将自动注销。

防止更改管理员设置

限制每个管理员可以更改的设置

根据管理员的类型，管理员可以对本机所做的设置会有所不同，这样就使得管理员可以执行的操作范围能够在各个管理员之间进行共享。

本机定义了以下管理员：

- 用户管理员
- 机器管理员
- 网络管理员
- 文件管理员

有关各个管理员可以进行的设置的详细信息，请参见 p.253 “设置的操作权限列表”。
请在使用机器前注册管理员。有关注册管理员的说明，请参见 p.16 “注册和更改管理员”。

禁止用户更改设置

可以禁止用户更改管理员设置。

在“管理员验证管理”的“可用设置”下，选择该项目可以防止此类更改。

有关可以在“可用设置”中选择的项目的详细信息，请参见 p.13 “配置管理员验证”。

指定菜单保护

使用菜单保护，您可以限制“用户工具”菜单中除系统设置外访问该设置的用户权限。无论是否有用户验证，均可使用此设置。要指定菜单保护设置，请提前为机器管理员启用管理员验证。有关如何设置管理员验证的详细信息，请参见 p.13 “配置管理员验证”。有关用户根据菜单保护级别可以指定的设置列表，请参见 p.253 “设置的操作权限列表”。

如果要启用“菜单保护”，请将它设置为[1 级]或[2 级]。选择[2 级]可以对用户访问机器设置的权限施加更加严格的限制。

如果要禁用“菜单保护”，请将它设置为[关]。

3

复印功能

1. 以机器管理员身份从控制面板中登录。
2. 按[复印机/文件服务器特性]。
3. 按[管理工具]。
4. 按[菜单保护]。
5. 选择菜单保护级别，然后按[确定]。
6. 注销。

打印功能

1. 以机器管理员身份从控制面板中登录。
2. 按[打印机特性]。
3. 按[数据管理]。
4. 按[菜单保护]。
5. 选择菜单保护级别，然后按[确定]。
6. 注销。

扫描功能

1. 以机器管理员身份从控制面板中登录。
2. 按[扫描仪特性]。
3. 按[初始的设置]。
4. 按[菜单保护]。
5. 选择菜单保护级别，然后按[确定]。

6. 注销。

防止用户注册/更改程序

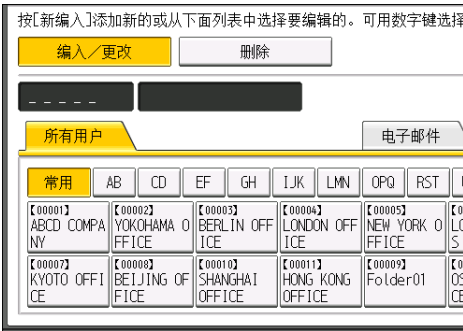
通过启用菜单保护设置，可以防止用户注册或更改程序。启用该设置后，机器管理员可注册和更改程序。

有关注册和更改程序的详细信息，请参见“便捷功能”中的“注册常用功能”。

限制可使用的功能

要防止未经授权的操作，您可以指定允许访问各个机器功能的具体用户。
指定注册用户可以使用的功能。通过配置此项设置，可以限制用户可以使用的功能。
您可以对复印机、文件服务器、扫描仪、打印机功能以及扩展功能的使用加以限制。

1. 以用户管理员身份从控制面板中登录。
2. 按[通讯簿管理]。
3. 选择用户。

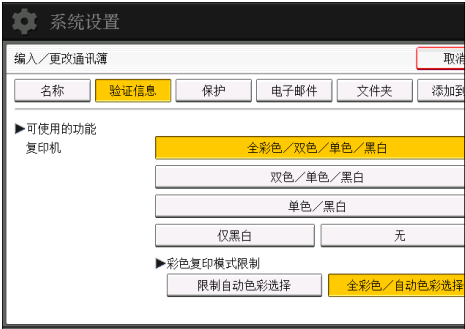


4. 按[验证信息]。



5. 按两次[▼向后]。

6. 在“可使用的功能”中，选择要指定的功能。

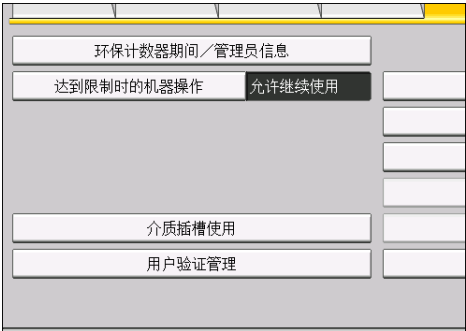


- 如果没有显示您要选择的功能，请按[▼向后]。
7. 按[确定]。
8. 注销。

限制使用介质插槽

在控制面板上指定是否允许用户使用介质插槽。借助该设置，可以限制要保存在移动存储设备上的扫描文件。同时，也可以限制打印移动存储设备上保存的文件。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[▼向后]。
5. 按[介质插槽使用]。



6. 要限制在移动存储设备上保存文件，请在“保存到存储设备”下按[禁止]。
7. 要限制打印移动存储设备上保存的文件，请在“从记忆存储设备打印”下按[禁止]。
8. 按[确定]。
9. 注销。

注

- 如果在“保存到存储设备”下选择[禁止]，则扫描仪功能的保存文件屏幕上不会显示[保存到存储设备]按钮。
- 如果在“从记忆存储设备打印”下选择[禁止]，则打印机功能的初始屏幕上不会显示[从记忆存储设备打印]按钮。

管理每个用户的打印容量

该功能可以为每个用户指定打印容量限制。如果每个用户可指定的打印容量达到最大值，则将会取消打印作业，并显示打印容量已达到最大值的信息。

打印量

通过将页数和单组计数相乘，可以计算打印量。

单组计数可以根据打印条件进行指定。例如，如果单组计数为 10，则打印 1 页时，打印容量为 10。

系统会跟踪各个用户的打印量。

3

设置项目

项目	说明	设置
达到限制时的机器操作	指定是否限制打印容量和限制打印方法。 • 停止作业 达到最大打印容量时，当前作业和等待作业均将被取消。 • 结束作业并限制 达到最大打印容量时，会完成当前作业，但等待作业将被取消。 • 允许继续使用 不为打印容量指定限制。	• 停止作业 • 结束作业并限制 • 允许继续使用（默认设置）
打印容量使用限制：单组计数设置	可以指定下列 8 种情况下每个用户的打印容量限制。 • 复印机：彩色：A3/DLT • 复印机：黑白：A3/DLT • 复印机：彩色：其他 • 复印机：黑白：其他 • 打印机：彩色：A3/DLT • 打印机：黑白：A3/DLT • 打印机：彩色：其他 • 打印机：黑白：其他	0 到 200 (每种打印条件的默认每页单组计数为 1。)

打印容量限制注意事项

如果发生下列情况，则无法进行打印：

- 用户登录和验证时，系统会更改通讯簿中注册的登录用户名或用户代码。

如果出现以下情况，打印容量管理将无法正确运行：

- 在 Windows 或 LDAP 验证下，用户通过使用多个登录用户名登录到相同用户帐户，这些登录名称作为单个用户注册在通讯簿中。

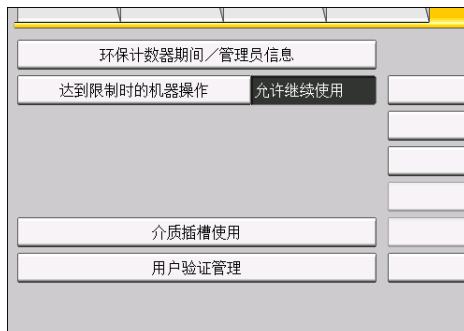
打印容量限制不适用于下列操作：

- 从不支持当前验证方法的操作系统打印

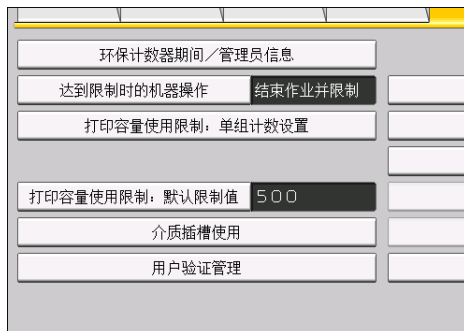
3

指定打印容量限制

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[▼向后]。
5. 按[达到限制时的机器操作]。



6. 选择[停止作业]或[结束作业并限制]，然后按[确定]。
若不想限制打印容量，请选择[允许继续使用]。
7. 按[打印容量使用限制：单组计数设置]。



8. 对于每种打印条件，请使用数字键输入“0”和“200”之间的每页单位计数，然后按[#]。

选择项目。	
复印机:彩色:A3/DLT 0	复印机:彩色:其
<0~200>	
复印机:黑白:A3/DLT 0	复印机:黑白:其
<0~200>	
打印机:彩色:A3/DLT 0	打印机:彩色:其
<0~200>	
打印机:黑白:A3/DLT 0	打印机:黑白:其
<0~200>	

若为打印条件指定“0”，则匹配该条件的作业不应用容量限制。

9. 按[确定]。

10. 注销。

注

- 在 Web Image Monitor 的“配置”下的[打印容量使用限制]中，也可指定打印容量限制。

启用用户代码验证时的限制

启用用户代码验证时，以下限制适用于打印容量限制设置：

- 若为打印机功能选择[PC 控制]，为打印容量使用单组指定的值可能不适用于用户的打印计数器。启用用户代码验证时，如果要指定限制打印容量限制，请勿选择[PC 控制]。
- 使用基本验证、Windows 验证和 LDAP 验证时，控制面板左下方显示的数字指示管理员为该用户指定的打印总量。使用用户代码验证时，用户无法自行使用控制面板或 Web Image Monitor 来检查打印总量。因此，用户需要向管理员询问打印总量。
- 作业日志或访问日志中不会记录关于打印使用限制的日志数据。
- 根据为用户代码验证配置的设置，无论管理员设置的打印容量限制如何，用户可在登录之前打印。在[用户验证管理]的[用户代码验证]中，通过“功能限制”限制所有功能。

指定默认的最大使用计数

- 以机器管理员身份从控制面板中登录。
- 按[系统设置]。
- 按[管理工具]。
- 按[▼向后]。

5. 按[打印容量使用限制：默认限制值]。

环保计数器期间／管理员信息

达到限制时的机器操作

结束作业并限制

打印容量使用限制：单组计数设置

打印容量使用限制：默认限制值

500

介质插槽使用

用户验证管理

如果您在“达到限制时的机器操作”中选择了[允许继续使用]，则屏幕上不会出现[打印容量使用限制：默认限制值]。

6. 使用数字键输入“0”和“999,999”之间的值作为最大打印容量，然后按[#]。
7. 按[确定]。
8. 注销。

指定每个用户的最大使用计数

1. 以机器管理员身份从控制面板中登录。
2. 按[通讯簿管理]。
3. 选择要指定其最大打印容量的用户。

按[新编入]添加新的或从下面列表中选择要编辑的。可用数字键选择

编入／更改

删除

所有用户

电子邮件

常用	AB	CD	EF	GH	IJK	LMN	OPQ	RST	U
【00001】 ABCD COMP NY	【00002】 YOKOHAMA OFFICE	【00003】 BERLIN OFF ICE	【00004】 LONDON OFF ICE	【00005】 NEW YORK OFFICE	【00006】 LOS ANGE LES	【00007】 KYOTO OFFI CE	【00008】 BEIJING OF FICE	【00009】 SHANGHAI OFFICE	【00010】 HONG KONG OFFICE
				【00011】 Folder01	【00012】 Folder02	【00013】 Folder03	【00014】 Folder04	【00015】 Folder05	【00016】 Folder06

4. 按[验证信息]。

5. 按 4 次[▼向后]。

6. 在“打印容量使用限制”中，按[限制]。

如果您在“达到限制时的机器操作”中选择了[允许继续使用]，则屏幕上不会出现“打印容量使用限制”。

若不想指定打印容量限制，请按[不限制]。

7. 按[更改]，然后使用数字键输入“0”和“999,999”之间的值作为最大可用打印量，然后按[#]。

最大打印容量设为“0”的用户只能打印条件与“0”匹配的作业。

8. 按[确定]。

9. 注销。

↓ 注

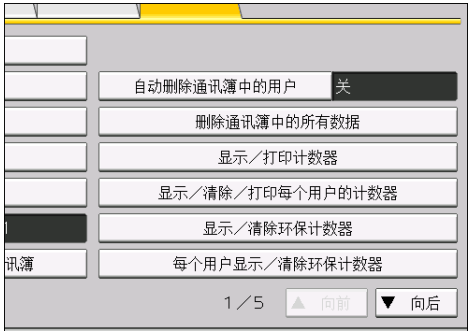
- 在 Web Image Monitor 的[通讯簿]中，也可为每个用户指定最大打印容量。

检查每个用户的打印容量

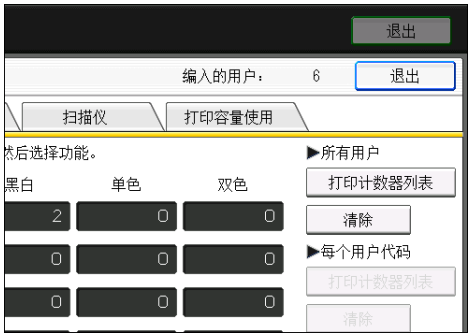
可由任何一个管理员管理此步骤。

1. 以管理员身份从控制面板中登录。

2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[显示/清除/打印每个用户的计数器]。



5. 按[打印容量使用]。



显示每个用户的打印容量限制和打印总量。

6. 确认设置以后，请注销。

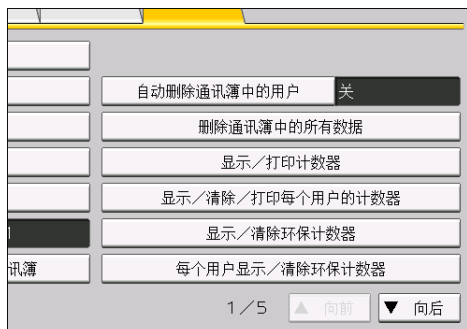
注

- 授权用户和用户管理员也可使用 Web Image Monitor 中的[通讯簿]来检查每个用户的打印容量使用计数器。

对打印容量使用计数器列表进行打印

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。

4. 按[显示/清除/打印每个用户的计数器]。



5. 按[打印容量使用]。

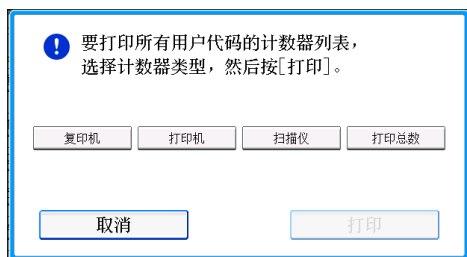
显示每个用户的打印容量使用计数器列表。

要选择页面上显示的所有用户，请按[选择所有页面项目]。

6. 要打印每个用户的容量使用计数器列表，请按“所有用户”下的[打印计数器列表]。要只打印所选用户的容量使用计数器列表，请选择要打印其计数器的用户，然后按“Per User”下的[打印计数器列表]。



7. 在列表中选择要打印的计数器，然后按[打印]。



8. 注销。

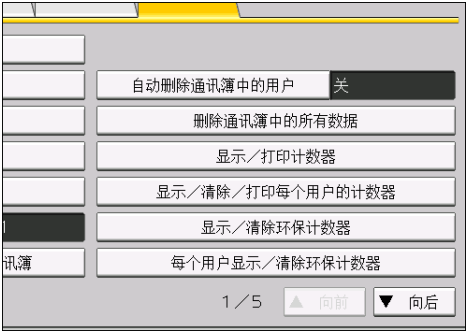
↓ 注

- 只有在以下纸张尺寸装入纸盘时，才能对打印量使用计数器列表进行打印：A4、8 1/2 × 11 英寸、B4、8 1/2 × 14 英寸、A3 或 11 × 17 英寸。

重置打印容量使用计数器

重置每个用户的打印容量计数器或增加每个用户的打印容量限制时，用户可以超过其允许打印数量进行打印。

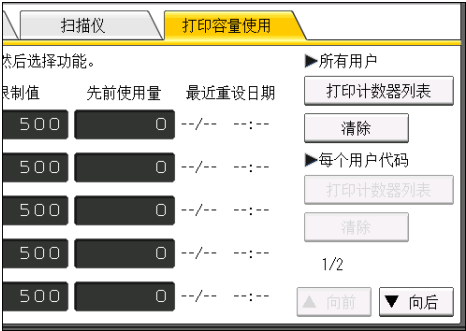
1. 以用户管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[显示/清除/打印每个用户的计数器]。



5. 按[打印容量使用]。

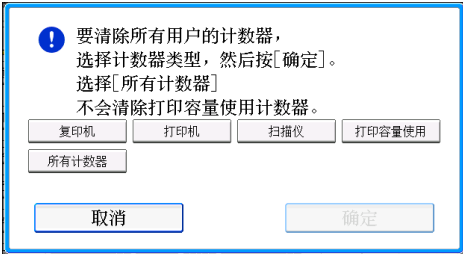
显示每个用户的打印容量使用计数器列表。

6. 要重置每个用户的打印容量使用计数器，请按“所有用户”下的[清除]。要只重置所选用户的打印容量使用计数器，请选择要重置其计数器的用户，然后按“每个用户代码”下的[清除]。



要选择页面上显示的所有用户，请按[选择所有页面项目]。

7. 选择[打印容量使用]，然后按[确定]。



8. 注销。

注

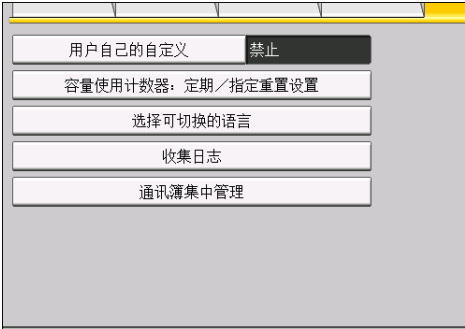
- 也可使用 Web Image Monitor 中的[通讯簿]来重置打印容量使用计数器。然而，若要同时重置所有用户的打印容量使用计数器，请使用控制面板。

配置自动重置功能

打印量计数器可以在指定时间重置。

选项	详细信息
每月	在每月的指定时间/日期重置打印量。
指定日期	在指定时间/日期重置打印容量（仅一次）。
指定周期	在参考日期之后的指定时间间隔重置，然后在相同时间间隔重置。

- 以机器管理员身份从控制面板中登录。
- 按[系统设置]。
- 按[管理员工具]。
- 按 4 次[▼向后]。
- 按[容量使用计数器：定期／指定重置设置]。



6. 选择[每个月]、[指定日期]和[指定周期]之一。

7. 配置条件。

8. 按[确定]。

9. 注销。

↓ 注

- 如果机器在指定日期的指定时间处于关闭状态，则打开电源以后，打印容量将重置。
- 如果在[每月]中选择了某些月份没有的日期（例如 31 日），则会在没有 31 日的月份的下个月第一天 0:00 时重置打印容量。

4. 防止从机器中泄漏信息

本章介绍如何保护机器内存或硬盘中保存的信息。

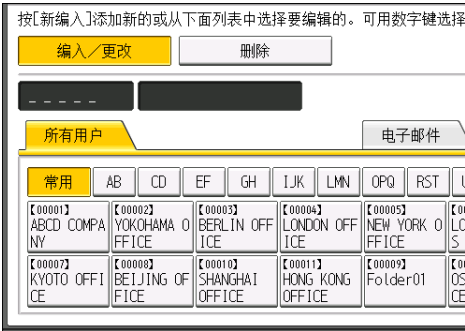
保护通讯簿

您可以指定允许哪些用户访问通讯簿中的数据。要防止未经授权用户读取数据，也可以加密通讯簿中的数据。

指定通讯簿访问权限

已在通讯簿中注册的用户、具有完全控制权限的用户以及用户管理员可以指定这些访问权限。

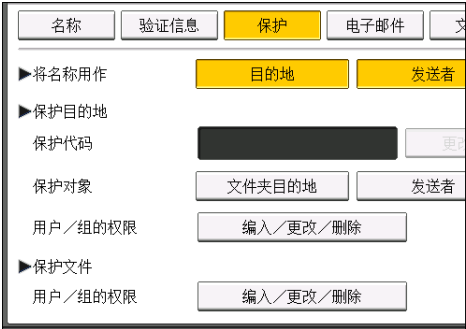
1. 以用户管理员身份从控制面板中登录。
2. 按[通讯簿管理]。
3. 选择您想要更改其访问权限的用户。



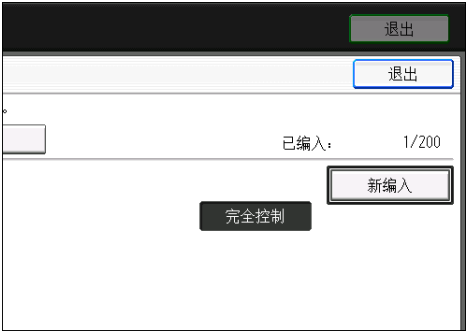
4. 按[保护]。



5. 在“保护目的地”下，按与“用户/组的权限”对应的[编入/更改/删除]。



6. 按[新编入]。



7. 选择要对其应用访问权限的用户或组。

您可以选择多个用户。

您可以按[所有用户]选择所有用户。

8. 按[退出]。

9. 选择要分配访问权限的用户，然后指定权限。

从[只读]、[编辑]、[编辑/删除]或[完全控制]中选择。

10. 按[退出]。

11. 按[确定]。

12. 注销。

↓ 注

- “编辑”、“编辑/删除”和“完全控制”访问权限允许用户执行可能导致敏感信息丢失或更改的操作。建议您仅向一般用户授予“只读”权限。

对通讯簿中的数据进行加密

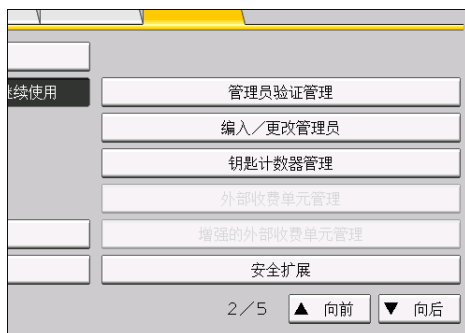
★重要信息

- 加密过程中不能使用机器。

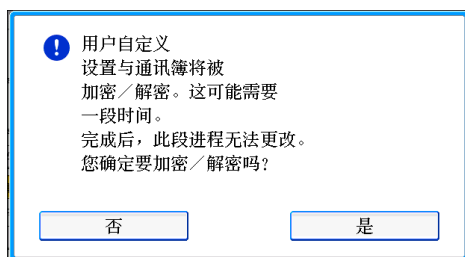
加密通讯簿中的数据所用时间取决于注册用户数量。

加密通讯簿中的数据可能需要较长时间。

1. 以用户管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[▼向后]。
5. 按[安全扩展]。



6. 为“加密用户自定义设置和通讯簿”按[开]。
7. 按“加密密钥”所对应的[更改]。
8. 输入加密密钥，然后按[确定]。
输入的加密密钥最多可由 32 个字母数字字符组成。
9. 按[加密/解密]。
10. 按[是]。



切勿在加密过程中关闭主电源，否则可能会损坏数据。

如果在加密过程中按[停止]，将不对数据进行加密。

如果在解密过程中按[停止]，将不对数据进行解密。

通常情况下，完成加密后会出现“加密／解密成功完成。请按[退出]。”信息。

11. 按[退出]。

12. 按[确定]。

13. 注销。

↓ 注

- 如果在加密通讯簿中的数据后注册了其他用户，则这些用户数据也将被加密。
- 存储在 SD 卡中的通讯簿数据备份副本已经过加密。有关使用 SD 卡备份和恢复通讯簿的详细信息，请参见《连接机器/系统设置》中的“管理员工具”。

对机器上的数据进行加密

⚠ 注意

- 请将 SD 卡或者 USB 闪存设备置于儿童接触不到的地方。如果儿童误吞 SD 卡或者 USB 闪存设备，请立即送医。

即使存储设备或硬盘失窃，也可以通过对机器上的数据（如通讯簿、验证数据和文件）进行加密来防止数据泄露。

一旦启用加密，随后保存在机器上的所有数据都将加密。

您也可以选择加密或删除当前保存在机器上的数据。

加密算法是 AES-256。

加密的数据

此功能会对机器的 NVRAM（即便关闭了机器也仍能保留数据的内存）和硬盘上保存的数据进行加密。

加密以下数据：

NVRAM

- 系统设置信息
- 网络 I/F 设置信息
- 用户代码信息
- 计数器信息

硬盘

- 通讯簿
- Embedded Software Architecture 应用程序的程序/日志
- 日志（作业日志/访问日志/环保日志）
- 发送/接收的电子邮件
- 注册的字体
- 假脱机作业
- 保存的文件缩略图
- 保存的文件
- 注册的印记

加密类型

指定是要加密现有数据并将其保存在硬盘上还是将其删除（格式化）。如果要保存大量数据，加密会需要一些时间。NVRAM 数据不会被删除（初始化）。

设置	要保留的数据	要初始化的数据	所需的时间
仅文件系统数据	• 通讯簿 • Embedded Software Architecture 应用程序的程序/日志 • 日志（作业日志/访问日志/环保日志） • 发送/接收的电子邮件 • 注册的字体 • 假脱机作业 • 保存的文件缩略图	• 保存的文件（文件服务器中保存的文件和锁定打印文件/样张打印文件/保存的打印文件/保留打印文件） • 注册的印记	大约 3 小时
所有数据	所有数据： 指定[仅文件系统数据]时要保留的数据和不保留的数据	无	大约 7 小时 45 分钟
格式化所有数据	无	所有数据： 指定[仅文件系统数据]时要保留的数据和不保留的数据	几分钟

启用加密设置注意事项

- 如果您使用 Embedded Software Architecture 应用程序或 App2Me，请务必指定[仅文件系统数据]或[所有数据]。
- 请注意，即使指定[格式化所有数据]、[仅文件系统数据]或[所有数据]，本机的设置也不会初始化为系统默认值。

恢复数据

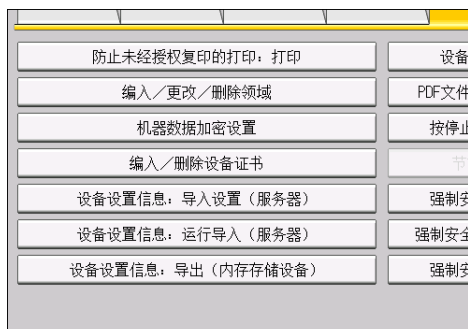
- 要将数据传送至新机器，请恢复加密数据。有关详细信息，请咨询服务代表。
- 需要提供用于数据加密的加密密钥才能恢复数据。
- 您可以指定是打印加密密钥还是将其保存在 SD 卡中。
- 您可以稍后更改加密密钥。

启用加密设置

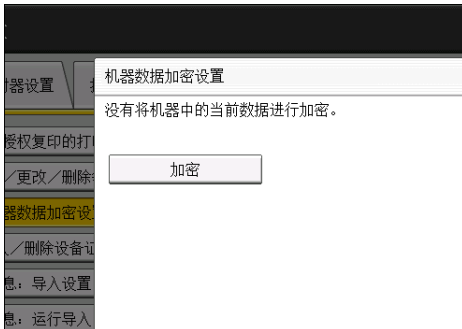
★重要信息

- 当数据正在被加密时，机器无法操作。
- 一旦加密进程开始，就不能被停止。当加密进程正在进行时，确保机器的主电源不会被关闭。如果在加密进程正在进行时关闭了机器的主电源，硬盘将受到损伤，同时在硬盘上保存的所有数据将无法使用。
- 如果机器出现故障，则必须使用加密密钥进行数据恢复。请务必妥善保存用于取回备份数据的加密密钥。
- 完成控制面板的操作步骤并且通过先关闭主电源开关再打开主电源开关来重新启动机器以后，系统将开始进行加密。如果同时指定了清除所有内存功能和加密功能，则会在覆盖保存在硬盘上的数据并通过先关闭再打开主电源开关来重新启动机器之后开始加密。
- 如果同时使用清除所有内存和加密功能，并为“随机数”选择了覆盖 3 次，该流程最多将花费 13 小时。从已经加密的状态重新加密需要花费相同的时间。
- 此外，“清除所有内存”功能还会清除机器的安全设置，导致机器或用户管理无法使用。确保在完成“清除所有内存”以后，用户不会在机器上保存任何数据。
- 若不需要将任何数据转移到硬盘，且加密设置为[格式化所有数据]，即使需要格式化硬盘上的所有数据，重新启动用时也将更短。在执行加密之前，我们建议您备份重要数据（例如通讯簿）以及保存在文件服务器中的所有数据。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按 3 次[▼向后]。
5. 按[机器数据加密设置]。



6. 按[加密]。



7. 选择要转入硬盘且不会删除的数据。

要将所有数据转入硬盘，请选择[所有数据]。要仅转入机器设置数据，请选择[仅文件系统数据]。要删除所有数据，请选择[格式化所有数据]。

8. 指定如何备份加密密钥。

如果选择了[保存至 SD 卡]，请将 SD 卡插入控制面板侧面的介质插槽中，然后按[确定]以备份机器的数据加密密钥。

有关处理和插入 SD 卡的详细信息，请参见《开始使用》中的“插入/取出存储设备”。

如果您选择了[打印到纸张]，请按[开始]键并打印出机器的数据加密密钥。

9. 按[确定]。

10. 按[退出]。

11. 按[退出]。

12. 注销。

13. 关闭主电源开关，然后重新打开主电源开关。

打开机器后，机器将开始转换内存上的数据。等到出现“内存转换完毕。关闭主电源开关。”信息，然后再次关闭主电源开关。

有关关闭主电源的详细信息，请参见《开始使用》中的“打开/关闭电源”。

备份加密密钥

您可以在不更改加密设置的情况下备份加密密钥。

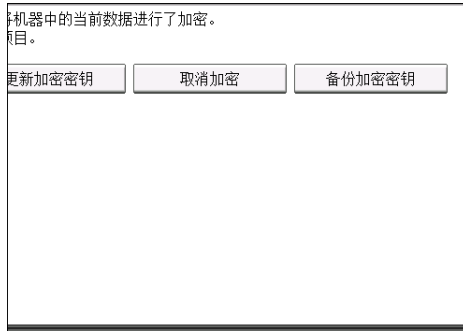
★重要信息

- 如果机器出现故障，则必须使用加密密钥进行数据恢复。请务必妥善保存用于取回备份数据的加密密钥。

1. 以机器管理员身份从控制面板中登录。

2. 按[系统设置]。

3. 按[管理员工具]。
4. 按 3 次[▼向后]。
5. 按[机器数据加密设置]。
6. 按[备份加密密钥]。



7. 指定如何备份加密密钥。

如果选择了[保存到 SD 卡]，请将 SD 卡插入控制面板侧面的介质插槽中，然后按[确定]。备份机器的数据加密密钥时，按[退出]。

有关处理和插入 SD 卡的详细信息，请参见《开始使用》中的“插入/取出存储设备”。

如果您选择了[打印到纸张]，请按[开始]键并打印出机器的数据加密密钥。

8. 按[退出]。

9. 注销。

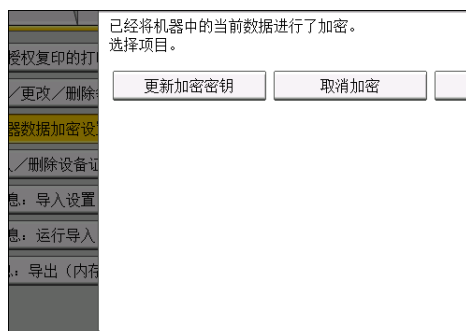
更新加密密钥

您可以更新加密密钥。应用新的加密密钥与开始加密花费的时间相同。如果机器工作正常，可以进行更新。

★重要信息

- 更新加密密钥期间，机器将无法使用。
- 如果机器出现故障，则必须使用加密密钥进行恢复。请务必妥善保存用于取回备份数据的加密密钥。
- 如果更新了加密密钥，将使用新密钥执行加密。在机器的控制面板中完成该步骤后，关闭主电源并重新启动机器以启用新设置。如果存在要转入硬盘的数据，重新启动可能会很慢。
- 一旦开始更新加密密钥，便无法停止。当加密进程正在进行时，确保机器的主电源不会被关闭。如果在加密进程正在进行时关闭了机器的主电源，硬盘将受到损伤，同时在硬盘上保存的所有数据将无法使用。
- 如果未完成加密密钥更新，则创建的加密密钥将无效。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理工具]。
4. 按 3 次[▼向后]。
5. 按[机器数据加密设置]。
6. 按[更新加密密钥]。



7. 选择要转入硬盘且不会删除的数据。

要将所有数据转入硬盘，请选择[所有数据]。要仅转入机器设置数据，请选择[仅文件系统数据]。要删除所有数据，请选择[格式化所有数据]。

8. 指定如何备份加密密钥。

如果选择了[保存至 SD 卡]，请将 SD 卡插入控制面板侧面的介质插槽中，然后按[确定]以备份机器的数据加密密钥。

有关处理和插入 SD 卡的详细信息，请参见《开始使用》中的“插入/取出存储设备”。

如果您选择了[打印到纸张]，请按[开始]键并打印出机器的数据加密密钥。

9. 按[确定]。
10. 按[退出]。
11. 按[退出]。
12. 注销。
13. 关闭主电源开关，然后重新打开主电源开关。

打开机器后，机器将开始转换内存上的数据。等到出现“内存转换完毕。关闭主电源开关。”信息，然后再次关闭主电源开关。

有关关闭主电源的详细信息，请参见《开始使用》中的“打开/关闭电源”。

取消数据加密

不再需要加密时，请通过以下步骤取消加密设置。启用和禁用加密设置所需的时间一样长。

★重要信息

- 取消数据加密期间，机器将无法使用。
- 在机器的控制面板中完成该步骤后，关闭主电源并重新启动机器以启用新设置。如果存在要转入硬盘的数据，重新启动可能会很慢。
- 一旦开始取消数据加密，便无法停止。当加密进程正在进行时，确保机器的主电源不会被关闭。如果在加密进程正在进行时关闭了机器的主电源，硬盘将受到损伤，同时在硬盘上保存的所有数据将无法使用。
- 废弃机器时，请完全删除内存。有关清除所有内存的详细信息，请参见 p.86 “删除机器上的数据”。

1. 以机器管理员身份从控制面板中登录。

2. 按[系统设置]。

3. 按[管理员工具]。

4. 按 3 次[▼向后]。

5. 按[机器数据加密设置]。

6. 按[取消加密]。

7. 选择要转入硬盘且不会删除的数据。

要将所有数据转入硬盘，请选择[所有数据]。要仅转入机器设置数据，请选择[仅文件系统数据]。要删除所有数据，请选择[格式化所有数据]。

8. 按[确定]。

9. 按[退出]。

10. 按[退出]。

11. 注销。

12. 关闭主电源开关，然后重新打开主电源开关。

有关关闭主电源的详细信息，请参见《开始使用》中的“打开/关闭电源”。

删除机器上的数据

通过覆盖保存在机器上的数据，可以防止数据泄露。

有以下两种覆盖方式：

自动清除内存

临时保存在机器硬盘中以便复印或打印的数据会自动被清除。有关详细信息，请参见 p.86 “自动清除内存”。

清除所有内存

保存在机器硬盘中的所有数据会通过覆盖来清除。保存在机器内存中的设备设置会被初始化。在迁移或处理机器时执行此操作将清除所有数据和设置。有关详细信息，请参见 p.90 “清除所有内存”。

4

自动清除内存

在复印或扫描模式下扫描的文件，或通过打印机驱动程序发送的打印数据将暂时保存在机器的硬盘上。即使在作业完成后，这些数据也仍作为临时数据保留在硬盘中。“自动清除内存”会通过覆盖来清除硬盘中的临时数据。

作业完成时覆盖功能即会自动启动。

复印机和打印机功能的优先级高于“自动清除内存”功能。如果正在进行复印或打印作业，则作业完成后才会进行覆盖。

“自动清除内存”可以或无法覆盖的数据类型

通过自动清除内存覆盖的数据

复印

- 复印作业

打印

- 打印作业
- 样张打印/锁定打印/保留打印/保存的打印作业

您只能在样张打印/锁定打印/保留打印作业执行以后覆盖该作业。对于保存的打印作业，在将其删除之后才能将其覆盖。

- 假脱机打印作业

扫描

- 通过电子邮件发送扫描的文件
- 通过扫描至文件夹发送的文件
- 使用 Web Image Monitor 发送的文档

- 网络 TWAIN 扫描仪

选中 TWAIN 驱动程序的“ADF(预先读取)”功能时，使用网络 TWAIN 扫描仪扫描的数据将被自动清除内存覆盖。如果未选中“ADF(预先读取)”功能，则不会覆盖扫描的数据。

文件服务器

- 用户使用复印机、打印机或扫描仪功能在文件服务器中保存的文件
只有将保存的文件从文件服务器打印或删除后，才能将其覆盖。

其他

- 在通讯簿中注册的信息
保存在通讯簿中的数据只有在更改或删除后才能被覆盖。
- 使用 Embedded Software Architecture 的应用程序
Embedded Software Architecture 程序的数据只有在删除后才能被覆盖。

不能通过“自动清除内存”覆盖的数据

- 在每个用户代码下保存的计数器

覆盖方法

可以选择以下覆盖方法中的一种：

- NSA
两次用随机数、一次用零覆盖临时数据。
- DoD
每个数据项目将被一个随机数覆盖，之后是其补足数，然后是另一个随机数，再进行验证。
- 随机数
使用随机数多次覆盖临时数据。覆盖次数可以从 1 到 9 中进行选择。

↓ 注

- 覆盖的默认方法为“随机数”，默认的覆盖次数为 3。
- NSA 代表美国“国家安全局”。
- DoD 代表美国“国防部”。

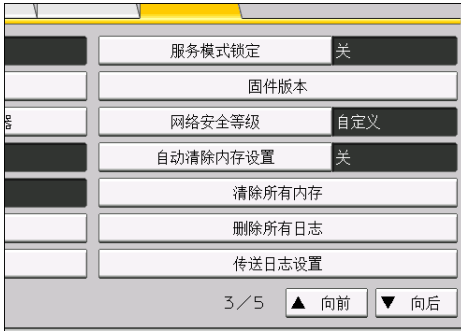
使用“自动清除内存”

★ 重要信息

- 如果将“自动清除内存”设置为[开]，“自动清除内存”设置为[关]时硬盘中保留的临时数据可能不会被覆盖。

- 如果在“自动清除内存”完成前关闭主电源开关，覆盖操作将停止，数据将遗留在硬盘中。
- 请不要中途停止覆盖。这样做会损伤硬盘。
- 如果在自动清除内存完成前关闭主电源开关，则再次打开主电源开关后覆盖操作将继续执行。
- 如果覆盖完成前出错，请关闭主电源。再次打开主电源，然后重复步骤 1 及以后的操作。
- 在覆盖还未完成之前，机器将不会进入“睡眠”模式。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按两次[▼向后]。
5. 按[自动清除内存设置]。



6. 按[开]。
7. 选择要使用的覆盖方式。
如果选择[NSA]或[DoD]，请转至步骤 10。
如果选择[随机数]，请转至步骤 8。
8. 按[更改]。
9. 使用数字键输入您要覆盖的次数，然后按[#]。
10. 按[确定]。
“自动清除内存”设置完毕。
11. 注销。

↓ 注

- 如果您启用了覆盖和数据加密，则覆盖的数据也会被加密。

取消自动清除内存

- 1. 以机器管理员身份从控制面板中登录。
- 2. 按[系统设置]。
- 3. 按[管理员工具]。
- 4. 按两次[▼向后]。
- 5. 按[自动清除内存设置]。
- 6. 按[关]。
- 7. 按[确定]。
“自动清除内存” 将被禁用。
- 8. 注销。

4

覆盖图标

启用“自动清除内存” 后，数据覆盖图标将显示在机器显示屏的右下角。



图标	图标名称	说明
	有数据	存在要覆盖的临时数据时，该图标会亮起，在覆盖过程中会闪烁。
	清除	此图标会在没有要覆盖的临时数据时亮起。

★重要信息

- 当存在样张打印/锁定打印/保留打印/保存的打印作业时，数据覆盖图标将显示“无数据”。

↓ 注

- 如果未显示“数据覆盖”图标，请先检查是否已将“自动清除内存”设置为[关]。如果即使“自动清除内存”设置为[开]，仍未显示图标，请联系您的服务代理商。
- 如果正在进行覆盖时机器进入节能模式，请按[节能]键恢复显示，以检查该图标。
- 如果没有数据需要覆盖时数据覆盖图标继续显示为“有数据”，请关闭机器主电源。重新打开机器，查看图标是否更改为“无数据”。如果没有，请联系您的销售或服务代表。

清除所有内存

4

迁移或处理机器时覆盖并清除硬盘上保存的所有数据。保存在机器内存中的设备设置会被初始化。

有关在执行清除所有内存后使用本机的详细信息，请与您的销售代表联系。

★ 重要信息

- 如果在“清除所有内存”完成前关闭主电源开关，覆盖操作将停止，数据将遗留在硬盘中。
- 请不要中途停止覆盖。这样做会损伤硬盘。
- 我们建议您在清除硬盘之前，先使用 Device Manager NX 备份通讯簿。地址簿也可以使用 Web Image Monitor 来进行备份。有关详细信息，请参见 Device Manager NX 的帮助或 Web Image Monitor 的帮助。
- “清除所有内存”过程中唯一可执行的操作是暂停。如果选择了“随机数”并设置为覆盖 3 次，则完成“清除所有内存”过程需多达 5 小时 15 分钟。
- 此外，“清除所有内存”功能还会清除机器的安全设置，导致机器或用户管理无法使用。确保在完成“清除所有内存”以后，用户不会在机器上保存任何数据。

清除所有内存可覆盖的数据类型

复印

- 复印作业

打印

- 打印作业
- 样张打印/锁定打印/保留打印/保存的打印作业
- 假脱机打印作业

扫描

- 通过电子邮件发送扫描的文件
- 通过扫描至文件夹发送的文件

- 使用 Web Image Monitor 发送的文档
- 网络 TWAIN 扫描仪

选中 TWAIN 驱动程序的“ADF(预先读取)”功能时，使用网络 TWAIN 扫描仪扫描的数据将被自动清除内存覆盖。如果未选中“ADF(预先读取)”功能，则不会覆盖扫描的数据。

文件服务器

- 用户使用复印机、打印机或扫描仪功能在文件服务器中保存的文件

其他

- 在通讯簿中注册的信息
- 在每个用户代码下保存的计数器
- 使用嵌入式软件体系结构的应用程序

系统设置或与设备相关的其他设置会被初始化。

清除方式

可以选择以下清除方法中的一种：

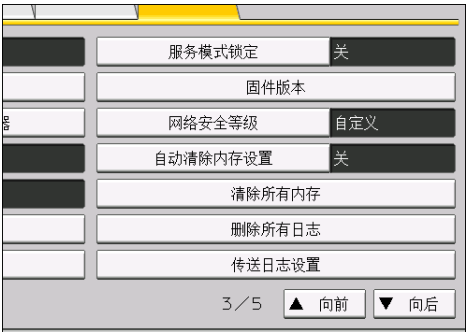
- NSA
两次用随机数、一次用零覆盖数据。
- DoD
数据将被一个随机数覆盖，之后是其补足数，然后是另一个随机数，再进行验证。
- 随机数
使用随机数多次覆盖数据。覆盖次数可以从 1 到 9 中进行选择。
- BSI/VSITR
使用下列图案覆盖数据 7 次：0x00、0xFF、0x00、0xFF、0x00、0xFF、0xAA。
- 安全清除
使用硬盘驱动器中内置的算法覆盖数据。
- 格式化
将格式化硬盘。数据未覆盖。

↓ 注

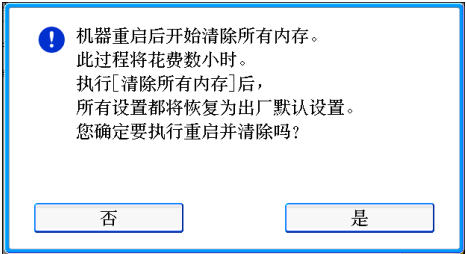
- 清除的默认方法为“随机数”，默认的覆盖次数为 3。
- NSA 代表美国“国家安全局”。
- DoD 代表美国“国防部”。

使用清除所有内存

1. 断开连接至机器的通讯电缆。
2. 以机器管理员身份从控制面板中登录。
3. 按[系统设置]。
4. 按[管理员工具]。
5. 按两次[▼向后]。
6. 按[清除所有内存]。



7. 选择清除方法。
如果选择[NSA]、[DoD]、[BSI/VSITR]、[安全清除]或[格式化]，请转至步骤 10。
如果选择[随机数]，请转至步骤 8。
8. 按[更改]。
9. 使用数字键输入您要覆盖的次数，然后按[#]。
10. 按[消除]。
11. 按[是]。



12. 清除完成后，按[退出]，然后关闭主电源。
有关关闭主电源的详细信息，请参见《开始使用》中的“打开/关闭电源”。

注

- 如果在“清除所有内存”完成前关闭主电源开关，则再次打开主电源开关后覆盖操作将重新执行。

- 如果覆盖完成前出错，请关闭主电源。再次打开主电源，然后重复步骤 2 及以后的操作。

暂停清除所有内存

要在启用清除所有内存时关闭机器电源，请提前暂停清除所有内存。打开主电源后，清除所有内存会继续进行。

★重要信息

- 如果选择了[安全清除]或[格式化]，则无法暂停该过程。
- 但不能取消清除所有内存。

1. 在清除所有内存进行过程中按[暂停]。

2. 按[是]。

将暂停清除所有内存。

3. 关闭主电源。

有关关闭主电源的详细信息，请参见《开始使用》中的“打开/关闭电源”。

5. 提升网络安全

本章介绍用于在机器连接到网络时提高安全性的功能。

访问控制

机器可以控制 TCP/IP 访问。

通过指定访问控制范围来限制可以作为访问入口的 IP 地址。

例如，如果将访问控制范围指定为[192.168.15.16]-[192.168.15.20]，则可以作为访问入口的客户端 PC 地址将是[192.168.15.16]到[192.168.15.20]。

★重要信息

- 使用访问控制，可以限制从以下功能进行访问：LPR、RCP/RSH、FTP、ssh/sftp、Bonjour、SMB、WSD（设备）、WSD（打印机）、WSD（扫描仪）/DSM、IPP、DIPRINT、RHPP 或 Web Image Monitor。使用 SNMPv1 监控时，无法限制从 telnet 或 Device Manager NX 进行访问。

1. 以网络管理员身份从 Web Image Monitor 登录。

2. 指向[设备管理]，然后单击[配置]。

3. 在“安全”下，单击[访问控制]。

4. 要指定 IPv4 地址，请在“访问控制范围”中输入有权访问机器的 IP 地址。

要指定 IPv6 地址，请在“访问控制范围”下的“范围”中输入有权访问机器的 IP 地址，或在“掩码”中输入 IP 地址并指定“掩码长度”。

5. 单击[确定]。

6. 将出现“正在更新...”。等待约 1 至 2 分钟后，单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

7. 注销。

启用和禁用协议

指定是启用还是禁用每个协议的功能。进行此项设置可以指定可用的协议，从而防止通过网络进行未经授权的访问。可以在控制面板上指定网络设置，也可以使用 Web Image Monitor、telnet、Device Manager NX 或 Remote Communication Gate S 来指定网络设置。

协议	端口	设置方法	禁用时
IPv4	-	• 控制面板 • Web Image Monitor • telnet	不能使用所有通过 IPv4 运行的应用程序。 当使用 IPv4 传输时，不能从 Web Image Monitor 中禁用 IPv4。
IPv6	-	• 控制面板 • Web Image Monitor • telnet	不能使用所有通过 IPv6 运行的应用程序。
IPsec	-	• 控制面板 • Web Image Monitor • telnet	将禁用使用 IPsec 的加密传输。
FTP	TCP: 21	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	不能使用需要 FTP 的功能。 在控制面板上通过使用“限制显示用户信息”进行设置，可以限制显示个人信息。

协议	端口	设置方法	禁用时
ssh/sftp	TCP: 22	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	不能使用需要 sftp 的功能。 在控制面板上通过使用“限制显示用户信息”进行设置，可以限制显示个人信息。
telnet	TCP: 23	• Web Image Monitor • Device Manager NX	将禁用使用 telnet 的命令。
SMTP	TCP: 25 (可变)	• 控制面板 • Web Image Monitor • Device Manager NX • Remote Communication Gate S	不能使用需要 SMTP 接收的电子邮件通知功能。
HTTP	TCP: 80	• Web Image Monitor • telnet	不能使用需要 HTTP 的功能。 不能使用端口 80 上的 IPP 进行打印。
HTTPS	TCP: 443	• Web Image Monitor • telnet	不能使用需要 HTTPS 的功能。 不能使用@Remote。 还可以使用控制面板或 Web Image Monitor 进行设置以要求 SSL 传送。

协议	端口	设置方法	禁用时
SMB	TCP: 139	• 控制面板 • Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	不能使用 SMB 打印功能。
NBT	UDP: 137 UDP: 138	• telnet	不能使用通过 TCP/IP 进行的 SMB 打印功能和 WINS 服务器上的 NetBIOS 指定功能。
SNMPv1,v2	UDP: 161	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	不能使用需要 SNMPv1、v2 的功能。 使用控制面板、Web Image Monitor 或 telnet，可以指定 SNMPv1、v2 设置是只读的，不能编辑。
SNMPv3	UDP: 161	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	不能使用需要 SNMPv3 的功能。 您还可以使用控制面板、Web Image Monitor 或 telnet 指定设置，以要求进行 SNMPv3 加密传送和限制使用其他传送方法。

协议	端口	设置方法	禁用时
RSH/RCP	TCP: 514	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	不能使用需要 RSH 和网络 TWAIN 功能的功能。 在控制面板上通过使用“限制显示用户信息”进行设置，可以限制显示个人信息。
LPR	TCP: 515	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	不能使用 LPR 功能。 在控制面板上通过使用“限制显示用户信息”进行设置，可以限制显示个人信息。
IPP	TCP: 631	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	不能使用 IPP 功能。
SSDP	UDP: 1900	• Web Image Monitor • telnet	不能使用从 Windows 使用 UPnP 进行设备查找的功能。
Bonjour	UDP: 5353	• Web Image Monitor • telnet	不能使用 Bonjour 功能。
@Remote	TCP: 7443 TCP: 7444	• 控制面板 • telnet	不能使用@Remote。

协议	端口	设置方法	禁用时
DIPRINT	TCP: 9100	• Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	不能使用 DIPRINT 功能。
RFU	TCP: 10021	• 控制面板 • telnet	您可以通过 FTP 更新固件。
NetWare	(IPX/SPX)	• 控制面板 • Web Image Monitor • telnet • Device Manager NX • Remote Communication Gate S	不能使用 NetWare 打印。 不能使用 IPX 上的 SNMP。
WSD (设备)	TCP: 53000 (可变)	• Web Image Monitor • telnet	不能使用 WSD (设备) 功能。
WSD (打印机)	TCP: 53001 (可变)	• Web Image Monitor • telnet	不能使用 WSD (打印机) 功能。
WSD (扫描仪) /DSM	TCP-53002 (可变)	• Web Image Monitor • telnet	不能使用 WSD (扫描仪) 和 DSM 功能。
WS-Discovery	UDP/ TCP: 3702	• telnet	不能使用 WSD (设备、打印机、扫描仪) 搜索功能。

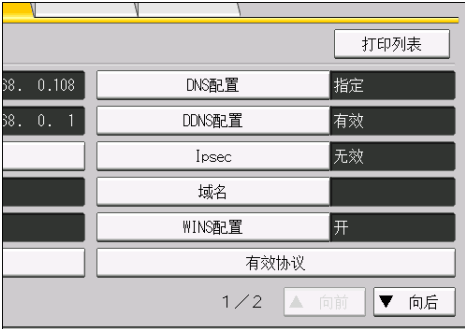
协议	端口	设置方法	禁用时
RHPP	TCP: 59100	• Web Image Monitor • telnet	不能使用 RHPP 打印。
LLTD	-	• telnet	不能使用 LLTD 执行设备搜索功能。
LLMNR	UDP: 5355	• Web Image Monitor • telnet	不能响应使用 LLMNR 发出的名称解析请求。

注

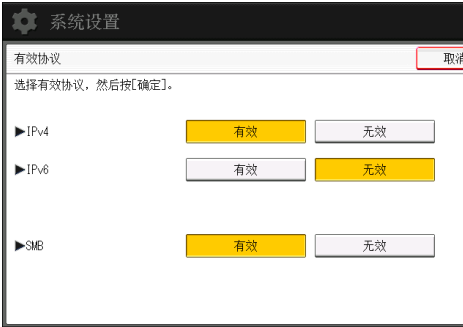
- “限制显示用户信息”是安全扩展功能之一。关于进行此设置的详细信息，请参见 p.225 “指定扩展安全功能”。

使用控制面板启用和禁用协议

1. 以网络管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[接口设置]。
4. 按[有效协议]。



5. 选择要启用或禁用的协议。



6. 按[确定]。

7. 注销。

5 使用 Web Image Monitor 启用和禁用协议

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[网络安全]。
4. 选择要启用或禁用的协议，或选择要打开或关闭的端口。
5. 单击[确定]。
6. 将出现“正在更新...”。等待约 1 至 2 分钟后，单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

7. 注销。

指定网络安全等级

利用此设置，可更改安全等级，以限制未经授权的访问。您可以使用控制面板或 Web Image Monitor 来配置网络安全等级设置。请注意，可以指定的协议不一而定。

★重要信息

- 使用某些实用程序时，通信或登录可能会失败，具体取决于网络安全等级。

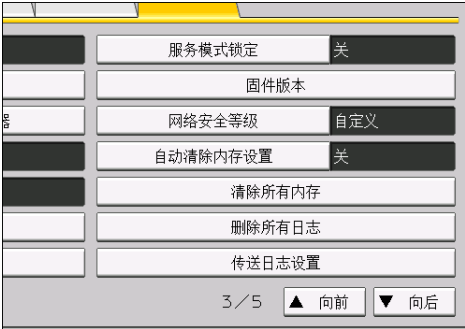
网络安全等级

安全等级	描述
[0 级]	选择[0 级]可使用全部功能。不需要保护信息免受外部威胁时可使用此设置。
[1 级]	选择[1 级]的安全性为中等，用来保护重要信息。如果该机器与局域网(LAN)相连，请使用此设置。
[FIPS140]	提供介于[1 级]和[2 级]之间的安全强度。您只能使用美国政府建议的代码作为其编码/验证算法。除算法以外的设置与[2 级]相同。
[2 级]	选择[2 级]的安全性最高，用来保护机密信息。需要保护机密信息免受外部威胁时可使用此设置。
[自定义]	用于不同于以上等级的配置。使用 Web Image Monitor 进行配置。

使用控制面板指定网络安全等级

1. 以网络管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按两次[▼向后]。

5. 按[网络安全等级]。



6. 选择所需的网络安全等级。

选择[0 级]、[1 级]、[2 级]或[FIPS140]。

7. 按[确定]。

8. 注销。

5

使用 Web Image Monitor 指定网络安全等级

1. 以网络管理员身份从 Web Image Monitor 登录。

2. 指向[设备管理]，然后单击[配置]。

3. 在“安全”下，单击[网络安全]。

4. 在“安全等级”中选择网络安全等级。

5. 单击[确定]。

6. 将出现“正在更新...”。等待约 1 至 2 分钟后，单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

7. 注销。

每种网络安全等级下的功能状态

TCP/IP

功能	0 级	1 级	FIPS 140	2 级
TCP/IP	有效	有效	有效	有效
HTTP>端口 80	打开	打开	打开	打开
IPP>端口 80	打开	打开	打开	打开

功能	0 级	1 级	FIPS 140	2 级
IPP>端口 631	打开	打开	关闭	关闭
SSL/TLS>端口 443	打开	打开	打开	打开
SSL/TLS>允许 SSL/TLS 通信	密文优先级	密文优先级	仅限密文	仅限密文
SSL/TLS 版本>TLS1.2	有效	有效	有效	有效
SSL/TLS 版本>TLS1.1	有效	有效	有效	有效
SSL/TLS 版本>TLS1.0	有效	有效	有效	有效
SSL/TLS 版本>SSL3.0	有效	有效	无效	无效
加密强度设置>AES	128 位/256 位	128 位/256 位	128 位/256 位	128 位/256 位
加密强度设置>3DES	168 位	168 位	168 位	-
加密强度设置>RC4	-	-	-	-
DIPRINT	有效	有效	无效	无效
LPR	有效	有效	无效	无效
FTP	有效	有效	有效	有效
sftp	有效	有效	有效	有效
ssh	有效	有效	有效	有效
RSH/RCP	有效	有效	无效	无效
TELNET	有效	无效	无效	无效
Bonjour	有效	有效	无效	无效
SSDP	有效	有效	无效	无效
SMB	有效	有效	无效	无效
NetBIOS over TCP/IPv4	有效	有效	无效	无效
WSD (Device)	有效	有效	有效	有效
WSD (Printer)	有效	有效	有效	有效

功能	0 级	1 级	FIPS 140	2 级
WSD (Scanner) /DSM	有效	有效	有效	有效
WSD (设备的加密通信)	无效	无效	有效	有效
RHPP	有效	有效	无效	无效

相同的设置将应用到 IPv4 和 IPv6。

TCP/IP 设置不受安全等级影响。手动指定是启用还是禁用该设置。

NetWare

功能	0 级	1 级	FIPS 140	2 级
NetWare	有效	有效	无效	无效

如果网络中未使用 NetWare，则上述设置将不适用。

SNMP

功能	0 级	1 级	FIPS 140	2 级
SNMP	有效	有效	有效	有效
允许通过 SNMPv1 和 v2 设置	开	关	关	关
SNMPv1, v2 功能	有效	有效	无效	无效
SNMPv3 功能	有效	有效	有效	有效
允许 SNMPv3 通信	加密/明文	加密/明文	仅加密	仅加密

TCP/IP 加密强度设置

功能	0 级	1 级	FIPS 140	2 级
ssh>加密算法	DES/3DES/ AES-128/ AES-192/ AES-256/ Blowfish/ Arcfour	3DES/ AES-128/ AES-192/ AES-256/ Arcfour	3DES/ AES-128/ AES-192/ AES-256	3DES/ AES-128/ AES-192/ AES-256
S/MIME>加密算法	3DES-168 位	3DES-168 位	3DES-168 位	AES-256 位

功能	0 级	1 级	FIPS 140	2 级
S/MIME>摘要算法	SHA1	SHA1	SHA1	SHA-256 位
SNMPv3>验证算法	MD5	SHA1	SHA1	SHA1
SNMPv3>加密算法	DES	DES	AES-128	AES-128
Kerberos 验证>加密 算法	AES256- CTS-HMAC- SHA1-96/ AES128- CTS-HMAC- SHA1-96/ DES3-CBC- SHA1/RC4- HMAC/ DES-CBC- MD5	AES256- CTS-HMAC- SHA1-96/ AES128- CTS-HMAC- SHA1-96/ DES3-CBC- SHA1/RC4- HMAC	AES256- CTS-HMAC- SHA1-96/ AES128- CTS-HMAC- SHA1-96/ DES3-CBC- SHA1	AES256- CTS-HMAC- SHA1-96/ AES128- CTS-HMAC- SHA1-96
驱动程序加密密钥>加 密强度	简单加密	DES	AES	AES

通过设备证书保护通信路径

本机可以使用 SSL/TLS、IPsec、S/MIME 或 IEEE 802.1X 保护其通信路径以及建立加密通信。它还可以使用 PDF 或 PDF/A 数字签名保护 PDF。

要使用这些功能，需要事先为机器创建并安装设备证书。

可使用以下类型的设备证书：

- 机器创建的自签证书
- 证书颁发机构颁发的证书

★重要信息

- 管理员需要处理证书到期的情况，并在证书到期之前更新证书。
- 管理员需要检查证书颁发机构是否有效。

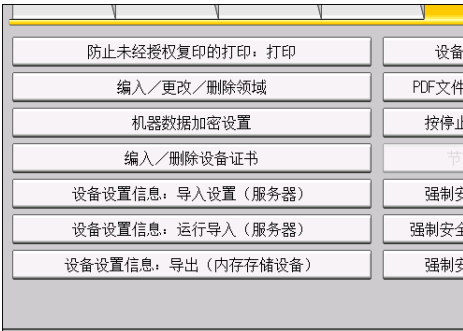
5

从控制面板创建并安装设备证书（自签证书）

使用控制面板创建并安装设备证书。

本节说明如何将自签证书用作设备证书。

1. 以网络管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按 3 次[▼向后]。
5. 按[编入／删除设备证书]。



6. 检查是否选择了[编入]。
7. 按[证书 1]。

只有[证书 1]可以从控制面板创建。

8. 配置必要的设置。

要将设备证书用于 S/MIME、PDF 数字签名或 PDF/A 数字签名，请在电子邮件地址设置中输入机器管理员的电子邮件地址。

9. 按[确定]。

“证书状态”下出现“已安装”，说明已安装了机器的设备证书。

10. 注销。

↓ 注

- 选择[删除]从机器中删除设备证书。
- 要将在机器上创建的设备证书用于 S/MIME 或 PDF/A 数字签名，请将 Web Image Monitor 中的“证书”设置为[证书 1]。

从 Web Image Monitor 创建并安装设备证书（自签证书）

5

使用 Web Image Monitor 创建和安装设备证书。有关所显示项目和可选项目的详细信息，请参见 Web Image Monitor 帮助。

本节说明如何将自签证书用作设备证书。

1. 以网络管理员身份从 Web Image Monitor 登录。

2. 指向[设备管理]，然后单击[配置]。

3. 在“安全”下，单击[设备证书]。

4. 选中想要创建的证书编号旁边的单选按钮。

要使用 SSL/TLS，请选择[证书 1]。要使用任何其他协议，请选择要使用的证书编号。

5. 单击[创建]。

单击[删除]从机器中删除设备证书。

6. 配置必要的设置。

要将设备证书用于 S/MIME、PDF 数字签名或 PDF/A 数字签名，请在电子邮件地址设置中输入机器管理员的电子邮件地址。

7. 单击[确定]。

设置即被更改。

8. 单击[确定]。

9. 如果出现安全警告信息，请检查详细信息，然后选择“继续访问此网站”。

“证书状态”下出现“已安装”，说明已安装了机器的设备证书。

10. 注销。

创建（证书机构颁发的）设备证书

使用 Web Image Monitor 创建设备证书。有关所显示项目和可选项目的详细信息，请参见 Web Image Monitor 帮助。

本节说明如何将证书颁发机构签发的证书用作设备证书。

1. 以网络管理员身份从 Web Image Monitor 登录。

2. 指向[设备管理]，然后单击[配置]。

3. 在“安全”下，单击[设备证书]。

4. 选中想要创建的证书编号旁边的单选按钮。

要使用 SSL/TLS，请选择[证书 1]。要使用任何其他协议，请选择要使用的证书编号。

5. 单击[申请]。

6. 配置必要的设置。

7. 单击[确定]。

设置即被更改。

8. 单击[确定]。

“证书状态”中出现“正在申请”。

9. 注销。

10. 向证书颁发机构申请设备证书。

申请程序视证书颁发机构而定。有关详细信息，请与证书颁发机构联系。

要进行申请，请单击 Web Image Monitor 详细资料图标，然后使用出现在“证书详细资料”中的信息。

注

- 如果您同时申请 2 个证书，则可能不会显示签发位置。当您安装证书时，请务必检查证书目的地和安装步骤。
- Web Image Monitor 可用来创建设备证书，但不能用来向证书颁发机构申请证书。
- 单击[取消申请]可取消对设备证书的申请。

安装（证书机构颁发的）设备证书

使用 Web Image Monitor 安装设备证书。有关所显示项目和可选项目的详细信息，请参见 Web Image Monitor 帮助。

本节说明如何将证书颁发机构签发的证书用作设备证书。

输入证书颁发机构签发的设备证书内容。

1. 以网络管理员身份从 Web Image Monitor 登录。

2. 指向[设备管理]，然后单击[配置]。

3. 在“安全”下，单击[设备证书]。

4. 选中想要安装的证书编号旁边的单选按钮。

要使用 SSL/TLS，请选择[证书 1]。要使用任何其他协议，请选择要使用的证书编号。

5. 单击[安装]。

6. 输入设备证书的内容。

在证书框中，输入证书机构颁发的设备证书的内容。

如果正在安装中间证书，则也要输入中间证书的内容。

有关所显示项目和可选项目的详细信息，请参见 Web Image Monitor 帮助。

7. 单击[确定]。

8. 等待约 1 至 2 分钟后，单击[确定]。

“证书状态”下出现“已安装”，说明已安装了机器的设备证书。

9. 注销。

5

安装中间证书（由证书颁发机构颁发）

本节介绍如何使用 Web Image Monitor 安装证书颁发机构所颁发的中间证书。

如果没有证书颁发机构所颁发的中间证书，通信期间将出现警告信息。如果证书颁发机构已颁发中间证书，则建议安装中间证书。

1. 以网络管理员身份从 Web Image Monitor 登录。

2. 指向[设备管理]，然后单击[配置]。

3. 在“安全”下，单击[设备证书]。

4. 选中想要安装的证书编号旁边的单选按钮。

5. 单击[安装中间证书]。

6. 输入中间证书的内容。

在证书框中，输入证书颁发机构所颁发中间证书的内容。有关证书的项目及设置的详细信息，请参见 Web Image Monitor 帮助。

7. 单击[确定]。

8. 等待约 1 至 2 分钟后，单击[确定]。

中间证书将被安装在设备上。“证书详细资料”屏幕将显示是否安装了中间证书。有关“证书详细资料”屏幕的详细信息，请参见 Web Image Monitor 帮助。

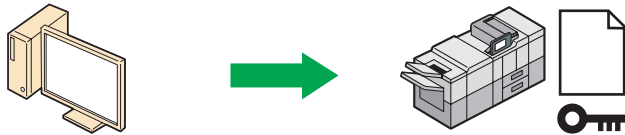
9. 注销。

配置 SSL/TLS 设置

配置机器使用 SSL/TLS 可以启用加密通信。这样做有助于防止数据在传输过程中被截获、破解或篡改。

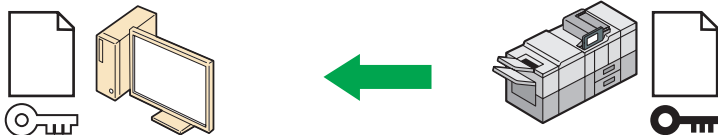
SSL/TLS 加密通信流程

1. 要从用户计算机访问机器，请申请 SSL/TLS 设备证书和公共密钥。



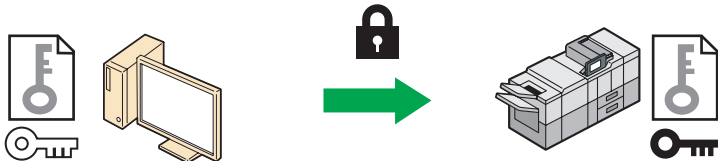
CZB002

2. 设备证书和公共密钥从机器发送到用户计算机。



CZB003

3. 计算机创建的共享密钥将使用公钥进行加密并发送给机器，然后使用机器中的私钥进行解密。



CZB004

4. 共享密钥用于数据加密和解密，从而实现安全的传送。



CZB005

使用自签证书时的配置流程

1. 创建和安装设备证书：
从控制面板或 Web Image Monitor 创建并安装设备证书。
2. 启用 SSL/TLS:

使用 Web Image Monitor 启用 SSL/TLS 设置。

使用证书颁发机构颁发的证书时的配置流程

1. 创建设备证书并应用到证书颁发机构：

在 Web Image Monitor 中创建设备证书以后，请将其应用到证书颁发机构。

创建证书后的申请步骤视证书颁发机构而定。请按证书颁发机构指定的步骤操作。

2. 安装设备证书：

使用 Web Image Monitor 安装设备证书。

3. 启用 SSL/TLS：

使用 Web Image Monitor 启用 SSL/TLS 设置。

注

- 要检查是否启用了 SSL/TLS 配置，请在 Web 浏览器的地址栏中输入 “https://（机器的 IP 地址或主机名）/” 以访问本机。如果出现消息 “无法显示该页”，说明当前 SSL/TLS 配置无效，请检查配置。
- 如果为 IPP（打印机功能）启用了 SSL/TLS，则系统会对发送的数据进行加密，从而防止数据被截取、分析或篡改。

启用 SSL/TLS

在机器中安装设备证书后，请启用 SSL/TLS 设置。

此步骤用于自签证书或证书颁发机构签发的证书。

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[SSL/TLS]。
4. 对于 IPv4 和 IPv6，如果您想要启用 SSL/TLS，请选择“有效”。
5. 选择“允许 SSL/TLS 通信”的加密通信模式。
6. 如果您要禁用协议，请单击“TLS1.2”、“TLS1.1”、“TLS1.0”或“SSL3.0”旁边的[无效]。
您必须至少启用这些协议之一。
7. 在“加密强度设置”下，为“AES”、“3DES”和/或“RC4”指定要应用的加密强度。必须勾选一个复选框。
请注意，根据您为“TLS1.2”、“TLS1.1”、“TLS1.0”或“SSL3.0”指定的设置，加密强度的可用性会有所不同。
8. 单击[确定]。

9. 将出现“正在更新...”。等待约 1 至 2 分钟后，单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

10. 注销。

↓ 注

- 如果您将“允许 SSL/TLS 通信”设置为[仅限密文]，并且选择的协议不支持 Web 浏览器，或仅指定了一个加密强度设置，则无法通信。出现这种情况，可使用机器的控制面板将[允许 SSL/TLS 通信]设置为[密文/明文]，然后指定正确的协议和加密强度，即可启动通信。
- 即使在[网络安全]下，SSL/TLS 版本和加密强度设置仍可以更改。
- 根据您为“TLS1.2”、“TLS1.1”、“TLS1.0”和“SSL3.0”指定的状态，机器可能无法连接到外部 LDAP 服务器。
- 以下类型的通信和数据始终由 SSL3.0 进行加密：通过@Remote 通信和传输到 Remote Communication Gate S 的日志。

SSL/TLS 的用户设置

在主单元上安装私人证书颁发机构的自签名证书或设备证书并启用 SSL/TLS（通信加密）以后，建议您指示用户在他们的计算机上安装该证书。对于希望通过 IPP-SSL 从 Windows Vista/7/8/8.1、Windows Server 2008/2008 R2/2012/2012 R2 进行打印的用户，尤其需要安装证书。网络管理员必须指示每个用户安装证书。

通过 IPP 访问机器时，请为证书保存位置选择[受信任的根证书颁发机构]。

↓ 注

- 当收到用户查询相关问题（如证书到期等）时，请采取相应步骤。
- 如果机器中安装了某证书颁发机构签发的证书，请与证书颁发机构确认证书的保存位置。
- 在 Windows Vista/7/8/8.1 或 Windows Server 2008/2008 R2/2012/2012 R2 下使用操作系统的标准 IPP 端口时，如果要更改设备证书的[通用名称]中的主机名或 IP 地址，请事先删除先前配置的 PC 打印机，并在更改[通用名称]后重新安装该打印机。此外，如果还要更改用户验证设置（登录用户名和密码），也请事先删除先前配置的 PC 打印机，并在更改用户验证设置后重新安装该打印机。

设置 SSL/TLS 加密模式

您可以通过指定 SSL/TLS 加密通信模式来更改安全等级。

加密的通信模式

使用加密的通信模式，可以指定加密的通信。

加密的通信模式	描述
仅限密文	只允许进行加密通信。 如果无法加密，机器将不会进行通信。
密文优先级	如果可以加密，则执行加密通信。 如果不能加密，机器将在不加密的情况下进行通信。
密文／明文	根据设置在加密或不加密的情况下通信。

安装设备证书后，请指定 SSL/TLS 加密通信模式。通过配置此设置，可以更改安全等级。

1. 以网络管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[接口设置]。
4. 按[▼向后]。
5. 按[允许 SSL/TLS 通信]。

5

6. 选择要使用的加密通信模式。
选择[仅限密文]、[密文优先级]或[密文／明文]作为加密的通信模式。
7. 按[确定]。
8. 注销。

注

- 还可以使用 Web Image Monitor 指定 SSL/TLS 加密通信模式。有关详细信息，请参见 Web Image Monitor 帮助。

为 SMTP 连接启用 SSL

使用以下步骤为 SMTP 连接启用 SSL 加密。

- 1. 以网络管理员身份从控制面板中登录。
- 2. 按[系统设置]。
- 3. 按[文件转送]。
- 4. 按[SMTP 服务器]。

SMTP服务器	smtpserver	电子
SMTP验证	关	在服务
SMTP之前的POP	关	
接收协议	POP3	
POP3/IMAP4设置		
管理员的电子邮件地址		
电子邮件通讯端口		

5

- 5. 在“使用安全连接 (SSL)” 中，请按[开]。
如果未使用用于 SMTP 连接的 SSL，则按[关]。
“使用安全连接(SSL)” 设置为[开]时，端口号将更改为 465。
- 6. 按[确定]。
- 7. 注销。

配置 S/MIME

通过在通讯簿中注册用户证书，您可以发送使用公共密钥加密的电子邮件，这防止了邮件内容在传送过程中被改动。您还可以防止发送者通过在机器上安装设备证书，并附加使用个人密钥创建的电子签名进行假冒（欺骗）。您可以单独应用这些功能或将这些功能一起应用来提高安全性。

要发送加密的电子邮件，发送者（本机）和接收者都必须支持 S/MIME。

★重要信息

- 要使用 S/MIME，您必须先在[系统设置]中指定[管理员的电子邮件地址]。

兼容的邮件应用程序

S/MIME 功能可与以下应用程序一起使用：

- Microsoft Outlook 2003 和更高版本
- Thunderbird 3.1.7 和更高版本
- Windows Live Mail

↓注

- 如果已为电子邮件指定了电子签名，管理员的地址会出现在“发件人”字段中，而用户的地址将会被指定为“发送者”而出现在“回复”字段中。
- 给邮件客户端支持 S/MIME 的用户和客户端不支持 S/MIME 的用户发送电子邮件时，针对 S/MIME 客户端的电子邮件会进行加密，而针对非 S/MIME 客户端的电子邮件则以纯文本形式发送。
- 使用 S/MIME 时，电子邮件大小会超过普通大小。
- 有关将 S/MIME 与扫描仪功能一起使用的详细信息，请参见《扫描》中的“电子邮件安全设置”。

电子邮件加密

要使用 S/MIME 发送加密的电子邮件，必须先使用 Web Image Monitor 准备用户证书，然后由用户管理员在通讯簿中注册该证书。在通讯簿中注册证书会指定每个用户的公共密钥。安装证书后，使用 Web Image Monitor 指定加密算法。网络管理员可以指定算法。

电子邮件加密

1. 准备用户证书。
2. 使用 Web Image Monitor 在通讯簿中安装用户证书。（在通讯簿中指定证书上的公共密钥。）
3. 使用 Web Image Monitor 指定加密算法。
4. 使用共享密钥加密电子邮件消息。
5. 使用用户的公共密钥加密共享密钥。

6. 发送加密的电子邮件。
7. 接收者使用与公共密钥对应的密钥解密共享密钥。
8. 使用共享密钥解密电子邮件。

 注

- 可在本机中安装 3 种类型的用户证书：“DER Encoded Binary X.509”、“Base 64 Encoded X.509”和“PKCS #7”证书。
- 使用 Web Image Monitor 将用户证书安装到通讯簿时，如果证书文件包含多个证书，可能会出现一条错误信息。如果出现这种情况，则一次只安装一个证书。

指定用户证书

提前准备每个用户证书。

5

1. 以用户管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[地址簿]。
3. 选择要为其安装证书的用户。
4. 单击[详细输入]，然后单击[更改]。
将出现更改用户屏幕。
5. 在“电子邮件”下的“电子邮件地址”字段中输入用户地址。
6. 单击“用户证书”中的[更改]。
7. 单击[浏览]，选择用户证书文件，然后单击[打开]。
8. 单击[确定]。
将安装用户证书。
9. 将出现“正在更新...”。等待约 1 至 2 分钟后，单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

10. 注销。

 注

- 选定的用户证书有效期过了以后，系统将无法再发送加密的消息。选择处于有效期内的证书。

指定加密算法

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[S/MIME]。

4. 在“加密”下，从“加密算法”旁边的下拉菜单中选择加密算法。

5. 单击[确定]。

将设置针对 S/MIME 的算法。

6. 注销。

注

- 配置涉及用户电子邮件软件支持的加密算法和摘要算法的设置。

附加电子签名

要附加电子签名以发送电子邮件，必须预先安装设备证书。

作为设备证书，您可以使用由机器创建的自签证书或由证书颁发机构颁发的证书。有关创建和安装设备证书的详细信息，请参见 p.108 “通过设备证书保护通信路径”。

★重要信息

- 要安装 S/MIME 设备证书，您必须先在[系统设置]中将“管理员的电子邮件地址”注册为设备证书的电子邮件地址。请注意，即使未使用 S/MIME，您也必须为 S/MIME 设备证书指定电子邮件地址。

电子签名

1. 在机器中安装设备证书。在机器中配置该证书上的密钥。
2. 使用由设备证书提供的密钥将电子签名附加到电子邮件。
3. 将附加了电子签名的电子邮件发送给用户。
4. 接收者从机器申请公共密钥和设备证书。
5. 使用公共密钥，您可以确定附加的电子签名的真实性，以了解消息是否发生了变动。

配置流程（自签证书）

1. 使用 Web Image Monitor 创建和安装设备证书。
2. 使用 Web Image Monitor 配置要用于 S/MIME 的证书设置。
3. 使用 Web Image Monitor 配置电子签名设置。

配置流程（证书颁发机构签发的证书）

1. 使用 Web Image Monitor 创建设备证书。
已创建证书的申请步骤视证书颁发机构而定。请按证书颁发机构指定的步骤操作。
2. 使用 Web Image Monitor 安装设备证书。
3. 使用 Web Image Monitor 配置要用于 S/MIME 的证书设置。
4. 使用 Web Image Monitor 配置电子签名设置。

选择设备证书

使用 Web Image Monitor 选择要用于 S/MIME 的设备证书。

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[设备证书]。
4. 在“证书”下，从“S/MIME”中的下拉框中选择要用于电子签名的证书。
5. 单击[确定]。

将设置要用于 S/MIME 电子签名的证书。

6. 将出现“正在更新...”。等待约 1 至 2 分钟后，单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

7. 注销。

注

- 如果选定的设备证书已过期，则签名无法附加到电子邮件中。选择处于有效期内的证书。

指定电子签名

将设备证书安装到机器以后，请为 S/MIME 签名配置条件。无论您是使用自签证书还是使用由证书颁发机构签发的证书，配置步骤都是相同的。

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[S/MIME]。
4. 在“签名”下选择“摘要算法”，然后选择要在电子签名中使用的摘要算法。
5. 在“签名”下选择“当通过扫描仪发送电子邮件时”，然后选择从扫描仪发送电子邮件时附加电子签名的方法。
6. 在“签名”下选择“当转送文件保存在服务器(实用程序)中时”，然后选择转发保存的文件时附加电子签名的方法。
7. 单击[确定]。

将启用针对 S/MIME 电子签名的设置。

8. 注销。

注

- 根据用户电子邮件软件支持的加密算法和摘要算法配置设置。

检查证书的有效期

发送电子邮件时，系统将验证 S/MIME 所用证书的有效期。
您可以更改检查有效期的时间。

操作模式	描述
安全优先	系统会在以下时间验证有效期： 用户证书 (a) 选择地址时 (b) 按[开始]键时 设备证书 (c) 选择第一个地址时 (d) 按[开始]键时
执行优先	不执行(b)和(c)。 如果选择了地址或按下[开始]键，则可能更长时间来验证有效期。要缩短时间，请选择“执行优先”。

5

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[S/MIME]。
4. 在“操作模式”中，选择[安全优先]或[执行优先]。
5. 单击[确定]。
6. 注销。

↓ 注

- 如果证书在传送时有效，但在将电子邮件从邮件服务器提取到客户端计算机之前过期，则可能无法提取该电子邮件。
- 使用“记忆传送”或在指定时间自动发送 S/MIME 电子邮件时，如果在证书有效期之后发生错误，则会以纯文本形式向发件人或管理员的电子邮件地址发送电子邮件来报告错误。您可以在作业日志中查看错误详细信息。使用 S/MIME 时，请务必启用作业日志收集功能。有关查看日志的详细信息，请参见 p.173 “管理日志文件”。

配置带有电子签名的 PDF

本机可以创建带有电子签名的 PDF。带有电子签名的 PDF 可以证明 PDF 文件的创建者以及创建的日期和时间。由于可以检测被篡改的文件，因此可以防止篡改。

要创建带有电子签名的 PDF，请首先从创建并安装的设备证书中选择用于签名的证书。

作为设备证书，您可以使用由机器创建的自签证书或由证书颁发机构颁发的证书。有关创建和安装设备证书的详细信息，请参见 p.108 “通过设备证书保护通信路径”。

★重要信息

- 要创建数字签名的 PDF，首先必须在[系统设置]的[文件转送]中指定[管理员的电子邮件地址]。
- 要将设备证书用于数字签名的 PDF，首先必须指定管理员的电子邮件地址，以使之等同于在[系统设置]中注册的“管理员的电子邮件地址”。

5

选择用于签名的证书。

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[设备证书]。
4. 在“证书”下的“PDF 数字签名”或“PDF/A 数字签名”中，从下拉框选择用于电子签名的证书。

PDF 数字签名：此签名可以附加到不同于 PDF/A 格式的 PDF。

PDF/A 数字签名：此签名可以附加到 PDF/A 格式的 PDF。

5. 单击[确定]。
6. 将出现“正在更新...”。等待约 1 至 2 分钟，然后单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

7. 注销。

↓注

- 如果选定的设备证书已过期，则签名将无法附加到 PDF。选择处于有效期内的证书。
- 可以连接到 PDF/A 文件的设备证书的数字签名的签名算法是“sha1WithRSA-1024”。

配置 IPsec 设置

为了实现通信安全性，本机支持 IPsec。IPsec 使用共享密钥的加密方法在 IP 协议级别传送安全数据包，其中发送者和接收者保留相同的密钥。本机使用自动密钥交换来为双方配置预共享的密钥。通过使用自动交换设置，您可以在指定的有效期内更新共享密钥交换设置，从而实现更高的传送安全性。

★重要信息

- 为“排除 HTTPS 通信”指定“无效”时，若未正确配置密钥设置，访问 Web Image Monitor 将会失败。为防止出现此种状况，通过选择“有效”，可指定 IPsec 以排除 HTTPS 传送。若要包括 HTTPS 传送，确认正确配置 IPsec 后，建议您为“排除 HTTPS 通信”选择“无效”。为“排除 HTTPS 通信”选择“有效”时，即使未通过 IPsec 确定 HTTPS 传送，通过 IPsec 从计算机侧确定 TCP 时，Web Image Monitor 也可能变得无法使用。
- 如果由于 IPsec 配置问题导致您无法访问 Web Image Monitor，请在控制面板的系统设置中禁用 IPsec，然后访问 Web Image Monitor。
- 有关使用控制面板启用和禁用 IPsec 的详细信息，请参见《连接机器/系统设置》中的“接口设置”。
- IPsec 不适用于通过 DHCP、DNS 或 WINS 获取的数据。

5

所支持的操作系统

操作系统	注意事项
• Windows Server 2003/2003 R2	可使用通过 IPv4 实现的 IPsec。
• Windows Vista/7/8/8.1 • Windows Server 2008/2008 R2/2012/2012 R2 • Mac OS X 10.4.8 或更高版本 • Red Hat Enterprise Linux WS 4.0 • Solaris 10	可使用通过 IPv4 和 IPv6 实现的 IPsec。

根据操作系统，某些设置项目不受支持。请确保所指定的 IPsec 设置与操作系统的 IPsec 设置一致。

通过 IPsec 进行加密和验证

IPsec 包括 2 大功能，即加密功能和验证功能，前者用于确保数据的机密性，后者用于验证数据的发送者及数据的完整性。本机的 IPsec 功能支持 2 个安全协议，即 ESP 协议和 AH 协议，前者同时支持 IPsec 的这两种功能，而后者仅支持验证功能。

ESP 协议

ESP 协议提供通过加密和验证的安全传送功能。此协议不提供报头验证。

- 为实现成功加密，发送者和接收者必须指定相同的加密算法和加密密钥。如果使用加密密钥自动交换方法，则会自动指定加密算法和加密密钥。
- 为实现成功验证，发送者和接收者必须指定相同的验证算法和验证密钥。如果使用加密密钥自动交换方法，则会自动指定验证算法和验证密钥。

AH 协议

AH 协议通过仅验证数据包（包括报头）的方式提供安全传送功能。

- 为实现成功验证，发送者和接收者必须指定相同的验证算法和验证密钥。如果使用加密密钥自动交换方法，则会自动指定验证算法和验证密钥。

AH 协议+ESP 协议

合并之后，ESP 和 AH 协议通过加密和验证提供安全传送功能。这些协议提供报头验证。

- 为实现成功加密，发送者和接收者必须指定相同的加密算法和加密密钥。如果使用加密密钥自动交换方法，则会自动指定加密算法和加密密钥。
- 为实现成功验证，发送者和接收者必须指定相同的验证算法和验证密钥。如果使用加密密钥自动交换方法，则会自动指定验证算法和验证密钥。

↓ 注

- 某些操作系统使用术语“符合”来代替“验证”。

加密密钥自动交换设置

对于密钥配置，本机支持使用自动密钥交换来为发送者和接收者双方指定 IPsec 算法等协议。此类协议即构成所谓的 SA（安全关联）。仅当接收者和发送者的 SA 设置相同时，才能进行 IPsec 通信。

如果使用自动交换方法指定加密密钥，则会在双方的机器上自动配置 SA 设置。但在设置 IPsec SA 之前，将自动配置 ISAKMP SA（阶段 1）设置。之后，将自动配置 IPsec SA（阶段 2）设置，通过这些设置进行实际 IPsec 传送。

此外，为了进一步实现安全性，通过为 SA 设置应用有效期（时间限制）来自动定期更新 SA。对于加密密钥自动交换，本机仅支持 IKEv1。

请注意，可以配置多个 SA。

设置 1-4 和默认设置

使用自动交换方法，您可以分别配置四组 SA 详细信息（如，不同的共享密钥和 IPsec 算法）。在这些组的默认设置中，您可以包括 1 到 4 组的字段中无法包含的设置。

启用 IPsec 时，组 1 的优先级最高，组 4 的优先级最低。您可以使用此优先级系统更加安全地定位 IP 地址。例如，在最低优先级（4）处设置最宽的 IP 范围，而在较高的优先级（3 或更高）处设置特定的 IP 地址。这样，当为特定 IP 地址启用 IPsec 传送时，系统将应用较高等级的设置。

IPsec 设置

本设备的 IPsec 设置可在 Web Image Monitor 上进行设置。下表介绍了各个设置项目。

IPsec 设置项目

设置	描述	设置值
IPsec	指定是启用还是禁用 IPsec。	• 有效 • 无效
排除 HTTPS 通信	指定是否支持 IPsec 进行 HTTPS 传送。	• 有效 • 无效 如果不想使用 IPsec 进行 HTTPS 传送，请指定“有效”。

您还可以从控制面板配置 IPsec 设置。

加密密钥自动交换安全等级

选择某个安全等级后，就会自动配置一定的安全设置。下表介绍了安全等级特性。

安全等级	安全等级特性
仅验证	如果要验证传送方并防止未经授权篡改数据，但不执行数据包加密，请选择此等级。 由于数据以明文发送，因此数据包易于受到窃听攻击。如果要交换敏感信息，请勿选择此等级。
验证和低等级的加密	如果要加密数据包和验证传送方，并防止未经授权篡改数据，请选择此等级。数据包加密有助于防止窃听攻击。此等级提供的安全性低于“验证和高等级的加密”。

安全等级	安全等级特性
验证和高等级的加密	如果要加密数据包和验证传送方，并防止未经授权篡改数据，请选择此等级。数据包加密有助于防止窃听攻击。此等级提供的安全性高于“验证和低等级的加密”。

下表列出了根据安全等级自动配置的设置。

设置	仅验证	验证和低等级的加密	验证和高等级的加密
安全策略	应用	应用	应用
封装模式	传输	传输	传输
IPsec 需求等级	当在可能的情况下使用	当在可能的情况下使用	始终需要
验证方式	PSK	PSK	PSK
阶段 1 散列算法	MD5	SHA1	SHA256
阶段 1 加密算法	DES	3DES	AES-128-CBC
阶段 1 Diffie-Hellman 组	2	2	2
阶段 2 安全协议	AH	ESP	ESP
阶段 2 验证算法	HMAC-SHA1-96/ HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256	HMAC-SHA1-96/ HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256	HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256
阶段 2 加密算法许可	明文（NULL 加密）	3DES/AES-128/ AES-192/ AES-256	AES-128/AES-192/ AES-256
阶段 2 PFS	无效	无效	2

加密密钥自动交换设置项目

指定安全等级后，将自动配置相应的安全设置，但其他设置（如，地址类型、本地地址和远程地址）仍必须手动进行配置。

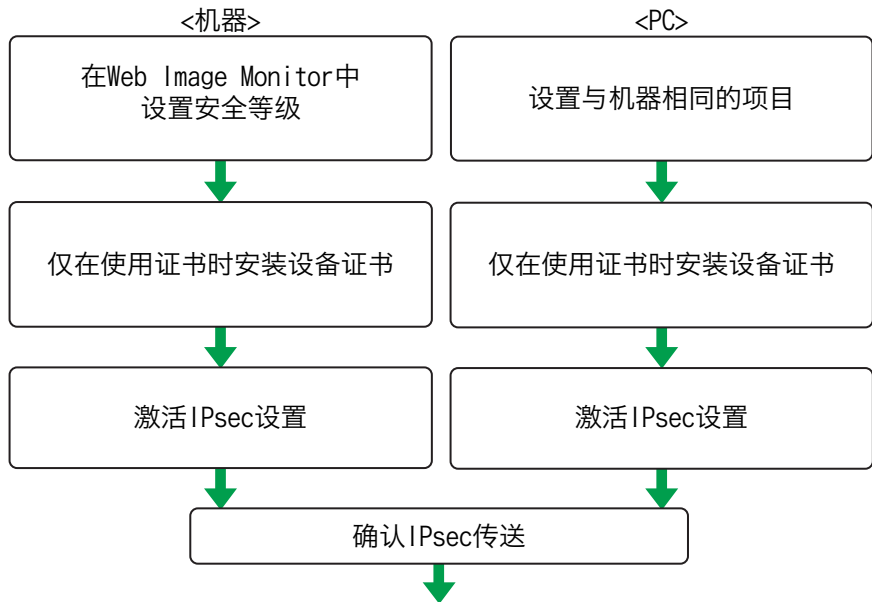
指定安全等级后，仍可对自动配置的设置进行更改。更改自动配置的设置后，安全等级会自动切换到“用户设定”。

设置	描述	设置值
地址类型	指定使用 IPsec 传送的地址类型。	• 无效 • IPv4 • IPv6 • IPv4/IPv6（仅限默认设置）
本地地址	指定机器的地址。如果使用 IPv6 中的多个地址，也可以指定地址范围。	机器的 IPv4 或 IPv6 地址。 如果未设置地址范围，请在 IPv4 地址后输入 32，或在 IPv6 地址后输入 128。
远程地址	指定 IPsec 传送方的地址。您也可以指定地址范围。	IPsec 传送方的 IPv4 或 IPv6 地址。 如果未设置地址范围，请在 IPv4 地址后输入 32，或在 IPv6 地址后输入 128。
安全策略	指定处理 IPsec 的方式。	• 应用 • 手送 • 废弃
封装模式	指定封装模式。 (自动设置)	• 传输 • 通道 如果指定“通道”，则必须指定“通道端点”，即起始和结束 IP 地址。将起始点的地址设置为您在“本地地址”中设置的地址。

设置	描述	设置值
IPsec 需求等级	指定是仅使用 IPsec 传送，还是在无法建立 IPsec 时允许明文传送。 (自动设置)	• 当在可能的情况下使用 • 始终需要
验证方式	指定用于验证传送方的方法。 (自动设置)	• PSK • 证书 如果指定“PSK”，则必须设置 PSK 文本（使用 ASCII 字符）。 如果使用“PSK”，请指定 PSK 密码（最多使用 32 个 ASCII 字符）。 如果指定“证书”，则必须先安装并指定 IPsec 的证书，然后才能使用。
PSK 字符串	为 PSK 验证指定预共享密钥。	输入 PSK 验证所需的预共享密钥。
阶段 1 散列算法	指定要在阶段 1 中使用的散列算法。 (自动设置)	• MD5 • SHA1 • SHA256 • SHA384 • SHA512
阶段 1 加密算法	指定要在阶段 1 中使用的加密算法。 (自动设置)	• DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC
阶段 1 Diffie-Hellman 组	选择用于生成 IKE 加密密钥的 Diffie-Hellman 组编号。 (自动设置)	• 1 • 2 • 14

设置	描述	设置值
阶段 1 有效期	指定 SA 设置在阶段 1 中生效的时间段。	设置范围（以秒计），从 300 秒（5 分钟）到 172800 秒（48 小时）。
阶段 2 安全协议	指定要在阶段 2 中使用的安全协议。 若要向所发送数据同时应用加密和验证，请指定“ESP”或“ESP+AH”。 若要仅应用验证数据，请指定“AH”。 (自动设置)	• ESP • AH • ESP+AH
阶段 2 验证算法	指定要在阶段 2 中使用的验证算法。 (自动设置)	• HMAC-MD5-96 • HMAC-SHA1-96 • HMAC-SHA256-128 • HMAC-SHA384-192 • HMAC-SHA512-256
阶段 2 加密算法许可	指定要在阶段 2 中使用的加密算法。 (自动设置)	• 明文（NULL 加密） • DES • 3DES • AES-128 • AES-192 • AES-256
阶段 2 PFS	指定是否激活 PFS。如果激活了 PFS，则随后选择 Diffie-Hellman 群组。 (自动设置)	• 无效 • 1 • 2 • 14
阶段 2 有效期	指定 SA 设置在阶段 2 中生效的时间段。	指定时间段（以秒计），从 300（5 分钟）到 172800（48 小时）。

加密密钥自动交换设置配置流程



CJD015

★重要信息

- 要使用证书验证加密密钥自动交换设置中的传送方，必须安装设备证书。
- 配置完 IPsec 后，您可以使用“Ping”命令来检查是否正确地建立了连接。但是，当 ICMP 在计算机端被排除在 IPsec 传送之外时，您无法使用“Ping”命令。此外，因为初始密钥交换期间响应缓慢，可能需要一些时间来确认已经建立了的传送。

指定加密密钥自动交换设置

若要将加密密钥自动交换设置的传送方的验证方法更改为“证书”，您必须首先安装并分配证书。有关创建和安装设备证书的详细信息，请参见 p.108 “通过设备证书保护通信路径”。有关向 IPsec 分配安装证书的方式，请参见 p.131 “选择用于 IPsec 的证书”。

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[IPsec]。
4. 在“加密密钥自动交换设置”下，单击[编辑]。
5. 在[设置 1]中进行加密密钥自动交换设置。
如果要进行多次设置，选择设置次数并添加设置。
6. 单击[确定]。
7. 在“IPsec”中将“IPsec”选为[有效]。

8. 如果不想使用 IPsec 进行 HTTPS 传送，将“排除 HTTPS 通信”设置为[有效]。
9. 单击[确定]。
10. 将出现“正在更新...” 。等待约 1 至 2 分钟，然后单击[确定]。
单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。
11. 注销。

选择用于 IPsec 的证书

使用 Web Image Monitor，选择要用于 IPsec 的证书。使用证书前必须安装证书。有关创建和安装设备证书的详细信息，请参见 p.108 “通过设备证书保护通信路径”。

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[设备证书]。
4. 从“证书”的“IPsec”下的下拉框中选择要用于 IPsec 的证书。
5. 单击[确定]。

IPsec 的证书已指定。

6. 将出现“正在更新...” 。等待约 1 至 2 分钟，然后单击[确定]。
单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。
7. 注销。

指定计算机的 IPsec 设置。

配置计算机的 IPsec SA 设置，以便它们与机器的安全等级完全匹配。设置方法因计算机操作系统而异。此处所示的示例步骤是在选择验证和低等级的加密时使用 Windows 7。

1. 在[开始]菜单中，单击[控制面板]，再单击[系统和安全]，然后单击[管理工具]。
在 Windows 8 下，将鼠标指针悬停在屏幕的顶部或右下角，然后依次单击[设置]、[控制面板]、[系统和安全]，最后单击[管理工具]。
2. 双击[本地安全策略]。
如果出现“用户帐户控制”对话框，请单击[是]。
3. 单击[IP 安全策略，在本地计算机上]。
4. 在“操作”菜单中，单击[创建 IP 安全策略]。
出现 IP 安全策略向导。
5. 单击[下一步]。

6. 在“名称”中输入安全策略名称，然后单击[下一步]。
7. 清除“激活默认响应规则”复选框，然后单击[下一步]。
8. 选择“编辑属性”，然后单击[完成]。
9. 在“常规”选项卡中，单击[设置]。
10. 在“身份验证和生成新密钥间隔”中，输入在“加密密钥自动交换设置阶段 1”中指定的机器上的相同有效期（分钟），然后单击[方法]。
11. 检查“安全方法优先顺序”中的散列算法（“完整性”）、加密算法（“加密”）和“Diffie-Hellman 组”设置是否全部与机器上的“加密密钥自动交换设置阶段 1”中指定的设置一致。

如果没有显示设置，单击[添加]。

12. 单击[确定]两次。
13. 在“规则”选项卡中单击[添加]。

出现安全规则向导。

14. 单击[下一步]。
15. 选择“此规则不指定隧道”，然后单击[下一步]。
16. 选择 IPsec 的网络类型，然后单击[下一步]。
17. 在 IP 筛选器列表中单击[添加]。
18. 在[名称]中，输入 IP 筛选器名称，然后单击[添加]。

出现 IP 筛选器向导。

19. 单击[下一步]。
20. 如果需要，请输入 IP 筛选器说明，然后单击[下一步]。
21. 在“源地址”中选择“我的 IP 地址”，然后单击[下一步]。
22. 在“目标地址”中选择“一个特定的 IP 地址或子网”，输入机器的 IP 地址，然后单击[下一步]。
23. 选择 IPsec 的协议类型，然后单击[下一步]。

如果您将 IPsec 与 IPv6 搭配使用，请选择“58”作为“其他”目标协议类型的协议编号。

24. 单击[完成]。
25. 单击[确定]。
26. 选择刚创建的 IP 筛选器，然后单击[下一步]。
27. 单击[添加]。

此时会出现筛选器操作向导。

28. 单击[下一步]。
29. 在[名称]中，输入 IP 筛选器操作名称，然后单击[下一步]。

30. 选择“协商安全”，然后单击[下一步]。
31. 选择“如果无法建立安全的连接，则允许无安全性的通讯。”，然后单击[下一步]。
32. 选择“自定义”，然后单击[设置]。
33. 在“完整性算法”中，选择在“加密密钥自动交换设置阶段 2”中指定的机器上的验证算法。
34. 在“加密算法”中，选择在“加密密钥自动交换设置阶段 2”中指定的机器上的加密算法。
35. 在会话密钥设置中，选择“生成新密钥间隔”，然后输入在机器的“加密密钥自动交换设置阶段 2”中指定的有效期（秒）。
36. 单击[确定]。
37. 单击[下一步]。
38. 单击[完成]。
39. 选择刚创建的筛选器操作，然后单击[下一步]。

如果您将“加密密钥自动交换设置”设置为“验证和高等级的加密”，请选择刚创建的 IP 筛选器操作，单击[编辑]，然后选中筛选器上“使用会话密钥完美转发保密(PFS)”的属性对话框。如果在 Windows 中使用 PFS，则阶段 2 中使用的 PFS 组号将在阶段 1 从 Diffie-Hellman 组号自动议定（在步骤 11 中设置）。因此，如果您更改了本机上自动设置中指定的安全级别，并且出现了“用户设定”，必须在本机上设置相同的“阶段 1 Diffie-Hellman 组”和“阶段 2 PFS”组号以便建立 IPsec 传输。
40. 选择验证方法，然后单击[下一步]。

如果在机器上的“加密密钥自动交换设置”中选择“证书”作为验证方法，请指定设备证书。

如果选择“PSK”，请输入在机器上指定的相同 PSK 文本和预共享密钥。
41. 单击[完成]。
42. 单击[确定]。

新的 IP 安全策略（IPsec 设置）即被指定。
43. 选择刚创建的安全策略，右键单击，然后单击[分配]。

将启用计算机的 IPsec 设置。

↓ 注

- 要禁用计算机的 IPsec 设置，请选择安全策略，右键单击，然后单击[取消分配]。

telnet 设置命令

您可以使用 telnet 来确认 IPsec 设置和更改设置。本节介绍用于 IPsec 的 telnet 命令。有关用于登录 telnet 的用户名和密码的信息，请向管理员咨询。有关登录到 telnet 和 telnet 操作的详细信息，请参见《连接机器/系统设置》中的“使用 telnet 进行远程维护”。

★重要信息

- 如果您要使用证书作为加密密钥自动交换设置（IKE）中的验证方法，使用 Web Image Monitor 安装证书。无法使用 telnet 安装证书。

ipsec

若要显示 IPsec 相关设置信息，使用 “ipsec” 命令。

显示当前设置

```
msh> ipsec
```

显示以下 IPsec 设置信息：

- IPsec 设置值
- 加密密钥自动交换设置，IKE 设置 1-4 值
- 加密密钥自动交换设置，IKE 默认设置值

显示当前设置部分

```
msh> ipsec -p
```

- 显示部分中的 IPsec 设置信息。

ipsec exclude

若要显示或指定 IPsec 排除的协议，使用 “ipsec exclude” 命令。

显示当前设置

```
msh> ipsec exclude
```

- 显示当前从 IPsec 传送中排除的协议。

指定要排除的协议

```
msh> ipsec exclude {https|dns|dhcp|wins|all} {on|off}
```

- 指定协议，然后输入[on]或者[off]，以在 IPsec 传送中排除或包括该协议。输入 [all]可以集中指定所有协议。

ipsec ike

若要显示或指定加密密钥自动交换设置，使用 “ipsec ike” 命令。

显示当前设置

```
msh> ipsec ike {1|2|3|4|default}
```

- 若要显示设置 1-4，请指定编号[1-4]。
- 若要显示默认设置，请指定[default]。
- 不指定任何值会显示全部设置。

禁用设置

```
msh> ipsec ike {1|2|3|4|default} disable
```

- 若要禁用设置 1-4，请指定编号[1-4]。
- 若要禁用默认设置，请指定[default]。

指定用户专有的本地地址/远程地址。

```
msh> ipsec ike {1|2|3|4} {ipv4|ipv6} "local address" "remote address"
```

- 输入设置编号[1-4]中的一个编号和地址类型以指定本地和远程地址。
- 若要设置本地或远程地址值，设置 IPv4 地址时，通过输入[/]和 0 到 32 之间的一个整数来指定 masklen。设置 IPv6 地址时，通过输入[/]和 0 到 128 之间的一个整数来指定 masklen。
- 不指定地址值会显示当前设置。

指定默认设置的地址类型

```
msh> ipsec ike default {ipv4|ipv6|any}
```

- 指定默认设置的地址类型。
- 若要指定 IPv4 和 IPv6，输入[any]。

安全策略设置

```
msh> ipsec ike {1|2|3|4|default} proc {apply|bypass|discard}
```

- 输入设置编号[1-4]中的一个编号或输入[default]，并指定在所选设置中指定的地址的安全策略。
- 若要将 IPsec 应用到相关包，指定[apply]。不想应用 IPsec，指定[bypass]。
- 如果指定[discard]，则可以应用 IPsec 的任何包都将被丢弃。
- 不指定安全策略会显示当前设置。

安全协议设置

```
msh> ipsec ike {1|2|3|4|default} proto {ah|esp|dual}
```

- 输入单独的设置编号[1-4]或[default]，然后指定安全协议。
- 若要指定 AH，请输入[ah]。若要指定 ESP，请输入[esp]。若要指定 AH 和 ESP，请输入[dual]。
- 不指定协议会显示当前设置。

IPsec 要求等级设置

```
msh> ipsec ike {1|2|3|4|default} level {require|use}
```

- 输入单独的设置编号[1-4]或[default]，然后指定 IPsec 需求等级。
- 如果指定[require]，当无法使用 IPsec 时数据将不会被传送。如果指定[use]，当无法使用 IPsec 时数据将被正常发送。可以使用 IPsec 时，会执行 IPsec 传送。
- 不指定要求等级会显示当前设置。

封装模式设置

```
msh> ipsec ike {1|2|3|4|default} mode {transport|tunnel}
```

- 输入单独的设置编号[1-4]或[default]，然后指定封装模式。
- 若要指定传输模式，请输入[transport]。若要指定通道模式，请输入[tunnel]。
- 如果已经在默认设置中将地址类型设置为[any]，则不能在封装模式中使用[tunnel]。
- 不指定封装模式会显示当前设置。

通道端点设置

```
msh> ipsec ike {1|2|3|4|default} tunneladdr "beginning IP address" "ending IP address"
```

- 输入设置编号[1-4]中的一个编号或输入[default]，然后指定通道端点的起始和结束 IP 地址。
- 不指定起始或结束地址会显示当前设置。

IKE 合作验证方法设置

```
msh> ipsec ike {1|2|3|4|default} auth {psk|rsasig}
```

- 输入单独的设置编号[1-4]或[default]，然后指定验证方法。
- 指定[psk]以使用共享密钥作为验证方法。指定[rsasig]以使用证书作为验证方法。
- 选择[psk]时，还必须指定 PSK 字符串。
- 请注意，如果选择“证书”，则必须先安装并指定 IPsec 的证书，然后才能使用它。要安装和指定证书，使用 Web Image Monitor。

PSK 字符串设置

```
msh> ipsec ike {1|2|3|4|default} psk "PSK character string"
```

- 如果选择 PSK 作为验证方法，输入设置编号[1-4]中的一个编号或输入[default]并指定 PSK 字符串。
- 指定 ASCII 字符形式的字符串。其中不能包含任何缩写词。

ISAKMP SA（阶段 1）散列算法设置

```
msh> ipsec ike {1|2|3|4|default} ph1 hash {md5|sha1|sha256|sha384|sha512}
```

- 输入设置编号[1-4]中的一个编号或输入[default]，并指定 ISAKMP SA（阶段 1）散列算法。
- 不指定散列算法会显示当前设置。

ISAKMP SA（阶段 1）加密算法设置

```
msh> ipsec ike {1|2|3|4|default} ph1 encrypt {des|3des|aes128|aes192|aes256}
```

- 输入设置编号[1-4]中的一个编号或输入[default]，并指定 ISAKMP SA（阶段 1）加密算法。
- 不指定加密算法会显示当前设置。

ISAKMP SA (阶段 1) Diffie-Hellman 群组设置

```
msh> ipsec ike {1|2|3|4|default} ph1 dhgroup {1|2|14}
```

- 输入设置编号[1-4]中的一个编号或输入[default]，并指定 ISAKMP SA (阶段 1) Diffie-Hellman 群组数。
- 指定要使用的群组数。
- 不指定群组数会显示当前设置。

ISAKMP SA (阶段 1) 有效期设置

```
msh> ipsec ike {1|2|3|4|default} ph1 lifetime "validity period"
```

- 输入设置编号[1-4]中的一个编号或输入[default]，并指定 ISAKMP SA (阶段 1) 有效期。
- 输入有效期 (秒)，范围从 300 到 172800。
- 不指定有效期会显示当前设置。

IPsec SA (阶段 2) 验证算法设置

```
msh> ipsec ike {1|2|3|4|default} ph2 auth {hmac-md5|hmac-sha1|hmac-sha256|hmac-sha384|hmac-sha512}
```

- 输入设置编号[1-4]中的一个编号或输入[default]，并指定 IPsec SA (阶段 2) 验证算法。
- 用逗号 (,) 分隔多个加密算法条目。当前设置值会以最高优先级顺序显示。
- 不指定验证算法会显示当前设置。

IPsec SA (阶段 2) 加密算法设置

```
msh> ipsec ike {1|2|3|4|default} ph2 encrypt {null|des|3des|aes128|aes192|aes256}
```

- 输入设置编号[1-4]中的一个编号或输入[default]，并指定 IPsec SA (阶段 2) 加密算法。
- 用逗号 (,) 分隔多个加密算法条目。当前设置值会以最高优先级顺序显示。
- 不指定加密算法会显示当前设置。

IPsec SA (阶段 2) PFS 设置

```
msh> ipsec ike {1|2|3|4|default} ph2 pfs {none|1|2|14}
```

- 输入设置编号[1-4]中的一个编号或输入[default]，并指定 IPsec SA (阶段 2) Diffie-Hellman 群组数。
- 指定要使用的群组数。
- 不指定群组数会显示当前设置。

IPsec SA (阶段 2) 有效期设置

```
msh> ipsec ike {1|2|3|4|default} ph2 lifetime "validity period"
```

- 输入设置编号[1-4]中的一个编号或输入[default]，并指定 IPsec SA（阶段 2）有效期。
- 输入有效期（秒），范围从 300 到 172800。
- 不指定有效期会显示当前设置。

重置设置值

```
msh> ipsec ike {1|2|3|4|default|all} clear
```

- 输入单独的设置编号[1-4]或[default]，然后重设指定的设置。指定[all]重置所有设置，包括默认值。

配置 IEEE 802.1X 验证

IEEE 802.1X 是验证标准和它使用的验证服务器（RADIUS 服务器）。

共有 4 种 EAP 验证方式可供选择：EAP-TLS、LEAP、EAP-TTLS 和 PEAP。请注意每种 EAP 验证方法都有不同配置设置和验证步骤。

证书的类型和要求如下：

EAP 类型	所需证书
EAP-TLS	站点证书、设备证书（IEEE 802.1X 客户端证书）
LEAP	-
EAP-TTLS	站点证书
PEAP	站点证书
PEAP（阶段 2 仅用于 TLS）	站点证书、设备证书（IEEE 802.1X 客户端证书）

5

安装站点证书

安装站点证书（根目录 CA 证书），用于核实验证服务器的可靠性。您至少需要一个由签署了服务器证书的证书颁发机构或更高级别的证书颁发机构颁发的证书。

只能导入 PEM（Base64 编码的 X.509）站点证书。

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[站点证书]。
4. 单击“导入的站点证书”的[浏览]，然后选择所获得的 CA 证书。
5. 单击[打开]。
6. 单击[导入]。
7. 检查所导入的证书的[状态]是否显示“可信的”。
- 如果[站点证书检查]显示[有效]，而证书的[状态]显示[不可信的]，则可能无法通信。
8. 单击[确定]。
9. 注销。

选择设备证书

从事先在机器上创建并安装的设备证书中，选择要在 IEEE 802.1X 下使用的证书。有关创建和安装设备证书的详细信息，请参见 p.108 “通过设备证书保护通信路径”。

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[设备证书]。
4. 从“证书”下的“IEEE 802.1X”中的下拉框中选择要用于 IEEE 802.1X 的证书。
5. 单击[确定]。
6. 将出现“正在更新...”。等待约 1 至 2 分钟，然后单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

7. 注销。

为以太网设置 IEEE 802.1X 项

1. 以网络管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“安全”下，单击[IEEE 802.1X]。
4. 在“用户名称”中输入在 RADIUS 服务器中设置的用户名。
5. 在“域名”中输入域名。
6. 选择“EAP 类型”。EAP 类型不同，配置也不同。

EAP-TLS

- 根据正在使用的操作系统，进行如下设置：
 - 在“验证服务器证书”中选择[开]或[关]。
 - 在“可信的中间证书颁发机构”中选择[开]或[关]。
 - 在“服务器 ID”中输入 RADIUS 服务器的主机名。
 - 在“允许子域”中选择[开]或[关]。

LEAP

- 在“密码”中单击[更改]，然后输入在 RADIUS 服务器中设置的密码。

EAP-TTLS

- 在“密码”中单击[更改]，然后输入在 RADIUS 服务器中设置的密码。
- 在“阶段 2 用户名称”中单击[更改]，然后输入在 RADIUS 服务器中设置的用户名。

- 在“阶段 2 方式”中选择[CHAP]、[MSCHAP]、[MSCHAPv2]、[PAP]或[MD5]。

根据要使用的 RADIUS 服务器不同，某些方式可能不可用。

- 根据正在使用的操作系统，进行如下设置：
 - 在“验证服务器证书”中选择[开]或[关]。
 - 在“可信的中间证书颁发机构”中选择[开]或[关]。
 - 在“服务器 ID”中输入 RADIUS 服务器的主机名。
 - 在“允许子域”中选择[开]或[关]。

PEAP

- 在“密码”中单击[更改]，然后输入在 RADIUS 服务器中设置的密码。
如果为“阶段 2 方式”选择了[TLS]，则无需指定密码。
- 在“阶段 2 用户名称”中单击[更改]，然后输入在 RADIUS 服务器中设定的用户名。
- 在“阶段 2 方式”中选择[MSCHAPv2]或[TLS]。
如果选择[TLS]，则必须安装“IEEE 802.1X 客户端证书”。
- 根据正在使用的操作系统，进行如下设置：
 - 在“验证服务器证书”中选择[开]或[关]。
 - 在“可信的中间证书颁发机构”中选择[开]或[关]。
 - 在“服务器 ID”中输入 RADIUS 服务器的主机名。
 - 在“允许子域”中选择[开]或[关]。

7. 单击[确定]。

8. 将出现“正在更新...” 。等待约 1 至 2 分钟，然后单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

9. 在“接口”下，单击[接口设置]。

10. 在“以太网安全”中选择[有效]。

11. 单击[确定]。

12. 将出现“正在更新...” 。等待约 1 至 2 分钟，然后单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

13. 注销。



注

- 如果设置中有问题，可能无法与机器通信。在这种情况下，请在控制面板上的[接口设置]中访问[打印列表]，然后打印该网络摘要以便检查状态。

- 如果无法确定问题，请在控制面板上[接口设置]的[网络]中执行[将 IEEE 802.1X 验证恢复到默认值]，然后重复该步骤。

SNMPv3 加密

使用 Device Manager NX 或其他通过 SNMPv3 进行通信的应用程序时，可以对传输的数据进行加密。

进行此项设置可防止数据被篡改。

1. 以网络管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[接口设置]。
4. 按[▼向后]。
5. 按[允许 SNMPv3 通信]。

6. 按[仅限加密]。
7. 按[确定]。
8. 注销。

注

- 要使用 Device Manager NX 对指定设置的数据进行加密，除了要在机器上指定[允许 SNMPv3 通信]外，还需要在 Device Manager NX 下的[SNMP 账户设置]中指定网络管理员的[加密密码]设置和[加密密码]。有关在 Device Manager NX 中指定[加密密码]的详细信息，请参见 Device Manager NX 的帮助。
- 如果未指定网络管理员的[加密密码]设置，则可能无法加密或发送要传送的数据。有关指定网络管理员的[加密密码]设置的详细信息，请参见 p.16 “注册和更改管理员”。

加密传送的密码

为 IPP 验证配置驱动程序加密密钥和密码加密，可以使通信带有加密密码，并提高密码的安全性，防止破解。要进一步提高安全性，建议您配合使用 IPsec、SNMPv3 和 SSL/TLS。此外，还可加密用于管理员验证和用户验证的登录密码。

驱动程序加密密钥

此密钥是一个字符串，用于加密启用用户验证时从每个驱动程序发送的登录密码或文件密码。

要加密登录密码，请在机器上和在用户计算机中安装的打印机驱动程序上指定驱动程序加密密钥。

IPP 验证的密码

若要在 Web Image Monitor 上加密 IPP 验证密码，将“验证”设为[DIGEST]，然后指定在机器上设置的 IPP 验证密码。

您可以使用 telnet 或 FTP 来管理 IPP 验证密码，尽管我们不建议这样做。

↓ 注

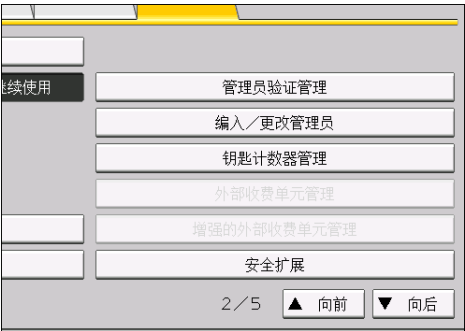
- 有关对用于管理员验证的登录密码进行加密的详细信息，请参见 p.16 “注册和更改管理员”。

指定驱动程序加密密钥

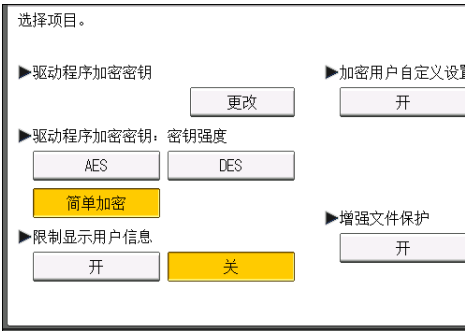
在机器上指定驱动程序加密密钥。

此设置可以启用对登录密码的加密传输，并提高安全性，防止密码被破解。

1. 以网络管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[▼向后]。
5. 按[安全扩展]。



6. 对于“驱动程序加密密钥”，按[更改]。



7. 输入驱动程序加密密钥，然后按[确定]。

输入的驱动程序加密密钥最多可由 32 个字母数字字符组成。

网络管理员必须将在机器上指定的驱动程序加密密钥提供给用户，以便他们能够在其计算机上注册密钥。请确保输入的驱动程序加密密钥与在机器上指定的密钥相同。

8. 按[确定]。

9. 注销。

注

- 有关在打印机驱动程序或 TWAIN 驱动程序上指定加密密钥的详细信息，请参见驱动程序帮助。

指定 IPP 验证密码

为本机指定 IPP 验证密码。此设置可以启用对 IPP 验证密码的加密传输，并提高安全性，防止密码被破解。

- 以网络管理员身份从 Web Image Monitor 登录。
- 指向[设备管理]，然后单击[配置]。
- 在“安全”下，单击[IPP 验证]。
- 从“验证”列表中选择[DIGEST]。
- 在“用户名称”框中输入用户名。
- 在“密码”框中输入密码。
- 单击[确定]。

IPP 验证即被指定。

8. 将出现“正在更新...”。等待约 1 至 2 分钟，然后单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

9. 注销。

Kerberos 验证加密设置

如果启用了 Kerberos 验证，则您可以指定机器和密钥分发中心(KDC)服务器之间的加密传输。

将 Kerberos 验证与 Windows 或 LDAP 验证、LDAP 搜索等搭配使用，可以确保进行安全的通信。

根据 KDC 服务器的类型，受支持的加密算法会有所不同。选择适合您环境的算法。

KDC 服务器	受支持的加密算法
Windows Server 2003 Active Directory	• RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008 R2/2012/2012 R2	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5*
Heimdal	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • DES3-CBC-SHA1 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5

* 要使用 Kerberos 验证，请在操作系统设置中启用它。

1. 以机器管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“设备设置”下，单击[Kerberos 验证]。

4. 选择您要启用的加密算法。

请务必选择一个或多个加密算法。

5. 单击[确定]。**6. 注销。**

6. 防止文件泄漏

本章介绍如何保护机器中保存的文件数据或使用机器打印的文件数据。

管理文件夹

本节介绍如何管理文件服务器中的文件夹、删除文件夹、更改其密码以及在锁定时取消锁定。

删除文件夹

文件管理员或用户可执行此操作。

要删除旁边带有🔒图标文件夹，需要该文件夹的密码。

如果用户忘记了访问文件夹的密码，文件管理员可更改该密码。

文件管理员无需使用密码即可删除文件夹。

无法删除包含用户没有删除权限的文件文件夹。

无法删除共享文件夹。

1. 以文件管理员或用户身份从控制面板中登录。

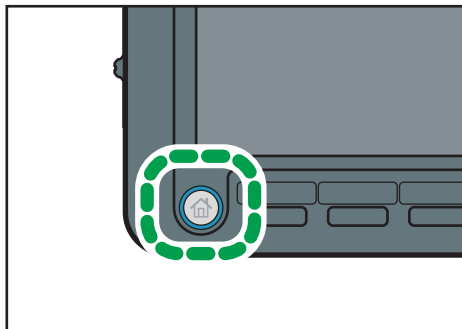
2. 按[用户工具]键，关闭用户工具菜单。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。

3. 按控制面板中的[主页]键，然后按屏幕中的[文件服务器]图标。

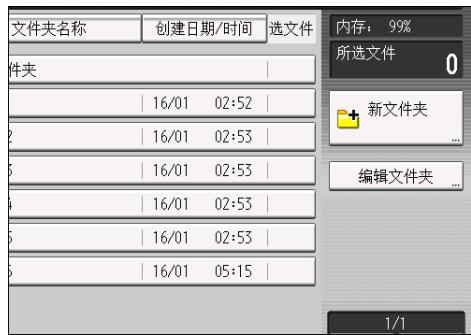
如果[文件服务器]图标未显示，请按屏幕右上角的🏠图标以切换至菜单屏幕。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。



CWW220

4. 按[编辑文件夹]。



5. 选择文件夹。

6. 按[删除]。

7. 如果出现密码输入屏幕，请输入文件夹的密码，然后按[确定]。

若文件管理员登录，则不会出现密码输入屏幕。

8. 按[删除]。

9. 注销。

↓ 注

- 此外也可以通过 Web Image Monitor 进行指定。有关详细信息，请参见 Web Image Monitor 的帮助。

更改文件夹的密码

可由文件管理员或用户指定。

如果用户忘记了访问文件夹的密码，文件管理员可更改该密码。

无法为共享文件夹指定密码。

1. 以文件管理员或用户身份从控制面板中登录。

2. 按[用户工具]键，关闭用户工具菜单。

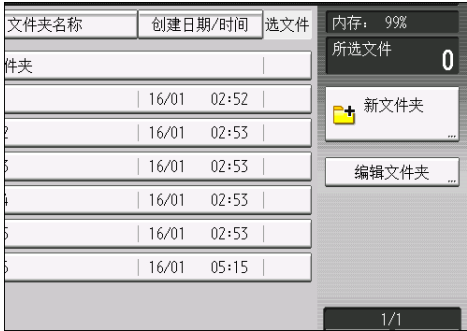
如果出现“您没有使用此功能的权限。”信息，请按[退出]。

3. 按控制面板中的[主页]键，然后按屏幕中的[文件服务器]图标。

如果[文件服务器]图标未显示，请按屏幕右上角的图标以切换至菜单屏幕。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。

4. 按[编辑文件夹]。



5. 选择文件夹。

6. 按[更改密码]。

7. 如果出现密码输入屏幕，请输入文件夹的密码，然后按[确定]。

若文件管理员登录，则不会出现密码输入屏幕。

8. 输入文件夹的新密码，然后按[确定]。

您可以使用 4 到 8 位数字作为文件夹的密码。

9. 再次输入密码进行确认，然后按[确定]。

受密码保护的文件夹旁边将出现🔒图标。

10. 注销。

↓ 注

- 此外也可以通过 Web Image Monitor 进行指定。有关详细信息，请参见 Web Image Monitor 的帮助。

解除文件夹锁定

只有文件管理员才可以解除文件夹的锁定。

如果将“增强文件保护”指定为[开]，则在输入 10 次无效密码后，文件夹将被锁定并且无法访问。本节说明如何解除文件夹的锁定。

“增强文件保护”是扩展安全功能之一。有关此功能和其他扩展安全功能的详细信息，请参见 p.225 “指定扩展安全功能”。

1. 以文件管理员身份从控制面板中登录。

2. 按[用户工具]键。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。

3. 按控制面板中的[主页]键，然后按屏幕中的[文件服务器]图标。

如果[文件服务器]图标未显示，请按屏幕右上角的🖥️图标以切换至菜单屏幕。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。

4. 按[编辑文件夹]。

5. 选择文件夹。

使用增强文件保护功能锁定的文件夹旁边将出现图标。

6. 按[解除锁定]。

图标更改为图标。

7. 按[解除锁定]。

8. 注销。

 注

- 此外也可以通过 Web Image Monitor 进行指定。有关详细信息，请参见 Web Image Monitor 的帮助。

管理保存的文件

本节介绍如何指定保存文件的访问权限。

您可以指定允许哪些用户访问所保存的扫描文件及保存在文件服务器中的文档。

这可以防止未经授权的用户进行打印或发送所保存文件之类的活动。

还可以指定哪些用户可以更改或删除保存的文件。

要限制对所保存文件的使用，您可以指定 4 种访问权限。

访问权限类型

访问权限	描述
只读	您可以查看所保存文件的内容和关于这些文件的信息，以及打印和发送文件。
编辑	您可以更改所保存文件的打印设置。 其中包括查看文件的权限。
编辑／删除	您可以删除保存的文件。 其中包括查看和编辑文件的权限。
完全控制	您可以指定用户和访问权限。 其中包括查看、编辑和编辑/删除文件的权限。

6

保存文件的密码

- 文件管理员或所有者可以指定保存文件的密码。这样可以更有效防止文件被未经授权的使用。有关为保存文件分配密码的详细信息，请参见 p.159 “为保存的文件指定密码”。
- 即使未设置用户验证，也可以为保存的文件设置密码。

↓ 注

- 任何被允许使用文件服务器、复印功能、扫描仪功能或打印机功能的用户均可保存文件。
- 您可以使用 Web Image Monitor 检查所保存文件的内容。有关详细信息，请参见 Web Image Monitor 帮助。
- 所有者的默认访问权限为“只读”。您也可以指定访问权限。
- 文件管理员不仅可以配置访问权限，而且还可以删除保存的文件。有关删除文件的方法的详细信息，请参见《复印/文件服务器》中的“删除保存的文件”。

配置各个保存文件的访问权限

可由文件管理员或所有者指定。

为每个保存的文件指定用户及其访问权限。

★重要信息

- 如果文件无法访问，则所有者可重设其访问权限。文件管理员可以重置访问权限。如果想访问某文件但不具备访问权限，请咨询所有者。
- 文件管理员可以使用文件的[更改访问权限]设置更改文件的所有者。通过此设置，文件管理员还可以更改所有者和其他用户的访问权限。
- 对文件拥有[完全控制]权限的文件所有者和用户可以在[更改访问权限]设置下，更改所有者和其他用户的访问权限。

1. 以文件管理员或所有者身份从控制面板中登录。

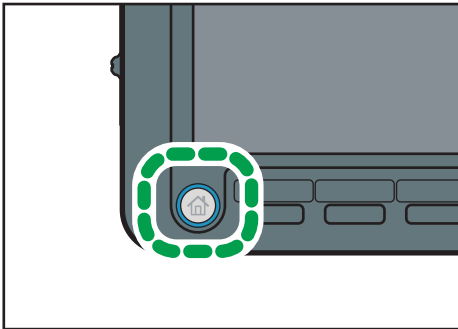
2. 按[用户工具]键，关闭用户工具菜单。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。

3. 按控制面板中的[主页]键，然后按屏幕中的[文件服务器]图标。

如果[文件服务器]图标未显示，请按屏幕右上角的图标以切换至菜单屏幕。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。



CWW220

4. 选择文件夹。

编号	文件夹名称	创建日期/时间	选文件
	共享文件夹		
001	User001	16/01 02:52	
002	User002	16/01 02:53	
003	User003	16/01 02:53	
004	User004	16/01 02:53	
005	User005	16/01 02:53	
006	User006	16/01 05:15	

5. 选择文件。



6. 按[编辑文件]。



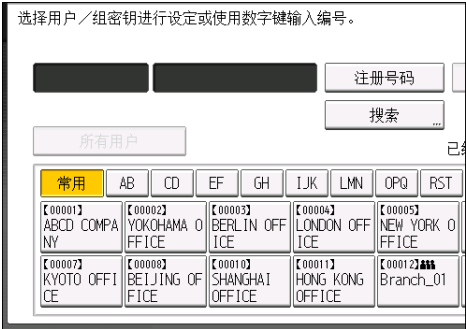
7. 按[更改访问权限]。

8. 按[编入／更改／删除]。



9. 按[新编入]。

10. 选择要分配访问权限的用户或群组。

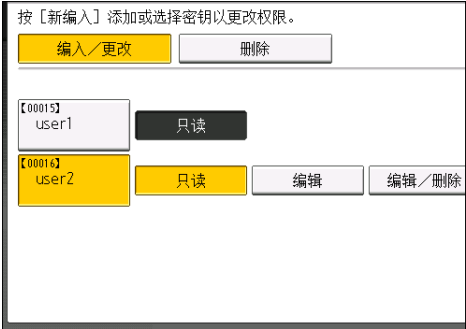


您可以选择多个用户。

您可以按[所有用户]选择所有用户。

11. 按[退出]。

12. 选择要分配访问权限的用户，然后选择权限。



从[只读]、[编辑]、[编辑/删除]或[完全控制]中选择访问权限。

13. 按[退出]。

14. 按[确定]。

15. 注销。

↓ 注

- 此外也可以通过 Web Image Monitor 进行指定。有关详细信息，请参见 Web Image Monitor 帮助。
- “编辑”、“编辑/删除”和“完全控制”访问权限允许用户执行高级操作，有可能导致敏感信息丢失或发生变化。建议您仅向一般用户分配“只读”权限。

更改文件的所有者

使用此步骤可以更改文件的所有者。

只有文件管理员才能更改文件的所有者。

1. 以文件管理员身份从控制面板中登录。

2. 按[用户工具]键，关闭用户工具菜单。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。

3. 按控制面板中的[主页]键，然后按屏幕中的[文件服务器]图标。

如果[文件服务器]图标未显示，请按屏幕右上角的图标以切换至菜单屏幕。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。

4. 选择文件夹。

5. 选择文件。

6. 按[编辑文件]。

7. 按[更改访问权限]。

8. 对“所有者”按[更改]。

9. 选择您想要注册的用户。

10. 按[退出]。

11. 按[确定]。

12. 注销。

配置各个用户对保存文件的访问权限

可由用户管理员或所有者指定。

为特定用户保存的文件指定用户及其访问权限。

与为每个保存的文件指定和管理访问权限相比，这简化了访问权限的管理。

★重要信息

- 如果文件变得无法访问，请务必让用户管理员重置文件的访问权限。

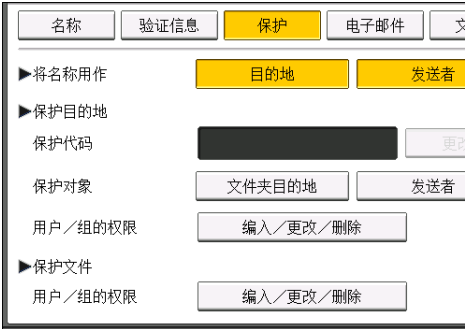
1. 用户管理员或所有者从控制面板登录。

2. 按[通讯簿管理]。

3. 选择用户。

4. 按[保护]。

5. 在“保护文件”下，按“用户／组的权限”所对应的[编入／更改／删除]。



6. 按[新编入]。

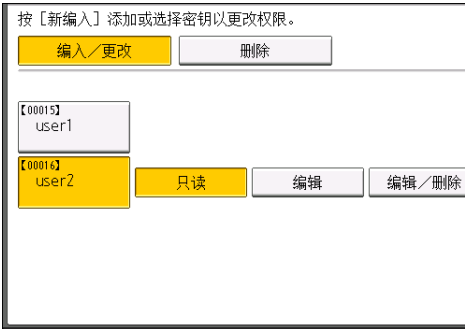
7. 选择要注册的用户或组。

您可以选择多个用户。

您可以按[所有用户]选择所有用户。

8. 按[退出]。

9. 选择要分配访问权限的用户，然后选择权限。



从[只读]、[编辑]、[编辑／删除]或[完全控制]中选择访问权限。

10. 按[退出]。

11. 按[确定]。

12. 按[退出]。

13. 注销。

↓ 注

- “编辑”、“编辑／删除”和“完全控制”访问权限允许用户执行高级操作，有可能导致敏感信息丢失或发生变化。建议您仅向一般用户分配“只读”权限。

为保存的文件指定密码

可由文件管理员或所有者指定。

1. 文件管理员或所有者从控制面板登录。

2. 按[用户工具]键，关闭用户工具菜单。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。

3. 按控制面板中的[主页]键，然后按屏幕中的[文件服务器]图标。

如果[文件服务器]图标未显示，请按屏幕右上角的图标以切换至菜单屏幕。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。

4. 选择文件夹。



编号	文件夹名称	创建日期/时间	选文件
	共享文件夹		
001	User001	16/01 02:52	
002	User002	16/01 02:53	
003	User003	16/01 02:53	
004	User004	16/01 02:53	
005	User005	16/01 02:53	
006	User006	16/01 05:15	

5. 选择文件。



类型	用户名	文件名	日期	页	印序
	user1	COPY0005	16/01	5	
	user1	COPY0004	16/01	5	
	user1	COPY0003	16/01	5	
	user1	COPY0002	16/01	5	
	user1	COPY0001	16/01	5	

6. 按[编辑文件]。



7. 按[更改密码]。

8. 输入所保存文件的新密码，然后按[确定]。

您可以使用 4 到 8 位数字作为所保存文件的密码。

9. 再次输入密码进行确认，然后按[确定]。

受密码保护的保存文件旁边将出现🔒图标。

10. 按[确定]。

11. 注销。

解除对保存文件的锁定

只有文件管理员才可以解除文件的锁定。

如果指定“增强文件保护”，则在输入 10 次无效密码后，文件将被锁定并变得无法访问。本节说明如何解除文件的锁定。

“增强文件保护”是扩展安全功能之一。有关此功能和其他扩展安全功能的详细信息，请参见 p.225 “指定扩展安全功能”。

1. 以文件管理员身份从控制面板中登录。

2. 按[用户工具]键，关闭用户工具菜单。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。

3. 按控制面板中的[主页]键，然后按屏幕中的[文件服务器]图标。

如果[文件服务器]图标未显示，请按屏幕右上角的🖥️图标以切换至菜单屏幕。

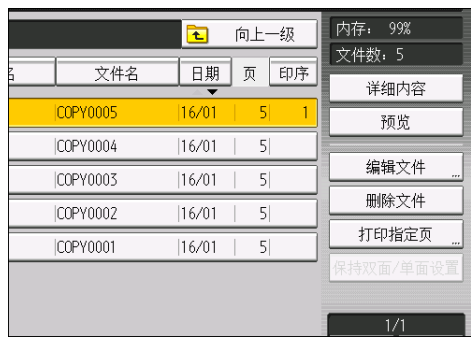
如果出现“您没有使用此功能的权限。”信息，请按[退出]。

4. 选择文件夹。

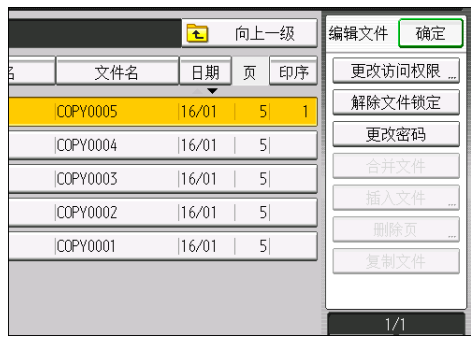
5. 选择文件。

由增强文件保护功能锁定的文件旁边将出现🔒图标。

6. 按[编辑文件]。



7. 按[解除文件锁定]。



8. 按[是]。

图标更改为图标。

9. 按[确定]。

10. 注销。

管理锁定打印文件

由于打印机所在的位置，有时可能很难避免未经许可的人员查看打印机出纸盘中的打印件。打印机密文件时，请使用“锁定打印”功能。

锁定打印

- 使用打印机的锁定打印功能，可以在机器中将文件保存为锁定打印文件。然后，从控制面板打印文件，并立即取回，以便其他人无法查看。

注

- 无论用户验证设置为何，都可以打印机密文件。
- 要临时保存文件，请在打印机驱动程序中选择[保存的打印]。如果选择[保存的打印（共享）]，便可以共享这些文件。
- 有关如何使用锁定打印功能的详细信息，请参见《打印》中的“锁定打印”。

删除锁定打印文件

可由文件管理员或所有者指定。

如果所有者要删除锁定的打印文件，需要访问文件的密码。如果所有者忘记了密码，可以请文件管理员更改密码。

文件管理员删除锁定的打印文件时，无需使用密码。

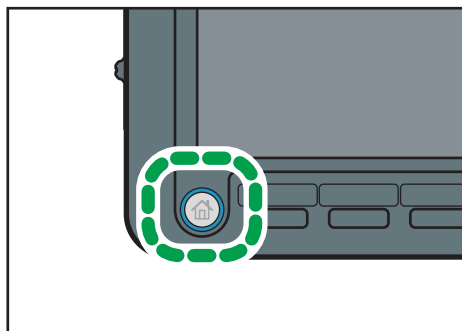
1. 以文件管理员或所有者身份从控制面板中登录。

2. 按[用户工具]键，关闭用户工具菜单。

如果出现“您没有使用此功能的权限。”信息，请按[退出]。

3. 按控制面板中的[主页]键，然后按屏幕中的[打印机]图标。

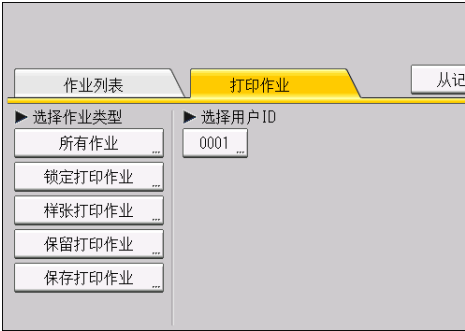
如果[打印机]图标未显示，请按屏幕右上角的图标以切换至菜单屏幕。



CWW220

4. 按[打印作业]。

5. 按[锁定打印作业]。



6. 选择文件。



7. 按[删除]。



8. 如果出现密码输入屏幕，请输入锁定打印文件的密码，然后按[确定]。

若文件管理员登录，则不会出现密码输入屏幕。

9. 按[是]。

10. 注销。

↓ 注

- 通过将“自动删除临时打印作业”选项设置为[开]，可以将本机配置为自动删除保存的文件。有关“自动删除临时打印作业”的详细信息，请参见《打印》中的“数据管理”。

- 此外也可以通过 Web Image Monitor 进行指定。有关详细信息，请参见 Web Image Monitor 帮助。

更改锁定打印文件的密码

可由文件管理员或所有者指定。

如果所有者忘记了密码，可以请文件管理员更改密码。

1. 以文件管理员或所有者身份从控制面板中登录。

2. 按[用户工具]键，关闭用户工具菜单。

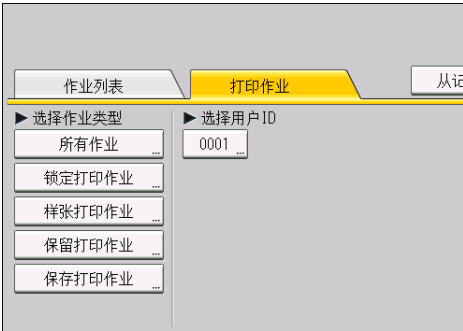
如果出现“您没有使用此功能的权限。”信息，请按[退出]。

3. 按控制面板中的[主页]键，然后按屏幕中的[打印机]图标。

如果[打印机]图标未显示，请按屏幕右上角的图标以切换至菜单屏幕。

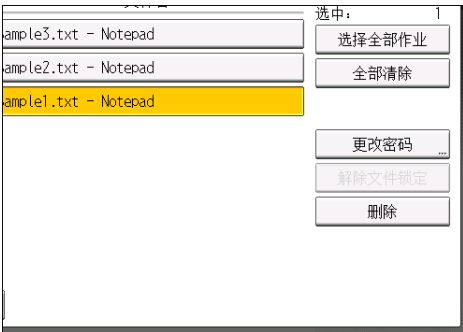
4. 按[打印作业]。

5. 按[锁定打印作业]。



6. 选择文件。

7. 按[更改密码]。



8. 如果出现密码输入屏幕，请输入保存文件的密码，然后按[确定]。

若文件管理员登录，则不会出现密码输入屏幕。

- 9. 输入所保存文件的新密码，然后按[确定]。
- 10. 再次输入密码进行确认，然后按[确定]。
- 11. 注销。

注

- 此外也可以通过 Web Image Monitor 进行指定。有关详细信息，请参见 Web Image Monitor 帮助。

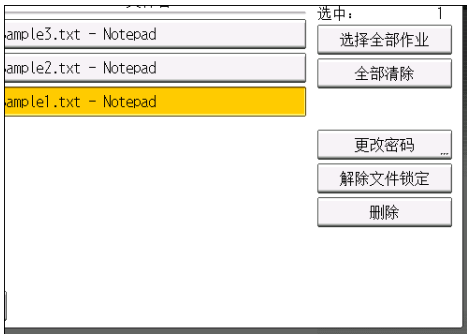
解除锁定打印文件的锁定

只有文件管理员才可以解除文件的锁定。

如果将“增强文件保护”指定为[开]，则在输入 10 次无效密码后，文件将被锁定并变得无法访问。本节说明如何解除文件的锁定。

“增强文件保护”是扩展安全功能之一。有关此功能和其他扩展安全功能的详细信息，请参见 p.225 “指定扩展安全功能”。

- 1. 以文件管理员身份从控制面板中登录。
- 2. 按[用户工具]键，关闭用户工具菜单。
如果出现“您没有使用此功能的权限。”信息，请按[退出]。
- 3. 按控制面板中的[主页]键，然后按屏幕中的[打印机]图标。
如果[打印机]图标未显示，请按屏幕右上角的图标以切换至菜单屏幕。
- 4. 按[打印作业]。
- 5. 按[锁定打印作业]。
- 6. 选择文件。
由增强文件保护功能锁定的文件旁边将出现图标。
- 7. 按[解除文件锁定]。



- 8. 按[是]。
图标将消失。

9. 注销。



- 此外也可以通过 Web Image Monitor 进行指定。有关详细信息，请参见 Web Image Monitor 帮助。

防止未经授权复印/复印数据安全性

打印机功能允许您在打印的副本中嵌入图案以阻止或防止未经授权的复印。

如果启用了防止未经授权复印功能，在非法复印文件时将显示嵌入的文字图案（例如，诸如“禁止复印”等的警告信息）。因此，可防止未经授权进行复印。

如果使用复印数据安全性功能并启用了文件中嵌入特殊图案的设置，带有嵌入图案的文件副本将以灰色套印形式打印。由此，可防止信息泄露。要通过灰色套印保护文件，必须使用安装有 Copy Data Security Unit 的复印机或多功能打印机。

有关详细信息，请参见以下信息：

使用防止未经授权复印

1. 启用嵌入式图案打印。机器管理员可配置此设置。有关如何配置该设置的详细信息，请参见 p.167 “启用图案打印”。
2. 在打印机功能中指定用于防止未经授权的复印的设置。指定设置的权限取决于[强制防止未经授权复印]中指定的设置。有关详细信息，请参见 p.167 “启用图案打印”。

使用复印数据安全性

1. 启用嵌入式图案打印设置。机器管理员可配置此设置。有关如何配置该设置的详细信息，请参见 p.167 “启用图案打印”。
2. 在打印机功能中指定复印数据安全的设置。指定设置的权限取决于[强制防止未经授权复印]中指定的设置。有关详细信息，请参见 p.167 “启用图案打印”。

启用图案打印

您可以启用嵌入的图案打印来阻止或防止未经授权的复印。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按 3 次[▼向后]。
5. 按[防止未经授权复印的打印：打印]。
6. 按“防止未经授权复印设置”的[更改]。
7. 按[开]，然后按[确定]。
8. 按“强制防止未经授权复印”的[更改]。
9. 指定是否强制打印嵌入式图案。

- [驱动/命令]

打印嵌入式图案不是强制性的。

通过打印机驱动程序，用户可选择是否打印嵌入式图案并且可指定其设置。

- [驱动／命令(多数设置)]

打印嵌入式图案是强制性的。

通过打印机驱动程序，用户可指定类型、颜色和厚度之外的嵌入式图案设置。

- [机器设置]

打印嵌入式图案是强制性的。

用户无法使用打印机驱动程序指定嵌入图案的设置。

10. 按两次[确定]。

11. 注销。

↓ 注

- 有关使用机器指定图案设置的详细信息，请参见《连接机器/系统设置》中的“管理工具”。

在纸张上打印用户信息

打印作业的开始时间、作业打印人员的有关信息（名称或登录用户名）、机器编号和机器的 IP 地址都可以强制嵌入在打印页上。此功能称为强制安全印记。

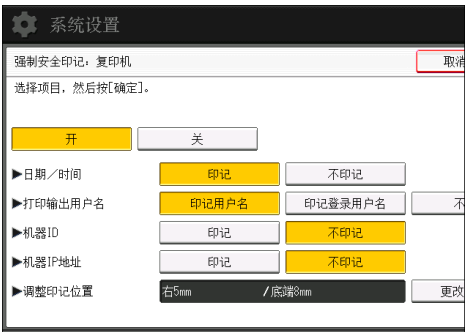
始终打印输出作业打印人员的有关信息可阻止信息泄漏。它也可用于确定信息泄漏源。

强制安全印记可与复印、文件服务器和打印一起使用。

- 1. 以机器管理员身份从控制面板中登录。
- 2. 按[系统设置]。
- 3. 按[管理员工具]。
- 4. 按 3 次[▼向后]。
- 5. 为强制安全印记选择功能。
 - 要设置需要印记的复印功能，请按[强制安全印记：复印机]。
 - 要设置需要印记的文件服务器，请按[强制安全印记：文件服务器]。
 - 要设置需要印记的打印机功能，请按[强制安全印记：打印机]。

6. 按[开]，然后选择要印记的数据。

要关闭强制安全印记，请按[关]。



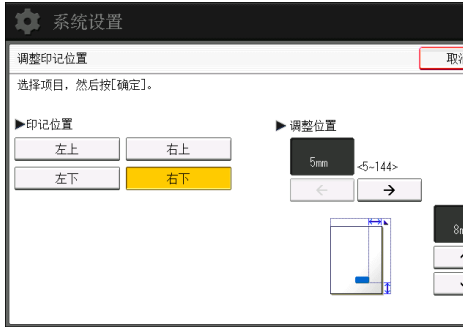
- 日期／时间
系统将会打印作业开始时间。
- 打印输出用户名
如果启用了用户验证，将会打印这些用户名。
 - 印记用户名
将打印通讯簿中“名称”中的“名称”。
 - 印记登录用户名
将会打印通讯簿中“验证信息”中的用户代码或登录用户名。
- 机器 ID
系统将打印[查询]中显示为“机器的序列号”的编号。

- 机器 IP 地址

系统将会打印本机的 IP 地址。如果同时存在 IPv4 和 IPv6 地址，则系统将会打印 IPv4 地址。如果尚未配置任何 IP 地址，则系统会将此留空。

7. 为“调整印记位置”按[更改]。

8. 设置印记位置。



9. 按两次[确定]。

10. 注销。

在打印机上强制保存要打印的文件

通过在打印作业前强制将其保存在机器中，可防止由于用户未能收集打印件或打印件无人看管而导致信息泄露。下列打印作业可强制保存。

- 普通打印
- 样张打印
- 保存并打印

1. 以机器管理员身份从控制面板中登录。

2. 按[打印机特性]。

3. 按[系统]。

4. 按[▼向后]。

5. 按[限制直接打印作业]。

6. 按[自动保存作业]。

7. 按[确定]。

8. 注销。

- 如果选择[取消全部直接打印作业]，则打印作业将被取消而不进行保存。
- 有关如何打印保存文件的信息，请参见《打印》中的“打印保存的文件”。

7. 管理机器

本章介绍用于提高机器安全性以及有效操作机器的功能。

管理日志文件

通过收集本机中保存的日志，您可以跟踪有关以下情况的详细数据：对机器的访问、用户身份、对机器各种功能的使用以及错误历史记录。

可定期删除日志以释放硬盘空间。

您可以使用 Web Image Monitor 或日志收集服务器查看日志。您可以将收集的日志转换为 CSV 文件，也可以同时下载收集的所有日志。您无法从硬盘直接阅读日志。

日志类型

本机会保存 3 种类型的日志：作业日志、访问日志和环保日志。

- 作业日志

存储用户的文件相关操作（如复印、打印和保存在文件服务器中）和控制面板操作（如发送扫描文件和打印配置列表等报告）的详细信息。

- 访问日志

存储以下方面的详细信息：登录/注销活动、保存文件的操作（如创建、编辑和删除）、客户工程师操作（如硬盘格式化）、系统操作（如查看日志传送结果）以及安全操作（如指定加密、无权访问检测、用户锁定和固件验证的设置）。

- 环保日志

存储以下方面的详细信息：主电源打开、关闭、电源状态转变、作业运行时间或作业之间的时间间隔、每个小时的耗纸量、耗电量。

注

- 有关日志收集服务器的详细信息，请参见日志收集服务器的用户手册。
- 使用日志收集服务器时，您必须在日志收集服务器上配置日志传输设置。

使用 Web Image Monitor 管理日志文件

您可以指定保存在机器上的日志类型和日志收集等级。也可批量删除或下载日志文件。

可以使用 Web Image Monitor 进行管理的日志

下表介绍使用 Web Image Monitor 启用日志收集时机器创建的作业日志和访问日志中的项目。如果需要日志收集，则使用 Web Image Monitor 对其进行配置。此设置可以在 Web Image Monitor 的[配置]下的[日志]中指定。

作业日志信息项目

作业日志项目	日志类型属性	内容
复印机：复印	Copier: Copying	普通和样张复印作业的详细信息。
复印机：复印并保存	Copier: Copying and Storing	文件服务器中所保存文件（保存时也将复印的文件）的详细信息。
文件服务器：保存	Document Server: Storing	使用文件服务器屏幕保存的文件的详细信息。
文件服务器：下载保存的文件	Document Server: Stored File Downloading	文件服务器中保存的文件和使用 Web Image Monitor 下载的文件的信息。
应用程序：保存	Utility: Storing	使用应用程序保存的文件的详细信息。
保存的文件打印	Stored File Printing	使用文件服务器打印文件屏幕的信息。
扫描仪：发送	Scanner: Sending	所发送扫描文件的详细信息。
扫描仪：发送并保存 URL 链接	Scanner: URL Link Sending and Storing	文件服务器中保存所扫描文件的详细信息。保存时通过电子邮件发送 URL。
扫描仪：发送并保存	Scanner: Sending and Storing	文件服务器中保存所扫描文件（保存时也将发送的文件）的详细信息。
扫描仪：保存	Scanner: Storing	文件服务器中保存所扫描文件的详细信息。

作业日志项目	日志类型属性	内容
扫描仪：下载保存的文件	Scanner: Stored File Downloading	文件服务器中保存的扫描文件和使用 Web Image Monitor 或 Desk Top Editor For Production 下载的扫描文件的详细信息。
扫描仪：发送保存的文件	Scanner: Stored File Sending	保存所扫描文件（也将发送）的详细信息。
扫描仪：发送保存文件的 URL 链接	Scanner: Stored File URL Link Sending	保存所扫描文件（通过电子邮件发送其 URL）的详细信息。
打印机：打印	Printer: Printing	普通打印作业的详细信息。
打印机：锁定打印（未完成）	Printer: Locked Print (Incomplete)	显示临时保存在机器上的锁定打印文件的日志。
打印机：锁定打印	Printer: Locked Print	显示临时保存在机器上并通过控制面板或 Web Image Monitor 打印的锁定打印文件的日志。
打印机：样张打印（未完成）	Printer: Sample Print (Incomplete)	显示临时保存在机器上的样张打印文件的日志。
打印机：样张打印	Printer: Sample Print	显示临时保存在机器上并通过控制面板或 Web Image Monitor 打印的样张打印文件的日志。
打印机：保留打印（未完成）	Printer: Hold Print (Incomplete)	显示临时保存在机器上的保留打印文件的日志。
打印机：保留打印	Printer: Hold Print	显示临时保存在机器上并通过控制面板或 Web Image Monitor 打印的保留打印文件的日志。
打印机：保存的打印	Printer: Stored Print	保存在机器中的保存的打印文件的详细信息。
打印机：保存并普通打印	Printer: Store and Normal Print	保存时打印（在打印机属性中，“作业方式：” 设置为“保存并打印”时）的保存的打印文件的详细信息。
打印机：打印保存的文件	Printer: Stored File Printing	从控制面板或 Web Image Monitor 打印的保存的打印文件的详细信息。

作业日志项目	日志类型属性	内容
打印机：发送至文件服务器	Printer: Document Server Sending	在打印机属性中“作业方式：”设置为“文件服务器”时文件服务器中所保存文件的详细信息。
报告打印	Report Printing	从控制面板打印的报告的详细信息。
打印/发送电子邮件结果报告	Result Report Printing/Emailing	从控制面板打印或通过电子邮件通知的作业结果的详细信息。
扫描仪：TWAIN 驱动程序扫描	Scanner: TWAIN Driver Scanning	保存所扫描文件（使用网络 TWAIN 扫描仪发送）的详细信息。
打印机：保留打印文件打印	Printer: Hold Print File Printing	当文件被保留打印并临时保存在机器上时，此项会记录用户通过控制面板或 Web Image Monitor 指定打印该文件的时间。

访问日志信息项目

访问日志项目	日志类型属性	内容
登录	Login	登录次数和登录用户的身份。
注销	Logout	注销次数和注销用户的身份。
文件保存	File Storing	文件服务器中所保存文件的详细信息。
删除保存的文件	Stored File Deletion	从文件服务器删除的文件的详细信息。
删除所有保存的文件	All Stored Files Deletion	删除所有文件服务器文件的详细信息。
硬盘格式化	HDD Format	硬盘格式化的详细信息。
删除所有日志	All Logs Deletion	删除所有日志的详细信息。
更改日志设置	Log Setting Change	更改日志设置的详细信息。
转送日志结果	Transfer Log Result	系统向 Remote Communication Gate S 传送日志的结果日志。
更改日志收集项目	Log Collection Item Change	更改作业日志收集等级、访问日志收集等级和所收集日志类型的详细信息。

访问日志项目	日志类型属性	内容
收集加密通信日志	Collect Encrypted Communication Logs	在 Web Image Monitor 实用程序或外部设备之间进行加密传送的日志。
访问冲突	Access Violation	失败的访问尝试的详细信息。
锁定	Lockout	激活锁定的详细信息。
固件：更新	Firmware: Update	固件更新的详细信息。
固件：更改结构	Firmware: Structure Change	插入或删除 SD 卡或插入不受支持的 SD 卡时出现的结构更改的详细信息。
固件：结构	Firmware: Structure	检查固件模块结构是否更改（如开启机器时等）的详细信息。
更改机器数据加密密钥	Machine Data Encryption Key Change	使用“更改机器数据加密密钥”设置对加密密钥所做更改的详细信息。
固件：无效	Firmware: Invalid	检查固件有效性（如开启机器时等）的详细信息。
更改日期/时间	Date/Time Change	更改日期和时间设置的详细信息。
更改文件访问权限	File Access Privilege Change	更改所保存文件的访问权限的日志。
更改密码	Password Change	更改登录密码的详细信息。
更改管理员	Administrator Change	更改管理员的详细信息。
更改地址簿	Address Book Change	更改地址簿条目的详细信息。
机器配置	Machine Configuration	对机器设置所做更改的日志。
备份地址簿	Back Up Address Book	备份地址簿中数据时的日志。
恢复地址簿	Restore Address Book	恢复地址簿中数据时的日志。

访问日志项目	日志类型属性	内容
增强打印容量使用限制：跟踪许可结果	Enhanced Print Volume Use Limitation: Tracking Permission Result	出现跟踪错误时的日志。
计数器清除结果：选择的用户	Counter Clear Result: Selected User(s)	清除单个用户计数器时的日志。
计数器清除结果：所有用户	Counter Clear Result: All Users	清除所有用户计数器时的日志。
导入设备设置信息	Import Device Setting Information	导入设备设置信息文件时的日志。
导出设备设置信息	Export Device Setting Information	导出设备设置信息文件时的日志。
创建/删除文件夹	Creating/Deleting Folders	创建和删除文件夹时的记录。
保存的文件编辑	Stored File Editing	用于编辑文件的日志。
插入另一文件	Insertion into another File	用于将文件插入另一文件的日志。

对于 SNMPv3，没有“登录”日志。

如果对硬盘进行了格式化，则格式化操作之前的所有日志条目都会被删除，并且系统会记录一个指示格式化操作已完成的日志条目。

“访问冲突”指示系统曾受到频繁的远程 DoS 攻击，包括尝试通过用户验证进行登录。

打开电源后创建的第一条日志为“固件：结构”日志。

环保日志信息项目

环保日志项目	日志类型属性	内容
主电源开启	Main Power On	打开主电源开关时的日志。

环保日志项目	日志类型属性	内容
主电源关闭	Main Power Off	关闭主电源开关时的日志。
电源状态传送结果	Power Status Transition Result	电源状态转变结果日志。
作业相关信息	Job Related Information	作业相关信息日志。
纸张使用	Paper Usage	纸张用量日志。
功耗	Power Consumption	功耗日志。

可下载日志的属性

如果使用 Web Image Monitor 下载日志，将生成包含下表所示信息项目的 CSV 文件。
请注意，空白字段表示日志中未出现的项目。

文件输出格式

- 字符代码集：UTF-8
- 输出格式：CSV（逗号分隔值）
- 作业日志和访问日志的文件名：“机器名称+_log.csv”
- 环保日志的文件名：“机器名称+_ecolog.csv”

日志条目的顺序

日志条目是按日志 ID 的升序顺序打印的。

文件结构

数据标题打印在文件的第一行（标题行）。

日志数据格式差异

- 作业日志

按通用项目（作业日志和访问日志）、来源（作业输入数据）和目标（作业输出数据）的顺序显示多行。系统会为对应于单个作业日志条目的所有行分配同一个日志 ID。

	Start Date/Time	...	Result	...	Access Result	Source	...	Print File Name	Target	...	Stored File Name
1—	20XX-12-03T15:43:03.0	...	Completed	...			...			...	
2—		...	Completed	...		Report	...			...	
3—		...	Completed	...			...		Print	...	

CJ0022

1. 通用项目

通用项目中的每个项目均显示在单独的行上。

2. 源

通用项目和作业日志输入条目中将会出现“Result”和“Status”。
如果有多个源，则系统会显示多个行。

3. 目标

通用项目和作业日志输出条目中将会出现“Result”和“Status”。
如果有多个目标，则系统会显示多个行。

- 访问日志
通用项目和访问日志条目显示在不同的行上。
- 环保日志
环保日志条目显示在不同的行上。

通用项目（作业日志和访问日志）

Start Date/Time

指示操作或事件的开始日期和时间。

End Date/Time

指示操作或事件的结束日期和时间。

Log Type

日志类型的详细信息。
有关各种类型的日志中包含的信息项目的详细信息，请参见 p.174 “可以使用 Web Image Monitor 进行管理的日志”。

Result

指示操作或事件的结果。
仅当成功执行登录的操作时，才会记录以下日志项目：
“Document Server: Stored File Downloading”、“Stored File Printing”、“Scanner: Storing”、“Scanner: Stored File Sending”、“Printer: Stored File Printing”（作业日志）和“File Storing”和“Stored File Deletion”（访问日志）。

值	内容
Succeeded	已成功完成操作或事件。
Failed	操作或事件失败。
<空白>	正在执行操作或事件。

Operation Method

指示操作过程。

值	内容
Control Panel	控制面板
Driver	驱动程序
Utility	实用程序
Web	Web
Email	电子邮件

Status

指示操作或事件的状态。

值	内容
Completed	已成功完成关于作业日志条目的操作或事件。
Failed	关于作业日志条目的操作或事件失败。
Succeeded	已成功完成关于访问日志条目的操作或事件。
Password Mismatch	由于密码不匹配，出现访问错误。
User Not Programmed	由于用户未注册，发生访问错误。
Other Failures	由于未指定的故障，发生访问错误。
User Locked Out	由于用户被锁定，发生访问错误。
Communication Failure	由于通信故障，发生访问错误。
Communication Result Unknown	由于未知的通信结果，发生访问错误。
Failure in some or all parts	清除用户特定的计数器或所有用户计数器失败。
Importing/Exporting by Other User	正在由其他用户执行导入或导出。
Connection Failed with Remote Machine	连接到输出目的地失败。

值	内容
Write Error to Remote Machine	写入输出目的地时发生错误。
Specified File: Incompatible	指定的文件不兼容。
Specified File: Format Error	指定的文件发生格式错误。
Specified File: Not Exist	找不到指定的文件。
Specified File: No Privileges	访问指定文件的权限缺失。
Specified File: Access Error	访问指定的文件时发生错误。
Memory Storage Device Full	外部介质已满。
Memory Storage Device Error	外部介质出现异常。
Encryption Failed	加密失败。
Decoding Failed	解码失败。
Common Key Not Exist	公用密钥缺失。
Connection Error	出现通信错误。
Specified Server Error	由于服务器未正确配置而发生访问错误。
Specified Client Error	由于客户端未正确配置而发生访问错误。
Authentication Settings Mismatch	通讯簿规格不匹配。
Authentication Method Mismatch	验证方法不匹配。
Maximum Limit of Registered Number	可以注册的最大机器数。
Invalid Password	输入的密码无效。
Processing	正在处理作业。

值	内容
Error	已发生错误。
Suspended	作业已暂停。

Cancelled: Details

指示操作或事件失败的状态。

值	内容
Cancelled by User	用户已取消操作。
Input Failure	输入异常终止。
Output Failure	输出异常终止。
Other Error	执行作业前检测到错误或发生其他错误。
Power Failure	断电。
External Charge Unit Disconnected	在操作过程中拔出了所述设备。
Insufficient No. of Original for Overlay	执行叠放复印时遗失手稿的部分页面。
Exceed Max. Stored Page (File Storage)	超过文件服务器上的页数保存容量。
Exceed Max. Stored File (File Storage)	超过文件服务器上的文件保存容量。
Hard Disk Full (File Storage Memory)	超过文件服务器上的硬盘容量。
Exceeded Max. Email Size	超过电子邮件的大小限制。
Exceeded Max. File Size	超过单个文件的大小限制。
Scanner Error	自动文件送稿时发生读取错误。
Timeout	发生超时。
Specified Folder to Store does not Exist	找不到要保存文件的指定文件夹。

值	内容
Password for Folder Specified to Store is Incorrect	要保存文件的指定文件夹的密码不正确。
Folder is Locked	已锁定文件夹。
Memory Full	用于处理数据的内存范围已满。
Print Data Error	已尝试使用机器上未安装的 PDL 或端口。
Data Transfer Interrupted	要记录的情况如下所示： - 与正在使用的驱动程序不匹配。 - 发生网络故障。
Over Job Limit	超过可接收的作业数限制。
Specifying Destination Error	指定的地址无效或包含的位数超过 41 位。
Authentication Failed (Access Restricted)	设备验证失败。
Exceeded Print Volume Use Limitation	超过登录用户的页数使用限制。
No Privilege	该用户没有访问文件或功能的权限。
Unavailable Size to Store	无法保存指定的纸张尺寸（包括自定义尺寸）。
Transmission Failed (Data Deleted)	文件被删除或未送达的文件超过其等待时间并被删除。
Not Entered Document Password	未输入文件的密码。
Connection Failed with Destination	找不到指定的服务器或文件夹。
Authentication Failed with Destination	通过目的地进行验证失败。
Transmission Failed with Memory Full	目的地内存已满。

值	内容
Invalid Device Certificate	要记录的情况如下所示： - 设备证书缺失。 - 有效期已过。 - 如果管理员的电子邮件地址和证书的电子邮件地址不匹配。
Invalid Expiration Date: Destination's Certificate	目的地证书的有效期已过。
Invalid Device/ Destination's Certificate	目的地证书和设备证书均无效。
Fold Function Error	发生折叠功能错误。
Print Cancelled (Error)	由于系统错误，已取消打印作业。

User Entry ID

指示用户的条目 ID。

这是一个十六进制 ID，它标识执行与作业或访问日志相关的操作的用户。

值	内容
0x00000000	系统操作，由未经验证的用户执行的操作
0x00000001-0xfffffeff	用于一般用户和用户代码
0xffffffff80	系统操作
0xffffffff81	系统操作，由未经验证的用户执行的操作
0xffffffff86	超级用户
0xffffffff87	管理员
0xffffffff88	管理员 1
0xffffffff89	管理员 2
0xffffffff8a	管理员 3
0xffffffff8b	管理员 4

User Code/User Name

标识执行操作的用户的用户代码或用户名。
如果管理员执行该操作，其 ID 包含管理员的登录用户名。

Log ID

标识分配给日志的 ID。
这是一个标识日志的十六进制 ID。

访问日志信息项目

Access Log Type

指示访问的类型。

值	内容
Authentication	用户验证访问
Stored File	保存的文件访问
System	系统访问
Network Attack Detection/Encrypted Communication	网络冲突或加密的通信访问
Firmware	固件验证访问
Address Book	通讯簿访问
Device Settings	对用户工具菜单中的设置进行的更改。

Authentication Server Name

指示最后一次尝试验证的服务器的名称。

No. of Authentication Server Switches

指示系统在验证服务器不可用时切换服务器的次数。
您可以检查验证服务器是否可用。
服务器切换次数指示为 0 到 4。
“0” 指示验证服务器可用。

Logout Mode

注销方式。

值	内容
by User's Operation	用户手动注销
by Auto Logout Timer	超时后自动注销

Login Method

指示收到验证请求的路径。

值	内容
Control Panel	使用控制面板执行登录。
via Network	使用网络计算机执行远程登录。
Others	使用其他方法执行登录。

Login User Type

指示登录用户的类型。

值	内容
User	普通用户
Guest	访客用户
User Administrator	用户管理员
Machine Administrator	机器管理员
Network Administrator	网络管理员
File Administrator	文件管理员
Supervisor	超级用户
Customer Engineer (Service Mode)	客户工程师
Others	来自以上所指定人员以外用户的登录请求

Target User Entry ID

指示目标用户的条目 ID。

这是一个十六进制 ID，它指示应用以下设置的用户：

- Lockout

- Password Change

Target User Code/User Name

访问其数据的用户的用户代码或用户名。
如果访问管理员的数据，则记录管理员的用户名。

Address Book Registration No.

指示执行操作的用户的注册号码。

Address Book Operation Mode

指示用于更改通讯簿中注册的数据的方法。

Address Book Change Item

指示更改通讯簿中的哪个项目。

Address Book Change Request IP Address

指示使用通讯簿的用户的 IP 地址类型(IPv4/IPv6)。

Lockout/Release

指示锁定状态。

值	内容
Lockout	激活密码锁定
Release	取消密码锁定激活

Lockout/Release Method

指示用于解除锁定的方法。

值	内容
Manual	手动对机器解锁。
Auto	通过锁定解除定时器对机器解锁。

Lockout Release Target Administrator

指示解除锁定时所解锁的管理员。

Counter to Clear

指示为每个用户重置哪个计数器。

Export Target

指示要导出的设备设置文件中包含的设置。

值	内容
System Settings	系统设置
Copier Features	复印机功能
Printer Features	打印机功能
Scanner Features	扫描仪功能
Program (Copier)	程序（复印机）
Program (Scanner)	程序（扫描仪）
Program (Document Server)	程序（文件服务器）
Web Image Monitor Setting	Web Image Monitor 设置
Web Service Settings	Web 服务设置
System/Copier SP	系统/复印机 SP
Scanner SP	扫描仪 SP
Printer SP	打印机 SP

Target File Name

指示要导入/导出的设备信息文件的名称。

Stored File ID

标识创建或删除的文件。

这是一个十六进制 ID，它指示创建或删除的存储文件。

Stored File Name

指示所创建或删除文件的名称。

Delete File Type

表明文件删除的类型。

值	内容
Delete Normal File	常规文件删除
Delete Editing File	编辑时删除
Auto Delete	自动文件删除

值	内容
Others	其他原因删除文件

Folder Number

指示文件夹号码。

Folder Name

指示文件夹名称。

Creating/Deleting Folders

指示对文件夹执行的操作。

值	内容
Delete Folder	已删除文件夹
New Folder	已创建文件夹

File Location

指示所有已删除文件的原始位置。“Document Server”表示从机器的硬盘删除所有文件。

Collect Job Logs

指示作业日志收集设置的状态。

值	内容
Active	启用作业日志收集设置。
Inactive	禁用作业日志收集设置。
Not Changed	不对作业日志收集设置进行任何更改。

Collect Access Logs

指示访问日志收集设置的状态。

值	内容
Active	启用访问日志收集设置。
Inactive	禁用访问日志收集设置。
Not Changed	不对访问日志收集设置进行任何更改。

Collect Eco-friendly Logs

指示环保日志收集设置的状态。

值	内容
Active	启用环保日志收集设置。
Inactive	禁用环保日志收集设置。
Not Changed	不对环保日志收集设置进行任何更改。

Transfer Logs

指示日志传送设置的状态。

值	内容
Active	启用日志传送设置。
Inactive	禁用日志传送设置。
Not Changed	不对日志传送设置进行任何更改。

Log Type

如果日志的收集级别设置已更改，则此功能指示更改的详细信息。

值	内容
Job Log	作业日志
Access Log	访问日志
Eco-friendly Log	环保日志

Log Collect Level

指示日志收集的级别。

值	内容
Level 1	1 级
Level 2	2 级
User Settings	用户设置

Encryption/Cleartext

指示通信加密已启用还是已禁用。

值	内容
Encryption Communication	启用加密。
Cleartext Communication	禁用加密。

Machine Port No.

指示机器的端口号。

Protocol

目的地协议。

“Unknown” 指示无法识别目的地的协议。

IP Address

目的地 IP 地址。

Port No.

目的地端口号。

端口号以十进制数表示。

MAC Address

目的地 MAC（物理）地址。

Primary Communication Protocol

指示主要的通信协议。

Secondary Communication Protocol

指示次要的通信协议。

Encryption Protocol

指示用于对通信进行加密的协议。

Communication Direction

指示通信的方向。

值	内容
Communication Start Request Receiver (In)	机器收到开始通信的请求。

值	内容
Communication Start Request Sender (Out)	机器发送了开始通信的请求。

Communication Start Log ID

指示通信开始时间的日志 ID。

这是一个十六进制 ID，它指示启动通信的时间。

Communication Start/End

指示启动和结束通信的时间。

Network Attack Status

指示发生网络冲突时机器的状态。

值	内容
Violation Detected	检测到网络冲突。
Recovered from Violation	网络从冲突中恢复过来。
Max. Host Capacity Reached	由于传入数据量达到主机最大容量，机器无法操作。
Recovered from Max. Host Capacity	在降低传入数据量后，机器再次无法操作。

7

Network Attack Type

标识网络冲突类型。

值	内容
Password Entry Violation	密码破解
Device Access Violation	拒绝服务攻击 (DoS)
Request Falsification Violation	请求伪造

Network Attack Type Details

指示网络冲突类型的详细信息。

值	内容
Authentication Error	验证错误
Encryption Error	加密错误

Network Attack Route

标识网络冲突的路径。

值	内容
Attack from Control Panel	与使用机器控制面板进行的未经授权操作相冲突
Attack from Other than Control Panel	与非使用机器控制面板进行的未经授权操作相冲突

Login User Name used for Network Attack

标识网络冲突时所使用的登录用户名。

Add/Update/Delete Firmware

指示用于添加、更新或删除机器固件的方法。

值	内容
Updated with SD Card	SD 卡用于执行固件更新。
Added with SD Card	SD 卡用于安装固件。
Deleted with SD Card	SD 卡用于删除固件。
Moved to Another SD Card	将固件移到另一张 SD 卡中。
Updated via Remote	从远程计算机更新固件。
Updated for Other Reasons	通过以上方式之外的方法执行固件更新。

Module Name

固件模块名。

Parts Number

固件模块部件号。

Version

固件版本。

Machine Data Encryption Key Operation

指示所执行加密密钥操作的类型。

值	内容
Back Up Machine Data Encryption Key	已执行加密密钥备份。
Restore Machine Data Encryption Key	已恢复加密密钥。
Clear NVRAM	已清除 NVRAM。
Start Updating Machine Data Encryption Key	已开始加密密钥更新。
Finish Updating Machine Data Encryption Key	加密密钥更新完成。

Machine Data Encryption Key Type

标识加密密钥的类型。

值	内容
Encryption Key for Hard Disk	硬盘的加密密钥
Encryption Key for NVRAM	NVRAM 的加密密钥
Device Certificate	设备证书

Validity Error File Name

指示在其中检测到有效性错误的文件的名称。

Configuration Category

指示设置更改的类别。

值	内容
User Lockout Policy	用户锁定策略

值	内容
Auto Logout Timer	自动注销定时器
Device Certificate	设备证书
IPsec	IPsec
Compulsory Security Stamp	强制安全印记
S/MIME	S/MIME
WIM Auto Logout Timer	Web Image Monitor 自动注销定时器
Extended Security	安全扩展
Firmware Update Start	固件更新
Prohibit printing stored files from Web Image Monitor	禁止从 Web Image Monitor 打印保存的文件

7

Configuration Name/Configuration Value

指示类别的属性。

指示属性的值。

属性	描述
Lockout	记录锁定是有效(Active)还是无效(Inactive)。
Number of Attempts before Lockout	记录用户可能输入登录密码的次数。
Lockout Release Timer	记录锁定释放定时器是有效(Active)还是无效(Inactive)。
Lock Out User for	记录锁定释放之前的时间。
Auto Logout Timer	记录自动注销定时器是设置为(On)还是(Off)。
Auto Logout Timer (seconds)	记录自动注销操作之前的时间。
Operation Mode	记录操作的类型。
Certificate No.	记录要使用的证书编号。

属性	描述
Certificate No. : IEEE 802. 1X (WPA/WPA2)	记录用于应用程序的证书编号。 如果没有使用证书, 则系统会记录 “Do not Use” 。
Certificate No.: S/MIME	记录用于应用程序的证书编号。 如果没有使用证书, 则系统会记录 “Do not Use” 。
Certificate No.: IPsec	记录用于应用程序的证书编号。 如果没有使用证书, 则系统会记录 “Do not Use” 。
Certificate No.: Digital Signature PDF	记录用于应用程序的证书编号。 如果没有使用证书, 则系统会记录 “Do not Use” 。
Certificate No.: Digital Signature PDF/A	记录用于应用程序的证书编号。 如果没有使用证书, 则系统会记录 “Do not Use” 。
IPsec	记录 IPsec 是有效(Active)还是无效(Inactive)。
Encryption Key Auto Exchange: Setting1-4: Remote Address	记录远程地址。
Encryption Key Auto Exchange: Setting1-4, Default: Security Level	记录安全等级。 如果选择了[仅验证], 则系统会记录 “Authentication Only” 。 如果选择了[验证和低等级的加密], 则系统会记录 “Authentication and Low Level Encryption” 。 如果选择了[验证和高等级的加密], 则系统会记录 “Authentication and High Level Encryption” 。 如果选择了[用户设置], 则系统会记录 “User Settings” 。
Encryption Key Auto Exchange: Setting1-4, Default: Authentication Method	记录用于自动密钥交换格式的验证方式。记录 “PSK” 或 “Certificate” 。
Compulsory Security Stamp	记录[强制安全印记]是设置为(On)还是(Off)。
Scanner: Email Sending	如果扫描仪用于发送电子邮件, 则系统会记录签名。

属性	描述
Document Server (Utility): Stored File Transferring	如果文件服务器（应用程序）用于传送其保存的文件，则系统会记录签名。
WIM Auto Logout Timer (minutes)	Web Image Monitor 的自动注销定时器的记录以一分钟为增量。
Update Firmware	记录报告[更新固件]设置更改的日志条目。 记录 “Prohibit” 或 “Do not Prohibit” 。
Change Firmware Structure	记录报告[更改固件结构]设置更改的日志条目。 记录 “Prohibit” 或 “Do not Prohibit” 。
Firmware Update Start	记录报告固件更新的日志条目。
Prohibit printing stored files from Web Image Monitor	记录报告[禁止从 Web Image Monitor 打印保存的文件]设置更改的日志条目。 记录 “Prohibit” 或 “Do not Prohibit” 。

7

Destination Server Name

如果日志类型为 “Enhanced Print Volume Use Limitation: Tracking Permission Result”，指示未向其发送跟踪信息的目的地服务器的名称。

如果日志类型为导入或导出首选项信息，指示从中发布数据导出或导入请求的服务器的名称。

HDD Format Partition

指示格式化硬盘的原因。

值	内容
HDD Exchange	硬盘已更换。
Problem with HDD Encryption Key	硬盘加密密钥存在问题。
Problem with Disk Label	磁盘标签无法读取。
Problem with File System	文件系统存在问题。

Access Result

指示记录的操作的结果。

值	内容
Completed	操作已成功完成。
Failed	操作未成功完成。

作业日志（来源）

Source

指示作业文件的来源。

值	内容
Scan File	扫描作业文件。
Stored File	在硬盘上保存作业文件。
打印机	从打印机驱动程序发送作业文件。
Report	作业文件为打印的报告。

Start Date/Time

指示启动“Scan File”、“Received File”和“Printer”操作的时间。

End Date/Time

指示结束“Scan File”、“Received File”和“Printer”操作的时间。

Stored File ID

指示输出为存储文件的数据的 ID。

这是一个十进制 ID，它指示存储的文件。

Stored File Name

“Stored File”文件的名称。

Folder Number

指示在其中保存文件的文件夹号码。

Folder Name

指示在其中保存文件的文件夹名称。

Print File Name

“Printer”文件的名称。

作业日志（目标）

Target

作业目标的类型。

值	内容
Print	打印
Store	保存
Send	传送

Start Date/Time

指示开始“Print”、“Store”和“Send”操作的时间。

End Date/Time

指示结束“Print”、“Store”和“Send”操作的时间。

Destination Name

“Send”目的地的名称。

Destination Address

“Send”目的地的 IP 地址、路径或电子邮件地址。

Stored File ID

指示输出为存储文件的数据的 ID。

这是一个十进制 ID，它指示存储的文件。

Stored File Name

当目标类型为“Store”时，指示保存的文件的名称。

Folder Number

指示在其中保存文件的文件夹号码。

Folder Name

指示在其中保存文件的文件夹名称。

环保日志信息项目

Start Date/Time

记录事件开始日期和时间。

End Date/Time

记录事件结束日期和时间。

Log Type

记录环保日志的类型。

值	内容
Main Power On	主电源开启
Main Power Off	主电源关闭
Power Status Transition Result	电源状态转换结果
Job Related Information	作业相关的信息
Paper Usage	纸张使用
Power Consumption	功耗

Log Result

显示事件是否已结束。

值	内容
Completed	已完成
Failed	失败

7

Result

记录事件的结果。

值	内容
Succeeded	成功
Failed	失败

Log ID

标识分配给日志的 ID。这是一个标识日志的十六进制 ID。

Power Mode

记录机器的电源状态（状态转变以后）。

值	内容
Standby	待机状态

值	内容
Low Power	省电状态
Silent	静音状态
HDD On	HDD 打开状态
Engine Off	发动机关闭状态
Controller Off	控制器关闭状态
STR	STR 状态
Silent Print	静音打印状态
Low Power Print	低功率打印状态
Fusing Unit Off	定影单元关闭状态

Log Type

系统会记录作业日志的类型。

Job Interval(seconds)

指示从上一作业开始到当前作业开始过去的时间。

Job Duration (seconds)

指示从作业开始到结束过去的时间。

Paper Usage (Large Size)

指示每小时大尺寸纸张的单面打印数。

大尺寸指的是 A3（11 × 17 英寸）或更大。

Paper Usage (Small Size)

指示每小时小尺寸纸张的单面打印数。

小尺寸指的是比 A3（11 × 17 英寸）小。

Paper Usage (2 Sided: Large Size)

指示每小时大尺寸纸张的双面打印数。

大尺寸指的是 A3（11 × 17 英寸）或更大。

Paper Usage (2 Sided: Small Size)

指示每小时小尺寸纸张的双面打印数。

小尺寸指的是比 A3（11 × 17 英寸）小。

Detected Power

使用机器时，系统会测量机器的功耗状态并将其记录在日志中。

值	内容
Controller Standby	控制器待机模式
STR	暂存于 RAM (STR)模式
Main Power Off	主电源处于关闭状态。
Scanning/Printing	同时扫描和打印
Printing	机器的打印状态
Scanning	机器的扫描状态
Engine Standby	发动机的待机状态
Engine Low	发动机的省电状态
Engine Night	发动机的静音状态
Engine Total	机器的耗电总量
Fusing Unit Off	定影单元关闭状态

Power Consumption(Wh)

指示每种功率状态下的功耗。

7

指定日志收集设置

启用各种日志的收集设置并配置收集等级。

作业日志收集等级

如果“作业日志收集等级”设置为“[等级 1]”，则系统会收集所有作业日志。

访问日志收集等级

如果“访问日志收集等级”设置为“[等级 1]”，则访问日志中会记录以下项目：

- 硬盘格式化
- 删除所有日志
- 更改日志设置
- 更改日志收集项目

如果“访问日志收集等级”设置为“[等级 2]”，则系统会收集所有访问日志。

环保日志收集等级

如果“环保日志收集等级”设置为“[等级 1]”，则系统不会收集环保日志。

如果“环保日志收集等级”设置为“[等级 2]”，则系统会收集所有环保日志。

1. 以机器管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在设备设置下，单击[日志]。
4. 为以下各种功能选择[有效]：“收集作业日志”、“收集访问日志”和“收集环保日志”。
5. 为以下各种功能指定收集等级：“作业日志收集等级”、“访问日志收集等级”和“环保日志收集等级”。

如果更改了等级，则日志详细信息的选择状态将根据等级而变化。

要更改日志详细信息的各个项目，请配置各个项目的设置。即使收集等级已设置为[等级 1]或[等级 2]，当更改日志详细信息的各个项目以后，等级也会变为[用户设置]。

6. 单击[确定]。
7. 将出现“正在更新...” 。等待约 1 至 2 分钟，然后单击[确定]。

单击[确定]后，如果没有重新显示上一屏幕，请等待一段时间，然后单击 Web 浏览器的“刷新”按钮。

8. 注销。

↓ 注

- “访问日志收集等级”的设置值越大，所收集的日志就越多。

下载日志

根据以下步骤将机器中保存的日志转换为 CSV 文件，用于同时进行批量下载。

要收集日志，请将作业日志、访问日志和环保日志的收集设置配置为[有效]。

此设置可以在 Web Image Monitor 的[配置]下的[日志]中指定。

1. 以机器管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在“设备设置”下，单击[下载日志]。
4. 从“下载的日志”的下拉框中选择要下载的日志类型。

安全日志包括 2 种类型的日志：作业日志和访问日志。
5. 单击[下载]。
6. 指定要保存文件的文件夹。
7. 单击[后退]。
8. 注销。

注

- 所下载的日志包含单击[下载]按钮之前记录的数据。不会下载单击[下载]按钮后记录的任何日志。未完成作业的日志条目的“Result”字段将是空白的。
- 根据日志的数量，下载时间可能会有所不同。
- 若下载或创建 CSV 文件时出现错误，则下载将被取消，文件结尾处包括错误的详细信息。
- 如果成功下载了日志，则日志文件的最后一行将显示“Download completed.”。
- 有关保存 CSV 日志文件的详细信息，请参见浏览器的帮助。
- 下载的日志文件使用 UTF-8 字符编码。要查看日志文件，请使用支持 UTF-8 的应用程序打开它。
- 有关日志中包含的项目的详细信息，请参见 p.179 “可下载日志的属性”。

可以保存在机器上的日志数

如果作业日志、访问日志或环保日志的数量超过机器上可以保存的最大数量，并且有新的日志生成，则新日志将覆盖旧日志。如果没有定期下载日志，则无法将旧日志记录到文件中。

使用 Web Image Monitor 来管理日志时，请按照适合下表中条件的时间间隔下载日志。

下载日志以后，请执行日志的批量删除操作。

如果更改日志收集的[收集]/[不收集]设置，则必须执行日志的批量删除操作。

可以存储在机器中的最大日志数

日志类型	最大日志数
作业日志	4000
访问日志	12000
环保日志	4000

预计每天创建的日志数

日志类型	每天创建的日志数
作业日志	100
访问日志	300 此数字基于 100 次操作（例如初始化和通过 Web 进行的访问操作）以及 200 个作业条目（每个作业 2 个条目：1 个登录条目和 1 个注销条目）。

日志类型	每天创建的日志数
环保日志	100

根据这些条件，机器可以保留日志 40 天，而不会进行覆盖。为了防止发生错误，建议每 20 天下载一次日志。

机器管理员必须适当地管理下载的日志文件。

注

- 下载日志时，请勿执行会创建日志条目的操作，因为正在下载的日志无法记录新条目。
- 日志的批量删除操作可以通过控制面板或 Web Image Monitor 执行。

有关日志条目数达到最大值时的操作注意事项

如果机器上可以保存的日志数超过指定的最大值，则新日志将覆盖旧日志。为各个作业日志、访问日志和环保日志定义可以保存的最大日志数。

作业日志和访问日志将作为一个文件下载。

下面所说的“如果下载日志而不覆盖”表示作业日志和访问日志在下载以后合并在一起。

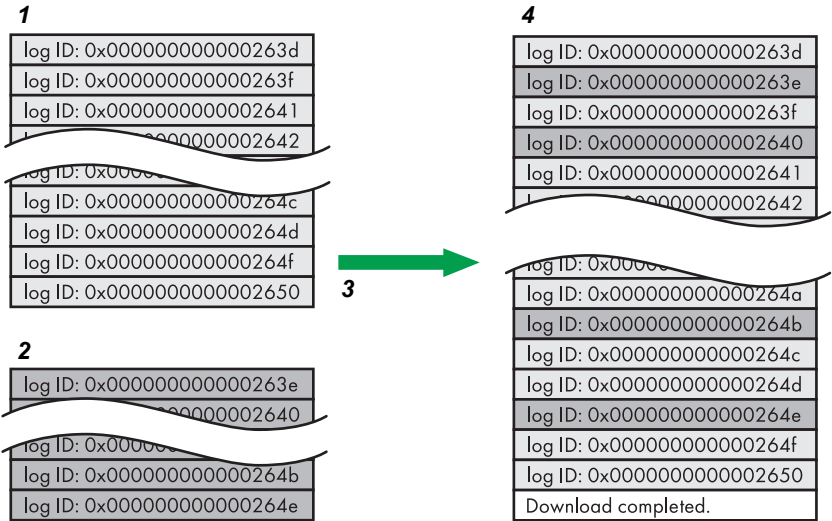
下面所说的“如果在覆盖过程中下载日志”表示部分访问日志会被覆盖。

在此示例中，部分访问日志会被下载的日志覆盖并删除。

环保日志将作为独立的文件下载。

日志条目按优先级顺序进行覆盖。优先级较高的日志条目将不会被覆盖或删除。

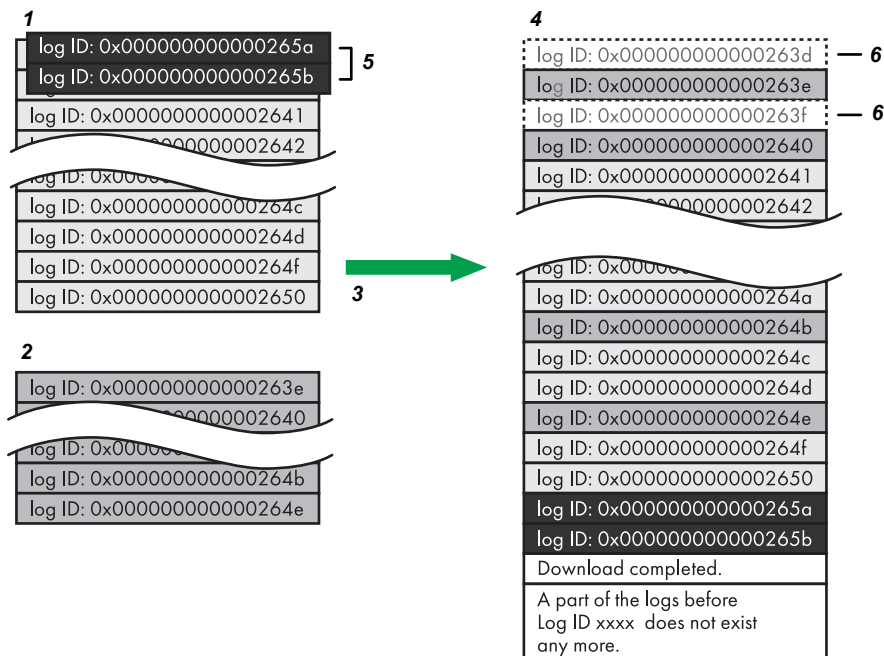
如果在不覆盖日志的情况下下载日志



CJD006

1. 访问日志
2. 作业日志
3. 下载
4. 下载的日志

如果在覆盖期间下载日志



CJD007

1. 访问日志
2. 作业日志
3. 下载
4. 下载的日志
5. 覆盖
6. 通过覆盖删除

要确定在下载日志时是否存在覆盖的情况，请检查所下载日志的最后一行信息。

- 如果没有出现覆盖情况，则最后一行将包含以下消息：Download completed.
- 如果出现覆盖情况，则最后一行将包含以下消息：Download completed. A part of the logs before Log ID xxxx does not exist any more.

↓ 注

- 如果发生覆盖，覆盖将删除一部分日志，因此请检查日志 “Log ID xxxx” 以及较新的日志。

打印机作业日志

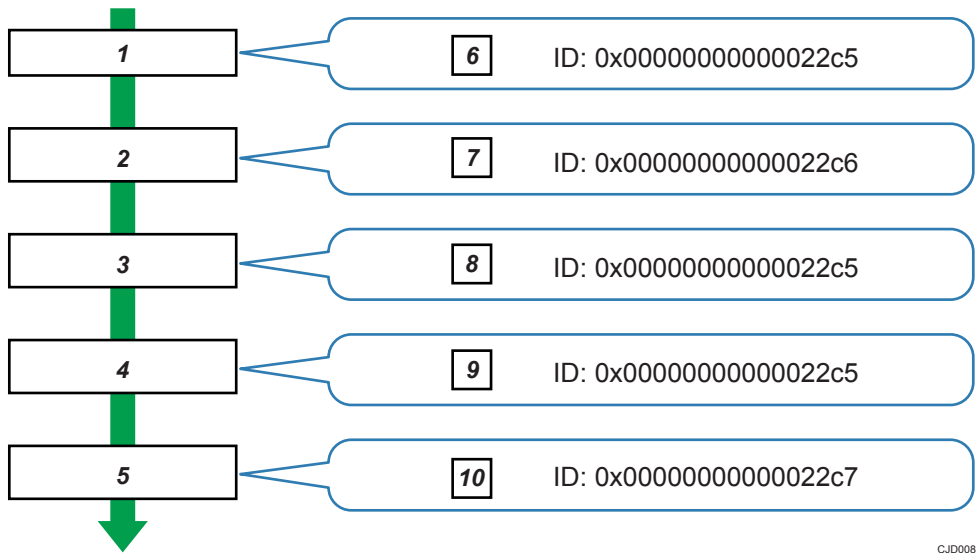
在访问日志中，打印日志条目是在登录条目之前记录的。

作业的详细信息（接收、处理、作业数据的输出等）记录为单个条目。

机器收到打印作业时，将为该作业创建一个 ID，并且在作业日志中记录此信息。随后，机器将为打印作业创建一个登录 ID，并且在访问日志中记录此信息。之后，会创建作业日志条目，记录所处理和输出的作业的详细信息（在同一登录 ID 下）。机器处理完作业以后，将创建一个注销条目，并且将其记录在访问日志中。

机器将首先在作业日志中创建打印作业接收、处理和输出等操作的详细信息的条目，然后在访问日志中记录这些作业的登录和注销详细信息。

打印作业流程图



CJD008

1. 收到打印作业数据。
2. 收到验证（登录）数据。
3. 处理打印作业。
4. 输出打印作业。
5. 收到验证（登录）数据。
6. 机器为打印作业分配一个 ID，并且在作业日志中将其记录为一个条目。
7. 机器在访问日志中将验证（登录）数据记录为一个条目。
8. 机器在作业日志中将有关打印作业处理的信息记录为一个条目（使用同一个 ID）。
9. 机器在作业日志中将有关打印作业输出的信息记录为一个条目（使用同一个 ID）。
10. 机器在访问日志中将验证（注销）数据记录为一个条目。

删除所有日志

根据以下步骤删除机器中保存的所有日志。

如果将作业日志、访问日志或环保日志之一设置为[有效]，则会出现“删除所有日志”。

1. 以机器管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在设备设置下，单击[日志]。
4. 在“删除所有日志”下单击[删除]。
5. 单击[确定]。
6. 注销。

禁止向日志收集服务器传送日志

使用以下步骤可以禁止向日志收集服务器传送日志。请注意，只有当日志传送设置已经设为[有效]时，方可将其改为[无效]。

1. 以机器管理员身份从 Web Image Monitor 登录。
2. 指向[设备管理]，然后单击[配置]。
3. 在设备设置下，单击[日志]。
4. 在“所有日志的通用设置”下方的[转送日志]区域中选择[无效]。
5. 单击[确定]。
6. 注销。

从机器中管理日志

您可以指定设置，如日志收集设置、是否向日志收集服务器传输日志以及是否删除所有日志。

指定日志收集设置

启用每种日志类型的收集设置。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按 4 次[▼向后]。
5. 按[收集日志]。
6. 为以下各种功能选择[有效]：“作业日志”、“访问日志”和“环保日志”。
7. 按[确定]。
8. 注销。
9. 关闭主电源开关，然后重新打开主电源开关。

7

禁止向日志收集服务器传送日志

使用以下步骤可禁止从机器向日志收集服务器传送日志。请注意，只有当前日志传送设置已经设为[开]时，方可将其改为[关]。

有关日志收集服务器的详细信息，请与销售代表联系。

有关传送日志设置的详细信息，请参见日志收集服务器手册。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按两次[▼向后]。
5. 按[传送日志设置]。
6. 按[关]。
7. 按[确定]。
8. 注销。

指定删除所有日志

根据以下步骤删除机器中保存的所有日志。

仅当日志收集服务器正在运行或者如果 Web Image Monitor 设置已经被指定为收集作业日志、访问日志和环保日志时，才能一次批量删除机器的所有日志。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按两次[▼向后]。
5. 按[删除所有日志]。
6. 按[是]。
7. 按[退出]。
8. 注销。

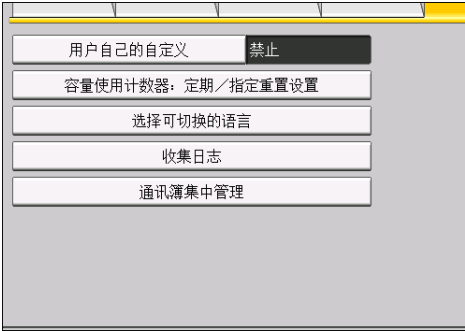
通过日志收集服务器管理日志

有关使用日志收集服务器管理日志文件的详细信息，请参见日志收集服务器附带的手册。

为单个用户配置主页屏幕

这样可以让各个用户使用自己的主页屏幕。
用户登录以后，将会显示其个性化主页屏幕。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按 4 次[▼向后]。
5. 按[用户自己的自定义]。



6. 按[允许]，然后按[确定]。
7. 注销。

注

- 此外也可以通过 Web Image Monitor 进行配置。有关详细信息，请参见 Web Image Monitor 帮助。
- 即使用户自己的自定义设置为[禁止]，系统仍然会保留各个用户的主页信息。该设置更改回[允许]以后，用户可以再次使用这些信息。

有关使用用户自己的主页屏幕的警告

使用此功能之前，请注意这些警告。

- 在通讯簿中注册用户以后，系统会为该用户创建主页屏幕。用户自己的主页屏幕将使用默认的设置进行配置（图标排列）。
- 如果菜单保护设置为[1 级]或[2 级]，则用户无法使用该功能的程序注册，也无法编辑或删除屏幕。但是，用户可以添加图标到自己的主页屏幕。
- 如果菜单保护已设置为[1 级]或[2 级]，请让机器管理员创建所需的任何程序。
- 将仅显示用户有权访问的功能图标。
- 如果从通讯簿中删除了用户，则系统也会删除该用户的主页屏幕信息。

- 用户编辑程序时，更改会出现在包含该程序图标的各个用户的主页屏幕上。
- 用户删除程序时，该程序的图标从包含该程序图标的所有用户的主页屏幕上删除。
- 由于每个用户都可以自定义其主页屏幕，因此管理员无法检查每个用户的主页信息。

管理设备信息

注意

- 请将 SD 卡或者 USB 闪存设备置于儿童接触不到的地方。如果儿童误吞 SD 卡或者 USB 闪存设备，请立即送医。

具有权限管理设备、用户、网络和管理文件的设备管理员可以设置机器的设备信息。

机器的设备信息可作为设备设置信息文件导出到外部设备。通过将导出的设备设置信息文件导入到机器，您可将其用作备份文件来恢复设备设置。

此外，通过管理设备服务器管理设备设置信息文件，可以定期在指定时间或设备启动时导入设备设置信息文件。

可以导入和导出的数据

- 复印机/文件服务器特性
- 打印特性
- 扫描仪特性
- 编入（文件服务器）
- 程序（复印机）
- 程序（扫描仪）
- Web Image Monitor 设置
- Web 服务设置
- 系统设置

无法导入或导出的数据

- 部分系统设置*1 *2

*1 日期设置、需要设备证书的设置和需要为每台机器调整的设置（如图像调整设置）无法导入或导出。

*2 只针对执行功能和查看的设置无法导入或导出。

- 扩展功能设置
- 通讯簿
- 程序（打印机功能）
- 复印机/文件服务器特性中的用户印记
- 可通过 telnet 指定设置
- @Remote-相关数据
- 计数器
- 外部打印机单元设置

- 只能通过 Web Image Monitor 或 Web 服务（例如，Bonjour、SSDP 设置）指定的设置

↓ 注

- 导出的文件格式为 CSV。
- 导入设备设置信息文件的机器与导出了设备设置信息文件的机器的设备配置必须相同。否则，将无法导入设备设置信息文件。
- 只有在型号、使用地区以及下列设备配置相匹配的机器之间才可以导入和导出。
 - 输入纸盘
 - 输出纸盘
 - 是否配备文件制成机和文件制成机的类型
 - ADF
- 如果设备配置已发生变化，则请导出更新的设备设置信息文件。
- 如果存在设备配置相同的机器，则可通过导入相同的设备设置文件，以同样的方式指定其设置。
- 如果主屏幕中包含 JPG 图像文件，这些文件也会被导出。
- 用户正在操作机器时，系统无法导入或导出任何内容，直到用户完成操作为止。
- 在导出和导入过程中，机器无法执行其他操作。
- 有关处理 SD 卡的详细信息，请参见“开始使用”中的“插入/取出存储设备”。
- 您也可以使用 Web Image Monitor 来配置导入、导出和服务器设置。

导出设备信息

从控制面板导出设备信息时，数据将保存在 SD 卡上。

1. 在控制面板侧面的介质插槽中插入 SD 卡。

有关插入 SD 卡的详细信息，请参见《开始使用》中的“插入/取出存储设备”。

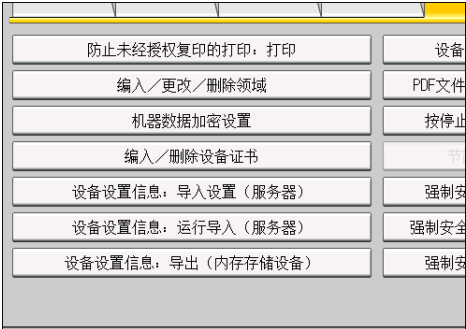
2. 从控制面板作为具有用户管理员、机器管理员、网络管理员和文件管理员权限的管理员登录。

3. 按[系统设置]。

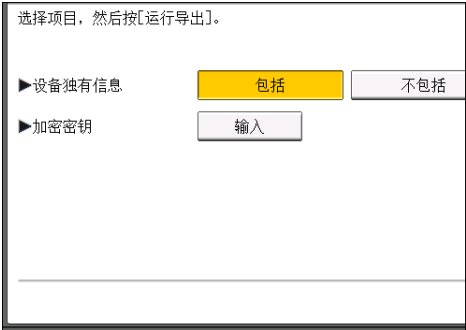
4. 按[管理员工具]。

5. 按 3 次[▼向后]。

6. 按[设备设置信息：导出（内存存储设备）]。



7. 设置导出条件。



- 指定要[包括]还是[不包括]“设备独有信息”。“设备独有信息”包括 IP 地址、主机名称等等。
- 指定一个加密密钥。

8. 按[运行导出]。

9. 按[确定]。

10. 按[退出]。

11. 注销。

↓ 注

- 如果导入或导出失败，您可以查看错误日志。日志存储在与导出的设备设置信息文件相同的位置。

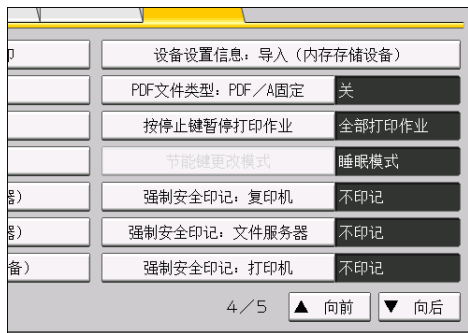
导入设备信息

导入 SD 卡上保存的设备信息。

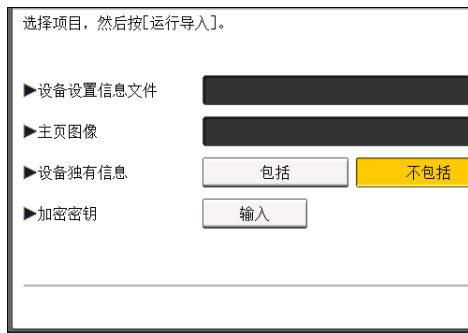
1. 在控制面板侧面的介质插槽中插入 SD 卡。

有关插入 SD 卡的详细信息，请参见《开始使用》中的“插入/取出存储设备”。

- 2. 从控制面板作为具有用户管理员、机器管理员、网络管理员和文件管理员权限的管理员登录。
- 3. 按[系统设置]。
- 4. 按[管理工具]。
- 5. 按 3 次[▼向后]。
- 6. 按[设备设置信息：导入（内存存储设备）]。



7. 配置导入条件。



- 按“设备设置信息文件”的[选择]，以选择要导入的文件。
- 向主屏幕上添加图像时，按“主页图像”的[选择]，然后选择文件。
- 指定要[包括]还是[不包括]“设备独有信息”。“设备独有信息”包括 IP 地址、主机名称等等。
- 输入导出文件时指定的加密密钥。

8. 按[运行导入]。

9. 按[确定]。

10. 按[退出]。

机器会重新启动。

↓ 注

- 如果导入或导出失败，您可以查看错误日志。日志存储在与导出的设备设置信息文件相同的位置。

定期导入设备信息

该设置会将保存在服务器中的设备信息自动导入机器。

1. 从控制面板作为具有用户管理员、机器管理员、网络管理员和文件管理员权限的管理员登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按 3 次[▼向后]。
5. 按[设备设置信息：导入设置（服务器）]。
6. 配置导入条件。

选择项目，然后按[确定]。

▶导入文件从

设备管理服务器 Web服务器 不指定

服务器设置 更改

▶在指定时间预订导入

在指定时间1 在指定时间1&2

指定时间1 00:00 更改

指定时间2 00:00 更改

- 选择导入文件的来源。使用服务器的详细设置，配置 URL、用户名、密码等设置。
- 选择导入设备设置信息文件的频率，并设置用于定期在指定时间导入的时间。
- 选择是否要在以下情况下导入设备设置信息文件：如果该文件与上次导入的文件相同。
- 对要导入的设备设置信息文件进行加密时，请配置加密密钥。
- 选择是否要在导入失败时向机器管理员发送电子邮件通知。

7. 按[确定]。

8. 注销。

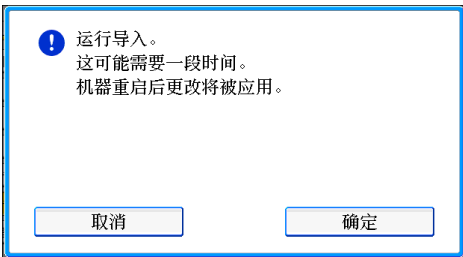
注

- 此外也可以通过 Web Image Monitor 进行配置。有关详细信息，请参见 Web Image Monitor 帮助。
- 当使用管理设备服务器时，可以进行更多详细的导入设置。有关更多详细信息，请参见管理设备服务器的用户手册。
- 如果导入或导出失败，您可以查看错误日志。日志存储在与导出的设备设置信息文件相同的位置。

手动导入服务器的设备设置信息文件

手动向机器导入用[设备设置信息：导入设置（服务器）]指定的设备设置信息文件。

1. 从控制面板作为具有用户管理员、机器管理员、网络管理员和文件管理员权限的管理员登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按 3 次[▼向后]。
5. 按[设备设置信息：运行导入（服务器）]。
6. 按[确定]。



7. 按[退出]。
机器会重新启动。

注

- 如果导入或导出失败，您可以查看错误日志。日志存储在与导出的设备设置信息文件相同的位置。

故障排除

如果出现错误，请首先查看日志的结果代码。0 以外的数值表示发生错误。结果代码将显示在以下图示的圆形区域中。

日志文件示例

```
"1.0.0"
"ExecType", "Date", "SerialNo", "PnP", "Model", "Destination", "IP", "Host", "Storage", "FileName", "FileID", "TotalItem", "NumOfOkItem", "ResultCode", "ResultName", "Identifier"
"IMPORT"
"20XX-07-05T15:29:16+09:00"
"3C35-7M0014"
"Brand Name"
"Product Name"
"0"
"10"
"10.250.155.125"
"RNP00267332582D"
"SD"
"20XX07051519563C35-710220.csv"
"20XX07051519563C35-710220"
" 0"
- - -
" 2"
- - - REQUEST
"TargetID", "ModuleID", "PrefID", "Item", "NgCode", "NgName"
```

CJD023

如果您在查看代码后无法解决问题或不知道如何解决，请记下错误日志条目，然后联系服务代表。

7	ResultCode	原因	解决方法
	2 (INVALID REQUEST)	尝试在不同型号或具有不同设备配置的机器之间导入文件。	导入从具有相同设备配置的相同型号导出的文件。
	4 (INVALID OUTPUT DIR)	将设备信息写入目标设备失败。	检查目标设备是否正常运行。
	7 (MODULE ERROR)	导入或导出时出现意外错误。	关闭电源后再打开，然后再次尝试操作。如果仍出现错误，请与服务代表联系。
	8 (DISK FULL)	外部媒介的可用存储空间不足。	确保存储空间足够后重新执行操作。
	9 (DEVICE ERROR)	写入或读取日志文件失败。	检查用于存储文件的文件夹路径或存储文件的文件夹路径是否可用。
	10 (LOG ERROR)	写入日志文件失败。硬盘存在故障。	请与服务代表联系。

ResultCode	原因	解决方法
20 (PART FAILED)	导入部分设置失败。	失败原因记录在“NgName”中。请检查代码。 错误原因(NgName) 2 INVALID VALUE 指定的数值超过允许的范围。 3 PERMISSION ERROR 不具备编辑设置的权限。 4 NOT EXIST 系统中不存在该设置。 5 INTERLOCK ERROR 由于系统状态或与其他指定设置的关系，该设置无法更改。 6 OTHER ERROR 由于某种其他原因，该设置无法更改。
21 (INVALID FILE)	由于外部媒介中的格式错误，文件导入失败。	检查文件格式是否正确。日志为 CSV 文件格式。
22 (INVALID KEY)	加密密钥无效。	请使用正确的加密密钥。

管理环保计数器

如果正在使用用户验证，则系统会在用户登录时显示有关环保计数器的信息。

环保计数器指示总打印页数中使用彩色、双面和合并打印的频率。

同时，环保指数也指示节省的碳粉量和纸张数。环保指数越高，表示节省的资源越多。

↓ 注

- 使用基本验证、Windows 验证或 LDAP 验证来进行用户验证时，机器会收集数据并显示各个用户的环保计数器。
- 使用用户代码验证来进行用户验证或者不使用用户验证时，机器会收集数据并显示它的总环保计数器。

配置环保计数器

设置收集环保计数器数据的时段以及管理员的消息。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[▼向后]。
5. 按[环保计数器期间/管理员信息]。
6. 更改设置。
7. 按[确定]。
8. 按[退出]。
9. 注销。

计数期间

设置收集环保计数器数据的时段。

如果选择了[指定日]，则系统会收集每个指定天数的环保计数器数据。

默认设置：[不计数]

管理员信息

选择用户登录时显示的信息。

如果您选择“固定信息 1”或“固定信息 2”，则会显示默认消息。

如果您选择“用户信息”，则机器管理员可以输入要显示的消息。

默认设置：[固定信息 1]

显示信息画面

指定用户登录时是否显示信息屏幕。

默认设置: [关]

显示时间

指定何时显示信息屏幕。

默认设置: [每次登录]

重置机器的环保计数器

您可以重置机器的环保计数器。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[显示/清除环保计数器]。
5. 按[清除当前值]或[清除当前和上次的值]。
6. 按[确定]。
7. 注销。

重置用户的环保计数器

通过重置用户的环保计数器，将重置所有用户的环保计数器。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[每个用户显示/清除环保计数器]。
5. 按[清除当前值]或[清除当前和上次的值]。
6. 按[确定]。
7. 注销。

管理通讯簿

指定自动删除通讯簿数据

指定在通讯簿中注册的数据达到限额后，机器如何处理自动注册请求。

如果您将此设置为[开]，则会自动添加新用户帐户并删除旧用户帐户。首先会删除那些很长时间不使用的帐户。

如果将此设置为[关]，则不会删除旧用户帐户，所以在注册数据数达到限额后将不会再添加新的用户帐户。

1. 以用户管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[自动删除通讯簿中的用户]。
5. 选择[开]，然后按[确定]。
6. 注销。

↓ 注

- 仅当机器收到数据注册请求后，才会自动删除数据。如果手动添加用户帐户，则不会执行自动删除。
- 仅会自动删除具有用户代码或登录用户名和密码的用户帐户。

删除通讯簿中的所有数据

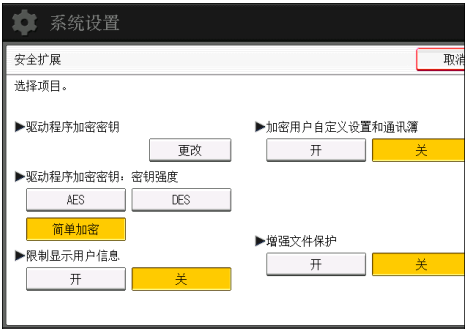
您可以删除通讯簿中注册的所有数据。

1. 以用户管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按[删除通讯簿中的所有数据]。
5. 按[是]，然后按[退出]。
6. 注销。

指定扩展安全功能

除了通过用户验证和每个管理员指定对机器的访问限制来提供基本安全功能外，还可以通过
对传送的数据和地址簿中的数据进行加密来提高安全性。

- 1. 以具有权限的管理员身份从控制面板登录。
- 2. 按[系统设置]。
- 3. 按[管理员工具]。
- 4. 按[▼向后]。
- 5. 按[安全扩展]。
- 6. 按您要更改的设置，然后更改设置。



- 7. 按[确定]。
- 8. 注销。

注

- 根据设置，管理员的操作权限会有所不同。

驱动程序加密密钥

网络管理员可以指定此设置。

当用户验证设置为“开”时，指定用于对从驱动程序发送的登录密码或文件密码进行解密的文本字符串。

要指定驱动程序加密密钥，请在驱动程序中注册使用机器指定的加密密钥。

有关详细信息，请参见 p.144 “指定驱动程序加密密钥”。

驱动程序加密密钥：密钥强度

网络管理员可以指定此设置。

指定用于从驱动程序向机器发送作业的加密强度。

机器确认附加到作业的密码的加密强度并进行处理。

如果指定了[简单加密]，则系统会接受通过用户验证的所有作业。

如果指定了[DES]，则系统会接受使用 DES 或 AES 加密的作业。

如果指定了[AES]，则系统会接受使用 AES 加密的作业。

如果您选择了[AES]或[DES]，请使用打印机驱动程序指定加密设置。有关指定打印机驱动程序的信息，请参见打印机驱动程序的帮助。

默认值：[简单加密]

限制显示用户信息

如果指定了用户验证，机器管理员可以指定此设置。

使用未进行验证的网络连接检查作业历史记录时，所有个人信息将显示为“*****”。由于无法查看表明注册用户身份的信息，因此可以防止未经授权的用户获得有关注册文件的信息。

默认设置：[关]

加密用户自定义设置和通讯簿

用户管理员可以指定此设置。

对机器用户的个别设置和通讯簿中的数据进行加密。

即使有人非法获取了机器内部的信息，加密措施也可以防止他人读取各个用户的设置或通讯簿数据。

有关详细信息，请参见 p.75 “保护通讯簿”。

默认设置：[关]

增强文件保护

文件管理员可以指定此设置。

通过指定密码，文件管理员可以限制打印、删除和发送文件等操作。同时，文件管理员可以防止未经授权的用户访问文件。不过，仍有可能防止密码被破解。

通过指定“增强文件保护”，如果输入十次无效密码，文件将被锁定并变得无法访问。这可以防止有人使用随机密码尝试未经授权访问文件。

如果已启用增强文件保护功能，屏幕右下角将会显示图标。

锁定的文件只能由文件管理员解除锁定。

文件锁定后，即使您输入了正确的密码，也无法选择它们。

默认设置：[关]

限制目的地的使用

用户管理员可以指定此设置。

扫描仪可用的目的地仅限于在通讯簿中注册的目的地。

所有用户均不能直接输入传送目的地。

如果指定通过 SMTP 接收电子邮件的设置，则不能使用“限制目的地的使用”。

您可以使用通过“LDAP 搜索”搜索到的目的地。

有关详细信息，请参见 p.57 “限制使用目的地列表”。

默认设置：[关]

限制添加用户目的地

用户管理员可以指定此设置。

如果设置了“限制添加用户目的地”，则用户只需通过以下方式即可在通讯簿中注册扫描仪目的地：输入目的地，然后按[编入地址]。如果您将这些功能设置为[开]，则屏幕上不会显示[编入地址]键。尽管如此，用户仍可以使用扫描仪屏幕直接输入目的地，但不能通过按[编入地址]在通讯簿中注册该目的地。

此外，还要注意，即使您将这些功能设置为[开]，在通讯簿中注册的用户仍然可以更改其密码。只有用户管理员可以更改除密码以外的项目。

默认设置：[关]

SNMPv1,v2 设置

网络管理员可以指定此设置。

如果使用 SNMPv1 或 SNMPv2 协议访问机器，则无法执行验证，因此可以更改机器管理员指定的纸张设置或其他设置。如果您选择[禁止]，则可以查看该设置，但不能使用 SNMPv1,v2 来指定它。

默认值：[不禁止]

验证当前作业

机器管理员可以指定此设置。

利用此设置，可指定在复印机和打印机功能下取消作业等操作是否需要验证。

如果选择[登录权限]，则获得授权的用户和机器管理员可以使用机器。当选择此设置时，对于在选择[登录权限]前就登录到机器的用户，不需要进行验证。

如果指定了[访问权限]，则执行了复印或打印作业的任何用户都可以取消该作业。此外，机器管理员还可以取消用户的复印或打印作业。

如果您无权使用复印和打印机功能，则即使选择了[登录权限]而且也登录到机器，也无法取消正在处理的复印或打印作业。

只有在指定了“用户验证管理”时，您才能指定“验证当前作业”。

默认设置：[关]

密码策略

用户管理员可以指定此设置。

利用此设置，可以指定密码的[复杂性设置]和[最小字符数]。指定此设置后，只能使用满足“复杂性设置”和“最小字符数”中所指定条件的密码。

如果选择[1 级]，请从大写字母、小写字母、十进制数字和诸如#之类的符号中选择 2 种字符，通过这 2 种字符的组合来指定密码。

如果选择[2 级]，请从大写字母、小写字母、十进制数字和诸如#之类的符号中选择 3 种字符，通过这 3 种字符的组合来指定密码。

默认值：[关]字符数没有限制，且未指定字符类型。

@Remote 服务

机器管理员可以指定此设置。

如果选择[禁止]，则会禁用@Remote 服务通过 HTTPS 进行的通信。

将它设置为[禁止]时，请向服务代表咨询。

如果它被设置为[禁止部分服务]，则不能通过远程连接更改设置，从而以最佳方式提供安全的操作。

默认值：[不禁止]

更新固件

机器管理员可以指定此设置。

该设置用于指定是否允许机器进行固件更新。可以由服务代表更新固件，或通过网络执行固件更新。

如果选择[禁止]，机器上的固件将不能更新。

如果选择[不禁止]，则不限制固件更新。

默认值：[不禁止]

更改固件结构

机器管理员可以指定此设置。

该设置用于指定是否防止更改机器的固件结构。“更改固件结构”功能会在插入、卸下或更换 SD 卡时检测机器的状态。

如果选择[禁止]，启动过程中检测到固件结构更改时，机器就会停止，并会显示请求管理员登录的消息。机器管理员登录后，机器会以更新后的固件完成启动。

管理员可以检查控制面板屏幕上显示的固件版本来确认是否允许固件结构更改。如果不允许固件结构更改，请在登录前联系服务代理商。

“Change Firmware Structure”设置为[禁止]时，必须启用管理员验证。

指定[禁止]以后，请禁用管理员验证。再次启用管理员验证时，您可以将设置恢复为[不禁止]。

如果选择[不禁止]，则会禁用固件结构更改检测。

默认值：[不禁止]

密码输入非法

机器管理员可以指定此设置。

如果验证请求的次数超过该设置指定的次数，则系统会将访问归类为密码攻击。该访问会记录在访问日志中，并且系统会通过电子邮件将日志数据发送给机器管理员。

如果“允许最多访问次数”设置为[0]，则系统不会检测密码攻击。

- 允许最多访问次数

指定允许验证尝试的最大次数。

使用数字键指定“0”和“100”之间的值，然后按[#]。

默认值: [30]

- 监测时间

指定导致验证失败的重复验证尝试之间的间隔。超过监测时间后，将会清除验证尝试记录。

使用数字键指定“1”和“10”之间的值，然后按[#]。

默认值: [5]

注

- 根据为[允许最多访问次数]和[监测时间]等设置指定的值，您可能会频繁收到非法访问检测电子邮件。
- 如果您频繁收到非法访问检测电子邮件，请检查内容并复查设置值。

非法访问的安全设置

机器管理员。

当通过网络应用程序登录到机器时，可能由于用户验证尝试的次数与机器上指定的尝试次数不匹配而使用户被错误锁定。

例如，从某个应用程序发出多份多页面的打印作业时，访问可能会被拒绝。

如果您在“非法访问的安全设置”下选择[开]，则可以防止此类验证错误。

- 开

- 非法访问的禁止期限

指定允许多少用户访问。

使用数字键指定“0”和“60”之间的值，然后按[#]。

默认值: [15]

- 设备可管理的用户数量

指定可在“非法访问的安全设置”下管理的用户帐户数量。

使用数字键指定“50”和“200”之间的值，然后按[#]。

默认值: [200]

- 设备可输入密码条目数量

指定可在“非法访问的安全设置”下管理的密码数量。

使用数字键指定“50”和“200”之间的值，然后按[#]。

默认值: [200]

- 状态监控间隔

指定“设备可管理的用户数量”和“设备可输入密码条目数量”的监控间隔。

使用数字键指定“1”和“10”之间的值，然后按[#]。

默认值: [3]

- 关

默认设置: [关]

非法访问设备

机器管理员可以指定此设置。

如果登录请求次数超过设置的指定值，则系统会将访问归类为非法访问。该访问会记录在访问日志中，并且系统会通过电子邮件将日志数据发送给机器管理员。此外，控制面板和 Web Image Monitor 上将显示一条消息。

如果“允许最多访问次数”设置为[0]，则不会检测非法访问。

在“验证延迟时间”中，您可以指定登录请求的响应延迟时间，以防止系统在检测到非法访问时停止响应。

在“设备可同时接受的访问数量”中，您可以指定同时访问机器的最大主机数量。如果同时访问数量超过设置指定的数字，则不会进行监控，且机器的监控状态会记录在日志中。

- 允许最多访问次数

指定允许访问尝试的最大次数。

使用数字键指定“0”和“500”之间的值，然后按[#]。

默认值: [100]

- 监测时间

指定超过最大访问数量之间的间隔。超过监测时间后，将删除超过最大访问数量的记录。

使用数字键指定“10”和“30”之间的值，然后按[#]。

默认值: [10]

- 验证延迟时间

指定检测到非法访问的验证延迟时间。

使用数字键指定“0”和“9”之间的值，然后按[#]。

默认值: [3]

- 设备可同时接受的访问数量

指定当由于非法访问导致验证延迟时，可接受的验证尝试次数。

使用数字键指定“50”和“200”之间的值，然后按[#]。

默认值: [200]

↓ 注

- 根据[允许最多访问次数]和[监测时间]设置的指定值，您可能会频繁收到非法访问检测电子邮件。
- 如果您频繁收到非法访问检测电子邮件，请检查内容并复查设置值。

其他安全功能

本节介绍防止信息泄露的设置。

它还介绍了启用用户验证时受到限制的功能。

扫描仪功能

打印和删除扫描仪日志

如果启用了用户验证，则“打印和删除扫描仪日志”将自动设置为[勿打印：不能发送]，以防止自动打印传送/传输历史记录中的个人信息。在这种情况下，在日志历史记录超过 250 次传送或传输时，会自动禁用扫描仪。发生这种情况时，请选择[打印扫描仪日志]或[删除扫描仪日志]。要自动打印扫描仪日志，请将“打印和删除扫描仪日志”设置为[打印并删除全部]。

有关详细信息，请参见《扫描》中的“扫描仪特性”。

WSD 扫描仪功能

指定用户验证后，会自动禁用 WSD 扫描仪功能。即使已自动禁用，您也可以从 Web Image Monitor 中可用的“初始的设置”启用此功能。

有关详细信息，请参见《扫描》中的“准备使用 WSD 扫描仪（推式）”和“准备使用 WSD 扫描仪（拉式）”。

7

系统状态

按控制面板上的[检查状态]键可以检查机器的当前状态和设置。如果指定了管理员验证，则只有在您以管理员身份登录到机器时，[维修/查询/机器信息]中才会显示[机器地址信息]。

检查固件有效性

机器启动时，系统将使用该功能检查固件是否有效。

执行验证过程中发生错误时，控制面板上会显示验证错误。

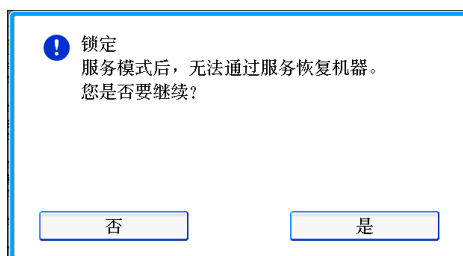
请注意，机器启动以后，您还可以在 Web Image Monitor 中检查固件有效性。如果 Web Image Monitor 的验证过程中发生错误，则无法使用 Web Image Monitor。如果发生这种情况，请检查控制面板。

限制客户工程师操作

您可以限制客户工程师访问服务模式。

客户工程师使用服务模式进行检修。如果将“服务模式锁定”设置为[开]，则无法使用服务模式，除非机器管理员登录到机器并取消服务模式锁定，以允许客户工程师操作机器来进行检查和维修。这样可以确保机器的检修工作在机器管理员的监督下进行。

1. 以机器管理员身份从控制面板中登录。
2. 按[系统设置]。
3. 按[管理员工具]。
4. 按两次[▼向后]。
5. 按[服务模式锁定]。
6. 按[开]，然后按[确定]。
7. 按[是]。



8. 注销。

增强安全性的附加信息

本节介绍为增强机器安全性所配置的设置。

可使用控制面板配置的设置

使用控制面板配置下表中所显示的安全设置。

系统设置

选项卡	项目	设置
定时器设置	自动注销定时器	开：180 秒或更少。 请参见 p.55 “自动注销”。
管理员工具	用户验证管理	选择[基本验证]，然后将“打印机作业验证”设置为[全部]。 请参见 p.31 “基本验证”。
管理员工具	管理员验证管理→用户管理	选择[开]，然后在“可用设置”中选择[管理员工具]。 请参见 p.13 “配置管理员验证”。
管理员工具	管理员验证管理→机器管理	选择[开]，然后选择各个“可用设置”。 请参见 p.13 “配置管理员验证”。
管理员工具	管理员验证管理→网络管理	选择[开]，然后在“可用设置”中选择[接口设置]、[文件转送]和[管理员工具]。 请参见 p.13 “配置管理员验证”。
管理员工具	管理员验证管理→文件管理	选择[开]，然后在“可用设置”中选择[管理员工具]。 请参见 p.13 “配置管理员验证”。
管理员工具	安全扩展→SNMPv1,v2 设置	禁止 请参见 p.225 “指定扩展安全功能”。
管理员工具	安全扩展→驱动程序加密密钥：密钥强度	AES 请参见 p.225 “指定扩展安全功能”。
管理员工具	安全扩展→验证当前作业	访问权限 请参见 p.225 “指定扩展安全功能”。

选项卡	项目	设置
管理员工具	安全扩展→密码策略	“复杂性设置”：等级 1 或更高，“最小字符数”：8 或更大 请参见 p.225 “指定扩展安全功能”。
管理员工具	网络安全等级	2 级 要通过打印机驱动程序或 Web Image Monitor 获取机器状态，请在 Web Image Monitor 上启用“SNMP”。 请参见 p.103 “指定网络安全等级”。
管理员工具	服务模式锁定	开 请参见 p.232 “限制客户工程师操作”。
管理员工具	机器数据加密设置	选择[加密]，然后为“保留所有数据或仅文件系统数据（不进行格式化），或格式化所有数据。”选择[所有数据]。 如果已经选择了[加密]，则不需要进行其他加密设置。 请参见 p.79 “对机器上的数据进行加密”。

扫描仪特性

选项卡	项目	设置
初始设置	菜单保护	2 级 请参见 p.60 “指定菜单保护”。

注

- SNMP 设置可以在 Web Image Monitor 的[配置]下的[SNMP]中指定。

可使用 Web Image Monitor 配置的设置

使用 Web Image Monitor 配置下表中所示安全设置。

设备管理→配置

类别	项目	设置
设备设置→日志	收集作业日志	有效
设备设置→日志	收集访问日志	有效
安全→用户锁定策略	锁定	有效 有关详细信息，请参见 p.53 “用户锁定功能”。
安全→用户锁定策略	在锁定前尝试的次数	不少于 5 次。 有关详细信息，请参见 p.53 “用户锁定功能”。
安全→用户锁定策略	锁定解除定时器	设置为[有效]或[无效]。 设置为[有效]时，将锁定解除定时器设置为不少于 60 分钟。 有关详细信息，请参见 p.53 “用户锁定功能”。
安全→用户锁定策略	锁定用户的时间	将“锁定解除定时器”设置为[有效]时，请将其设置为 60 分钟或更长时间。 有关详细信息，请参见 p.53 “用户锁定功能”。
网络→SNMPv3	SNMPv3 功能	无效 要使用 SNMPv3 功能，请将“SNMPv3 功能”设置为[有效]，并将“允许 SNMPv3 通信”设置为[仅加密]。由于 SNMPv3 强制每个软件包验证，因此只要 SNMPv3 有效，登录日志就会被禁用。
安全→网络安全	FTP	无效 指定此设置之前，在控制面板上将“网络安全等级”设置为[2 级]。
安全	S/MIME	“加密算法”：AES-128 位、AES-256 位或 3DES-168 位 为使用 S/MIME，必须注册用户证书。

设备管理

类别	项目	设置
地址簿→详细输入→添加用户/更改→电子邮件	用户证书	为使用 S/MIME，必须注册用户证书。

注

- 管理员必须指明可为加密算法指定的强度等级。
- 有关指定加密算法和注册用户证书的详细信息，请参见 p.117 “配置 S/MIME”。

IPsec 可用/不可用时配置的设置

与启用 IPsec 的机器之间往来的所有通信都会进行加密。

如果网络支持 IPsec，我们建议将其启用。

IPsec 可用时配置的设置

如果 IPsec 可用，请配置下表中显示的设置以提高数据在网络上传输时的安全性。

控制面板设置

系统设置

选项卡	项目	设置
接口设置	IPsec	有效
接口设置	允许 SSL/TLS 通信	仅限密文

Web Image Monitor 设置

设备管理→配置

类别	项目	设置
安全→IPsec→加密密钥自动交换设置	编辑→安全等级	验证和高等级的加密

IPsec 不可用时配置的设置

如果 IPsec 不可用，请配置下表中显示的设置以提高数据在网络上传输时的安全性。

控制面板设置

系统设置

选项卡	项目	设置
接口设置	IPsec	无效
接口设置	允许 SSL/TLS 通信	仅限密文

注

- 您可以使用 Web Image Monitor 设置 “IPsec” 和 “允许 SSL/TLS 通信” 。

IPsec 不可用时保护数据

IPsec 不可用时，以下步骤可增强用户数据安全性。

管理员必须指导用户执行这些步骤。

打印

- 使用支持加密的协议进行打印：
要使用打印机功能，请将协议指定为 sftp，或者指定 IPP 并启用 SSL/TLS。
有关 IPP 设置的详细信息，请参见《打印机驱动安装指南》中的“为选定的端口安装打印机驱动程序”。
- 有关 SSL/TLS 设置的详细信息，请参见 p.112 “配置 SSL/TLS 设置”。

扫描

- 发送保存文件的 URL 地址
通过在[扫描仪特性]中配置[发送设置]将所扫描文件的 URL 发送到目的地，而不是发送实际的扫描文件。有关详细信息，请参见《扫描》中的“通过电子邮件发送 URL”。
- 使用 Web Image Monitor 管理扫描的文件
使用 Web Image Monitor 通过网络查看、删除、发送及下载所扫描的文件。
- S/MIME 验证功能
当发送附加到电子邮件的扫描文件时，通过应用 S/MIME 证书来保护这些文件。为此，请在发送文件之前配置“安全”设置。有关从扫描仪发送电子邮件的详细信息，请参见《扫描》中的“电子邮件的安全设置”。

注

- 有关使用控制面板启用和禁用 IPsec 的详细信息，请参见《连接机器/系统设置》中的“接口设置”。
- 有关通过 Web Image Monitor 指定 IPsec 设置的详细信息，请参见 p.123 “配置 IPsec 设置”。

8. 故障排除

本章说明机器不能正常工作时应采取的措施。

如果显示信息

本节说明在用户验证期间屏幕上出现信息时应如何处理相关故障。

如果屏幕上出现下面没有显示的消息，请按照该消息的提示来解决问题。

“您没有使用此功能的权限。”

未指定使用该功能的权限。

如果使用功能时出现此消息：

- 未在通讯簿管理设置中指定该功能。
- 用户管理员必须决定是否要额外分配使用该功能的权限。

如果指定机器设置时出现此消息：

- 用户想要指定的机器设置不同，管理员也会不同。
- 使用设置列表，负责管理用户想要指定的机器设置的管理员必须决定是否额外分配使用该功能的权限。

“验证已失败。”

验证失败的原因各有不同，具体以错误代码来指示。

有关详细信息，请参见 p.240 “如果显示错误代码”。

“用户管理的管理员验证必须设置为开才能进行此项选择。”

在[管理员验证管理]中尚未启用用户管理员权限。

- 要指定基本验证、Windows 验证或 LDAP 验证，您必须首先在[管理员验证管理]中启用用户管理员权限。

有关详细信息，请参见 p.13 “配置管理员验证”。

“所选文件中包含没有访问权限的文件。将删除只有访问权限的文件。”

您曾尝试在没有相应权限的情况下删除文件。

- 所有者或文件管理员可以删除文件。要删除您没有权限删除的文件，请与所有者或文件管理员联系。

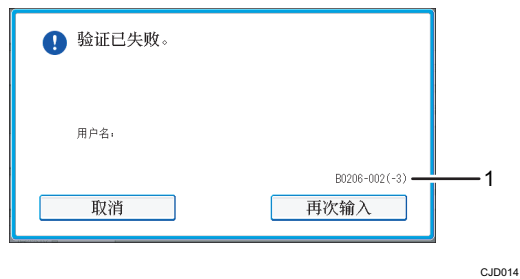
↓ 注

- 如果出现服务呼叫信息，请联系服务代理商。

如果显示错误代码

如果验证失败，则将出现带有错误代码的信息“验证已失败。”。下表为每个错误代码提供了解决方案。如果错误代码不在此表中，请记住该错误代码并联系您的服务代表。

错误代码显示位置



1. 错误代码

出现错误代码。

基本验证

B0103-000

在验证过程中发生 TWAIN 操作。

- 确保没有其他用户登录到机器，然后重试。

B0104-000

解密密码失败。

- 出现密码错误。
确保正确输入密码。
- 为“Driver Encryption Key: Encryption Strength”选择了[DES]或[AES]。
您可以通过指定驱动程序加密密钥进行访问。
- 出现驱动程序加密密钥错误。
确保在驱动程序中正确指定了加密密钥。

B0206-002: 情况 1

出现登录用户名或密码错误。

- 确保正确输入了登录用户名和密码，然后登录。

B0206-002: 情况 2

用户尝试通过“系统设置”屏幕上的应用程序进行验证，然而只有管理员具有验证权限。

- 在此屏幕上只有管理员具有登录权限。
- 通过应用程序的登录屏幕以一般用户身份登录。

B0206-003

出现验证错误，因为用户名包含空格、冒号（:）或引号（"）。

- 如果帐户名称包含以上任何禁止的字符，则请重新创建帐户。
- 如果未正确输入帐户名称，请正确输入并再次登录。

B0207-001

出现验证错误，因为通讯簿正在另一位置被使用。

- 稍等几分钟，然后重试。

B0208-000/B0208-002

由于已达到允许的最大验证尝试次数，帐户被锁定。

- 请求用户管理员解除帐户的锁定。

Windows 验证

W0103-000

在验证过程中发生 TWAIN 操作。

- 确保没有其他用户登录到机器，然后重试。

W0104-000

加密密码失败。

- 出现密码错误。
确保正确输入密码。
- 为“Driver Encryption Key: Encryption Strength”选择了[DES]或[AES]。
您可以通过指定驱动程序加密密钥进行访问。
- 出现驱动程序加密密钥错误。
确保在驱动程序中正确指定了加密密钥。

W0206-002

用户尝试通过“系统设置”屏幕上的应用程序进行验证，然而只有管理员具有验证权限。

- 在此屏幕上只有管理员具有登录权限。
- 通过应用程序的登录屏幕以一般用户身份登录。

W0206-003

出现验证错误，因为用户名包含空格、冒号（:）或引号（"）。

- 如果帐户名称包含以上任何禁止的字符，则请重新创建帐户。
- 如果未正确输入帐户名称，请正确输入并再次登录。

W0207-001

出现验证错误，因为通讯簿正在另一位置被使用。

- 稍等几分钟，然后重试。

W0208-000/W0208-002

由于已达到允许的最大验证尝试次数，帐户被锁定。

- 请求用户管理员解除帐户的锁定。

W0400-102

Kerberos 验证失败的原因是因为服务器运行不正常。

- 确保服务器工作正常。

W0400-200

由于验证尝试的数量很高，所有资源都很繁忙。

- 稍等几分钟，然后重试。

W0400-202: 情况 1

验证服务器上的 SSL 设置和机器不匹配。

- 确保验证服务器上的 SSL 设置和机器匹配。

W0400-202: 情况 2

用户在用户名中输入 sAMAccountName 以登录。

- 如果用户输入 sAMAccountName 作为登录用户名，ldap_bind 将在父/子域环境中失败。改用 UserPrincipalName 作为登录名。

W0406-003

出现验证错误，因为用户名包含空格、冒号 (:) 或引号 (")。

- 如果帐户名称包含以上任何禁止的字符，则请重新创建帐户。
- 如果未正确输入帐户名称，请正确输入并再次登录。

W0406-101

无法完成验证，因为验证尝试数量很高。

- 稍等几分钟，然后重试。
- 如果这种情况没有改善，请确保没有出现验证攻击。
- 通过电子邮件向管理员通知屏幕信息，然后检查系统日志是否存在验证攻击可能。

W0406-107: 情况 1

UserPrincipalName (用户@域名.xxx.com) 格式正被用于登录用户名。

- 如果使用 UserPrincipalName (user@domainname.xxx.com)形式, 则无法获取用户组。
- 使用 “sAMAccountName(user)” 登录, 因为此帐户可让您获取用户组。

W0406-107: 情况 2

当前设置不允许进行组检索。

- 在组属性中, 确保用户组的组范围设置为 “全局组”, 组类型设置为 “安全”。
- 确保帐户已添加到用户组。
- 确保机器上注册的用户组名称和 DC (域控制器) 上的组名称完全相同。DC 区分大小写。
- 在机器上注册用户帐户的 “验证信息” 中, 确保已指定 “在登录时使用验证信息”。
- 如果有多个 DC, 请确保各个 DC 之间已配置机密关系。

W0406-107: 情况 3

域名无法解析。

- 请确保在 “接口设置” 的域名中指定了 DNS/WINS。

W0406-107: 情况 4

无法连接到验证服务器。

- 确保可以连接到验证服务器。
- 在 “接口设置” 使用 “Ping 命令” 来检查连接情况。

W0406-107: 情况 5

出现登录用户名或密码错误。

- 确保用户已在服务器上注册。
- 使用注册的登录用户名和密码。

W0406-107: 情况 6

出现域名错误。

- 确保正确指定 Windows 验证域名。

W0406-107: 情况 7

无法解析域名。

- 在域名中指定 IP 地址并确认证验成功。

如果验证成功:

- 如果在域名中指定了顶级域名 (如域名.xxx.com), 请确保在 “接口设置” 中指定了 DNS。

- 如果在域名中指定了 NetBIOS 域名（如 DOMAINNAME），请确保在“接口设置”中指定 WINS。

如果验证不成功：

- 确保“域控制器安全策略”或“域安全策略”中未设置“限制 LM/NTLM”。
- 确保域控制防火墙端口以及设备与域控制连接路径之间的防火墙端口均处于打开状态。
- 如果激活了 Windows 防火墙，则会在 Windows 防火墙的“高级设置”中创建防火墙规则来授权端口 137 和 139。
- 在“网络连接”的属性窗口中，打开 TCP/IP 属性。然后单击详细信息设置、WINS，然后选中“启用 TCP/IP 上的 NetBIOS”框并将数字 137 设置为“打开”。

W0406-107: 情况 8

Kerberos 验证失败。

- 未正确配置 Kerberos 验证设置。
确保正确指定了领域名、KDC（密钥分发中心）名称和相应的域名。
- KDC 和机器定时不匹配。
如果 KDC 和机器定时之间的差值超过 5 分钟，则验证将失败。确保定时匹配。
- 如果使用小写字母指定领域名，则 Kerberos 验证将失败。确保以大写指定领域名。
- 如果对 KDC 的自动检索失败，则 Kerberos 验证将失败。
询问服务代表，确保 KDC 检索设置为“自动检索”。
如果自动检索工作不正常，请切换为手动检索。

W0409-000

验证超时，因为服务器未响应。

- 检查网络配置或验证服务器上的设置。

W0511-000/W0517-000

验证服务器登录用户名与已在机器中注册的用户名相同。（通过在 LDAP 验证设置中指定的唯一属性识别这些名称。）

- 删除旧的重复名称或更改登录名。
- 如果刚更改了验证服务器，删除服务器上的旧名称。

W0606-004

验证失败，因为用户名包含一般用户无法使用的字词。

- 请勿在一般用户帐户中使用“other”、“admin”、“supervisor”或“HIDE*”。

W0607-001

出现验证错误，因为通讯簿正在另一位置被使用。

- 稍等几分钟，然后重试。

W0612-005

验证失败，因为不能注册更多的用户。（在通讯簿中注册的用户数量已达到了最大数。）

- 请求用户管理员删除通讯簿中未使用的用户帐户。

W0707-001

出现验证错误，因为通讯簿正在另一位置被使用。

- 稍等几分钟，然后重试。

W09XX-019

验证使用通讯簿集中管理功能从客户端访问时无法在服务器上进行自动用户注册。

- 请检查客户端与服务器之间的网络连接。
- 在服务器上编辑通讯簿时无法注册用户。

LDAP 验证

L0103-000

在验证过程中发生 TWAIN 操作。

- 确保没有其他用户登录到机器，然后重试。

L0104-000

加密密码失败。

- 出现密码错误。
确保正确输入密码。
- 为“Driver Encryption Key: Encryption Strength”选择了[DES]或[AES]。
您可以通过指定驱动程序加密密钥进行访问。
- 出现驱动程序加密密钥错误。
确保在驱动程序中正确指定了加密密钥。

L0206-002

用户尝试通过“系统设置”屏幕上的应用程序进行验证，而只有管理员具有验证权限。

- 在此屏幕上只有管理员具有登录权限。
- 通过应用程序的登录屏幕以一般用户身份登录。

L0206-003

出现验证错误，因为用户名包含空格、冒号（:）或引号（"）。

- 如果帐户名称包含以上任何禁止的字符，则请重新创建帐户。
- 如果未正确输入帐户名称，请正确输入并再次登录。

L0207-001

出现验证错误，因为通讯簿正在另一位置被使用。

- 稍等几分钟，然后重试。

L0208-000/L0208-002

由于已达到允许的最大验证尝试次数，帐户被锁定。

- 请求用户管理员解除帐户的锁定。

L0307-001

出现验证错误，因为通讯簿正在另一位置被使用。

- 稍等几分钟，然后重试。

L0400-210

无法在 LDAP 搜索中获取用户信息。

- 可能无法指定登录属性的搜索条件或无法获取指定的搜索信息。
- 确保已正确指定登录名属性。

L0406-003

出现验证错误，因为用户名包含空格、冒号（:）或引号（"）。

- 如果帐户名称包含以上任何禁止的字符，则请重新创建帐户。
- 如果未正确输入帐户名称，请正确输入并再次登录。

L0406-200

无法完成验证，因为验证尝试数量很高。

- 稍等几分钟，然后重试。
- 如果这种情况没有改善，请确保没有出现验证攻击。
- 通过电子邮件向管理员通知屏幕信息，然后检查系统日志是否存在验证攻击可能。

L0406-201

在 LDAP 服务器设置中禁用验证。

- 在“系统设置”中，更改管理员工具中的 LDAP 服务器设置。

L0406-202/L0406-203: 情况 1

在 LDAP 验证设置、LDAP 服务器或网络配置中存在错误。

- 确保使用当前 LDAP 服务器配置的连接测试成功。
如果连接失败，则可能网络设置发生了错误。
检查“接口设置”中的域名或 DNS 设置。
- 确保在 LDAP 验证设置中正确指定了 LDAP 服务器。
- 确保在 LDAP 验证设置中正确输入了登录名属性。
- 确保 LDAP 服务器支持 SSL 设置。

L0406-202/L0406-203: 情况 2

出现登录用户名或密码错误。

- 确保正确输入了登录用户名和密码。
- 确保机器上已注册可用的登录名。

在以下情况下，验证将失败：

如果登录用户名包含空格、冒号 (:) 或引号 (")。

如果登录用户名超过 128 个字节。

L0406-202/L0406-203: 情况 3

简单加密方法中存在错误。

- 如果在简单验证模式下将密码留空，则验证将失败。
要允许使用空密码，请联系您的服务代理商。
- 在简单验证模式下，在用户帐户中获取登录用户名的 DN。
如果无法获取 DN，则验证失败。

确保在服务器名、登录用户名、密码或为搜索过滤器输入的信息中没有错误。

L0406-204

Kerberos 验证失败。

- 未正确配置 Kerberos 验证设置。
确保已正确指定领域名、KDC（密钥分发中心）名称和支持域名。
- KDC 和机器定时不匹配。
如果 KDC 和机器定时之间的差值超过 5 分钟，则验证将失败。确保定时匹配。
- 如果使用小写字母指定领域名，则 Kerberos 验证将失败。确保以大写字母指定领域名。

L0409-000

验证超时，因为服务器未响应。

- 联系服务器或网络管理员。
- 如果情况没有改善，请与服务代表联系。

L0511-000

验证服务器登录用户名与已在机器中注册的用户名相同。（通过在 LDAP 验证设置中指定的唯一属性识别这些名称。）

- 删除旧的重复名称或更改登录名。
- 如果刚更改了验证服务器，删除服务器上的旧名称。

L0606-004

验证失败，因为用户名包含一般用户无法使用的字词。

- 请勿在一般用户帐户中使用“other”、“admin”、“supervisor”或“HIDE*”。

L0607-001

出现验证错误，因为通讯簿正在另一位置被使用。

- 稍等几分钟，然后重试。

L0612-005

验证失败，因为不能注册更多的用户。（在通讯簿中注册的用户数量已达到了最大数。）

- 请求用户管理员删除通讯簿中未使用的用户帐户。

L0707-001

出现验证错误，因为通讯簿正在另一位置被使用。

- 稍等几分钟，然后重试。

L09XX-019

验证使用通讯簿集中管理功能从客户端访问时无法在服务器上进行自动用户注册。

- 请检查客户端与服务器之间的网络连接。
- 在服务器上编辑通讯簿时无法注册用户。

如果无法操作机器

如果用户操作机器时出现以下情况，提供如何处理这些情况的说明。

问题	原因	解决方法
不能执行以下操作： - 使用打印机驱动程序进行打印 - 与 TWAIN 驱动程序连接	用户验证被拒绝。	如果使用 Windows 验证或 LDAP 验证，请通过在用网络的管理员确认用户名和登录名。 如果使用基本验证，请通过用户管理员进行确认。
不能执行以下操作： - 使用打印机驱动程序进行打印 - 与 TWAIN 驱动程序连接	在驱动程序中指定的加密密钥与机器的驱动程序加密密钥不匹配。	指定在机器中注册的驱动程序加密密钥。 有关详细信息，请参见 p.144 “指定驱动程序加密密钥”。
无法与 TWAIN 驱动程序连接。	SNMPv3 帐户、密码以及加密算法与本机指定的设置不匹配。	使用网络连接工具指定在机器中注册的 SNMPv3 的帐户、密码以及加密算法。
无法使用 TWAIN 驱动程序执行验证。	另一个用户已登录此机器。	请等待该用户注销。
无法使用 TWAIN 驱动程序执行验证。	由于操作条件，验证操作很耗时。	确保 LDAP 服务器设置正确。 确保网络设置正确。
无法使用 TWAIN 驱动程序执行验证。	当机器编辑通讯簿数据时，无法进行验证。	请稍等，直到通讯簿数据的编辑操作完成。
在 Device Manager NX 中启动“地址簿”并输入正确的登录用户名和密码后，出现了一则指明已输入错误密码的信息。	没有正确设置“驱动程序加密密钥：密钥强度”。或者，尽管在计算机中未安装所需的证书，但是启用了“SSL/TLS”。	将“驱动程序加密密钥：密钥强度”设置为[简单加密]。或者，启用“SSL/TLS”，在机器中安装服务器证书，然后在计算机中安装证书。 有关详细信息，请参见 p.225 “指定扩展安全功能”和 p.112 “配置 SSL/TLS 设置”。

问题	原因	解决方法
使用复印或扫描仪功能时无法注销。	原稿扫描未完成。	完成原稿扫描后，按[#]，取出原稿，然后注销。
“编入地址”未出现在用于指定目的地的扫描仪屏幕上。	“限制添加用户目的地”在“安全扩展”下设置为[开]，因此只有用户管理员才能在扫描仪屏幕上的通讯簿中注册目的地。	必须由用户管理员来执行注册。
无法从扫描仪发送电子邮件。 同样地： - 无法选择地址。 - 无法指定签名。 - 无法在介质中保存数据。	以下是可能的原因： - 用户证书（目的地证书）的有效期已过期。 - 设备证书(S/MIME)的有效期已过期。 - 设备证书(S/MIME)不存在或无效。 - 设备证书（带有数字签名的 PDF 或者带有数字签名的 PDF/A）的有效期已过期。 - 设备证书（带有数字签名的 PDF 或者带有数字签名的 PDF/A）不存在或无效。 - 管理员的电子邮件地址不正确。	- 请安装用户证书（目的地证书）。 您可以从 Web Image Monitor 通讯簿安装用户证书（目的地证书）。您必须事先准备用户证书（目的地证书）本身。 - 请为 S/MIME 安装设备证书。 - 为带有数字签名的 PDF 或者带有数字签名的 PDF/A 安装设备证书。 有关详细信息，请参见 p.108 “通过设备证书保护通信路径”。 - 指定管理员的电子邮件地址。 有关详细信息，请参见“连接机器/系统设置”中的“文件转送”。
禁用了用户验证，但未显示保存的文件。	禁用用户验证时，可能未针对用户访问保存的文件选择“所有用户”。	重新启用用户验证，然后选择[所有用户]作为所要显示文件的访问权限设置。 有关详细信息，请参见 p.153 “管理保存的文件”和 Web Image Monitor 帮助。

问题	原因	解决方法
禁用了用户验证，但未显示使用机器指定的目的地。	用户验证被禁用，可能是"保护目的地"没有选择"所有用户"。	重新启用用户验证，然后选择[所有用户]作为所要显示的目的地访问权限设置。 有关详细信息，请参见 p.75 “保护通讯簿”。
无法在启用了用户验证的情况下打印。	可能未在打印机驱动程序中指定用户验证。	在打印机驱动程序中指定用户验证。有关详细信息，请参见打印机驱动程序帮助。
在“达到限制时的机器操作”中选择了[结束作业并限制]，但当前作业却在完成之前被取消了。	根据正在使用的应用程序，机器可能将一份作业识别为多份，导致该作业在完成之前被取消。	通过清除打印容量使用计数器为用户重置打印容量使用设置，然后再次执行打印。 有关详细信息，请参见 p.72 “重置打印容量使用计数器”。
如果您在复印或扫描时尝试中断作业，将出现验证屏幕。	对于本机，您可以在复印或扫描时注销。如果您在注销后尝试中断复印或扫描，将出现验证屏幕。	只有执行复印或扫描作业的用户才能中断作业。 等待作业完成，或咨询执行作业的用户。 机器管理员可以删除作业。
执行“加密用户自定义设置和通讯簿”之后，等了很长时间，并没有出现“退出”消息。	验证可能需要较长时间，因为地址簿中注册了大量条目。另外，某个文件可能已损坏或硬盘可能出现故障。	如果根据 p.79 “对机器上的数据进行加密”指定的“仅文件系统数据”时间过去后仍未更新屏幕，请与服务代表联系。

9. 设置的操作权限列表

本章提供了管理员验证或用户验证启用时机器设置的管理员和用户操作权限列表。

如何读取

了解标题

- 用户
用户管理员具有执行此操作的权限。
- 机器
机器管理员具有执行此操作的权限。
- 网络
网络管理员具有执行此操作的权限。
- 文件
文件管理员具有执行此操作的权限。
- 未设置
登录的用户具有执行此操作的权限。
适用于没有在[管理员验证管理]的“可用设置”中选择任何设置的情况。
- 设置
登录的用户具有执行此操作的权限。
在[管理员验证管理]的“可用设置”中选择了设置时的状态。
- 1 级
适用于[菜单保护]设置设定为[1 级]的情况。
- 2 级
适用于[菜单保护]设置设定为[2 级]的情况。

了解符号

- R/W: 可以执行、更改和读取。
R: 可以读取。
-: 无法执行、更改和读取。

系统设置

如果指定了管理员验证，则根据“可用设置”中的配置，用户操作限制会有所不同。

[常规设置]

设置	用户	机器	网络	文件	未设置	设置
[编入／更改／删除用户文字]	R	R/W	R	R	R/W	R
[面板按键音]	R	R/W	R	R	R/W	R
[预热蜂鸣器]	R	R/W	R	R	R/W	R
[复印计数显示]	R	R/W	R	R	R/W	R
[功能优先顺序]	R	R/W	R	R	R/W	R
[功能键分配]	R	R/W	R	R	R/W	R
[打印优先顺序]	R	R/W	R	R	R/W	R
[功能重置定时器]	R	R/W	R	R	R/W	R
[打印作业时间间隔]	R	R/W	R	R	R/W	R
[屏幕颜色设置]	R	R/W	R	R	R/W	R
[输出：复印机]	R	R/W	R	R	R/W	R
[输出：文件服务器]	R	R/W	R	R	R/W	R
[输出：打印机]	R	R/W	R	R	R/W	R
[输出纸盘设置]	R	R/W	R	R	R/W	R
[纸盘优先顺序：复印机]	R	R/W	R	R	R/W	R
[纸盘优先顺序：打印机]	R	R/W	R	R	R/W	R
[按键重复]	R	R/W	R	R	R/W	R
[ADF 原稿台提升]	R	R/W	R	R	R/W	R
[系统状态／作业列表显示时间]	R	R/W	R	R	R/W	R
[交替打印]	R	R/W	R	R	R/W	R
[状态指示灯]	R	R/W	R	R	R/W	R

设置	用户	机器	网络	文件	未设置	设置
[Z 形折叠位置]	R	R/W	R	R	R/W	R
[对折位置]	R	R/W	R	R	R/W	R
[信纸向外折叠位置]	R	R/W	R	R	R/W	R
[信纸向内折叠位置]	R	R/W	R	R	R/W	R
[双联折叠位置]	R	R/W	R	R	R/W	R
[门式折叠位置]	R	R/W	R	R	R/W	R
[外部键盘]	R	R/W	R	R	R/W	R
[编入/更改 USB 设备列表]	R	R/W	R	R	R/W	R
[兼容 ID]	R	R/W	R	R	R/W	R

[定时器设置]

设置	用户	机器	网络	文件	未设置	设置
[睡眠模式定时器]	R	R/W	R	R	R/W	R
[低功率模式定时器]	R	R/W	R	R	R/W	R
[系统自动重置定时器]	R	R/W	R	R	R/W	R
[复印/文件服务器自动重置定时器]	R	R/W	R	R	R/W	R
[打印机自动重置定时器]	R	R/W	R	R	R/W	R
[扫描仪自动重置定时器]	R	R/W	R	R	R/W	R
[设置日期]	R	R/W	R	R	R/W	R
[设定时间]	R	R/W	R	R	R/W	R
[自动注销定时器]	R	R/W	R	R	R/W	R
[定影单元关闭模式（节能）开/关]	R	R/W	R	R	R/W	R
[周定时器]	R	R/W	R	R	R/W	R

[接口设置]

[网络]

设置	用户	机器	网络	文件	未设置	设置
[机器 IPv4 地址]* ¹	R	R	R/W	R	R/W	R
[IPv4 网关地址]	R	R	R/W	R	R/W	R
[机器 IPv6 地址]	R	R	R	R	R	R
[IPv6 网关地址]	R	R	R	R	R	R
[IPv6 无状态地址自动配置]	R	R	R/W	R	R/W	R
[DHCPv6 配置]	R	R	R/W	R	R/W	R
[DNS 配置]* ²	R	R	R/W	R	R/W	R
[DDNS 配置]	R	R	R/W	R	R/W	R
[Ipsec]	R	R	R/W	R	R/W	R
[域名]* ¹	R	R	R/W	R	R/W	R
[WINS 配置]	R	R	R/W	R	R/W	R
[有效协议]	R	R	R/W	R	R/W	R
[NCP 传送协议]	R	R	R/W	R	R/W	R
[NW 帧类型]	R	R	R/W	R	R/W	R
[SMB 计算机名]	R	R	R/W	R	R/W	R
[SMB 工作组]	R	R	R/W	R	R/W	R
[以太网速度]	R	R	R/W	R	R/W	R
[Ping 命令]	-	-	R/W	-	R/W	R
[允许 SNMPv3 通信]	R	R	R/W	R	R/W	R
[允许 SSL/TLS 通信]	R	R	R/W	R	R/W	R
[主机名]	R	R	R/W	R	R/W	R
[机器名]	R	R	R/W	R	R/W	R

设置	用户	机器	网络	文件	未设置	设置
[以太网 IEEE 802.1X 验证]	R	R	R/W	R	R/W	R
[将 IEEE 802.1X 验证恢复到默认值]	-	-	R/W	-	R/W	-

*1 如果设置了自动获取，则数据为只读数据。

*2 所有管理员和用户都可以运行连接测试。

[打印列表]

设置	用户	机器	网络	文件	未设置	设置
[打印列表]	-	-	R/W	-	R/W	-

[文件转送]

设置	用户	机器	网络	文件	未设置	设置
[SMTP 服务器]	R	R	R/W	R	R/W	R
[SMTP 验证]* ³	R	R/W	R	R	R/W	R
[SMTP 之前的 POP]	R	R/W	R	R	R/W	R
[接收协议]	R	R/W	R	R	R/W	R
[POP3/IMAP4 设置]	R	R/W	R	R	R/W	R
[管理员的电子邮件地址]	R	R/W	R	R	R/W	R
[电子邮件通讯端口]	R	R	R/W	R	R/W	R
[电子邮件接收间隔]	R	R	R/W	R	R/W	R
[可接收的最大电子邮件尺寸]	R	R	R/W	R	R/W	R
[在服务器上存储电子邮件]	R	R	R/W	R	R/W	R
[默认用户名/密码（发送）]* ³	R	R/W	R	R	R/W	R
[编入/更改/删除电子邮件消息]	R	R/W	R	R	R/W	R/W
[自动指定发送者名称]	R	R	R/W	R	R/W	R

设置	用户	机器	网络	文件	未设置	设置
[扫描仪再发送时间间隔]	R	R	R/W	R	R/W	R
[扫描仪再发送的次数]	R	R	R/W	R	R/W	R

*3 无法读取密码。

[管理员工具]

设置	用户	机器	网络	文件	未设置	设置
[通讯簿管理]	R/W	R/W *4	R/W *4	R/W *4	R/ W*5	R*5
[通讯簿：编入／更改／删除组]	R/W	R/W *4	R/W *4	R/W *4	R/ W*5	R*5
[通讯簿：更改顺序]	R/W	-	-	-	R/W	-
[打印通讯簿：目的地列表]	R/W	-	-	-	R/W	R/W
[通讯簿：编辑标题]	R/W	-	-	-	R/W	-
[通讯簿：切换标题]	R/W	-	-	-	R/W	R
[备份／恢复：用户自定义设置和通讯簿]	R/W	-	-	-	R/W	-
[地址簿自动编入的数据保留设置]	R/W	R	R	R	R/W	R
[自动删除通讯簿中的用户]	R/W	-	-	-	R/W	-
[删除通讯簿中的所有数据]	R/W	-	-	-	R/W	-
[显示／打印计数器]	R	R/W	R	R	R/W	R/W
[显示／清除／打印每个用户的计数器]	R/ W*6	R/ W*7	R	R	R/W	-
[显示／清除环保计数器]	-	R/W	-	-	-	-
[每个用户显示／清除环保计数器]	-	R/W	-	-	-	-
[环保计数器期间／管理员信息]	R	R/W	R	R	R	R
[达到限制时的机器操作]	R	R/W	R	R	R	R

设置	用户	机器	网络	文件	未设置	设置
[打印容量使用限制：单组计数设置]	R	R/W	R	R	R	R
[扩充打印容量使用限制]	R	R/W	R	R	R	R
[打印容量使用限制：默认限制值]	R/W	R	R	R	R	R
[介质插槽使用]	R	R/W	R	R	R	R
[用户验证管理]	R	R/W	R	R	R/W	R
[增强的用户验证管理]	R	R/W	R	R	R/W	R
[管理员验证管理]	R/W *8 *9	R/W *9	R/W *9	R/W *9	R/W	-
[编入／更改管理员]	R/ W*10	R/ W*10	R/ W*10	R/ W*10	-	-
[钥匙计数器管理]	R	R/W	R	R	R/W	R
[外部收费单元管理]	R	R/W	R	R	R/W	R
[增强的外部收费单元管理]	R	R/W	R	R	R/W	R
[安全扩展]						
• [驱动程序加密密钥]	-	-	R/W	-	R/W	-
• [驱动程序加密密钥：密钥强度]	R	R	R/W	R	R/W	R
• [限制显示用户信息]	R	R/W	R	R	R/W	R
• [加密用户自定义设置和通讯簿]	R/W	R	R	R	R	R
• [增强文件保护]	R	R	R	R/W	R	R
• [限制目的地的使用]	R/W	R	R	R	R	R
• [限制添加用户目的地]	R/W	R	R	R	R	R
• [SNMPv1,v2 设置]	R	R	R/W	R	R/W	R
• [验证当前作业]	R	R/W	R	R	R/W	R
• [密码策略]	R/W	-	-	-	-	-
• [@Remote 服务]	R	R/W	R	R	R/W	R

设置	用户	机器	网络	文件	未设置	设置
• [更新固件]	R	R/W	R	R	-	-
• [更改固件结构]	R	R/W	R	R	-	-
• [密码输入非法]	-	R/W	-	-	-	-
• [非法访问的安全设置]	-	R/W	-	-	-	-
• [非法访问设备]	-	R/W	-	-	-	-
[自动删除文件服务器中的文件]	R	R	R	R/W	R/W	R
[删除文件服务器中的所有文件]	-	-	-	R/W	R/W	-
[编入/更改/删除 LDAP 服务器]* ³	-	R/W	-	-	R/W	R
[LDAP 搜索]	R	R/W	R	R	R/W	R
[通过睡眠模式定时器进入睡眠模式]	R	R/W	R	R	R/W	R
[服务测试通信]	-	R/W	-	-	R/W	-
[通知机器状态]	-	R/W	-	-	R/W	-
[服务模式锁定]	R	R/W	R	R	R/W	R
[固件版本]	R	R	R	R	R	R
[网络安全等级]	R	R	R/W	R	R	R
[自动清除内存设置]	R	R/W	R	R	R	R
[清除所有内存]	-	R/W	-	-	-	-
[删除所有日志]	-	R/W	-	-	R/W	-
[传送日志设置]* ¹¹	R	R/W	R	R	R/W	R
[防止未经授权复印的打印: 打印]	R	R/W	R	R	R/W	R
[编入/更改/删除领域]	-	R/W	-	-	R/W	R
[机器数据加密设置]	-	R/W	-	-	-	-
[编入/删除设备证书]	-	-	R/W	-	-	-

设置	用户	机器	网络	文件	未设置	设置
[设备设置信息：导入设置（服务器）]* ¹²	-	-	-	-	-	-
[设备设置信息：运行导入（服务器）]* ¹²	-	-	-	-	-	-
[设备设置信息：导出（内存存储设备）]* ¹²	-	-	-	-	-	-
[设备设置信息：导入（内存存储设备）]* ¹²	-	-	-	-	-	-
[PDF 文件类型：PDF/A 固定]	R	R/W	R	R	R/W	R
[按停止键暂停打印作业]	R	R/W	R	R	R/W	R
[节能键更改模式]	R	R/W	R	R	R/W	R
[强制安全印记：复印机]	R	R/W	R	R	R/W	R
[强制安全印记：文件服务器]	R	R/W	R	R	R/W	R
[强制安全印记：打印机]	R	R/W	R	R	R/W	R
[用户自己的自定义]	R	R/W	R	R	R/W	R
[容量使用计数器：定期/指定重置设置]	R	R/W	R	R	R	R
[选择可切换的语言]	-	R/W	-	-	R/W	-
[收集日志]	R	R/W	R	R	R/W	R
[通讯簿集中管理]						
• [通讯簿集中管理]	R	R/W	R	R	R	R
• [客户端同步]* ¹³	R/W	R/W	R	R	R	R
• [与服务器同步]* ¹⁴	R/W	R/W	R	R	R	R

*3 无法读取密码。

*4 只能更改标题和搜索用户。

*5 根据访问权限，可以执行、更改和读取的项目会有所不同。

*6 只能清除。

- *7 只能打印。
- *8 使用单个验证功能时，无法更改。
- *9 只能更改管理员权限设置。
- *10 管理员只能更改自己的帐户。
- *11 只能更改为[关]。
- *12 具有所有权限（包括用户管理员、机器管理员、网络管理员和文件管理员权限）的管理员可以执行 R/W。
- *13 将机器用作服务器时出现。
- *14 将机器用作客户端时出现。

纸盘纸张设置

本节列出了在控制面板上按[纸张设置]键时显示的设置。

如果设置了管理员验证，则根据“可用设置”中的配置，用户操作限制会有所不同。

[纸盘纸张设置]

设置	用户	机器	网络	文件	未设置	设置
[纸盘]	R	R/W	R	R	R/W	R
[封页/指定页/隔页/分隔页]	R	R/W	R	R	R/W	R
[编辑自定义纸张]	-	R/W	-	-	R/W	-

编辑主页

如果设置了管理员验证，则根据“可用设置”中的配置，用户操作限制会有所不同。

[编辑主页]

设置	用户	机器	网络	文件	未设置	设置
[移动图标]	R	R/W	R	R	R/W	R
[删除图标]	R	R/W	R	R	R/W	R
[添加图标]	-	R/W	-	-	R/W	-
[恢复默认设置图标显示]	-	R/W	-	-	R/W	-
[主页上插入图像]	-	R/W	-	-	R/W	-

为操作员调整设置

设置	用户	机器	网络	文件	未设置	设置
[为操作员调整设置]	R/W	R/W	R/W	R/W	R/W	R/W

为技术熟练的操作员调整设置

设置	用户	机器	网络	文件	未设置	设置
[为技术熟练的操作员调整设置]	-	R/W	-	-	-	-

复印机／文件服务器特性

如果设置了管理员验证，则根据“菜单保护”设置，用户操作限制会有所不同。

[常规设置]

设置	用户	机器	网络	文件	1 级	2 级
[自动图像浓度优先顺序]	R	R/W	R	R	R	R
[原稿类型优先顺序]	R	R/W	R	R	R	R
[原始照片类型优先级]	R	R/W	R	R	R	R
[在双面模式中的原稿方向]	R	R/W	R	R	R	R
[在双面模式中的复印件方向]	R	R/W	R	R	R	R
[保留作业模式]	R	R/W	R	R	R	R
[预约屏幕自动关闭定时器]	R	R/W	R	R	R	R
[最大复印数量]	R	R/W	R	R	R	R
[手动原稿计数器重设]	R	R/W	R	R	R	R
[自动纸盘切换]	R	R/W	R	R	R	R
[深色背景]	R	R/W	R	R	R	R
[面板特性默认值]	R	R/W	R	R	R	R
[图像调整优先]	R	R/W	R	R	R	R
[纸张显示]	R	R/W	R	R	R	R
[原稿类型显示]	R	R/W	R	R	R	R
[提示音：原稿遗留在曝光玻璃上]	R	R/W	R	R	R	R
[工作完毕提示音]	R	R/W	R	R	R	R
[切换原稿计数器显示]	R	R/W	R	R	R	R
[纸盘 A 的纸张设置画面]	R	R/W	R	R	R	R
[用户自定义功能：复印件]	R	R/W	R	R	R/W	R
[用户自定义功能：文件服务器存储]	R	R/W	R	R	R/W	R

[复印比例]

设置	用户	机器	网络	文件	1 级	2 级
[快捷缩小／放大]	R	R/W	R	R	R	R
[复印比例]	R	R/W	R	R	R	R
[缩小／放大比例优先]	R	R/W	R	R	R	R
[用于创建页边距的比例]	R	R/W	R	R	R	R

[编辑]

设置	用户	机器	网络	文件	1 级	2 级
[正面页边距：左／右]	R	R/W	R	R	R	R
[背面页边距：左／右]	R	R/W	R	R	R	R
[正面页边距：顶端／底端]	R	R/W	R	R	R	R
[背面页边距：顶端／底端]	R	R/W	R	R	R	R
[单面→双面自动页边距：顶端到顶端]	R	R/W	R	R	R	R
[单面→双面自动页边距：顶端到底端]	R	R/W	R	R	R	R
[杂志渐变设置]	R	R/W	R	R	R	R
[消除边框宽度]	R	R/W	R	R	R	R
[消除合并中的原稿阴影]	R	R/W	R	R	R/W	R
[消除中间宽度]	R	R/W	R	R	R	R
[合并中的封面复印件]	R	R/W	R	R	R/W	R
[合并中的复印顺序]	R	R/W	R	R	R/W	R
[方向：小册、杂志]	R	R/W	R	R	R/W	R
[图像重复分割线]	R	R/W	R	R	R/W	R
[双重复印分割线]	R	R/W	R	R	R/W	R
[合并中的分割线]	R	R/W	R	R	R/W	R
[在合并模式中指定页上复印]	R	R/W	R	R	R/W	R

设置	用户	机器	网络	文件	1 级	2 级
[复印封底]	R	R/W	R	R	R/W	R
[双重复印位置]	R	R/W	R	R	R/W	R

[印记]

[预设印记]

设置	用户	机器	网络	文件	1 级	2 级
[印记语言]	R	R/W	R	R	R/W	R
[印记优先顺序]	R	R/W	R	R	R	R
[印记格式]: 复印件	R	R/W	R	R	R/W * ₁	R
[印记格式]: 紧急	R	R/W	R	R	R/W * ₁	R
[印记格式]: 优先	R	R/W	R	R	R/W * ₁	R
[印记格式]: 仅供参考	R	R/W	R	R	R/W * ₁	R
[印记格式]: 暂定	R	R/W	R	R	R/W * ₁	R
[印记格式]: 仅供内部使用	R	R/W	R	R	R/W * ₁	R
[印记格式]: 机密	R	R/W	R	R	R/W * ₁	R
[印记格式]: 草稿	R	R/W	R	R	R/W * ₁	R
[印记颜色]: 复印	R	R/W	R	R	R	R
[印记颜色]: 紧急	R	R/W	R	R	R	R
[印记颜色]: 优先顺序	R	R/W	R	R	R	R
[印记颜色]: 仅供参考	R	R/W	R	R	R	R
[印记颜色]: 暂定	R	R/W	R	R	R	R

设置	用户	机器	网络	文件	1 级	2 级
[印记颜色]: 仅供内部使用	R	R/W	R	R	R	R
[印记颜色]: 机密	R	R/W	R	R	R	R
[印记颜色]: 草稿	R	R/W	R	R	R	R

*1 只能指定打印位置调整。无法配置打印位置本身。

[用户印记]

设置	用户	机器	网络	文件	1 级	2 级
[编入/删除印记]	R	R/W	R	R	R/W	R
[印记格式]: 1-5	R	R/W	R	R	R/W	R
[印记颜色]: 1-5	R	R/W	R	R	R/W	R

[日期印记]

设置	用户	机器	网络	文件	1 级	2 级
[格式]	R	R/W	R	R	R	R
[字体]	R	R/W	R	R	R/W	R
[尺寸]	R	R/W	R	R	R/W	R
[重叠]	R	R/W	R	R	R/W	R
[印记颜色]	R	R/W	R	R	R	R
[印记设置]	R	R/W	R	R	R/W*2	R

*2 只能设置打印位置调整。无法配置打印位置本身。

[页码编号]

设置	用户	机器	网络	文件	1 级	2 级
[印记格式]	R	R/W	R	R	R	R
[字体]	R	R/W	R	R	R/W	R
[尺寸]	R	R/W	R	R	R/W	R
[双面打印背面印记位置]	R	R/W	R	R	R/W	R

设置	用户	机器	网络	文件	1 级	2 级
[在合并中的页码编号]	R	R/W	R	R	R/W	R
[在指定隔页上加印记]	R	R/W	R	R	R/W	R
[印记位置: P1, P2...]	R	R/W	R	R	R/ W*3	R
[印记位置: 1/5, 2/5...]	R	R/W	R	R	R/ W*3	R
[印记位置: -1-, -2-...]	R	R/W	R	R	R/ W*3	R
[印记位置: P.1, P.2...]	R	R/W	R	R	R/ W*3	R
[印记位置: 1, 2...]	R	R/W	R	R	R/ W*3	R
[印记位置: 1-1, 1-2...]	R	R/W	R	R	R/ W*3	R
[重叠]	R	R/W	R	R	R/W	R
[印记颜色]	R	R/W	R	R	R	R
[页面编号首字母]	R	R/W	R	R	R	R

*3 只能设置打印位置调整。无法配置打印位置本身。

[印记文本]

设置	用户	机器	网络	文件	1 级	2 级
[字体]	R	R/W	R	R	R/W	R
[尺寸]	R	R/W	R	R	R/W	R
[重叠]	R	R/W	R	R	R/W	R
[印记颜色]	R	R/W	R	R	R	R
[印记设置]	R	R/W	R	R	R/W	R
[更改第一个作业的序列号]	R	R/W	R	R	R	R

[输入／输出]

设置	用户	机器	网络	文件	1 级	2 级
[SADF 自动重设]	R	R/W	R	R	R	R
[玻璃模式下以复印面方法输出]	R	R/W	R	R	R	R
[内存已满自动扫描重新开始]	R	R/W	R	R	R	R
[分页／分类移动纸盘设置]	R	R/W	R	R	R	R
[插入分隔页]	R	R/W	R	R	R	R
[信头设置]	R	R/W	R	R	R	R
[前缘裁剪设置]	R	R/W	R	R	R	R
[装订位置]	R	R/W	R	R	R/W	R
[打孔类型]	R	R/W	R	R	R/W	R
[折叠类型 / 叠纸器输出纸盘]* ⁴	R	R/W	R	R	R/W	R
[文件制成机：装订位置]	R	R/W	R	R	R/W	R
[文件制成机：打孔类型]	R	R/W	R	R	R/W	R
[简单屏幕：印后处理类型]	R	R/W	R	R	R/W	R
[对折设置(文件制成机：小册纸盘)]	R	R/W	R	R	R	R
[Z 形折叠输出纸盘]	R	R/W	R	R	R	R
[对折设置]	R	R/W	R	R	R	R
[信纸向外折叠设置]	R	R/W	R	R	R	R
[信纸向内折叠设置]	R	R/W	R	R	R	R
[双联折叠设置]	R	R/W	R	R	R	R
[门式折叠设置]	R	R/W	R	R	R	R

*4 项目名称根据安装的不同而不同。

[调整彩色图像]

设置	用户	机器	网络	文件	1 级	2 级
[ADS 的背景浓度（全彩／双色）]	R	R/W	R	R	R/W	R
[感色性]	R	R/W	R	R	R/W	R
[A.C.S.敏感度]	R	R/W	R	R	R/W	R
[A.C.S.优先级]	R	R/W	R	R	R/W	R

[管理员工具]

设置	用户	机器	网络	文件	1 级	2 级
[菜单保护]	R	R/W	R	R	R	R

打印机功能

本节列出了您在主页屏幕上按[打印机]以后显示的打印机功能。
如果设置了管理员验证，则根据“菜单保护”设置，用户操作限制会有所不同。

打印机功能

设置	用户	机器	网络	文件	1 级	2 级
[作业列表]	R	R	R	R	R	R
[打印作业]	R	R	R	R/W	R/W	R/W
[从记忆存储设备打印]	-	-	-	-	R/W	R/W
[作业重设]	R/W	R/W	R/W	R/W	R/W	R/W
[作业操作]	R/W	R/W	R/W	R/W	R/W	R/W
[强制进纸]	R/W	R/W	R/W	R/W	R/W	R/W
[假脱机作业列表]	R	R/W	R	R	R	R
[错误记录]	-	R	-	-	R	R

打印特性

如果设置了管理员验证，则根据“菜单保护”设置，用户操作限制会有所不同。

[列表／测试打印]

设置	用户	机器	网络	文件	1 级	2 级
[多个列表]	-	R/W	-	-	R/W	R/W
[配置页]	-	R/W	-	-	R/W	R/W
[错误记录]	-	R/W	-	-	R/W	R/W
[PCL 配置／字体页]	-	R/W	-	-	R/W	R/W
[PS 配置／字体页]	-	R/W	-	-	R/W	R/W
[PDF 配置／字体页]	-	R/W	-	-	R/W	R/W
[十六进制数]	-	R/W	-	-	R/W	R/W

[数据管理]

设置	用户	机器	网络	文件	1 级	2 级
[菜单保护]	R	R/W	R	R	R	R
[列表／测试打印锁定]	R	R/W	R	R	R	R
[删除所有临时打印作业]	-	-	-	R/W	-	-
[删除所有保存的打印作业]	-	-	-	R/W	-	-
[自动删除临时打印作业]	R	R	R	R/W	R	R
[自动删除保存的打印作业]	R	R	R	R/W	R	R
[4 色图形模式]	R	R	R	R/W	R	R

[系统]

设置	用户	机器	网络	文件	1 级	2 级
[打印错误报告]	R	R/W	R	R	R	R
[自动继续]	R	R/W	R	R	R	R

设置	用户	机器	网络	文件	1 级	2 级
[保存并跳过错误的作业]	R	R/W	R	R	R	R
[内存溢出]	R	R/W	R	R	R	R
[自动取消 PDL 错误作业的确认]	R	R/W	R	R	R	R
[错误时打印作业自动取消]	R	R/W	R	R	R	R
[作业分割]	R	R/W	R	R	R	R
[旋转 180 度]	R	R/W	R	R	R	R
[打印压缩的数据]	R	R/W	R/W	R	R	R
[双面]	R	R/W	R	R	R	R
[打印份数]	R	R/W	R	R	R	R
[空白页打印]	R	R/W	R	R	R	R
[假脱机图像]	R	R/W	R	R	R	R
[预定的作业的等待时间]	R	R/W	R	R	R	R
[打印机语言]	R	R/W	R	R	R	R
[副纸张尺寸]	R	R/W	R	R	R	R
[纸张尺寸]	R/W	R/W	R	R	R	R
[信头设置]	R	R/W	R	R	R	R
[纸盘设置优先顺序]	R	R/W	R	R	R	R
[边缘到边缘打印]	R	R/W	R	R	R	R
[默认打印机语言]	R	R/W	R	R	R	R
[纸盘切换]	R	R/W	R	R	R	R
[扩展自动纸盘切换]	R	R/W	R	R	R	R
[机器关闭时不打印作业]	R	R/W	R	R	R	R
[限制直接打印作业]	R	R/W	R	R	R	R
[切换到初始画面]	R	R/W	R	R	R	R

[主机接口]

设置	用户	机器	网络	文件	1 级	2 级
[I/O 缓冲区]	R	R/W	R	R	R	R
[I/O 超时]	R	R/W	R	R	R	R

[PCL 菜单]

设置	用户	机器	网络	文件	1 级	2 级
[方向]	R	R/W	R	R	R	R
[行宽]	R	R/W	R	R	R	R
[字体资源]	R	R/W	R	R	R	R
[字体编号]	R	R/W	R	R	R	R
[字体尺寸]	R	R/W	R	R	R	R
[字体间距]	R	R/W	R	R	R	R
[字符集]	R	R/W	R	R	R	R
[Courier 字体]	R	R/W	R	R	R	R
[扩展 A4 宽度]	R	R/W	R	R	R	R
[附加 CR 到 LF]	R	R/W	R	R	R	R
[分辨率]	R	R/W	R	R	R	R

[PS 菜单]

设置	用户	机器	网络	文件	1 级	2 级
[作业超时]	R	R/W	R	R	R	R
[等待超时]	R	R/W	R	R	R	R
[纸张选择方式]	R	R/W	R	R	R	R
[在单面和双面打印功能之间切换]	R	R/W	R	R	R	R
[数据格式]	R	R/W	R	R	R	R
[分辨率]	R	R/W	R	R	R	R

设置	用户	机器	网络	文件	1 级	2 级
[节省碳粉]	R	R/W	R	R	R	R
[颜色设置]	R	R/W	R	R	R	R
[颜色配置文件]	R	R/W	R	R	R	R
[处理彩色模块]	R	R/W	R	R	R	R
[自动检测方向]	R	R/W	R	R	R	R
[灰度再现]	R	R/W	R	R	R	R

[PDF 菜单]

设置	用户	机器	网络	文件	1 级	2 级
[更改 PDF 密码]	R	R/W	R	R	R	R
[PDF 组密码]	R	R/W	R	R	R	R
[倒序打印]	R	R/W	R	R	R	R
[分辨率]	R	R/W	R	R	R	R
[节省碳粉]	R	R/W	R	R	R	R
[颜色设置]	R	R/W	R	R	R	R
[颜色配置文件]	R	R/W	R	R	R	R
[处理彩色模块]	R	R/W	R	R	R	R
[自动检测方向]	R	R/W	R	R	R	R

扫描仪特性

如果设置了管理员验证，则根据“菜单保护”设置，用户操作限制会有所不同。

[常规设置]

设置	用户	机器	网络	文件	1 级	2 级
[切换标题]	R	R/W	R	R	R	R
[搜索目的地]	R	R/W	R	R	R	R
[外部验证：文件夹路径覆盖设置]	R	R/W	R	R	R	R
[计算机扫描命令待机时间]	R	R/W	R	R	R	R
[地址列表显示优先级 1]	R	R/W	R	R	R	R
[地址列表显示优先级 2]	R	R/W	R	R	R	R
[打印和删除扫描仪日志]	R	R/W	R	R	R	R
[打印扫描仪日志]	R	R/W	R	R	R	R
[删除扫描仪日志]	R	R/W	R	R	R	R
[删除目的地历史]	R	R/W	R	R	R	R
[使用 WSD 或 DSM]	R	R/W	R	R	R/W	R
[使用非 DSM 的目的地列表]	R	R/W	R	R	R/W	R
[目的地的编入设置]	R	R/W	R	R	R	R

9

[扫描设置]

设置	用户	机器	网络	文件	1 级	2 级
[A.C.S.敏感级别]	R	R/W	R	R	R	R
[等待下一份原稿的时间：曝光玻璃]	R	R/W	R	R	R	R
[等候下一张原稿的时间：SADF]	R	R/W	R	R	R	R
[ADS 的背景浓度（全彩）]	R	R/W	R	R	R	R
[空白页检测]	R	R/W	R	R	R	R
[复印比例]	R	R/W	R	R	R	R

设置	用户	机器	网络	文件	1 级	2 级
[编入／更改／删除扫描尺寸]	R	R/W	R	R	R	R

[发送设置]

设置	用户	机器	网络	文件	1 级	2 级
[压缩（黑白）]	R	R/W	R	R	R/W	R
[压缩方式（黑白）]	R	R/W	R	R	R/W	R
[压缩（灰度／全彩）]	R	R/W	R	R	R/W	R
[高压缩 PDF 的压缩方法]	R	R/W	R	R	R/W	R
[高压缩 PDF 等级]	R	R/W	R	R	R/W	R
[OCR 扫描的 PDF：空白页敏感度]	R	R/W	R	R	R/W	R
[最大电子邮件尺寸]	R	R	R/W	R	R	R
[分割和发送电子邮件]	R	R	R/W	R	R	R
[插入附加的电子邮件信息]	R	R/W	R	R	R/W	R
[单页文件的位数]	R	R/W	R	R	R/W	R
[保存的文件的电子邮件方法]	R	R/W	R	R	R/W	R
[默认电子邮件主题]	R	R/W	R	R	R	R

[初始设置]

设置	用户	机器	网络	文件	1 级	2 级
[菜单保护]	R	R/W	R	R	R	R

扩展功能设置

[扩展功能设置]

设置	用户	机器	网络	文件	未设置	设置
[启动设置]	R	R/W	R	R	R	R
[安装]	R	R/W	R	R	R	R
[卸载]	R	R/W	R	R	R	R
[扩展功能信息]	R	R/W	R	R	R	R
[管理员工具]	-	R/W	-	-	-	-
[附加程序启动设置]	R	R/W	R	R	R	R
[安装附加的程序]	R	R/W	R	R	R	R
[卸载附加的程序]	R	R/W	R	R	R	R
[附加的程序信息]	R	R/W	R	R	R	R

维护

如果设置了管理员验证，则根据“可用设置”中的配置，用户操作限制会有所不同。

[维护]

设置	用户	机器	网络	文件	未设置	设置
[自动颜色校准]	-	R/W	-	-	R/W	-
[色彩校色]	-	R/W	-	-	R/W	-

Web Image Monitor: 显示环保计数器

这些设置在[状态/信息]中。
用户只能查看自己的计数器。

设置	用户	机器	网络	文件	未设置	设置
[下载]	-	R/W	-	-	-	-
[设备总计数器]	-	R	-	-	-	-
[每个用户的计数器]	-	R	-	-	R	R

Web Image Monitor: 作业

这些设置在[状态/信息]中。

用户只能更改自己执行的作业。

[作业列表]

设置	用户	机器	网络	文件	未设置	设置
[当前/正在等待作业]: [删除预约]	-	R/W	-	-	-	R/W
[当前/正在等待作业]: [暂停打印]/[恢复打印]	-	R/W	-	-	-	-
[当前/正在等待作业]: [更改顺序]	-	R/W	-	-	-	-
[作业历史]	-	R	-	-	R	R* ¹

*¹ 启用用户代码验证作为用户验证方法时可以查看。

[打印机]

设置	用户	机器	网络	文件	未设置	设置
[假脱机打印]: [删除]	R	R/W	R	R	R	R
[作业历史]	R	R/W	R	R	R	R
[错误日志]	-	R	-	-	R	R

[文件服务器]

设置	用户	机器	网络	文件	未设置	设置
[打印作业历史]	-	R	-	-	R	R* ¹
[扫描仪远程发送历史]	-	R	-	-	R	R* ¹

*¹ 启用用户代码验证作为用户验证方法时可以查看。

Web Image Monitor: 设备设置

这些设置在[设备管理]的[配置]中。
如果设置了管理员验证，则根据“可用设置”中的配置，用户操作限制会有所不同。

[系统]

设置	用户	机器	网络	文件	未设置	设置
[设备名称]	R	R	R/W	R	R/W	R
[注释]	R	R	R/W	R	R/W	R
[位置]	R	R	R/W	R	R/W	R
[显示面板语言]	R	R/W	R	R	R/W	R
[假脱机打印]	R	R/W	R	R	R/W	R
[保护打印机显示面板]	R	R/W	R	R	-	-
[打印优先]	R	R/W	R	R	R/W	R
[功能重置定时器]	R	R/W	R	R	R/W	R
[按节能键改变模式]	R	R/W	R	R	R/W	R
[按停止键暂停打印作业]	R	R/W	R	R	R/W	R
[在设备显示面板上显示 IP 地址]	R	R/W	R	R	-	-
[介质插槽的使用]	R	R/W	R	R	R	R
[兼容的 ID]	R	R/W	R	R	R/W	R
[PDF 文件类型：PDF/A 固定]	R	R/W	R	R	R/W	R
[禁止从 Web Image Monitor 打印保存的文件]	R	R/W	R	R	R	R
[输出纸盘]	R	R/W	R	R	R/W	R
[纸盘优先]	R	R/W	R	R	R/W	R
[封面页纸盘]	R	R/W	R	R	R/W	R
[封底页纸盘]	R	R/W	R	R	R/W	R

设置	用户	机器	网络	文件	未设置	设置
[隔页纸盘]	R	R/W	R	R	R/W	R
[指定页 1-11 纸盘]	R	R/W	R	R	R/W	R
[分割页纸盘]	R	R/W	R	R	R/W	R

[功能键分配/功能优先]

设置	用户	机器	网络	文件	未设置	设置
[功能键分配]	R	R/W	R	R	R/W	R
[功能优先]	R	R/W	R	R	R/W	R

[纸张]

设置	用户	机器	网络	文件	未设置	设置
[纸盘 1-8]	R	R/W	R	R	R/W	R
[纸盘 A]	R	R/W	R	R	R/W	R
[插纸机上纸盘]	R	R/W	R	R	R/W	R
[插纸机下纸盘]	R	R/W	R	R	R/W	R
[低容量纸张检测]	R	R/W	R	R	R	R

[自定义纸张]

设置	用户	机器	网络	文件	未设置	设置
[编入/更改]	-	R/W	-	-	R/W	-
[删除]	-	R/W	-	-	R/W	-
[调用纸库]	-	R/W	-	-	R/W	-

[日期/时间]

设置	用户	机器	网络	文件	未设置	设置
[设置日期]	R	R/W	R	R	R/W	R
[设定时间]	R	R/W	R	R	R/W	R
[SNTP 服务器名称]	R	R/W	R	R	R/W	R
[SNTP 轮询间隔]	R	R/W	R	R	R/W	R
[时区]	R	R/W	R	R	R/W	R

[定时器]

设置	用户	机器	网络	文件	未设置	设置
[睡眠模式定时器]	R	R/W	R	R	R/W	R
[低功率模式定时器]	R	R/W	R	R	R/W	R
[系统自动重置定时器]	R	R/W	R	R	R/W	R
[复印机/文件服务器自动重置定时器]	R	R/W	R	R	R/W	R
[扫描器自动重置定时器]	R	R/W	R	R	R/W	R
[打印机自动重置定时器]	R	R/W	R	R	R/W	R
[自动注销定时器]	R	R/W	R	R	R/W	R
[定影单元关闭模式开/关]	R	R/W	R	R	R/W	R
[周定时器]	R	R/W	R	R	R/W	R

[日志]

设置	用户	机器	网络	文件	未设置	设置
[作业日志]	R	R/W	R	R	R/W	R
[访问日志]	R	R/W	R	R	R/W	R
[环保日志]	R	R/W	R	R	R/W	R

设置	用户	机器	网络	文件	未设置	设置
[转送日志] ^{*2}	R	R/W	R	R	R/W	R
[分类代码]	R	R/W	R	R	R/W	R
[删除所有日志]	-	R/W	-	-	R/W	-

^{*2} 只能更改为[无效]。

[下载日志]

设置	用户	机器	网络	文件	未设置	设置
[下载的日志]	-	R/W	-	-	-	-
[下载]	-	R/W	-	-	-	-

[电子邮件]

设置	用户	机器	网络	文件	未设置	设置
[管理员电子邮件地址]	-	R/W	-	-	R/W	R
[自动指定发送者名称]	-	R/W	-	-	R/W	R
[签名]	-	R/W	-	-	R/W	R
[接收协议]	-	R/W	-	-	R/W	R
[电子邮件接收间隔]	-	-	R/W	-	R/W	R
[可接收的最大电子邮件尺寸]	-	-	R/W	-	R/W	R
[在服务器上存储电子邮件]	-	-	R/W	-	R/W	R
[SMTP 服务器名称]	-	-	R/W	-	R/W	R
[SMTP 端口号]	-	-	R/W	-	R/W	R
[使用安全连接(SSL)]	-	-	R/W	-	R/W	R
[SMTP 验证]	-	R/W	-	-	R/W	R
[SMTP 验证电子邮件地址]	-	R/W	-	-	R/W	R

设置	用户	机器	网络	文件	未设置	设置
[SMTP 验证用户名称]	-	R/W	-	-	R/W	-
[SMTP 验证密码]* ³	-	R/W	-	-	R/W	-
[SMTP 验证加密]	-	R/W	-	-	R/W	R
[SMTP 前 POP]	-	R/W	-	-	R/W	R
[POP 电子邮件地址]	-	R/W	-	-	R/W	R
[POP 用户名称]	-	R/W	-	-	R/W	-
[POP 密码]* ³	-	R/W	-	-	R/W	-
[POP 验证后的超时设置]	-	R/W	-	-	R/W	R
[POP3/IMAP4 服务器名称]	-	R/W	-	-	R/W	R
[POP3/IMAP4 加密]	-	R/W	-	-	R/W	R
[POP3 接收端口号]	-	-	R/W	-	R/W	R
[IMAP4 接收端口号]	-	-	R/W	-	R/W	R
[电子邮件通知的电子邮件地址]	-	R/W	-	-	R/W	R
[接收电子邮件通知]	-	R/W	-	-	R/W	-
[电子邮件通知用户名称]	-	R/W	-	-	R/W	-
[电子邮件通知密码]* ³	-	R/W	-	-	R/W	-

*3 无法读取密码。

[自动电子邮件通知]

设置	用户	机器	网络	文件	未设置	设置
[通知信息]	R	R/W	R	R	R/W	R
[要通知的群组]	R	R/W	R	R	R/W	R
[选择要通知的群组/项目]	R	R/W	R	R	R/W	R
[每个项目的详细设置]	R	R/W	R	R	R/W	R

[随选电子邮件通知]

设置	用户	机器	网络	文件	未设置	设置
[通知主题]	R	R/W	R	R	R/W	R
[通知信息]	R	R/W	R	R	R/W	R
[信息访问限制]	R	R/W	R	R	R/W	R
[可接受的电子邮件地址/域名设置]	R	R/W	R	R	R/W	R

[文件转送]

设置	用户	机器	网络	文件	未设置	设置
[SMB 用户名称]	-	R/W	-	-	R/W	-
[SMB 密码]* ³	-	R/W	-	-	R/W	-
[FTP 用户名称]	-	R/W	-	-	R/W	-
[FTP 密码]* ³	-	R/W	-	-	R/W	-
[NCP 用户名称]	-	R/W	-	-	R/W	-
[NCP 密码]* ³	-	R/W	-	-	R/W	-

*3 无法读取密码。

[用户验证管理]

设置	用户	机器	网络	文件	未设置	设置
[用户验证管理]	R	R/W	R	R	R/W	R
[打印机作业验证设置]	R	R/W	R	R	R/W	R
[用户代码验证设置]	R	R/W	R	R	R/W	R
[基本验证设置]	R	R/W	R	R	R/W	R
[Windows 验证设置]	R	R/W	R	R	R/W	R
[Windows 验证的群组设置]	R	R/W	R	R	R/W	R

设置	用户	机器	网络	文件	未设置	设置
[LDAP 验证设置]	R	R/W	R	R	R/W	R

[管理员验证管理]

设置	用户	机器	网络	文件	未设置	设置
[用户管理员验证]	R/W	R	R	R	R	R
[机器管理员验证]	R	R/W	R	R	R	R
[网络管理员验证]	R	R	R/W	R	R	R
[文件管理员验证]	R	R	R	R/W	R	R

[编入/更改管理员]

设置	用户	机器	网络	文件	未设置	设置
[用户管理员]	R/W	R	R	R	-	-
[机器管理员]	R	R/W	R	R	-	-
[网络管理员]	R	R	R/W	R	-	-
[文件管理员]	R	R	R	R/W	-	-
[登录用户名]* ⁴	R/W	R/W	R/W	R/W	-	-
[登录密码]* ⁴	R/W	R/W	R/W	R/W	-	-
[加密密码]* ⁴	R/W	R/W	R/W	R/W	-	-

*⁴ 管理员只能更改自己的帐户。

[打印容量使用限制]

设置	用户	机器	网络	文件	未设置	设置
[当达到限制时的机器操作]	R	R/W	R	R	R	R
[打印容量使用限制：单组计数设置]	R	R/W	R	R	R	R

设置	用户	机器	网络	文件	未设置	设置
[容量使用计数器：定期/指定的重置设置]	R	R/W	R	R	R	R

[LDAP 服务器]

设置	用户	机器	网络	文件	未设置	设置
[LDAP 搜索]	-	R/W	-	-	R/W	-
[更改]	-	R/W	-	-	R/W	-
[删除]	-	R/W	-	-	R/W	-

[固件更新]

设置	用户	机器	网络	文件	未设置	设置
[更新]	-	R/W	-	-	-	-
[固件版本]	-	R	-	-	-	-

[Kerberos 验证]

设置	用户	机器	网络	文件	未设置	设置
[加密算法]	-	R/W	-	-	-	-
[领域 1-5]	-	R/W	-	-	-	-

[设备设置信息：导入设置（服务器）]

设置	用户	机器	网络	文件	未设置	设置
[导入文件来自]* ⁵	-	-	-	-	-	-
[定期在指定的时间导入]* ⁵	-	-	-	-	-	-
[新文件和最新导入文件的比较]* ⁵	-	-	-	-	-	-

设置	用户	机器	网络	文件	未设置	设置
[电子邮件失败通知]* ⁵	-	-	-	-	-	-
[再试次数]* ⁵	-	-	-	-	-	-
[再试间隔]* ⁵	-	-	-	-	-	-
[加密密钥]* ⁵	-	-	-	-	-	-

*⁵ R/W 是具有所有权限（包括用户管理员、机器管理员、网络管理员和文件管理员权限）的管理员。

[导入测试]

设置	用户	机器	网络	文件	未设置	设置
[开始]* ⁵	-	-	-	-	-	-

*⁵ R/W 是具有所有权限（包括用户管理员、机器管理员、网络管理员和文件管理员权限）的管理员。

[导入/导出设备设置信息]

设置	用户	机器	网络	文件	未设置	设置
[导出设备设置信息]* ⁵	-	-	-	-	-	-
[导入设备设置信息]* ⁵	-	-	-	-	-	-
[导出主页画面的图像文件]* ⁵	-	-	-	-	-	-

*⁵ R/W 是具有所有权限（包括用户管理员、机器管理员、网络管理员和文件管理员权限）的管理员。

[环保计数器期间/管理员信息]

设置	用户	机器	网络	文件	未设置	设置
[显示信息画面]	R	R/W	R	R	R/W	R
[显示时间]	R	R/W	R	R	R/W	R
[计数期间]	R	R/W	R	R	R/W	R

设置	用户	机器	网络	文件	未设置	设置
[计数期间（日数）]	R	R/W	R	R	R/W	R
[管理员信息]	R	R/W	R	R	R/W	R

[强制安全印记]

设置	用户	机器	网络	文件	未设置	设置
[复印机]	R	R/W	R	R	R	R
[文件服务器]	R	R/W	R	R	R	R
[打印机]	R	R/W	R	R	R	R

[防止未授权的复印：打印机]

设置	用户	机器	网络	文件	未设置	设置
[防止未授权的复印设置]	R	R/W	R	R	R	R
[强制防止未授权的复印]	R	R/W	R	R	R	R
[防止未授权的复印类型]	R	R/W	R	R	R	R
[图案/浓度/效果的掩码类型]	R	R/W	R	R	R	R
[防止文本设置]	R	R/W	R	R	R	R

[编入/更改 USB 设备列表]

设置	用户	机器	网络	文件	未设置	设置
[设备 1]	R	R/W	R	R	R/W	R
[设备 2]	R	R/W	R	R	R/W	R

Web Image Monitor: 打印机

这些设置在[设备管理]的[配置]中。

如果设置了管理员验证，则根据“菜单保护”设置，用户操作限制会有所不同。

[基本设置]

设置	用户	机器	网络	文件	1 级	2 级
[打印错误报告]	R	R/W	R	R	R	R
[自动继续]	R	R/W	R	R	R	R
[内存溢出]	R	R/W	R	R	R	R
[自动取消 PDL 错误作业的确认]	R	R/W	R	R	R	R
[错误时自动取消打印作业]	R	R/W	R	R	R	R
[作业分割]	R	R/W	R	R	R	R
[自动删除临时打印作业]	R	R	R	R/W	R	R
[自动删除保存的打印作业]	R	R	R	R/W	R	R
[机器关闭时的未打印作业]	R	R/W	R	R	R	R
[旋转 180 度]	R	R/W	R	R	R	R
[打印压缩的数据]	R	R/W	R/W	R	R	R
[双面]	R	R/W	R	R	R	R
[份数]	R	R/W	R	R	R	R
[空白页打印]	R	R/W	R	R	R	R
[假脱机图像]	R	R/W	R	R	R	R
[保留作业等待时间]	R	R/W	R	R	R	R
[打印机语言]	R	R/W	R	R	R	R
[子纸张尺寸]	R	R/W	R	R	R	R
[页尺寸]	R	R/W	R	R	R/W	R
[信头设置]	R	R/W	R	R	R	R
[纸盘设置优先]	R	R/W	R	R	R	R

设置	用户	机器	网络	文件	1 级	2 级
[保存并跳过错误的作业]	R	R/W	R	R	R	R
[边缘到边缘打印]	R	R/W	R	R	R	R
[默认打印机语言]	R	R/W	R	R	R	R
[纸盘切换]	R	R/W	R	R	R	R
[列表/测试打印锁定]	R	R/W	R	R	R	R
[扩展自动纸盘切换]	R	R/W	R	R	R	R
[虚拟打印机]	R	R/W	R	R	R	R
[限制直接打印作业]	R	R/W	R	R	R	R
[初始画面切换设置]	R	R/W	R	R	R	R
[主机接口]	R	R/W	R	R	R	R
[PCL 菜单]	R	R/W	R	R	R	R
[PS 菜单]	R	R/W	R	R	R	R
[PDF 菜单]	R	R/W	R	R	R	R

[纸盘参数 (PCL)]

设置	用户	机器	网络	文件	1 级	2 级
[纸盘参数 (PCL)]	-	R/W	-	-	-	-

[纸盘参数 (PS)]

设置	用户	机器	网络	文件	1 级	2 级
[纸盘参数 (PS)]	-	R/W	-	-	-	-

[PDF 临时密码]

设置	用户	机器	网络	文件	1 级	2 级
[PDF 临时密码]	-	-	-	-	R/W	R/W

[PDF 群组密码]

设置	用户	机器	网络	文件	1 级	2 级
[PDF 群组密码]	-	R/W	-	-	-	-

[PDF 固定密码]

设置	用户	机器	网络	文件	1 级	2 级
[PDF 固定密码]	-	R/W	-	-	-	-

[虚拟打印机设置]

设置	用户	机器	网络	文件	1 级	2 级
[虚拟打印机名称]	R	R/W	R	R	R	R
[协议]	R	R/W	R	R	R	R
[打印错误报告]	R	R/W	R	R	R	R
[作业分割]	R	R/W	R	R	R	R
[旋转 180 度]	R	R/W	R	R	R	R
[双面]	R	R/W	R	R	R	R
[份数]	R	R/W	R	R	R	R
[空白页打印]	R	R/W	R	R	R	R
[子纸张尺寸]	R	R/W	R	R	R	R
[输入纸盘]	R	R/W	R	R	R/W	R/W
[页尺寸]	R	R/W	R	R	R/W	R
[纸张类型]	R	R/W	R	R	R/W	R/W
[输出纸盘]	R	R/W	R	R	R/W	R/W
[信头设置]	R	R/W	R	R	R	R
[边缘到边缘打印]	R	R/W	R	R	R	R
[PCL 菜单]	R	R/W	R	R	R	R
[PS 菜单]	R	R/W	R	R	R	R

设置	用户	机器	网络	文件	1 级	2 级
[PDF 菜单]	R	R/W	R	R	R	R
[RHPP 设置]	R	R/W	R	R	R/W	R/W

[允许打印机语言操作文件系统]

设置	用户	机器	网络	文件	1 级	2 级
[PJL]	R	R/W	R	R	R	R
[PDF, PostScript]	R	R/W	R	R	R	R

Web Image Monitor: 扫描仪

这些设置在[设备管理]的[配置]中。

如果设置了管理员验证，则根据“菜单保护”设置，用户操作限制会有所不同。

[常规设置]

设置	用户	机器	网络	文件	1 级	2 级
[切换标题]	R	R/W	R	R	R	R
[搜索目的地]	R	R/W	R	R	R	R
[计算机扫描命令待机时间]	R	R/W	R	R	R	R
[目的地列表显示优先 1]	R	R/W	R	R	R	R
[目的地列表显示优先 2]	R	R/W	R	R	R	R
[打印并删除扫描仪日志]	R	R/W	R	R	R	R
[外部验证：文件夹路径覆盖设置]	R	R/W	R	R	R	R

[扫描设置]

设置	用户	机器	网络	文件	1 级	2 级
[A.C.S.感色性等级]	R	R/W	R	R	R	R
[下一原稿的等待时间]	R	R/W	R	R	R	R
[ADS 背景浓度（全彩色）]	R	R/W	R	R	R	R
[空白页检测]	R	R/W	R	R	R	R

[发送设置]

设置	用户	机器	网络	文件	1 级	2 级
[压缩（黑白）]	R	R/W	R	R	R/W	R
[压缩（灰度级／全彩色）]	R	R/W	R	R	R/W	R
[OCR 扫描的 PDF：空白页敏感度]	R	R/W	R	R	R/W	R
[高压压缩 PDF 等级]	R	R/W	R	R	R/W	R
[高压压缩 PDF 的压缩方式]	R	R/W	R	R	R/W	R

设置	用户	机器	网络	文件	1 级	2 级
[最大电子邮件大小]	R	R	R/W	R	R ^{*1}	R ^{*1}
[分割并发送电子邮件]	R	R	R/W	R	R ^{*1}	R ^{*1}
[插入附加的电子邮件信息]	R	R/W	R	R	R/W	R
[单页文件的位数]	R	R/W	R	R	R/W	R
[保存的文件电子邮件方式]	R	R/W	R	R	R/W	R
[默认电子邮件主题]	R	R/W	R	R	R	R

*1 如果[管理员验证管理]中的[网络管理]设置为[关]，则用户具有 R/W 权限。

[初始设置]

设置	用户	机器	网络	文件	1 级	2 级
[菜单保护]	R	R/W	R	R	R	R
[使用 WSD 或 DSM]	R	R/W	R	R	R	R
[显示 WSD 目的地列表]	R	R/W	R	R	R	R
[禁止 WSD 扫描命令]	R	R/W	R	R	R	R
[使用非 DSM 的目的地列表]	R	R/W	R	R	R	R

9

[在设备普通显示面板上的默认设置]

设置	用户	机器	网络	文件	1 级	2 级
[保存文件]	-	R/W	-	-	R	R
[预览]	-	R/W	-	-	R	R
[扫描设置]	-	R/W	-	-	R	R
[发送文件类型]	-	R/W	-	-	R	R

[在设备简单显示面板上的默认设置]

设置	用户	机器	网络	文件	1 级	2 级
[扫描设置]	-	R/W	-	-	R	R

设置	用户	机器	网络	文件	1 级	2 级
[发送文件类型]	-	R/W	-	-	R	R

Web Image Monitor: 接口

这些设置在[设备管理]的[配置]中。

如果设置了管理员验证，则根据“可用设置”中的配置，用户操作限制会有所不同。

[接口设置]

设置	用户	机器	网络	文件	未设置	设置
[网络]	R	R	R	R	R	R
[MAC 地址]	R	R	R	R	R	R
[以太网安全]	R	R	R/W	R	R/W	R
[以太网速度]	R	R	R/W	R	R/W	R
[USB 主机]	R	R/W	R	R	R/W	R

Web Image Monitor: 网络

这些设置在[设备管理]的[配置]中。
如果设置了管理员验证，则根据“可用设置”中的配置，用户操作限制会有所不同。

[IPv4]

设置	用户	机器	网络	文件	未设置	设置
[IPv4]	R	R	R/W* ₁	R	R/W* ₁	R
[主机名称]	R	R	R/W	R	R/W	R
[DHCP]	R	R	R/W	R	R/W	R
[域名]	R	R	R/W	R	R/W	R
[IPv4 地址]	R	R	R/W	R	R/W	R
[子网掩码]	R	R	R/W	R	R/W	R
[DDNS]	R	R	R/W	R	R/W	R
[WINS]	R	R	R/W	R	R/W	R
[主 WINS 服务器]	R	R	R/W	R	R/W	R
[次 WINS 服务器]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[作用域 ID]	R	R	R/W	R	R/W	R
[详细资料]	R	R	R/W	R	R/W	R

*₁ 通过 IPv4 连接使用 Web Image Monitor 时无法禁用 IPv4。

[IPv6]

设置	用户	机器	网络	文件	未设置	设置
[IPv6]	R	R	R/W* ₂	R	R/W* ₂	R
[主机名称]	R	R	R/W	R	R/W	R

设置	用户	机器	网络	文件	未设置	设置
[域名]	R	R	R/W	R	R/W	R
[链路本地地址]	R	R	R	R	R	R
[无状态地址]	R	R	R/W	R	R/W	R
[手动配置地址]	R	R	R/W	R	R/W	R
[DHCPv6]	R	R	R/W	R	R/W	R
[DHCPv6 地址]	R	R	R	R	R	R
[DDNS]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[详细资料]	R	R	R/W	R	R/W	R

*2 通过 IPv6 连接使用 Web Image Monitor 时无法禁用 IPv6。

[NetWare]

设置	用户	机器	网络	文件	未设置	设置
[NetWare]	R	R	R/W	R	R/W	R
[NetWare 打印设置]	R	R	R/W	R	R/W	R
[NCP 传送]	R	R	R/W	R	R/W	R

[SMB]

设置	用户	机器	网络	文件	未设置	设置
[SMB]	R	R	R/W	R	R/W	R
[协议]	R	R	R	R	R	R
[工作组名称]	R	R	R/W	R	R/W	R
[计算机名称]	R	R	R/W	R	R/W	R
[注释]	R	R	R/W	R	R/W	R

设置	用户	机器	网络	文件	未设置	设置
[共享名]	R	R	R	R	R	R
[通知打印完毕]	R	R	R/W	R	R/W	R

[SNMP]

设置	用户	机器	网络	文件	未设置	设置
[SNMP]	-	-	R/W	-	-	-
[协议]	-	-	R/W	-	-	-
[SNMPv1, v2 设置]	-	-	R/W	-	-	-
[社区]	-	-	R/W	-	-	-

[SNMPv3]

设置	用户	机器	网络	文件	未设置	设置
[SNMP]	-	-	R/W	-	-	-
[协议]	-	-	R/W	-	-	-
[SNMPv3 设置]	-	-	R/W	-	-	-
[SNMPv3 陷阱通信设置]	-	-	R/W	-	-	-
[帐户 (用户)]	-	-	R/W	-	-	-
[帐户 (网络管理员)]	-	-	R/W	-	-	-
[帐户 (机器管理员)]	-	R/W	-	-	-	-

[SSDP]

设置	用户	机器	网络	文件	未设置	设置
[SSDP]	-	-	R/W	-	-	-
[UUID]	-	-	R	-	-	-

设置	用户	机器	网络	文件	未设置	设置
[配置文件过期]	-	-	R/W	-	-	-
[TTL]	-	-	R/W	-	-	-

[Bonjour]

设置	用户	机器	网络	文件	未设置	设置
[Bonjour]	R	R	R/W	R	R/W	R
[本地主机名称]	R	R	R	R	R	R
[详细资料]	R	R	R/W	R	R/W	R
[打印顺序优先]	R	R	R/W	R	R/W	R

[系统日志]

设置	用户	机器	网络	文件	未设置	设置
[系统日志]	R	R	R	R	R	-

Web Image Monitor: 安全

这些设置在[设备管理]的[配置]中。

设置	用户	机器	网络	文件	未设置	设置
[网络安全]	-	-	R/W	-	-	-
[访问控制]	-	-	R/W	-	-	-
[IPP 验证]	-	-	R/W	-	-	-
[SSL/TLS]	-	-	R/W	-	-	-
[ssh]	-	-	R/W	-	R	R
[站点证书]	-	-	R/W	-	-	-
[设备证书]	-	-	R/W	-	-	-
[S/MIME]	-	-	R/W	-	-	-
[IPsec]	-	-	R/W	-	-	-
[用户锁定策略]	-	R/W	-	-	-	-
[IEEE 802. 1X]	-	-	R/W	-	-	-
[安全扩展]						
• [驱动程序加密密钥]	-	-	R/W	-	R/W	-
• [驱动程序加密密钥: 加密强度]	R	R	R/W	R	R/W	R
• [限制显示用户信息]	R	R/W	R	R	R/W	R
• [加密用户自定义设置和通讯簿]	R/W	R	R	R	R	R
• [增强文件保护]	R	R	R	R/W	R	R
• [限制目的地的使用 (扫描仪)]	R/W	R	R	R	R	R
• [限制添加用户目的地 (扫描仪)]	R/W	R	R	R	R	R
• [验证当前作业]	R	R/W	R	R	R/W	R
• [@Remote 服务]	R	R/W	R	R	R/W	R

设置	用户	机器	网络	文件	未设置	设置
• [更新固件]	R	R/W	R	R	-	-
• [更改固件结构]	R	R/W	R	R	-	-
• [密码策略]	R/W	-	-	-	-	-
• [SNMPv1,v2 设置]	R	R	R/W	R	R/W	R
• [非法访问的安全设置]	-	R/W	-	-	-	-
• [密码输入非法]	-	R/W	-	-	-	-
• [非法访问设备]	-	R/W	-	-	-	-

Web Image Monitor: @Remote

这些设置在[设备管理]的[配置]中。

设置	用户	机器	网络	文件	未设置	设置
[设置 RC Gate]	-	R/W	-	-	-	-
[更新 RC Gate 固件]	-	R/W	-	-	-	-
[RC Gate 代理服务器]	-	R/W	-	-	-	-
[通知设备功能故障]	-	R/W	-	-	-	-

Web Image Monitor: 网页

这些设置在[设备管理]的[配置]中。

如果设置了管理员验证，则根据“可用设置”中的配置，用户操作限制会有所不同。

[网页]

设置	用户	机器	网络	文件	未设置	设置
[网页语言]	R	R	R/W	R	R/W	R
[Web Image Monitor 自动注销]	R	R	R/W	R	R/W	R
[设置链接页的 URL 目标]	R	R	R/W	R	R/W	R
[设置帮助 URL 目标]	R	R	R/W	R	R/W	R
[WSD/UPnP 设置]	R	R	R/W	R	R/W	R
[下载帮助文件]	R/W	R/W	R/W	R/W	R/W	R/W

Web Image Monitor: 扩展功能设置

这些设置在[设备管理]的[配置]中。

设置	用户	机器	网络	文件	未设置	设置
[启动设置]	-	R/W	-	-	-	-
[扩展功能信息]	R	R	R	R	R	R
[安装]	-	R/W	-	-	-	-
[卸载]	-	R/W	-	-	-	-
[管理员工具]	-	R/W	-	-	-	-
[附加的程序的启动设置]	-	R/W	-	-	-	-
[安装附加的程序]	-	R/W	-	-	-	-
[卸载附加的程序]	-	R/W	-	-	-	-
[复制扩展功能]	-	R/W	-	-	-	-
[复制卡保存数据]	-	R/W	-	-	-	-

Web Image Monitor：地址簿

这些设置在[设备管理]中。

设置	用户	机器	网络	文件	未设置	设置
[添加用户]	R/W	-	-	-	R/W *1	R/W *1
[更改]	R/W	-	-	-	R/W *1	R/W *1
[删除]	R/W	-	-	-	R/W *1	R/W *1
[添加群组]	R/W	-	-	-	R/W *1	R/W *1
[地址簿自动编入的数据保留设置]	R/W	-	-	-	R/W	R
[维护]	R/W	-	-	-	-	-
[通讯簿集中管理]	R/W	-	-	-	-	-

*1 如果[安全扩展]的[限制添加用户目的地]设置为[开]，且对机器应用了基本验证，则每位用户只能更改各自帐户的密码。

Web Image Monitor: 通讯簿集中管理

这些设置在[设备管理]中。

如果您具有管理员权限，则不会显示该设置。在这种情况下，请通过访问[设备管理] > [地址簿]来指定该设置。

设置	用户	机器	网络	文件	未设置	设置
[通讯簿集中管理]	-	R/W	-	-	-	-

Web Image Monitor: 主电源关闭

这些设置在[设备管理]中。

设置	用户	机器	网络	文件	未设置	设置
[主电源关闭模式]	-	R/W	-	-	-	-
[确定]	-	R/W	-	-	-	-

Web Image Monitor: 重置打印机作业

这些设置在[设备管理]中。

设置	用户	机器	网络	文件	未设置	设置
[重置当前作业]	-	R/W	-	-	-	-
[重置全部作业]	-	R/W	-	-	-	-

Web Image Monitor: 重置该机器

这些设置在[设备管理]中。

如果设置了管理员验证，则根据“可用设置”中的配置，用户操作限制会有所不同。

设置	用户	机器	网络	文件	未设置	设置
[重置该机器]	-	R/W	-	-	R/W	-

Web Image Monitor: 设备主页管理

这些设置在[设备管理]中。

如果设置了管理员验证，则根据“可用设置”中的配置，用户操作限制会有所不同。

设置	用户	机器	网络	文件	未设置	设置
[编辑图标]	R	R/W	R	R	R/W	R
[恢复默认图标显示]	-	R/W	-	-	R/W	-
[主页画面设置]	R	R/W	R	R	R/W	R

Web Image Monitor: 画面监控

这些设置在[设备管理]中。

设置	用户	机器	网络	文件	未设置	设置
[显示设备画面]	-	R/W	-	-	-	-

Web Image Monitor: 每个用户的自定义画面

如果[用户自己的自定义]设置为[允许]，将会出现此设置。

用户只能更改自己的设置。

设置	用户	机器	网络	文件	未设置	设置
[编辑图标]	-	-	-	-	-	R/W
[恢复默认图标显示]	-	-	-	-	-	R/W
[每个用户的功能优先]	-	-	-	-	-	R/W

Web Image Monitor：文件服务器

这些设置在[打印作业/保存的文件]。

用户可以对保存的文件进行什么样的处理取决于访问权限。有关详细信息，请参见 p.322 “保存文件操作权限列表”。

设置	用户	机器	网络	文件	未设置	设置
[新文件夹]	-	-	-	R/W	R/W	R/W
[编辑文件夹]	-	-	-	R/W	R/W	R/W
[删除文件夹]	-	-	-	R/W	R/W	R/W
[解锁文件夹]	-	-	-	R/W	-	-
[打印]	-	-	-	-	R/W	R/W
[发送]	-	-	-	-	R/W	R/W
[删除]	-	-	-	R/W	R/W	R/W
[ 编辑详细信息]	-	-	-	R/W	R/W	R/W
[下载]	-	-	-	-	R/W	R/W
[解除文件锁定]	-	-	-	R/W	-	-

Web Image Monitor: 打印机: 打印作业

这些设置在[打印作业/保存的文件]。

用户可以管理的打印机文件为用户自己保存的文件，或禁用用户验证时可以管理打印机文件。

屏幕上不会显示其他用户保存的打印机文件。

设置	用户	机器	网络	文件	未设置	设置
[打印]	-	-	-	-	R/W *1	R/W *1
[删除]	-	-	-	R/W	R/W *1	R/W *1
[ 编辑详细信息]	-	-	-	R/W	R/W *1	R/W *1
[解除作业锁定]	-	-	-	R/W	-	-

*1 根据用户的访问权限，系统可能会限制对保存文件的访问。

保存文件操作权限列表

了解标题

- 只读
分配了读取权限的用户。
- 编辑
分配了编辑权限的用户。
- E/D
分配了编辑/删除权限的用户。
- 充满时
分配了完全控制权限的用户。
- 所有者
指示注册了文件的用户或指定为所有者的用户。
- 文件
指示文件管理员。

了解符号

R/W：可以执行

-：无法执行

设置	只读	编辑	E/D	充满时	所有者	文件
[正在打印]	R/W	R/W	R/W	R/W	R/W	-
[详细内容]	R/W	R/W	R/W	R/W	R/W	R/W
[预览]	R/W	R/W	R/W	R/W	R/W	-
[更改访问权限]：[所有者]	-	-	-	-	-	R/W
[更改访问权限]：[用户/组的权限]	-	-	-	R/W	R/W* ¹	R/W
[更改文件名]	-	R/W	R/W	R/W	R/W* ¹	-
[更改密码]	-	-	-	-	R/W	R/W
[解除文件锁定]	-	-	-	-	-	R/W
[合并文件]	-	-	R/W	R/W	R/W* ¹	-
[插入文件]	-	-	R/W	R/W	R/W* ¹	-

设置	只读	编辑	E/D	充满时	所有者	文件
[删除页]	-	-	R/W	R/W	R/W* ¹	-
[复制文件]	R/W	R/W	R/W	R/W	R/W* ¹	-
[删除文件]	-	-	R/W	R/W	R/W* ¹	R/W
[打印指定页]	R/W	R/W	R/W	R/W	R/W* ¹	-
[保持双面/单面设置]	R/W	R/W	R/W	R/W	R/W* ¹	-

*1 所有者可以更改操作权限。

可以将[合并文件]和[插入文件]应用到具有“编辑/删除”访问权限的文件。

执行[合并文件]或[插入文件]时，最初选择的文件所配置的访问权限将应用到新创建的文件。

通讯簿操作权限列表

了解标题

- 只读
分配了读取权限的用户。
- 编辑
分配了编辑权限的用户。
- E/D
分配了编辑/删除权限的用户。
- 充满时
分配了完全控制权限的用户。
- 输入
指示在通讯簿中注册了其个人信息的用户。同时，也指示知道其用户登录名和密码的任何用户。
- 用户
指示用户管理员。

了解符号

- R/W：可以执行、更改和读取。
- R：可以读取。
- ：无法执行、更改和读取。

[名称]

设置	只读	编辑	E/D	充满时	输入	用户
[名称]	R	R/W	R/W	R/W	R/W	R/W
[主要显示]	R	R/W	R/W	R/W	R/W	R/W
[注册号码]	R	R/W	R/W	R/W	R/W	R/W
[显示优先顺序]	R	R/W	R/W	R/W	R/W	R/W
[选择标题]	R	R/W	R/W	R/W	R/W	R/W

[验证信息]

设置	只读	编辑	E/D	充满时	输入	用户
[用户代码]	-	-	-	-	-	R/W
[登录用户名]	-	-	-	-	R	R/W
[登录密码]	-	-	-	-	R/W *1	R/W *1
[SMTP 验证]	-	-	-	-	R/W *1	R/W *1
[文件夹验证]	R	R/W *1	R/W *1	R/W *1	R/W *1	R/W *1
[LDAP 验证]	-	-	-	-	R/W *1	R/W *1
[可使用的功能]	-	-	-	-	R	R/W
[打印容量使用限制]	-	-	-	-	R	R/W

*1 无法读取密码。

[保护]

设置	只读	编辑	E/D	充满时	输入	用户
[将名称用作]	R	R/W	R/W	R/W	R/W	R/W
[保护目的地]: [保护代码]	-	-	-	R/ W*2	R/ W*2	R/ W*2
[保护目的地]: [保护对象]	-	R/W	R/W	R/W	R/W	R/W
[保护目的地]: [用户/组的权限]	-	-	-	R/W	R/W	R/W
[保护文件]: [用户/组的权限]	-	-	-	R/W	R/W	R/W

*2 无法读取[保护代码]的代码。

[电子邮件]

设置	只读	编辑	E/D	充满时	输入	用户
[电子邮件地址]	R	R/W	R/W	R/W	R/W	R/W

[文件夹]

设置	只读	编辑	E/D	充满时	输入	用户
[SMB/FTP/NCP]	R	R/W	R/W	R/W	R/W	R/W
[SMB]: [路径]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [服务器名称]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [路径]	R	R/W	R/W	R/W	R/W	R/W
[FTP]: [端口号]	R	R/W	R/W	R/W	R/W	R/W
[NCP]: [路径]	R	R/W	R/W	R/W	R/W	R/W
[NCP]: [连接类型]	R	R/W	R/W	R/W	R/W	R/W
[测试连接]	R	R/W	R/W	R/W	R/W	R/W

[添加到组]

设置	只读	编辑	E/D	充满时	输入	用户
[注册号码]	R	R/W	R/W	R/W	R/W	R/W
[搜索]	R	R/W	R/W	R/W	R/W	R/W
[切换标题]	R/W	R/W	R/W	R/W	R/W	R/W

注

- 当[安全扩展]的[限制添加用户目的地]设置为[开]时，无论用户的操作权限如何，仅用户管理员可以访问通讯簿。

索引

A

AH 协议.....	124
AH 协议+ESP 协议.....	124
authfree.....	50

B

保存文件的访问权限.....	153
保存文件的密码.....	153

C

菜单保护.....	60
操作权限.....	253
操作问题.....	249
超级用户.....	22
传送的密码.....	144
从介质打印.....	64
错误代码.....	240
错误信息.....	239

D

打印机作业验证.....	48
打印容量使用.....	65
带有电子签名的 PDF.....	122
登录（管理员）.....	19
登录的验证信息.....	34
电子签名.....	119
电子邮件加密.....	117

E

ESP 协议.....	124
-------------	-----

F

访问控制.....	95
服务模式锁定.....	232

G

更改固件结构.....	228
更新固件.....	228
固件有效性.....	231
管理员.....	12
管理员权限.....	14
管理员注册.....	16

H

环保计数器.....	222
------------	-----

I

IEEE 802.1X.....	139
设备证书.....	140
以太网.....	140
站点证书.....	139
IPP 验证密码.....	145
IPsec.....	123
IPsec telnet 设置命令.....	133
IPsec 设置.....	125

J

基本验证.....	31
加密密钥.....	82
加密密钥自动交换设置.....	125, 130
加密用户自定义设置和通讯簿.....	226
介质插槽使用.....	64

K

Kerberos 验证.....	36, 146
可使用的功能.....	62
扩展安全功能.....	225

L

LDAP 验证.....	43
--------------	----

M

每个用户的打印容量限制.....	65
密码策略.....	227
密码锁定功能.....	53

N

NTLM 验证.....	35
--------------	----

Q

启用/禁用协议.....	96
强制保存文件.....	171
清除所有内存.....	90
驱动程序加密密钥.....	144, 225
密钥强度.....	225

R

Remote 服务.....	228
日志文件管理-Web Image Monitor.....	174
日志信息.....	174

S

S/MIME.....	117
SNMPv1,v2 设置.....	227
SNMPv3.....	143
SSL/TLS.....	112
SSL/TLS 加密模式.....	114
扫描到介质.....	64
扫描仪功能的安全性.....	231
设备证书安装.....	110
设备证书创建.....	110
使用外部设备进行验证.....	56
数据覆盖.....	86
数据加密（通讯簿）.....	77
数据加密（硬盘）.....	79
锁定打印.....	162

T

通讯簿访问权限.....	75
--------------	----

W

Windows 验证.....	35
网络安全等级.....	103

X

系统状态检查.....	231
限制目的地的使用.....	226
限制添加用户目的地.....	227
限制显示用户信息.....	226

Y

验证当前作业.....	227
用户.....	25
用户代码验证.....	29
用户验证.....	26, 27
用于 SMTP 连接的 SSL.....	115

Z

增强安全性信息.....	233
增强文件保护.....	226
中间证书.....	111
注销（管理员）.....	21
自动清除内存.....	86
自动注销.....	55
自签证书.....	109

