SOPHOS
Security made simple.

Sophos Mobile

启动指南

产品版本号： 8

内容

1 关于本指南

本指南详细介绍了如何对 Sophos Mobile 进行设置，以便管理您的设备。

有关详细信息，请参阅 Sophos Mobile 管理员帮助。

本指南主要介绍 Android 和 iOS 这两种最常见的移动平台。这些设置可以按类似的方式应用于其他支持的操作系统。

2 Sophos Mobile 许可证

Sophos Mobile 提供了两种类型的许可证：

- Mobile Standard 许可证
- Mobile Advanced 许可证

使用Mobile Advanced类型的许可证，您可以管理 Sophos Mobile Security、Sophos Secure Workspace 和 Sophos Secure Email 应用。

有关通过 Sophos Mobile 管理 Sophos Mobile Security、Sophos Secure Workspace 和 Sophos Secure Email 的详细信息，请参阅 Sophos Mobile 管理员帮助。

作为超级管理员，可以在超级管理员客户中激活购买的许可证，并向单个客户分配所需数量的授权用户。

2.1 试用许可证

Sophos 为 Sophos Mobile 提供了免费试用。您可以在 Sophos 网站上注册，以便试用：http://www.sophos.com/zh-cn/products/free-trials/mobile-control.aspx.

试用许可证可用于管理最多五个用户，有效期为 30 天。

安装 Sophos Mobile 进行评估时，您唯一需要的是下载安装程序时用于注册的电子邮件地址。

2.2 将试用许可证升级为完整许可证

要将试用许可证升级为完整许可证，只需在 Sophos Mobile 中输入您的完整许可证密钥。有关详细信息，请参阅 Sophos Mobile 管理员帮助。

2.3 更新许可证

要更新您的许可证，您必须在 Sophos Mobile 中激活新的许可证密钥。有关详细信息，请参阅 Sophos Mobile 超级管理员指南。

3 有哪些重要步骤？

要开始使用 Sophos Mobile：

1. 以超级管理员身份登录 Sophos Mobile Admin。
2. 启动配置向导，执行 Sophos Mobile 服务器的初始配置。

> 注释
> 配置向导将包括一个用于申请试用许可证的选项。

3. 检查您的许可证。
4. 创建用于管理您设备的新客户。
5. 切换到新客户。
6. 为新客户创建管理员，并以该管理员身份登录 Sophos Mobile Admin。
7. 配置个人设置、管理员帐户的密码策略、技术支持联系人详细信息和自助服务门户设置。
8. 上传用于管理 iOS 设备的 Apple 推送通知服务证书。
9. 创建合规性策略。
10. 创建设备组。
11. 配置设备。
12. 更新自助服务门户设置，并添加自助服务门户测试用户。
13. 如果使用内部用户管理：通过创建用户或上传用户列表，添加用户。
14. 如果使用外部用户管理：配置 LDAP 目录的连接。
    这在 Sophos Mobile 超级管理员指南中有介绍。
15. 在自助服务门户中测试设备注册。

4 以超级管理员身份登录

要执行某些初始配置步骤，必须以安装 Sophos Mobile 时配置的超级管理员帐户身份登录 Sophos Mobile Admin。

1. 打开您在安装 Sophos Mobile 时配置的 Sophos Mobile Admin Web 地址。
2. 在登录对话框中，输入超级管理员客户名称和超级管理员的凭据，然后单击登录。

注释

以超级管理员身份登录时，将得到与超级管理员任务相适应的特殊版本的 Sophos Mobile Admin。

有关如何以超级管理员身份使用 Sophos Mobile Admin 的详细说明，请参阅 Sophos Mobile 超级管理员指南。

5 运行配置向导

安装后首次登录 Sophos Mobile Admin时，会启动配置向导，对某些服务器设置进行配置。

您需要提供：

- Mobile Standard 许可证密钥，或者附加的 Mobile Advanced 许可证密钥
- SSL/TLS 证书
- SMTP 凭据

> 注释
> 作为超级管理员，以后您可以在 Sophos Mobile Admin的系统设置页面对这些设置进行调整。要打开系统设置页面，请从侧边的菜单栏中，单击设置 > 设置 > 系统设置。

要运行配置向导：

1. 作为超级管理员首次登录 Sophos Mobile Admin时，将显示欢迎视图。单击下一步。
2. 在许可证视图中，输入您的 Mobile Standard 标准许可证密钥或申请试用许可证：
   - Mobile Standard 标准许可证密钥：

     输入 Mobile Standard 标准许可证密钥并单击激活后，可以选择是否输入 Mobile Advanced 高级许可证密钥。如果您购买了 Mobile Advanced 许可证，请在高级许可证密钥中输入该密钥。
   - 申请试用许可证：

     要申请试用许可证，请单击申请试用，并输入您为了从 www.sophos.com 下载 Sophos Mobile 安装程序而进行注册时所用的电子邮件地址。然后再次单击申请试用。

   > 注释
   > 您随时可以在 Sophos Mobile Admin中更改许可证设置。

   单击下一步。
3. 在 SSL/TLS 视图中，配置要用于在 Sophos Mobile 服务器和客户端之间保证 SSL 连接的证书。

   可以配置最多四个证书，因为（根据您的网络架构）从 Internet 或本地 Intranet 连接的客户端的不同证书可能正在使用。Sophos Mobile 服务器将把证书列表传送到客户端。建立 SSL 或 TLS 连接时，如果提供的证书包括在列表中，客户端将只信任服务器（证书锁定）。

   a) 单击自动发现证书。

      大多数情况下，自动发现功能可以找到当前在用的证书。

   b) 如果不能自动找到证书，可以通过单击上传文件并选择相应的 .CER 或 .DER 文件，手动上传证书。

   证书将显示在 SSL/TLS 视图中。

   > 重要提示
   > 修改或续订 SSL 证书后，请更新该列表。在任何时间，至少必须有一个有效的证书可用。否则，客户端将不会信任服务器，且不会连接到服务器。

4. 在 SMTP 视图中，配置 SMTP 服务器信息和登录凭据。必须配置 SMTP 才能向新用户发送电子邮件，向他们提供登录凭据。而且还需要对它进行配置，才能通过电子邮件进行注册。

选项	描述
SMTP 主机	SMTP 服务器地址。
连接端口	要连接的服务器端口。 注释 显示的连接类型（TLS、SSL 和未加密）仅显示标准端口使用情况。请参阅 SMTP 服务器的文档，了解使用的端口。
SMTP 用户	如果 SMTP 服务器要求，请输入允许连接的用户的名称。
SMTP 密码	SMTP 用户的密码。
邮件建立者	将显示在 Sophos Mobile 中的电子邮件“发件人”字段中的电子邮件地址。
发件人名称	将显示在“发件人”字段中的作者名称。 如果需要，可以在以后为每个客户配置不同的发件人名称（但不是电子邮件地址）。请参阅 Sophos Mobile 管理员帮助。
发送错误邮件	Sophos Mobile 将发送错误消息电子邮件，如在 APNs 证书过期时。
邮件收件人	输入将收到错误消息电子邮件的收件人的电子邮件地址。

注释
Sophos Mobile 不支持 SMTP 身份验证的 OAUTH 机制。更喜欢 OAUTH 的电子邮件提供商（如 Google Gmail）可能会将通过 Sophos Mobile 进行登录的尝试视为不安全。

5. 配置相关信息后，单击发送测试电子邮件，对电子邮件配置进行验证。
6. 单击保存。

6 激活 Mobile Advanced 许可证

使用 Mobile Advanced 高级许可证，可以使用 Sophos Mobile 管理 Sophos Mobile Security、Sophos Secure Workspace 和 Sophos Secure Email 应用。

如果在对 Sophos Mobile 进行初始配置时没有激活 Mobile Advanced 许可证，超级管理员以后可以通过 Sophos Mobile Admin 将它们激活：

1. 在侧边的菜单栏中，单击设置下的设置 > 系统设置。
2. 在许可证选项卡上，在高级许可证密钥中输入您的许可证密钥，然后单击激活。

密钥激活后，将显示许可证详细信息。

7 检查您的许可证

Sophos Mobile 采用基于用户的许可证授权方案。一个用户许可证对分配给该用户的所有设备都有效。每个未分配给用户的设备都需要一个许可证。

要检查可用的许可证：

1. 在侧边的菜单栏中，单击设置下的设置 > 系统设置。
2. 在系统设置页面上，单击许可证选项卡。

将显示以下信息：

- 最大许可证数目：可以管理的设备用户（和未分配的设备）的最大数目。

  如果超级管理员没有为客户设置配额，许可证的数量将受 Sophos Mobile 服务器的总量限制。
- 使用的许可证：在用的许可证数量。
- 有效期至：许可证的到期日期。
- 许可 URL：颁发有许可证的 Sophos Mobile 服务器的 URL。

如果您对显示的许可证信息有任何问题或疑问，请联系您的 Sophos 销售代表。

8 创建客户

要执行此任务，必须以超级管理员身份登录到 Sophos Mobile Admin。

1. 在侧边的菜单栏中，单击通知下的仪表板。
2. 单击创建客户。
3. 在编辑客户页面上，配置以下设置。

选项	描述
名称	客户的名称。
描述	描述客户帐户用途的文本。
最大许可证数目	可以为客户管理的设备用户和未分配设备的数目。
高级许可证	如果选中，客户可以使用 Sophos Mobile 管理 Sophos Mobile Security、Sophos Secure Workspace 和 Sophos Secure Email 应用。
有效期至	分配给客户的许可证的到期日期。超过此日期后，将不能再对为该客户管理的设备创建新的任务。
停用账户	如果选中，将不能登录到该客户。作为超级管理员，您仍然可以使用页面标题中的客户列表切换到客户的视图。 停用的帐户可以通过取消选择停用账户复选框再次激活。
激活的平台	选择可以注册设备的平台。
定位设备	选中允许用户让用户在其设备丢失或被盗时可以定位设备。选中允许管理员让管理员定位设备。
克隆设置	如果要让在超级管理员帐户中创建的所有配置文件、捆绑包和软件包在该客户的帐户中可用，请选中设置和软件包复选框。
用户目录	选择可供 Sophos Mobile 管理的自助服务门户 (SSP) 用户的数据源。 选项有： • 无。没有可用的 SSP、用户特定的配置文件或 LDAP 管理员：这将禁用自助服务门户用户帐户的创建，并禁用从 LDAP 目录对 Sophos Mobile Admin 的帐户进行搜索。 • 内部目录：使用针对 Sophos Mobile Admin 和自助服务门户的内部用户管理。有关详细信息，请参阅 Sophos Mobile 管理员帮助。 • 外部 LDAP 目录：除内部用户管理外，您还可以从 LDAP 目录搜索 Sophos Mobile Admin 和自助服务门户的帐户。单击配置外部 LDAP 可指定服务器详细信息。

4. 单击保存。

将创建客户。

9 切换到客户

要完成在前一部分创建的客户的初始配置，需要从超级管理员客户切换到该客户。

要切换到新客户的视图：

1. 在超级管理员视图的页面标题中，单击当前客户名称以打开可用客户的列表。在该列表中，超级管理员客户标记有星号，并显示在顶部。
2. 选择在前一节中创建的客户。

视图将更改为该客户的视图，也就是您以该客户的管理员帐户登录时得到的视图。

10 为客户创建管理员

1. 在侧边的菜单栏中，单击设置下的设置 > 管理员。
2. 在显示管理员页面上，单击创建管理员。
3. 在编辑管理员页面上，配置管理员的帐户详细信息。
   - 当外部 LDAP 目录选择为客户的用户目录时，可以单击通过 LDAP 查找用户以选择现有的 LDAP 帐户。
   - 当内部目录或无选择为客户的用户目录时，在登录名、名、姓、电子邮件地址和密码字段中输入相应的数据。

   指定的密码是一次性密码。首次登录时，将提示管理员修改密码。
4. 在角色列表中，选择管理员用户角色。
5. 单击保存创建管理员帐户。

要继续进行客户配置，请退出 Sophos Mobile Admin，然后使用刚创建的管理员的凭据（客户名称、登录名、一次性密码）再次登录。

11 配置设置

配置以下设置：

- 个人设置，例如您要管理的平台
- 密码策略
- 技术支持联系人详细信息
- 自助服务门户设置

11.1 配置个人设置

为了更有效地使用 Sophos Mobile Admin，您可以自定义用户界面，以只显示使用的平台。

> 注释
> 通过对平台进行配置，可以只更改当前登录用户的视图。不能在这里停用任何功能。

前提条件：您已经以为新客户创建的管理员身份登录 Sophos Mobile Admin。

1. 在侧边的菜单栏中，单击设置下的设置 > 常规，然后单击个人选项卡。
2. 配置以下设置：

选项	说明
语言	为 Sophos Mobile Admin选择语言。
时区	选择显示哪个时区的日期。
单位系统	选择长度值的单位系统（公制或英制）。
表格中每个页面的行数	选择要在每个页面中显示的最大表格行数。
显示扩展的设备详细信息	选中此复选框将显示设备的所有可用信息。自定义属性和内部属性选项卡将添加到显示设备页面上。
激活的平台	选择要为客户管理的平台： • Android • Android Things • iOS • Windows Mobile（包括 Windows Phone 8.1 和 Windows 10 Mobile 操作系统） • Windows • Windows IoT 根据选择的平台，将调整 Sophos Mobile Admin 的用户界面。只显示与所选平台相关的视图和功能。 注释 可用的平台取决于超级管理员配置中的平台设置。有关详细信息，请参阅 Sophos Mobile 超级管理员指南。

3. 单击保存。

11.2 配置密码策略

为加强密码安全性，请为 Sophos Mobile Admin 用户和自助服务门户配置密码策略。

注释
密码策略不适用于外部 LDAP 目录中的用户。有关外部用户管理的详细信息，请参阅 Sophos Mobile 超级管理员指南。

1. 在侧边的菜单栏中，单击设置下的设置 > 常规，然后单击密码策略选项卡。
2. 在规则下，可以定义密码要求，如有效密码必须包含的小写、大写或数字字符的最小数目。
3. 在设置下，配置以下设置：
   a) 更改密码的间隔天数（天）：输入密码过期之前的天数（1 和 730 之间），或将该字段保留为空以禁用密码过期。
   b) 不得重复使用的旧密码的数目：选择 1 和 10 之间的值，或选择 --- 禁用此限制。
   c) 登录尝试失败的最大次数：选择帐户被锁定之前可以尝试的失败登录次数（1 和 10 之间），或选择 --- 允许无限次失败的登录尝试。
4. 单击保存。

11.3 配置技术支持联系人详细信息

为支持有问题或疑问的用户，可以向他们提供有关如何联系技术支持的详细信息。在这里输入的信息将显示在 Sophos Mobile Control应用和自助服务门户中。

1. 在侧边的菜单栏中，单击设置下的设置 > 常规，然后单击技术联系人选项卡。
2. 为技术联系人输入必要的信息。
3. 单击保存。

11.4 配置自助服务门户设置

1. 在侧边的菜单栏中，单击设置下的设置 > 自助服务门户。
   将打开自助服务门户页面。
2. 在配置选项卡中，根据需要配置自助服务门户设置。

   如果在此阶段无法确定需要应用哪些设置，我们建议使用默认设置。

   有关设置的详细说明，请单击页面标题中的帮助。
3. 在使用条款选项卡上，单击编辑，输入移动策略免责声明或协议文本。

   此文本将在开始设备注册时显示。用户必须接受该文本，然后才可以进行注册。

   提示
   可以使用编辑器工具栏，将基本的 HTML 格式应用到文本。这也适用于下一步中所述的安装后文本。

4. 可选：在安装后文本选项卡上，单击编辑，输入设备注册结束时显示的文本。

可以使用此文本解释用户在注册后必须执行的步骤。

5. 单击保存。

12 Apple 推送通知服务证书

要使用 iOS 和 macOS 设备的内置移动设备管理 (MDM) 协议，Sophos Mobile 必须使用 Apple 推送通知服务 (APNs) 触发设备。

Sophos Mobile 按客户管理 APNs 证书。必须为使用的每个客户创建并上传证书。

APNs 证书的有效期为一年。

为方便续订 APNs 证书，超级管理员可以在一个步骤中续订所有使用相同证书的客户的证书。请参阅 Sophos Mobile 管理员帮助。

以下各节介绍使用自己的客户端证书访问 APNs 时，必须满足的要求和必须执行的步骤。

12.1 要求

为了与 Apple 推送通知服务 (APNs) 进行通信，必须允许以下端口的双向 TCP 数据流：

- Sophos Mobile 服务器需要连接到 gateway.push.apple.com:2195 TCP (17.0.0.0/8)
- 每个只有 Wi-Fi 访问权限的 iOS 设备需要连接到 *.push.apple.com:5223 TCP (17.0.0.0/8)

12.2 创建 APNs 证书

1. 在侧边的菜单栏上，在 设置 下，单击 安装 > 系统设置然后单击 APNs 选项卡。
   该选项卡上的说明将引导您完成必须执行的步骤，以便从 Apple 申请证书并将其上传到 Sophos Mobile。
2. 在下载证书签名请求步骤中，单击下载证书签名请求。
   将把证书签名请求文件 apple.csr 保存到您的本地计算机。签名请求文件特定于当前客户。
3. 您需要 Apple ID。即便您已经有 ID，我们还是建议您创新一个新的 ID 用于 Sophos Mobile。在创建 Apple ID 步骤中，单击创建一个新的 Apple ID。
   将打开一个 Apple 网页，您可以在其中为您的公司创建 Apple ID。

   > 注释
   > 将凭据存储在一个您的同事可以访问的安全地方。您的公司每年都需要这些凭据来续订证书。

4. 为方便您参考，在 APNs 选项卡顶部的 Apple ID 字段中输入您的新 Apple ID。
   当您每年续订证书时，始终必须使用相同的 Apple ID。
5. 在创建或续订 APNs 证书步骤中，单击 Apple 推送证书门户。
   将打开 Apple 推送证书门户。
6. 用您的 Apple ID 登录，并上传证书签名请求文件 apple.csr。
7. 下载 .pem APNs 证书文件，并将其保存到您的计算机上。
8. 在上传 APNs 证书步骤中，单击上传证书，然后浏览并找到您从 Apple 推送证书门户收到的 .pem 文件。
9. 单击保存，将 APNs 证书添加到 Sophos Mobile。

Sophos Mobile 读取证书，并在 APNs 选项卡上显示证书详细信息。

13 合规性策略

合规性策略可用于：

- 允许、禁止或强制执行设备的某些功能。
- 定义违反合规性规则时执行的操作。

您可以创建不同的合规性策略，并将它们分配到设备组。这样就可以对托管设备应用不同的安全级别。

提示
如果要同时管理公司和个人的设备，我们建议至少为这两类设备分别定义合规性策略。

13.1 创建合规性策略

1. 在侧边的菜单栏中，单击配置下的合规性策略。
2. 在合规性策略页面上，单击创建合规性策略，然后选择策略将基于哪个模板：
   - 默认模板：一组合规性规则，未定义操作。
   - PCI 模板，HIPAA 模板：分别基于 HIPAA 和 PCI DSS 安全标准的合规性规则和操作。

   您选择的模板不限制您的后续配置选项。
3. 为合规性策略输入名称，并选择性地输入描述。

对所有要求的平台重复以下步骤。

4. 确保每个选项卡上的启用平台复选框已选中。

   如果此复选框未选中，将不会对该平台的设备进行合规性检查。
5. 在规则下，为特定的平台配置合规性规则。

   有关每种设备类型可用规则的说明，请单击页面标题中的帮助。

   注释
   每条合规性规则有固定的严重性级别（高、中、低），通过蓝色图标指示。严重性有助于了解每条规则的重要性，以及违反该规则时应执行的操作。

   注释
   如果 Sophos Mobile 管理 Sophos 容器而非整个设备，则这些设备中只能使用合规性规则的一个子集。在突出显示规则中，选择管理类型以突出显示相关的规则。

6. 在如果违反规则下，定义违反规则时要执行的操作：

选项	说明
拒绝电子邮件	禁止访问电子邮件。 只有在超级管理员配置了与内部或独立 EAS 代理的连接后，才能执行此操作。请参阅 Sophos Mobile 超级管理员指南。

选项	说明
	此操作仅可用于 Android、iOS、Windows 和 Windows Mobile 设备。
锁定容器	禁用 Sophos Secure Workspace 和 Secure Email 应用。这将影响由这些应用管理的文档、电子邮件和 Web 的访问。 此操作只能在激活 Mobile Advanced 许可证后执行。 此操作仅可用于 Android 和 iOS 设备。
拒绝网络	禁止访问网络。 只有在超级管理员配置了网络访问控制后，才能执行此操作。请参阅 Sophos Mobile 超级管理员指南。
创建警报	创建警报。 警报将显示在警报页面上。
传输任务捆绑包	将特定的任务捆绑包传输到设备。 此操作仅可用于 Android、iOS、macOS 和 Windows 设备。 我们建议在此阶段将其设置为无。有关详细信息，请参阅 Sophos Mobile 管理员帮助。 重要提示 如果使用不正确，可能会导致任务捆绑包配置错误，甚至擦除设备。要为合规性规则分配正确的任务捆绑包，需要对系统有深入的了解。

7. 对所有要求的平台进行设置后，单击保存，以指定的名称保存合规性策略。
   新的合规性策略将显示在合规性策略页面上。

要使用合规性策略，可以将其分配给设备组。这将在下一节中介绍。

14 设备组

设备组用于对设备进行分类。它们可以帮助您有效地管理设备，因为您可以对设备组执行任务，而不是对单个设备。

一个设备始终属于一个设备组。当您将设备添加到 Sophos Mobile 时，您可以将其分配至设备组。

提示
仅在相同的操作系统中对设备进行分组。这样更便于用设备组执行安装和其他操作系统特定任务。

14.1 创建设备组

1. 在侧边的菜单栏中，单击管理下的设备组，然后单击创建设备组。
2. 在编辑设备组页面中，输入新设备组的名称和描述。
3. 在合规性策略下，选择应用到公司和个人设备的合规性策略。
4. 单击保存。

注释
设备组的设置包括启用 iOS 自动注册选项。此选项让您可以通过 Apple Configurator 注册 iOS 设备。有关详细信息，请参阅 Sophos Mobile 管理员帮助。

新设备组将创建，并显示在设备组页面上。

15 配置 iOS 设备

15.1 创建 iOS 设备配置文件

在此步骤中，您将为 iOS 设备的初始配置创建配置文件。

我们建议设置以下单独的配置文件：

- 密码策略和限制
- Exchange 帐户设置（如果需要）
- VPN 设置（如果需要）
- Wi-Fi 设置（如果需要）
- 根证书和客户端证书（如果需要）

> 注释
> Sophos Mobile 提供了两种为 iOS 设备创建配置文件的方法：
>
> - 直接在 Sophos Mobile Admin中创建配置文件。
> - 导入用 Apple Configurator 创建的配置文件。
>
> 本节介绍如何在 Sophos Mobile Admin中创建配置文件。有关如何导入使用 Apple Configurator 创建的配置文件的信息，请参阅 Sophos Mobile 管理员帮助

要为 iOS 设备创建密码策略和限制配置文件：

1. 在侧边的菜单栏中，单击配置下的配置文件，策略 > iOS。
2. 在配置文件和策略页面上，单击创建 > 设备配置文件。
3. 在编辑配置文件页面，配置以下设置：
   a) 名称：输入配置文件的名称。对于在自助服务门户中进行注册的过程中应用的配置文件，建议使用 iOS SSP 配置文件作为名称。
   b) 组织：输入配置文件的组织名称，如公司名称。
   c) 描述：为配置文件输入一段说明，如基本配置文件。
4. 要在配置文件中添加密码策略，请单击添加配置，然后选择密码策略。
5. 在密码策略页面中，配置要求的密码设置。
   有关设置的详细说明，请单击页面标题中的帮助。
6. 单击应用，保存设置。
   密码策略配置将显示在配置下的编辑配置文件页面中。
7. 要在配置文件中添加限制，请再次单击添加配置，然后选择限制。
8. 在限制页面中，选择要求的限制。

   有些限制需要特定的设备类型或 iOS 版本。这些要求将显示在每条限制的右侧。

   有关设置的详细说明，请单击页面标题中的帮助。
9. 单击应用，保存设置。
   限制配置将显示在配置下的编辑配置文件页面中。
10. 在编辑配置文件页面中，单击保存，保存配置文件。

配置文件将显示在配置文件和策略页面中，并且可以传输到 iOS 设备上。

如果需要，为 Exchange 帐户设置、VPN 设置、Wi-Fi 设置和安装的根证书和客户端证书创建额外的配置文件。

15.2 为 iOS 设备创建任务捆绑包

1. 在侧边的菜单栏中，单击配置下的任务捆绑包 > iOS。
2. 在任务捆绑包页面上，单击创建任务捆绑包。
   将显示编辑任务捆绑包页面。
3. 在相应字段中输入新的任务捆绑包的名称，并选择性地输入说明。
   当您每次保存任务捆绑包时，版本将自动递增。
4. 可选： 选中对合规性操作可选，以便在设备违反合规性规则时将任务捆绑包传送到设备上。请参阅合规性策略 （第 16 页）。

   > 注释
   > 编辑现有的任务捆绑包并且该任务捆绑包已用于合规性操作时，此选项将禁用。

5. 可选： 对于 iOS 任务捆绑包，如果选择忽略应用安装失败，即使在应用安装失败时也可以继续处理任务捆绑包。
   如果任务捆绑包不包含安装应用任务，此选项将禁用。
6. 单击创建任务，选择注册，然后输入任务的名称。单击应用，创建任务。
   在此处输入的名称将在处理该任务时显示在自助服务门户中。
7. 再次单击创建任务，并选择安装配置文件或分配政策。为任务提供一个有意义的名称，如安装密码策略配置文件，选中已经创建的配置文件。单击应用，创建任务。
8. 如果已经为 Exchange、VPN 或 Wi-Fi 设置配置了配置文件，请对每个配置文件重复前一步骤。
9. 可选： 在任务捆绑包中添加其他任务。

   > 提示
   > 可以使用任务列表右侧的排序箭头，更改任务的安装顺序。

10. 将所有需要的任务添加到任务捆绑包后，单击编辑任务捆绑包页面上的保存。

任务捆绑包可以进行传输。它将显示在任务捆绑包页面上。

16 配置 Android 设备

16.1 创建 Android 设备配置文件

在此步骤中，您将为 Android 设备的初始配置创建配置文件。

我们建议设置以下单独的配置文件：

- 密码策略和限制
- Exchange 帐户设置（如果需要）
- VPN 设置（如果需要）
- Wi-Fi 设置（如果需要）
- 根证书和客户端证书（如果需要）

1. 在侧边的菜单栏中，单击配置下的配置文件，策略 > Android。
2. 在配置文件和策略页面上，单击创建 > 设备配置文件。
3. 在编辑配置文件页面，配置以下设置：
   a) 名称：输入配置文件的名称。对于在自助服务门户进行注册的过程中应用的配置文件，建议使用 Android SSP 配置文件作为名称。
   b) 可选： 描述：为配置文件输入一段说明，如基本配置文件。
4. 要在配置文件中添加密码策略，请单击添加配置，然后选择密码策略。
   将打开密码策略页面。
5. 在密码类型字段中，选择要定义的密码类型，如复杂。
6. 配置要求的密码设置。
   可用的设置取决于选择的密码类型。有关所有设置的详细说明，请单击页面标题中的帮助。
7. 单击应用，保存设置。
   密码策略配置将显示在配置下的编辑配置文件页面中。
8. 要在配置文件中添加限制，请再次单击添加配置，然后选择限制。
9. 在限制页面中，选择要求的限制。

   有些限制需要特定的设备类型或 Android 版本。这些要求将显示在每条限制的右侧。

   有关设置的详细说明，请单击页面标题中的帮助。
10. 单击应用，保存设置。
    限制配置将显示在配置下的编辑配置文件页面中。
11. 在编辑配置文件页面中，单击保存，保存配置文件。

配置文件将显示在配置文件和策略页面中，并且可以传输到 Android 设备上。

如果需要，为 Exchange 帐户设置、VPN 设置、Wi-Fi 设置和安装的根证书和客户端证书创建额外的配置文件。

16.2 为 Android 设备创建任务捆绑包

1. 在侧边的菜单栏中，单击配置下的任务捆绑包 > Android。
2. 在任务捆绑包页面上，单击创建任务捆绑包。
   将显示编辑任务捆绑包页面。
3. 在相应字段中输入新的任务捆绑包的名称，并选择性地输入说明。

当您每次保存任务捆绑包时，版本将自动递增。

4. 可选： 选中对合规性操作可选，以便在设备违反合规性规则时将任务捆绑包传送到设备上。请参阅合规性策略 （第 16 页）。

   > 注释
   > 编辑现有的任务捆绑包并且该任务捆绑包已用于合规性操作时，此选项将禁用。

5. 可选： 对于 iOS 任务捆绑包，如果选择忽略应用安装失败，即使在应用安装失败时也可以继续处理任务捆绑包。

   如果任务捆绑包不包含安装应用任务，此选项将禁用。

6. 单击创建任务，选择注册，然后输入任务的名称。单击应用，创建任务。

   在此处输入的名称将在处理该任务时显示在自助服务门户中。

7. 再次单击创建任务，并选择安装配置文件或分配政策。为任务提供一个有意义的名称，如安装密码策略配置文件，选中已经创建的配置文件。单击应用，创建任务。
8. 如果已经为 Exchange、VPN 或 Wi-Fi 设置配置了配置文件，请对每个配置文件重复前一步骤。
9. 可选： 在任务捆绑包中添加其他任务。

   > 提示
   > 可以使用任务列表右侧的排序箭头，更改任务的安装顺序。

10. 将所有需要的任务添加到任务捆绑包后，单击编辑任务捆绑包页面上的保存。

任务捆绑包可以进行传输。它将显示在任务捆绑包页面上。

17 更新自助服务门户设置

在创建好用户在自助服务门户中注册其设备时要传输的任务捆绑包后，需要用所需的组设置更新自助服务门户设置：

1. 在侧边的菜单栏中，单击设置下的设置 > 自助服务门户，然后单击组设置选项卡。
2. 单击默认组设置。
   将打开编辑组设置对话框。
3. 在初始包-企业设备和初始包-个人设备列表中，选择为 Android 和 iOS 设备创建的任务包。
4. 对于应该在自助服务门户中可用的平台，选中激活复选框：
5. 在添加到设备组列表中，选择在自助服务门户中注册设备时要将设备添加到哪个组。
6. 单击应用。
7. 在组设置选项卡中，单击保存。

18 创建自助服务门户测试用户

要通过自助服务门户对设置进行测试，请为您自己创建一个自助服务门户用户帐户。将使用此帐户登录自助服务门户，并测试设备注册。

注释
此过程假定客户是通过内部用户管理创建的，请参阅创建客户 （第 9 页）。有关外部用户管理的详细信息，请参阅 Sophos Mobile 超级管理员指南。

要为自助服务门户创建测试用户帐户：

1. 在侧边的菜单栏中，单击管理下的用户，然后单击创建用户。
2. 配置所需的帐户详细信息。
   确保选中发送注册邮件。
3. 单击保存。

用户将添加到自助服务门户用户列表中，并向您在帐户详细信息中指定的电子邮件地址发送注册电子邮件。

19 通过自助服务门户测试设备注册

我们建议您在向用户推出自助服务门户前，通过自助服务门户对设备注册进行测试。

用您在创建自助服务门户测试用户 （第 24 页）中为自己创建的测试用户帐户登录自助服务门户，并对您要通过 Sophos Mobile 进行管理的所有平台执行注册测试。

20 将用户导入 Sophos Mobile

通过自助服务门户对设备注册进行测试后，可以将用户列表导入 Sophos Mobile。

用户导入只与内部用户管理相关。对于外部用户管理，分配给某些 LDAP 组的所有用户都可以登录到系统。

有关外部用户管理的详细信息，请参阅 Sophos Mobile 超级管理员指南。

可以通过导入 UTF-8 编码的逗号分隔值 CSV 文件添加新的自助服务门户用户，最多可添加 300 个用户。

注释

使用文本编辑器编辑 CSV 文件。如果使用 Microsoft Excel，输入的值可能无法正确处理。确保使用 .csv 扩展名保存该文件。

提示

可从导入用户页面中下载带有正确列名和列顺序的样本文件。

要从 CSV 文件导入用户：

1. 在侧边的菜单栏中，单击管理下的用户，然后单击导入用户。
2. 在导入用户页面上，选择发送注册邮件。
3. 单击上传文件，然后导航至准备好的 CSV 文件。
   将从文件中读入记录，并显示出来。
4. 如果数据的格式不正确或不一致，整个文件都不能导入。如果出现这种情况，请按相应记录旁边显示的错误消息对 CSV 文件的内容进行相应的修改，然后再次上传。
5. 单击完成以创建用户帐户。

用户将导入，并显示在显示用户页面上。他们将收到电子邮件，其中包括他们的自助服务门户登录凭据。

21 使用设备注册向导分配和注册新设备

使用设备注册向导很容易注册新设备。它提供了可以合并以下任务的工作流：

- 将新设备添加到 Sophos Mobile。
- 可选：将用户分配到设备。
- 注册设备。
- 可选：将任务捆绑包传输到设备。

要启动设备注册向导：

1. 在侧边的菜单栏中，单击管理下的设备，然后单击添加 > 注册向导。

   提示
   或者，通过单击添加设备小组件，从仪表板页面启动该向导。

2. 在输入用户搜索参数向导页面上，可以输入搜索条件以查找将要分配该设备的用户，或选择跳过用户分配以注册尚未分配给用户的设备。
3. 输入搜索条件后，向导将显示匹配用户的列表。选择所需的用户。
4. 在设备详细信息向导页面中，配置以下设置：

选项	说明
平台	设备平台。 只能选择对登录的客户启用的平台。
名称	Sophos Mobile 管理的设备的唯一名称。
描述	设备的可选描述。
电话号码	可选的电话号码。输入国际格式的号码，如 +491701234567。
电子邮件地址	用于接收注册说明的电子邮件地址。 如果为该客户配置了用户管理，则是分配给该设备的用户的电子邮件地址。 如果没有配置用户管理，请在此处输入电子邮件地址。
所有者	选择设备所有者类型：企业或个人。
设备组	选择设备将要分配到哪个设备组。如果还没有创建设备组，可以选择始终可选的默认设备组。

5. 选择在设备注册后将传送到设备的任务捆绑包。或选择仅注册设备以注册设备但不传送任务捆绑包。
   当您单击下一步后，设备将添加到 Sophos Mobile。
6. 在注册向导页面上，按说明完成注册操作。

   注释
   在 Mac 设备上，必须由将受到 Sophos Mobile 管理的用户执行注册程序。要安装注册配置文件，用户必须输入管理员密码。

7. 注册成功完成后，单击完成，关闭设备注册向导。

注释

- 完成所有选择后，可以关闭向导，不必等到完成按钮出现。将在后台创建并处理注册任务。

22 术语表

客户	管理设备的租户。
设备	要托管的设备（如智能手机、平板电脑或 Windows 10 设备）。
注册	使用 Sophos Mobile 进行设备注册。
企业应用商店	托管在 Sophos Mobile 服务器上的应用存储库。管理员可以使用 Sophos Mobile Admin，将应用程序添加到 Enterprise App Store。然后，用户可以使用 Sophos Mobile Control 应用，将这些应用安装在他们的设备上。
设置	在设备上安装 Sophos Mobile Control 应用的过程。
自助服务门户	Web 界面，允许用户注册自己的设备并执行其他任务，无需联系支持人员。
Mobile Advanced 许可证	使用 Mobile Advanced类型的许可证，您可以通过 Sophos Mobile 管理 Sophos Mobile Security、Sophos Secure Workspace 和 Sophos Secure Email 应用。
SMSec	Sophos Mobile Security 的缩写。
Sophos Mobile 客户端	安装在 Sophos Mobile 托管的设备上的 Sophos Mobile Control 应用。
Sophos Mobile 控制台	您用于管理设备的 Web 界面。
Sophos Mobile Security	适用于 Android 设备的安全应用。可以使用 Sophos Mobile 管理该应用程序，只要激活了 Mobile Advanced 类型的许可证。
Sophos Secure Email	一款针对 Android 和 iOS 设备的应用，它为管理电子邮件、日历和联系人提供了安全的容器。可以使用 Sophos Mobile 管理该应用程序，只要激活了 Mobile Advanced 类型的许可证。
Sophos Secure Workspace	一款针对 Apple iOS 和 Android 设备的应用，它提供的安全工作区可用于浏览、管理、编辑、共享、加密和解密来自不同存储提供程序的文档或贵公司分发的文档。可以使用 Sophos Mobile 管理该应用程序，只要激活了 Mobile Advanced 类型的许可证。
任务捆绑包	您可以创建一个包，将多项任务捆绑在一项事务中。可以捆绑所有必需的任务，让设备完全注册和运行。

23 技术支持

可以通过以下任意方式获得 Sophos 产品的技术支持：

- 访问 community.sophos.com/ 的 Sophos Community 论坛，并搜索遇到相同问题的其它用户。
- 访问 www.sophos.com/zh-cn/support.aspx 的 Sophos 技术支持知识库。
- 访问 www.sophos.com/en-us/support/documentation.aspx 下载产品的技术文档。
- 访问 https://secure2.sophos.com/support/contact-support/support-query.aspx 联系我们的技术支持团队。

24 法律声明