SOPHOS

Cybersecurity made simple.

Sophos Mobile

启动指南（Sophos Central）

产品版本号： 9.6

内容

1 关于本文档

本文档详细介绍了如何对 Sophos Mobile 进行设置，以便管理您的设备。

这些描述适用于 Sophos Central 中的 Sophos Mobile 产品。

有关此文档的其他版本，请参阅 Sophos Mobile 文档网页。

2 有哪些重要步骤？

要开始使用 Sophos Mobile：

1. 可选： 激活您的 Mobile Advanced 许可证以管理 Sophos Intercept X for Mobile、Sophos Secure Workspace 和 Sophos Secure Email。
2. 配置个人设置、技术支持联系人详细信息和自助服务门户设置。
3. 上传用于管理 iPhone、iPad 和 Mac 设备的 Apple 推送通知服务证书。
4. 可选： 设置独立的 EAS 代理，以筛选从托管设备到电子邮件服务器的电子邮件数据流。
5. 创建合规性策略。
6. 创建设备组。
7. 配置设备。
8. 更新自助服务门户设置。
9. 在自助服务门户中测试设备注册。

3 激活 Mobile Advanced 许可证

通过Mobile Advanced许可证，您可以使用 Sophos Mobile 管理 Sophos Intercept X for Mobile、Sophos Secure Workspace 和 Sophos Secure Email。

在 Sophos Central Admin 中激活 Mobile Advanced 许可证：

在 Sophos Central Admin 中，单击您的帐户名 (用户界面的右上角)，选择授权，然后在应用激活代码字段中输入您的许可证密钥。

密钥激活后，将显示许可证详细信息。

4 配置设置

配置以下设置：

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

4.1 配置个人设置

您可以根据自己的喜好调整 Sophos Mobile Admin 的外观。例如，您可以设置语言、时区或可见的设备平台。

注释
这些设置只影响您当前用于登录的管理员帐户。

1. 在侧边的菜单栏中，单击设置 下，单击 设置 > 常规然后单击 个人 选项卡。
2. 配置以下设置：

选项	说明
时区	显示日期的时区。
单位系统	长度单位（公制或英制）。
表格中每个页面的行数	每个表页显示的最大条目数。
专家模式	此设置开启附加功能： • 显示设备页面包括带有自定义设备属性的自定义属性选项卡。 • 显示设备页面包括带有附加属性设备报告的内部属性选项卡。 • 多个策略配置页面包括用于配置可选设置的额外设置部分。
激活的平台	您要查看的设备平台。 在 Sophos Mobile Admin 中，只显示与所选平台相关的页面和设置。

3. 单击保存。

4.2 配置 IT 部门联系人

提供 IT 部门联系人详细信息，以便用户遇到问题时可以寻求帮助。

您在此处输入的信息将显示在用户的设备上。

1. 在侧边的菜单栏中，单击设置 下，单击 设置 > 常规然后单击 IT 部门联系人 选项卡。

2. 输入联系人信息。
3. 单击保存。

5 设置 Android 管理模式

对于 Android 设备，您可以选择Android 企业和 设备管理员 (旧功能)管理模式。

要设置 Android 管理模式，请执行以下操作：

1. 在侧边的菜单栏中，选择设置下的设置 > Android 设置，然后选择Android选项卡。
2. 在管理模式中，选中Android 企业。
3. 单击保存。

接下来，为您的组织设置 Android Enterprise。

5.1 设置 Android 企业 - 概述

要为您的组织设置 Android 企业，您可以选择以下不同方案中的一种：托管的 Google Play 帐户方案是设置 Android 企业最简单的方法，将在本文档中介绍。

有关其他 Android 企业方案的详细信息，请参阅Sophos Mobile管理员帮助。

相关信息
Sophos Mobile 管理员帮助

5.2 设置 Android 企业 (托管的 Google Play 帐户方案)

Sophos Mobile 将引导您完成为组织设置 Android 企业的过程。

1. 在侧边的菜单栏中，选择设置下的设置 > Android 设置，然后选择Android 企业选项卡。
2. 选择配置。
3. 选择“托管的 Google Play 帐户”方案，然后选择下一步。
4. 选择注册帐户。
   这会将您重定向至您将组织注册到 Android 企业的 Google 网站。
5. 使用您的 Google 帐户登录 Google 网站。

   注释
   为此，我们建议您创建一个新的 Google 帐户。

6. 在 Google 网站上，按照步骤注册您的组织。

   提示
   在指定您的组织名称时，我们建议您包含 Sophos Mobile。例如：

   Organization name (Sophos Mobile)

   完成注册步骤后，Google 网站会将您重定向回 Sophos Mobile。
7. 在 Sophos Mobile 中，选择完成设置完成注册过程。

6 Apple 推送通知服务证书

要使用 iPhone、iPad 和 Mac 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。

APNs 证书的有效期为一年。

6.1 创建 APNs 证书

1. 在侧边的菜单栏中，单击设置 下，单击 设置 > Apple 设置然后单击 APNs 选项卡。
2. 单击APNs 证书向导。
3. 在模式页面上，单击创建新的 APNs 证书。
4. 在CSR页面上，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。
5. 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Apple ID页面上，单击在 Apple 门户中创建 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。

6. 在向导中，将新的 Apple ID 输入 Apple ID 字段。
7. 在证书页面上，单击在 Apple 门户中创建证书。
   将打开 Apple 推送证书门户。
8. 用您的 Apple ID 登录，并上传证书签名请求文件 apple.csr。
9. 下载 .pem APNs 证书文件，并将其保存到您的计算机上。
10. 在上传页面上，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。
11. 单击保存。

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

7 独立的 EAS 代理

您可以设置 EAS 代理，以控制托管设备对电子邮件服务器的访问。您的托管设备的电子邮件数据流将通过该代理进行传输。您可以阻止设备，如违反合规性规则的设备访问电子邮件。

必须将设备配置为使用 EAS 代理作为接收和发送电子邮件的电子邮件服务器。如果设备在 Sophos Mobile 中是已知设备，并且与要求的策略相匹配，EAS 代理将只转发数据流到实际的电子邮件服务器。这可以确保更高的安全性，因为电子邮件服务器不需要从 Internet 访问，并且只有经过授权（经过正确配置，如按密码原则）的设备可以访问。此外，还可以配置 EAS 代理，以阻止来自特定设备的访问。

EAS 代理可以单独从 Sophos Mobile 下载和安装。它通过 HTTPS Web 接口与 Sophos Mobile 服务器通信。

有关独立 EAS 代理支持的邮件服务器的列表，请参阅Sophos Mobile 发行说明。

注释
因为 macOS 不支持 ActiveSync 协议，因此您不能使用 EAS 代理来筛选来自 Mac 设备的电子邮件数据流。

功能

- 支持多个 Microsoft Exchange 或 IBM Notes Traveler 电子邮件服务器。可以为每个电子邮件服务器设置一个 EAS 代理实例。
- 支持负载平衡器。可以在多台计算机上设置独立的 EAS 代理实例，然后使用负载平衡器在它们中间分配客户端请求。
- 支持基于证书的客户端身份验证。可以选择来自证书颁发机构 (CA) 的证书，客户端证书必须从该证书派生出来。
- 支持通过 PowerShell 控制电子邮件访问。在这种方案下，EAS 代理服务通过 PowerShell 与电子邮件服务器进行通信，从而控制您的托管设备的电子邮件访问。电子邮件数据流将直接从设备传输到电子邮件服务器，不通过代理进行传输。请参阅通过 PowerShell 设置电子邮件访问控制 （第 11 页）。
- EAS 代理会记住设备状态 24 小时。如果 Sophos Mobile 服务器离线，例如在更新过程中，电子邮件数据流将根据最后已知的设备状态进行筛选。24 小时后，将阻止所有电子邮件数据流。

注释
对于非 iOS 设备，由于 IBM Notes Traveler 协议的要求，独立 EAS 代理的筛选能力会受到限制。非 iOS 设备上的 Traveler 客户端不会随每个请求发送设备 ID。即使 EAS 代理不能验证设备是否获得授权，不带设备 ID 的请求也会转发到 Traveler 服务器。

7.1 下载 EAS 代理安装程序

1. 登录 Sophos Central Admin 并转到 Mobile。
2. 在侧边的菜单栏中，单击设置 下，单击 设置 > Sophos 设置然后单击 EAS 代理 选项卡。
3. 单击外部下的链接下载 EAS 代理安装程序。

将安装程序文件保存到您的本地计算机。

7.2 安装独立的 EAS 代理

前提条件：

- 所有必需的电子邮件服务器都可以访问。EAS 代理安装程序将不会配置与不可用服务器的连接。
- 您是准备安装 EAS 代理的计算机上的管理员。
- 您知道 Sophos Mobile 服务器的 URL。请参阅确定 Sophos Mobile 服务器 URL （第 15 页）。

注释
Sophos Mobile 部署指南中包含将独立的 EAS 代理集成到贵公司基础设施的示意图。在安装和部署独立的 EAS 代理前，我们建议您阅读该信息。

1. 运行 Sophos Mobile EAS Proxy Setup.exe 以启动 Sophos Mobile EAS Proxy - Setup Wizard。
2. 在 Choose Install Location 页面上，选择目标文件夹并单击 Install 开始安装。
   安装完成后，将自动启动 Sophos Mobile EAS Proxy - Configuration Wizard，并引导您完成配置步骤。
3. 在 Sophos Mobile server configuration 对话框中，输入 EAS 代理将要连接的 Sophos Mobile 服务器的 URL。

   如果需要，请选择 Use proxy server 配置 EAS 代理用于连接 Sophos Mobile 服务器的代理服务器。

   您还应选中 Use SSL for incoming connections (Clients to EAS Proxy)，以保护客户端和 EAS 代理之间的通信。

   除 EAS 代理凭据外，如果还想让客户端使用证书进行身份验证，则可以选中 Use client certificates for authentication。这将为连接添加额外一层安全性。
4. 如果您之前选中了 Use SSL for incoming connections (Clients to EAS Proxy)，将显示 Configure server certificate 页面。在此页面上，可以创建或导入用于安全 (HTTPS) 访问 EAS 代理的证书。

   - 如果您还没有信任的证书，请选择 Create self-signed certificate。
   - 如果已有信任的证书，请单击 Import a certificate from a trusted issuer，并从列表中选择以下其中一个选项：
     - PKCS12 with certificate, private key and certificate chain (intermediate and CA)
     - Separate files for certificate, private key, intermediate and CA certificate
5. 在下一页面上，根据所选证书的类型，输入相应的证书信息。

   注释
   对于自签名证书，需要指定可以从客户端设备访问的服务器。

6. 如果您之前选中了 Use client certificates for authentication，将显示 SMC client authentication configuration 页面。在此页面上，选择来自证书颁发机构 (CA) 的证书，客户端证书必须从该证书派生出来。
   当客户端尝试连接时，EAS 代理将检查客户端证书是否是由此处指定的 CA 派生出来的。
7. 在 EAS Proxy instance setup 页面上，配置一个或多个 EAS 代理实例。
   - Instance type: 选择 EAS proxy。
   - Instance name: 用于标识该实例的名称。

- Server port: EAS 代理用于传入电子邮件数据流的端口。如果设置多个代理实例，每个实例必须使用不同的端口。
- Require client certificate authentication: 电子邮件客户端连接到 EAS 代理时，必须自己进行身份验证。
- ActiveSync server: 代理实例将连接的 Exchange ActiveSync 服务器实例的名称或 IP 地址。
- SSL: 代理实例和 Exchange ActiveSync 服务器之间的通信受到 SSL 或 TLS 的保护（取决于服务器支持的类型）。
- Allow EWS (Sophos Secure Email): 允许邮件客户端请求访问 Exchange 服务器的 Exchange Web 服务 (EWS) 界面。

  仅当您在 iPhone 和 iPad 上使用 Sophos Secure Email 时才开启此设置。
- Enable Traveler client access: 仅在需要允许非 iOS 设备上的 IBM Notes Traveler 客户端访问时选中此复选框。

8. 输入实例信息后，单击 Add 将实例添加到 Instances 列表中。

   安装程序将为每个代理实例创建一个证书，需要将该证书上传到 Sophos Mobile 服务器。单击 Add 后，将打开一个消息窗口，解释如何上传证书。
9. 在消息窗口中，单击 OK。
   将打开一个对话框，显示创建的证书所在的文件夹。

   注释
   也可以通过选择相应的实例，并单击 EAS Proxy instance setup 页面上的 Export config and upload to Sophos Mobile server 链接，打开该对话框。

10. 记录证书文件夹。将证书上传到 Sophos Mobile 时，您需要此信息。
11. 可选： 再次单击 Add 并配置其他 EAS 代理实例。
12. 配置所有要求的 EAS 代理实例后，单击 Next。
    将测试您输入的服务器端口，并配置 Windows 防火墙的入站规则。
13. 在 Allowed mail user agents 页面上，可以指定允许连接到 EAS 代理的邮件用户代理 (即电子邮件客户端应用程序)。当客户端使用未指定的电子邮件应用程序连接到 EAS 代理时，请求将被拒绝。
    - 选择 Allow all mail user agents 配置无限制。
    - 选择 Only allow the specified mail user agents，然后从列表中选择邮件用户代理。单击 Add 将记录添加到允许代理列表中。对所有允许连接到 EAS 代理的邮件用户代理，重复此操作。
14. 在 Sophos Mobile EAS Proxy - Configuration Wizard finished 页面上，单击 Finish 关闭配置向导并返回安装向导。
15. 在安装向导中，确保选中 Start Sophos Mobile EAS Proxy server now 复选框，然后单击 Finish 完成配置，并开始首次启动 Sophos Mobile EAS 代理。

要完成 EAS 代理配置，请把为每个代理实例创建的证书上传到 Sophos Mobile：

16. 登录 Sophos Central Admin 并转到 Mobile。
17. 在侧边的菜单栏中，单击设置 下，单击 设置 > Sophos 设置然后单击 EAS 代理 选项卡。
18. 在外部下，单击上传文件。上传配置期间创建的证书。

    如果您设置了多个实例，请对所有实例证书重复此操作。
19. 单击保存。
20. 在 Windows 中，打开服务对话框并重新启动 EASProxy 服务。

这样就完成了独立 EAS 代理的初始设置。

注释
每天，EAS 代理日志记录都会移入一个新文件，命名方式为 EASProxy.log.yyyy-mm-dd。这些日常的日志文件不会自动删除，因此随着时间的推移可能会导致磁盘空间问题。我们建议设置一个过程，将日志文件移动到备份位置。

7.3 通过 PowerShell 设置电子邮件访问控制

如果在 PowerShell 模式下设置独立 EAS 代理，它将通过 PowerShell 连接到您的 Exchange 邮件服务器，并根据设备的合规性状态设置电子邮件访问。

在 PowerShell 模式下，邮件数据流直接从 Exchange 邮件服务器传输到您的设备，不使用代理。有关通信流的示意图，请参阅Sophos Mobile 技术指南。

PowerShell 模式的优点：

- 对于来自您的设备的传入电子邮件数据流，您不需要在 Sophos Mobile 服务器上为其打开端口。
- 您可以阻止未注册到 Sophos Mobile 的设备访问电子邮件。

Exchange 邮件服务器可以是 Exchange Server 或 Exchange Online (Office 365 的一部分)。支持的版本有：

- Exchange Server 2013
- Exchange Server 2016
- 采用 Exchange Online 方案的 Office 365

限制
因为 macOS 不支持 ActiveSync 协议，因此您不能使用 PowerShell 来控制 Mac 设备的电子邮件访问权限。

要通过 PowerShell 设置电子邮件访问控制，请按下述内容操作。

相关信息
Sophos Mobile 技术指南 (Sophos Central)

配置 PowerShell

1. 可选： 如果需要，请在要安装 EAS 代理的计算机上安装 Windows PowerShell。
2. 以管理员身分打开 PowerShell，并运行以下命令：

   Set-ExecutionPolicy RemoteSigned

Exchange Server 需要额外的配置：

3. 打开 Exchange 命令行管理程序。
4. 设置 PowerShell 执行策略：

   Set-ExecutionPolicy RemoteSigned

5. 获取 PowerShell 虚拟目录的名称：

   Get-PowerShellVirtualDirectory -Server <服务器名称>

   <服务器名称>是安装 Exchange Server 的计算机的名称。

   在标准安装中，PowerShell 虚拟目录为 PowerShell (Default Web Site)。

6. 为 PowerShell 虚拟目录设置基本身份验证：

   ```
   Set-PowerShellVirtualDirectory -Identity "PowerShell (Default Web Site)" -
   BasicAuthentication $true
   ```

相关信息

安装 Windows PowerShell (Microsoft 文档)

打开 Exchange 命令行管理程序 (Microsoft 文档)

创建服务帐户

服务帐户是 Exchange 邮件服务器上的一个特殊用户帐户，Sophos Mobile 用它来执行 PowerShell 命令。

1. 登录到相关的管理控制台：
   - 对于 Exchange Server：Exchange 管理中心
   - 对于 Exchange Online：Office 365 管理中心
2. 创建用户帐户。
   - 使用用户名（如 smc_powershell）标识帐户用途。
   - 关闭要求用户在下次登录时更改其密码的设置。
   - 删除自动分配给该新帐户的所有 Office 365 许可证。服务帐户不需要许可证。
3. 创建一个新的角色组，并为其分配所需的权限。
   - 使用如 smc_powershell 之类的角色组名称。
   - 添加邮件收件人和组织客户端访问角色。
   - 将该用户帐户添加为成员。

配置 PowerShell 连接

1. 像您安装独立 EAS 代理一样，使用设置助手。在 EAS Proxy instance setup 页面上，配置以下设置：
   - Instance type: 选择 PowerShell Exchange/Office 365。
   - Instance name: 用于标识该实例的名称。
   - Exchange server: 对于 Exchange Server，输入服务器的名称或 IP 地址。

     对于 Exchange Online，如果您使用的是全球版 Office 365 服务，请输入 outlook.office365.com。对于其他服务，如 Office 365 Germany，您可以在 Microsoft 文档连接到 Exchange Online PowerShell 中找到相应地址。

     请勿在名称中输入协议 https:// 或后缀 /powershell-liveid。设置向导会自动添加这些内容。
   - Allow all certificates: EAS 代理不验证服务器证书。例如，如果您使用的是带有自签名证书的 Exchange Server，可选中此选项。

     警告
     此设置会降低邮件服务器连接的安全性。请仅在您的网络环境需要时选择。

- Service account: 您在 Exchange Server 或 Exchange Online 管理控制台中创建的用户帐户的名称。
- Password: 该用户帐户的密码。

2. 单击 Add 将实例添加到 Instances 列表中。
3. 重复前面的步骤设置到其他 Exchange Server 实例的 PowerShell 连接。
4. 完成设置。
5. 可选： 如果需要，配置 EAS 代理用于连接到 Exchange Server 或 Exchange Online 的代理服务器。在您安装 EAS 代理的计算机上，使用以管理员身份运行选项打开命令提示符，然后键入以下命令：

   netsh winhttp set proxy <服务器名称或 IP>:<端口>

   警告
   此命令用于配置系统范围的代理。计算机上运行的其他程序可能会受到它的影响。

相关信息
安装独立的 EAS 代理 （第 9 页）
连接到 Exchange Online PowerShell (Microsoft 文档)

上传 PowerShell 证书

将 PowerShell 连接的证书上载到 Sophos Mobile。

1. 登录 Sophos Central Admin 并转到 Mobile。
2. 在侧边的菜单栏中，单击设置 下，单击 设置 > Sophos 设置然后单击 EAS 代理 选项卡。
3. 可选： 在 常规 下，选择 对 Sophos Secure Email 的限制 以限制 Sophos Secure Email 应用的电子邮件访问权限，可用于 Android 和 iOS。
4. 在外部下，单击上传文件。上传配置期间创建的证书。

   如果您设置了多个实例，请对所有实例证书重复此操作。
5. 单击保存。
6. 在 Windows 中，打开服务对话框并重新启动 EASProxy 服务。

7.4 阻止非托管设备访问电子邮件

您可以阻止未注册到 Sophos Mobile 的设备访问电子邮件。

前提条件：您已在 PowerShell 模式下设置独立 EAS 代理。

在这些说明中，Exchange 指的是您的本地 Exchange 服务器或在 Office 365 中包含的 Exchange Online 计划。

您可以配置 Exchange 以隔离非托管设备。用户将收到电子邮件，告诉他们将设备注册到 Sophos Mobile。设备注册后，将自动从隔离区中删除。

警告
在生产环境中应用这些设置之前，请确保您的设备已注册并可以与 Sophos Mobile 同步。默认情况下，将隔离所有设备，只有当 Sophos Mobile 服务器将设备设置为合规时，才能访问电子邮件。

此外，如果 EAS 代理不知道注册设备的合规性状态，这些设备也会被隔离。当设备长时间未与 Sophos Mobile 同步或 EAS 代理无法与 Sophos Mobile 服务器通信时，可能会发生这种情况。

要阻止非托管设备访问电子邮件：

1. 打开 Exchange 命令行管理程序（如果您有 Exchange 服务器）或连接到 Exchange Online PowerShell。

   要了解详细信息，请参阅相关信息中的链接。
2. 运行以下命令（一行）：

```
Set-ActiveSyncOrganizationSettings -DefaultAccessLevel quarantine
-UserMailInsert "Please enroll your device with Sophos Mobile."
```

   您使用 -UserMailInsert 指定的文本将添加到用户的设备被隔离时 Exchange 发送给用户的通知电子邮件中。

有关控制电子邮件访问的一般详细信息，请参阅 Microsoft 文档使用允许/阻止/隔离列表控制 Exchange ActiveSync 设备访问。

相关信息

在 PowerShell 模式下设置独立 EAS 代理 （第 11 页）
如果在 PowerShell 模式下设置独立 EAS 代理，它将通过 PowerShell 连接到您的 Exchange 邮件服务器，并根据设备的合规性状态设置电子邮件访问。

打开 Exchange 命令行管理程序 (Microsoft 文档)

连接到 Exchange Online PowerShell (Microsoft 文档)

使用允许/阻止/隔离列表控制 Exchange ActiveSync 设备访问 (Microsoft 文档)

7.5 配置与独立 EAS 代理服务器的连接

要配置 Sophos Mobile 与独立 EAS 代理之间的连接，请将 EAS 代理服务器的证书上传到 Sophos Mobile。该证书是您配置 EAS 代理实例时生成的。

有关安装和配置独立 EAS 代理的信息，请参阅独立的 EAS 代理 （第 8 页）。

警告
如果 EAS 代理服务在您上传证书前已启动，Sophos Mobile 将会拒绝连接到该服务器，且该服务无法启动。

要上传独立 EAS 代理的证书：

1. 在侧边的菜单栏中，单击设置 下，单击 设置 > Sophos 设置然后单击 EAS 代理 选项卡。
2. 可选： 在 常规 下，选择 对 Sophos Secure Email 的限制 以限制 Sophos Secure Email 应用的电子邮件访问权限，可用于 Android 和 iOS。
3. 单击 外部 下的 上传文件，找到证书文件。

   如果您设置了多个 EAS 代理实例，请对所有实例重复此操作。
4. 单击保存。

5. 在 Windows 中，打开服务对话框并重新启动 EASProxy 服务。

7.6 确定 Sophos Mobile 服务器 URL

配置独立的 EAS 代理需要 Sophos Mobile 服务器 URL。该值显示在 Sophos Mobile 系统设置中。

1. 登录 Sophos Central Admin 并转到 Mobile。
2. 在侧边的菜单栏中，单击设置 下，单击 设置 > Sophos 设置然后单击 EAS 代理 选项卡。

Sophos Mobile 服务器的 URL 显示在外部下。

8 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。

8.1 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。 只有配置了与独立 EAS 代理的连接后，才能执行此操作。请参阅配置与独立 EAS 代理服务器的连接 （第 14 页）。

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。 此操作仅适用于 Android 设备、iPhone 和 iPad。
设置健康状况	选择设备违反此规则时获取的健康状况（红色、黄色、绿色）。如果设备违反多个规则，它将从与最坏健康状况相关的规则获取其健康状况。 Sophos Mobile 向 Sophos Wireless 报告健康状况。根据您的 Sophos Wireless 配置，网络访问权限可能会受到限制。 如果您开启了 Synchronized Security，此操作将适用于 Android 设备、iPhone 和 iPad。
创建警报	触发警报。 警报将显示在 Sophos Central Admin 的警报页面上。
传输任务捆绑包	将特定的任务捆绑包传输到设备。 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。 警告 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。

注释
当 Android Enterprise 完全托管设备不合规时，将禁用所有应用。

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。

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。

9 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。

9.1 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 iPhone 和 iPad。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。

10 开始使用设备策略

策略启动向导帮助您为所有平台创建基本的设备策略。以后您可以加强这些策略。

限制
这些说明不适用于 Chrome 设备。

要使用策略启动向导创建策略：

1. 在仪表板上，单击入门任务小组件中的策略启动向导。

   提示
   如果您找不到该小组件，请单击添加小组件 > 开始使用。

2. 在平台页面上，选择您要为其创建策略的设备平台。
   选择 Android 和 iOS 和 iPadOS。
3. 对于Android，您可以选择管理模式。
   此设置影响可用的策略类型。我们建议您使用Android 企业模式。
4. 在策略页面上，配置以下设置：
   a) 为策略输入一个名称。
      将为每个平台创建一个该名称的策略。
   b) 选择该策略管理的区域。
      如果不选中某个复选框，将跳过相应的向导页面。您可以稍后配置跳过的区域（以及其他设置）。
      我们建议您至少选择密码要求和限制。
5. 在密码页面上，配置设备密码的要求。
6. 在限制页面上，配置应用于设备的限制，如关闭相机或其他可能存在安全风险的设备功能。
7. 在Wi-Fi页面上，配置与您的公司 Wi-Fi 网络的连接。
   如果您的 Wi-Fi 网络使用 WPA/WPA2 PSK 以外的安全类型，您可以稍后更改该设置。
8. 在电子邮件页面上，配置与您的公司 Microsoft Exchange 电子邮件服务器的连接。
   占位符 %_USERNAME_% 和 %_EMAILADDRESS_% 将被分配给设备的用户的用户名和电子邮件地址代替。
9. 单击完成。

向导将为您选择的每个平台创建一个策略。

要查看策略，请单击侧边菜单栏中的策略，然后单击设备平台。

要修改管理的区域，请单击策略的名称，然后单击添加配置。

您必须先为您的组织设置 Android Enterprise，然后才能注册设备。请参阅 Sophos Mobile 管理员帮助。

11 为 Android 设备创建任务捆绑包

您可以为要管理的 Android、iOS 和其他设备平台创建单独的任务捆绑包。

要为您的 Android 设备创建注册任务捆绑包：

1. 在侧边的菜单栏中，选择配置下的任务捆绑包 > Android。
2. 在任务捆绑包页面上，选择创建任务捆绑包。
3. 在编辑任务捆绑包页面上，为任务捆绑包输入名称，并选择性地输入描述。
   当您每次保存任务捆绑包时，版本将自动递增。
4. 可选： 如果您选中对于合规性操作可选，则可在设备不合规时将任务捆绑包传递到设备上。
   您可以在合规性策略中对此进行配置。
5. 选择添加任务 > 注册。系统将指导您将注册任务添加到任务捆绑包中。
   a) 可选： 更改任务的名称。
      设备注册后，该名称将显示在自助服务门户中。
   b) 选择注册类型。
      要使用此任务捆绑包注册 Android 企业完全托管设备，请选择全设备。
   c) 在下一页面上，选择设备注册时将分配给设备的策略。
      将仅显示与您选择的注册类型相匹配的策略。
   d) 选择完成。
6. 可选： 选择添加任务 > 分配策略将更多策略添加到任务捆绑包（例如，如果您为 Exchange、VPN 或 Wi-Fi 设置配置了单独的策略）。
7. 可选： 将更多任务添加到任务捆绑包中，例如，在设备上安装应用或显示消息。
8. 可选： 使用任务列表右侧的箭头图标更改任务的安装顺序。

12 为 iPhone 和 iPad 创建任务捆绑包

您可以为要管理的 Android、iOS 和其他设备平台创建单独的任务捆绑包。

要为您的 iPhone 和 iPad 设备创建注册任务捆绑包：

1. 在侧边的菜单栏中，选择配置下的任务捆绑包 > iOS 和 iPadOS。
2. 在任务捆绑包页面上，选择创建任务捆绑包。
3. 在编辑任务捆绑包页面上，为任务捆绑包输入名称，并选择性地输入描述。
   当您每次保存任务捆绑包时，版本将自动递增。
4. 可选： 如果您选中对于合规性操作可选，则可在设备不合规时将任务捆绑包传递到设备上。
   您可以在合规性策略中对此进行配置。
5. 可选： 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。
   此选项仅在任务捆绑包包含安装应用任务时可用。
6. 选择添加任务 > 注册。系统将指导您将注册任务添加到任务捆绑包中。
   a) 可选： 更改任务的名称。
      设备注册后，该名称将显示在自助服务门户中。
   b) 选择注册类型。
      要使用此任务捆绑包注册完全托管设备，请选择完全 MDM。
   c) 在下一页面上，选择设备注册时将分配给设备的策略。
      将仅显示与您选择的注册类型相匹配的策略。
   d) 选择完成。
7. 可选： 选择添加任务 > 分配策略将更多策略添加到任务捆绑包（例如，如果您为 Exchange、VPN 或 Wi-Fi 设置配置了单独的策略）。
8. 可选： 将更多任务添加到任务捆绑包中，例如，在设备上安装应用或显示消息。
9. 可选： 使用任务列表右侧的箭头图标更改任务的安装顺序。

13 创建自助服务门户配置

通过自助服务门户配置，您可以配置用户可以注册的设备类型、注册详细信息以及他们可以在自助服务门户中执行的设备操作。

您可以对不同的用户使用不同的自助服务门户配置。为此，请将用户添加到用户组，并将组与配置相关联。您可以在相关信息中找到有关用户组的详细信息。

如果用户属于多个与自助服务门户配置相关联的组，将应用优先级最高的配置。

要创建自助服务门户配置：

1. 在侧边的菜单栏中，选择设置下的设置 > 自助服务门户。
2. 选择注册文本，然后添加使用条款文本和注册后文本。
   将这些文本分配给自助服务门户配置后，它们将分别在注册前后显示。
3. 在自助服务门户配置页面上，选择添加创建配置。
4. 配置以下设置：

选项	描述
姓名	配置的名称。 在自助服务门户中，用户通过这个名称选择配置。
用户组	选择添加，然后输入用户组。配置将应用于该组的所有成员。
最大设备数目	用户可以在自助服务门户中注册的最大设备数目。
操作	选择显示，然后选择用户可以在自助服务门户中执行的管理操作。

5. 选择添加 > Android。
6. 在配置平台设置对话框中，配置以下设置：

选项	描述
显示名称	平台设置的名称。 在自助服务门户中，用户通过这个名称选择注册类型。
描述	平台设置的描述。 此描述将显示在自助服务门户中的名称旁边。
所有者	使用此配置注册的设备的所有者模式（公司或个人）。
设备组	向其添加设备的设备组。
注册包	选择您创建的 Android 任务捆绑包。
使用条款	要在注册之前在自助服务门户中显示的文本。 将此字段留空将不显示文本。 用户必须同意该文本，才能继续注册。

选项	描述
注册后文本	要在注册之后在自助服务门户中显示的文本。 将此字段留空将不显示文本。

7. 选择应用，将平台设置添加到自助服务门户配置。
8. 选择添加 > iOS 和 iPadOS，然后重复对 Android 执行的配置步骤。
9. 在编辑自助服务门户配置页面上，选择保存。

始终会有一个 Default 配置。此配置的优先级最低，因此只有在没有其他配置与用户匹配时才会使用。

14 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。

15 使用添加设备向导

使用添加设备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。

1. 在侧边的菜单栏中，单击管理下的设备，然后单击添加 > 添加设备向导。

   提示
   另外，您可以通过以下方式启动该向导：
   - 从仪表板页面通过单击添加设备小组件。
   - 从 Sophos Central Admin 菜单通过单击 Protect Devices > Start device enrollment wizard。

2. 在用户页面上，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。

   注释
   您可以搜索部分字符串，但只能从字段的开头部分。例如，搜索字符串 example 匹配 Example User 和 example@company.com，但不匹配 user@example.com。

3. 在用户选择页面上，从匹配搜索条件的用户列表中选择所需的用户。
4. 在设备详细信息页面上，配置以下设置：

选项	说明
平台	设备平台。
姓名	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。
邮箱地址	用于接收注册说明的电子邮件地址。 和 Sophos Central 用户管理中配置的一样，这是分配给该设备的用户的电子邮件地址。
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. 在注册类型页面上，选择是要注册设备还是只注册 Sophos 容器。

   选择注册设备。
6. 选择为该设备平台配置的任务捆绑包。
7. 在注册页面上，按说明完成注册操作。

8. 注册成功完成后，单击完成。

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。

16 用语表

专用设置配置文件	您添加到自己开发的 iOS 应用的分发设置配置文件。这样，您就可以在指定的设备上安装应用，而不必将其发布到 App Store。
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。
Mobile Advanced 许可证	使用Mobile Advanced类型的许可证，您可以管理 Sophos Intercept X for Mobile、Sophos Secure Workspace 和 Sophos Secure Email。
设置	在设备上安装 Sophos Mobile Control 应用的过程。
Sophos Central Admin	您用于管理设备的 Web 界面。
Sophos Central 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。
Sophos Mobile 客户端	安装在 Sophos Mobile 托管的设备上的 Sophos Mobile Control 应用。
Sophos Intercept X for Mobile	一款针对 Android 设备、iPhone 和 iPad 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 设备、iPhone 和 iPad 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 Android 设备、iPhone 和 iPad 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。
Team ID	每个 iOS 和 macOS 应用都有 Team ID 签名。Team ID 由 Apple 提供，对于特定的开发团队是唯一的。

17 支持

您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。
- 在 www.sophos.com/zh-cn/support/documentation.aspx 中下载产品的技术文档。
- 访问 https://secure2.sophos.com/zh-cn/support/contact-support/support-query.aspx 联系我们的技术支持团队。

18 法律声明