SOPHOS
Security made simple.

Sophos Mobile as a Service

启动指南

产品版本号： 8

内容

1 关于本指南

本指南介绍如何对 Sophos Mobile 即服务 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 有哪些重要步骤？

要开始使用 Sophos Mobile：

1. 重置您的密码，登录到 Sophos Mobile Admin，并更改您的管理员用户名。
2. 可选： 激活您用于管理 Sophos Mobile Security、Sophos Secure Workspace 和 Sophos Secure Email 应用的 Mobile Advanced 许可证。
3. 检查您的许可证。
4. 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。
5. 上传用于管理 iOS 设备的 Apple 推送通知服务证书。
6. 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。
7. 可选： 配置第三方网络访问控制系统的接口。
8. 创建合规性策略。
9. 创建设备组。
10. 配置设备。
11. 更新自助服务门户设置。
12. 配置用户管理。
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。
15. 在自助服务门户中测试设备注册。

3 更改您的密码

出于安全考虑，我们建议您在首次登录 Sophos Mobile Admin前重置密码。

1. 在您的 Web 浏览器中打开 Sophos Mobile Admin。
2. 在登录对话框中，单击忘记密码？。
3. 在重置密码对话框中，输入收到的电子邮件中的客户和用户信息，激活您的 Sophos Mobile 即服务帐户，然后单击重置密码。
   您将会收到一封含有重置密码链接的电子邮件。
4. 单击该链接，打开更改密码对话框。
5. 输入新密码，然后单击更改密码。
   将更改您的密码。请记得在下次登录到控制台时使用此新密码。

注释

我们建议修改密码策略以强制要求更强的密码，如要求小写字母、大写字母或特殊字符的最小位数。请参阅配置密码策略 （第 7 页）。

4 更改登录名

出于安全考虑，建议您首次登录 Sophos Mobile Admin后更改管理员登录名。

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，单击登录名旁边的蓝色三角形，然后单击编辑。
3. 在编辑管理员页面上，在登录名字段中输入一个新值。
4. 可选： 调整其余字段的值：
   - 名
   - 姓
   - 电子邮件地址
5. 单击保存。

将更改您的帐户详细信息。请记得在下次登录到 Sophos Mobile Admin时使用新的登录名。

5 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。

在 Sophos Mobile Admin 中激活 Mobile Advanced 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。

6 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。
- 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。

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。

7 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

7.1 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。

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。

3. 单击保存。

7.2 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。

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。

7.3 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。

7.4 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。

8 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。

APNs 证书的有效期为一年。

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。

8.1 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)

8.2 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。
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。

9 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。

独立的 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。

注释

因为 macOS 不支持 ActiveSync 协议，因此您不能使用内部或独立的 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 13 页）。

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。

9.1 下载 EAS 代理安装程序

1. 登录 Sophos Mobile Admin。
2. 在侧边的菜单栏中，单击设置下的设置 > 系统设置，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。

9.2 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。

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

   还应选中 Use SSL for incoming connections (Clients to EAS Proxy) (对传入连接 (客户端到 EAS 代理) 使用 SSL)，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 (使用客户端证书进行身份验证)。这将为连接添加额外一层安全性。

   如果 Sophos Mobile 服务器向 EAS 代理提供了不同的证书，例如，因为负载平衡器后有多个服务器实例，且每个实例使用不同的证书，请选中 Allow all certificates (允许所有证书)。选中此选项后，EAS 代理将接受来自 Sophos Mobile 服务器的所有证书。

   > 重要提示
   > 因为 Allow all certificates (允许所有证书) 选项会降低服务器通信的安全级别，我们强烈建议您仅在您的网络环境需要时才选中它。

4. 如果之前选中了 Use SSL for incoming connections (Clients to EAS Proxy) (对传入连接 (客户端到 EAS 代理) 使用 SSL)，将显示 Configure server certificate (配置服务器证书) 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。

   > 注释
   > 可以从 MySophos 下载 SSL 证书向导，用于为 Sophos Mobile EAS 代理申请 SSL/TLS 证书。
   >
   > 有关如果下载 Sophos 软件的一般信息，请参阅 Sophos 知识库文章 111195。

   - 如果您还没有信任的证书，请选择 Create self-signed certificate (创建自签名证书)。
   - 如果已有信任的证书，请单击 Import a certificate from a trusted issuer (导入来自信任的颁发机构的证书)，并从列表中选择以下其中一种选项：
     - 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. 如果之前选中了 Use client certificates for authentication (使用客户端证书进行身份验证)，将显示 SMC client authentication configuration (SMC 客户端身份验证配置) 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 (EAS 代理实例设置) 页面上，配置一个或多个 EAS 代理实例。
   - Instance type (实例类型)：选择 EAS proxy (EAS 代理)。
   - Instance name: 用于标识该实例的名称。
   - Server port (服务器端口)：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 (需要进行客户端证书身份验证)：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 (ActiveSync 服务器)：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 subscription requests from Secure Email: 选中此选项以允许 iOS 设备上的 Sophos Secure Email 应用预订通过 Exchange Web 服务 (EWS) 发送的推送通知。有 Secure Email 消息时，将向设备发送推送通知。

     注释
     出于安全考虑，默认情况下，EAS 代理会阻止所有对 Exchange 服务器的 EWS 界面的请求。如果您选中此复选框，将允许预订请求。仍会阻止其他请求。

   - Enable Traveler client access (启用 Traveler 客户端访问)：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 (添加) 将实例添加到 Instances (实例) 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 (添加) 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 (确定)。
   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 (EAS 代理实例设置) 页面上的 Export config and upload to Sophos Mobile (导出配置并上传到 Sophos Mobile) 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 (添加) 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 (下一步)。
    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（允许的邮件用户代理）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（允许所有邮件用户代理）配置无限制。
    - 选择 Only allow the specified mail user agents（只允许指定的邮件用户代理），然后从列表中选择邮件用户代理。单击 Add（添加）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（Sophos Mobile EAS 代理 - 配置向导完成）页面上，单击 Finish（完成）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（现在启动 Sophos Mobile EAS 代理服务器），然后单击 Finish（完成）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 Mobile Admin。
17. 单击外部下的上传文件。上传安装向导为 PowerShell 连接创建的证书。
    如果您设置了多个实例，请对所有实例证书重复此操作。
18. 单击保存。
19. 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。

9.3 通过 PowerShell 设置电子邮件访问控制

您可以设置到 Exchange 或 Office 365 服务器的 PowerShell 连接。这就说，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。电子邮件数据流直接从设备传输到电子邮件服务器。不通过代理进行传输。

> 注释
> 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。

PowerShell 方案有以下优点：

- 设备直接与 Exchange 服务器通信。
- 对于来自您的托管设备的传入电子邮件数据流，您不需要在服务器上为其打开端口。

支持的电子邮件服务器有：

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

要设置 PowerShell：

1. 配置 PowerShell。

2. 在 Exchange 服务器上或在 Office 365 中创建服务帐户。Sophos Mobile 将使用此帐户执行 PowerShell 命令。
3. 设置一个或多个到 Exchange 或 Office 365 的 PowerShell 连接实例。
4. 将实例证书上传到 Sophos Mobile。

配置 PowerShell

1. 在准备安装 EAS 代理的计算机上，以管理员身份打开 Windows PowerShell，并输入：

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

> 注释
> 如果没有 PowerShell，按 Microsoft 文章安装 Windows PowerShell（外部链接）中所述进行安装。

2. 如果您要连接到本地 Exchange 服务器，请在该计算机上以管理员身份打开 Windows PowerShell，并输入和之前相同的命令：

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

> 注释
> Office 365 不需要执行此步骤。

创建服务帐户

3. 登录到相关的管理控制台：
   - 对于 Exchange Server 2013/2016：Exchange 管理中心
   - 对于 Office 365：Office 365 管理中心
4. 创建用户帐户。Sophos Mobile 将使用此帐户作为服务帐户执行 PowerShell 命令。
   - 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。
5. 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Mail Recipients（邮件收件人）和Organization Client Access（组织客户端访问）角色。
   - 将该服务帐户添加为成员。

设置 PowerShell 连接

6. 就像您要安装独立 EAS 代理一样，使用安装向导。在 EAS Proxy instance setup（EAS 代理实例设置）向导步骤中，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: Exchange 服务器的名称或 IP 地址（对于本地安装的 Exchange 服务器）或 outlook.office365.com（对于 Office 365）。不要包括前缀 https:// 或后缀 /powershell。它们会自动添加。
   - Allow all certificates: Exchange 服务器提供的证书未经过验证。例如，如果您的 Exchange 服务器上安装有自签名证书，则可使用此选项。因为 Allow all certificates（允许所有证书）选项会降低服务器通信的安全级别，我们强烈建议您仅在您的网络环境需要时才选中它。

- Allow EWS subscription requests from Secure Email: 选中此选项以允许 iOS 设备上的 Sophos Secure Email 应用预订通过 Exchange Web 服务 (EWS) 发送的推送通知。有 Secure Email 消息时，将向设备发送推送通知。

  注释
  出于安全考虑，默认情况下，EAS 代理会阻止所有对 Exchange 服务器的 EWS 界面的请求。如果您选中此复选框，将允许预订请求。仍会阻止其他请求。

- Service account: 您在 Exchange 或 Office 365 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。

7. 单击 Add (添加) 将实例添加到 Instances (实例) 列表中。
8. 可选：重复前面的步骤设置到其他 Exchange 或 Office 365 服务器的 PowerShell 连接。
9. 如安装独立的 EAS 代理 （第 11 页）中所述，完成安装向导步骤。

上传证书

10. 登录 Sophos Mobile Admin。
11. 在侧边的菜单栏上，在 设置 下，单击 安装 > 系统设置然后单击 EAS 代理 选项卡。
12. 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。
    这可以防止其他电子邮件应用连接到您的电子邮件服务器。
13. 单击外部下的上传文件。上传安装向导为 PowerShell 连接创建的证书。
    如果您设置了多个实例，请对所有实例证书重复此操作。
14. 单击保存。
15. 在 Windows 中，打开服务对话框并重新启动 EASProxy 服务。

这样就完成了 PowerShell 连接的初始设置。如果设备违反合规性规则，托管设备和 Exchange 或 Office 365 服务器之间的电子邮件数据流将被阻止。通过将单台设备的电子邮件访问模式设置为拒绝，您可以阻止该设备。

注释
根据您的 Exchange 服务器的配置，设备的电子邮件访问被阻止时，设备将会收到通知。

9.4 配置与内部 EAS 代理服务器的连接

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 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。
   这可以防止其他电子邮件应用连接到您的电子邮件服务器。
3. 在内部下的 Exchange/groupware server URL 文本字段中输入 Exchange 或群组软件服务器 URL。
4. 选择使用 SSL/TLS 以使用安全连接。
5. 选中允许来自 Secure Email 的 EWS 预订请求以允许 iOS 设备上的 Sophos Secure Email 应用预订通过 Exchange Web 服务 (EWS) 发送的推送通知。有 Secure Email 消息时，将向设备发送推送通知。
   出于安全考虑，默认情况下，EAS 代理会阻止所有对 Exchange 服务器的 EWS 界面的请求。如果您选中此复选框，将允许预订请求。仍会阻止其他请求。
6. 单击检查连接测试该连接。

如果服务器可以访问，将显示一条消息。

7. 单击保存。

9.5 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。

重要提示

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. 在侧边的菜单栏上，在 设置 下，单击 安装 > 系统设置然后单击 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。

   这可以防止其他电子邮件应用连接到您的电子邮件服务器。
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。

10 配置网络访问控制

Sophos Mobile 包括针对第三方网络访问控制 (NAC) 系统的接口。通过配置 NAC 系统的连接，可以让它们获取设备列表及其合规性状态。此外，如果按本节所述配置网络访问控制，以后还可以定义合规性策略，以便在违反特定合规性规则时拒绝网络访问。

有关如何定义合规性策略的信息，请参阅 Sophos Mobile 管理员帮助。

要配置网络访问控制：

1. 在侧边的菜单栏中，单击设置下的设置 > 系统设置，然后单击网络访问控制选项卡。
2. 从列表中选择一种可用的 NAC 集成方式：

- Sophos UTM

  此选项支持 Sophos UTM 集成（对于 9.2 或更高版本）。该集成方式需要在管理 > Sophos Mobile 下的 Sophos UTM WebAdmin 界面中设置 SMC 服务器 URL 和管理员用户凭据。有关详细信息，请参阅 Sophos UTM 管理指南。

- Cisco ISE

  此选项支持 Cisco ISE 集成。配置以下设置：

用户名	必须在 Cisco ISE 中指定的用户名。Cisco ISE 将用它登录 Sophos Mobile。
密码	输入用于登录 Sophos Mobile 的密码。
密码确认	重复该密码。
被阻止设备的重定向页面	如果不允许设备访问网络，将把设备重定向到该 URL。 我们建议使用自助服务门户的 URL 或带有自助服务门户链接的信息页面的 URL。

  必须在 Cisco ISE 上配置相关的设置，才能在连接到 NAC 接口时使用 Sophos Mobile 服务器的 URL 和在此处输入的凭据。

- Check Point

  此选项支持 Check Point 集成（对于 R77.10 或更高版本）。配置以下设置：

用户名	必须在 Check Point 中指定的用户名。Check Point 将用它登录 Sophos Mobile。
密码	输入用于登录 Sophos Mobile 的密码。
密码确认	重复该密码。

  在 Check Point Mobile Access Gateway 中，必须配置一些特定的设置，如 Check Point 支持中心的文章针对移动设备的 MDM 联合强化中所述。

- Web 服务

  此选项允许将第三方 NAC 系统连接到 Web 服务接口。

  Sophos Mobile 提供了 RESTful Web 服务接口，可用于提供托管设备的 MAC 地址和网络访问状态。

第三方 NAC 系统可以使用 Sophos Mobile 管理员帐户的登录凭据，连接到该接口。

有关 Web 服务接口的详细使用信息，请参阅 Sophos Mobile Network Access Control 界面指南。

- 自定义

  此选项可用于配置基于证书的 NAC 接口访问权限。

  > 注释
  > 旧的自定义选项已弃用，并将在以后版本中删除。而是使用 Web 服务选项，将第三方 NAC 系统连接到 Sophos Mobile。

  单击上传文件，然后浏览并找到第三方 NAC 系统的证书。证书将上传并显示在表格中。

  向 Sophos Mobile 服务器提供证书的第三方 NAC 系统将获得访问 NAC 接口的权限。

3. 在网络访问控制选项卡中，单击保存。

11 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。

11.1 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 16 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。 此操作仅可用于 Android 和 iOS 设备。
拒绝网络	禁止访问网络。 只有在您配置了网络访问控制后，才能执行此操作。请参阅配置网络访问控制 （第 17 页）。
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。

12 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。

12.1 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。

13 配置 iOS 设备

13.1 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。

13.2 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 19 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。

14 配置 Android 设备

14.1 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。

14.2 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 19 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。

15 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。

16 配置用户管理

Sophos Mobile 提供了两种不同的方法管理 Sophos Mobile Admin和自助服务门户的用户帐户：

- 使用内部用户管理，可通过在 Sophos Mobile Admin中手动添加用户或通过从逗号分隔值 (CSV) 文件导入用户的形式创建用户。
- 使用外部用户管理，可以连接到现有的 LDAP 目录，并将设备分配至基于目录成员的组或配置文件。

注释

- 设备分配给用户后，将不能更改用户管理方法。
- 对于外部用户管理，LDAPS（在 SSL/TLS 之上使用 LDAP）环境必须可用。Sophos Mobile 使用默认的 LDAPS 端口 636 连接到 LDAP 服务器。

要选择用户管理方法：

1. 在侧边的菜单栏中，单击设置下的设置 > 系统设置，然后单击用户设置选项卡。
2. 为 Sophos Mobile Admin和自助服务门户 (SSP) 的用户帐户选择数据源：
   - 选择内部目录可使用内部用户管理。
   - 选择外部 LDAP 目录可使用外部用户管理或结合使用内部用户管理。
3. 如果选择外部 LDAP 目录，请单击配置外部 LDAP 并指定服务器详细信息。请参阅配置外部目录连接 （第 30 页）。
4. 单击保存。

注释

保存设置后，只有选中的用户管理方法会显示在用户设置选项卡上。要在以后更改选项，请选择并保存无。没有可用的 SSP、用户特定配置文件或 LDAP 管理员可以使所有选项再次可用。

17 使用内部用户管理

17.1 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。

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。

17.2 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 28 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。

17.3 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。

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。

18 使用外部用户管理

18.1 配置外部目录连接

使用外部 LDAP 目录管理 Sophos Mobile Admin和自助服务门户的用户帐户时，必须配置目录连接，这样 Sophos Mobile 才能从 LDAP 服务器检索用户数据。

注释
LDAP 目录和 Sophos Mobile 之间没有同步。Sophos Mobile 将只访问 LDAP 目录以查找用户信息。对 LDAP 用户帐户的更改将不会在 Sophos Mobile 数据库中进行，反之亦然。

1. 在侧边的菜单栏中，单击设置下的设置 > 系统设置，然后单击用户设置选项卡。
2. 选择外部 LDAP 目录。
3. 单击配置外部 LDAP，指定服务器详细信息。
4. 在服务器详细信息页面上，配置以下设置：
   a) 在 LDAP 类型字段中，选择 LDAP 服务器类型：
      - Active Directory
      - IBM Domino
      - NetIQ eDirectory
      - Red Hat Directory Server
      - Zimbra
   b) 在主 URL 字段中，输入主目录服务器的 URL。可以输入服务器 IP 或服务器名称。选择 SSL/TLS 通过 SSL 或 TLS（取决于服务器支持的类型）保护服务器连接。对于 Sophos Mobile 即服务，无法取消选择 SSL/TLS。
   c) 可选： 在辅助 URL 字段中，输入在主服务器无法连接时用作回退方法的目录服务器的 URL。可以输入服务器 IP 或服务器名称。选择 SSL/TLS 通过 SSL 或 TLS（取决于服务器支持的类型）保护服务器连接。对于 Sophos Mobile 即服务，无法取消选择 SSL/TLS。
   d) 在用户字段中，输入用于在目录服务器上执行查找操作的帐户。Sophos Mobile 将在连接到目录服务器时使用该帐户凭据。

      对于 Active Directory，还需要输入相关的域。支持的格式有：
      - <域>\<用户名>
      - <用户名>@<域>.<域代码>

      注释
      出于安全考虑，我们建议您指定只有目录服务器读取权限而没有写入权限的用户。

   e) 在密码字段中，输入用户的密码。

   单击下一步。
5. 在搜索库页面上，输入搜索库对象的可分辨名称。
   搜索库对象用于定义外部目录中的位置，搜索用户或用户组时将从这里开始。
6. 在搜索字段页面上，定义使用哪些目录字段来解析配置文件和策略中的占位符 %_USERNAME_% 和 %_EMAILADDRESS_%。键入所需字段的名称或在用户名和电子邮件列表中选择。

> 注释
> 列表只包含为当前连接到 LDAP 目录的用户配置的字段，这是在本说明前面部分的步骤 4.d（第 30 页） 中指定的。例如，如果没有为该用户配置电子邮件字段，则需要在电子邮件字段中手动输入所需的值。

对于 Active Directory，将应用以下字段映射：

- 用户名：sAMAccountName
- 名：givenName
- 姓：sn
- 电子邮件：mail

7. 在 SSP 配置页面上，指定允许登录到自助服务门户的用户。使用以下任一选项，在 LDAP 目录组字段中输入相关信息：
   - 如果输入星号 *，将允许所有 LDAP 目录组的成员登录到自助服务门户。

     > 注释
     > 值 * 表示所有组，而不是所有用户。不包括不是任何 LDAP 目录组成员的用户。

   - 如果输入的组名已经定义在目录服务器中，将允许该组的所有成员登录自助服务门户。输入组名后，单击解析组，将组名解析为可分辨名称 (DN)。
   - 如果将该字段保留为空，将不允许该目录服务器的用户登录自助服务门户。如果要对 Sophos Mobile Admin启用外部用户管理，但不对自助服务门户启用，则可使用此选项。

   > 注释
   > 在这里指定的组与在自助服务门户页面的组设置选项卡中定义的用户组不相关。使用这些设置，可以为每个用户组定义任务捆绑包、Sophos Mobile 组成员身份和可用的设备平台。
   >
   > 有关自助服务门户组设置的详细信息，请参阅 Sophos Mobile 管理员帮助。

8. 单击应用。
9. 在用户设置选项卡上，单击保存。

18.2 为 LDAP 用户测试设备注册

我们建议您在向用户推出自助服务门户使用之前，通过自助服务门户对设备注册进行测试。

使用您的 LDAP 凭据登录到自助服务门户，并在要通过 Sophos Mobile 管理的所有平台上执行注册测试。

19 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。
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。

20 术语表

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。

21 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。

22 法律声明