SOPHOS

Cybersecurity made simple.

Sophos Mobile 安装指南

产品版本号： 8.6

内容

关于本指南 1
关于 Sophos Mobile 2
Sophos Mobile 许可证 3
试用许可证 3
将试用许可证升级为完整许可证 3
更新许可证 3
设置 Sophos Mobile 4
安装前提条件 4
系统环境要求 4
申请 SSL/TLS 证书 5
安装和设置 Sophos Mobile 服务器 5
配置 Sophos Mobile Web 服务器 8
更改 SQL 登录语言 8
独立的 EAS 代理 9
独立 EAS 代理的使用方案 10
下载 EAS 代理安装程序 11
安装独立的 EAS 代理 11
通过 PowerShell 设置电子邮件访问控制 14
负载平衡和高可用性 17
要求 17
设置群集节点 18
设置 Sophos UTM 负载平衡 19
更新 Sophos Mobile 21
更新 Sophos Mobile 服务器 21
更新后的任务 21
更新服务器群集 21
更新独立的 EAS 代理 22
技术参考 23
Sophos Mobile 服务器功能 23
Sophos Mobile Web 界面 23
技术支持 25
法律声明 26

1 关于本指南

本指南介绍如何安装和设置 Sophos Mobile 版本 8.6。还将介绍如何更新已经安装的现有Sophos Mobile。

除非另有说明，所有程序都必须以 Microsoft Windows Server 管理员身份或相关组的用户身份执行。

2 关于 Sophos Mobile

Sophos Mobile

Sophos Mobile 是一套 EMM 解决方案，适合希望节省管理和保护移动设备的时间和精力的公司。通过易于使用、基于 Web 的统一 Sophos Central 管理界面管理移动设备，享受 Sophos 提供的端点、网络或服务器安全性。安全的容器应用以及在 iOS、Android 企业和 Samsung Knox 中对移动 OS 容器化的支持，可以确保设备上敏感的公司数据和个人信息相分离。

Sophos Mobile 提供了一流的数据保护、综合的安全性、很高的资金利用价值以及灵活的管理选项，是允许将移动设备用于工作、保持用户的生产效率、保持企业数据安全和保护个人数据隐私的最佳途径。

Sophos Mobile Security

Sophos Mobile Security 不仅可以保护您的 Android 设备，而且不会影响设备的性能或电池的寿命。Sophos Mobile Security 利用领先的 Sophos 反恶意软件技术，提供屡获殊荣的反恶意软件和反病毒功能，能够检测可能不需要的应用，并且提供了隐私和安全顾问、丢失和被盗保护、Web 保护等功能。

Sophos Secure Workspace

Sophos Secure Workspace 是针对 iOS 和 Android 系统的容器化移动内容管理应用，为保护、管理和分发企业文档及 Web 内容提供了安全的途径。不离开容器环境即可编辑 Office 格式的文档，可以确保加密内容保持安全。防钓鱼技术能够阻止用户打开文档或内容中的恶意链接。

通过 Sophos Mobile 托管时，管理员能够根据设备合规性规则，轻松限制内容的访问。和 Sophos SafeGuard Encryption 一起使用，Sophos Secure Workspace 能够在 Windows、macOS、iOS 和 Android 用户之间提供加密文件（存储在本地或云上）的无缝交换。

Sophos Secure Email

Sophos Secure Email 是针对 Android 和 iOS 系统的全功能、安全且容器化的电子邮件应用，通过 Sophos Mobile 托管时，它让您可以在移动设备上分离企业电子邮件、日历及联系人和个人数据。所有公司信息都受到 AES-256 加密方式的保护，并且可以根据设备合规性规则轻松取消访问权限。Sophos Secure Email 还让 IT 人员可以跨不同的设备和操作系统安全一致地设置企业电子邮件。

3 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。

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。

3.1 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。

3.2 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。

3.3 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。

4 设置 Sophos Mobile

本节介绍如何安装新的 Sophos Mobile 服务器。有关如何更新现有安装的信息，请参阅更新 Sophos Mobile （第 21 页）。

4.1 安装前提条件

安装 Sophos Mobile 服务器前，检查是否满足以下前提条件：

- 已经阅读 Sophos Mobile 部署指南。本文档包含将 Sophos Mobile 服务器集成到贵公司基础设施的架构实例、容量指导原则和所需网络端口和协议的列表。
- 已经阅读 Sophos Mobile 8.6 发行说明并且确认 Sophos Mobile 支持托管 Sophos Mobile 服务器的计算机（服务器计算机）、您要管理的设备以及其他相关的组件。
- 有 Sophos Mobile 服务器的 SSL/TLS 证书。请参阅申请 SSL/TLS 证书 （第 5 页）。
- 服务器计算机上没有安装 Internet Information Services (IIS) Web 服务器或使用端口 80 或 443 的其他应用程序。
- 可以通过 Internet 解析服务器计算机的 DNS 名称。
- 如果用户帐户存储在 LDAP 目录中，有一个或多个 LDAP 组包含允许使用自助服务门户的用户。

如果您想使用现有的数据库服务器管理 Sophos Mobile 数据库，则必须满足以下条件：

- Microsoft SQL Server 或 Microsoft SQL Server Express：
  - 使用 Windows 身份验证或 SQL Server 身份验证。
  - 开启 TCP/IP。
  - 启用 SQL Server Browser 服务。
  - 用于登录 SQL 的帐户的语言设置为英语。
- Microsoft SQL Server Express：
  - 安装了 SQL 管理工具。

4.2 系统环境要求

Sophos Mobile 安装程序运行一系列测试，验证您的系统环境是否满足 Sophos Mobile 的所有必需要求。

这些要求是：

- 您是该计算机的管理员。
- Sophos Mobile 支持该计算机的操作系统。
- 该计算机至少有一个网络适配器。
- 该计算机至少有 4 GB 内存。
- 该计算机上已禁用 Microsoft Internet Information Services (IIS) Web 服务器。
- 该计算机上的以下 HTTP/S 端口可以使用：80, 443, 8080, 8181
- 该计算机可以连接到 Apple 推送通知服务 (APNs)。

- 该计算机可以连接到 Google Firebase Cloud Messaging (FCM) 服务。
- 该计算机可以连接到 Google reCAPTCHA 服务。
- 该计算机可以连接到 Windows 推送通知服务。
- 该计算机可以连接到 Sophos 服务。
- 可选：该计算机可以连接到 Apple 批量购买计划 (VPP) Web 服务。
- 可选：该计算机可以连接到 Apple 设备注册计划 (VPP) Web 服务。
- 可选：该计算机可以连接到 Apple iTunes Web 服务。
- 可选：该计算机可以连接到 Apple 激活锁定跳过 Web 服务。
- 可选：该计算机可以连接到针对 Android enterprise 的 Google Web 服务。
- 可选：该计算机可以连接到 Microsoft Web 服务以进行 Intune 应用保护。

4.3 申请 SSL/TLS 证书

提供的 Sophos 产品包括 SSL 证书向导，可用于为 Sophos Mobile EAS 代理申请 SSL/TLS 证书。从 %MDM_HOME%\tools\Wizard 文件夹中运行向导，或从 www.sophos.com/mysophos 下载。

注释
如果您使用自签名证书或您自己的证书颁发机构 (CA) 颁发的证书，将应用以下限制：

- 您必须先在您的设备上手动安装自签名证书或 CA 证书，然后再将它们注册到 Sophos Mobile。如果您不这样做，Sophos Mobile Control 应用程序将不会信任您的服务器，且会拒绝连接。由全球受信任的 CA 颁发的证书不需要进行此手动安装。
- 您不能从托管在 Sophos Mobile 服务器上的 APK 文件安装 Android 应用。
- 您不能使用 Android Zero-touch 注册或 Samsung Knox Mobile Enrollment。

要申请 SSL/TLS 证书：

- 双击 Sophos Mobile SSL Certificate Wizard.exe 文件，启动 SSL 证书向导。
  该向导将指导您完成安装过程。按以下说明输入所需的信息：
  a) 在 Upload CSR (上传 CSR) 页面上，可以单击 Open CSR (打开 CSR) 按钮以打开 CSR 文件 (如果您的证书供应商支持复制和粘贴)。
  b) 在 Import Certificate Files (导入证书文件) 页面上，把在 Upload CSR (上传 CSR) 页面上下载的 CA 证书输入到 Select CA certificate file (选择 CA 证书文件) 字段中。
  c) 在 Certificate created (证书已创建) 页面上，将显示创建的证书的位置。设置 Sophos Mobile 时需要引用此位置。

注释
应创建一个包含证书文件的备份文件夹。

4.4 安装和设置 Sophos Mobile 服务器

前提条件：

- 如果要将 Sophos Mobile 连接到现有数据库，请在开始安装前确保有可用的登录凭据，并且有足够的权限创建新的数据存储、用户帐户和数据记录。

- 如果数据库不在本地，需要通过 TCP 端口 1433 访问 Microsoft SQL Server 和端口 3306 访问 MySQL。此外，还需要 Sophos Mobile 服务器可以用于登录数据库的管理员帐户。

1. 以管理员身份运行 Sophos Mobile 安装程序，查看并同意 License Agreement（许可协议）。
2. 在 System Property Checks（系统属性检查）页面上，单击 Check（检查）运行测试，验证您的系统环境是否满足 Sophos Mobile 的所有必需要求。请参阅系统环境要求 （第 4 页）。

   可以单击 Report（报告），生成测试结果报告。
3. 在 Choose Install Location（选择安装位置）页面上，选择 Sophos Mobile 服务器的目标文件夹。
4. 在 Database Type Selection（数据库类型选择）页面上，选择要使用的数据库：
   - Install and use Microsoft SQL Server Express：将立即安装 Microsoft SQL Server Express 并将其配置为用于 Sophos Mobile。
   - Use existing Microsoft SQL Server installation：使用已经安装的 Microsoft SQL Server，为 Sophos Mobile 创建新的数据库。
   - Use existing MySQL installation：使用已经安装的 MySQL，为 Sophos Mobile 创建新的数据库。
5. 在 Database Settings（数据库设置）页面上，输入数据库的登录凭据。

   注释
   如果选择 Use SQL Server Authentification（使用 SQL 服务器身份验证）选项，需要确保 SQL 登录语言设置为英语。参见更改 SQL 登录语言 （第 8 页）了解详细信息。

6. 在 Database Selection（数据库选择）页面上，单击 Create a new database named（创建新的数据库，名称为），输入要创建的数据库的名称，如 SMCDB。
7. 在 Database Configuration（数据库配置）页面上，将在创建数据库期间显示进度消息。数据库成功创建并填充后，单击 Next（下一步）继续。
8. 如果已经选择 Windows 身份验证进行数据库访问，将有一个Set service credentials页面可用于设置 Windows 帐户，Sophos Mobile 服务将在该帐户下运行。

   可以使用本地系统帐户或用户帐户。在后一种情况下，请输入用户帐户作为<计算机名>\<用户名>或<域>\<用户名>。

   安装程序将为该帐户分配数据库访问权限。

   注释
   出于安全考虑，我们建议您以拥有有限访问权限的用户身份运行 Sophos Mobile 服务。该用户帐户应具有以下属性：
   - 用户帐户是安装 Sophos Mobile 的计算机上的本地 Windows 帐户。
   - 用户不是任何组的成员，甚至不是用户组的成员。
   - 用户可以访问您的 SQL 数据库，并有必要的更改权限。对于 MS SQL 数据库，这意味着用户必须是 db_datareader 和 db_datawriter 角色的成员。

9. 在Configure super admin account页面上，配置管理员的帐户详细信息。

   超级管理员主要用于进行客户管理，不应该用于日常设备管理。超级管理员登录到超级管理员客户，可以（例如）预定义新客户的设置，并将设置和配置推送给现有客户。有关详细信息，请参阅 Sophos Mobile 超级管理员指南.

注释
首次登录 Sophos Mobile Admin 时，需要超级管理员凭据。完成安装后，可以在 Sophos Mobile Admin 中添加其他超级管理员。

10. 在 Configure external server name（配置外部服务器名称）页面上，输入 Sophos Mobile 服务器名称（如 smc.mycompany.com）。

注释
服务器名称必须能够由托管的设备解析。

11. 在 Configure server certificate（配置服务器证书）页面上，导入用于安全（HTTPS）访问 Web 服务器的证书。
    - 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）并选择下拉列表中的选项。
    - 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）。

注释
提供的 Sophos 产品包括 SSL 证书向导，可用于为 Sophos Mobile 申请 SSL/TLS 证书。请参阅申请 SSL/TLS 证书 （第 5 页）。

12. 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，需要指定可以从托管的设备访问的服务器。

13. 在 Server Information（服务器信息）页面上，检查服务器信息，然后单击 Next（下一步），确认服务器和配置过程。
14. 安装完成后，将显示 Sophos Mobile Control - Installation finished（Sophos Mobile Control - 安装完成）对话框。确保选中 Start Sophos Mobile server now（现在启动 Sophos Mobile 服务器）复选框，并单击 Finish（完成），开始首次启动 Sophos Mobile 服务器。

注释
启动服务后，可能需要几分钟时间才会显示 Sophos Mobile Web 界面。

安装后，需要执行几个初始配置步骤：

- 将 Sophos Mobile Web 服务器配置为只接受指向您的域名的请求。请参阅配置 Sophos Mobile Web 服务器 （第 8 页）。
- 首次登录 Sophos Mobile Admin，启动第一步向导。请参阅 Sophos Mobile 启动指南。
- 对于 iOS 设备，需要有 Apple 推送通知服务证书。请参阅 Sophos Mobile 启动指南。
- 也可以设置独立的 EAS 代理用于电子邮件筛选。请参阅独立的 EAS 代理 （第 9 页）。

4.5 配置 Sophos Mobile Web 服务器

Sophos Mobile 包括 Web 服务器组件，用于提供 Sophos Mobile Admin 的内容和自助服务门户 Web 应用程序。您可以配置该 Web 服务器，使其适合您的环境。

对 Web 服务器的请求在请求标题中包括有 Host 字段，用于指定处理该请求的 Web 应用程序。攻击者可能会操纵该 Host 字段的值，引发意想不到的行为。

安装后，Sophos Mobile 的 Web 服务器组件不会检查 Host 字段的值。我们建议您配置该 Web 服务器，使其只接受指向您的域名的请求。

1. 在安装 Sophos Mobile 服务器的计算机上，运行脚本 %MDM_HOME%\tools\HostValidationUndertowFilter\addModule.bat

   请将 %MDM_HOME% 替换为您的 Sophos Mobile 安装文件夹。
2. 在文本编辑器中打开文件 %MDM_HOME%\wildfly\standalone\configuration\smc-config.xml，并搜索以下内容：

   ```
   <filter name="hostheadervalidation" ...>
       <param name="allowedHosts" value="localhost"/>
   </filter>
   ```
3. 在 localhost 后，添加您的 Sophos Mobile Admin 和自助服务门户的域名。

   例如，如果您的域名是 smc.example.com，请按以下方式修改该行。

   ```
   <param name="allowedHosts" value="localhost,smc.example.com"/>
   ```

   如果您的 Sophos Mobile 服务器可以通过多个域名访问，请输入所有域名，并以逗号隔开。
4. 保存 smc-config.xml 文件
5. 重新启动 Sophos Mobile 服务。

4.6 更改 SQL 登录语言

如果已经将 Sophos Mobile 服务器配置为使用 SQL Server 身份验证连接到数据库，则必须将 SQL 登录语言设置为英语。否则，启动 Sophos Mobile 服务时将会出现错误。

本主题介绍如何将 SQL 登录语言更改为英语。

1. 停止 Sophos Mobile 服务。
2. 在服务器上打开 SQL Server Management Studio，并选择安全 > 登录。
3. 在登录属性的常规页面上，将默认语言设置为英语，然后单击确定保存修改。
4. 重新启动 Sophos Mobile 服务。

5 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。

有两种类型的 EAS 代理：

- 随 Sophos Mobile 自动安装的内部 EAS 代理。它支持 Microsoft Exchange 或 IBM Notes Traveler for iOS 和 Samsung Knox 设备使用的传入 ActiveSync 数据流。
- 可以下载并单独安装的独立 EAS 代理。它通过 HTTPS Web 接口与 Sophos Mobile 服务器通信。

注释
出于性能方面的考虑，必须管理超过 500 个客户端设备的电子邮件流量时，我们建议您使用独立的 EAS 代理，而不是内部版本。

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

与内部版本相比，独立的 EAS 代理具有额外的功能：

- 支持用于非 iOS 设备（如 Android）的 IBM Notes Traveler。用于这些设备的 Traveler 客户端使用内部 EAS 代理不支持的协议（不是 ActiveSync）。
- 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 14 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。

5.1 独立 EAS 代理的使用方案

注释
除本节提供的信息外，Sophos Mobile 部署指南还包含将独立的 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。

对于以下方案，应使用独立的 EAS 代理服务器。

对非 iOS 设备使用 IBM Notes Traveler（以前的 IBM Lotus Notes Traveler）

内部 EAS 代理不适合这种方案，因为它只支持 ActiveSync 协议，通过 Microsoft Exchange 和 IBM Notes Traveler 用于 iOS 设备。用于非 iOS 设备（如 Android）的 IBM Notes Traveler 使用独立的 EAS 代理支持的不同协议。

对于非 iOS 设备，需要专用的 Traveler 客户端软件。该软件可以在 <traveler-server>/servlet/traveler 或 Traveler 文件系统中找到。Sophos Mobile 的安装应用和卸载应用功能可用于安装和卸载 Traveler 客户端软件。配置必须手动执行。

要支持多个后端服务器

使用独立的 EAS 代理，可以设置多个后端电子邮件系统实例。每个实例需要一个 TCP 接收端口。每个端口可以连接到不同的后端。每个 EAS 代理实例需要一个 URL。

要为 EAS 设置负载平衡

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。

对于这种方案，需要使用现有的 HTTP 负载平衡器。

要使用基于客户端证书的身份验证

对于这种方案，需要使用现有的 PKI，并且 CA 证书的公共部分必须在 EAS 代理中设置。

您需要管理超过 500 个设备

出于性能方面的考虑，必须管理超过 500 个客户端设备的电子邮件流量时，我们建议您使用独立的 EAS 代理，而不是内部版本。

5.2 下载 EAS 代理安装程序

1. 以超级管理员身份登录 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。

5.3 安装独立的 EAS 代理

前提条件：

- 已经安装和设置 Sophos Mobile。
- 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
提供的 Sophos 产品包括 SSL 证书向导，可用于为 Sophos Mobile EAS 代理申请 SSL/TLS 证书。有关更多信息，请参阅申请 SSL/TLS 证书 （第 5 页）。

- 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。
     - 有关如何为您的 Exchange 服务器配置 EWS 的信息，请参阅 Sophos 知识库文章 127137。

   - 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. 以超级管理员身份登录 Sophos Mobile Admin。
17. 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。
18. 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。
19. 单击保存。
20. 在 Windows 中，打开服务对话框并重新启动 EASProxy 服务。
21. 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。
22. 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。
23. 单击保存。
24. 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。

5.4 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
有关 PowerShell 通信的说明，请参阅 Sophos Mobile 部署指南。

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: 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。
     — 有关如何为您的 Exchange 服务器配置 EWS 的信息，请参阅 Sophos 知识库文章 127137。

   - 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. 以超级管理员身份登录 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。

6 负载平衡和高可用性

Sophos Mobile 可用于设置高可用性环境。这可以确保即便是在 Sophos Mobile 节点出现故障后，仍然可以从外部访问 SMC 服务和继续处理任务。为此，需要能够使用 DNS 轮循机制将客户端和浏览器会话分配给可用节点的负载平衡。

下面介绍如何为 Sophos Mobile 设置群集，以及如何通过 Sophos UTM 配置负载平衡。

6.1 要求

- 一个单独的 Windows 服务器，用于每个 Sophos Mobile 节点。
- 所有节点必须在同一网络上。
- 一个 Microsoft SQL 或 MySQL 数据库服务器或群集。
- Sophos UTM 或 Apache 反向代理 (mod_proxy)，用于负载平衡。负载平衡器必须支持永久会话 Cookie 和正式的 SSL/TLS Web 服务器证书。

注释
有关安装要求的详细信息，请参阅 Sophos Mobile 8.6 发行说明。

架构

有关三节点 Sophos Mobile 群集的示例，请参阅 Sophos Mobile 部署指南。

对于单个 Sophos Mobile 节点间的多播通信，可以选择使用单独的网络。要使用的网络接口可以在进行群集配置时选择，如设置第一个节点 （第 18 页）中所述。它也可能是 VLAN。

注释
如果出于测试目的而要运行第二个 Sophos Mobile 群集，则需要单独的网络。

端口和协议

下表显示了 Sophos Mobile 服务器群集的单个节点之间的通信所需的端口和协议。

协议	端口	目标
TCP	7600, 8181, 57600	<传入>
TCP	7600, 8181, 57600	<传出>
UDP	45700	<传入>

服务器证书

当您设置 Sophos Mobile 时，可以配置 SSL/TLS Web 服务器证书，以使 Sophos Mobile Control 应用可以和 Sophos Mobile 服务器建立安全连接。我们建议您使用由全球受信任证书颁发机构 (CA) 颁发的证书。在负载平衡器后有多个 Sophos Mobile 服务器节点的群集环境中，这可能不可行。您可以改用自签名证书。

注释
如果您使用自签名证书或您自己的证书颁发机构 (CA) 颁发的证书，将应用以下限制：

- 您必须先在您的设备上手动安装自签名证书或 CA 证书，然后再将它们注册到 Sophos Mobile。如果您不这样做，Sophos Mobile Control 应用程序将不会信任您的服务器，且会拒绝连接。由全球受信任的 CA 颁发的证书不需要进行此手动安装。
- 您不能从托管在 Sophos Mobile 服务器上的 APK 文件安装 Android 应用。
- 您不能使用 Android Zero-touch 注册或 Samsung Knox Mobile Enrollment。

6.2 设置群集节点

要设置群集环境，请按安装和设置 Sophos Mobile 服务器 （第 5 页）中所述安装第一个节点。之后，群集本身将使用 Configuration Wizard (配置向导) 激活。

对于所有其他节点，必须选中在安装首个节点时创建的数据库，并且必须激活群集。

注释
也可以配置现有 SMC 服务器进行群集，并通过添加其他节点扩展该环境。

6.2.1 设置第一个节点

1. 安装和设置 Sophos Mobile 服务器 （第 5 页）中所述的步骤安装 Sophos Mobile，并记录创建的数据库的名称。安装其他节点时，指定此数据库。
2. 在安装结束时，在 Sophos Mobile - Installation finished (Sophos Mobile - 安装已完成) 对话框中，取消选中 Start Sophos Mobile server now (现在启动 Sophos Mobile Control 服务器) 选项。

   注释
   如果 Sophos Mobile 服务已启动，在进行本节后面部分介绍的配置时，它将会自动停止并重新启动。另外，也可以通过 Sophos Mobile 系统托盘图标的菜单手动停止该服务。

3. 在服务器上，单击 Start (开始)，转到 Sophos Mobile，并单击 SMC Configuration Wizard (配置向导)。
4. 将显示 Sophos Mobile 配置向导的 Welcome (欢迎) 页面。单击 Next。
5. 在 Database Selection (选择配置步骤) 页面上，选择 Skip database configuration (配置群集支持) 并单击 Next (下一步)。
6. 在 Choose configuration steps (选择配置步骤) 页面上，选择 Configure cluster support (配置群集支持) 并单击 Next (下一步)。

7. 在 Cluster Configuration（群集配置）页面上，使用可用网络接口的下拉列表，选择要设置的服务器节点和其他节点之间的多播通信将要使用的接口。
8. 在配置向导的其余页面单击确定。确保在询问是否启动 SMC 服务时单击 Yes（是）。
首个 SMC 服务器节点的配置即完成。在 Sophos Mobile - Configuration Wizard finished（Sophos Mobile - 配置向导已完成）对话框中，单击 Finish（完成）。

6.2.2 设置其他节点

1. 按安装和设置 Sophos Mobile 服务器 （第 5 页）中所述的步骤，开始安装 Sophos Mobile。
2. 在 Database selection（数据库选择）页面上，选择在安装第一个节点时创建的数据库，然后单击 Next（下一步）。
将显示 Database configuration（数据库配置）对话框。它会显示配置过程的进度。
3. 在 Database configuration（数据库配置）页面上，等待配置过程完成，然后单击 Next（下一步）。
4. 在 Choose configuration steps（选择配置步骤）页面上，选择 Configure cluster support（配置群集支持）并单击 Next（下一步）。
5. 在 Configure server certificate（配置服务器证书）页面上，按安装和设置 Sophos Mobile 服务器 （第 5 页）中所述的步骤创建自签名证书，然后单击 Next（下一步）。
6. 在 Cluster Configuration（群集配置）页面上，使用可用网络接口的下拉列表，选择要设置的 Sophos Mobile 服务器节点的接口，然后单击 Next（下一步）。
7. 在配置向导的其余页面单击确定。在 Sophos Mobile - Installation finished（Sophos Mobile Control - 安装已完成）页面上，选择 Start Sophos Mobile server now（现在启动 Sophos Mobile Control 服务器）以启动刚刚配置的群集节点。
8. 如果您已经在第一个节点上将 Sophos Mobile 的 Web 服务器组件配置为只接受指向您的域名的请求，请对所有其他节点重复此操作。请参阅配置 Sophos Mobile Web 服务器 （第 8 页）。

如果需要，重复此过程以配置其他节点。

6.3 设置 Sophos UTM 负载平衡

本主题介绍如何将 Sophos UTM 设置为 Sophos Mobile 服务器节点群集的负载平衡器。有关配置 Sophos UTM 的详细信息，请参阅 Sophos UTM 文档。

注释

- 为使用 Sophos UTM 进行群集分析，需要订阅了 Sophos Webserver Protection 的 Sophos UTM 许可证。
- 如本节后面部分所述，需要指定证书，用于保护托管的设备和在 Sophos UTM 中设置的虚拟 Web 服务器之间的通信。为简单起见，推荐使用用于 Sophos Mobile 服务器的相同证书（请参阅申请 SSL/TLS 证书 （第 5 页））。如果使用自签名证书，强制要求使用此同一证书。

1. 登录 Sophos UTM WebAdmin。
2. 从 WebAdmin 的 Webserver Protection 菜单部分，转到 Web 应用程序防火墙 > 实际 Web 服务器选项卡。
3. 单击新建实际 Web 服务器，创建 SMC 节点。
4. 在添加实际 Web 服务器对话框中，输入以下设置：
   a) 名称：输入 Web 服务器的描述性名称（如 SMC node）。
   b) 主机：选择或添加主机。通过单击主机字段旁边的文件夹符号选择主机。从可用主机列表中，将主机拖入主机字段。

有关如何添加定义的详细信息，请参阅 UTM 管理指南中的网络定义主题。

c) 类型：选择加密 (HTTPS)。

单击保存，保存配置。

对每个 Sophos Mobile 服务器节点重复上述步骤。

5. 从 WebAdmin 的 Webserver Protection 菜单部分，转到证书管理 > 证书选项卡。
6. 单击新建证书，上传 SSL/TLS Web 服务器证书。
7. 在添加证书对话框中，输入以下设置:
   a) 名称：为证书输入描述性名称。
   b) 方法: 选择上传。
   c) 文件类型：选择 PKCS#12(Cert+CA)
   d) 密码：输入证书文件的密码。
   e) 文件: 单击文件框旁边的文件夹图标，选择要上传的证书，并单击开始上传。

   单击保存，保存配置。证书将添加到证书列表中。
8. 从 WebAdmin 的 Webserver Protection 菜单部分，转到 Web 应用程序防火墙 > 虚拟 Web 服务器选项卡。
9. 单击新建虚拟 Web 服务器，为群集添加虚拟 Web 服务器。
10. 在添加虚拟 Web 服务器对话框中，进行以下设置：
    a) 名称：输入虚拟 Web 服务器的描述性名称 (如 SMC cluster)。
    b) 在接口列表中，选择可用于从外部访问群集的 WAN 口。
    c) 类型：选择加密 (HTTPS) 和重定向。
    d) 在证书列表中，选择之前上传的 Web 服务器证书。
    e) 域 (仅用于通配符证书，即可用于多个子域的公钥证书)：输入 Web 服务器负责的域，如 shop.example.com，或使用操作图标导入域名列表。

       必须以完全限定的域名 (FQDN) 输入域。

       可以用星号 (*) 作为通配符用作域前缀，如 *.mydomain.com。带通配符的域将作为回退设置: 仅在没有配置带有更详细域名的其他虚拟 Web 服务器时，才使用带有通配符域条目的虚拟 Web 服务器。

       示例：对 a.b.c 的客户端请求将优先匹配 a.b.c，然后匹配 *.b.c，最后匹配 *.c。
    f) 实际 Web 服务器: 选择之前创建的 SMC 节点。

    重要提示
    请勿选择防火墙配置文件。

    单击保存，保存配置。服务器将添加到虚拟 Web 服务器列表中。
11. 启用虚拟 Web 服务器。

    新的虚拟 Web 服务器在默认情况下是禁用的。单击切换开关启用虚拟 Web 服务器。切换开关的颜色应从灰色 (禁用) 改变为绿色 (启用)。
12. 转到站点路径路由选项卡。
13. 在虚拟 Web 服务器列表中，转到添加的虚拟 Web 服务器，并单击编辑。
14. 在编辑站点路径路由对话框中，单击高级，然后选择启用粘性会话 Cookie。
    单击保存，保存配置。

7 更新 Sophos Mobile

安装的 Sophos Mobile 服务器可以直接从版本8、8.1 或 8.5 到更新到 8.6。

更旧的版本需要先更新到版本 8。有关详细信息，请参阅 Sophos Mobile 8 文档。

7.1 更新 Sophos Mobile 服务器

要将安装的 Sophos Mobile 服务器更新到版本 8.6，请运行Sophos Mobile 8.6 安装程序，并按说明进行操作。安装程序将自动检测是否有现有的安装需要更新到版本 8.6。

开始更新前，将执行系统属性检查。所有检查都通过后，即可进行更新。数据库和文件将自动更新，无需任何用户交互。更新完成后，Sophos Mobile 服务将再次启动。

注释
如果初始安装 Sophos Mobile 服务器时使用的是 Windows 身份验证，现在启动 Start Sophos Mobile server now 服务器选项将显示为灰色。必须手动启动该服务。

7.2 更新后的任务

7.2.1 重新配置 Sophos Mobile Web 服务器

如果您已经将 Sophos Mobile 的 Web 服务器组件配置为只接受指向您的域名的请求，在更新 Sophos Mobile 后，您必须重复此步骤。请参阅配置 Sophos Mobile Web 服务器 （第 8 页）。

7.2.2 重新配置 Windows 计算机的自助服务门户注册

如果您已经为 Windows 计算机配置了自助服务门户注册，将 Sophos Mobile 从版本 8 更新到版本 8.6 以后，必须对配置进行调整。在Sophos Mobile 8 中，初始软件包是一个策略，而在Sophos Mobile 8.1 和更高版本中是一个任务捆绑包。

在 Sophos Mobile Admin 中，执行以下步骤：

1. 在任务捆绑包 > Windows 下，创建一个包含注册任务以及（可选）一个或多个分配策略和/或安装应用任务的新任务捆绑包。

   根据要求，为公司设备和个人设备创建不同的任务捆绑包。
2. 在安装 > 自助服务门户 > 组设置下，选择这些任务捆绑包作为Windows平台的初始包，然后单击Windows旁边的复选框。

有关任务捆绑包和自助服务门户设置的详细信息，请参阅 Sophos Mobile 管理员帮助。

7.3 更新服务器群集

更新 Sophos Mobile 服务器节点群集时，有一点很重要，那就是所有节点在所有时间都运行在相同的版本上，且服务器版本和数据库版本一致。为此：

1. 停止相关计算机上的 Sophos Mobile 服务，关闭所有服务器节点。
2. 如更新 Sophos Mobile 服务器 （第 21 页）中所述，更新第一个节点。
   这将同时更新数据库。
3. 启动更新后的服务器节点，并检查更新是否已成功。
4. 更新其他服务器节点。

提示
如果您使用独立的 EAS 代理，即使在所有 Sophos Mobile 服务器节点都停止时，您的托管设备也可以访问您的电子邮件服务器。这是因为，在未连接到 Sophos Mobile 服务器时，EAS 代理会缓存设备状态最多 60 分钟。

7.4 更新独立的 EAS 代理

要更新独立的 EAS 代理，请运行 EAS 代理安装程序，并按说明进行操作。安装程序将自动检测是否有目前安装的程序需要更新。

如果您在负载平衡器后使用 EAS 代理服务器节点群集，您可以按任意顺序对这些节点进行相互独立的更新。

提示
请勿在同一时间停止所有 EAS 代理服务器节点。这样可以确保在更新过程中，您的托管设备的电子邮件通讯不会受到影响。

8 技术参考

8.1 Sophos Mobile 服务器功能

Sophos Mobile 产品的核心组件是 Sophos Mobile 服务器。其主要功能包括:

- 服务器连接到 Internet。
- 服务器可用于设置高可用性环境。
- 管理员可以使用 Web 界面控制服务器。
- 最终用户可以使用自助服务门户注册他们自己的设备，或从管理员处获得已做好自动注册准备的设备。
- 托管的设备通过 HTTPS 与服务器同步。
- 可以使用现有的 Microsoft SQL Server 或 MySQL 数据库存储设备和应用程序信息。也可以让 Sophos Mobile 安装程序使用 Microsoft SQL Server Express 创建新的数据库。
- 数据库可以存放在相同的或单独的计算机上。这样就可以使用数据库群集。
- 服务器支持多租户设置，允许在同一台服务器上创建不同的客户。
- 可以通过集成的或独立的 EAS 代理访问电子邮件。对于独立方式，需要通过 HTTPS 访问 SMC 服务器。

Sophos Mobile 服务器是针对 Java EE (Enterprise Edition) 开发的。它安装和运行在经过严格测试、作为行业标准的 WildFly 应用程序服务器上。

服务器可以安装在虚拟环境中。

8.2 Sophos Mobile Web 界面

8.2.1 Sophos Mobile 管理界面

Sophos Mobile 通过 Web 界面进行管理，Web 界面通过登录和会话机制进行保护。可以实施密码策略。访问控制允许不同的用户角色。这些角色有不同的访问权限集。每个用户可以分配一个角色。

有关详细信息，请参阅 Sophos Mobile 管理员帮助。

8.2.2 超级管理员界面

超级管理员主要用于设置和管理进行设备管理的客户。第一个超级管理员帐户是在安装 Sophos Mobile 时创建的。请参阅安装和设置 Sophos Mobile 服务器 （第 5 页）。

以超级管理员身份登录到同样是在安装 Sophos Mobile 时创建的超级管理员客户。对于超级管理员客户，Sophos Mobile Admin 控制台将显示针对超级管理员任务的定制视图。

8.2.3 自助服务门户

自助服务门户通过登录、会话机制和密码策略进行保护。帐户必须由 Sophos Mobile 管理员设置，并且可以和某个租户关联。自助服务门户用于让最终用户注册其使用 Sophos Mobile 的设备。最终用户还可以对他们的设备执行任务，如远程锁定或远程擦除。他们可以执行的任务因设备平台和配置而不同。作为管理员，您可以配置最终用户可以使用的自助服务门户功能。

有关如何为最终用户配置自助服务门户的信息，请参阅 Sophos Mobile 管理员帮助。

9 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/ 中的 Sophos 社区，并搜索遇到相同问题的其他用户。
- 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/support/contact-support/support-query.aspx 联系我们的技术支持团队。

10 法律声明