SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

帮助 (Android)

产品版本号： 9.6

内容

1 辅助功能

Sophos Intercept X for Mobile 符合网页内容无障碍指南 (WCAG) 2.1 AA 级要求。您可以在相关信息中找到有关这些指南的更多信息。

我们建议您将 Sophos Intercept X for Mobile 与 TalkBack 配合使用，TalkBack 是 Android 设备包含的 Google 屏幕阅读器。您可以在相关信息中找到使用 TalkBack 的链接。如果您需要有关 TalkBack 的进一步帮助，请联系 Google 技术支持。

如果您想将辅助技术产品与我们的软件配合使用，建议您熟悉所选产品的工作方式和可用的键盘命令。

已知限制

由于 Android 操作系统的限制，只有 Android 9 或更高版本的屏幕阅读器用户可以使用标题进行导航。

相关信息

网页内容无障碍指南

Android 辅助功能帮助：开始在 Android 上使用 TalkBack

2 关于 Sophos Intercept X for Mobile

Sophos Intercept X for Mobile 可以保护您的 Android 设备和隐私，不会影响性能和电池使用寿命。采用 SophosLabs 提供的最新信息，在安装应用时自动扫描它是否包含恶意软件，防止数据丢失和意外损失。

3 仪表板

Sophos Intercept X for Mobile 仪表板提供了设备安全状态的概况。

功能的颜色因其状态而不同：

- 绿色：未发现问题
- 红色：发现问题
- 蓝色：功能已开启
- 灰色：功能已关闭或未配置

4 设备安全

与所有操作系统一样，Android 允许您配置使设备安全性较低的设置。Sophos Intercept X for Mobile 可以检查这些与安全相关的设置，并提供让您的设备更安全的建议。

注释
如果 Sophos Intercept X for Mobile 由 Sophos Mobile 管理，与安全相关的系统设置将由您的组织配置。

设备安全下列出的设置有不同的颜色，具体取决于其状态：

- 绿色（安全）：该设置可确保最大程度的设备安全性。
- 红色（不安全）：该设置可能导致安全问题。请按照建议进行更改。
- 黄色（未知）：Android 设备有不同的设置，具体取决于设备型号和 Android 版本。如果 Sophos Intercept X for Mobile 无法确定设置是否安全，则显示为黄色。请考虑进行更改。
- 灰色（关闭）：将关闭检查。在确定设备安全状态时，不考虑该设置。

点击设置可对其进行更改或了解有关设置如何影响设备安全的更多信息。

4.1 Update Advisor

Update Advisor 显示有关您的 Android 版本的信息，并检查是否有新的版本可用。

Update Advisor 使用 Sophos 安装统计信息来查找是否有新的 Android 版本可供您的设备使用。

要打开 Update Advisor，请在设备安全页面上选择最新的 Android 版本。

我们建议您自动安装更新。如果您的设备有可选设置执行此操作，请点击检查设置，并在设备的设置应用中开启自动更新。

5 网站筛选

您可以使用网站过滤功能指定要在打开之前发出警告的网站类型。这可以让您避免浏览包含恶意、不需要或非法内容的网站。

配置网站过滤

在仪表板上，可以在网络安全下找到网站过滤。

- 在网站过滤页面上，开启网站过滤。
- 要启用恶意网站过滤，请点击恶意内容并选择警告或阻止。
- 要启用特定类别的网站过滤，请点击该类别并选择警告或阻止。
- 允许列表：可以永久性地抑制特定的恶意或类别的页面的警告。如果您经常访问的其中一个页面属于触发警告或被阻止的类别，这将很有用。在网站过滤警告对话框中选择总是允许访问此页面。要再次过滤此类页面，请点击清除允许的页面列表。

提示
为了测试网站过滤，Sophos 创建了包含每个类别的示例页面的网站 sophostest.com。尽管其中一些页面被归类为具有潜在的攻击性或危险性，但是页面内容本身在所有情况下都是无害的。

支持的 Web 浏览器

当您使用受保护的浏览器下列出的其中一个应用时，网站过滤将会保护您。

支持的浏览器：

- Google Chrome
- Firefox
- Android Web 浏览器
- Microsoft Edge

在受保护的浏览器（未经测试）下列出可能运行正常但尚未经过测试的应用。

提示
如果您的设备上安装了支持的 Web 浏览器，但没有在受保护的浏览器下列出，请检查 Sophos 辅助功能服务是否开启（在系统设置的辅助功能下）。

6 Link Checker

您可以使用 Link Checker 检查电子邮件或文档中的链接是否包含恶意或不良的内容。

Link Checker 可以处理您在非浏览器应用中点击的所有链接。您可以使用网络筛选检查网页上的链接。请参阅网站筛选 （第 5 页）。

在仪表板上，可以在网络安全下找到 Link Checker。

要设置 Link Checker：

1. 在 Link Checker 页面上，开启 Link Checker。
2. 选择您常用的浏览器应用打开 Web 链接。
3. 在您开启 Link Checker 后首次点击链接时，Android 会要求您选择用于打开该链接的应用。选择 Sophos Link Checker。

当您点击链接时，链接将传递到 Link Checker，并根据 SophosLabs 提供的分类，检查是否包含恶意或不良内容。然后，链接将在您的浏览器中打开。

注释

对于那些在内部打开链接，而不是将链接传递到浏览器的应用，Link Checker 不能在这些应用中检查链接。如果应用让您选择如何打开网页链接，请使用浏览器，这样 Link Checker 才能对链接进行处理。

例如，在 Gmail 中，该设置称为在 Gmail 中打开 Web 链接。关闭该设置可以让 Link Checker 检查您的电子邮件中的链接。

7 Wi-Fi Security

您可以使用 Wi-Fi Security 检查您的 Wi-Fi 连接是否存在基于网络的威胁。

注释
如果 Sophos Intercept X for Mobile 已注册到 Sophos Mobile，此功能将由您的组织管理。

在仪表板上，可以在网络安全下找到 Wi-Fi Security。

问题类型

Sophos Intercept X for Mobile 可以检测以下问题：

ARP 欺骗	ARP 欺骗是指攻击者向您的计算机发送恶意的地址解析协议 (ARP) 消息，使其相信攻击者的 MAC 地址与您的网络网关的 IP 地址是关联的。这让他们可以访问您的私人网络、窃取敏感数据，并发起其他攻击，如拒绝服务或中间人攻击。
强制网络门户	强制网络门户是公共 Wi-Fi 网络要求在授予网络访问权限前进行身份验证的方式。因为所有数据流都被重定向到强制网络门户，您可能会收到额外的警告。
内容操纵	内容操纵是指攻击者操纵网站的内容，迫使您执行有害的操作。这让他们可以做一些绕过身份验证或删除数据之类的事情。
SSL 拦截	SSL 拦截是指攻击者利用虚假的服务器证书，拦截您的计算机与网站之间的安全连接。攻击者可以解密敏感数据，同时让您相信您的连接仍然是安全的。
SSL 隔离	SSL 隔离是指攻击者将与网站的连接从安全的 HTTPS 降级为不安全的 HTTP。攻击者可以通过自己的代理服务器，重定向您的计算机和网站之间的所有数据流。这让他们可以解密敏感数据，同时让您相信您仍然通过 HTTPS 连接。

运行检查

- 要检查您连接的 Wi-Fi 网络，请点击检查 Wi-Fi。
- 要在后台自动执行网络检查，请开启后台检查。这样，设备每次连接到 Wi-Fi 网络时，都会进行检查。

8 应用安全

您可以扫描设备是否包含恶意应用或文件。

Sophos Intercept X for Mobile 可以扫描设备是否包含恶意软件，并报告所有恶意或可能不需要的应用。扫描程序使用在线查找的方法，通过对比 SophosLabs 云数据库中的最新威胁数据，对应用进行检查。同时，内置的全功能扫描引擎无论是在线还是离线环境下都能改善检测的效果。通过对 Android 威胁全天 24 小时的不间断分析，SophosLabs 不断更新防病毒数据。

执行扫描

Sophos Intercept X for Mobile 在应用安装时对其进行扫描。此外，您还可以配置计划扫描和运行手动扫描。

要配置计划扫描：

在应用设置中，选择计划扫描，然后在计划的扫描间隔中选择扫描间隔。您还可以配置扫描设备的哪些部分以及报告哪些类型的应用。

要运行手动扫描：

在应用安全页面上，选择显示扫描详细信息，然后选择开始。

查看扫描结果

在应用安全页面上，扫描结果的概要情况显示在应用安全问题下。

要查看单个问题，请选择显示扫描详细信息。

要查看有关问题的更多详细信息，请选择威胁和可能不需要的应用下所列的应用，并打开其对象详细信息页面。在该页面上，您可以：

- 查看应用的安装方式及其请求的权限。
- 查看威胁描述。
- 在您的浏览器中打开包含详细威胁信息的网页。
- 卸载该应用。
- 允许该应用。

相关参考

设置 （第 20 页）

9 验证器

使用验证器生成一次性密码（也称为验证码），以登录使用多因素身份验证的帐户。

请与您的帐户提供者确定您的帐户是否支持多因素身份验证，以及如何启用多因素身份验证。

验证器支持基于时间和基于计数器的一次性密码。请参阅关于一次性密码 （第 9 页）。

要启动验证器，请长按 Sophos 图标，然后点击验证器。

功能：

- 对于基于时间的密码，验证器将显示当前有效的一次性密码和一个动画图标，动画图标描述密码将变为无效并计算下一个密码前的剩余时间。
- 对于基于计数器的密码，点击帐户条目旁边的刷新可生成新的一次性密码。为防止在一行中意外生成多个密码，每次生成密码后，在可以生成下一个密码前，会有几秒钟延迟。
- 要将帐户当前的一次性密码复制到剪贴板，请点击并按住帐户条目，然后点击复制。
- 要编辑帐户的详细信息，请点击并按住帐户条目，然后点击编辑。出于安全原因，您不能显示或编辑密钥。
- 要删除帐户，请点击并按住帐户条目，然后点击删除。

警告
删除验证器项后，您将会失去为该帐户生成一次性密码的能力。这不会关闭多因素身份验证。删除验证器项可能会让您无法登录到您的帐户。

删除某项前，请确保您有替代方法生成一次性密码，或有替代方法登录到您未采用多因素身份验证的帐户。

9.1 关于一次性密码

一次性密码（也称为验证码）由多个数字组成。它们是通过以下参数计算的：

- 只有您的帐户提供者和您自己才知道的共享密钥。
- 特定于您的帐户提供者的配置值。
- 连续的计数器。

使用一次性密码自己进行身份验证时，您的帐户提供者需要通过特定计数器值计算的密码。因为验证器使用与您的帐户提供者相同的规则确定当前的计数器值，所以提供者将接受您的一次性密码。

验证器支持基于时间和基于计数器的一次性密码。这些类型不同于确定当前计数器值的方式：

- 基于时间的一次性密码（TOTP，依据 RFC 6238）：计数器值基于当前时间不断递增。验证码序列中的下一个值在经过定义的时间段时生成。
- 基于计数器的一次性密码（HOTP，依据 RFC 4226）：计数器值根据需要递增。验证码序列中的下一个值在您请求时生成。

9.2 通过 QR 码添加帐户

如果您为帐户启用了多因素身份验证，且您的帐户提供者向您提供了 QR 代码与配置详细信息，则可使用此过程。

1. 点击 +，然后点击扫描 QR 码。
2. 用您的设备扫描 QR 码。

该应用从 QR 码读取配置详细信息后，将设置新的验证器帐户。

9.3 手动添加帐户

如果您为帐户启用了多因素身份验证，且您的帐户提供者向您提供了一系列配置详细信息，则可使用此过程。

1. 点击 +，然后点击手动添加。
2. 在名称字段中，为新的验证器帐户键入一个名称。
3. 在密钥字段中，键入您的帐户提供者指定的密钥。该密钥特定于您的帐户，并且构成一次性密码的计算基础。
4. 在类型字段中，选择您的帐户提供者指定的计算类型。
5. 如果您的帐户提供者指定了其他设置，请点击高级显示其他输入字段。

   警告
   仅填写您的帐户提供者指定的信息。

   - 在颁发机构字段中，输入字符串，用于指示与帐户关联的提供者。
   - 在时间段字段中，以秒为单位输入有效期。仅适用于基于时间的一次性密码。
   - 在计数器字段中，输入计数器初始值。仅适用于基于计数器的一次性密码。
   - 在代码长度字段中，选择一次性密码的位数。
   - 在哈希算法字段中，选择用于计算一次性密码的哈希算法。
6. 可选： 在背景色字段中，为帐户条目选择一个颜色，以便在帐户列表中轻松地识别它。
7. 准备就绪后，点击确定 ✓。

将设置新的验证器帐户。

10 密码保险箱

您可以使用密码保险箱在受主密码保护的同一位置存储您的所有帐户数据。

要启动密码保险箱，请长按 Sophos 图标，然后点击密码保险箱。

您有以下选项：

- 创建新的密码保险箱文件。
- 导入现有的 KeePass KDBX 文件。编辑密码项时，只修改本地副本。

开启自动填入密码

在 iOS 12 和更高版本的设备中，您可以使用密码保险箱自动填入密码。

要为密码保险箱开启自动填入密码：

1. 进入设置，向下滚动到密码和帐户。
2. 点击自动填入密码并开启自动填入密码。
3. 在允许填充：下，选择 Intercept X。

现在，当提示您输入凭据时，只需在键盘上方的 QuickType 栏上点击密码即可访问密码保险箱。

10.1 创建密码保险箱项

要在密码保险箱文件中添加项或项组：

1. 在密码保险箱中，点击 +。
2. 选择您要创建的密码项类型：
    - 添加帐户项可创建具有适合 Web 帐户和类似项目的预定义字段的密码项。
    - 添加信用卡项可创建具有适合信用卡和类似项目的预定义字段的密码项。
    - 添加组可以在密码保险箱中创建一个文件夹来管理密码项。
3. 在密码项字段中输入您的数据。
4. 可选： 点击添加字段在项中添加自定义字段。

    如果为自定义字段开启受到保护，您必须点击该字段旁边的眼睛按钮以查看该值。此外，受保护字段也不会出现在搜索结果中。
5. 点击磁盘图标保存该项。

您可以使用密码数据，轻松登录到网页或应用中。请参阅使用密码数据登录 （第 12 页）。

10.2 生成密码

1. 打开您要为其生成密码的密码保险箱项。
2. 点击编辑 切换到编辑模式。
3. 点击密码字段旁边的 +，打开密码生成器。
4. 定义密码长度以及密码中必须包含的字符类型。
5. 点击生成密码，根据您指定的要求生成密码。

6. 如果您对生成的密码感到满意，则关闭密码生成器。密码会以所生成的值进行更新。
7. 保存该密码项。

10.3 使用密码数据登录

- 要将字段的值复制到剪贴板，请点击所需字段。
- 要显示受保护字段的值，请点击该字段旁边的眼睛图标。
- 要在 Web 浏览器中打开 URL，请点击它：要将 URL 复制到剪贴板，请点击并按住它。

提示
每次当您打开密码保险箱项时，Android 通知区域都会新增一条通知。通过该通知，您可以将用户名和密码值复制到剪贴板。

10.4 管理密码保险箱项

1. 点击并按住某个项可以切换到选择模式。
2. 可选： 选择您要对其执行相同操作的更多项。
3. 点击以下图标以执行所需操作：
   - 编辑：编辑该项内容。仅在选择单一项时可用。
   - 剪切：将所选项移动到密码保险箱文件中的其他组。
   - 复制：将所选项复制到密码保险箱文件中的其他组。
   - 删除：将所选项移动到特殊的回收站组。要永久删除密码项，请点击回收站组中密码项上的删除图标。
   - 要粘贴您剪切或复制的密码项，请导航至目标位置，然后点击剪贴板图标。

10.5 搜索密码保险箱项

在密码保险箱中，您可以搜索密码项和密码项组的名称，以及密码项字段的值。

注释
您不能搜索密码字段或已经配置为受保护的字段。

1. 在密码保险箱中，点击搜索切换到搜索模式。
2. 输入搜索字符串。输入后，搜索结果的列表会更新。

10.6 备份密码保险箱

定期备份您的密码保险箱文件非常重要。如果您丢失了密码保险箱文件，例如，因为您不小心删除了它或丢失了您的设备，您将不能访问您的密码数据，除非您有最近备份的副本。

1. 在密码保险箱中，点击更多，然后点击导出。
2. 选择要将密码保险箱文件导出到哪个应用。

将与您选择的应用共享密码保险箱文件的副本。

注释
我们建议您写下备份副本的位置，并将其存储在安全的位置。

11 QR 码扫描程序

您可以使用 QR 码扫描程序扫描 QR 码，然后处理嵌入的信息。

要启动 QR 码扫描程序，请长按 Sophos 图标，然后点击 QR 码扫描程序。

Web 地址

扫描 QR 码时，将根据 SophosLabs 提供的分类，检查嵌入的 URL 是否包含恶意或不良内容。

- 报告 URL 安全时，点击打开，在您的 Web 浏览器中将其打开。

联系人

扫描 QR 码，然后：

- 点击添加联系人，使用嵌入的名片信息在您的联系人中创建一个条目。
- 点击在地图中显示，在您的地图应用（默认情况下为谷歌地图）中显示嵌入的位置。
- 点击拨打电话，用嵌入的号码打电话。如果 QR 码包含多个电话号码，它们将按以下顺序依次使用：
  1. 移动电话号码
  2. 工作电话号码
  3. 住宅电话号码
- 点击发送电子邮件，创建一封新的电子邮件，发给嵌入的电子邮件地址。如果 QR 码包含多个电子邮件地址，所有这些电子邮件地址都将添加到收件人字段中。

Additional information

Sophos Intercept X for Mobile 可以读取 vCard 2.1 和 3.0 格式的名片信息。

Wi-Fi 配置

扫描 QR 码，然后点击连接到网络，连接到 QR 码中配置的 Wi-Fi 网络。

注释

如果尝试连接到不安全的网络，即不受 WPA 或 WPA2 保护的网络，将会收到警告 。

12 App Protection

您可以使用 App Protection 配置一个应用列表，列表中的应用仅在您进行自我授权后方可打开。这非常有用，例如，如果您想要将您的设备交予他人，这可用来防止他们使用特定的应用。

注释
如果 Sophos Intercept X for Mobile 由 Sophos Mobile 管理，App Protection 将不可用。App 访问权限由您所在的组织管理。

1. 在应用菜单中，选择 App Protection。
2. 在基本配置中，开启 App Protection。
3. Intercept X 应用必须是 Android 设备管理员。如果您还没有激活此功能，则会转到相关的 Android 设置页面。点击激活。
4. 选择 App Protection 的身份验证类型。
   您可以选择图案、PIN、密码或指纹（如果您的设备配备了指纹传感器）。

   注释
   如果 Sophos Intercept X for Mobile 由 Sophos Mobile 管理，管理员将可以关闭指纹身份验证。

5. 一些任务管理器可以通过终止其进程禁用 App Protection。要进行任务管理器保护，您需要安装 Sophos Security & Antivirus Guard 应用。基本配置中的消息将指出这一点。点击该消息并在 Google Play 中打开该应用，然后安装该应用。
6. 点击宽限期并选择时间长度，在这段时间内您退出应用并再次进入时您的密码将被记住。
7. 保护配置将列出可用于卸载或禁用应用保护的应用。还可以保护 Google Play 和其他安装程序，以防止在设备上不受控制地安装应用。
8. 向左轻扫。将显示应用选择视图。您可以：
   - 选择未受保护列表中的应用，对它们进行保护。这些应用将显示在受到保护列表中。
   - 取消选中受到保护列表中的应用，可让它们不受保护。这些应用将显示在未受保护列表中。

Sophos Security & Antivirus Guard 监控 App Protection 进程，并在必要时重启它们。

注释
如果您没有安装 Sophos Security & Antivirus Guard，在您离开 App Protection 设置时，系统将会再次提示您安装。强烈建议您这样做。

13 Privacy Advisor

Privacy Advisor 显示有关安装在您的设备上的应用所拥有的权限的信息。

注释
本节介绍 Android 6 及更高版本的 Privacy Advisor。对于 Android 5 的 Privacy Advisor，请参阅Privacy Advisor (Android 5) （第 18 页）。

Android 权限处理

权限是 Android 的中央安全机制，可以将某些权限授予一个应用。Android 版本 6 修改了应用请求权限的方式：

- 为 Android 6 或更高版本创建的应用在运行时请求您授予权限，即在您访问您尚未授予所需权限的应用的功能时。
- 为 Android 5 或以下版本（被称为旧应用）创建的应用在安装时请求所有所需的权限。在 Android 6 和更高版本上安装旧应用时，您可以拒绝请求的单项权限。但因为这种应用没有设计成处理这种情况，所以它可能会停止工作。

您可以在 Privacy Advisor 中看到什么

Privacy Advisor 向您显示被 Google 归类为危险的权限的状态，因为这些权限会影响您的隐私或其他应用的操作：

- 日历权限 日历
- 摄像头权限 相机
- 联系人权限 联系人
- 位置权限 位置
- 麦克风权限 麦克风
- 电话权限 电话
- 身体感应器权限 身体感应器
- 短信权限 短信
- 存储权限 存储

权限的状态可以是：

- 授权 请求且已授权
- 拒绝 请求但被拒绝

注释
对于旧的应用，即使您在应用设置中关闭权限，权限也会始终显示为“请求且已授权”。

您可以在 Privacy Advisor 中做什么

- 要查看应用请求的所有权限（包括不危险的权限）的详细信息：点击应用图标。
- 要授予或拒绝权限：点击应用图标，然后点击修改权限打开应用的应用信息页面。在其中点击权限。
- 要显示权限修改历史记录：点击标题栏中的 权限变更历史记录 。
- 要配置您可以在 Privacy Advisor 中看到什么：点击筛选。您可以排除特定的权限或特定类型的应用，如系统应用或旧应用。
- 要修改应用的顺序：点击排序 ，然后选择应用的排序方式。

14 Privacy Advisor (Android 5)

Privacy Advisor 显示有关安装在您的设备上的应用所拥有的权限的信息。

注释
本节介绍适用于 Android 5 的 Privacy Advisor。要了解适用于 Android 6 及更高版本的 Privacy Advisor，请参阅Privacy Advisor （第 16 页）。

有三个权限筛选器：

- 可能需要收费的应用程序

  一些应用程序可能会产生额外的费用。根据应用程序请求的权限，应用程序可能会呼叫收费服务电话号码、更改您电话的网络状态（当您的手机漫游时，可能需要收费）或不经您的允许发送短信。

- 可能侵犯您隐私的应用程序

  您的智能手机或平板电脑包含私人信息。获得特定权限的应用程序可读取您的联系人列表。您将无法控制应用程序会使用这些信息做哪些事情，因为您已经授予该应用程序使用这些信息的权限。结合特定连接权限，即使没有用户的操作允许，应用程序也可以很容易地将您所有的联系人信息发送到第三方。这类应用程序将会侵犯您的隐私。

- 可能访问互联网的应用程序

  目前，大多数应用程序需要连接到 Internet 的权限。与其他权限相结合，可能会给您带来巨大的安全问题。发送到 Internet 以及从 Internet 接收的信息无法被监控。检查应用程序是否需要 Internet 访问权限，以及该应用程序是否值得信赖。

Privacy Advisor 可以列出设备上安装的所有应用。三个 Privacy Advisor 筛选器的图标显示在屏幕的底部。点击图标可以启用或禁用相应的筛选器。

可以组合筛选器，以便显示拥有与当前所选筛选器相关的权限的所有应用程序。

所列出的应用程序根据应用程序的权限与所选筛选器的关联方式进行排列：

- 显示为红色的应用：应用请求的权限表明对于选定的筛选器具有高风险。
- 显示为黄色的应用程序：应用程序请求的权限表明相对于选定的筛选器来说具有普通风险。
- 显示为白色的应用程序：应用程序请求的权限表明相对于选定的筛选器来说具有低风险。

点击列表记录可以显示有关应用程序的详细信息。显示将表明应用程序拥有哪些权限，以及哪些权限可用于应用程序。

如果您要从设备中卸载应用，请点击卸载。

15 企业管理

在公司环境中，Sophos Intercept X for Mobile 可以由 Sophos Mobile 管理。这让您的组织可以监控设备的合规性状态。

要将 Sophos Intercept X for Mobile 注册到 Sophos Mobile，请按您的组织发送给您的说明进行操作。

如果 Sophos Intercept X for Mobile 由 Sophos Mobile 管理，会有以下差异：

- 应用设置由您的组织集中定义。
- 您的组织可以触发扫描，从而确定您的设备的安全状态。
- 如果您的设备不符合您所在组织的策略要求，网络访问或其他功能可能会受到限制。您可以在应用的仪表板上查看合规性状态。请参阅解决合规性违反问题 （第 19 页）。

注释
另外，您的组织也可以通过 Sophos Mobile Control 应用，管理您的设备或设备上的工作区。这为您的组织提供了甚至更多控制权，如安装或卸载应用，或关闭设备功能。在这种情况下，您可以通过 Sophos Mobile Control 应用，查看设备的合规性状态或联系 IT 团队。有关详细信息，请参阅 Sophos Mobile 用户帮助。

15.1 解决合规性违反问题

如果 Sophos Intercept X for Mobile 由 Sophos Mobile 管理，仪表板将根据您的组织策略显示合规性状态。

要查看和解决合规性违反问题：

1. 在仪表板上，点击公司管理。
   如果有合规性违反问量，图块将有红色图标。
2. 点击合规性违反问题，并按说明解决问题。

注释
如果您的设备不合规，网络访问或其他功能可能会受到限制。

15.2 获取支持

如果 Sophos Intercept X for Mobile 由 Sophos Mobile 管理，您可以显示有关如何联系 IT 团队的详细信息以及提供的所有其他信息。

在仪表板上，点击公司管理。

联系人详细信息将显示在 IT 部门联系人和附加信息下。

提示
可以点击电子邮件、电话或移动电话字段，撰写电子邮件或给 IT 团队打电话。

16 设置

设置	描述
计划扫描	执行自动定期扫描。
计划扫描间隔	计划扫描的频率。 如果您选择每天充电时，则设备会在连接到电源超过 30 分钟后执行扫描。
管理允许的应用程序	点击以显示允许应用的列表。这些应用不会显示在扫描结果中。可以从此列表中删除应用。您删除的所有应用将再次显示在威胁和可能不需要的应用列表中。
清除默认	点击可停止使用 Intercept X 作为打开支持链接的默认应用。
扫描系统应用	选中此选项可以在扫描中包括 Android 系统应用。 默认情况下不扫描系统应用，因为它们受到 Android 的保护，而且用户不能将它们删除。
扫描存储	选中此选项可以在扫描中包括 SD 卡和 USB 存储设备。
检测 PUA	选中此选项将开启对可能不需要的应用 (PUA) 的检测。 可能不需要的应用是指虽不是恶意软件，但通常被认为是不适合企业网络的应用。主要的 PUA 分类有广告软件、拨号器、系统监控、远程管理工具以及黑客工具。但是，某些被归为 PUA 的应用可能对用户很有帮助。
应用程序信誉	选中此选项将开启对低信誉应用的扫描。 低信誉应用是根据 Sophos Live Protection 数据具有较低信誉的应用。
扫描通知	选中此选项将开启有关清除应用的扫描通知。 如果不选中此选项，您将只收到有关恶意软件、可能不需要的应用以及低信誉应用的通知。 在 Android 设备上安装或从 SD 卡或 USB 存储设备启动应用时，Sophos Intercept X for Mobile 将对应用进行扫描。您可以在“通知面板”中找到通知。
监控存储	选中此选项将扫描所有下载或复制到 SD 卡或 USB 存储设备的新应用和文件。对于所有新连接的存储设备，扫描都将自动启动。
版本	防病毒引擎和防病毒数据的版本。
最近更新	从 Sophos 检索防病毒数据的日期。 点击可检查更新。

设置	描述
更新模式	此设置定义 Sophos Intercept X for Mobile 用于下载病毒检测数据更新的数据连接。
通过电子邮件发送日志	点击发送附带该应用日志文件的电子邮件。 默认情况下，会插入 Sophos 支持团队的电子邮件地址。
跟踪数据可帮助提高可用性	允许 Sophos 收集匿名的使用情况数据以改进该应用。
卸载 Sophos Intercept X for Mobile	点击可卸载 Intercept X 应用和关联的 Security & Antivirus Guard 应用（如果已安装）。

17 备份与恢复

例如，您可以备份应用设置，以便在其他设备上使用。

您可以备份以下内容：

- 设置
- 扫描程序
- 网站筛选
- App Protection
- 验证器

如果Sophos Intercept X for Mobile由Sophos Mobile托管，您只能备份验证器帐户。

备份设置

1. 在应用菜单中，选择备份和恢复。
2. 点击备份。
3. 选择您要导出的设置。
4. 点击备份。
5. 输入您的设备凭据并点击下一步。
6. 选择用于创建备份副本的位置。

   提示
   将备份保存到云存储，以便您可以在其他设备上使用。

7. 为文件输入名称，然后单击保存。
8. 为备份副本输入密码，确认并点击确定。

恢复设置

1. 在备份和恢复页面上，点击恢复。
2. 进入您保存文件的位置，并点击备份副本。
3. 输入备份副本的密码，并点击确定。
4. 选择您要恢复的设置。
5. 点击恢复。

18 日志记录

Sophos Intercept X for Mobile 在它自己的日志中记录重要的操作。这是对 Android 日志的补充。您不会收到有关应用程序执行后台操作的结果的直接反馈，如安装其他应用程序时扫描的恶意软件。日志提供了有关这些操作的详细报告。它详细记录了这些操作的执行时间和相关的结果。

- 要显示日志，请点击菜单 ≡，然后点击日志。
- 要清除日志，请点击标题栏中的删除 🗑。

19 法律声明