SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

帮助（iOS）

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 iOS 设备中包含的 VoiceOver 屏幕阅读器和 Zoom 放大软件配合使用。您可以在相关信息中找到使用 VoiceOver 和 Zoom 的链接。如果您需要有关 VoiceOver 或 Zoom 的进一步帮助，请联系 Apple 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。

相关信息

网页内容无障碍指南

iPhone 用户指南：在 iPhone 上打开和练习“旁白”

iPhone 用户指南：放大 iPhone 屏幕

2 关于 Sophos Intercept X for Mobile

Sophos Intercept X for Mobile 帮助您在 iPhone 或 iPad 设备上安全地工作。

如果长按 Sophos 图标，可以打开快速操作菜单。在 3D Touch 设备上，短按该图标即可看到菜单。

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

在设备安全下，您可以查看设备的运行状况。

Sophos Intercept X for Mobile 显示以下信息：

- 常规设备信息，如型号名称和 iOS 版本。
- 更新建议（如果您没有安装最新版本的 iOS）。
- 越狱信息（如果 Sophos Intercept X for Mobile 在设备上检测到越狱）。

5 网站过滤

您的组织可能会使用网站过滤功能让您避免浏览包含恶意、不需要或非法内容的网站。

如果您的组织管理您的设备，则可能会指定在您打开之前向您发出警告的网站类型，或屏蔽网站。这可以让您避免浏览包含恶意、不需要或非法内容的网站。

在仪表板上，可以在网络安全下找到网站过滤。

注释

- 您的组织必须开启此功能。

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的类别，这将很有用。向下滑动 Web 请求被阻止通知，并点击添加到允许列表。

在允许列表下，将显示允许的页面数。点击计数器可显示所有页面。

您添加的条目和您的组织预定义的条目显示在不同的部分。

要再次过滤某个页面，请向左滑动该条目将其删除。您只能对自己添加的条目执行此操作。

阻止列表

您可以将引发警告的网页添加到阻止列表，以便始终阻止这些网页。向下滑动 Web 请求被阻止通知，并点击添加到阻止列表。

在阻止列表下，将显示阻止的页面数。点击计数器可显示所有页面条目。

您添加的条目和您的组织预定义的条目显示在不同的部分。

要再次发出警告，请向左滑动该条目将其删除。您只能对自己添加的条目执行此操作。

6 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。 iOS 10.3 或更高版本的设备上无法检测 ARP 欺骗。
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。

隐藏问题

您可以隐藏特定网络的 Wi-Fi 问题。隐藏的问题不会影响设备的运行状况。

要再次显示所有问题，请在应用设置中选择显示所有 Wi-Fi 问题。

7 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 8 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，请点击点击获取代码生成第一个代码，或点击下一步生成第二个代码。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，请点击它。
- 要编辑帐户的详细信息，请点击编辑，选中帐户条目，然后点击修改。出于安全原因，您不能显示或编辑密钥。
- 要删除帐户，请点击编辑，选中帐户条目，然后点击删除 图标。

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。

7.1 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。

7.2 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. 选择创建 > 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。

7.3 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. 选择创建 > 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，请在以下字段中输入这些设置

   警告
   仅填写您的帐户提供者指定的信息。

   - 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，点击保存。

将设置新的验证器帐户。

8 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。
- 打开现有的 KeePass KDBX 文件。编辑密码项时，只修改原始文件。

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。

8.1 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，点击加号 ⊕。
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。
   - 备注可创建一条安全记录项。
   - 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： 点击加号 ⊕，然后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。

   使用加号 ⊕，您还可以在项中添加文件或图片。
5. 点击完成保存该项。

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 11 页）。

注释
如果您在项中附加的文件过大或过多，则可能会影响性能。我们建议您使用 Sophos Secure Workspace 应用对这些文件加密，将它们安全地存储起来。

8.2 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. 点击齿轮 图标打开密码生成器。
4. 定义密码长度以及密码中必须包含的字符类型。
5. 点击刷新 ，根据您的规范生成一个密码。
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。

8.3 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 Safari 中打开 URL，请点击 URL 字段旁边的地球 图标。

8.4 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。

8.5 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。

提示
如果您不想搜索整个密码保险箱文件，可以浏览到组或子组。该组中的所有项都按递归方式进行搜索。

1. 在密码保险箱中，向下扫，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。

8.6 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. 在该应用仪表板的密码保险箱图块中，点击信息 ⓘ。
2. 点击备份密码保险箱文件。
3. 选择用于创建备份副本的位置。

注释
我们建议您同时打印一份恢复表，以帮助您访问您的密码数据，例如，在您忘记主密码或丢失密钥文件时。请参阅打印密码保险箱恢复详细信息表 （第 12 页）。

8.7 打印密码保险箱恢复详细信息表

如果您忘记了密码保险箱主密码或丢失了密钥文件，则不能访问存储在密码保险箱中的数据。为防止出现这种情况，请打印包含所需信息的恢复详细信息表。

警告
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，仅有恢复详细信息表还不足以取回您的密码数据。请参阅备份密码保险箱（第 12 页）。

1. 在该应用仪表板的密码保险箱图块中，点击信息 ⓘ。
2. 点击打印恢复详细信息表。
3. 选择打印机和份数，然后点击打印。
4. 在打印输出中，填写以下信息：
   - 您的主密码
   - 您的密码保险箱文件的位置
   - 您的备份副本的位置
5. 将恢复详细信息表存储在安全的位置。
   每个能够访问恢复详细信息表和您的密码保险箱文件的人都可以读取您的密码数据。

如果您已用密钥文件保护密码保险箱文件，恢复详细信息表中将以 QR 码的形式包含该文件的指纹。您可以使用该 QR 码代替实际密钥文件打开您的密码保险箱文件。

9 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，点击继续，在 Safari 中将其打开。

联系人

扫描 QR 码，然后点击添加，使用嵌入的名片信息在您的联系人中创建一个条目。

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，然后点击复制，将密码复制到剪贴板。在设置中，进入 Wi-Fi，选择网络，并在提示时输入该密码。

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 。

10 消息过滤

您的组织可能会使用消息过滤来检查传入的短信/彩信消息是否包含钓鱼 URL。

可疑的消息将被过滤到单独的垃圾短信选项卡。

如果您在应用设置中看到开启消息过滤，则需要根据您的组织的要求在设置应用中开启消息过滤。

开启消息过滤

进入您的 iOS 设置应用，进入消息，点击未知与过滤信息并开启短信过滤下的 Intercept X。

消息应用中的垃圾短信选项卡

如果来自未知发件人的消息被确定为垃圾信息，该消息将被移至消息应用的垃圾短信选项卡。来自同一发件人的现有消息和后续消息也将移至垃圾短信。

注释

- 来自已知联系人的消息不会确定为垃圾信息。
- 消息过滤对 iMessages 不起作用。

11 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。
- 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 15 页）。

11.1 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。

11.2 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。

12 设置

设置	描述
开启消息过滤	检查传入的短信/彩信消息是否包含钓鱼 URL。您的组织必须开启此功能。请参阅消息过滤 （第 14 页）。
开启网站筛选	阻止连接到恶意或分类的网页。您的组织必须开启此功能。请参阅网站过滤 （第 5 页）。
显示所有 Wi-Fi 问题	显示所有 Wi-Fi 问题，包括您之前隐藏的问题。
日志等级	如果 Sophos 支持人员要求，请选择日志记录信息的级别。
发送日志文件	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。
数据跟踪	允许 Sophos 收集匿名的使用情况数据以改进该应用。

13 备份与恢复

您可以备份您的验证器帐户，以将其移动到新的 iOS 或 Android 设备。

备份帐户

1. 在应用菜单中，选择备份和恢复。
2. 点击备份。
3. 为备份副本输入名称。
4. 输入密码，确认密码，然后点击确定。
5. 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。

6. 点击添加。

恢复帐户

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。

14 法律声明