TREND MICRO™

9.8 趋势科技™ 移动安全™ 企业版 管理员指南

（适用于安全扫描部署模式）

Endpoint Security

文档编号 TSCM98142/180126

发布日期：2017 年 11 月

趋势科技™ 移动安全企业版用户文档介绍了产品的主要功能并提供了针对生产环境的安装说明。在安装或使用产品之前，请阅读该文档。

有关如何使用该产品中特定功能的详细信息，请参阅联机帮助与趋势科技网站上的知识库。

趋势科技一直致力于改进其文档。如对该文档或趋势科技的任何其他文档有任何问题、意见或建议，

请通过 service@trendmicro.com.cn 与我们联系。

我们始终欢迎您的反馈。

目录

前言

第 1 章：简介

第 2 章：移动安全入门

第 3 章：与其他 MDM 解决方案集成

第 4 章：管理移动设备

第 8 章：更新组件

第 9 章：查看和维护日志

第 10 章：使用通知和报告

第 11 章：疑难解答与联系技术支持

索引

前言

前言

欢迎使用趋势科技™ 移动安全企业版 9.8 管理员指南。本指南提供了关于所有移动安全配置选项的详细信息。包括的主题有：如何更新软件使防护处于最新状态以阻止最新安全风险，如何配置和使用策略以支持安全目标，如何在移动设备上配置扫描、同步策略及使用日志和报表。

本前言讨论了下列主题：

预期读者

本移动安全文档供管理员（负责管理企业环境中的 Mobile Device Agents）和设备用户使用。

管理员应了解 Windows 系统管理和移动设备策略的高级知识，包括：

- 安装和配置 Windows 服务器
- 在 Windows 服务器上安装软件
- 配置和管理移动设备
- 网络概念（例如，IP 地址、网络掩码、拓扑和 LAN 设置）
- 各种网络拓扑
- 网络设备及其管理
- 网络配置（例如，VLAN、HTTP 和 HTTPS 的使用）

移动安全文档

移动安全文档包括：

- *安装和部署指南* — 本指南通过移动安全简介帮助您启动并运行移动安全，同时帮助您进行网络规划和安装。
- *管理员指南* — 本指南提供了有关移动安全配置策略和技术的详细信息。
- *联机帮助* — 联机帮助的目的是提供所有主要产品任务的执行方法、使用建议以及特定方面的信息，例如有效的参数范围和最佳值。
- *自述文件* — 自述文件包含在联机或打印文档中未披露的最新的产品信息。主题包括新功能的说明、安装提示、已知问题和版本历史。
- *知识库* — 知识库是包含问题解决和故障排除信息的联机数据库。可提供关于已知产品问题的最新信息。要访问知识库，请打开：

  http://esupport.trendmicro.com/zh-cn/default.aspx

提示

趋势科技建议检查下载专区 (http://www.trendmicro.com/download/zh-cn/) 上的相应链接，获取对产品文档的更新。

文档约定

文档使用以下约定。

表 1. 文档约定

约定	描述
大写	首字母缩写词、缩写、某些命令名和键盘上的键
粗体	菜单和菜单命令、命令按钮、选项卡和选项
斜体	对其他文档的引用
`Monospace`	示例命令行、程序代码、Web URL、文件名和程序输出
导航 > 路径	到达特定窗口的导航路径 例如，**文件 > 保存**意思是单击**文件**，然后单击界面上的**保存**
注意	配置说明
提示	推荐或建议
重要信息	与所需或缺省配置设置相关的信息以及产品限制
警告!	重要处理措施和配置选项

第 1 章

简介

趋势科技™ 移动安全企业版 9.8 是一套应用于移动设备的集成式安全解决方案。请阅读本章，以了解移动安全的组件、功能以及它们是如何保护您的移动设备的。

本章包括以下几节内容：

了解移动设备威胁

由于标准化平台的使用及其不断增强的连接能力，移动设备越来越容易受到更多威胁。在移动平台上运行的恶意软件程序数量不断增加，越来越多的垃圾信息通过短信发送。新的内容来源（例如，WAP 和服务信息）也被用于提供不需要的内容。

此外，移动设备盗用可能会危害个人数据或敏感数据。

关于趋势科技移动安全

趋势科技™ 移动安全企业版是一套应用于移动设备的全面的安全解决方案。移动安全结合了趋势科技防恶意软件技术，能有效防范最新的移动设备威胁。

集成的过滤功能使移动安全能够阻止发送到移动设备的不需要的网络通信。

此版本的移动安全独立于防毒墙网络版™，并且可以作为独立应用程序单独在 Windows 计算机上安装。

警告!

趋势科技无法保证移动安全与文件系统加密软件之间的兼容性。提供类似功能（例如防恶意软件扫描）的软件产品也可能与移动安全不兼容。

关于趋势科技移动安全中的机器学习

趋势科技预测机器学习使用高级机器学习技术关联威胁信息并执行深入的文件分析，以便通过数字 DNA 指纹验证、API 映射和其他文件功能来检测新兴未知安全风险。预测机器学习是一款功能强大的工具，有助于保护您的环境免受无法识别的威胁和零日攻击。

检测到未知或流行度较低的文件之后，移动安全使用新一代移动引擎扫描文件，以提取文件功能并向趋势科技云安全智能防护网络上托管的预测机器学习引擎发送报告。通过使用恶意软件建模，预测机器学习将示例与恶意软件模型

进行比较，指定概率分值并确定文件是否为恶意文件。移动安全可阻止安装受影响的文件并提醒用户将其卸载或删除。

移动安全系统的体系结构

根据公司需求，可以使用不同的客户端-服务器通信方法实施移动安全。也可选择在网络中使用一种客户机－服务器通信方法或任意几种方法的组合。

趋势科技移动安全支持三种不同的部署型号：

- 包含云通信服务器的增强安全型号（双服务器安装）
- 包含本地通信服务器的增强安全型号（双服务器安装）
- 基本安全型号（单服务器安装）

有关详细信息，请参阅*《安装和部署指南》*。

移动安全系统的组件

下表提供了移动安全组件的描述。

表 1-1. 移动安全系统的组件

组件	描述	必需或可选
管理服务器	利用管理服务器，可通过管理 Web 控制台管理移动安全客户端。移动设备注册到服务器后，即可配置移动安全客户端策略并执行更新。	必需

组件	描述	必需或可选
通信服务器	通信服务器处理管理服务器与移动安全客户端之间的通信。 Trend Micro Mobile Security 提供两种类型的 Communication Server： • 本地通信服务器 (LCS) — 这是在您的网络中本地部署的 Communication Server。 • Cloud Communication Server (CCS) — 这是在云中部署的 Communication Server，它不需要安装。趋势科技会管理 Cloud Communication Server，您只需要从管理服务器连接到该服务器即可。 请参阅 本地和云通信服务器的比较 第 1-5 页。	必需
移动安全客户端 (MDA)	移动安全代理安装在托管的 Android 和 iOS 移动设备上。该客户端与移动安全通信服务器通信并执行移动设备上的命令和策略设置。	必需
Microsoft SQL Server	Microsoft SQL Server 托管移动安全管理服务器的数据库。	必需
Active Directory	移动安全管理服务器从 Active Directory 导入用户和组。	可选
证书颁发机构	证书颁发机构负责管理安全凭证、公钥和私钥以保证安全通信。	可选
SCEP	简单证书注册协议 (SCEP) 是一种向私有证书颁发机构提供网络前端的通信协议。 在某些环境中，确保企业设置和策略得到保护、防止遭到窥探非常重要。为提供这种保护，可通过 iOS 对概要文件加密，如此一来，只有单个设备才能读取概要文件。加密的概要文件就像正常的配置概要文件一样，只是配置概要文件的有效负荷采用与设备 X.509 身份关联的公钥进行加密。 大型企业会将 SCEP 和证书颁发机构结合起来颁发证书。它可处理数字证书的颁发和撤销。SCEP 和证书颁发机构可以安装在同一服务器上。	可选

组件	描述	必需或可选
SSL 证书	（仅**完整版本**部署模式以及**安全扫描**部署模式且未列出 MDM 供应商的情况。） 为了在移动设备和使用 HTTPS 的通信服务器之间进行安全通信，趋势科技移动安全需要公认公共证书授权机构颁发的 SSL 服务器证书。	如果要管理 iOS 移动设备，则为必需
SMTP 服务器	连接 SMTP 服务器，以确保管理员能够从移动安全管理服务器获取报告，并向用户发送邀请。	可选

本地和云通信服务器的比较

下表提供了本地通信服务器 (LCS) 和云通信服务器 (CCS) 的比较。

表 1-2. 本地和云通信服务器比较

功能	Cloud Communication Server	本地通信服务器
是否需要安装	否	是
支持的用户身份验证方法	注册密钥	Active Directory 或注册密钥
Android 客户端定制	支持	支持

此版本 (9.8) 的新增功能

Trend Micro Mobile Security 9.8 新增了以下功能：

功能	描述
邀请电子邮件（仅限 Android）	使管理员能够在通过 AirWatch 部署移动安全客户端时向所有用户发送邀请电子邮件。

功能	描述
更多安全扫描和检测：	支持扫描移动设备的以下各项： • 恶意 SSL 证书 • 恶意 iOS 配置文件（仅限 iOS） • 网络流量解密 • 不安全的接入点 (Wi-Fi) • 开发人员选项和 USB 调试（仅限 Android） • 被篡改的应用程序
新增小部件、管理员通知和报告	针对恶意 SSL 证书、恶意 iOS 配置文件、网络流量解密、不安全的接入点 (Wi-Fi)、开发人员选项、USB 调试、被篡改的应用程序和具有 Root 权限的/越狱版移动设备引入新增小部件、管理员通知和报告。
应用程序允许列表	针对管理员引入允许列表以将检测为恶意软件、易受攻击的应用程序、隐私风险或被篡改的应用程序添加为安全应用程序，从而允许在移动设备上安装此类应用程序。
iOS 移动安全客户端支持	仅在 AirWatch 和 MobileIron 安全扫描模式下支持 iOS 移动安全客户端。

版本 9.7 Patch 3 的新增功能

Trend Micro Mobile Security 9.7 Patch 3 新增了以下功能：

功能	描述
提供 QR 码用于快速部署客户端 （仅安全扫描部署模式）	在客户端部署设置窗口上提供使用 QR 码进行注册的信息，用于快速轻松地部署客户端。 此功能仅在安全扫描部署模式下可用，并与 AirWatch 和 MobileIron 集成。
支持预测机器学习	支持趋势科技预测机器学习以执行深入的文件分析，从而检测新兴已知安全风险。

版本 9.7 Patch 2 的新增功能

Trend Micro Mobile Security 9.7 Patch 2 新增了以下功能：

功能	描述
与 MobileIron 移动设备管理解决方案集成	提供对 Android 和 iOS 移动设备的安全扫描，同时与以下 MobileIron 移动设备管理解决方案集成： • 已托管 MobileIron 核心 • 内部部署 MobileIron 核心
与联机帮助集成	将所有 UI 窗口链接到趋势科技联机帮助中心提供的帮助文件。
支持 iOS 激活锁 （仅完整版本部署模式）	激活锁是使用 iOS 7 或更高版本的移动设备内置的“查找我的 iPhone”功能。该功能要求用户在提供 Apple ID 和密码后才能关闭“查找我的 iPhone”、擦除或重新激活并使用移动设备，从而防止任何人重新激活丢失或被盗的移动设备。

版本 9.7 的新增功能

Trend Micro Mobile Security 9.7 新增了以下功能：

功能	描述
多个部署模式	可以使用以下模式部署 Trend Micro Mobile Security： • **完整版本**部署模式，它包括 Trend Micro Mobile Security 的所有功能。 • **仅安全**部署模式，在与其他移动设备管理 (MDM) 解决方案集成时，该模式提供对 Android 和 iOS 移动设备的安全扫描。
与 AirWatch 集成	与 AirWatch 移动设备管理解决方案集成时提供对 Android 和 iOS 移动设备的安全扫描。

功能	描述
“控制台”窗口上的网络安全新闻小部件	在**控制台**窗口上包括一个小部件，用于为移动设备显示趋势科技发布的网络安全新闻。
Android 设备上的服务器证书验证	让您能够在 Android 移动设备上执行服务器证书验证。
用于安全扫描的新 MARS API	集成最新的移动应用程序信誉服务 (MARS) API，以增强漏洞检测和描述。
支持最新 Android 和 iOS 版本	添加了 Android 7 和 iOS 10 支持。

版本 9.6 SP1 的新增功能

Trend Micro Mobile Security 9.6 SP1 新增了以下功能：

功能	描述
勒索软件检测小部件	通过“控制台”上的新小部件，管理员可以查看勒索软件检测统计信息。
Android 应用程序版本选择	管理员可以选择为 Android 和 iOS 设备部署**完整版本**或**仅安全扫描**应用程序。
Android 设备上的自动应用程序激活	此版本的移动安全在应用程序部署期间在 Android 设备上提供自动激活。
Exchange 服务器数据清除 （仅完整版本部署模式）	在传输到其他 Exchange 服务器之前，管理员可以执行数据清除。这让管理员可以删除移动安全上的现有 Exchange 连接器和 Exchange ActiveSync 设备数据。
对多个 Active Directory 用户应用组设置	管理员可以对多个 Active Directory 用户应用组设置。
按设备平台生成报告	通过改进报告生成功能，管理员可以为选定设备平台生成报告。

功能	描述
设备信息更新	在下一次预设更新之前，管理员可以更新托管移动设备的设备信息。

版本 9.6 的新增功能

Trend Micro Mobile Security 9.6 新增了以下功能：

功能	描述
用户管理	使管理员可以分别管理用户和邀请。
按需报告	管理员现在可以选择根据需要生成报告。
预设扫描	使管理员可以基于指定的预设每日、每周或每月运行一次恶意软件扫描和安全扫描。
适用于 Android 的安全扫描	除了隐私扫描外，移动安全现在还支持漏洞扫描和已被篡改的应用程序扫描以提高安全性。
新增小部件	此版本新增了五个小部件，用于显示有关 Android 安全扫描和 iOS 恶意软件扫描的信息。
新增 iOS 应用程序版本	管理员可以选择部署新版本的 iOS 应用程序，该新版本仅支持安全扫描，并与第三方移动设备管理 (MDM) 应用程序结合使用。

移动安全代理的主要功能

功能名称	描述		Android	iOS
安全扫描	移动安全结合了趋势科技防恶意软件技术，可有效检测威胁并防止攻击者利用移动设备上的漏洞。移动安全特别设计用于扫描移动威胁。	恶意软件扫描	●	●
		隐私扫描	●	
		漏洞扫描	●	
		被篡改的应用程序扫描	●	●
		USB 调试扫描	●	
		开发人员选项扫描	●	
		具有 Root 权限的移动设备扫描	●	
		越狱版移动设备扫描		●
		恶意 iOS 配置文件扫描		●
		网络流量解密扫描	●	●
		恶意 SSL 证书扫描	●	●
		不安全的接入点 (Wi-Fi) 扫描	●	
身份验证	安装了移动安全代理后，移动设备用户需要提供身份验证信息，将移动设备注册到移动安全管理服务器。		●	●
定期更新	为防范最新威胁，可手动更新移动安全或将其配置为自动更新。为了节约成本，可以为“漫游”移动设备设置不同的更新频率。更新包括组件更新和移动安全程序补丁更新。		●	

功能名称	描述		ANDROID	IOS
移动安全客户端日志	管理服务器上提供的移动安全客户端日志。	应用程序扫描日志	●	●
		设备漏洞日志	●	●
		网络保护日志	●	●
		Web 威胁防护日志	●	
	移动安全客户端将用户日志保留在移动设备上。	恶意软件扫描历史记录	●	
		漏洞扫描日志	●	
		被篡改的应用程序扫描日志	●	
		隐私扫描历史记录	●	
		Web 阻止历史记录	●	

支持的移动设备操作系统功能

下表展示了趋势科技移动安全在每个平台上支持的功能列表。

表 1-3. 趋势科技移动安全 9.8 功能矩阵

策略	功能	设置		
设备安全	安全设置	实时扫描		●
		病毒码更新后扫描		●
		手动扫描	●	●
数据保护	Web 威胁防护	服务器端控制		●

策略	功能	设置		
		使用阻止列表		●
		使用允许列表		●
		仅允许特定 Web 站点		●
		允许有限的成人内容		●

第 2 章

移动安全入门

本章将帮助您了解如何使用移动安全并且提供了基本的使用说明。在继续前，请确认已在移动设备上安装管理服务器、通信服务器和移动安全客户端。

本章包括以下几节内容：

管理 Web 控制台

可通过移动安全管理 Web 控制台访问配置窗口。

Web 控制台是用于管理和监控企业网络中移动安全的中心点。控制台附带一组缺省设置和值，可根据安全需求和规格进行配置。

可使用 Web 控制台执行以下操作：

- 管理安装在移动设备上的移动安全代理
- 配置移动安全代理的安全策略
- 在单个或多个移动设备上配置扫描设置
- 将设备分组为易于配置和管理的逻辑组
- 查看注册和更新信息

访问管理 Web 控制台

过程

1. 使用以下 URL 结构登录管理 Web 控制台：

   ```
   https://
   <External_domain_name_or_IP_address>:<HTTPS_port>/mdm/web
   ```

   注意

   将 <External_domain_name_or_IP_address> 替换为实际 IP 地址，将 <HTTPS_port> 替换为管理服务器的实际端口号。

将显示以下窗口。

图 2-1. 管理 Web 控制台登录窗口

2. 在提供的文本框中键入用户名和密码，并单击**登录**。

注意

管理 Web 控制台的缺省**用户名**为 “root”，**密码**为 “mobilesecurity”。

首次登录后，确保更改用户 “root” 的管理员密码。有关步骤，请参阅编辑管理员帐户 第 2-13 页。

重要信息

如果使用 Internet Explorer 访问管理 Web 控制台，请确保以下事项：

- **Web 站点的兼容性视图**选项已关闭。有关详细信息，请参阅关闭 Internet Explorer 中的兼容模式 第 2-4 页。
- 浏览器中已启用 JavaScript。

注意

如果无法使用 Metro 模式下的 Internet Explorer 10 访问 Windows 2012 中的管理 Web 控制台，验证 Internet Explorer 中的**增强保护模式**选项是否已禁用。

关闭 Internet Explorer 中的兼容模式

趋势科技移动安全不支持 Internet Explorer 中的**兼容性视图**。如果使用 Internet Explorer 来访问移动安全管理 Web 控制台，则为该 Web 站点关闭 Web 浏览器的兼容性视图（如果已启用）。

过程

1. 打开 Internet Explorer 并单击**工具** > **兼容性视图设置**。

   显示**兼容性视图设置**窗口。

2. 如果管理控制台已添加到**兼容性视图**列表，选择该 Web 站点并单击**删除**。

3. 清除**在兼容性视图中显示 Intranet 站点**和**在兼容性视图中显示所有网站**复选框，然后单击**关闭**。

产品使用授权

评估版使用授权到期后，所有的程序功能将被禁用。完整使用授权版本使您即使在使用授权到期后，也能继续使用所有功能。但是，需要注意的是，移动安全客户端将无法从服务器获取更新，这会使防恶意软件组件容易受到最新的安全风险的威胁。

如果使用授权过期，则需要使用新的激活码注册移动安全管理服务器。有关详情，请咨询当地的趋势科技销售代表。

要下载更新并允许远程管理，移动安全客户端必须注册到移动安全管理服务器。有关如何在移动设备上手动注册移动安全客户端的说明，请参阅*《安装和部署指南》*。

要查看管理服务器的使用授权升级说明，请在移动安全**产品使用授权**窗口中单击**查看使用授权升级说明**链接。

控制台信息

当您访问管理服务器时，首先显示的是**控制台**窗口。此窗口提供了移动设备的注册状态和组件详细信息的概览。

“控制台”窗口分为两个选项卡：

- **摘要** — 显示与移动设备相关的网络安全新闻、移动设备健康和安全状态以及移动设备操作系统版本摘要。
- **安全** — 显示 Android 设备漏洞扫描摘要、iOS 设备漏洞扫描摘要、Android 网络保护摘要、iOS 网络保护摘要、Android 应用程序风险摘要、iOS 应用程序风险摘要。在此类别中，您可以看到下列小部件和状态：
  - **Android/iOS 漏洞摘要：**
    - **Root 权限：**（仅限 Android）具有 Root 权限的移动设备数量
    - **USB 调试：**（仅限 Android）已启用 USB 调试模式的移动设备数量
    - **开发人员选项：**（仅限 Android）已启用开发模式的移动设备数量
    - **越狱版：**（仅限 iOS）越狱版移动设备的数量
    - **恶意 iOS 配置文件：**（仅限 iOS）已安装恶意 iOS 配置文件的移动设备数量
  - **Android/iOS 网络保护摘要：**
    - **不安全的接入点 (Wi-Fi)：**（仅限 Android）使用弱密码或不使用密码连接到可疑或不安全的接入点 (Wi-Fi) 的移动设备数量
    - **网络流量解密：**通过已解密的网络流量检测到的移动设备数量
    - **恶意 SSL 证书：**已安装恶意 SSL 证书的移动设备数量
  - **Android/iOS 应用程序风险摘要：**
    - **恶意软件：**检测为恶意软件的已安装应用程序数量

- **漏洞应用程序**：（仅限 Android）检测为易受攻击的已安装应用程序数量
- **隐私风险**：（仅限 Android）检测到泄露隐私的已安装应用程序数量
- **被篡改的应用程序**：应用程序包被篡改的已安装应用程序数量

自定义控制台

移动安全让您能够根据需要和要求自定义**控制台**信息。

添加新选项卡

过程

1. 在**控制台**窗口中，单击 + 按钮。
2. 在**新选项卡**弹出窗口上，执行以下步骤：
   - **标题**：键入选项卡名称。
   - **布局**：为显示在选项卡上的小部件选择布局。
   - **自动适应**：选择**打开**或者**关闭**以启用或者禁用选项卡上小部件的设置。
3. 单击**保存**。

删除选项卡

过程

1. 单击选项卡，然后单击选项卡中显示的 × 按钮。

2. 单击确认弹出式对话框上的**确定**。

添加小部件

过程

1. 在**控制台**窗口中，单击要添加小部件的选项卡。
2. 单击选项卡右上方的**添加小部件**。

   显示**添加小部件**窗口。
3. 从左侧菜单中选择类别以及/或者在搜索文本框中键入关键词，以显示相关小部件列表。
4. 选择要添加的小部件，然后单击**添加**。

   所选的小部件会出现在**控制台**的选项卡中。

删除小部件

过程

1. 在**控制台**窗口中，单击要删除小部件的选项卡。
2. 在要删除的小部件上，单击小部件右上方的 ×。

更改小部件的位置

过程

1. 在**控制台**窗口中，单击要重新安排小部件的选项卡。

2. 单击并按住小部件的标题栏，然后将其拖放到新的位置。

刷新小部件上的信息

过程

1. 在**控制台**窗口中，单击要刷新小部件的选项卡。
2. 在要刷新的小部件上，单击小部件右上方的 。

查看或修改选项卡设置

过程

1. 在**控制台**窗口中，单击要查看或修改其设置的选项卡。
2. 单击**选项卡设置**。
3. 根据要求修改设置，然后单击**保存**。

管理设置

配置 Active Directory (AD) 设置

趋势科技移动安全使您能够根据 Active Directory (AD) 配置用户授权。您还可以使用 AD 向设备列表添加移动设备。有关详细配置步骤，请参见*《安装和部署指南》*中的*服务器的初始设置*一节。

配置用户身份验证

趋势科技移动安全使您能够根据 Active Directory (AD) 或通过注册密钥来配置用户身份验证。有关详细配置步骤，请参见*《安装和部署指南》*中的*服务器的初始设置*一节。

配置数据库设置

有关详细配置步骤，请参见*《安装和部署指南》*中的*服务器的初始设置*一节。

配置通信服务器设置

有关详细配置步骤，请参见*《安装和部署指南》*中的*服务器的初始设置*一节。

配置部署设置

有关详细配置步骤，请参见*《安装和部署指南》*中的*服务器的初始设置*一节。

从完整版本切换到安全扫描部署模式

您可以随时切换移动安全的部署模式。

有关从**完整版本**部署模式切换到**安全扫描**部署模式的信息，请参阅以下知识库文章：

https://success.trendmicro.com/solution/1115884

配置 AirWatch 与趋势科技移动安全集成

您可以使用趋势科技移动安全集成 AirWatch 设备管理解决方案。

有关详细信息，请参阅与 AirWatch 集成 第 3-2 页。

配置 MobileIron 与趋势科技移动安全集成

您可以使用趋势科技移动安全集成 MobileIron 设备管理解决方案。

有关详细信息，请参阅与 MobileIron 集成 第 3-15 页。

管理管理员帐户

管理员帐户管理窗口让您能够为管理服务器创建拥有不同访问角色的用户帐户。

缺省管理员帐户名称和角色

缺省管理员帐户是“root”（密码：“mobilesecurity”）。root 帐户只能修改不能删除。有关详细步骤，请参阅编辑管理员帐户 第 2-13 页。

表 2-1. root 帐户属性

ROOT 帐户属性		是否可以修改？
管理员帐户	帐户名称	否
	全名	是
	密码	是
	电子邮件地址	是
	手机号码	是
管理员角色	管理员角色修改	否

缺省管理员角色为**超级管理员**，对所有设置拥有最大访问权。**超级管理员**角色只能修改不能删除。有关详细步骤，请参阅编辑管理员角色 第 2-15 页。

表 2-2. 超级管理员角色属性

超级管理员角色属性		是否可以修改？
角色详细信息	管理员角色	否
	描述	是
组管理控制	托管组	否

表 2-3. 超级管理员和组管理员的访问权

服务器组件	权限	超级管理员	组管理员
管理	更新	支持	不支持
	管理员帐户管理	可以修改所有帐户	只能修改自身帐户信息
	设备注册设置	支持	不支持
	证书管理	支持	支持
	命令队列管理	可以管理所有命令	只能查看相关组的命令
	数据库设置	支持	不支持
	通信服务器设置	支持	不支持
	Active Directory 设置	支持	不支持
	管理服务器设置	支持	不支持
	部署设置	支持	不支持
	配置和验证	支持	不支持
	产品使用授权	支持	不支持

服务器组件	权限	超级管理员	组管理员
通知/报告	日志查询	所有组	仅托管组
	日志维护	所有组	仅托管组
	管理员通知/报告	支持	不支持
	用户通知	支持	不支持
	设置	支持	不支持
应用程序		支持	仅支持托管组
策略	创建策略	支持	仅支持托管组
	查看策略	支持	仅支持托管组
	复制策略	支持	仅支持托管组
	删除策略	支持	仅支持托管组
设备	查看设备	支持	仅支持托管组
	添加组	支持	支持
用户	邀请用户	支持	仅支持托管组

添加管理员帐户

过程

1. 在移动安全管理 Web 控制台上，转到**管理** > **管理员帐户管理**。
2. 在**管理员帐户**选项卡上，单击**创建**以添加新帐户。

   显示**创建管理员帐户**窗口。
3. 在**帐户详细信息**下，执行以下操作之一：
   - 选择**趋势科技移动安全用户**，并指定以下用户帐户详细信息：
     - **帐户名称**：用于登录管理服务器的名称。

- **全名**：用户的全名。
- **密码**（以及**确认密码**）。
- **电子邮件地址**：用户的电子邮件地址。
- **手机号码**：用户的手机号码。

- 选择 **Active Directory 用户**，并执行以下操作之一：

  a. 在搜索文本框中键入用户名，并单击**搜索**。

  b. 请从左侧列表中选择用户名，然后单击 > 将用户移到右侧**选择的用户**列表中。

注意

要从右侧**选择的用户**列表中删除用户，选择用户名并单击 <。

还可以通过在单击用户名的同时按住 Ctrl 或 Shift 键同时选择多个用户。

4. 在**管理员角色**部分下，从**选择管理员角色:** 下拉列表中选择角色。

   有关创建管理员角色的步骤，请参阅创建管理员角色 第 2-14 页

5. 单击**保存**。

编辑管理员帐户

过程

1. 在移动安全管理 Web 控制台上，转到**管理** > **管理员帐户管理**。
2. 在**管理员帐户**选项卡上，单击**创建**以添加新帐户。

   显示**编辑管理员帐户**窗口。
3. 按需要修改管理员帐户详细信息和访问角色。
   - 帐户详细信息
     - **帐户名称**：用于登录管理服务器的名称。

- **全名**：用户的全名。
- **电子邮件地址**：用户的电子邮件地址。
- **手机号码**：用户的手机号码。
- **密码**：单击**重置密码**更改用户帐户密码，在**新密码**和**确认密码**文本框中键入新密码，并单击**保存**。

- **管理员角色**
  - **选择管理员角色**：从下拉列表中选择管理员角色。

    有关创建管理员角色的步骤，请参阅创建管理员角色 第 2-14 页。

4. 单击**保存**。

删除管理员帐户

过程

1. 在移动安全管理 Web 控制台上，转到**管理** > **管理员帐户管理**。
2. 在**管理员帐户**选项卡上，选择要删除的管理员帐户，然后单击**删除**。

   将显示确认消息。

创建管理员角色

过程

1. 在移动安全管理 Web 控制台上，转到**管理** > **管理员帐户管理**。
2. 在**管理员角色**选项卡中，单击**创建**。

   显示**创建管理员角色**窗口。

3. 在**角色详细信息**部分下，提供以下信息：
   - 管理员角色
   - 描述
4. 在**组管理控制**部分下，选择此管理员角色可以管理的移动设备组。
5. 单击**保存**

编辑管理员角色

过程

1. 在移动安全管理 Web 控制台上，转到**管理** > **管理员帐户管理**。
2. 在**管理员角色**选项卡中，单击**创建**。

   显示**创建管理员角色**窗口。
3. 根据需要修改角色详细信息，然后单击**保存**。

删除管理员角色

过程

1. 在移动安全管理 Web 控制台上，转到**管理** > **管理员帐户管理**。
2. 在**管理员角色**选项卡上，选择要删除的管理员角色，并单击**删除**。

   将显示确认消息。

更改管理员密码

请参阅主题编辑管理员帐户 第 2-13 页，获取更改管理员帐户密码的程序。

命令队列管理

移动安全会保留您从 Web 控制台执行的所有命令的记录，让您能够取消或重新发送命令（如果需要）。您还可以删除已经执行且不需要显示在列表中的命令。

要访问**命令队列管理**窗口，请转到**管理** > **命令队列管理**。

下表介绍了**命令队列管理**窗口中的所有命令状态。

命令状态	描述
等待发送	移动安全管理服务器正在将命令发送到移动设备。 您可以取消处于此状态的命令。
等待确认	移动安全管理服务器已经将命令发送到移动设备，且正在等待移动设备确认。
不成功	无法在移动设备上执行命令。
成功	已成功在移动设备上执行命令。
已取消	在命令在移动设备上执行之前，命令已取消。

为避免命令在硬盘上占用过多空间，请手动删除命令或配置移动安全管理 Web 控制台，以便根据**命令队列维护**窗口中的预设自动删除命令。

配置删除旧命令的预设

过程

1. 单击**管理** > **命令队列管理**。

   将显示**命令队列管理**窗口。

2. 在**命令队列维护**选项卡上，选择**启用预设命令删除**。
3. 指定您要删除的旧命令的数量。
4. 指定命令队列删除频率和时间。

5. 单击**保存**。

手动删除旧命令

过程

1. 单击**管理** > **命令队列管理**。

   将显示**命令队列管理**窗口。

2. 在**命令队列维护**选项卡上，选择**启用预设命令删除**。
3. 指定您要删除存在了多少天的旧命令。
4. 单击**立即删除**。

管理证书

使用**证书管理**窗口将 .pfx、.p12、.cer、.crt、.der 证书上传至移动安全管理服务器。

上传证书

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**管理** > **证书管理**。
3. 单击**添加**。

   将出现**添加证书**窗口。

4. 单击**选择文件**，然后选择 .pfx、.p12、.cer、.crt、.der 证书文件。

5. 在**密码**文本框中键入证书密码。
6. 单击**保存**。

删除证书

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**管理** > **证书管理**。
3. 选择要删除的证书，然后单击**删除**。

第 3 章

与其他 MDM 解决方案集成

您可以使用趋势科技移动安全将其他移动设备管理解决方案与移动安全集成。

本章介绍了设置移动安全与其他移动设备管理解决方案集成的过程。

本章包含下列主题：

与 AirWatch 集成

您可以使用趋势科技移动安全将 AirWatch MDM 解决方案与移动安全集成。

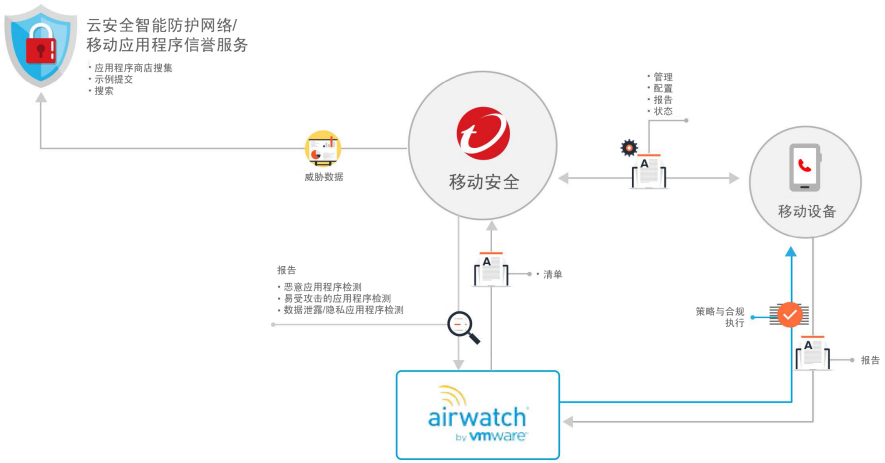
集成的先决条件

要将其他 MDM 解决方案与趋势科技移动安全集成，必须使用以下产品：

- 移动安全企业版 9.7 或更高版本
- 在移动安全中配置的本地通信服务器或云通信服务器
- AirWatch v9.1 或更高版本
- AirWatch 管理 Web 控制台上的管理员帐户

AirWatch 集成体系结构

下图显示了与 AirWatch 集成的高级体系结构。



移动应用程序信誉是一种基于云的技术，可以基于应用程序行为自动识别移动威胁，从各种 Android Market 爬网并收集大量的 Android 应用程序，识别现有移动恶意软件和全新移动恶意软件，识别可能会滥用隐私/设备资源的应用程序。这是全球首个自动移动应用程序评估服务。

趋势科技云安全智能防护网络提供针对零小时威胁的主动型全球威胁情报，以确保您始终受到保护。趋势科技使用最新的威胁情报即时消除攻击，让这些攻击没有机会得逞。**云安全智能防护网络**支持所有趋势科技产品和服务。

移动安全使用云安全智能防护网络和移动应用程序信誉服务来发现移动设备安全问题，并利用 AirWatch 合规策略来管理您的移动设备。

集成功能

趋势科技移动安全在与 AirWatch 集成方面提供以下功能：

功能	描述
移动设备自动分组	移动安全根据移动设备的风险等级添加 Dangerous、Risky、No_TMMS 后缀来标记移动设备。 有关详细信息，请参阅移动设备自动分组 第 3-4 页。
应用程序自动分组	移动安全根据移动应用程序的风险等级添加 Malware、Vulnerability 和 Privacy 前缀来对移动应用程序进行分组。 有关详细信息，请参阅移动应用程序自动分组 第 3-4 页。
AirWatch 违反策略的应用程序黑名单自动更新	使用此功能，可以（根据安全扫描结果）将应用程序放在违反 AirWatch 合规策略的黑名单中，并向用户发送电子邮件警报。 有关详细信息，请参阅配置 AirWatch 应用程序黑名单合规策略 第 3-5 页。

功能	描述
移动安全客户端应用程序自动部署	您可以将 AirWatch 配置为自动将移动安全客户端部署到移动设备。 • **Android**: 有关步骤，请参阅通过移动安全服务器部署 Android 客户端 第 3-11 页。 您还可以将 Samsung 移动设备配置为自动启动移动设备上的移动安全客户端。有关详细信息和过程，请参阅配置 Android 移动设备自动启动 第 3-12 页。 • **iOS**: 有关步骤，请参阅部署 iOS 客户端 第 3-13 页。

移动设备自动分组

移动安全使用前缀创建三 (3) 个类（Dangerous、Risky 和 NO_TMMS），并对风险设备进行如下标记：

- PREDEFINEDPREFIX_Dangerous
- PREDEFINEDPREFIX _Risky
- PREDEFINEDPREFIX _NO_TMMS

使用移动安全可在管理 Web 控制台上定义前缀 (PREDEFINEDPREFIX)。移动安全检测到具有不同安全级别的移动设备时，它会自动更改设备的智能组。

例如，如果移动安全检测到某个移动设备上存在恶意软件，它会自动将该移动设备移到 PREDEFINEDPREFIX _Dangerous 组。

移动应用程序自动分组

移动安全会根据风险应用程序所产生风险的类型自动在应用程序组下将其分组在一起。

- PREDEFINEDPREFIX _Malware_App_Android

- PREDEFINEDPREFIX _Privacy_App_Android
- PREDEFINEDPREFIX _Vulnerability_App_Android
- PREDEFINEDPREFIX _Malware_App_iOS

使用移动安全可在管理 Web 控制台上定义前缀 (PREDEFINEDPREFIX)。

配置 AirWatch 应用程序黑名单合规策略

配置 AirWatch 集成设置后，可在 AirWatch 管理 Web 控制台上创建合规策略，以将恶意应用程序添加到 AirWatch **黑名单**。

过程

1. 登录到 AirWatch Web 控制台，并导航到**设备** > **合规策略** > **列表视图**。
2. 单击**添加**，选择平台（Android 或 Apple iOS），然后从下拉列表中选择**应用程序列表**和**包含列入黑名单的应用程序**。
3. 单击**下一步**。
4. 在**操作**选项卡上，配置以下操作：
   a. 选择**标记为不合规**。
   b. 从下拉列表中选择**通知**和**向用户发送电子邮件**。
   c. 单击**下一步**。
5. 在**分配**选项卡上，配置以下设置：
   - **管理者**：趋势科技
   - **已分配的组**
   - **排除项**
6. 单击**下一步**。
7. 在**摘要**选项卡上，配置名称和描述。

8. 单击**完成并激活**。

在移动设备上检测到恶意软件时，移动安全会将应用程序置于 AirWatch 黑名单中，然后移动设备会被标记为不合规。

AirWatch 集成的帐户权限要求

移动安全支持与 AirWatch 集成。要将移动安全与 AirWatch 集成，您需要拥有一个具备在移动安全服务器和 AirWatch 之间进行通信所需权限的 AirWatch 帐户。

您可以使用三个不同的权限选项在 AirWatch 上创建帐户：

- **选项 1：创建具备所有权限的 AirWatch 管理员帐户进行通信**

  在 AirWatch 管理控制台上，导航到**帐户** > **管理员** > **列表视图** > **添加** > **添加管理员**，并创建具有以下角色和权限的帐户：

  ```
  AirWatch Administrator AirWatch Admins (Internal or External) Access to all
  ```

- **选项 2：创建具备所有 REST API 权限的 API ONLY 用户**

  在 AirWatch 管理控制台上，导航到**帐户** > **管理员** > **列表视图** > **添加** > **添加管理员**，并创建具有以下角色和权限的帐户：

  ```
  API Only Only provides access to REST APIs
  ```

- **选项 3：创建具备自定义 REST API 权限的 API ONLY 用户**

  此选项允许您选择移动安全使用的特定 REST API。

  执行以下操作：

  1. 在 AirWatch 管理控制台上，导航到**帐户** > **管理员** > **角色**，并创建具有移动安全使用的特定 REST API 权限的角色，如下表中所示：

类别	名称
管理员用户管理	搜索管理员用户

类别	名称
WTag 管理	创建标签
	搜索标签
	将设备添加到标签
	从标签中删除设备
	检索带有特定标签的设备
智能组管理	创建智能组
	搜索智能组
	删除智能组
应用程序组管理	创建应用程序组
	搜索应用程序组
	检索应用程序组详细信息
	将应用程序添加到应用程序组
	从应用程序组中删除应用程序
应用程序管理	内部应用程序安装：上传应用程序区块（iOS 和 Android）
	内部应用程序安装：开始内部应用程序安装
设备管理	检索设备信息
	设备全面搜索
	设备计数信息

2. 导航到**帐户** > **管理员** > **列表视图** > **添加** > **添加管理员**，并添加具有新建角色的帐户。

注意

AirWatch REST 权限设置页面不具有每个 API 的权限，但提供了许多 API 系列（例如，管理 API、应用程序 API 等）。请联系 AirWatch 技术支持，以了解需要在设置页面上启用的 REST API 权限。

配置 AirWatch 集成

过程

1. 登录移动安全管理 Web 控制台。
2. 在菜单栏上单击**管理** > **通信服务器设置**，并确保已配置通信服务器设置。如果未配置这些设置，请参阅*安装和部署指南*中的主题*“配置通信服务器设置”*了解配置步骤。
3. 单击**管理** > **部署设置**。
4. 在**服务器**部分下，选择**安全扫描**，然后从下拉列表中选择 **AirWatch** MDM 解决方案。
5. 在**注册服务**部分下，配置以下 AirWatch 设置：
   - **API URL**
   - **API 密钥**
   - **帐户**
   - **密码**
6. 单击**验证设置**，以确保移动安全可以连接到 AirWatch 服务器。
7. 在**数据同步设置**部分下，配置以下内容：
   - **安全类别前缀**

注意

移动安全使用前缀创建三 (3) 个类（Dangerous、Risky 和 NO_TMMS），并对风险设备进行如下标记：

- XXXX_Dangerous
- XXXX_Risky
- XXXX_NO_TMMS

风险设备和应用程序各自分组在**智能组**和**应用程序组**下，并包含其标记和类别已作为前缀添加到其名称的应用程序。

- 智能组：XXXX_Dangerous、XXXX_Risky、XXXX_NO_TMMS。
- 应用程序组：XXXX_Malware_App_Android、XXXX_Privacy_App_Android、XXXX_Vulnerability_App_Android、XXXX_Malware_App_iOS

客户端部署

您可以使用趋势科技移动安全从两个不同源部署客户端代理：

- **Google Play 商店**：您将需要配置 AirWatch 以部署移动安全客户端，并以文本或 QR 码的形式向用户提供注册信息。用户可以使用注册信息或扫描 QR 码来注册到服务器。注册信息包括服务器 IP 地址、端口号和注册密钥，该密钥可在**部署设置**窗口的 **Android 客户端**选项卡上获得。

  安装移动安全客户端后，用户将需要手动注册到移动安全服务器。如果从 Google Play 商店部署移动安全客户端，移动设备用户可以通过 Google Play 接收实时更新。

- **移动安全服务器**：通知用户从 AirWatch 应用程序商店下载名为**企业移动安全**的移动安全客户端。

  如果使用此部署选项，您将需要以文本或 QR 码的形式向用户提供注册信息。用户可以使用注册信息或扫描 QR 码来注册到服务器。注册信息包括服务器 IP 地址、端口号和注册密钥，该密钥可在**部署设置**窗口的 **Android 客户端**选项卡上获得。只要用户启动移动安全客户端，就必须将应用程序

注册到移动安全服务器。还可以将应用程序配置为自动注册。但是，有更新可用时，移动设备用户将需要手动更新自己的移动安全客户端。

在 Samsung 移动设备上，可以使用 AirWatch 管理控制台自动部署和配置移动安全客户端。

通过 Google Play 商店部署 Android 客户端

过程

1. 登录到 AirWatch Web 控制台，并导航到**应用程序和书籍** > **列表视图** > **公共 (选项卡)** > **添加应用程序**。
2. 在**添加应用程序**窗口上，配置以下字段：
   - **管理者**：键入趋势科技。
   - **平台**：从下拉列表中选择 **Android**。
   - **源**：选择**搜索应用程序商店**。
   - **名称**：键入企业移动安全以搜索应用程序商店。
3. 单击**下一步**。
4. 从搜索结果中选择**移动安全企业版**。
5. 在**添加应用程序**窗口上，单击**分配**选项卡，并从**已分配的组**字段中选择分配的组。
6. 单击**保存并发布**。
7. 单击**上传**。

移动安全使用注册密钥重新打包 Android 客户端，并将其上传到服务器。如果未配置任何预置的注册密钥，移动安全将在重新打包 Android 客户端前生成一个注册密钥。

注意

对于 Samsung 移动设备，您还可以在 AirWatch Web 控制台上配置移动安全 Android 客户端的自动启动功能。有关详细信息，请参阅以下文章：

https://success.trendmicro.com/solution/1115842

后续步骤

部署 Android 客户端之后，以文本或 QR 码的形式向用户提供注册信息。用户可以使用注册信息或扫描 QR 码来注册到服务器。注册信息包括服务器 IP 地址、端口号和注册密钥，该密钥可在**部署设置**窗口的 **Android 客户端**选项卡上获得。

通过移动安全服务器部署 Android 客户端

过程

1. 登录移动安全管理 Web 控制台。
2. 在菜单栏上单击**管理** > **设备注册设置**。
3. 在**身份验证**选项卡上，选择**使用注册密钥进行身份验证**，然后选择**使用预置的注册密钥**。
4. 单击**管理** > **部署设置** > **Android 客户端 (选项卡)**。
5. 选择**从 TMMS 服务器下载**，然后选择**自动注册**。
6. 单击**保存**以保存设置。
7. 单击**上传**，然后选择已修改的移动安全代理文件，以将其上传到 AirWatch 服务器。

   移动安全客户端将上传并出现在 AirWatch 管理 Web 控制台上。

后续步骤

部署 Android 客户端之后，以文本或 QR 码的形式向用户提供注册信息。用户可以使用注册信息或扫描 QR 码来注册到服务器。注册信息包括服务器 IP 地

址、端口号和注册密钥，该密钥可在**部署设置**窗口的 **Android 客户端**选项卡上获得。

配置 Android 移动设备自动启动

开始之前

执行此过程前，必须执行通过移动安全服务器部署 Android 客户端 第 3-11 页中所述的所有步骤。

过程

1. 登录到 AirWatch Web 控制台，并导航到**设备** > **暂存和预置** > **组件** > **文件/操作**。
2. 从 AirWatch 控制台配置**文件/操作**。执行以下操作：
   a. 导航到**设备** > **暂存和预置** > **组件** > **文件/操作**。
   b. • 单击**添加** > **Android**。
   c. 在**常规**选项卡上，提供**名称**和**描述**字段的信息。
   d. 在**清单**选项卡上，单击位于**安装清单**部分下的**添加操作**。
   e. 在**添加清单**选项上配置以下信息，然后单击**保存**：
      - **要执行的操作**：运行 Intent
      - **要运行的命令行和参数**：

        ```
        mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.trendmicro.tmmssuite.enterprise,class=com.trendmicro.tmmssuite.enterprise.ui.TmmsEnterpriseSplashScreen
        ```

      - 超时：[符合您的要求的任何持续时间]
   f. 在**添加文件/操作**窗口中，单击**保存**。
3. 配置产品。执行以下操作：

a. 导航到**设备** > **暂存和预置** > **产品列表视图**。

b. • 单击**添加产品** > **Android**。

c. 在**常规**选项卡上，提供**名称**、**描述**和**已分配的组**字段的信息。

d. 在**清单**选项卡上，单击**添加**以添加清单。

e. 在**添加清单**选项上配置以下信息，然后单击**保存**：

- **要执行的操作**：安装文件/操作
- **文件/操作**：

```
TestLauncher
```

f. 在**添加产品**窗口上，单击**保存**。

4. 配置应用程序。执行以下步骤：

a. 将 TMMS 客户端分配给智能组。

b. 将**推送模式**设置为**自动**。

部署 iOS 客户端

过程

1. 登录到 AirWatch Web 控制台，并导航到**应用程序和书籍** > **应用程序** > **列表视图**。
2. 在**公共**选项卡上，单击**添加应用程序**。
3. 在**添加应用程序**窗口上，配置以下字段：

- **管理者**：键入趋势科技。
- **平台**：选择 **Apple iOS**。
- **源**：选择**搜索应用程序商店**。
- **名称**：键入**企业移动安全**

4. 单击**下一步**。

5. 从搜索结果中，单击**移动安全企业版客户端**前面的**选择**。

6. 在**部署**选项卡上，选择**发送应用程序配置**，然后配置**应用程序配置**字段下的应用程序。

   要查找应用程序配置值，请参阅移动安全管理 Web 控制台上的**部署设置**窗口，如下图所示。（**管理** > **部署设置**）

配置项	值类型	配置值
CmdType	字符串	注册
EK	字符串	<注册密钥>
ServerUrl	字符串	<实际服务器 URL>
ServerPort	字符串	<实际服务器端口号>
DeviceSerialNumber	字符串	{DeviceSerialNumber}

配置项	值类型	配置值
DeviceWLANMac	字符串	{DeviceWLANMac}

7. 单击**保存并发布**。
8. 在**查看设备分配**窗口上，单击**发布**。

与 MobileIron 集成

您可以使用趋势科技移动安全将以下 MobileIron MDM 解决方案与移动安全集成：

- 已托管 MobileIron 核心
- 内部部署 MobileIron 核心

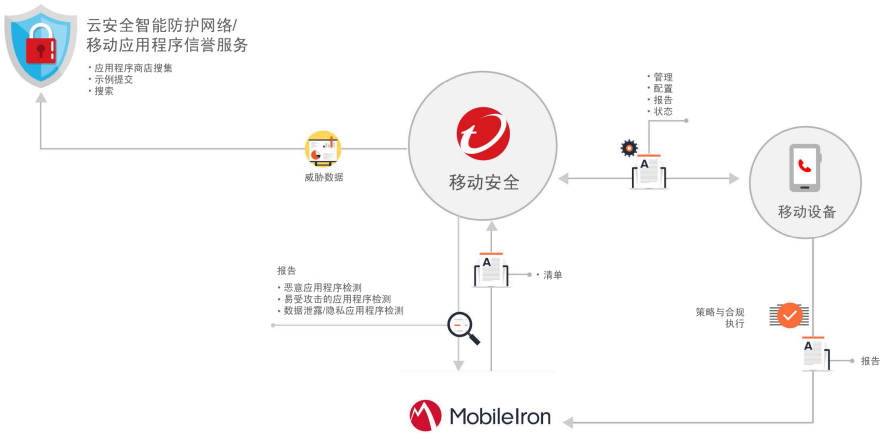
集成的先决条件

要将其他 MDM 解决方案与趋势科技移动安全集成，必须使用以下产品：

- 移动安全企业版 9.7 或更高版本
- 在移动安全中配置的本地通信服务器或云通信服务器
- MobileIron v9.3 或更高版本
- MobileIron 管理 Web 控制台上的管理员帐户

MobileIron 集成体系结构

下图显示了与 MobileIron 集成的高级体系结构。



移动应用程序信誉是一种基于云的技术，可以基于应用程序行为自动识别移动威胁，从各种 Android Market 爬网并收集大量的 Android 应用程序，识别现有移动恶意软件和全新移动恶意软件，识别可能会滥用隐私/设备资源的应用程序。这是全球首个自动移动应用程序评估服务。

趋势科技云安全智能防护网络提供针对零小时威胁的主动型全球威胁情报，以确保您始终受到保护。趋势科技使用最新的威胁情报即时消除攻击，让这些攻击没有机会得逞。**云安全智能防护网络**支持所有趋势科技产品和服务。

移动安全使用云安全智能防护网络和移动应用程序信誉服务来发现移动设备安全问题，并利用 MobileIron 合规策略来管理您的移动设备。

集成功能

趋势科技移动安全在与 AirWatch 集成方面提供以下功能：

功能	描述
移动设备自动分组	移动安全根据移动设备的风险等级添加 Dangerous、Risky 和 NO_TMMS 后缀来标记移动设备。 有关详细信息，请参阅移动设备自动分组 第 3-17 页。

功能	描述
移动安全客户端应用程序自动部署	您可以将 MobileIron 配置为自动将移动安全客户端部署到移动设备。 • **Android**: 有关步骤，请参阅通过移动安全服务器部署 Android 客户端 第 3-20 页。 • **iOS**: 有关步骤，请参阅部署 iOS 客户端 第 3-20 页。

移动设备自动分组

移动安全使用前缀创建三 (3) 个类（Dangerous、Risky 和 NO_TMMS），并对风险设备进行如下标记：

- PREDEFINEDPREFIX_Dangerous
- PREDEFINEDPREFIX _Risky
- PREDEFINEDPREFIX _NO_TMMS

使用移动安全可在管理 Web 控制台上定义前缀 (PREDEFINEDPREFIX)。移动安全检测到恶意应用程序时，它会自动更改设备的智能组。

例如，如果移动安全检测到某个移动设备上存在恶意软件，它会自动将该移动设备移到 PREDEFINEDPREFIX _Dangerous 组。

配置 MobileIron 集成

过程

1. 登录移动安全管理 Web 控制台。
2. 在菜单栏上单击**管理** > **通信服务器设置**，并确保已配置通信服务器设置。如果未配置这些设置，请参阅*安装和部署指南*中的主题*“配置通信服务器设置”*了解配置步骤。

3. 单击**管理** > **部署设置**。

4. 在**服务器**部分下，选择**安全扫描**，然后从下拉列表中选择**已托管 MobileIron 核心**或**内部部署 MobileIron 核心** MDM 解决方案。

5. 在**服务注册**部分下，配置以下 MobileIron 设置：

   - **API URL**
   - **帐户名称**
   - **密码**

6. 单击**验证设置**，以确保移动安全可以连接到 MobileIron 服务器。

7. 在**数据同步设置**部分下，配置以下内容：

   - **安全类别前缀**

   注意

   移动安全使用前缀创建三 (3) 个类（Dangerous、Risky 和 NO_TMMS），并对风险设备进行如下标记：

   - XXXX_Dangerous
   - XXXX_Risky
   - XXXX_NO_TMMS

客户端部署

您可以使用趋势科技移动安全从两个不同源部署客户端代理：

- **Google Play 商店**：您将需要配置 MobileIron 以部署移动安全客户端，并以文本或 QR 码的形式向用户提供注册信息。用户可以使用注册信息或扫描 QR 码来注册到服务器。注册信息包括服务器 IP 地址、端口号和注册密钥，该密钥可在**部署设置**窗口的 **Android 客户端**选项卡上获得。

安装移动安全客户端后，用户将需要手动注册到移动安全服务器。如果从 Google Play 商店部署移动安全客户端，移动设备用户可以通过 Google Play 接收实时更新。

- **移动安全服务器**：通知用户从 AirWatch 应用程序商店下载名为**企业移动安全**的移动安全客户端。

  如果使用此部署选项，您将需要以文本或 QR 码的形式向用户提供注册信息。用户可以使用注册信息或扫描 QR 码来注册到服务器。注册信息包括服务器 IP 地址、端口号和注册密钥，该密钥可在**部署设置**窗口的 **Android 客户端**选项卡上获得。只要用户启动移动安全客户端，就必须将应用程序注册到移动安全服务器。还可以将应用程序配置为自动注册。但是，有更新可用时，移动设备用户将需要手动更新自己的移动安全客户端。

通过 Google Play 商店部署 Android 客户端

过程

1. 登录到 MobileIron Web 控制台，然后在菜单栏上单击**应用程序目录**。
2. 单击**添加+**，然后选择 **Google Play**。
3. 在**应用程序名称**字段中，键入企业移动安全，然后单击**搜索**。
4. 从搜索结果中选择**移动安全企业版**，然后单击**下一步**。
5. 为**移动安全企业版**添加描述，并从**类别**下拉列表中选择要将此应用程序放置其中的类别。
6. 单击**完成**。
7. 从菜单栏中单击 **Apps@Work**。
8. 在 **APPS@WORK 目录**部分下，选择**在 Apps@Work 目录中突出此应用程序**。
9. 单击**保存**。

后续步骤

部署 Android 客户端之后，以文本或 QR 码的形式向用户提供注册信息。用户可以使用注册信息或扫描 QR 码来注册到服务器。注册信息包括服务器 IP 地

址、端口号和注册密钥，该密钥可在**部署设置**窗口的 **Android 客户端**选项卡上获得。

通过移动安全服务器部署 Android 客户端

过程

1. 登录移动安全管理 Web 控制台。
2. 在菜单栏上单击**管理** > **设备注册设置**。
3. 在**身份验证**选项卡上，选择**使用注册密钥进行身份验证**，然后选择**使用预置的注册密钥**。
4. 单击**管理** > **部署设置** > **Android 客户端 (选项卡)**。
5. 选择**从 TMMS 服务器下载**，然后选择**自动注册**。
6. 单击**保存**以保存设置。
7. 单击**上传**，然后选择已修改的移动安全代理文件，以将其上传到 AirWatch 服务器。

   移动安全客户端将上传并出现在 AirWatch 管理 Web 控制台上。

后续步骤

部署 Android 客户端之后，以文本或 QR 码的形式向用户提供注册信息。用户可以使用注册信息或扫描 QR 码来注册到服务器。注册信息包括服务器 IP 地址、端口号和注册密钥，该密钥可在**部署设置**窗口的 **Android 客户端**选项卡上获得。

部署 iOS 客户端

过程

1. 登录到 MobileIron Web 控制台，然后单击**应用程序目录**。
2. 单击**添加+**，然后选择 **iTunes**。

3. 在搜索字段中键入**企业移动安全**，然后单击**搜索**。
4. 选择**移动安全企业版客户端**，并单击**下一步**。
5. 不更改设置，并单击**下一步**。
6. 在 **APPS@WORK 目录**部分下，选择**在 Apps@Work 目录中突出此应用程序**，然后单击**下一步**。
7. 单击**完成**。
8. 登录移动安全管理 Web 控制台。
9. 单击**管理 > 部署设置 > iOS 客户端 (选项卡)**
10. 单击**下载**以下载配置文件。

注意

如果**下载**按钮处于不活动状态，请确保已在之前的步骤中正确配置了所有设置。

11. 在 MobileIron 管理 Web 控制台上，导航到**策略和配置**。
12. 单击**新增** > **iOS 和 OS X** > **托管应用程序配置**
13. 键入以下信息：
    - **名称**
    - **描述**
    - **BundleId**
14. 单击**下载**以下载配置文件。
15. 选择新创建的配置文件，然后单击**更多操作** > **应用至标签**。
16. 单击**应用**。

    移动安全会将**应用程序安装**通知推送至 iOS 移动设备。

第 4 章

管理移动设备

本章将帮助您了解如何使用移动安全。它提供了基本的安装和使用说明。在继续前，请确认已在移动设备上安装管理服务器、通信服务器和移动安全客户端。

本章包括以下几节内容：

托管的设备选项卡

您可以通过**设备**窗口上的**托管的设备**选项卡执行与移动安全客户端的设置、组织或搜索相关的任务。通过设备树视图上方的工具栏可执行以下任务：

- 配置设备树（例如，创建、删除或更名组，以及创建或删除移动安全代理）
- 配置移动安全客户端信息
- 搜索并显示移动安全代理状态
- 按需移动安全客户端组件更新、扫描设备和更新策略
- 导出数据供进一步分析或备份

移动安全中的组

移动安全管理服务器会自动创建名为**移动设备**的根组，其中包含以下子组：

- **缺省** — 此组包含不属于任何其他组的移动安全客户端。在移动安全设备树中不能删除或重命名**缺省**组。

有关说明，请参见移动安全管理服务器*联机帮助*。

管理组

可以添加、编辑或删除**移动设备**根组下面的组。但是，不能重命名或删除根组**移动设备**和组**缺省**。

添加组

过程

1. 登录移动安全管理 Web 控制台。

2. 单击菜单栏上的**设备**。

   显示**设备**窗口。

3. 在**托管的设备**选项卡上，单击根组**移动设备**，然后单击**添加组**。

4. 配置以下内容：

   - **父组**：选择要在其下创建子组的组。
   - **组名**：为组键入名称。
   - **策略**：从下拉列表中选择要应用于组的策略。

5. 单击**添加**。

更名组

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**设备**。

   显示**设备**窗口。

3. 在**托管的设备**选项卡中，单击要重命名的组。
4. 单击**编辑**。
5. 修改组名，然后单击**重命名**。

删除组

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**设备**。

显示**设备**窗口。

3. 在**托管的设备**选项卡中，单击要删除的组。
4. 单击**删除**，然后单击确认对话框中的**确定**。

管理移动设备

可以在**设备**窗口中编辑移动设备信息、删除移动设备或更改移动设备组。

重新分配设备

过程

1. 在移动安全管理 Web 控制台上，转到**设备** > **托管的设备**。

   显示**设备**窗口。
2. 从设备树中，选择要重新分配的设备。

   将显示设备信息。
3. 单击**更改用户**，然后在提供的文本框中修改用户名。
4. 单击**保存**。

编辑移动设备信息

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**设备**。

   显示**设备**窗口。

3. 在**托管的设备**选项卡中，从设备树中单击要编辑其信息的移动设备。
4. 单击**编辑**。
5. 更新以下文本框中的信息：
   - **电话号码** — 移动设备的电话号码。
   - **设备名称** — 移动设备的名称，以在设备树中标识设备。
   - **组** — 下拉列表中的移动设备所属组的名称。
   - **资产编号** — 键入分配给移动设备的资产编号。
   - **描述** — 与移动设备或用户相关的任何其他信息或说明。
6. 单击**保存**。

删除移动设备

移动安全为删除移动设备提供以下两个选项：

- 删除单个移动设备 第 4-5 页
- 删除多个移动设备 第 4-6 页

删除单个移动设备

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**设备**。

   显示**设备**窗口。
3. 在**托管的设备**选项卡中，从设备树中单击要删除的移动设备。
4. 单击**删除**，然后单击确认对话框中的**确定**。

移动设备将从移动设备树中删除，且不再注册到 Mobile Security 管理服务器。

删除多个移动设备

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**设备**。

   显示**设备**窗口。
3. 在**托管的设备**选项卡中，从设备树中单击要删除其移动设备的组。
4. 从右窗格的列表中选择移动设备，单击**删除**，然后单击确认对话框中的**确定**。

   移动设备将从移动设备树中删除，且不再注册到移动安全管理服务器。

将移动设备移动到其他组

可以将移动设备从一个组移动到另一个组。移动安全会自动向用户发送有关您应用于组的策略的通知。

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**设备**。

   显示**设备**窗口。
3. 在**托管的设备**选项卡中，单击要将其移动设备移动到其他组的组。
4. 从右窗格的列表中选择移动设备，然后单击**移动**。

   显示**移动设备**对话框。

5. 从下拉列表中选择目标组，然后单击**确定**。

移动设备状态

在**托管的设备**选项卡中的**设备**窗口中，选择要在右窗格中显示其状态信息的移动设备。移动设备信息分别显示在以下部分：

- **基本** — 包括注册状态、电话号码、LDAP 帐户和平台信息。
- **硬件、操作系统** — 显示详细的移动设备信息，包括设备和型号名称、操作系统版本、内存信息、蜂窝技术、IMEI 和 MEID 号以及固件版本信息。
- **安全** — 显示移动设备的越狱版/Root 权限、开发人员选项、USB 调试、网络流量解密状态；恶意 iOS 配置文件、恶意 SSL 证书、恶意应用程序、被篡改的应用程序、易受攻击的应用程序、隐私泄露应用程序的数量；以及连接的接入点 (Wi-Fi)。

基本移动安全代理搜索

要根据移动设备名称或电话号码搜索移动安全客户端，请在**设备**窗口上提供的搜索字段中键入信息，并单击**搜索**。搜索结果将在设备树中显示。

高级移动安全代理搜索

您可以使用**高级搜索**窗口指定更多移动安全代理搜索条件。

过程

1. 在**设备**窗口中，单击**高级搜索**链接。显示一个弹出窗口。
2. 选择搜索条件并在提供的文本框中键入值（如果适用）：
   - **设备名称** — 标识移动设备的描述性名称
   - **电话号码** — 移动设备的电话号码

- **用户名** — 移动设备的用户名
- **资产编号** — 移动设备的资产编号
- **IMEI** — 移动设备的 IMEI 号
- **序列号** — 移动设备的序列号
- **Wi-Fi MAC 地址** — 移动设备的 Wi-Fi MAC 地址
- **描述** — 移动设备的描述
- **操作系统** — 将搜索范围限定为移动设备正在运行的特定操作系统；或 Android 和 iOS 的版本号
- **组** — 移动设备所属组
- **代理版本** — 移动设备上移动安全客户端的版本号
- **最后连接** — 移动设备上一次连接到移动安全服务器的时间范围
- **恶意软件病毒码版本** — 移动设备上的恶意软件病毒码文件版本号
- **恶意软件扫描引擎版本** — 移动设备的恶意软件扫描引擎版本号
- **应用程序名称** — 在移动设备上安装的应用程序
- **被感染的移动安全客户端** — 将搜索范围限定为检测到指定数量恶意软件的移动设备

3. 单击**搜索**。搜索结果将在设备树中显示。

移动安全客户端任务

趋势科技移动安全使您能够从**设备**窗口在移动设备上执行不同的任务。

更新移动安全客户端

可以将更新通知发送到包含过期组件或来自**设备**窗口中**托管的设备**选项卡的安全策略的移动设备。

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**设备**。

   显示**设备**窗口。
3. 在**托管的设备**选项卡中，单击要更新移动设备的组。
4. 单击**更新**。

移动安全将更新通知发送到所有包含过期组件或安全策略的移动设备。

还可以使用**更新**窗口设置移动安全，以自动将更新通知发送到包含过期组件或策略的移动设备或手动启动该过程。

有关详细信息，请参阅更新移动安全组件 第 8-2 页。

更新移动设备信息

移动安全服务器自动以预设的时间间隔从托管移动设备中获取设备信息，然后将设备信息显示在**设备**窗口中。

在下一次预设的自动更新之前，您可以在**托管的设备**选项卡上更新托管设备的设备信息。

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**设备**。

   显示**设备**窗口。

3. 在**托管的设备**选项卡上，从设备树中选择移动设备。
4. 单击**更新**。

导出数据

您可从**设备**窗口的**托管的设备**选项卡中导出数据，以进行进一步分析或备份。

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**设备**。

   显示**设备**窗口。
3. 从设备树中选择要导出数据的移动设备组。
4. 单击**导出**。
5. 如果需要，在显示的弹出窗口中单击**保存**，将 `.zip` 文件保存在您的计算机中。
6. 将下载的 `.zip` 文件内容解压缩，并打开 `.csv` 文件，查看移动设备信息。

与趋势科技防毒墙控制管理中心集成

趋势科技移动安全提供与趋势科技防毒墙控制管理中心（也称为防毒墙控制管理中心或 TMCM）的集成。通过此集成，防毒墙控制管理中心管理员能够执行以下操作：

- 创建、编辑或删除移动安全的安全策略
- 将安全策略传送给已注册的移动设备
- 查看移动安全**控制台**窗口

有关趋势科技防毒墙控制管理中心和处理防毒墙控制管理中心中的移动安全策略的详细信息，请参阅以下 URL 中的产品文档：

http://docs.trendmicro.com/zh-cn/enterprise/control-manager.aspx

在防毒墙控制管理中心中创建安全策略

趋势科技防毒墙控制管理中心 Web 控制台显示与移动安全中相同的安全策略。如果防毒墙控制管理中心管理员为移动安全创建了安全策略，移动安全将为此策略创建新的组并将所有目标移动设备移动到此组。为了区分在移动安全中创建的策略和在防毒墙控制管理中心中创建的策略，移动安全会为组名称添加 **TMCM_** 前缀。

删除或修改安全策略

防毒墙控制管理中心管理员可以随时修改策略，并且策略将会立即部署到移动设备。

趋势科技防毒墙控制管理中心每 24 小时与趋势科技移动安全同步一次策略。如果删除或修改从防毒墙控制管理中心创建和部署的策略，同步发生后，该策略将恢复到原始设置或再次创建。

防毒墙控制管理中心中的安全策略状态

在趋势科技防毒墙控制管理中心 Web 控制台中，为安全策略显示以下状态：

- **挂起**：此策略在防毒墙控制管理中心 Web 控制台中创建，且尚未传送到移动设备。
- **已部署**：此策略已传送并已经在所有目标移动设备上部署。

第 5 章

查看用户

本章介绍了如何查看在移动安全中注册的用户。

本章包括以下几节内容：

“用户”选项卡

您可以使用**用户**选项卡查看在移动安全中注册的所有移动设备。

查看用户列表

过程

1. 在移动安全管理 Web 控制台上，转到**用户**。

   显示**用户**窗口。

2. 要对列表进行排序，请单击以下任何列的标题。
   - 用户名
   - 电子邮件
   - 设备
   - 邀请时间
3. 要搜索用户，请在**搜索**栏中键入用户名或电子邮件地址，然后按 Enter。

   如果用户处于列表中，则移动安全将显示相应信息。

第 6 章

保护包含策略的设备

本章说明了如何在移动安全组中配置安全策略并将其应用到移动设备。您可以使用与配置、设备安全和数据保护相关的策略。

本章包括以下几节内容：

关于策略

您可以在管理服务器或注册到移动安全的所有移动设备上为移动安全组配置策略。

表 6-1. 移动安全中的设备策略

策略	参考
允许列表	请参阅 应用程序允许列表 第 6-2 页。
可信网络流量解密证书列表	请参阅 可信网络流量解密证书列表 第 6-2 页。

表 6-2. 移动安全中的组策略

策略组	策略	参考
常规	通用策略	请参阅 通用策略 第 6-6 页。
设备安全	安全策略	请参阅 安全策略 第 6-6 页。

针对所有设备的策略

本节介绍移动安全中针对所有移动设备的可用策略。

应用程序允许列表

应用程序允许列表包括检测为安全风险（恶意软件、易受攻击、隐私风险或被篡改）、但管理员允许在移动设备上安装的所有应用程序。

要管理**应用程序允许列表**，请单击**策略** > **针对所有设备的策略**。

可信网络流量解密证书列表

如果移动安全检测到恶意 SSL 证书，则会在**检测** > **恶意 SSL 证书**窗口上显示这些证书。但是，您可以将这些“恶意”证书添加到**可信网络流量解密证书列**

表，以使移动安全能够在扫描期间跳过这些证书，并将其从**恶意 SSL 证书**窗口中隐藏。

要管理**可信网络流量解密证书列表**，请单击**策略** > **针对所有设备的策略**。

管理针对所有设备的策略

您可使用移动安全维护应用程序允许列表和可信网络流量解密证书列表，以允许用户使用这些应用程序和网络解密证书，而不受限制或出现警告。

使用**针对所有设备的策略**窗口创建、编辑、复制或删除移动设备的策略。

将应用程序添加到允许列表

过程

1. 登录移动安全管理 Web 控制台。
2. 执行下列操作之一：
   - 将移动安全扫描的已安装应用程序添加到**允许列表**。
     a. 在菜单栏上单击**检测** > **应用程序安全状态**。
     b. 单击 **Android** 或 **iOS** 选项卡，并从检测到的应用程序列表中选择要添加到**允许列表**的应用程序。
     c. 单击**添加到允许列表**。
   - 手动将应用程序添加到**允许列表**。
     a. 在菜单栏上单击**策略** > **针对所有设备的策略**。
     b. 在**应用程序允许列表**部分下，单击 **Android** 或 **iOS** 选项卡，然后单击**添加到允许列表**。

        显示**导入应用程序**窗口。
     c. 在提供的文本框中键入应用程序标识、名称和描述。使用分号 (;) 分隔每个应用程序信息。

d. 单击**导入应用程序**窗口上的**保存**。

e. 单击**针对所有设备的策略**窗口上的**保存**。

从允许列表中删除应用程序

过程

1. 登录移动安全管理 Web 控制台。
2. 执行下列操作之一：
   - 从**允许列表**中删除移动安全扫描的已安装应用程序。
     a. 在菜单栏上单击**检测** > **应用程序安全状态**。
     b. 单击 **Android** 或 **iOS** 选项卡，并从检测到的应用程序列表中选择要从**允许列表**中删除的应用程序。
     c. 单击**从允许列表中删除**。
   - 直接从**允许列表**中删除应用程序。
     a. 在菜单栏上单击**策略** > **针对所有设备的策略**。
     b. 在**应用程序允许列表**部分下，单击 **Android** 或 **iOS** 选项卡，然后选择要从列表中删除的应用程序。
     c. 单击**从允许列表中删除**。
     d. 单击**针对所有设备的策略**窗口上的**保存**。

添加可信网络流量解密证书

过程

1. 登录移动安全管理 Web 控制台。
2. 在菜单栏上单击**策略** > **针对所有设备的策略**。

显示**针对所有设备的策略**窗口。

3. 在**可信网络流量解密证书列表**部分下，单击**添加**。

   显示**添加证书**窗口。

4. 从本地硬盘中选择证书文件，然后在**描述**文本框中键入证书文件的描述。

5. 单击**确定**。

6. 单击**针对所有设备的策略**窗口上的**保存**。

删除可信网络流量解密证书

过程

1. 登录移动安全管理 Web 控制台。

2. 在菜单栏上单击**策略 > 针对所有设备的策略**。

   显示**针对所有设备的策略**窗口。

3. 在**可信网络流量解密证书列表**部分下，选择要删除的证书文件，然后单击**删除**。

4. 单击**针对所有设备的策略**窗口上的**保存**。

针对所有组的策略

本节介绍移动安全中针对所有组的可用策略。

使用超级用户帐户，您可将任何策略指定为模板，以便组管理员在 Mobile Security 中创建更多安全策略。但是，一旦您将安全策略指定为模板，您将无法将该安全策略分配给任何组。

通用策略

通用策略可为移动设备提供通用安全策略。要配置通用安全策略设置，请单击**策略**，然后单击策略名称，然后单击**通用策略**。

- **用户特权：**
  - 您可以选择是否允许用户配置移动安全客户端设置。

    如果不选择**允许用户配置移动安全客户端设置**复选框，则用户无法更改移动安全代理设置。但是，选中此选项时，**Web 威胁防护策略**的过滤列表不受影响。有关详细信息，请参阅 安全策略 第 6-6 页。
  - 您可以选择自动检查选项，让移动安全客户端定期在移动安全管理服务器上检查所有组件或配置更新。

安全策略

您可以从**安全策略**窗口配置**安全设置**。

注意

移动安全 Web 威胁防护仅支持移动设备上的缺省 Android 浏览器和 Google Chrome。

要配置安全保护策略设置，请单击**策略**，单击策略名称，然后单击**安全策略**。

下表介绍了此策略的可用设置。

表 6-3. 安全策略设置

部分	项	描述	支持的移动设备操作系统
安全设置	**仅扫描已安装的应用程序**	如果仅希望扫描已安装的应用程序，则选择此选项	

部分	项	描述	支持的移动设备操作系统
	扫描已安装的应用程序和文件	如果要扫描已安装应用程序和在移动设备上存储的其他文件，则选择此选项。 如果选择此选项，请指定是仅扫描 APK 文件还是扫描所有文件。	
	病毒码更新后扫描	如果您希望在每次更新病毒码后运行恶意软件扫描，则启用此选项。 在 Android 移动设备上成功执行病毒码更新后，移动安全将自动运行扫描。	
	应用程序扫描	如果要扫描应用程序中是否存在恶意软件、隐私风险、易受攻击和被篡改（重新打包）的应用程序，请启用此选项。	
	网络安全扫描	这些设置会扫描网络流量解密、不安全的接入点 (Wi-Fi) 或已安装的恶意 SSL 证书。此类别下的所有选项在缺省情况下处于启用状态，无法修改。	
	易受攻击的应用程序扫描	这些设置会扫描移动设备中因 USB 调试、开发人员选项、恶意配置文件和具有 Root 权限的或越狱版移动设备而产生的漏洞。	
	检测到网络流量解密时阻止网络	启用此选项可在移动安全在通信期间检测到数据泄露时停止网络流量解密。	
	检测到可疑接入点 (Wi-Fi) 具有高风险时阻止网络	启用此选项可在将网络连接检测为疑似虚假时断开移动设备与网络的连接。	

部分	项	描述	支持的移动设备操作系统
	扫描预设下的**启用预设扫描**	选择**每日一次**、**每周一次**或**每月一次**，分别每天、每周或每月运行一次扫描。	
Web 威胁防护设置	**启用集中控制的 Web 威胁防护策略**	此功能使您能在服务器端控制 Web 威胁防护策略。您可以根据需要配置以下防护等级： • **低**：此设置提供针对网络诈骗和来自其他网站的恶意活动的最小程度防御。 • **中**：此设置可以抵御在线安全威胁，但不会阻止大多数 Web 站点。趋势科技建议使用此缺省设置。 • **高**：此设置提供针对网络诈骗和其他网站的最大程度防御；允许打开具有良好信誉的网站，并阻止其他所有网站。	
	过滤列表	移动安全将阻止您在**阻止列表**中添加的所有 URL，并允许打开**允许列表**中的所有 URL。	
	重新评估 URL	如果遇到您认为分类错误的 URL，可通过以下 Web 站点通知趋势科技任何此类 URL： http://sitesafety.trendmicro.com/	

Web 威胁防护策略

可管理移动安全管理服务器中的 Web 威胁防护策略并在 Android 移动设备上部署该策略。它还可以使 Android 移动设备将 Web 威胁防护日志发送回服务器。

注意

移动安全 Web 威胁防护仅支持缺省的 Android 浏览器和 Google Chrome。

要配置 Web 威胁防护策略设置，请单击**策略**，然后单击策略名称，然后单击**Web 威胁防护策略**。

管理针对所有组的策略

移动安全让您能够使用缺省策略模板快速创建策略。

使用**针对所有组的策略**窗口创建、编辑、复制或删除移动设备的策略。

创建策略

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**策略** > **组策略**。

   显示**策略**窗口。
3. 单击**创建**。

   显示**创建策略**窗口。
4. 在相应的文本框中键入策略名称和描述，然后单击**保存**。

   移动安全使用缺省设置创建策略。但是，策略未分配给组。若要将策略分配给组，请参阅为组分配或删除策略 第 6-10 页。
5. （仅限超级管理员）如果要将此策略作为模板，单击**策略**窗口中**类型**列下方的箭头按钮。组管理员可使用超级管理员创建的模板为已分配的组创建策略。

注意

- 不能将模板分配到任何组。
- 也可将模板转换为策略。但是，只能在模板没有分配到组的情况下，才可将模板转换为策略。

编辑策略

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**策略** > **组策略**。

   显示**策略**窗口。
3. 在策略列表中，单击要编辑其详细信息的策略名称。

   显示**编辑策略**窗口。
4. 修改策略详细信息，然后单击**保存**。

为组分配或删除策略

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**策略** > **组策略**。

   显示**策略**窗口。
3. 在策略的**应用的组**列中，单击组名。如果策略未分配给组，单击**无**。
4. 执行下列操作之一：

- 若要将策略分配给组：从左侧的**可用组**列表中，选择要应用策略的组，然后单击 **>** 将组移动到右侧。
- 若要从组中删除策略：从右侧的组列表中，选择要删除的组，然后单击 **<** 将组移动到左侧的**可用组**列表。

5. 单击**保存**。

复制策略

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**策略** > **组策略**。

   显示**策略**窗口。
3. 选择要复制的策略，然后单击**复制**。

删除策略

不能删除**缺省**策略和已应用于某个组的任何策略。在删除策略之前，确保将其从所有组中删除。有关步骤，请参阅为组分配或删除策略 第 6-10 页。

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**策略** > **组策略**。

   显示**策略**窗口。
3. 选择要删除的策略，然后单击**删除**。

第 7 章

查看和管理检测

本章介绍了如何为 iOS 和 Android 移动设备管理检测到的恶意应用程序，以及查看 SSL 证书和 iOS 配置文件。

本章包括以下几节内容：

关于“可疑应用程序”窗口

可疑应用程序窗口显示移动设备上安装的所有应用程序的应用程序名称、版本、安全扫描状态、安装数量和上次扫描时间。

如果您认为此窗口上显示的应用程序安全，还可以将这些应用程序添加到应用程序**允许列表**。同样，还可以删除先前添加到**允许列表**、但现在认为不安全的应用程序。

有关步骤，请参阅将应用程序添加到允许列表 第 6-3 页和从允许列表中删除应用程序 第 6-4 页。

单击表右上方的**管理允许列表**链接，导航到**允许列表**窗口以管理列表。

下表列出了可用于 Android 和 iOS 应用程序的信息。

表 7-1. 应用程序安全状态

信息	描述	ANDROID	IOS
应用程序名称	应用程序的名称	●	●
版本	应用程序版本号	●	●
恶意软件扫描结果	恶意软件扫描可能有以下任一结果： • **正常** — 未检测到恶意软件 • **PUA** — 可能不需要的应用程序 (Potentially unwanted application, PUA) 是指可能对用户安全和/或隐私带来高风险的灰色软件应用程序。 有关详细信息，请参阅 http://about-threats.trendmicro.com/zh-cn/definition/potentially-unwanted-app。 • **恶意软件** — 已知恶意软件 • **未知** — 无可用信息	●	●

信息	描述	ANDROID	iOS
漏洞扫描结果	漏洞扫描可能有以下任一风险评级： • **正常** • **中** • **高** • **未知** — 无可用信息	●	
隐私扫描结果	隐私扫描可能有以下任一风险评级： • **正常** • **中** • **高** • **未知** — 无可用信息	●	
已被篡改	已被篡改的应用程序扫描可能有以下任一结果： • **是** — 原始应用程序已被篡改或者已被重新打包以达到可能的恶意目的 • **否** — 尚未对原始应用程序进行篡改 • **未知** — 无可用信息	●	●
安装数量	已安装该应用程序的设备数量	●	●
上次扫描	上次扫描的日期和时间	●	●

移动安全扫描应用程序是否存在安全风险时，它会根据安全扫描结果执行以下操作：

- 在**控制台**窗口的 **Android/iOS 应用程序风险摘要**小部件上显示检测
- 在**设备**窗口的相关类别下显示针对移动设备检测到的安全风险数量
- 生成日志条目

查看可疑 Android 应用程序

过程

1. 在移动安全 Web 控制台上，转到**检测** > **可疑应用程序** > **Android** 选项卡。

   显示 **Android** 选项卡。

2. 要查看应用程序的扫描详细信息，请单击以下任何列下方的结果。

   - 漏洞扫描结果
   - 隐私扫描结果

   显示选定结果的扫描详细信息页。

3. 要查看已安装某应用程序的设备，请单击**安装数量**列下的数字。

   将出现**设备**窗口，在**托管的设备**选项卡下显示设备列表。

4. 要查看有关特定应用程序的信息，请在**搜索**栏中键入应用程序名称，然后按 Enter。

   如果应用程序位于列表中，则表中将显示该应用程序的信息。

查看可疑 iOS 应用程序

过程

1. 在移动安全 Web 控制台上，转到**检测** > **可疑应用程序** > **iOS** 选项卡。

   显示 **iOS** 选项卡。

2. 要查看已安装某应用程序的设备，请单击**安装数量**列下的数字。

   将出现**设备**窗口，在**托管的设备**选项卡下显示设备列表。

3. 要查看有关特定应用程序的信息，请在**搜索**栏中键入应用程序名称，然后按 Enter。

如果应用程序位于列表中，则表中将显示该应用程序的信息。

查看恶意 SSL 证书

恶意 SSL 证书窗口显示移动安全检测为恶意的、安装在 Android 或 iOS 移动设备上的 SSL 证书。如果您信任**恶意 SSL 证书**窗口上列出的任何证书，则可将该证书添加到可信网络流量解密证书列表 第 6-2 页，使其从**恶意 SSL 证书**窗口中隐藏。

移动安全检测到恶意证书时，它会执行以下操作：

- 在**恶意 SSL 证书**窗口上显示恶意 SSL 证书
- 在**控制台**窗口的**网络保护摘要**小部件上显示检测
- 将设备安全状态更新为**危险**
- 向管理员发送通知电子邮件
- 生成日志条目

恶意 SSL 证书窗口上显示的证书详细信息包括证书名称和详细信息、移动设备上的安装数量和上次扫描时间。

过程

1. 在移动安全 Web 控制台上，转到**检测** > **恶意 SSL 证书**。

   显示**恶意 SSL 证书**窗口。

2. 单击 **Android** 或 **iOS** 选项卡。

3. 要查看有关特定应用程序的信息，请在**搜索**栏中键入应用程序名称，然后按 Enter。

   如果应用程序位于列表中，则表中将显示该应用程序的信息。

查看恶意 iOS 配置文件

恶意 iOS 配置文件窗口显示移动安全检测的安装在 iOS 移动设备上的恶意 iOS 配置文件。

移动安全检测到恶意 iOS 配置文件时，它会执行以下操作：

- 在**恶意 iOS 配置文件**窗口上显示恶意 iOS 配置文件
- 在**控制台**窗口的 **iOS 网络保护摘要**小部件上显示检测
- 将设备状态更新为**危险**
- 向管理员发送通知电子邮件
- 生成日志条目

恶意 iOS 配置文件窗口上显示的配置文件详细信息包括配置文件名称、其类型、扫描结果、移动设备上的安装数量和上次扫描时间。

过程

1. 在移动安全 Web 控制台上，转到**检测** > **恶意 iOS 配置文件**。

   显示**恶意 iOS 配置文件**窗口。

2. 要查看有关特定 iOS 配置文件的信息，请在**搜索**栏中键入证书名称，然后按 **Enter**。

   如果证书位于列表中，则表中将显示该应用程序的信息。

第 8 章

更新组件

本章介绍了如何更新移动安全组件。

本章包括以下几节内容：

关于组件更新

在移动安全中，通过趋势科技基于 Internet 的组件更新功能 ActiveUpdate 更新以下组件或文件：

- 移动安全服务器 — 移动安全通信服务器的程序安装包。
- 恶意软件病毒码 — 包含成千上万恶意软件特征的文件，并决定移动安全检测危害文件的能力。趋势科技定期更新病毒码文件，以确保对最新威胁的防护。
- 移动安全代理安装程序 - 移动安全代理的程序安装包。

更新移动安全组件

可在移动安全管理服务器上配置预设或手动组件更新，以便从 ActiveUpdate 服务器获取最新组件文件。从管理服务器下载新版组件后，管理服务器将自动通知移动设备更新组件。

手动更新

您可在**更新**窗口中的**手动**选项卡上执行手动服务器和移动安全客户端更新。在**源**窗口中，应该已配置下载源（更多信息，请参阅指定下载源 第 8-4 页）。

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**管理** > **更新**。

   显示**更新**窗口。
3. 单击**手动**选项卡。
4. 选中要更新的组件的复选框。选中**防恶意软件组件**、**代理安装包**和/或**服务器版本**复选框，以选择该组中所有组件。此窗口还显示各组件的当前版

本和组件的上次更新时间。有关各更新组件的更多信息，请参阅关于组件更新 第 8-2 页。

5. 单击**更新**，开始组件更新过程。

预设更新

预设更新允许用户执行定期更新，而无需用户交互；因此，减少了工作量。在**源**窗口中，应该已配置下载源（更多信息，请参见指定下载源 第 8-4 页）。

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**管理** > **更新**。

   显示**更新**窗口。
3. 单击**预设**选项卡。
4. 选中要更新的组件的复选框。选中**防恶意软件组件**、**代理安装包**和/或**服务器版本**复选框，以选择该组中所有组件。此窗口还显示各组件的当前版本和组件上次更新的时间。
5. 在**更新日程表**下面，配置执行服务器更新的时间间隔。选项包括：**每小时**、**每天**、**每周一次**和**每月一次**。
   - 如果每周更新一次，请指定一周中的某一天（例如，星期日、星期一等）。
   - 如果每月更新一次，请指定月份中的某一天（例如，每月的第一天或 01 等）。

注意

更新周期为 x 小时功能适用于**每日一次**、**每周一次**和**每月一次**选项。这意味，更新将在**开始时间**文本框中所选中时间后的指定小时数内的某个时间执行。此项功能有助于 ActiveUpdate 服务器上的负载均衡。

- 选择希望移动安全启动更新过程的**开始时间**。

6. 单击**保存**以保存设置。

指定下载源

可设置移动安全，使其使用缺省的 ActiveUpdate 源或指定下载源来更新服务器。

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**管理** > **更新**。

   显示**更新**窗口。有关更新的详细信息，请参阅手动更新 第 8-2 页；有关预设更新的详细信息，请参阅预设更新 第 8-3 页。
3. 单击**源**选项卡。
4. 选择以下任一下载源：
   - **趋势科技 ActiveUpdate 服务器** - 缺省更新源。
   - **其他更新源** — 指定 HTTP 或 HTTPS Web 站点（例如，您的本地企业内联网 Web 站点），包括移动安全代理可用于从中下载更新的端口号。

     注意

     最新组件必须适用于更新源（Web 服务器）。提供主机名或 IP 地址及目录（例如，`https://12.1.123.123:14943/source`）。
   - **包含当前文件副本的 Intranet 位置** — 本地 Intranet 更新源。指定下列内容：
     - **UNC 路径**：键入源文件存放的路径。

- **用户名**和**密码**：如果源位置需要身份验证，键入用户名和密码。

手动更新本地 AU 服务器

如果服务器/设备通过本地 AutoUpdate 服务器更新，但管理服务器却无法连接 Internet，则在服务器/设备更新之前，手动更新本地 AU 服务器。

过程

1. 从趋势科技代表那里获取安装软件包。
2. 解压缩安装软件包。
3. 将文件夹复制到本地 AutoUpdate 服务器。

注意

使用本地 AutoUpdate 服务器时，应该定期检查更新。

第 9 章

查看和维护日志

本章介绍了如何查看移动安全管理 Web 控制台上的日志，以及如何配置日志删除设置。

本章包括以下几节内容：

关于日志

移动安全保留以下类型的日志：

- **管理员日志**：当管理员在管理 Web 控制台上执行任何配置时，移动安全将在管理服务器上生成日志。
- **移动安全客户端日志**：移动安全客户端生成应用程序扫描日志、设备漏洞日志、网络保护日志或 Web 威胁防护日志时，会将日志发送到移动安全管理服务器。这样移动安全客户端日志就可以存储在中央位置，可以评估贵组织的防护策略，并可确定那些易被病毒感染或易于受到攻击的移动设备。

查看移动安全代理日志

可查看移动设备上的移动安全客户端日志或查看移动安全管理服务器上的所有移动安全客户端日志。在管理服务器中，可查看以下移动安全客户端日志：

- 应用程序扫描日志：当移动安全客户端在移动设备上检测到恶意软件、隐私威胁、漏洞风险或被篡改的应用程序时，将生成这些日志。
- 设备漏洞日志：当启用开发人员选项或 USB 调试模式、在移动设备上检测到恶意 iOS 配置文件或检测到具有 Root 权限的/越狱版移动设备时，将生成这些日志。
- 网络保护日志：在移动设备上检测到网络流量解密、不安全的接入点 (Wi-Fi) 或恶意 SSL 证书时，将生成这些日志。
- Web 威胁防护日志：移动安全客户端在阻止危险的或受恶意软件感染的 Web 页面时会生成 Web 威胁防护日志，然后将日志上传至服务器。

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**通知和报告** > **日志查询**。

显示**日志查询**窗口。

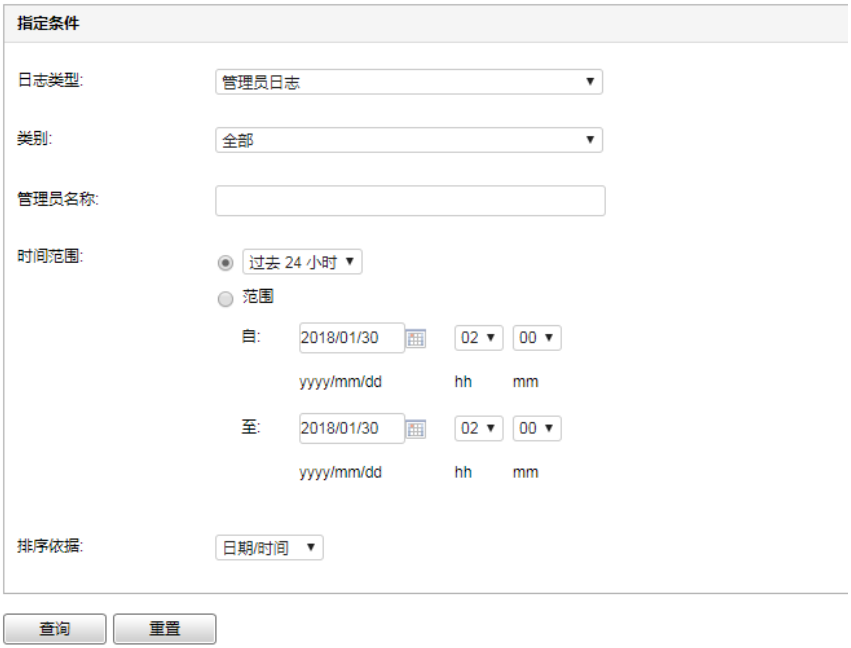


图 9-1. 日志查询窗口

3. 为要查看的日志指定查询条件。参数如下：

   - **日志类型** — 从下拉菜单中选择日志类型。
   - **类别** — 从下拉菜单中选择日志类别。
   - **管理员名称**或**设备名称** — 键入要搜索其相关日志的管理员或设备名称。
   - **时间范围** — 选择预定义的日期范围。选项包括：**全部**、**过去 24 小时**、**过去 7 天**和**过去 30 天**。如果上述选项中未包括所需时间段，则选择**范围**并指定日期范围。
     - **起始** — 键入要查看的最早日志的日期。单击该图标，从日历中选择日期。

- **终止** — 键入要查看的最近日志的日期。单击该图标，从日历中选择日期。
- **排序依据** — 指定日志的顺序和分组。

4. 单击**查询**开始查询。

日志维护

移动安全代理生成关于安全风险检测事件的日志时，将发送这些日志并存储在移动安全管理模块上。使用这些日志可以评估贵组织的防护策略，并可确定易于被病毒感染或易于受到攻击的移动设备。

为避免移动安全客户端日志在硬盘上占用过多空间，请手动删除日志或配置移动安全管理 Web 控制台以便根据在日志维护屏幕上的预设自动删除日志。

预设日志删除

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**通知和报告** > **日志维护**。

   显示**日志维护**窗口。
3. 选择**启用预设日志删除**。
4. 选择要删除的日志类型。
5. 选择是删除所有所选日志类型的日志还是只删除指定天数之前的日志。
6. 指定日志删除频率和时间。
7. 单击**保存**。

手动删除日志

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**通知和报告** > **日志维护**。

   显示**日志维护**窗口。
3. 选择要删除的日志类型。
4. 选择是删除所有所选日志类型的日志还是只删除指定天数之前的日志。
5. 单击**立即删除**。

第 10 章

使用通知和报告

本章介绍了如何在移动安全中配置与使用通知和报告。

本章包括以下几节内容：

关于通知邮件和报告

您可以配置移动安全，使其通过电子邮件向管理员和/或用户发送通知和报告。

- **管理员通知** — 如果出现任何系统异常，将向管理员发送电子邮件通知。
- **报告** — 向指定的电子邮件收件人发送报告。
- **用户通知** — 发送电子邮件和/或短信，以通知移动设备下载并安装移动安全代理。

配置通知设置

配置电子邮件通知

如果您想要向用户发送电子邮件消息通知，则必须配置以下设置。

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**通知和报告** > **设置**。

   显示**通知和报告设置**窗口。
3. 在**电子邮件设置**部分下，键入**发件人**电子邮件地址、SMTP 服务器 IP 地址和其端口号。
4. 如果 SMTP 服务器需要身份验证，请选择**身份验证**，然后键入用户名和密码。
5. 单击**保存**。

管理员通知

使用**管理员通知**窗口配置以下设置：

- **实时恶意软件检测警告** — 当客户端检测到恶意软件时向管理员发送电子邮件通知。
- **恶意证书警告** — 当客户端检测到恶意证书时向管理员发送电子邮件通知。
- **恶意 iOS 配置文件警告** — 当客户端检测到恶意 iOS 配置文件时向管理员发送电子邮件通知。
- **系统错误** — 如果出现任何系统异常，将向管理员发送电子邮件通知。标记变量 `<%PROBLEM%>`、`<%REASON%>` 和 `<%SUGGESTION%>` 将替换为实际问题、原因和解决问题的建议。
- **苹果推送通知服务证书过期警告** — 在苹果推送通知服务证书过期前一个月向管理员发送电子邮件通知。

启用管理员通知

过程

1. 转到**通知和报告** > **管理员通知**。

   显示**管理员通知**窗口。

2. 选择您想通过电子邮件接收的通知和报告。
3. 单击**保存**。

配置管理员通知设置

过程

1. 转到**通知和报告** > **管理员通知**。

   显示**管理员通知**窗口。

2. 在**通知设置**下，单击通知名称。

   显示所选通知的**电子邮件设置**窗口。

3. 根据需要进行如下更新：

   - **收件人**：管理员的电子邮件地址。

     注意
     使用分号 “;” 分隔多个电子邮件地址。

   - **主题**：通知电子邮件的主题行。
   - **消息**：通知的消息正文。

4. 单击**保存**。

报告

移动安全允许您生成和发送以下报告：

- **安全报告** — 显示有关检测到的恶意软件、被篡改的应用程序、隐私风险、易受攻击的应用程序、网络流量解密、不安全的接入点 (Wi-Fi)、恶意 SSL 证书、恶意 iOS 配置文件、开发人员选项、USB 调试状态、Root 权限/越狱版状态和前十 (10) 个阻止的 Web 站点的信息。
- **设备清单报告** — 显示有关所有托管设备的全面信息。
- **设备注册报告** — 显示有关设备注册的信息。

可以从**报告**窗口执行以下任务。

表 10-1. 报告任务

任务	描述
生成	可以根据需要随时生成新报告。 有关详细信息，请参阅生成报告 第 10-5 页。
查看	可以从“按需”选项卡查看上次生成的报告。 有关详细信息，请参阅查看报告 第 10-6 页。
发送	可以根据需要随时选择通过电子邮件发送报告。 有关详细信息，请参阅发送报告 第 10-7 页。
预设	可以指定固定的预设，向管理员和其他用户发送报告。 有关详细信息，请参阅预设报告 第 10-7 页。

生成报告

注意

移动安全仅在服务器上保留每种报告类型的一个副本。

在生成新版本之前，保存最新报告的副本。

过程

1. 在移动安全管理 Web 控制台上，转到**通知和报告** > **报告** > **按需**。

   显示**按需**窗口。

2. 选择时间范围。
   - 今天
   - 过去 7 天
   - 过去 30 天

3. 选择所有或一个设备平台。
   - 所有类型
   - iOS
   - Android
4. 选择要包括在报告中的用户信息。
   - 所有用户
   - 特定用户
5. 选择要生成的报告。
6. 单击**生成**。

   移动安全将生成所选报告并覆盖所有现有版本。

查看报告

过程

1. 在移动安全管理 Web 控制台上，转到**通知和报告** > **报告**。
2. 从以下任何选项卡中找到要查看的报告。
   - **按需** — 选择该选项卡可查看按需报告。
   - **预设** — 选择该选项卡可查看预设报告。
3. 单击**查看**。

注意

如果看不到链接，则必须先生成报告。

有关详细信息，请参阅生成报告 第 10-5 页。

所选报告将在新的选项卡或窗口中打开。

发送报告

过程

1. 在移动安全管理 Web 控制台上，转到**通知和报告** > **报告** > **按需**。

   显示**按需**窗口。

2. 从**报告**表中找到所需的报告。

3. 单击**发送**。

   注意

   如果看不到链接，则必须先生成报告。

   有关详细信息，请参阅生成报告 第 10-5 页。

   显示**发送报告**窗口。

4. 键入收件人的电子邮件地址。

5. 可以选择修改电子邮件的主题和消息。

6. 单击**发送**。

   将显示确认消息。

预设报告

过程

1. 在移动安全管理 Web 控制台上，转到**通知和报告** > **报告** > **预设**。

   显示**预设**窗口。

2. 从下拉列表中选择报告频率。
   - **每日一次**
   - **每周一次**：使用下拉列表指定报告将在一周中的哪一天发出。
   - **每月一次**：使用下拉列表指定报告将在一月中的哪一天发出。
3. 单击**保存**。

修改电子邮件模板

过程

1. 在移动安全管理 Web 控制台上，转到**通知和报告** > **报告** > **预设**。

   显示**预设**窗口。
2. 单击报告名称。

   显示所选报告的**电子邮件设置**窗口。
3. 根据需要进行如下更新：
   - **收件人**：管理员的电子邮件地址。

     注意

     使用分号 “;” 分隔多个电子邮件地址。
   - **主题**：报告电子邮件的主题行。
   - **消息**：报告的消息正文。
4. 单击**保存**。

   将显示确认消息。

用户通知

使用**用户通知**窗口配置以下电子邮件通知：

- **移动设备注册** — 发送电子邮件和/或短信，以通知移动设备下载并安装移动安全客户端。标记变量 <%DOWNLOADURL%> 将替换为安装包的实际 URL。

配置用户通知

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**通知和报告** > **用户通知**。

   显示**用户通知**窗口。
3. 选择要通过电子邮件或短信发送给用户的通知，然后单击单个通知以修改其内容。
   - 要配置电子邮件通知消息，请根据需要更新以下详细信息：
     - **主题**：电子邮件的主题。
     - **消息**：电子邮件的正文。
   - 要配置短信通知消息，请更新**消息**文本框中的消息正文。
4. 完成后单击**保存**，以返回到**用户通知**窗口。

第 11 章

疑难解答与联系技术支持

在这里您能够找到对常见问题的解答，并了解如何获取关于移动安全的其他信息。

本章包括以下几节内容：

疑难解答

此部分提供了相关提示，以帮助您解决在使用移动安全时可能遇到的问题。

- **取消通信服务器卸载进程之后，通信服务器无法正常运行。**

  如果在停止之前，卸载进程已经开始删除对通信服务器的正常运行有重要影响的文件和服务，则通信服务器可能无法正常运行。若要解决此问题，请再次安装并配置通信服务器。

- **如果您使用 SQL Server Express，则无法保存数据库设置。**

  如果您使用 SQL Server Express，请在“服务器地址”文本框中使用以下格式：`<SQL Server Express IP 地址>\sqlexpress`。

  注意

  使用 SQL Server Express 的 IP 地址替换 `<SQL Server Express IP 地址>`。

- **无法连接至 SQL Server。**

  如果 SQL Server 未配置为接受远程连接，可能会出现此问题。缺省情况下，SQL Server Express 和 SQL Server Developer 版本均不允许远程连接。若要将 SQL Server 配置为允许远程连接，请执行以下步骤：

  1. 在您希望从远程计算机连接到的 SQL Server 实例上启用远程连接。
  2. 开启 SQL Server 浏览器服务。
  3. 将防火墙配置为允许与 SQL Server 和 SQL Server 浏览器服务相关的网络通信。

- **无法连接到 SQL Server 2008 R2。**

  如果 Visual Studio 2008 未安装在默认位置，因此 SQL Server 2008 安装程序无法找到 devenv.exe.config 配置文件，则可能会出现此问题。若要解决此问题，请执行以下步骤：

  1. 转到 `<Visual Studio 安装文件夹>\Microsoft Visual Studio 9.0\Common7\IDE` 文件夹，找到并复制 `devenv.exe.config` 文件，然后将其粘贴至以下文件夹（您可能需要在文件夹选项中启用“显示已知文件类型的扩展名”）：

- 对于 64 位操作系统：

  ```
  C:\Program Files (x86)\Microsoft Visual Studio
  9.0\Common7\IDE
  ```

- 对于 32 位操作系统：

  ```
  C:\Program Files\Microsoft Visual Studio
  9.0\Common7\IDE
  ```

2. 再次运行 SQL Server 2008 安装文件并将 BIDS 功能添加至 SQL Server 2008 现有实例中。

- **无法在设备管理中导出客户机设备列表。**

  如果在 Internet Explorer 中禁用加密文件下载，则可能会出现此问题。执行以下步骤以启用加密文件下载：

  1. 在 Internet Explorer 中，选择**工具** > **Internet 选项**，然后单击 **Internet 选项**窗口中的**高级**选项卡。
  2. 在**安全**部分，清除**不将加密的页面存入硬盘**。
  3. 单击**确定**。

- **“策略”弹出窗口不显示内容且被 Internet Explorer 阻止。**

  如果 Internet Explorer 已配置为使用 .pac 自动配置文件，则会出现这种情况。在这种情况下，Internet Explorer 将阻止访问含有多个框架的安全 Web 站点。要解决此问题，可将移动安全管理服务器地址添加到 Internet Explorer 中的可信站点安全区。为此，请执行以下步骤：

  1. 启动 Internet Explorer。
  2. 转到**工具** > **Internet 选项**。
  3. 在**安全**选项卡上，单击**可信站点**，然后单击**站点**。
  4. 在**将此 Web 站点添加到该区**文本字段中，键入移动安全管理服务器 URL，然后单击“添加”。
  5. 单击**确定**。

  有关此问题的详细信息，请参见以下 URL：

http://support.microsoft.com/kb/908356

在联系技术支持之前

在联系技术支持之前，您可以做两件事以尝试快速找到问题的解决方案：

- **查看文档** - 手册和联机帮助为您提供了有关移动安全的全面信息。查找这两种文档以确定是否包含您所需要的解决方案。
- **访问我们的技术支持 Web 站点** - 我们的技术支持 Web 站点（亦称知识库），包含关于所有趋势科技产品的最新信息。该技术支持 Web 站点包含对先前用户咨询的解答。

  要搜索知识库，请访问

  http://esupport.trendmicro.com/zh-cn/default.aspx

与趋势科技联系

可通过电话、传真或电子邮件联系趋势科技代表：

地址	趋势科技•中国 趋势科技（中国）有限公司 上海市淮海中路 398 号世纪巴士大厦 8 楼
电话	021-6384 8899
传真	021-6384 1899
Web 站点	http://www.trendmicro.com.cn
电子邮件地址	service@trendmicro.com.cn

- 全球技术支持办公室：

  http://cn.trendmicro.com/cn/about/contact_us/index.html

- 趋势科技产品文档：

http://docs.trendmicro.com/zh-cn/home.aspx

将可疑内容发送给趋势科技

可以使用多种选项将可疑内容发送给趋势科技进行进一步分析。

文件信誉服务

收集系统信息并将可疑文件内容提交至趋势科技：

http://esupport.trendmicro.com/solution/zh-CN/1095943.aspx

记录案例编号以用于跟踪。

TrendLabs

趋势科技 TrendLabs℠ 是防病毒研究和产品支持中心的全球网络，为全球的趋势科技客户提供全天候的持续服务。

TrendLabs 全球的专业服务中心拥有 250 多名工程师和训练有素的技术支持人员组成的团队，可确保在全球范围内的任何地方出现任何病毒爆发或紧急客户支持问题时均可迅速做出反应。

TrendLabs 现代化的总部在 2000 年就获得了 ISO 9002 质量管理认证。TrendLabs 是首批获得这项国际认证的防病毒研究和技术支持机构之一。趋势科技相信 TrendLabs 是防病毒业界领先的服务和技术支持团队。

有关 TrendLabs 的更多信息，请访问：

http://us.trendmicro.com/us/about/company/trendlabs/

关于软件更新

产品发布后，趋势科技通常会开发软件更新内容，以增强产品性能、添加新增功能或解决已知问题。根据更新的发布原因，有多种不同的更新类型。

以下是趋势科技可能发布的项目的摘要：

- **Hot fix** — Hot fix 是对单个客户所报告问题的解决办法或解决方案。Hot fix 是针对特定客户的，因此并不适用于所有客户。Windows hot fix 包括安装程序、而非 Windows hot fix 不包括安装程序 — 通常需要停止守护程序、复制文件以覆盖所安装产品中相对应的文件并重新启动守护程序。
- **安全 Patch** — 安全 Patch 是适合部署到所有客户机的解决安全问题的 hot fix。Windows 安全补丁包括安装程序，而非 Windows 补丁通常包含安装脚本。
- **Patch** — patch 是一组 hot fix 和安全 patch，可解决多个程序问题。趋势科技定期发布 patch。Windows patch 包括安装程序，而非 Windows patch 通常包含安装脚本。
- **Service Pack** — Service pack 包含各种 hot fix、patch 和功能改进，可被视为产品升级。Windows 和非 Windows service pack 都包括安装程序和安装脚本。

请检查趋势科技知识库以搜索发布的 hot fix：

http://esupport.trendmicro.com/zh-cn/default.aspx

请定期检查趋势科技 Web 站点以下载 patch 和 service pack：

http://www.trendmicro.com/download/zh-cn

所有版本都包括自述文件，其中包含安装、部署和配置产品所需的信息。请首先仔细阅读自述文件，然后再安装 hot fix、patch 或 service pack 文件。

已知问题

已知问题是移动安全中可能暂时需要进行处理的功能。已知问题通常记录在您收到的产品附带自述文件里。趋势科技产品的自述文件也可在趋势科技下载中心找到：

http://www.trendmicro.com/download/zh-cn/

已知问题可在技术支持知识库中找到：

http://esupport.trendmicro.com/zh-cn/default.aspx

趋势科技建议始终查看自述文件文本中有关可能影响安装或性能的已知问题的信息，以及特定版本中新增功能的说明、系统需求以及其他提示信息。

其他有用的资源

移动安全通过其站点 http://www.trendmicro.com.cn 提供了诸多服务。

基于 Internet 的工具和服务包括：

- 病毒地图 — 监控全球范围的恶意软件事件
- 病毒风险评估 - 适用于企业网络的趋势科技在线恶意软件防护评估程序。

关于趋势科技

趋势科技（中国）有限公司在网络防恶意软件和 Internet 内容安全软件和服务领域处于领先地位。趋势科技（中国）有限公司成立于 1988 年，它将恶意软件防护从台式机扩展到网络服务器和 Internet 网关，一直以来在视觉和技术创新方面获得广泛赞誉。

如今，趋势科技提供集中式控制的基于服务器的恶意软件防护和内容过滤产品与服务，重点关注为客户提供全面的安全策略，用于处理信息风险所带来的影响。通过保护流经因特网网关、电子邮件服务器和文件服务器的信息，趋势科技帮助全球性公司和服务提供商自一个中心位置将恶意软件和其他恶意代码阻止于台式机之外。

如需更多信息或下载趋势科技产品的评估版本，请访问我们获奖的 Web 站点：

http://www.trendmicro.com.cn

索引

TREND MICRO™

趋势科技・中国 趋势科技（中国）有限公司

上海市淮海中路 398 号世纪巴士大厦 8 楼

电话：021-6384 8899　传真：021-6384 1899　service@trendmicro.com.cn

www.trendmicro.com

Item Code: TSCM98142/180126