TREND MICRO™

9.0

趋势科技™ 移动安全™企业版 管理员指南

应用于企业手持设备的全面安全解决方案

终端安全

文档编号 TSCM96388/140410

发布日期：2014 年 3 月

趋势科技™ 移动安全 9.0 SP1 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。

http://www.trendmicro.com/download/documentation/rating.asp

目录

前言

第 1 章：简介

第 2 章：移动安全入门

第 3 章：管理移动设备

第 4 章：利用策略保护设备

第 5 章：管理企业应用程序商店

第 6 章：更新组件

第 7 章：查看和维护日志

第 8 章：使用通知和报告

第 9 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 9.0 SP1 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（例如，智能手机和 Pocket PC/Pocket PC Phone）
- 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://cn.trendmicro.com/cn/support/techsupport/index.html

提示

趋势科技建议检查下载中心 (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 v9.0 SP1 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。

除受恶意软件、垃圾信息及其他多余内容的威胁之外，移动设备还容易受到黑客和拒绝服务 (DoS) 攻击。现在，多数移动设备同样也具有传统上只应用于较大计算设备（例如，笔记本电脑和台式机）的网络连接，因此也成为此类攻击的目标。

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 v9.0 SP1

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反恶意软件技术，能有效防范对移动设备的最新威胁。

集成的防火墙和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。这些不需要的网络通信包括：通过 3G/GPRS 连接接收到的短信、服务信息邮件和数据。

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。

此外，移动安全附带通用加密模块，可在 Symbian 和 Windows Mobile 设备上提供登录密码保护和数据加密功能。此加密模块有助于防止因移动设备丢失或被盗而危及数据安全。

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、短信管理和防火墙防护）的软件产品也可能与移动安全不兼容。

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机－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
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。 趋势科技移动安全提供两种类型的通信服务器： • 本地通信服务器 (LCS) — 这是在您的网络中本地部署的通信服务器。 • 云通信服务器 (CCS) — 这是在云中部署的通信服务器，不需要安装此服务器。趋势科技会管理云通信服务器，您只需要从管理服务器连接到该服务器。 请参阅 本地和云通信服务器比较 第 1-5 页。	必需

组件	描述	必需或可选
短信发送器	可以使用短信发送器向用户发送短信。	可选
Exchange 连接器	趋势科技移动安全使用 Exchange 连接器与 Microsoft Exchange 服务器通信，并检测使用 Exchange ActiveSync 服务的设备。	可选
移动安全客户端 (MDA)	移动安全客户端安装在托管移动设备上。该客户端与移动安全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 托管移动安全服务器的数据库。	必需
Active Directory	移动安全服务器从 Active Directory 导入用户和组。	可选
证书颁发机构	证书颁发机构管理安全凭证和公共和私人密钥，以保障安全通信。	可选
SCEP	简单证书注册协议 (SCEP) 和证书颁发机构一起为大企业颁发证书。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
苹果推送通知服务证书	移动安全服务器通过 iOS 设备的苹果推送通知服务证书 (APNs) 通信。	如果要管理 iOS 移动设备，则为必需
SSL 证书	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 5 或更高版本的移动设备，则为必需
BES 用户管理工具	要支持对在 BES 服务器中注册的 BlackBerry 设备的管理，BES 用户管理工具是必需的。	如果要管理 BlackBerry 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	云通信服务器	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	不支持	支持
管理 Symbian 移动设备	不支持	支持
管理 Windows Mobile 设备	不支持	支持

此版本 (v9.0 SP1) 的新增功能

下表介绍了趋势科技™ 移动安全企业版 v9.0 SP1 的附加功能。

功能名称	描述
独立管理服务器	此版本的趋势科技移动安全独立于防毒墙网络版，并且可以直接在 Windows 计算机上安装。
可选云通信服务器	除了本地安装的通信服务器（本地通信服务器），此版本还提供使用在云中部署的通信服务器（云通信服务器）的选项。管理员不需要安装云通信服务器，它是由趋势科技维护的。
Exchange 服务器集成	提供与 Microsoft Exchange 服务器的集成，并支持使用 Exchange ActiveSync 服务的 iOS、Android 和 Windows Phone 移动设备。
基于模板的策略	让您能够创建、复制或删除安全策略，并将其分配给特定的移动设备组。

功能名称	描述
支持多管理员帐户	让您能够根据需要创建拥有可自定义的不同角色的多管理员帐户。
最新设备状态	使用最新设备状态列表显示移动设备的更多适当当前状态。
iOS 设备配置	使您可以将配置概要文件推送到 iOS 移动设备，以配置 VPN、Wi-Fi 和 Exchange ActiveSync 设置。
iOS 移动设备的监管模式设备管理	此版本还添加了对监管模式 iOS 移动设备的支持。
控制台窗口管理	让您能够以小部件的形式管理显示在**控制台**窗口中的信息。可以根据需要添加或删除小部件。
服务器命令确认	提供**命令队列管理**界面，可以显示每个从服务器执行的命令的当前状态。
使用类别的应用程序控制	可以使用允许列表和阻止列表来允许或阻止在 iOS 和 Android 移动设备上安装属于特定类别的应用程序。
使用 QR 码的移动设备注册	引入使用在用户电子邮件中发送的 QR 码进行的移动设备注册。
功能锁定策略改进	向功能锁定列表中添加了更多功能和操作系统组件，便于管理员控制它们在移动设备上的可用性。
iOS 批量购买计划支持	让您能够将通过苹果批量购买计划购买的 iOS 应用程序导入移动安全管理 Web 控制台。
最新的移动安全客户端界面	引入了 Android 和 iOS 移动安全客户端的新用户界面。
与 MARS 集成	提供服务器和 Android 移动安全客户端与趋势科技移动应用程序信誉服务 (MARS) 的集成，以降低应用程序安全风险并提高资源利用率。
管理员报告下载	让您能够从移动安全管理 Web 控制台下载管理员报告。
策略违例日志	提供 Android 移动设备的策略违例日志。
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的集成。通过此集成，防毒墙控制管理中心管理员能够将企业策略传送到移动设备，并能够在防毒墙控制管理中心查看移动安全**控制台**窗口。

版本 8.0 SP1 的新增功能

下表对趋势科技™ 移动安全企业版 v8.0 Service Pack 1 (SP1) 中引进的附加功能进行了描述。

功能名称	描述
基于设备身份的身份验证	让您能够使用 IMEI 号和/或 Wi-Fi MAC 地址批量验证移动设备。
Android 和 iOS 非托管组	为禁用了设备管理员的 Android 移动设备和删除了注册配置文件的 iOS 移动设备引入非托管组。
增强事件日志	提供增强事件日志，以记录与移动设备密码重置、远程定位、远程锁定和远程擦除相关的事件。
可自定义注册 URL	为移动设备的注册提供更短且可自定义的 URL。
简单的 iOS 客户端	引入 iOS 客户端，以使用用户电子邮件地址进行简易用户身份验证和注册。iOS 客户端还提供对移动设备上企业应用程序商店的访问。

版本 8.0 的新增功能

下表对趋势科技™ 移动安全企业版 v8.0 中引入的附加功能进行了描述。

功能名称	描述
客户端定制	可在 Android 安装包中预置服务器 IP 地址和端口号。
Android 的 Web 代理支持	允许在 Android 移动设备中设置 Web 代理。
Android 的 HTTP(S) 推送通知设置	提供启用或禁用 Android 移动设备 HTTP(S) 推送通知的设置。
简化配置	可在 Android 移动设备中预先配置服务器 IP 地址、域名和服务器端口号，以减轻移动设备的部署和注册工作量。

功能名称	描述
病毒码更新后扫描	在病毒码更新成功后自动开始扫描移动设备中的安全威胁，并在通知栏中显示相关进程。
Web 威胁防护策略	可管理移动安全服务器中的 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。
添加 Android 的 SD 卡限制	可控制 Android 移动设备的 SD 卡的可用性。
应用程序清单	保留移动设备上安装的应用程序的列表，并在设备状态窗口中显示该列表。
应用程序控制	可以使用允许列表和阻止列表来允许或阻止在移动设备上安装特定应用程序。
应用程序推送	可将应用程序安装包或应用程序的 Web 链接推送到移动设备，以进行安装。
选择性擦除	可在不删除用户个人数据的情况下，删除服务器中的所有企业数据。
合规检查	可设置服务器上的合规条件，并检查移动设备的合规性。
使用 Active Directory 进行身份验证（可选）	可使用 Active Directory (AD) 或移动安全数据库对 Symbian、Windows Mobile、iOS 和 Android 移动设备进行注册前的用户身份验证。
控制台窗口	引入**控制台**窗口，替换 Web 控制台上的原**摘要**窗口，用以提供服务器组件和移动设备的状态摘要。
预设报告	您可以配置移动安全，使其按预定义的时间间隔发送预设报告。
快速配置验证窗口	引入**移动安全配置和验证**窗口，您可以快速验证移动安全配置并识别问题（如有）。如果配置验证窗口检测到任何错误的配置设置，其将提供更正建议。
适用于 iOS 和 Android 的按需远程密码重置	您可以从 Web 控制台远程对 iOS 和 Android 移动设备进行密码重置。
企业应用程序商店	您可以创建 Web 剪辑和应用程序列表，以便用户在其移动设备上下载和安装列表中的项目。

版本 7.1 的新增功能

下表对趋势科技™ 移动安全企业版 v7.1 中引进的附加功能进行了描述。

功能名称	描述
对 iOS 和 Blackberry 移动设备的支持	移动安全 v7.1 新增了对 iOS 和 BlackBerry 移动设备的支持。
与 Active Directory 集成	移动安全 v7.1 使用了企业的 Active Directory (AD) 以导入用户和执行用户身份验证。
更新的体系结构	移动安全 v7.1 引入了单、双服务器部署型号。v7.1 版本还删除了短信网关。
配置策略	此版本引入了针对移动设备的配置策略。

版本 7.0 的新增功能

本节对趋势科技™ 移动安全企业版 v7.0 中引进的附加功能进行了描述。

功能名称	描述
对 Android 移动设备的支持	移动安全 v7.0 增加了对 Android v2.1 及以上版本的移动设备的支持。
电话过滤策略	管理员能够控制 Android 移动设备上的来电或去电。
更新的功能锁定	管理员能够控制某个或某些接入点范围内的 Android 移动设备某些部件的可用性。
定位远程设备	管理员能够通过无线网络或使用移动设备的 GPS 在 Google 地图上显示设备位置来定位远程设备。此新功能有助于定位丢失、被盗或误放的移动设备。
更新的体系结构	移动安全 v7.0 增加了短信网关，其替代短信发送器，用于向移动设备发送短信。

移动安全代理的主要功能

功能名称	描述
防恶意软件扫描	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，允许用户隔离和删除受感染文件。
Web 安全	随着移动设备技术的提升，移动威胁的复杂性也在增加。趋势科技移动安全提供 Web 信誉和家长控制，用以保护您的移动设备免受不安全网站的侵扰，以及可能包含儿童、青少年和其他家庭人员不宜内容的网站的侵扰。您可以根据需要的设置修改 Web 信誉和家长控制设置级别。移动安全还将在 Web 信誉或家长控制的专门日志中保留它们所阻止的网站日志。
反垃圾信息	移动设备通常会通过短信传输接收到不需要的消息或垃圾信息。要将不需要的短信过滤到垃圾信息文件夹，可指定发送所有这些将被视为垃圾信息的短信的电话号码，或指定批准的电话号码列表并配置移动安全使其过滤来自不在允许列表的发件人的所有消息。还可以过滤无法识别的短信或没有发件人电话号码的消息。您的移动设备会自动将这些消息存储到收件箱的垃圾信息文件夹。 **注意** 反垃圾短信功能不适用于没有电话功能的移动设备。
电话过滤	移动安全可以过滤来自服务器的来电或去电。可以配置移动安全阻止来自特定电话号码的来电，或指定移动设备可以呼叫的允许电话号码列表。移动安全还可以让移动设备用户指定自己的阻止或允许列表，以过滤不想接听的来电。 **注意** 电话过滤功能不适用于没有电话功能的移动设备。

功能名称	描述
服务信息防护	服务信息是一种将内容自动传递到移动设备的有效方法。为发动内容传送，它会向用户发送特殊的短信（称为服务信息）。通常，这些消息包含关于内容的信息，并用作用户可接受或拒绝内容的方法。 恶意用户会发出不正确或非信息的服务信息，目的是欺骗用户接受可能包括不需要的应用程序、系统设置甚至恶意软件的内容。移动安全允许用户使用可信发件人列表来过滤服务信息，并防止不需要的内容进入移动设备。 服务信息防护功能不适用于没有电话功能的移动设备。
身份验证	安装移动安全代理后，移动设备与用户相关联。用户必须键入密码（亦称开机密码）才能登录到移动设备。
数据加密	移动安全为存储在移动设备和内存卡上的数据提供了动态数据加密。可指定要加密的数据类型和要使用的加密算法。
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。
防火墙（仅 BlackBerry、Symbian 和 Windows Mobile）	移动安全包括趋势科技防火墙模块，此模块具有多个用于过滤网络通信的预定义安全级别。您也可定义自己的过滤规则，并过滤来自特定 IP 地址和特定端口的网络通信。入侵检测系统 (IDS) 可阻止向移动设备连续发送多个数据包的尝试。通常，这些尝试会构成拒绝服务 (DoS) 攻击，并导致移动设备因过于繁忙而无法接受其他连接。

功能名称	描述

日志	管理服务器包括以下移动安全客户端日志：
	• 恶意软件防护日志
	• Web 威胁防护日志
	• 加密日志
	• 防火墙日志
	• 事件日志
	• 违例日志
	可在移动设备上查看到以下日志：
	• Windows Mobile 和 Symbian：
	  • 病毒/恶意软件日志
	  • 防火墙日志
	  • 反垃圾短信日志
	  • 服务信息防护日志
	  • 任务日志
	• Android：
	  • 恶意软件扫描历史记录
	  • 隐私扫描历史记录
	  • Web 阻止历史记录
	  • 来电阻止历史记录
	  • 短信阻止历史记录
	  • 更新历史记录

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不同平台上支持的功能列表。

表 1-3. 趋势科技移动安全 9.0 SP1 功能矩阵

策略	功能	设置					
预置	Wi-Fi	标准 Wi-Fi 配置	●	●	●		
		传统 Hotspot 配置	●				
		Hotspot 2.0 配置	●				
	Exchange ActiveSync	Exchange ActiveSync 配置	●				
	VPN	VPN 配置	●		●		
	全局 HTTP 代理	全局 HTTP 代理配置	●				
	单点登录	单点登录配置	●				
	证书	证书配置	●				
设备安全	恶意软件防护	实时扫描		●		●	●
		卡扫描				●	●
		病毒码更新后扫描		●			

策略	功能	设置					
数据保护	垃圾短信阻止	服务器端控制		●	●	●	●
		使用阻止列表		●	●	●	●
		使用允许列表		●	●	●	●
	垃圾服务信息阻止	服务器端控制		●		●	●
		使用允许列表		●		●	●
	电话过滤	服务器端控制		●	●		
		使用阻止列表		●	●		
		使用允许列表		●	●		
	防火墙	启用防火墙			●	●	●
		启用入侵检测系统 (IDS)				●	●
	Web 威胁防护	服务器端控制		●			
		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	●				

策略	功能	设置					
数据保护	密码设置	使用密码登录	●	●	●	●	
		管理员密码				●	
		允许简单密码	●	●	●	●	
		要求字母数字密码	●	●	●	●	
		最小密码长度	●	●	●	●	
		密码到期	●	●		●	
		密码历史	●	●		●	
		自动锁定	●	●		●	
		密码失败操作	●	●	●	●	
	加密	加密 PIM				●	
		加密文件				●	
		加密记忆卡				●	
	功能锁定	相机	●	●		●	
		FaceTime	●				
		屏幕抓图	●				
		应用程序安装	●				

策略	功能	设置					
数据保护	功能锁定	漫游时同步	●				
		语音拨号	●		●		
		应用程序内购买	●				
		多人游戏	●				
		添加 Game Center 好友	●				
		Game Center（仅限监管模式）	●				
		强制加密备份	●				
		显式音乐、播客和 iTunes U	●				
		设备锁定时使用 Passbook	●				
		蓝牙和蓝牙探测		●		●	
		红外线				●	
		USB 存储				●	
		WLAN/Wi-Fi		●		●	
		3G 数据网络		●			

策略	功能	设置					
数据保护	功能锁定	限制		●			
		开发模式		●			
		串行				●	
		扬声器/免提话筒/麦克风			●	●	
		Microsoft ActiveSync				●	
		彩信/短信				●	
		限制记忆卡		●		●	
		限制 GPS				●	
		Siri	●				
		设备锁定时使用 Siri	●				
		启用脏话过滤器	●				
		允许访问 iCloud 服务	●				
		云备份	●				
		云文档同步	●				
		照片流	●				

策略	功能	设置					
数据保护	功能锁定	共享照片流	●				
		诊断数据	●				
		接受不可信传输层安全 (TLS) 协议	●				
		强制 iTunes 存储密码	●				
		YouTube	●				
		在其他应用程序中打开托管应用程序的文档	●				
		在托管应用程序中打开其他应用程序的文档	●				
		iTunes	●				
		Safari Web 浏览器	●				
		自动填充	●				
		JavaScript	●				
		弹出窗口	●				
		强制欺诈警告	●				
		接受 Cookie	●				
		删除应用程序（仅限监管模式）	●				
		书店（仅限监管模式）	●				

策略	功能	设置					
数据保护	功能锁定	Erotica（仅限监管模式）	●				
		配置概要文件安装（仅限监管模式）	●				
		iMessage（仅限监管模式）	●				
		地区评分	●				
		电影	●				
		电视节目	●				
		应用程序	●				
远程控制		注册	●	●	●	●	●
		更新	●	●	●	●	●
	防盗	远程定位		●	●		
		远程锁定	●	●	●	●	
		远程擦除	●	●	●	●	
		重置密码	●	●	●	●	

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。

您可以使用 Web 控制台进行下列操作：

- 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 2-14 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服务器。有关详情，请咨询当地的趋势科技销售代表。

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更新说明，请在移动安全**产品使用授权**窗口中单击查看使用授权更新说明链接。

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。

控制台窗口分为五个选项卡：

- **摘要** — 显示设备的健康状态和设备的操作系统摘要。
- **健康** — 显示组件、策略更新以及移动设备的健康状态。在此类别中，您可以：
  - 查看移动设备的状态：
    - **正常** — 说明该设备已注册到移动安全服务器，且移动设备上的组件和策略为最新版本。
    - **不合规** — 说明设备已注册到移动安全服务器，但不符合服务器策略。
    - **未同步** — 说明该设备已注册到移动安全服务器，但是组件和策略为过期版本。
    - **非活动** — 说明该设备尚未注册到移动安全服务器。
  - 查看移动安全管理的已注册和未注册的移动设备总数。

    如果出现以下情况之一，则移动设备可能保持未注册状态：
    - 到通信服务器的连接失败
    - 移动设备用户已删除注册短信
  - 查看移动设备程序 Patch 和组件更新状态：
    - **当前版本** - 移动安全代理或移动安全服务器上组件的当前版本号
    - **最新** - 具有最新的移动安全代理版本或组件的移动设备数量
    - **过期** - 使用过期组件的移动设备数量
    - **更新率** - 使用最新组件版本的设移动备百分比
    - **已升级** - 使用最新移动安全代理版本的移动设备数量

- **未升级** — 未升级到使用最新移动安全代理版本的移动设备数量
- **升级率** - 使用最新移动安全代理版本的移动设备百分比

- 查看服务器更新状态：
  - **服务器** - 模块名称
  - **地址** - 作为模块主机的计算机的域名或 IP 地址
  - **当前版本** - 移动安全服务器模块的当前版本号
  - **上次更新** - 上次更新的时间和日期

- **清单** — 显示移动设备操作系统版本摘要、电话运营商摘要、移动设备供应商摘要以及移动设备上的应用程序安装前 10 位。
- **合规性** — 显示移动设备的应用程序控制、加密和越狱版/Root 权限状态。在此类别中，您可以：
  - 查看移动设备的越狱版/Root 权限状态：
    - **越狱版/Root 权限** — 越狱版/Root 权限的移动设备数量
    - **非越狱版/Root 权限** — 非越狱版/Root 权限的移动设备数量
  - 查看移动设备加密状态：
    - **已加密** — 已加密的移动设备的数量
    - **未加密** — 未加密的移动设备的数量
  - 查看移动设备应用程序控制状态：
    - **合规** — 符合移动安全合规和应用程序控制策略的移动设备数量
    - **不合规** — 不符合移动安全合规和应用程序控制策略的移动设备数量
- **防护** — 显示前五 (5) 项安全威胁的列表和前五 (5) 项已阻止 Web 站点的列表。

注意

在**控制台**窗口上的每个小部件中，可以从下拉列表中选择**全部**或组名，以显示相关设备的信息。

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。

配置设备验证

趋势科技移动安全使您能够根据 Active Directory (AD) 或移动安全数据库来配置设备验证。您还可以允许移动设备在无需身份验证的情况下注册到移动安全服

务器。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。

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

缺省管理员帐户为“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 2-14 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

ROOT 帐户属性		是否可以修改？
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 2-16 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
Exchange 服务器域控制	域选择	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
	Exchange 服务器集成	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
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
应用程序商店	应用程序商店	支持	不支持

服务器组件	权限	超级管理员	组管理员
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
	邀请设备	支持	仅支持托管组
	Exchange ActiveSync 设备	支持	仅支持托管组

添加管理员帐户

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**管理** > **管理员帐户管理**。
3. 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。
4. 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。

5. 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 2-15 页

6. 单击**保存**。

编辑管理员帐户

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**管理** > **管理员帐户管理**。
3. 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。
4. 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 2-15 页。

5. 单击**保存**。

删除管理员帐户

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**管理** > **管理员帐户管理**。
3. 在**管理员帐户**选项卡上，选择要删除的管理员帐户，并单击**删除**。

创建管理员角色

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**管理** > **管理员帐户管理**。
3. 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。
4. 在**角色详细信息**部分下，提供以下信息：
   - 管理员角色

- 描述

5. 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。
6. 单击**保存**

编辑管理员角色

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**管理** > **管理员帐户管理**。
3. 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。
4. 根据要求修改角色详细信息，然后单击**保存**。

删除管理员角色

过程

1. 登录移动安全管理 Web 控制台。
2. 单击**管理** > **管理员帐户管理**。
3. 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**。

更改管理员密码

请参阅主题编辑管理员帐户 第 2-14 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，导航到**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。

Exchange 服务器集成

配置 Exchange 服务器集成设置

有关详细配置步骤，请参阅*《安装和部署指南》*中的*配置 Exchange 服务器集成设置*主题。

配置 Exchange 连接器

可以将 Exchange 连接器配置为在出现更高版本时自动更新。

过程

1. 在安装 Exchange 连接器的计算机上，单击 Windows 任务栏（在系统时钟附近）系统托盘中的**显示隐藏图标**按钮。
2. 右击 **Exchange 连接器**图标，然后单击**关于趋势科技移动安全 - Exchange 连接器**。

   显示**关于趋势科技移动安全 - Exchange 连接器**窗口。
3. 配置以下内容：
   - **启用自动更新** — 选择后，Exchange 连接器会在有新版本可用时自动更新。
   - **服务器地址** — 移动安全服务器 IP 地址。
   - **HTTPS 端口** — 管理 Web 控制台的移动安全服务器 HTTPS 端口号。

管理证书

使用**证书管理**窗口将 `.pfx`、`.p12`、`.cer`、`.crt` 和 `.der` 证书上传到移动安全服务器。

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

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）
- 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、擦除/锁定/定位远程设备和更新策略
- 配置移动安全客户端信息
- 导出数据供进一步分析或备份

移动安全中的组

移动安全服务器会自动创建名为**移动设备**的根组，其中包含以下两个子组：

- **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。
- **未经授权** — 如果**设备注册设置**中启用了**设备验证**且使用移动设备列表进行验证，则移动安全服务器会自动创建此组。如果已注册的移动设备不在移动设备列表中，移动安全会将此类移动设备移动到**未经授权**组。移动安全还会创建其他组，并根据您使用的列表将所有移动设备重新分组。

注意

如果在**设备注册设置**中启用**设备验证**，并上传空的移动设备列表供验证，移动安全会将所有当前已注册移动设备移动到未经授权组。

注意

设备验证仅支持 Android 和 iOS 移动设备。

有关说明，请参见移动安全服务器*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. 键入**组名**并从下拉列表中选择要应用到组的**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**窗口中向移动设备发送邀请、编辑移动设备信息、删除移动设备或更改移动设备组。

向移动设备发送邀请

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. 您现在可以邀请单个移动设备、批量移动设备，以及来自 Active Directory 的用户或电子邮件组（分配列表）：
   - 要邀请移动设备，请执行以下步骤：
     a. 单击**邀请用户** > **邀请单个用户**。

        弹出**邀请单个用户**窗口。

b. 在**邀请单个用户**窗口上，配置以下文本框：

- **电话号码** — 键入移动设备的电话号码。为确保移动设备能够成功地接收来自短信发送器的通知消息，可键入国家/地区代码（长度为 1-5 个数字）。无需键入国际直接拨号前缀。
- **电子邮件** — 键入用于发送通知邮件的用户电子邮件地址。
- **用户名** — 键入移动设备的名称，以在设备树中标识设备。
- **组** — 从下拉列表中选择移动设备所属组的名称。可随时更改移动安全代理所属的组。

提示

要邀请更多设备，请单击 + 按钮。

- 要邀请批量移动设备，请执行以下步骤：

a. 单击**邀请用户** > **批量邀请**。

b. 在所显示窗口中的文本框内使用以下格式键入设备信息：

电话号码, 电子邮件地址, 设备名称, 组名称, 资产编号 (可选), 描述 (可选);

注意

使用分号 (;) 或 CR 分隔每个设备信息。

c. 单击**验证**，验证设备信息是否符合特定格式。

- 要邀请来自 Active Directory 的用户或电子邮件组（分配列表），请执行以下步骤：

a. 单击**邀请用户** > **从 Active Directory 邀请**。

b. 在提供的搜索文本框中键入用户信息，并单击**搜索**。

c. 从搜索结果中选择用户，然后单击**邀请设备**。

4. 单击**保存**。

Mobile Security 向受邀设备的用户发送邀请短信或电子邮件。

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。为确保移动设备能够成功地接收来自短信发送器的通知消息，可键入国家/地区代码（长度为 1-5 个数字）。无需键入国际直接拨号前缀。
   - **电子邮件** — 用于发送通知邮件的用户电子邮件地址。
   - **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 3-7 页

- 删除多个移动设备 第 3-7 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，且不再注册到移动安全服务器。

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** — 显示移动设备的加密状态及其是否已破解。
- **网络** — 显示集成电路卡 ID (ICCID)、蓝牙和 WiFi MAC 信息以及详细网络信息，包括载波网络名称、设置版本、漫游状态、移动国家代码 (MCC) 和移动网络代码 (MNC) 信息。
- **策略** — 显示配置和安全策略上次更新的时间。

- **已安装应用程序** — 显示移动设备上已安装的所有应用程序的列表，以及合规检查结果。此选项卡仅适用于 Android 和 iOS 移动设备。

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
   - **资产编号** — 移动设备的资产编号
   - **描述** — 移动设备的描述
   - **操作系统** — 移动设备正在运行的操作系统
   - **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
   - **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
   - **被感染的移动安全客户端** — 限制对检测到指定数量恶意软件的移动设备的搜索
   - **设备状态** — 限制对选定移动设备状态的搜索

3. 单击**搜索**。搜索结果将在设备树中显示。

设备树视图选项

如果在设备树中选择了一个组，便可以使用**列**下拉列表框选择以下预定义视图之一：**总视图**和**查看全部**。这使您可以在设备树中快速查看所显示的信息。在设备树中显示的信息随着所选选项的不同而有所不同。

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 6-2 页。

在 Windows Mobile 或 Symbian 移动设备上，如果没有为移动安全启用短信传输功能，则需要在**通用策略**窗口上配置更新时间表（请参阅通用策略 第 4-7 页），以定期更新组件。但是在 Android 移动设备上，即使没有为移动安全启用短信传输功能，还可以通过推送说明更新组件和同步策略。

防丢失设备

如果用户丢失了移动设备或将其放错了地方，可以对该移动设备上的所有数据进行远程定位、锁定或删除。

定位远程移动设备

可以通过无线网络或通过使用移动设备的 GPS 定位移动设备。移动安全服务器会在 Google 地图上显示移动设备的位置。

此功能仅适用于 Android 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，从设备树中单击要定位的移动设备。
4. 单击**设备定位**，然后单击确认对话框中的**确定**。

   移动安全服务器会尝试定位移动设备并在**远程定位设备**窗口中显示 Google 地图链接。
5. 单击**远程定位设备**窗口中的 Google 地图链接，查看移动设备在地图上的最近 GPS 位置。

锁定远程移动设备

可以从管理 Web 控制台发送锁定说明，以远程锁定移动设备。用户需要键入开机密码才能解锁移动设备。

注意

仅 Android、iOS、BlackBerry 和 Windows Mobile 设备支持此功能。

Windows Mobile 设备若要使用此功能，移动设备上必须启用加密。

Windows Mobile 设备只能使用短信通知消息锁定。如果要锁定 Windows Mobile 设备，确保已经配置短信发送器。有关配置详细信息，请参阅*《安装和部署指南》*。

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，从设备树中单击要锁定的移动设备。
4. 单击**远程锁定**，然后单击确认对话框中的**确定**。

   如果锁定命令生成成功，窗口中会显示**成功**消息。要检查移动设备是否已成功锁定，可以检查**命令队列管理**窗口中的命令状态。有关详细信息，请参阅命令队列管理 第 2-17 页。

擦除远程移动设备

可以远程将移动设备重置为出厂设置，并清除移动设备的内存/SD 卡。此功能有助于确保在移动设备丢失、被盗或误放时的数据安全。还可以选择只清除移动设备上的以下企业数据：

- 对于 Android：Exchange 邮件、日历和联系人
- 对于 iOS：MDM 配置文件、相关策略、配置和数据

警告!

请谨慎使用此功能，因为此操作无法恢复。所有数据都将丢失且无法恢复。

注意

仅 Android、iOS、BlackBerry 和 Windows Mobile 设备支持此功能。

有关擦除使用 Exchange ActiveSync 的移动设备的说明，请参阅擦除远程 ActiveSync 移动设备 第 3-21 页。

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，从设备树中单击要擦除的移动设备。
4. 单击**远程擦除**。

   显示**远程擦除设备**窗口。
5. 选中对应的设备名称复选框。
6. 执行下列操作之一：
   - 对于 Android 移动设备，选择以下任一选项：
     - **将所有数据恢复为出厂设置。（将删除所有应用程序及存储的数据。将格式化插入的内存卡。此操作无法撤消。）**
     - **擦除电子邮件、日历和联系人列表。** — 也称为选择性擦除。

       如果选择此选项，还可以选中**如果选择性擦除失败，所有数据将恢复为出厂设置。**复选框。
   - 对于 iOS 移动设备，选择以下任一选项：
     - **将所有数据恢复为出厂设置。（将删除所有应用程序及存储的数据。将格式化插入的内存卡。此操作无法撤消。）**

- **清除所有预置配置文件、策略、配置及其相关数据。**

7. 单击**远程擦除设备**。

   所选的数据会从移动设备上删除，且移动安全客户端会从服务器取消注册。

远程重置密码

如果用户忘记了开机密码，则您可以通过管理服务器远程重置密码并解锁移动设备。移动设备成功解锁后，用户可更改开机密码。

注意

仅 Android、iOS 和 Windows Mobile 设备支持此功能。

为 Android 移动设备重置密码

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. 从树中选择移动设备，然后单击**密码重置**。
4. 在弹出的对话框中键入并确认新的六位数密码。

删除 iOS 移动设备的密码

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. 从树中选择移动设备，然后单击**密码重置**。

4. 单击所显示的确认对话框上的**确定**。选定 iOS 移动设备的开机密码将被删除。

为 Windows Mobile 设备重置密码

要为 Windows Mobile 设备重置密码，在远程解锁移动设备之前，需要要求用户生成紧急恢复码（16 位十六进制数）。

过程

1. 获取用户在移动设备上生成的移动设备名称和紧急恢复码。请用户参阅移动安全客户端帮助或*用户指南*以了解紧急恢复码生成的说明。

2. 登录移动安全管理 Web 控制台。

3. 单击菜单栏上的**设备**。

   显示**设备**窗口。

4. 在**托管的设备**选项卡中，从设备树中单击要重置密码的移动设备。

5. 单击**密码重置**，然后单击**远程解锁**窗口中的**选择设备**。显示设备树。

6. 选择要远程解锁的移动设备，并单击**选择**。

7. 在字段中键入紧急恢复码，并单击**生成**。

8. 移动安全服务器生成响应码并在弹出式窗口上显示这些代码。

9. 指示用户在移动设备的**密码**窗口上点击**下一步**，并键入响应码，以解锁移动设备。

导出数据

在**设备**窗口的**托管的设备**选项卡中，可以导出数据，供进一步分析或备份。

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。

邀请的设备选项卡

设备窗口中的**邀请的设备**选项卡会保留移动安全向移动设备发送的注册邀请的记录。

缺省邀请电子邮件包括以下信息：

- 趋势科技移动安全简介
- 移动安全客户端下载 URL
- 要注册的移动设备服务器信息
- 用于快速注册的 QR 码

在**邀请的设备**选项卡上，可以执行以下操作：

- 查看邀请列表

- 向移动设备重新发送邀请消息
- 取消当前邀请
- 删除旧的邀请记录

查看邀请列表

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. 单击**邀请的设备**选项卡。

   下表提供了**邀请的设备**选项卡中显示的所有邀请状态的描述。

邀请状态	描述
活动	邀请有效，用户可以使用邀请消息中的信息进行注册。
已过期	邀请已过期，用户不能使用邀请消息中的信息进行注册。
已使用	用户已经使用邀请消息中的信息进行注册，注册密钥已无效。 **注意** 仅当设备注册设置中的**注册密钥使用限制**设置为**使用一次**时，才会出现此状态。
已取消	邀请已从服务器取消，用户不能使用邀请消息中的信息进行注册。

重新发送邀请消息

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. 单击**邀请的设备**选项卡。
4. 从列表中选择要重新向其发送邀请消息的移动设备。
5. 单击**重新发送邀请**。

取消活动邀请

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. 单击**邀请的设备**选项卡。
4. 从列表中选择要取消邀请的移动设备。
5. 单击**取消邀请**。

从列表中删除邀请

注意

只能删除状态为**已使用**或**已取消**的邀请消息。

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. 单击**邀请的设备**选项卡。
4. 从列表中选择要删除其邀请记录的移动设备。
5. 单击**删除邀请**。

Exchange ActiveSync 设备选项卡

在移动安全服务器上启用 Exchange 服务器集成后，**设备**窗口上的 **Exchange ActiveSync 设备**选项卡将显示通过 ActiveSync 服务连接到 Exchange 服务器的移动设备列表。

在 **Exchange ActiveSync 设备**选项卡中，可以执行以下操作：

- 邀请移动设备
- 允许或阻止访问 Exchange 服务器
- 按需远程擦除
- 取消远程擦除命令
- 从列表中删除移动设备

邀请 Exchange ActiveSync 移动设备

在邀请 Exchange ActiveSync 移动设备之前，确保已经在管理服务器上配置通知/报告设置。参阅*《安装和部署指南》*中的*配置通知/报告设置*主题。

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. 单击 **Exchange ActiveSync 设备**选项卡。
4. 选择要邀请访问 Exchange ActiveSync 的移动设备。
5. 单击**邀请**，然后单击确认窗口中的**确定**。

   移动安全会向受邀移动设备的用户发送邀请短信和电子邮件消息。移动设备注册到移动安全服务器后，**托管的设备**列会显示移动安全客户端的状态。

允许或阻止访问 Exchange 服务器

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. 单击 **Exchange ActiveSync 设备**选项卡。
4. 选择要允许或阻止访问 Exchange 服务器的移动设备。
5. 单击**允许访问**或**阻止访问**，然后单击确认对话框中的**确定**。

   移动设备与 Exchange 服务器同步后，**Exchange 访问状态**列中的移动设备状态会显示新的状态。

擦除远程 ActiveSync 移动设备

可以远程将 ActiveSync 移动设备重置为出厂设置，并清除移动设备的内存/SD 卡。此功能有助于确保在移动设备丢失、被盗或误放时的数据安全。

警告!

请谨慎使用此功能，因为此操作无法恢复。所有数据都将丢失且无法恢复。

有关擦除不使用 ActiveSync 的移动设备的说明，请参阅擦除远程移动设备 第 3-12 页。

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. 单击 **Exchange ActiveSync 设备**选项卡。
4. 选择要擦除的移动设备。
5. 单击**远程擦除**。

   弹出**远程擦除设备**窗口。
6. 选择设备，然后单击**远程擦除设备**。

删除 ActiveSync 移动设备

已经从移动安全服务器远程擦除的移动设备将无法再访问 Exchange 服务器。可以将此类移动设备信息从**设备**窗口中的 **Exchange ActiveSync 设备**选项卡中删除。

注意

可以只删除从移动安全服务器中远程擦除的移动设备。

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. 单击 **Exchange ActiveSync 设备**选项卡。
4. 选择要从列表中删除的移动设备。
5. 单击**删除**，然后单击确认窗口中的**确定**。

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 4 章

利用策略保护设备

本章说明了如何配置安全策略并将其应用到移动安全组中的移动设备。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：

关于安全策略

您可以在管理服务器上为移动安全组配置安全策略。这些策略适用于组中的所有移动设备。可通过选择**移动设备**组（根组）将安全策略应用到所有移动安全组。下表列出了移动安全中可用的安全策略。

表 4-1. 移动安全中的安全策略

策略组	策略	参考
常规	通用策略	请参阅通用策略 第 4-7 页。
预置	Wi-Fi 策略	请参阅 Wi-Fi 策略 第 4-8 页。
	Exchange ActiveSync 策略	请参阅 Exchange ActiveSync 策略 第 4-8 页。
	VPN 策略	请参阅 VPN 策略 第 4-8 页。
	全局 HTTP 代理策略	请参阅全局 HTTP 代理策略 第 4-9 页。
	证书策略	请参阅证书策略 第 4-9 页。
	单点登录策略	请参阅单点登录策略 第 4-9 页。
设备安全	恶意软件防护策略	请参阅恶意软件防护策略 第 4-10 页。
	垃圾信息阻止策略	请参阅垃圾信息阻止策略 第 4-11 页。
	电话过滤策略	请参阅电话过滤策略 第 4-14 页。
	防火墙策略	请参阅防火墙策略 第 4-15 页。
	Web 威胁防护策略	请参阅 Web 威胁防护策略 第 4-17 页。
设备	加密和密码策略	请参阅加密和密码策略 第 4-17 页。
	功能锁定策略	请参阅功能锁定策略 第 4-21 页。
	合规策略	请参阅合规策略 第 4-21 页。

策略组	策略	参考
应用程序管理	应用程序监控及控制策略	请参阅应用程序监控及控制策略 第 4-22 页。
	批量购买计划策略	请参阅批量购买计划策略 第 4-24 页。

管理策略

移动安全让您能够使用缺省安全策略模板快速创建策略。

使用**策略**窗口创建、编辑、复制或删除移动设备的安全策略。

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**。

   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 4-5 页。

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**。

   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**。

   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**。

   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 4-5 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**。

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

移动安全中的安全策略

本节介绍移动安全中可用的安全策略。

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**。

还可以在**通用策略**中为 BlackBerry 移动设备分配策略。

- **用户特权**：您可以启用或禁用允许用户卸载移动安全代理的功能。此外，您可以选择是否允许用户配置移动安全代理设置。

  以下为与卸载保护相关的功能列表：

  - 从管理控制台上开启或关闭卸载保护
  - 密码的长度必须至少为六 (6) 个字符，最多为十二 (12) 个字符；密码可以包含数字、字符或符号。
  - 可以从管理控制台为每个组设置密码。

  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，**垃圾信息阻止策略**、**电话过滤策略**和 **Web 威胁防护策略**的过滤列表不受影响。有关详细信息，请参阅垃圾短信阻止策略 第 4-12 页、垃圾服务信息阻止策略 第 4-13 页和Web 威胁防护策略 第 4-17 页。

- **更新设置**：在有新组件可供更新时，可选择让移动安全服务器来通知移动安全代理。或者可选择自动检查选项，让移动安全代理在移动安全服务器上定期检查所有组件或配置更新。

  启用无线连接通知选项后，在移动安全客户端通过无线连接（例如，3G 或 GPRS）连接到通信服务器前，会在移动设备上显示一个提示窗口。用户可选择接受或拒绝连接请求。

图 4-1. 通用策略 — 更新设置部分

- **日志设置**：移动安全代理检测到安全风险（例如，受感染文件或防火墙违例）时，会在移动设备上生成日志。如果加密模块被激活，则还生成加密

日志。可设置移动设备，将这些日志发送到移动安全服务器。如果要分析受感染文件的数量或可能的网络攻击的精确位置并采取适当的处理措施来防止威胁传播，请执行该操作。

- **通知/报告设置**：当移动安全客户端试图建立到通信服务器的连接时，选择是否在移动设备上显示一个提示窗口。
- **Blackberry 设置**：让您能够为 Blackberry 移动设备配置通用策略设置。

注意

在配置策略设置之前，必须在通信服务器设置中配置 Blackberry 设置。参阅*《安装和部署指南》*中的*配置 BlackBerry 通信服务器设置*。

Wi-Fi 策略

Wi-Fi 策略让您能够将组织的 Wi-Fi 网络信息传送到 Android 和 iOS 移动设备；包括网络名称、安全类型和密码。

要配置 Wi-Fi 策略设置，请单击**策略**，然后单击策略名称，然后单击 **Wi-Fi 策略**。

Exchange ActiveSync 策略

Exchange ActiveSync 策略让您能够为组织创建 Exchange ActiveSync 策略并将其传送到 iOS 移动设备。

要配置 Exchange ActiveSync 策略设置，请单击**策略**，然后单击策略名称，然后单击 **Exchange ActiveSync 策略**。

VPN 策略

VPN 策略设置让您能够为组织创建 VPN 策略并将其传送到 iOS 移动设备。

要配置 VPN 策略设置，请单击**策略**，然后单击策略名称，然后单击 **VPN 策略**。

全局 HTTP 代理策略

全局 HTTP 代理策略让您能够将组织的代理信息传送到移动设备。此策略仅适用于处于监管模式的 iOS 移动设备。

要配置全局 HTTP 代理策略设置，请单击**策略**，然后单击策略名称，然后单击**全局 HTTP 代理策略**。

证书策略

证书策略让您能够导入需要在 iOS 移动设备上部署的证书。

要配置证书策略设置，请单击**策略**，然后单击策略名称，然后单击**证书策略**。

单点登录策略

通过单点登录 (SSO) 策略，用户可以在不同应用程序中使用相同的凭证，包括移动安全和应用程序商店中的应用程序。每个配置有 SSO 证书的新应用程序都会验证用户对企业资源的权限，无需用户重新输入密码即允许用户登录。

单点登录策略包括以下信息：

- **名称**：Kerberos 主体名称。
- **领域**：Kerberos 领域名称。

  Kerberos 领域名称应采用大写形式正确书写。
- **URL 前缀**（可选）：必须匹配才能使用帐户通过 HTTP 进行 Kerberos 身份验证的 URL 列表。如果此字段为空，则帐户可以匹配所有 http 和 https URL。URL 匹配模式必须以 http 或 https 开头。

  此列表中的每个条目都必须包含 URL 前缀。只有开头为帐户中的一个字符串的 URL 才允许访问 Kerberos 票证。URL 匹配模式必须包括方案。例

如，http://www.example.com/。如果匹配模式不是以 / 结尾，将自动向 URL 添加一个 /。

- **应用程序标识符**（可选）：允许使用帐户的应用程序标识符的列表。如果此字段为空，此帐户将匹配所有应用程序标识符。

  应用程序标识符数组必须包含匹配应用程序捆绑 ID 的字符串。这些字符串可以精确匹配（如 com.mycompany.myapp），也可以使用 * 通配符指定捆绑 ID 上的前缀匹配。该通配符必须显示在句点字符 (.) 之后，并且可以只显示在字符串末尾（如 com.mycompany.*）。使用通配符后，捆绑 ID 的开头为该前缀的任何应用程序都有权访问该帐户。

要为 iOS 设置配置单点登录策略，请单击**策略**，然后单击策略名称，最后单击**单点登录策略**。

恶意软件防护策略

您可以配置威胁防护策略，包括：扫描类型（实时扫描和卡扫描）、针对恶意软件的处理措施、要扫描的压缩层数和文件类型。

要配置恶意软件防护策略设置，请单击**策略**，然后单击策略名称，然后单击**恶意软件防护策略**。

- **扫描类型**：移动安全提供了多种扫描类型，以保护移动设备免受恶意软件侵害。
  - **实时扫描**：移动安全代理可对移动设备上的文件进行实时扫描。如果移动安全代理未检测到安全风险，则用户可继续打开或保存文件。如果移动安全代理检测到安全风险，则显示扫描结果（显示文件和特定安全风险的名称）。移动安全将在移动设备上生成一个包含扫描结果的日志。扫描日志发送并存储在移动安全数据库中。
  - **在插入 SD 卡后扫描**：如果在**恶意软件防护策略**窗口中选择此选项，则移动安全会在将内存卡插入到移动设备时对内存卡上的数据进行扫描。这样可避免受感染文件在内存卡上传播。
  - **病毒码更新后扫描**：如果在**恶意软件防护策略**窗口中选择此选项，则在 Android 移动设备上成功进行病毒码更新后，移动安全会运行安全威胁自动扫描。

- **扫描选项**
  - **对恶意软件采取的措施**：在移动设备上检测到恶意软件时，移动安全会删除或隔离受感染文件。如果该文件正在使用中，操作系统可能拒绝访问它。
    - 隔离 — 重命名受感染文件并将其移至移动设备的隔离目录，即 `\TmQuarantine`（对于 Windows Mobile）或 `{Disk Label}\TmQuarantine`（对于 Symbian OS）。
    - 删除 — 删除受感染文件。

    连接后，移动安全代理会将恶意软件日志发送到移动安全服务器。

    注意

    扫描处理措施仅适用于实时扫描。

  - **要扫描的压缩层数**：对于 ZIP 或 CAB 文件，可指定要扫描的压缩层数。如果 ZIP/CAB 文件中的压缩层数超过这个数字，移动安全将不扫描该文件。在没有指定适当的压缩层数前，移动安全将不会采取进一步处理措施。

    可选择让移动安全扫描移动设备上的可执行文件、ZIP/CAB 文件或所有文件。

  - **扫描位置**：对于 Android 移动设备，选择是否扫描移动设备的内存和/或插入的 SD 卡。对于 Symbian，移动安全扫描移动设备的内存和插入的 SD 卡。
  - **文件类型**：选择要在移动设备上扫描的文件类型。

垃圾信息阻止策略

移动安全中的垃圾信息阻止策略提供了垃圾服务信息防护和短信防护。

要配置垃圾信息阻止策略设置，请单击**策略**，然后单击策略名称，然后单击**垃圾信息阻止策略**。

垃圾短信阻止策略

此功能使您能在服务器端控制垃圾短信阻止策略。当配置垃圾短信阻止策略时，以下功能可用：

- 启用或禁用移动设备的垃圾短信阻止策略
- 配置移动设备，以使用移动设备的阻止列表、允许列表或禁用反垃圾短信功能。
- 从管理控制台配置允许列表
- 从管理控制台配置阻止列表

有关允许或阻止的过滤列表配置详细信息，请参阅下表。

表 4-2. 垃圾短信阻止策略的过滤列表配置

中央控制	用户控制	描述
已禁用	已启用	用户可以编辑移动设备客户端中的允许/阻止列表。 移动安全根据以下优先级允许或阻止信息： 1. 移动安全客户端中的允许列表 2. 移动安全客户端中的阻止列表
已启用	已禁用	用户只能编辑移动安全客户端中的允许/阻止列表。 移动安全根据以下优先级允许或阻止信息： 1. 服务器上的允许列表或阻止列表 2. 移动安全客户端中的允许列表 3. 移动安全客户端中的阻止列表

中央控制	用户控制	描述
已启用	已启用	用户可以查看或编辑管理员定义的允许/阻止列表，并且还可以使用移动安全客户端中的允许/阻止列表。 安全策略与移动安全客户端同步时，不会同步过滤列表，且会根据策略更新所有其他设置。 移动安全根据以下优先级允许或阻止信息： 1. 移动安全客户端中的允许列表 2. 移动安全客户端中的阻止列表 3. 服务器上的允许列表或阻止列表

注意

短信允许列表和阻止列表必须使用以下格式：[名称 1:]号码 1;[名称 2:]号码 2;.....。

名称长度不得超过 30 个字符，而且电话号码应在 4 至 20 个字符之间，并可以包括以下字符：0-9、+、-、#、(、) 和空格。最大条目数不应超过 200。

垃圾服务信息阻止策略

此功能使您能在服务器端控制服务信息防护。如果启用，您可以选择是否使用服务信息允许列表。以下功能为配置服务信息防护策略时可用的功能列表：

- 启用或禁用移动设备的服务信息防护
- 配置移动设备，以使用允许列表或禁用移动设备上的服务信息防护
- 从管理控制台配置允许列表
- 如果管理员已经启用了服务器端控制，用户将不能更改管理员定义的服务信息防护类型
- 如果管理员已经禁用了服务器端控制，并且允许用户配置移动设备上的移动安全设置，用户将不能查看或编辑管理员配置的服务信息防护列表，且用户可以编辑移动设备端上的个人服务信息防护列表

服务器策略传送到移动设备后，个人设置将被清除。

注意

服务信息允许列表必须使用以下格式：[名称 1:]号码 1;[名称 2:]号码 2;.....。

名称长度不得超过 30 个字符，而且电话号码应在 4 至 20 个字符之间，并可以包括以下字符：0-9、+、-、#、(、) 和空格。最大条目数不应超过 200。

注意

垃圾信息阻止策略应用于移动安全客户端后，用户的垃圾信息个人设置将被清除。

电话过滤策略

此功能使您能在服务器端控制电话过滤策略。要配置电话过滤策略设置，请单击**策略**，然后单击策略名称，然后单击**过滤策略**。

当配置电话过滤策略时，以下功能可用：

- 启用或禁用移动设备的电话过滤
- 配置移动设备，以使用阻止列表或允许列表
- 从管理控制台配置允许列表
- 从管理控制台配置阻止列表

有关允许或阻止的过滤列表配置详细信息，请参阅下表。

表 4-3. 电话过滤策略的过滤列表配置

中央控制	用户控制	描述
已禁用	已启用	用户可以编辑移动设备客户端中的允许/阻止列表。 移动安全根据以下优先级允许或阻止 URL： 1. 移动安全客户端中的允许列表 2. 移动安全客户端中的阻止列表

中央控制	用户控制	描述
已启用	已禁用	用户只能编辑移动安全客户端中的允许/阻止列表。 移动安全根据以下优先级允许或阻止来电： 1. 服务器上的阻止列表 2. 移动安全客户端中的允许列表 3. 移动安全客户端中的阻止列表 还可以为 Android 移动设备中的去电配置服务器端控制。
已启用	已启用	用户可以查看或编辑管理员定义的允许/阻止列表，并且还可以使用移动安全客户端中的允许/阻止列表。 安全策略与移动安全客户端同步时，不会同步过滤列表，且会根据策略更新所有其他设置。 移动安全根据以下优先级允许或阻止来电： 1. 移动安全客户端中的允许列表 2. 移动安全客户端中的阻止列表 3. 服务器上的阻止列表 还可以为 Android 移动设备中的去电配置服务器端控制。

注意

电话过滤允许和阻止列表必须使用以下格式：[名称 1:]号码 1;[名称 2:]号码 2;.....。

名称长度不得超过 30 个字符，而且电话号码应在 4 至 20 个字符之间，并可以包括以下字符：0-9、+、-、#、(、) 和空格。最大条目数不应超过 200。

防火墙策略

移动安全防火墙使用状态检测、高性能网络通信控制和入侵检测系统 (IDS) 保护网络中的移动设备。可创建规则，使其按 IP 地址、端口号或协议对连接进行过滤，然后将规则应用到特定移动安全组中的移动设备。

注意

趋势科技建议在部署和启用移动安全防火墙之前在移动设备上卸载基于其他软件的防火墙应用程序。在同一台计算机上的多个供应商防火墙安装可产生异常结果。

要配置防火墙策略设置，请单击**策略**，然后单击策略名称，然后单击**防火墙策略**。

防火墙策略包括以下内容：

- **防火墙策略**：启用/禁用移动安全防火墙和 IDS。此外，还包括阻止或允许移动设备上所有入站和/或出站通信的通用策略
  - **启用入侵检测系统 (IDS)**：移动安全防火墙集成了入侵检测系统 (IDS)，其有助于防止 SYN Flood 攻击（一种拒绝服务攻击），在这种攻击中，程序会向一台计算机发送多个 TCP 同步 (SYN) 数据包，导致移动设备不断地发送同步确认 (SYN/ACK) 响应。这会耗尽系统资源，并可能使移动设备无法处理其他请求。
  - **安全级别**：移动安全防火墙附带三个预定义安全级别，允许您快速对防火墙策略进行配置。这些安全级别可根据通信方向限制网络通信。
    - **低** - 允许所有入站和出站通信。
    - **标准** - 允许所有出站通信，但阻止所有入站通信。
    - **高** - 阻止所有入站和出站通信。
- **例外**：例外规则包括更详细的设置，这些设置基于移动设备端口号和 IP 地址来允许或阻止不同类型的通信。列表中的规则将覆盖**安全级别**策略。

  例外规则设置包括下列设置：
  - **处理措施** - 阻止或允许/满足规则条件的日志通信
  - **方向** - 移动设备上的入站或出站网络通信
  - **协议** - 通信类型：TCP、UDP、ICMP
  - **端口** - 在其上执行处理措施的移动设备端口

- **IP 地址** - 通信条件应用到的网络设备的 IP 地址

Web 威胁防护策略

可管理移动安全服务器中的 Web 威胁防护策略并在 Android 和 iOS 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。

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**。

加密和密码策略

加密和密码模块提供了移动设备上的密码鉴定和数据加密。这些功能可阻止对移动设备上数据的未授权访问。

要配置加密和密码策略设置，请单击**策略**，然后单击策略名称，然后单击左侧菜单中的**加密和密码策略**。

密码安全设置

安装移动安全代理后，所有移动设备都与用户相关联。用户必须键入正确的开机密码才能登录到移动设备。当用户忘记了开机密码时，可以键入管理员密码以解锁移动设备。

下表对可配置的开机密码策略进行了描述：

选项	描述
密码类型	密码必须只能包含数字或字母数字字符。
最小密码长度	密码长度必须超过指定的字符数量。
密码复杂性	对于字母数字密码，用户必须配置包含大写、小写、特殊字符或数字的密码，以使得密码更难猜测。

选项	描述
初始移动安全代理密码	允许用户在安装移动安全代理和加密模块后登录到 Windows Mobile 设备的密码。缺省密码为 123456。
管理员密码	由管理员用于对移动设备解锁的密码。
有效期	登录密码的有效天数。密码过期后，用户必须配置用于登录的新密码。
闲置超时	在移动设备自动进入安全模式并显示登录窗口前没有用户活动的分钟数。
限制登录尝试次数	限制登录尝试次数，以阻止暴力密码攻击。达到限制时可能的处理措施： • **软重置** — 重新启动移动设备。 • **仅允许管理员访问** — 要求使用管理员密码登录。 • **硬重置** — 将移动设备重新设置回出厂缺省策略。 • **清除所有数据** — 将移动设备重新设置回出厂缺省策略，并删除移动设备和插入的内存卡上的所有数据。 **警告!** 执行清除所有数据操作后，用户需要重新格式化内存卡，才能将其再次用于存储数据。
更改初始开机密码	要求用户在首次登录后更改初始密码。
忘记密码问题	如果用户忘记了开机密码，则可使用此项功能对移动设备进行解锁并通过回答所选问题配置新的密码。

注意

为初始或管理员密码指定字符时，牢记移动设备使用的输入方法。否则，在加密启用后设备用户可能不能解锁设备。

加密设置

移动安全代理提供了实时数据加密功能，以确保移动设备上数据的安全。有两种加密算法：高级加密标准（AES，具有 128 位、192 位或 256 位密钥）和 XTS 高级加密标准 (AES)。

注意

移动安全只能管理 Windows Mobile 设备上的数据安全策略。

可在 Windows Mobile 设备上选择要加密的特定文件类型、要使用的加密算法、允许访问加密数据的可信应用程序，或在移动设备插入的内存卡上应用数据加密。

移动安全客户端不对动态链接库 (*.DLL) 文件进行加密。移动安全代理只对用户已修改的文件进行加密。读取文件并在关闭前不执行任何修改不会对正在加密的文件产生影响。

启用加密模块后，某些文件类型和 PIM 信息将被加密。这些文件类型和 PIM 信息列举下表中。

加密信息	类型
文件类型	• doc • txt • ppt • pxl • pdf • xls • psw • docx

加密信息	类型
PIM 信息	• 联系人 • 邮件 • 任务 • 日历 • 短信 • MMS

加密模块仅允许可信应用程序访问加密的数据。因此，必须将这些应用程序添加至可信应用程序列表。要将软件添加至可信应用程序列表中，可将完整的软件路径添加至相应的以下列表中："**允许更多应用程序访问加密数据**。

注意

对于高级配置，可设置移动安全，使其对其他文件类型进行加密。要启用自定义文件类型的加密，请在文件 `TmOMSM.ini`（位于 `\Trend Micro\Mobile Security`）中将参数 **Enable_Custom_Extension** 设置为 `1`。在文件 `TmOMSM.ini` 中将参数设置为 **1** 时，会在**数据安全策略**窗口上显示**加密其他文件类型**字段。在此字段中指定文件类型。

要禁用此功能，将 **Enable_Custom_Extension** 参数设置为 `0`。在文件 `TmOMSM.ini` 中将参数设置为 **0** 时，**数据安全策略**窗口中的**加密其他文件类型**字段将不可用。

在 `TmOMSM.ini` 文件中做出更改后，重启**移动安全管理模块服务**服务使更改生效。

警告!

趋势科技建议不要定制加密文件类型。用户无法对某些文件类型（例如，`.exe`、`.cert`、`.dll` 等）进行加密。如果设置移动安全使其对不应加密的文件类型进行加密，则系统可能发生异常错误。

功能锁定策略

此功能使您可以限制（禁用）或允许（启用）某些移动设备功能/组件的使用。例如，您可以在特定的组中禁用所有移动设备的摄像头。

要配置功能锁定策略设置，请单击**策略**，然后单击策略名称，然后单击左侧菜单中的**功能锁定策略**。

参阅支持的移动设备操作系统功能 第 1-12 页，获取支持的功能/组件的列表。

注意

功能锁定策略不适用于 Symbian 移动设备。

警告!

禁用 WLAN/WIFI 和/或 Microsoft ActiveSync 时应谨慎。如果两者都不可用，移动设备可能无法与服务器进行通信。

对于 Android 移动设备，您也可以增加访问点，以控制这些访问点范围内的设备组件的可用性。

注意

Windows 移动设备可能需要重新启动来使更改生效。

合规策略

合规策略允许为移动设备设置合规条件。如果有任何移动设备不符合合规条件，移动安全会在服务器 UI 上显示其不合规状态。移动安全还向不合规的 iOS 移动设备发送电子邮件，而在不合规的 Android 移动设备上则显示通知。合规检查列表包括：

- **Root 权限/越狱版** — 检查移动设备是否有 Root 权限/越狱版。
- **未加密** — 检查移动设备上是否启用了加密。
- **操作系统版本检查** — 检查操作系统版本是否与定义的条件相符。

要配置合规策略设置，请单击**策略**，然后单击策略名称，然后单击**合规策略**。

应用程序监控及控制策略

利用应用程序监控及控制策略，可以在服务器端控制移动设备上安装的应用程序，并将必需的应用程序推送至移动设备。

要配置应用程序监控及控制策略设置，请单击**策略**，然后单击策略名称，最后单击**应用程序监控及控制策略**。

- **必需应用程序** — 如果使用此选项，则会将您添加到列表中的所有应用程序推送到移动设备。您还可以将 VPN 链接到应用程序，以便应用程序始终使用此 VPN 连接网络。
- **允许应用程序** — 通过使用允许列表或阻止列表，控制移动设备上安装的应用程序。

  对于 iOS 移动设备，移动安全会向管理员和用户发送有关所有不符合策略的应用程序的通知。

  对于 Android 移动设备，移动安全会阻止不符合策略的应用程序并允许所有其他应用程序。

  - **启用系统应用程序阻止**（仅限 Android）：

    如果选中，移动安全会阻止 Android 移动设备上的所有系统应用程序。

  - **启用应用程序类别**：选择要在移动设备上启用或禁用的应用程序类别。还可以通过将属于这些类别的应用程序添加到允许或阻止列表来创建例外。例如，如果已禁用游戏类别类型，则移动安全将阻止属于此类别的所有应用程序，除非任何此类应用程序出现在允许列表中。

    移动安全根据以下优先级允许或阻止应用程序：

    1. **允许列表** — 移动安全允许处于允许列表中的应用程序，即使这些应用程序属于已禁用的类别。
    2. **阻止列表** — 移动安全阻止处于阻止列表中的应用程序，即使这些应用程序属于已启用的类别。

3. **应用程序权限** — 移动安全根据您选择的应用程序所属类别的权限状态允许或阻止应用程序。

- **启用应用程序权限**（仅限 Android）：选择要在 Android 移动设备上启用或禁用的应用程序服务。还可以通过将使用这些服务的应用程序添加到允许或阻止列表来创建例外。例如，如果已禁用**读取数据**服务类型，则移动安全将阻止使用此服务的所有应用程序，除非任何此类应用程序出现在允许列表中。

  移动安全根据以下优先级允许或阻止应用程序：

  1. **允许列表** — 移动安全允许处于允许列表中的应用程序，即使这些应用程序使用已禁用的服务。
  2. **阻止列表** — 移动安全阻止处于阻止列表中的应用程序，即使这些应用程序使用已启用的服务。
  3. **应用程序权限** — 移动安全根据您选择的应用程序所使用服务的权限状态允许或阻止应用程序。

- **仅允许以下应用程序**：将您允许用户在其移动设备上使用的应用程序添加到允许列表中。如果启用：
  - 如果移动安全检测到不在允许列表中的应用程序，它会在 Android 移动设备上显示弹出式警告消息。
  - 在 iOS 移动设备上，如果移动安全检测到任何不在允许列表中的应用程序，移动安全会向用户发送电子邮件通知。

- **仅阻止以下应用程序**：将您不希望用户在其移动设备上使用的应用程序添加到阻止列表中。如果启用：
  - 如果移动安全检测到在阻止列表中的应用程序，它会在 Android 移动设备上显示弹出式警告消息。
  - 在 iOS 移动设备上，如果移动安全检测到任何在阻止列表中的应用程序，移动安全会向用户发送电子邮件通知。

- **锁定到应用程序 (仅限监管模式)** — 将 iOS 移动设备限制于指定的应用程序。

移动安全检查限制的应用程序并向用户发送电子邮件警报：

- 自动根据**管理** > **通信服务器设置** > **常规设置（选项卡）**中的**信息收集频率**设置进行，或者
- 在更新**管理** > **通信服务器设置** > **常规设置（选项卡）**中的**信息收集频率**设置时进行。

批量购买计划策略

此策略让管理员能够将通过苹果批量购买计划购买的 iOS 应用程序导入移动安全管理 Web 控制台。移动安全会将批量购买计划列表中的所有应用程序推送给组中的移动设备。

配置批量购买计划策略：

1. 将应用程序添加到企业应用程序商店。有关步骤，请参阅添加应用程序 第 5-2 页。
2. 单击**策略**，然后单击策略名称，然后单击**批量购买计划策略**。
3. 单击**导入**，然后从企业应用程序商店选择要导入的应用程序。
4. 单击**保存**将所有应用程序推送到 iOS 移动设备。

第 5 章

管理企业应用程序商店

本章展示了如何管理 iOS 和 Android 移动设备企业应用程序商店。

本章包括以下几节内容：

关于企业应用程序商店

企业应用程序商店让您能够创建 Web 剪辑和应用程序列表，以便用户在其 Android 或 iOS 移动设备上下载和安装列表中的项目。

还可以将通过苹果批量购买计划购买的 iOS 应用程序上传到移动安全管理 Web 控制台上的企业应用程序商店。

管理企业应用程序

添加应用程序

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**应用程序商店**。

   显示**企业应用程序商店**窗口。
3. 单击 **iOS 应用程序**选项卡或 **Android 应用程序**选项卡。
4. 单击**添加**。

   显示**添加应用程序**窗口。
5. 可使用以下任一选项向列表中添加新的应用程序：
   - **从本地计算机添加** — 选择适用于 Android 和 iOS 移动设备的安装文件。
   - **添加 Web 剪辑** — 键入应用程序 URL，这时用户移动设备的主屏幕上将显示该应用程序的图标，链接将在移动设备的缺省 Web 浏览器中打开。

- (Android) **从外部应用程序商店添加** — 键入外部应用程序商店中相应应用程序的链接。应用程序图标将出现在用户移动设备的主屏幕上，链接将在移动设备的缺省 Web 浏览器中打开。
- (iOS) **请输入搜索关键词** — 键入要搜索的 VPP 应用程序的名称，并选择要在其苹果应用程序商店中搜索应用程序的国家/地区，然后从搜索结果中选择要添加的应用程序。添加后，VPP 应用程序仅在移动安全管理 Web 控制台中的**应用程序商店**中可用。要将应用程序推送到移动设备，需要将要应用程序添加到**批量购买计划策略**。有关步骤，请参阅批量购买计划策略 第 4-24 页。

6. 单击**继续**。

   显示**编辑应用程序**窗口。

7. 配置以下内容：
   - **应用程序名称**：为应用程序键入名称。
   - **应用程序图标**：如果未显示应用程序图标，单击上传应用程序图标以选择并上传应用程序图标。
   - **应用程序标识**：如果未显示应用程序标识，键入应用程序标识。
   - **VPP 代码文件**：对于 iOS VPP 应用程序，上传从苹果收到的批量购买代码文件。
   - **类别**：为应用程序选择类别。

     注意

     必须从下拉列表中选择一个类别。要添加或删除类别，单击**类别**按钮。

   - **描述**：为应用程序键入描述。
   - **发布**：选择以下选项之一：
     - **不发布** — 上传服务器中的应用程序，但是对移动设备保持隐藏。
     - **作为生产版本发布** — 上传服务器中的应用程序，并发布以供移动设备下载。

- **作为 Beta 版本发布** — 上传服务器中的应用程序，并发布为 Beta 版本以供移动设备下载。

- **屏幕截图：**选择并上传应用程序屏幕截图。

8. 单击**继续**。

   应用程序将出现在应用程序列表中。

编辑应用程序信息

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**应用程序商店**。

   显示**企业应用程序商店**窗口。
3. 单击 **iOS 应用程序**选项卡或 **Android 应用程序**选项卡。
4. 单击要编辑其信息的应用程序的名称。

   显示**编辑应用程序**窗口。
5. 在窗口中修改详细信息。
6. 单击**继续**。

从应用程序商店中删除应用程序

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**应用程序商店**。

   显示**企业应用程序商店**窗口。

3. 单击 **iOS 应用程序**选项卡或 **Android 应用程序**选项卡。
4. 选择要删除的应用程序。
5. 单击**删除**，然后单击确认对话框中的**确定**。

管理应用程序类别

添加应用程序类别

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**应用程序商店**。

   显示**企业应用程序商店**窗口。
3. 单击 **iOS 应用程序**选项卡或 **Android 应用程序**选项卡。
4. 单击**管理类别**。
5. 单击**添加**。

   显示**添加类别**窗口。
6. 键入类别名称和描述，然后单击**保存**。

编辑应用程序类别

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**应用程序商店**。

显示**企业应用程序商店**窗口。

3. 单击 **iOS 应用程序**选项卡或 **Android 应用程序**选项卡。
4. 单击**管理类别**。
5. 单击要编辑的类别名称。

   显示**编辑类别**窗口。
6. 修改类别详细信息，然后单击**保存**。

删除应用程序类别

过程

1. 登录移动安全管理 Web 控制台。
2. 单击菜单栏上的**应用程序商店**。

   显示**企业应用程序商店**窗口。
3. 单击 **iOS 应用程序**选项卡或 **Android 应用程序**选项卡。
4. 单击**管理类别**。
5. 选择要删除的类别，单击**删除**，然后单击确认对话框中的**确定**。

第 6 章

更新组件

本章介绍了如何配置预设和手动服务器更新，然后为 ActiveUpdate 指定更新源。同时还说明了如何在特定的移动安全代理上执行组件更新。

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 — 移动安全服务器的程序安装包。
- 恶意软件码 - 包含成千上万恶意软件特征的文件，并决定移动安全检测这些危害文件的能力。趋势科技定期更新病毒码文件，以确保对最新威胁的防护。
- 恶意软件扫描引擎 - 执行实际扫描和清除功能的组件。扫描引擎采用病毒码文件匹配技术，使用病毒码文件中的特征来检测恶意软件。趋势科技会间或发布新的扫描引擎来引入新技术。
- 移动安全代理安装程序 - 移动安全代理的程序安装包。
- 移动安全代理程序补丁 - 程序补丁文件，包括对安装在移动设备上的移动安全代理程序的最新更新。

更新移动安全组件

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

手动更新

可以在**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 6-5 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。

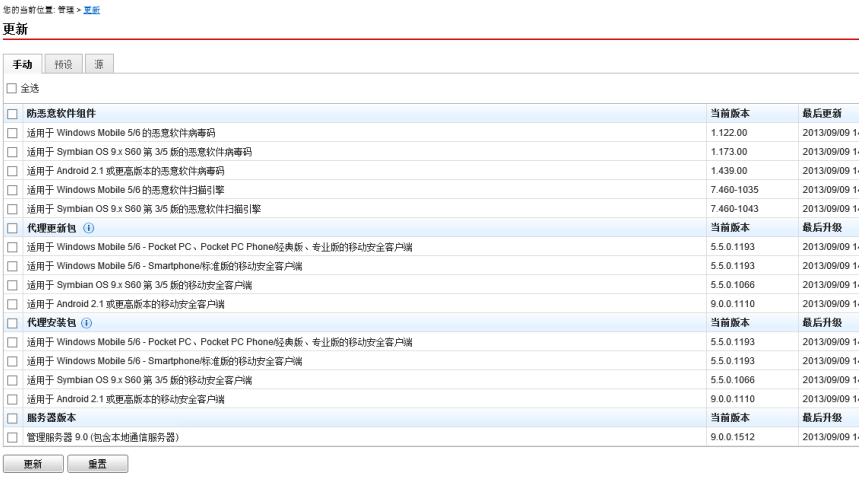

图 6-1. 更新窗口上的手动选项卡

4. 选中要更新的组件的复选框。选择**防恶意软件组件**、**程序**和/或**程序安装软件包**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 6-2 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 6-5 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。

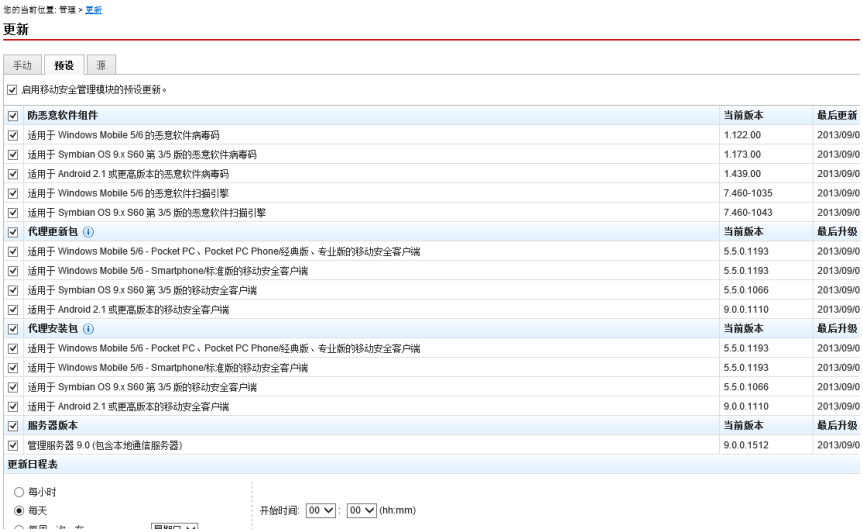

图 6-2. 更新窗口上的预设选项卡

4. 选中要更新的组件的复选框。选中**防恶意软件组件**、**代理更新包**、**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**。
   - 如果预设为每周更新一次，请指定一周中的某一天（例如，星期日、星期一等）。
   - 如果预设为每月一次，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 x 小时内执行。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 6-2 页；有关预设更新的详细信息，请参阅预设更新 第 6-3 页。
3. 单击**源**选项卡。

图 6-3. 更新窗口上的源选项卡

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，但移动安全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 7 章

查看和维护日志

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

本章包括以下几节内容：

关于移动安全代理日志

移动安全客户端生成恶意软件防护日志、Web 威胁防护日志、防火墙日志、加密日志、策略违例日志或事件日志时，会将日志发送到移动安全服务器。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。

注意

可查看移动设备上的反垃圾短信日志、服务信息防护日志和电话过滤日志。

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服务器上所有移动安全客户端日志。在移动安全服务器上，可查看以下移动安全客户端日志：

- 恶意软件防护日志 — 在移动设备上检测到恶意软件时，移动安全客户端会生成日志。通过这些日志，可跟踪检测到的恶意软件并对其采取相应的处理措施。
- 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 页面时会生成日志，并将日志上传至服务器。
- 防火墙日志 — 当与防火墙规则匹配或防火墙功能（例如，预定义的安全级别或 IDS）阻止连接时生成这些日志。
- 加密日志 — 包括诸如成功的用户登录尝试次数和达到登录尝试限制后采取的处理措施等信息。
- 事件日志 — 服务器和移动安全客户端采取某些处理措施时，会生成这些日志。
- 策略违例日志 — 这些日志包含有关移动安全客户端的策略合规状态的信息。

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。

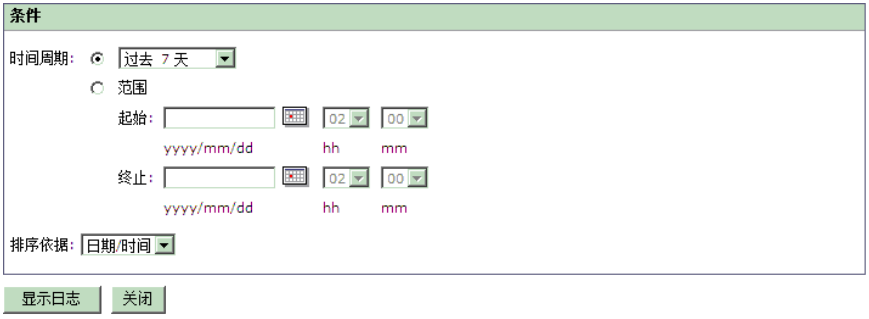

图 7-1. 日志查询窗口

3. 为要查看的日志指定查询条件。参数包括：
   - **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** — 键入要搜索由其生成的日志的管理员名称。
   - **时间周期** — 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：恶意软件、防火墙、加密、事件或策略违例。
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 8 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：

关于通知消息和报告

您可以配置移动安全，使其通过电子邮件或短信方式向管理员和/或用户发送通知。

- **管理员通知/报告** — 如果出现任何系统异常，将向管理员发送电子邮件通知和报告。
- **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/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**。

相关信息

↳ 配置短信发送器列表

配置短信发送器设置

管理服务器控制和监控连接到服务器的短信发送器。短信发送器向移动设备发送短信，以通知移动设备执行移动安全客户端的安装、注册、组件更新、安全策略设置以及远程擦除/锁定/定位。

使用短信发送器设置：

- 配置短信发送器的电话号码
- 查看短信发送器的连接状态
- 设置移动安全代理安装消息
- 配置短信发送器的断开通知

短信发送器列表

在管理服务器能指示短信发送器向移动设备发送信息之前，您需要配置短信发送器设备的电话号码。

注意

如果没有在短信发送器列表中配置短信发送器的电话号码，则管理服务器会阻止短信发送器向移动设备发送消息。

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/报告设置**窗口。在**短信发送器设置**部分，显示短信发送器的电话号码列表和连接状态。如果短信发送器成功连接到管理服务器，则**状态**文本框显示为：**已连接**。

注意

在三 (3) 次尝试发送短信失败后，移动设备将会显示断开。

配置短信发送器列表

指定短信发送器的电话号码，以开启移动安全服务器对短信发送器进行管理。短信发送器通过发送短信来通知移动设备执行以下操作：

- 下载和安装移动安全代理
- 注册到移动安全管理模块
- 注销移动安全管理模块
- 更新移动安全代理组件
- 将安全策略设置与移动安全管理模块同步
- 远程擦除移动设备
- 远程锁定移动设备
- 远程定位移动设备

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/报告设置**窗口。
3. 在**短信发送器设置**部分，单击**添加**，键入一个短信发送器的电话号码并单击**保存**。短信发送器显示在列表中。

4. 检查您已配置的电话号码的**状态**字段是否显示为**已连接**。如果**状态**文本框显示为**已断开**，请确保短信发送器设备已连接到管理服务器。

注意

现有的短信发送器能通过单击电话号码进行修改。

监控短信发送器

移动安全可以监控短信发送器的状态，并在任何短信发送器断开超过 10 分钟时发送电子邮件通知。此外，短信发送器设备也会显示连接状态：客户端已停止、客户端正在运行、客户端未使用或客户端已断开。有关配置详细信息，请参阅管理员通知和预设报告 第 8-8 页。

编辑短信发送器

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/报告设置**窗口。
3. 在**短信发送器设置**部分，单击要编辑的电话号码。

   此时将显示一个对话框。
4. 在提供的文本框中编辑电话号码，然后单击**保存**。
5. 单击**保存**以保存设置。

删除短信发送器

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/报告设置**窗口。
3. 在**短信发送器设置**部分，选择要删除的短信发送器，并单击**删除**。
4. 单击**保存**以保存设置。

处理短信发送器客户端应用程序

设置短信发送器客户端应用程序

过程

1. 在 Android 移动设备上打开短信发送器应用程序。
2. 点击**设置**，然后点击以下选项进行配置：
   - **服务器地址**：键入管理服务器名称或 IP 地址，并点击**确定**。
   - **服务器端口**：键入管理 Web 控制台端口号并点击**确定**。
   - **电话号码**：键入短信发送器的电话号码。
   - **协议类型**：选择用于发送消息的 HTTP 或 HTTPS 协议。
3. 点击**启动**以启动短信发送器。

停止短信发送器

过程

1. 在 Android 移动设备上打开短信发送器应用程序。
2. 点击**停止**以停止短信发送器。

短信发送器状态

移动安全可在移动设备上更新短信发送器的状态。根据连接状态，设备会显示以下状态：

- 正常：短信发送器连接到管理服务器
- 已停止：短信发送器当前已停止。
- 未使用：短信发送器应用程序上的设置与移动安全服务器上的设置不匹配。

查看短信发送器历史记录

过程

1. 在 Android 移动设备上打开短信发送器应用程序。
2. 点击**历史记录**查看发送到移动设备的消息。

查看短信发送器运行日志

过程

1. 在 Android 移动设备上启动短信发送器应用程序。

2. 点击**运行日志**查看短信发送器运行事件日志。

管理员通知和预设报告

使用**管理员通知/报告**窗口配置以下设置：

- 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。
  - **移动安全的设备管理员已禁用** — 当任何 Android 移动设备上**设备管理员**列表中的移动安全被禁用时，均将向管理员发送电子邮件通知。标记变量 <%DEVICE%> 将替换为电子邮件中的移动设备名称。
  - **苹果推送通知服务证书过期警告** — 苹果推送通知服务证书过期时向管理员发送电子邮件通知。
- 报告：
  - **设备清单报告** — 针对由移动安全管理的所有移动设备的全面报告。
  - **合规违例报告** — 针对由移动安全管理且不符合所配置策略的所有移动设备的报告。
  - **恶意软件检测报告** — 针对在由移动安全管理的移动设备上检测到的所有安全威胁的报告。
  - **Web 威胁防护报告** — 针对在由移动安全管理的移动设备上访问的所有不安全 URL 的报告。
  - **应用程序清单报告** — 针对在由移动安全管理的移动设备上安装的所有应用程序的报告。
  - **设备注册报告** — 针对由移动安全管理的移动设备注册信息的报告。
  - **设备停用报告** — 针对由移动安全管理的移动设备停用信息的报告。

- **策略违例报告** — 针对违反安全策略的移动设备的报告。

配置管理员通知

过程

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

   显示**通知/报告设置**窗口。
3. 选择要通过电子邮件接收的通知和报告，然后单击单个通知和报告以修改其内容。

   

   注意

   选择要接收的报告时，也可以从每个报告的下拉列表中单独调整其接收频率。

   

   注意

   在电子邮件通知消息中编辑**消息**文本框时，请确保包含标记变量 `<%PROBLEM%>`、`<%REASON%>` 和 `<%SUGGESTION%>`，这些变量在电子邮件中将替换为实际值。
4. 完成后单击**保存**，以返回到**管理员通知/报告**窗口。

用户通知

使用**用户通知**窗口配置以下电子邮件和/或短信通知：

- **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。

- **策略违例** — 如果不满足合规条件，将向移动设备发送电子邮件通知。标记变量 <%DEVICE%> 和 <%VIOLATION%> 将替换为电子邮件中的移动设备名称及移动设备违反的策略。

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** > **设置**。

   显示**通知/报告设置**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。

     注意

     在编辑**消息**文本框时，请确保包含标记变量 <%DOWNLOADURL%> 或 <%DEVICE_NAME%> 和 <%VIOLATION%>，这些变量在电子邮件中将会替换为实际 URL。
   - 要配置短信通知消息，请更新**消息**文本框中的消息正文。

     注意

     编辑**消息**文本框时，请确保包含标记变量 <%DOWNLOADURL%>，此变量将会在电子邮件中替换为实际 URL。
4. 完成后单击**保存**，以返回到**用户通知**窗口。

第 9 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处理可能遇到的问题。

- **用户无法在设备中输入纳米密码。**

  移动设备小键盘仅支持特定的字符组。移动安全建议管理员整理出设备支持的字符列表。整理出支持的字符列表之后，管理员便可使用支持的字符列表通过管理控制台设置卸载保护密码。

- **移动安全客户端无法接收服务器的短信通知或无法通过公共 DNS 名称连接到服务器。**

  对于 Windows Mobile 平台，用于支持 DNS 名字的移动安全客户端版本应高于 5.0.0.1099；对于 Symbian OS 9.x S60 第 3 版平台，其版本应高于 5.0.0.1061。先前版本只能通过 IP 地址连接。

- **启用加密模块之后应用程序无法正常运行。**

  用户在设备中使用加密模块时，某些现有应用程序可能无法正常运行。这是因为可信列表中可能不包含这些现有应用程序。启用加密模块之后，将对某些文件类型进行加密（例如 `doc`、`txt`、`ppt`、`pdf`、`xls` 等）。加密模块仅允许可信应用程序访问加密的数据。因此，管理员必须将这些应用程序添加至可信应用程序列表。有关详细信息请参阅加密设置 第 4-19 页。

- **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。

- **iOS 移动设备无法成功注册到管理服务器，并显示不受支持的 URL 错误消息。**

  如果 SCEP 服务器系统时钟的时间设置有误，或趋势科技移动安全未获取简单证书注册协议 (SCEP) 证书，则可能会出现以上问题。请确保 SCEP 服务器系统时钟的时间设置正确。如果问题依然存在，请执行以下步骤：

  1. 登录移动安全管理 Web 控制台。

2. 单击**管理** > **通信服务器**设置。

3. 不要更改设置，单击**保存**。

- **管理服务器无法接收来自 BlackBerry 企业服务器 (BES) 的策略。**

  如果策略名称包含特殊字符，则通信服务器无法接收来自 BlackBerry 企业服务器 (BES) 的策略。检查策略名称是否包含任何特殊字符，如有，请使用字母和数字将其替换。

- **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>`。

- **无法连接到 SQL Server 2005 或 SQL Server 2005 Express。**

  如果 SQL Server 2005 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 2005 精简版和 SQL Server 2005 开发者版均不允许远程连接。若要将 SQL Server 2005 配置为允许远程连接，请完成以下步骤：

  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 installation folder>\Microsoft Visual Studio 9.0\Common7\IDE` 文件夹，找到并复制 `devenv.exe.config` 文件并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**。

- **某些 Android 移动设备的状态总是显示为未同步。**

  这是因为该移动设备上的移动安全设备管理员未激活。如果用户未在设备管理员列表中激活移动安全，则移动安全无法与移动设备同步服务器策略，并会将其状态显示为未同步。

- **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 网站** - 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://cn.trendmicro.com/cn/support/techsupport/index.html

联系技术支持

趋势科技为所有注册用户提供为期一年的技术支持、病毒码下载和程序更新，此后必须购买更新维护。如果需要帮助或遇到任何问题，欢迎随时与我们联系。也欢迎您提出宝贵意见。

- 获取全球技术支持办公室的列表：http://cn.trendmicro.com/cn/support/techsupport/index.html
- 获取最新趋势科技产品文档：http://docs.trendmicro.com/zh-CN/home.aspx

可通过电话、传真或电子邮件联系趋势科技代表：

```
Trend Micro, Inc.
10101 North De Anza Blvd.,
Cupertino, CA 95014
Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address: http://www.trendmicro.com
Email: support@trendmicro.com
```

将受感染文件发送给趋势科技

可以将恶意软件和其他受感染文件发送给趋势科技。特别是如果您怀疑是某种恶意软件但扫描引擎却无法识别或不能清除的文件，则可使用下列网址将被怀疑的文件提交给趋势科技：

http://esupport.trendmicro.com/srf/srfmain.aspx

请在消息文本中提供对所遇症状的简要描述。我们的恶意软件工程师组将剖析该文件以确定和识别可能包含的任何恶意软件，并通常在 48 小时内将干净的文件返回给您。

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://cn.trendmicro.com/cn/about/company/trendlabs/index.html

关于软件更新

产品发布后，趋势科技通常会开发对软件的更新，以增强产品性能、添加新增功能或强调已知问题。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://cn.trendmicro.com/cn/support/techsupport/index.html

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://cn.trendmicro.com/cn/support/techsupport/index.html

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

移动安全提供了诸多服务，其 Web 站点是 http://www.trendmicro.com。

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

管理服务器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

索引

Z

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: TSCM96388/140410