TREND MICRO™

9.5

趋势科技™ 移动安全™ 企业版 安装和部署指南

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 TSCM97240/151028

发布日期：2015 年 9 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：规划服务器安装

第 2 章：设置环境

第 3 章：安装、更新和删除服务器组件

第 4 章：配置服务器组件

第 5 章：处理移动安全客户端

附录 A：网络端口配置

附录 B：可选配置

附录 C：生成和配置苹果推送通知服务证书

索引

前言

前言

欢迎使用趋势科技™ 移动安全企业版 9.5*《安装和部署指南》*。本指南用于帮助管理员部署和管理趋势科技™ 移动安全企业版 9.5。本指南介绍了各种移动安全组件和不同的移动安全客户端部署方法。

有关移动安全的更新信息，包括移动设备支持和最新版本，请访问 http://cn.trendmicro.com/cn/products/enterprise/mobile-security/index.html。

注意

此*《安装和部署指南》*只适用于移动安全版本 9.5。并不适用于其他版本的移动安全。趋势科技技术支持仅限于移动安全的使用。要获得在此指南中提及的第三方应用程序的支持，请联系这些应用程序相应的供应商。

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

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

规划服务器安装

本章帮助管理员为趋势科技™ 移动安全企业版 9.5 规划服务器组件。

本章包含以下几节内容：

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）

包含云通信服务器的增强安全型号（双服务器安装）

增强安全型号支持在云中部署通信服务器。下图显示了在典型增强安全型号中包含的所有移动安全组件。

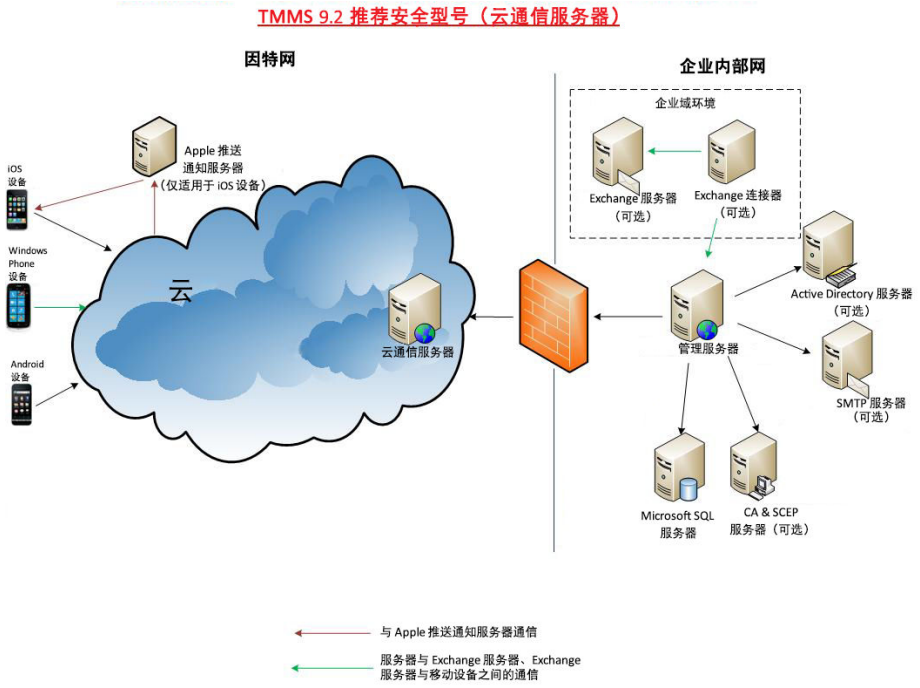

图 1-1. 包含云通信服务器的增强安全型号

包含本地通信服务器的增强安全型号（双服务器安装）

增强安全型号支持在两台不同的计算机上安装通信服务器和管理服务器。下图显示了在典型增强安全型号中包含的所有移动安全组件。

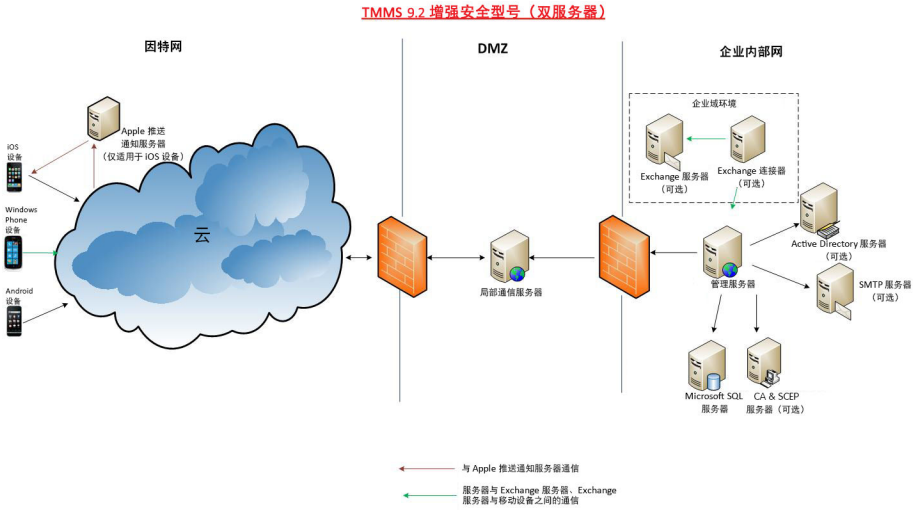

图 1-2. 包含本地通信服务器的增强安全型号

基本安全型号（单服务器安装）

基本安全型号支持在同一计算机上安装通信服务器和管理服务器。下图显示了在典型基本安全型号中包含的所有移动安全组件。

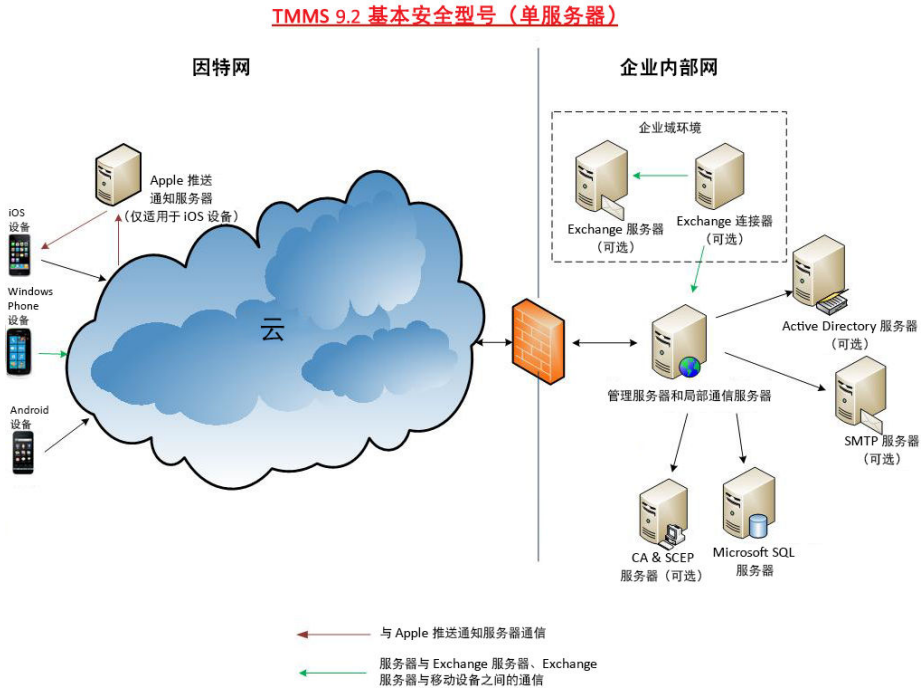

图 1-3. 基本安全型号

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。 Trend Micro Mobile Security 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，它不需要安装。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即可。 请参阅 本地和云通信服务器的比较 第 1-7 页。	必需
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，检测所有使用 Exchange ActiveSync 服务的移动设备，并将它们显示在移动安全 Web 控制台上。 通过 Microsoft Exchage 服务器与移动安全集成，管理员可监视访问 Microsoft Exchange 服务器的移动设备。此功能一旦启用和配置，移动安全管理员便可执行远程擦除，并阻止此类移动设备访问 Microsoft Exchange 服务器。 通过 Microsoft Exchange 服务器与移动安全的集成，管理员也可控制用户访问企业数据（如电子邮件、日历和联系人等）。	可选
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

组件	描述	必需或可选
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
苹果推送通知服务证书	移动安全通信服务器通过苹果推送通知服务 (APNs) 与 iOS 设备通信。	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 Windows Phone 或 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	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	支持	支持
管理 Windows Phone	不支持	支持

系统要求

在网络中安装各移动安全组件之前，请查看以下要求。

表 1-3. 系统要求

组件	要求
管理服务器和通信服务器	推荐的平台 • Windows Server 2008 R2 Enterprise Edition • Windows Server 2008 Enterprise Edition SP1 • Windows Server 2008 Standard Edition • Windows Web Server 2008 Edition SP1 其他平台 • Windows 2008 Server 系列 • Windows 2008 R2 Server 系列 • Windows 2012 Server 系列 • Windows Server 2012 R2 系列
	硬件 • 1-GHz Intel™ Pentium™ 处理器或同等产品 • 至少 1-GB 内存 • 至少 400-MB 可用磁盘空间 • 支持 256 色或更高颜色设置下 1024 x 768 分辨率的监视器

组件	要求
管理服务器的 IIS Web 服务器	Microsoft Internet Information Server (IIS) 7.0/7.5/8.0 **注意** • IIS 是 Microsoft Windows 的必要组成部分，且 IIS 版本号与安装的 Windows 版本相对应。 • 保留缺省设置并选择 使用管理服务器的 IIS 7.0 或更高版本时，保留缺省设置，并启用和安装应用程序开发中的 **CGI** 和 **ISAPI 扩展程序**、通用 HTTP 功能中的 **HTTP 重定向组件**和管理工具中的 **IIS6 管理兼容性**。 **注意** 趋势科技移动安全不支持 Apache Web 服务器。
Microsoft Exchange Server	• Microsoft Exchange Server 2007 • Microsoft Exchange Server 2010 • Microsoft Exchange Server 2013
Web 浏览器	• Internet Explorer 8.0 或更高版本 • Chrome 17 或更高版本 • Firefox 14 或更高版本 • Safari 6 或更高版本（在 Mac 中） **注意** 移动安全管理 Web 控制台需要 Adobe Flash player。

组件	要求
SQL Server	• Microsoft SQL Server 2008 • Microsoft SQL Server 2008 Express Edition • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 R2 Express Edition • Microsoft SQL Server 2012 • Microsoft SQL Server 2012 Express Edition • Microsoft SQL Server 2014 • Microsoft SQL Server 2014 Express Edition
移动安全 Exchange 连接器	平台 • Windows Server 2008 R2（64 位） • Windows Server 2012（64 位） • Windows Server 2012 R2（64 位） 硬件 • 1-GHz Intel™ Pentium™ 处理器或同等产品 • 至少 1-GB 内存 • 至少 200-MB 可用磁盘空间 其他 • Microsoft .Net Framework 3.5 SP1

安装摘要

以下是安装趋势科技移动安全涉及的步骤：

1. 为移动安全安装设置环境。

   有关详细信息，请参阅为移动安全安装设置环境 第 2-2 页。

   a. 在打算安装管理服务器的计算机上安装 Microsoft IIS Web 服务器。

有关详细信息，请参阅安装 Microsoft IIS Web 服务器 第 2-4 页。

b. （可选）安装数据库。

如果在这个阶段跳过此步骤，移动安全在安装过程中将自动安装 Microsoft SQL Server 2008 Express 版本。

有关详细信息，请参阅安装 SQL Server（可选） 第 2-5 页。

c. （可选）设置 Active Directory 帐户访问权。

如果要从企业的 Active Directory 服务器导入用户，请执行此步骤。

有关详细信息，请参阅设置 Active Directory 帐户访问权（可选） 第 2-6 页。

d. （可选）安装 Microsoft Exchange 服务器管理工具。

提供 Exchange 服务器与管理服务器的集成，以管理 Windows Phone、Android、iOS 移动设备。

有关详细信息，请参阅安装 Microsoft Exchange 服务器管理工具（可选） 第 2-7 页。

e. 应用网络访问规则。

有关详细信息，请参阅应用移动安全的网络访问规则 第 2-7 页。

2. （可选）设置 iOS 移动设备环境。

有关详细信息，请参阅设置 iOS 移动设备的环境（可选） 第 2-3 页。

3. 安装服务器组件。

有关详细信息，请参阅安装服务器组件 第 3-3 页。

a. 安装移动安全管理服务器。

有关详细步骤，请参阅安装管理服务器 第 3-4 页。

b. 登录移动安全企业版管理 Web 控制台。

有关详细步骤，请参阅访问管理 Web 控制台 第 3-9 页。

c. 注册产品。

有关详细步骤，请参阅注册产品 第 3-11 页。

d. （可选）下载和安装本地通信服务器 (LCS)。

如果打算使用云通信服务器 (CCS)，则可以跳过此步骤。

有关详细步骤，请参阅安装本地通信服务器 第 3-12 页。

e. （可选）设置 Exchange 服务器集成。

如果不希望管理使用 Exchange ActiveSync 的移动设备，则可以跳过此步骤。

有关详细步骤，请参阅安装 Exchange 连接器 第 3-17 页。

i. 确保安装了 Microsoft Exchange 服务器管理工具。

有关安装步骤，请参阅安装 Microsoft Exchange 服务器管理工具（可选） 第 2-7 页。

ii. 为 Exchange 连接器配置帐户。

为 Exchange 连接器提供访问权。

有关详细步骤，请参阅为 Exchange 连接器配置帐户 第 3-15 页。

iii. 安装 Exchange 连接器。

在管理服务器和 Exchange 服务器之间建立通信。

有关详细步骤，请参阅安装 Exchange 连接器 第 3-17 页。

iv. 配置 Exchange 服务器集成设置。

有关详细步骤，请参阅配置 Exchange 服务器集成设置 第 4-14 页。

4. 配置服务器组件。

有关详细信息，请参阅初始服务器安装 第 4-3 页。

a. 配置数据库设置。

有关详细步骤，请参阅配置数据库设置 第 4-5 页。

b. 配置通信服务器设置。

有关详细步骤，请参阅配置通用通信服务器设置 第 4-6 页。

c. （可选）配置 Android 通信服务器设置。

如果不希望管理 Android 移动设备，则可以跳过此步骤。

有关详细步骤，请参阅配置 Android 通信服务器设置 第 4-7 页。

d. （可选）配置 iOS 通信服务器设置。

如果不希望管理 iOS 移动设备，则可以跳过此步骤。

有关详细步骤，请参阅配置 iOS 通信服务器设置 第 4-8 页。

e. 配置设备注册设置。

有关详细步骤，请参阅配置设备注册设置 第 4-10 页。

f. （可选）自定义移动安全使用条款。

如果希望使用缺省移动安全使用条款，则可以跳过此步骤。

有关详细步骤，请参阅自定义移动安全使用条款 第 4-12 页。

g. （可选）配置 Active Directory 设置。

如果不希望从 Active Directory 服务器导入用户，则可以跳过此步骤。

有关详细步骤，请参阅配置 Active Directory (AD) 设置 第 4-12 页。

h. （可选）配置管理服务器设置。

如果您的管理服务器不使用代理访问 Internet，且您希望使用缺省服务器 IP 地址和端口号，则可以跳过此步骤。

有关详细步骤，请参阅配置管理服务器设置 第 4-13 页。

i. （可选）配置 Exchange 服务器集成设置。

如果不希望管理使用 Exchange ActiveSync 的移动设备，则可以跳过此步骤。

有关详细步骤，请参阅配置 Exchange 服务器集成设置 第 4-14 页。

j. （可选）配置通知和报告设置。

如果不希望向用户发送邀请电子邮件，则可以跳过此步骤。

请参阅配置通知和报告设置 第 4-16 页。

k. （可选）配置管理员通知。

如果不希望通过电子邮件接收错误消息通知和日常预设报告，则可以跳过此步骤。

有关详细步骤，请参阅配置管理员通知 第 4-16 页。

l. 验证移动安全配置（推荐）。

有关步骤，请参阅验证移动安全配置 第 4-17 页。

m. 更改管理 Web 控制台的管理员帐户密码。

有关步骤，请参阅 *管理员指南*中的*编辑管理员帐户*主题。

5. 设置移动安全客户端。

设置移动安全客户端 第 5-3 页

a. （可选）为移动设备配置通知设置。

有关详细步骤，请参阅配置通知和报告设置 第 4-16 页。

b. （可选）配置移动安全在电子邮件和/或短信中发送给用户的安装消息。

此安装消息包括用户可用于访问以下载和安装 MDA 安装软件包的 URL。

有关详细步骤，请参阅配置安装消息 第 5-3 页。

c. （可选）向移动设备发送邀请。

有关详细步骤，请参阅向移动设备发送邀请 第 5-4 页。

d. 在移动设备上安装 MDA。

有关详细步骤，请参阅在移动设备上安装 MDA 第 5-6 页。

e. 在管理服务器上注册 MDA。

有关详细步骤，请参阅在移动安全管理服务器中注册 MDA 第 5-10 页。

第 2 章

设置环境

本章提供了在安装趋势科技™ 移动安全企业版 9.5 之前设置环境所需的信息。

本章包含以下几节内容：

为移动安全安装设置环境

下表描述了为移动安全安装设置环境的过程。

表 2-1. 为移动安全安装设置环境的过程

步骤	处理措施	描述
步骤 1	在打算安装管理服务器的计算机上安装 Microsoft IIS Web 服务器。	有关详细信息，请参阅安装 Microsoft IIS Web 服务器 第 2-4 页。
步骤 2	（可选）安装数据库。	如果现在跳过此步骤，移动安全在安装过程中将自动安装 Microsoft SQL Server 2008 Express 版本。 有关详细信息，请参阅安装 SQL Server（可选） 第 2-5 页。
步骤 3	（可选）设置 Active Directory 帐户访问权。	如果要从企业的 Active Directory 服务器导入用户，请执行此步骤。 有关详细信息，请参阅设置 Active Directory 帐户访问权（可选） 第 2-6 页。
步骤 4	（可选）安装 Microsoft Exchange 服务器管理工具。	提供 Exchange 服务器与移动安全管理服务器的集成，以管理 Windows Phone、Android、iOS 移动设备。 有关详细信息，请参阅安装 Microsoft Exchange 服务器管理工具（可选） 第 2-7 页。
步骤 5	应用网络访问规则。	有关详细信息，请参阅应用移动安全的网络访问规则 第 2-7 页。 有关完整的网络端口配置，请参阅网络端口配置 第 A-1 页。
步骤 6	（可选）设置环境以管理 iOS 移动设备。	如果要管理 iOS 移动设备，此步骤为强制性步骤。 请参阅 设置 iOS 移动设备的环境（可选） 第 2-3 页。

设置 iOS 移动设备的环境（可选）

警告!

在设置环境以管理 iOS 移动设备之前，确保已经执行下表中提到的所有步骤。

下表描述了设置环境以管理 iOS 移动设备的过程。

表 2-2. 设置 iOS 移动设备环境的过程

步骤	处理措施	描述
步骤 1	苹果推送通知服务 (APNs) 证书。	如果要管理 iOS 移动设备，则需要设置苹果推送通知服务证书。 有关详细步骤，请参阅生成和配置苹果推送通知服务证书 第 C-1 页。
步骤 2	（可选）从公认的公共证书颁发机构获取 SSL 服务器证书。	SSL 证书提供了移动设备和通信服务器之间的安全通信。 如果要管理 Windows Phone 或 iOS 移动设备或打算使用本地通信服务器，则此步骤为强制性步骤。在安装本地通信服务器的过程中，需要导入公共 SSL 证书。 在以下情况下，可以跳过此步骤： • 要使用专用 SSL 证书时。在安装本地通信服务器的过程中，移动安全将会创建该证书。 • 打算使用云通信服务器时。

步骤	处理措施	描述
步骤 3	（可选）设置简单证书注册协议 (SCEP) 以实现额外的安全性	提供了移动设备和通信服务器之间的安全通信。 有关详细信息，请参阅设置 SCEP 第 B-5 页。 如果在环境中已经设置了 SCEP，则可以跳过此步骤。 **注意** 如果您不想为 iOS 移动设备使用 SCEP，那么您需要在安装管理服务器和通信服务器之后，在通信服务器设置中禁用它。有关步骤，请参阅配置 iOS 通信服务器设置 第 4-8 页。
步骤 4	在本地通信服务器上配置网络端口 2195 (TCP) 并在 Wi-Fi 网络中配置端口 5223	TCP 端口 2195 允许在 TCP 端口 2195 上建立通信服务器到苹果推送通知服务的出站连接。苹果推送通知服务的主机名是 **gateway.push.apple.com**。 端口 5223 允许 iOS 设备接收来自苹果服务器的推送通知，特别是当通过端口 5223 受阻的 Wi-Fi 网络连接时。然而，若移动设备使用的是 3G 网络，则不必配置此端口。 有关完整的网络端口配置，请参阅网络端口配置 第 A-1 页。

安装 Microsoft IIS Web 服务器

此任务是为移动安全安装设置环境过程中的一个步骤。

请参阅 为移动安全安装设置环境 第 2-2 页。

过程

- 导航到以下任一 URL，获取 IIS 的安装过程：
  - 对于 Windows 2008 或 Windows Server 2008 R2（IIS 7.0 或 7.5）

    http://www.iis.net/learn/install/installing-iis-7
  - 对于 Windows 2012 (IIS 8.0)

    http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012

注意

使用管理服务器的 IIS 7.0 或更高版本时，保留缺省设置，并启用和安装应用程序开发中的 **CGI** 和 **ISAPI 扩展程序**、通用 HTTP 功能中的 **HTTP 重定向组件**和管理工具中的 **IIS6 管理兼容性**。

安装 SQL Server（可选）

注意

如果不想安装任何特定的 SQL 服务器版本，则可以跳过此步骤。在安装过程中，移动安全会自动安装 Microsoft SQL Server 2008 Express 版本。

此任务是为移动安全安装设置环境过程中的一个步骤。

请参阅 为移动安全安装设置环境 第 2-2 页。

过程

- 导航到以下任一 URL，获取 SQL Server 的安装过程：
  - 对于 Microsoft SQL Server 2008/2008 R2（或 Express 版）：

    http://msdn.microsoft.com/zh-cn/library/ms143219(v=SQL.100).aspx
  - 对于 Microsoft SQL Server 2012（或 Express 版）：

http://msdn.microsoft.com/zh-cn/library/bb500395(v=SQL.110).aspx

注意

趋势科技建议对 SQL Server 使用 SQL Server 身份验证方法，而非 Windows 身份验证。但是，您也可以为 SQL Server 配置 Windows 身份验证。有关详细信息，请参阅对 SQL Server 使用 Windows 身份验证 第 B-2 页。

设置 Active Directory 帐户访问权（可选）

注意

只有在您计划使用 Active Directory 进行用户身份验证或从 Active Directory 导入用户的情况下，才需要执行此步骤。否则可跳过此步骤。

如果尚未安装 Active Directory，请参阅以下 URL 获取详细安装过程：

http://technet.microsoft.com/zh-cn/library/cc757211(WS.10).aspx

此任务是为移动安全安装设置环境过程中的一个步骤。

请参阅为移动安全安装设置环境 第 2-2 页。

过程

- 为移动安全 9.5 创建 Active Directory 服务帐户，并至少为该帐户分配对 Active Directory 的只读访问权限。有关为 Windows 2008 创建 Active Directory 帐户的信息，请参阅以下 URL：

  http://technet.microsoft.com/zh-cn/library/dd894463(WS.10).aspx

安装 Microsoft Exchange 服务器管理工具（可选）

Microsoft Exchange 服务器管理工具提供与管理服务器的 Exchange 服务器集成，可管理 Windows Phone、Android、iOS 移动设备。

此任务是为移动安全安装设置环境过程中的一个步骤。

请参阅为移动安全安装设置环境 第 2-2 页。

过程

- 导航到以下任一 URL，获取 Exchange 服务器管理工具的安装过程：
  - 对于安装 Exchange 服务器管理工具 2007：

    http://technet.microsoft.com/zh-cn/library/bb232090(v=EXCHG.80).aspx
  - 对于安装 Exchange 服务器管理工具 2010：

    http://technet.microsoft.com/library/bb232090(v=EXCHG.141)
  - 对于安装 Exchange 服务器管理工具 2013：

    http://technet.microsoft.com/zh-cn/library/bb232090(v=exchg.150).aspx

应用移动安全的网络访问规则

此任务是为移动安全安装设置环境过程中的一个步骤。

请参阅 为移动安全安装设置环境 第 2-2 页。

过程

- 应用以下网络访问规则：

- 如果打算使用 Active Directory，管理服务器应该能够连接到 Active Directory 服务器。如果使用防火墙，确保为管理服务器在防火墙设置中添加一个例外。
- 管理服务器应能够连接安装有趋势科技移动安全数据库的 SQL Server。如果使用防火墙，确保在 SQL 服务器和管理服务器中的防火墙设置中添加一个例外。
- 为端口 4343 添加一个例外，确保管理服务器和通信服务器之间的 https 连接：

  若需要自定义该端口号，请参阅配置通信服务器端口 第 B-4 页获取详细信息。
- 为端口号 80 和 443 添加例外，确保所有移动设备都能连接到通信服务器。

第 3 章

安装、更新和删除服务器组件

本章指导管理员安装趋势科技™ 移动安全企业版 9.5 服务器组件。此外，本章还针对如何删除服务器组件提供指导。

本章包含以下几节内容：

- 删除服务器组件 第 3-24 页

安装服务器组件

在安装之前

在开始安装移动安全服务器组件前：

- 请确保移动安全组件满足指定的系统要求。

  请参阅 系统要求 第 1-8 页。此外，可能还需要计算网络拓扑，并确定想要安装的移动安全服务器组件。

- 确保已执行设置环境 第 2-1 页一章中的所有先决条件步骤。

趋势科技移动安全安装工作流

下表描述了安装趋势科技移动安全的基本方法。

表 3-1. 趋势科技移动安全安装工作流

步骤	处理措施	描述
步骤 1	安装移动安全管理服务器。	有关详细步骤，请参阅安装管理服务器 第 3-4 页。
步骤 2	登录移动安全企业版管理 Web 控制台。	有关详细步骤，请参阅访问管理 Web 控制台 第 3-9 页。
步骤 3	注册产品。	有关详细步骤，请参阅注册产品 第 3-11 页。
步骤 4	（可选）下载和安装本地通信服务器。	如果打算使用云通信服务器 (CCS)，则可以跳过此步骤。 有关详细步骤，请参阅安装本地通信服务器 第 3-12 页。

步骤	处理措施	描述
步骤 5	（可选）安装 Exchange 连接器。	如果不希望管理使用 Exchange ActiveSync 的移动设备，则可以跳过此步骤。 有关详细步骤，请参阅安装 Exchange 连接器 第 3-17 页。

安装管理服务器

注意

移动安全需要 Java 运行时环境 (JRE)，以从管理服务器上的应用程序管理模块上传 .apk 文件。安装管理服务器时将自动安装 JRE。但是如果安装管理服务器的计算机上已安装 JRE，则安装管理服务器时不会安装 JRE。如果现有 JRE 版本低于 1.6，则需要手动卸载 JRE，并安装 1.6 版或更高版本。

过程

1. 从以下位置下载管理服务器安装程序：

   http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4415&lang_loc=1

2. 将下载的文件解压缩，然后运行管理服务器安装程序：MdmServerSetup.exe.

   显示**欢迎**窗口。

3. 单击**下一步**。

   显示**许可协议**窗口。

4. 选中**我同意**复选框并单击**下一步**。

注意

移动安全要求安装 Microsoft Visual C++ 2005 Redistributable 文件。如果您的计算机中已经安装了这些文件，在安装过程中将不会出现 Microsoft Visual C++ 2005 Redistributable 文件安装步骤。如果显示 Microsoft Visual C++ 2005 Redistributable 文件安装窗口，单击窗口中的**下一步**以继续安装。

显示**数据库选项**窗口。

图 3-1. “数据库选项”窗口

5. 执行下列操作之一：

   - 如果您尚未安装任何数据库或者要为移动安全创建新的数据库：

     a. 选择**在此计算机上安装 Microsoft SQL Server 2008 Express**，并单击**下一步**。

显示**数据库设置**窗口。

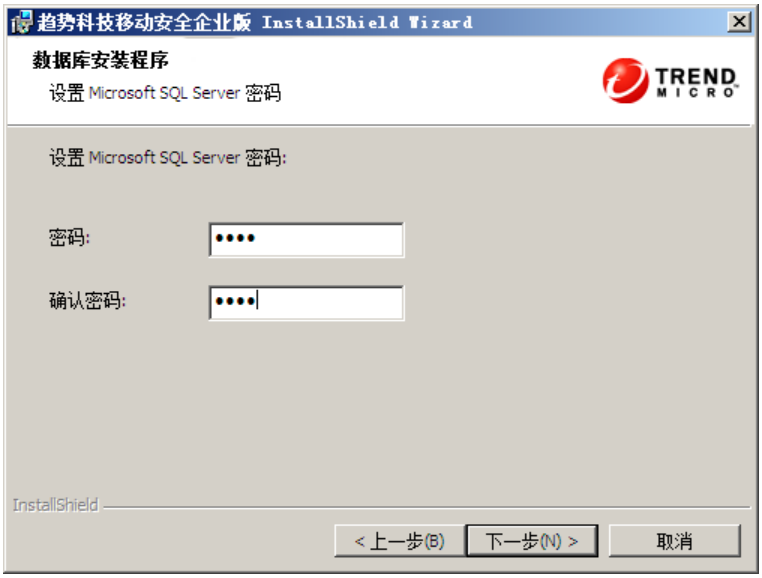

图 3-2. 新数据库的“数据库设置”窗口

b. 为新数据库键入密码，并单击**下一步**。

显示**安装进度**窗口，并显示当前安装状态。

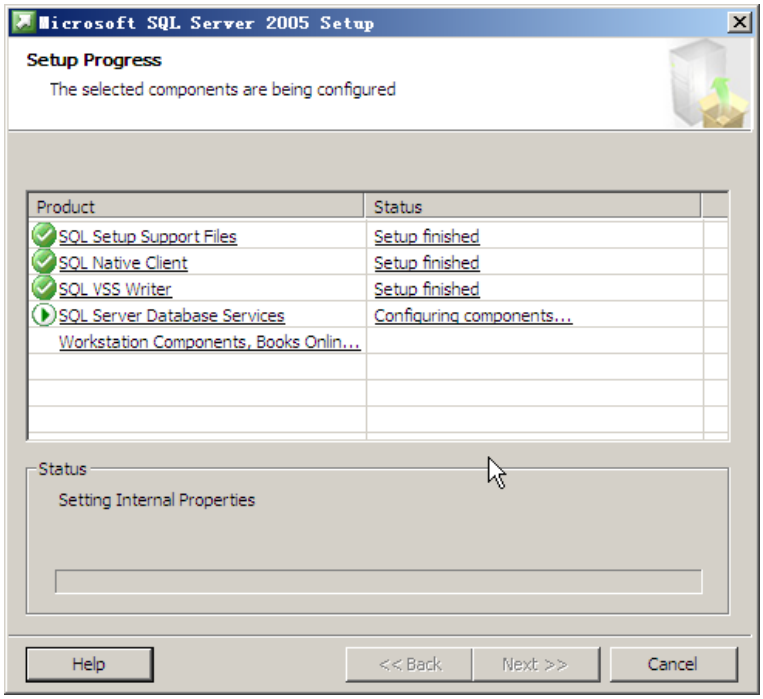

图 3-3. “安装进度”窗口

c. 安装完成后，单击**下一步**。

显示**服务器连接设置**窗口。

- 如果您已经安装了数据库并且希望使用现有数据库：

a. 选择**连接到现有数据库**并单击**下一步**。

显示**现有数据库**窗口。

图 3-4. 现有数据库服务器信息

b. 键入现有数据库服务器信息并单击**下一步**。

显示**服务器连接设置**窗口。

6. 从下拉列表中选择 IP 地址并键入服务器端口号，单击**下一步**。
7. 选择安装移动安全的位置，并单击**下一步**。

注意

单击**更改**以选择其他位置。

8. 单击**安装**，开始安装。

将出现安装进度窗口。安装完成后，会显示**趋势科技移动安全安装完成**窗口。

9. 单击**完成**。

后续步骤

有关下一个配置任务，请参阅趋势科技移动安全安装工作流 第 3-3 页。

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 3-5. 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*管理员指南*中的*编辑管理员帐户*。

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 3-10 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**。

注册产品

趋势科技在指定时间段内为所有已注册用户提供技术支持、恶意软件病毒码下载和程序更新，在之后必须购买更新维护才能继续享受这些服务。必须对移动安全服务器进行注册才能合法地获得最新的安全更新及其他产品和维护服务。

仅需使用激活码即可在管理服务器上注册移动安全服务器。在移动设备连接并注册到服务器之后，移动设备客户端从移动安全服务器自动获得使用授权信息。

以下列格式显示激活码：

XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

过程

1. 登录到管理 Web 控制台。

   如果这是您首次访问管理控制台，将会显示**产品使用授权**窗口；否则，请单击**管理** > **产品使用授权**，然后单击**新激活码**。

2. 在提供的文本框中键入激活码，并单击**保存**。

图 3-6. 安装后注册移动安全

3. 请验证产品注册是否成功。单击**控制台**以显示**控制台**窗口。

   如果产品注册成功，应该会看到“趋势科技移动安全 9.5 已经激活。”的消息。

完成注册后，会显示**移动安全配置和验证**窗口，其将指导您逐步完成初始设置。

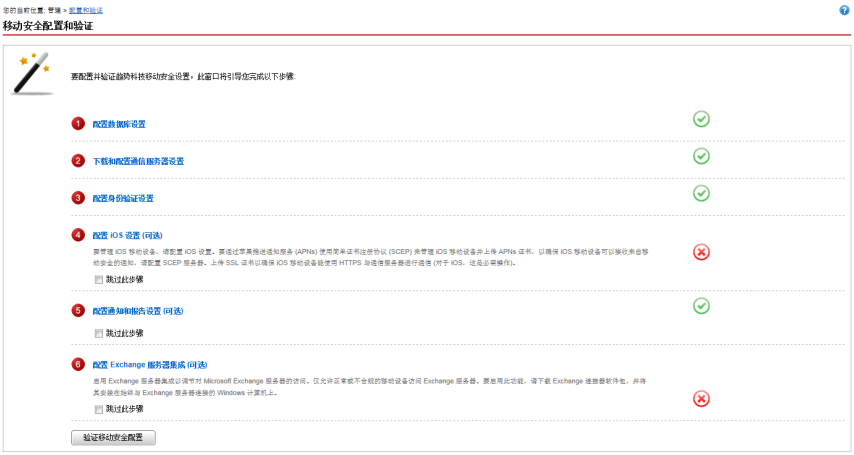

图 3-7. 移动安全配置和验证窗口

后续步骤

有关下一个配置任务，请参阅趋势科技移动安全安装工作流 第 3-3 页。

安装本地通信服务器

过程

1. 登录到要安装通信服务器的计算机上的管理 Web 控制台。
2. 单击**管理** > **通信服务器设置**。
3. 单击**通用设置**选项卡。
4. 从下拉列表中选择**本地通信服务器**，然后单击**单击此处下载**链接，将安装包下载到要安装通信服务器的计算机上。
5. 双击安装文件，启动安装过程。

显示**欢迎**窗口。

6. 单击**下一步**。

   显示**许可协议**窗口。

7. 选择**我接受该许可协议中的条款**，并单击**下一步**。

   显示**移动设备的通信服务器连接设置**窗口。

8. 从下拉列表中选择 IP 地址，并键入通信服务器的 HTTP 和 HTTPS 端口号。

   通信服务器与移动设备进行通信时将使用此窗口中的 IP 地址和端口号。

   注意

   趋势科技建议您为 IP 地址选择“所有”。

9. 单击**下一步**。

   显示**管理服务器的通信服务器连接设置**窗口。

10. 从下拉列表中选择 IP 地址，并键入通信服务器的 HTTPS 端口号。

    通信服务器与管理服务器进行通信时将使用此窗口中的 IP 地址和端口号。

    注意

    趋势科技建议您为 IP 地址选择“所有”。

11. 单击**下一步**。

    显示**服务器证书**窗口。

12. 执行下列操作之一：

    - 如果已经拥有用于 iOS 移动设备注册的 SSL 证书，执行以下操作：

      a. 选择**导入现有的 .pfx 或 .p12 证书文件**并单击**下一步**。

         显示**导入证书**窗口。

b. 单击**浏览**并从硬盘中选择公共证书。

c. 在**密码**文本框中键入证书密码。如果该证书没有密码，则将此文本框留空。

d. 单击**下一步**。

- 如果没有用于 iOS 移动设备注册的 SSL 证书，或者需要创建新的证书，执行以下操作：

  a. 选择**创建新的专用证书**并单击**下一步**。

  显示**创建证书**窗口。

  b. 在**通用名称**文本框中键入通信服务器 IP 地址，并在**密码**文本框中键入证书密码。

  c. 单击**下一步**。

13. 选择安装移动安全的位置，并单击**下一步**。

注意

单击**更改**以选择其他位置。

14. 单击**安装**，开始安装。

将出现安装进度窗口。安装完成后，会显示**安装完成**窗口。

15. 单击**完成**。

后续步骤

有关下一个配置任务，请参阅趋势科技移动安全安装工作流 第 3-3 页。

设置 Exchange 服务器集成

要在管理服务器和 Exchange 服务器之间建立通信，Exchange 服务器集成是必需的。

注意

趋势科技移动安全仅支持 Exchange Server 2007 或更高版本，并为 Windows Phone、iOS 和 Android 移动设备提供 Exchange 服务器集成支持。

下表描述了为趋势科技移动安全设置 Exchange 服务器集成的过程。

表 3-2. 设置 Exchange 服务器集成的过程

步骤	处理措施	描述
步骤 1	安装 Microsoft Exchange 服务器管理工具。	在配置 **Exchange 服务器设置**之前，确保 Microsoft Exchange 服务器管理工具已在要安装 Exchange 连接器的计算机上安装好。 有关安装步骤，请参阅安装 Microsoft Exchange 服务器管理工具（可选） 第 2-7 页。
步骤 2	为 Exchange 连接器配置帐户。	为 Exchange 连接器提供访问权。 有关详细步骤，请参阅为 Exchange 连接器配置帐户 第 3-15 页。
步骤 3	安装 Exchange 连接器。	在管理服务器和 Exchange 服务器之间建立通信。 有关详细步骤，请参阅安装 Exchange 连接器 第 3-17 页。
步骤 4	配置 Exchange 服务器集成设置。	有关详细步骤，请参阅配置 Exchange 服务器集成设置 第 4-14 页。

为 Exchange 连接器配置帐户

过程

1. 在 Active Directory 服务器中创建用户帐户。
2. 在要安装 Exchange 连接器的计算机上，导航到**开始** > **管理员工具** > **计算机管理**，并执行以下操作。

a. 从左侧的树中展开**本地用户和组**文件夹，然后双击**组**。

b. 右击**管理员**，然后单击**属性**。

c. 单击**常规**选项卡上的**添加**按钮，并执行以下操作：

i. 在**登录名**文本框中键入在此过程步骤 1 第 3-15 页 中创建的用户名并单击**搜索**。

显示**选择用户、计算机、服务、帐户或组**对话框。

ii. 将用户名和域名一起（例如：domainname\username）键入**输入要选择的对象名称**文本框中，并单击**检查名称**。

iii. 单击**确定**。

d. 单击**管理员属性**对话框上的**确定**。

3. 在 Active Directory 服务器上，执行以下操作：

a. 导航到**开始** > **管理员工具** > **Active Directory 用户和计算机**。

b. 从左侧的树中展开用户文件夹。

c. 右击在此过程步骤 1 第 3-15 页 中创建的帐户（用户名）并单击**添加到组**。

d. 执行下列操作之一：

- 对于 Exchange Server 2007，在**输入要选择的对象名称**文本框中键入 `Exchange 组织管理员`并单击**检查名称**。
- 对于 Exchange Server 2010 和 2013，在**输入要选择的对象名称**文本框中键入 **组织管理员**并单击**检查名称**。

e. 单击**确定**，然后单击确认窗口中的**确定**。

4. 在 Active Directory 服务器上，执行以下操作：

a. 导航到**开始** > **管理员工具** > **Active Directory 用户和计算机**。

b. 从菜单栏中，单击**查看** > **高级功能**。

c. 从左侧的树中展开用户文件夹。

d. 右击在此过程步骤 1 第 3-15 页 中创建的帐户（用户名）并单击**属性**。

e. 在**安全**选项卡上，单击**添加**。

f. 将在步骤 1 第 3-15 页 中所创建的用户名和域名一起（例如：domainname\username）键入**输入要选择的对象名称**文本框中，并单击**检查名称**，然后单击**确定**。

g. 在**组或用户名**列表中选择用户名，并单击**高级**。

h. 选择**包括来自此对象父对象的可继承权限**并单击**确定**。

i. 单击**属性**对话框上的**确定**。

安装 Exchange 连接器

注意

必须在计算机上安装 Exchange 连接器：

- Microsoft Exchange 服务器管理工具安装的位置，
- 与 Exchange 服务器位于相同的域，并且
- 应该能够连接到管理服务器。

过程

1. 登录到管理 Web 控制台。
2. 单击**管理 > Exchange 服务器集成**。
3. 单击**单击此处下载**，并将 ExchangeConnector.zip 文件保存到计算机。
4. 解压缩 ExchangeConnector.zip 文件内容并运行 ExchangeConnector.exe 文件。

   显示 Exchange 连接器安装向导。
5. 单击**欢迎**窗口中的**下一步**。
6. 选择**我接受该许可证协议中的条款**，并单击**下一步**。

安装程序现在会检查计算机中是否安装了 Microsoft Exchange 管理工具。如果安装了，安装程序会显示以下窗口。

图 3-8. Exchange 管理安装检查成功

7. 单击**正在检查系统要求**窗口中的**下一步**。
8. 单击**浏览**并选择要安装 Exchange 连接器的目标文件夹，然后单击**下一步**。

   显示**服务帐户**窗口。
9. 键入用户名、密码和域名（在为 Exchange 连接器配置帐户 第 3-15 页中创建）以访问 Exchange 管理工具，单击**下一步**。
10. 查看**查看设置**窗口中的设置并单击**安装**。

    安装程序开始安装 Exchange 连接器。

11. 安装完成时，单击**下一步**，然后单击**完成**。

注意

从 Exchange 服务器将移动设备信息导入管理服务器所需的时间取决于要导入的移动设备的数量。例如，从 Exchange 服务器将 5000 台移动设备的信息导入管理服务器可能需要长达几个小时。

后续步骤

有关其他配置任务，请参阅趋势科技移动安全安装工作流 第 3-3 页。

有关下一个设置 Exchange 服务器集成的任务，请参阅设置 Exchange 服务器集成 第 3-14 页。

更新组件

关于移动安全升级

趋势科技移动安全仅支持从 9.0 版或更高版本进行升级。

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 — 移动安全管理服务器和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，并使移动安全能够检测到这些危害文件。趋势科技定期更新特征码文件，以确保对最新威胁的防护。
- 移动安全客户端安装程序 — 移动安全客户端的程序安装包。

趋势科技移动安全仅支持从 9.0 版或更高版本进行升级。对于从低于 9.0 的版本进行升级，趋势科技提供迁移工具，可将您的数据从旧版本迁移到 v9.0 Patch 1。然后，您可以升级到移动安全 9.5。

有关将您的数据从旧版本迁移到 v9.5 的详细过程，请参阅以下链接：

http://esupport.trendmicro.com/solution/en-US/1098095.aspx

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 3-22 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。

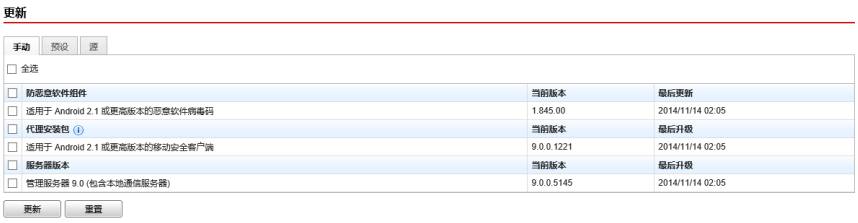

图 3-9. 更新窗口上的手动选项卡

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。

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 3-22 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。

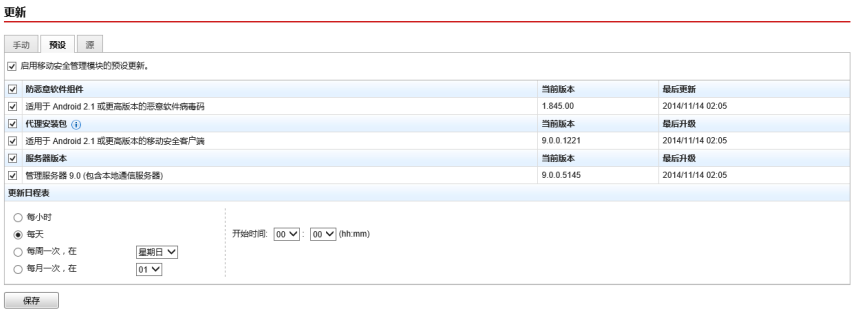

图 3-10. 更新窗口上的预设选项卡

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 3-20 页；有关预设更新的详细信息，请参阅预设更新 第 3-21 页。
3. 单击**源**选项卡。

图 3-11. 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。

删除服务器组件

本节指导您完成删除管理服务器和通信服务器所需执行的步骤。

过程

1. 在 Windows 控制面板中双击**程序和功能**。

   显示**卸载或更改程序**窗口。

2. 选择以下选项之一：
   - **趋势科技本地通信服务器** — 卸载通信服务器
   - **趋势科技移动安全** — 卸载管理服务器
3. 单击**卸载**。

   此时将显示一个对话框。

4. 在对话框中选择**安装完成后自动关闭应用程序并重启**，然后单击**确定**。

第 4 章

配置服务器组件

本章帮助管理员为趋势科技™ 移动安全企业版 9.5 配置服务器组件。

本章包含以下几节内容：

初始服务器安装

下表描述了安装趋势科技移动安全后的初始服务器安装。

表 4-1. 移动安全服务器的初始安装

步骤	处理措施	描述
步骤 1	配置数据库设置。	有关详细步骤，请参阅配置数据库设置 第 4-5 页。
步骤 2	配置通信服务器设置。	有关详细步骤，请参阅配置通用通信服务器设置 第 4-6 页。
步骤 3	（可选）配置 Android 通信服务器设置。	如果不希望管理 Android 移动设备，则可以跳过此步骤。 有关详细步骤，请参阅配置 Android 通信服务器设置 第 4-7 页。
步骤 4	（可选）配置 iOS 通信服务器设置。	如果不希望管理 iOS 移动设备，则可以跳过此步骤。 有关详细步骤，请参阅配置 iOS 通信服务器设置 第 4-8 页。
步骤 5	配置设备注册设置。	有关详细步骤，请参阅配置设备注册设置 第 4-10 页。
步骤 6	（可选）自定义移动安全使用条款。	如果希望使用缺省移动安全使用条款，则可以跳过此步骤。 有关详细步骤，请参阅自定义移动安全使用条款 第 4-12 页。
步骤 7	（可选）配置 Active Directory 设置。	如果不希望从 Active Directory 服务器导入用户，则可以跳过此步骤。 有关详细步骤，请参阅配置 Active Directory (AD) 设置 第 4-12 页。

步骤	处理措施	描述
步骤 8	（可选）配置管理服务器设置。	如果您的管理服务器不使用代理访问 Internet，且您希望使用缺省服务器 IP 地址和端口号，则可以跳过此步骤。 有关详细步骤，请参阅配置管理服务器设置 第 4-13 页。
步骤 9	（可选）配置 Exchange 服务器集成设置。	如果不希望管理使用 Exchange ActiveSync 的移动设备，则可以跳过此步骤。 有关详细步骤，请参阅配置 Exchange 服务器集成设置 第 4-14 页。
步骤 10	（可选）配置通知和报告设置。	如果不希望向用户发送邀请电子邮件，则可以跳过此步骤。 请参阅 配置通知和报告设置 第 4-16 页。
步骤 11	（可选）配置管理员通知。	如果不希望通过电子邮件接收错误消息通知和日常预设报告，则可以跳过此步骤。 有关详细步骤，请参阅配置管理员通知 第 4-16 页。
步骤 12	验证移动安全配置（推荐）。	使用**配置和验证**窗口验证移动安全配置。 有关步骤，请参阅验证移动安全配置 第 4-17 页。
步骤 13	更改管理 Web 控制台的管理员帐户密码。	登录管理 Web 控制台后，使用**管理帐户管理**窗口。 有关步骤，请参阅*管理员指南*中的*编辑管理员帐户*主题。

注意

在移动设备上继续安装移动安全代理前，必须完成移动安全服务器的初始设置。

配置数据库设置

过程

1. 登录到管理 Web 控制台。
2. 单击**管理** > **数据库设置**。
3. 键入服务器名称或 IP 地址、您的用户名、密码和数据库名称。

   注意

   如果您要使用特定端口连接 SQL Server，请使用以下格式：

   <SQL server name or IP address>,<Port>

4. 单击**保存**。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

配置通信服务器设置

通信服务器设置窗口提供以下设置：

- **通用设置** — 配置通信服务的基本设置。
- **Android 设置** — 为 Android 移动设备管理配置通知和客户端定制设置。
- **iOS 设置** — 为 iOS 移动设备管理配置 SCEP 设置并上传苹果推送通知服务和 SSL 证书。
- **Windows Phone 设置** — 配置预设，其中定义 Windows Phone 移动设备连接到通信服务器以更新策略设置和命令的频率。

配置通用通信服务器设置

过程

1. 登录到管理 Web 控制台。
2. 单击**管理** > **通信服务器设置**。
3. 单击**通用设置**选项卡。
4. 在**通信服务器类型**部分下，选择以下两个选项之一：
   - **本地通信服务器** — 已经在网络中本地安装了通信服务器时。
   - **云通信服务器** — 要使用在云中部署的通信服务器时。
5. 在**通信服务器与移动设备之间的通信设置**部分下，配置以下内容：
   - **外部域名或 IP 地址** — 本地通信服务器的域名或 IP 地址。
   - **HTTP 端口**和 **HTTPS 端口** — 用于本地通信服务器与移动设备进行通信。

     缺省 HTTP 和 HTTPS 端口为 8080 和 4343。

     注意

     如果两个端口都进行了配置，移动设备将使用 HTTPS 端口与通信服务器进行通信。只有当无法使用 HTTPS 端口进行通信时，移动设备才会使用 HTTP 端口。
6. 在**通信服务器与管理服务器之间的通信设置**部分下，配置以下内容：
   - **通信服务器名称或 IP 地址** — 本地通信服务器的域名或 IP 地址。
   - **HTTPS 端口** — 用于本地通信服务器与管理服务器进行通信。

     注意

     若需要自定义 HTTPS 端口，请参阅配置通信服务器端口 第 B-4 页获取详细信息。

7. 在**信息收集频率**部分下，配置以下内容：

   - **信息收集频率** — 选择移动安全收集移动设备上安装的应用程序的信息的频率。
   - **移动设备漫游时的信息收集频率** — 选择当移动设备漫游时移动安全收集移动设备上安装的应用程序的信息的频率。

   注意

   此设置仅适用于 Android 和 iOS 移动设备。

   从移动设备注册起，移动安全便会根据您选择的频率收集移动设备上安装的应用程序的信息。

   更改频率将重置计时器。

8. 如果您想要自动选择性擦除 Root 权限或越狱版移动设备，在 **Root 权限/越狱版设备检测**部分下，选择**选择性擦除 Root 权限或越狱版设备**。

9. 单击**保存**。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

配置 Android 通信服务器设置

过程

1. 登录到管理 Web 控制台。
2. 单击**管理** > **通信服务器设置**。
3. 单击 **Android 设置**选项卡。
4. 如果要向 Android 移动设备发送推送通知，在**推送通知设置**部分下，选择**启用推送通知**。

注意

如果不启用此设置，Android 移动设备用户将需要手动更新移动设备上的公司政策。

5. 在**客户端定制**部分下，选择**启用客户端定制**，以便向用户从移动安全通信服务器下载的 Android 客户端应用程序添加服务器 IP 地址和端口号。如果在设备注册设置中选择了**启用预置的注册密钥**，还会自动将预置的注册密钥添加到 Android 客户端应用程序。

   这意味着系统将在客户端应用程序中自动填充服务器 IP 地址、端口号和预置的注册密钥，用户无需手动键入这些信息。

6. 如果要对移动设备上的系统设置提供密码保护，在**系统设置的密码保护**部分下，选择**启用系统设置的密码保护**，然后在**密码**文本框中键入密码。

7. 单击**保存**。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

配置 iOS 通信服务器设置

过程

1. 登录到管理 Web 控制台。
2. 单击**管理** > **通信服务器设置**。
3. 单击 **iOS 设置**选项卡。
4. 在**苹果推送通知服务 (APN) 设置**部分下，配置以下内容：
   - **证书类型**：选择您的证书类型。
   - **证书**：从下拉列表中选择苹果推送通知服务证书，或上传新证书。
5. 在**简单证书注册协议 (SCEP) 设置**部分下，配置以下内容：
   a. 选择**启用 SCEP**。

b. 如果启用，请使用以下信息填写文本框：

- **SCEP 用户 URL：**

  http://SCEP_IP/certsrv/mscep

- **SCEP 管理员 URL：**

  对于 Windows Server 2008：

  http://SCEP_IP/certsrv/mscep_admin

注意

有关 SCEP 的信息，请参阅移动安全系统的组件 第 1-5 页。

6. 在**客户端配置文件签名凭证**部分下，配置以下内容：

- **客户端概要文件签名凭证：**从下拉列表中选择签名凭证证书，或上传新证书。

注意

为在 iOS 移动设备上配置移动安全客户端，移动安全会在移动设备上安装**安装配置概要文件**。要想将**安装配置概要文件**的状态更改为**已验证**，需要使用**客户端概要文件签名证书**。如果不对此设置进行配置，**安装配置概要文件**的状态将显示为**未验证**。

对此设置进行配置后，在移动设备上，安装配置概要文件的状态将显示为“已验证”。

7. 单击**保存**。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

配置 Windows Phone 通信服务器设置

过程

1. 登录到管理 Web 控制台。
2. 单击**管理** > **通信服务器设置**。
3. 单击 **Windows Phone 设置**选项卡。
4. 设置频率，以定义 Windows Phone 移动设备连接到移动安全通信服务器以更新 **Windows Phone 同步时间间隔**中的策略设置和命令的频率。

配置设备注册设置

过程

1. 登录到管理 Web 控制台。
2. 单击**管理** > **设备注册设置**。
3. 单击**身份验证**选项卡。
4. 在**用户验证**部分下，选择以下任一选项：
   - **使用 Active Directory 进行身份验证** — 使用来自 Active Directory 的用户信息验证移动设备。
   - **使用注册密钥进行身份验证** — 使用注册密钥验证移动设备。

     移动安全会自动生成注册密钥并将其通过邀请消息发送到移动设备。
     - **注册密钥使用限制** — 选择以下任一选项：
       - **使用了多次** — 如果要将一个注册密钥用于每个要注册的移动设备，则选择此项。
       - **使用一次** — 如果为每个要注册的移动设备使用不同的注册密钥，则选择此项。

- **注册密钥在达到以下条件后到期:** — 如果要在某个特定时间之后停止使用自动生成的注册密钥，则选择此设置，然后从下拉列表中选择时间。
- **使用预置的注册密钥** — 如果要手动生成注册密钥，则选择此设置，然后单击“生成”以生成注册密钥。该注册密钥不会在邀请消息中发送给用户。
- **注册密钥到期日期** — 如果要在某个特定日期停止使用手动生成的注册密钥，则选择此设置，然后从日历中选择日期。

5. 在**设备验证**部分下，选择以下任一选项：
   - **禁用此设置** — 禁用对移动设备的设备验证。
   - **使用 IMEI 或 Wi-Fi MAC 地址进行验证** — 此设置让您能够上传要验证的移动设备列表。

   a. 单击**导出允许设备列表模板**以下载模板并创建允许设备列表。

   b. 创建列表之后，单击**浏览**以选择和导入您在之前步骤中创建的移动设备列表。

   c. 单击**检查数据格式**，验证允许设备列表中的数据格式。验证之后，移动安全会在**允许设备的状态**列表中显示所有移动设备。

   d. 选择以下选项之一:
      - **删除未验证的设备** — 删除已经存在于**设备管理**窗口中但不存在于导入的允许设备列表中的移动设备。
      - **在“未验证”组中显示未验证设备** — 将所有已经存在于**设备管理**窗口中但不存在于导入的允许设备列表中的已注册移动设备移动到**未验证**组。

注意

如果使用“设备验证”，移动安全会根据您使用的允许设备列表将所有移动设备重新分组。

6. 单击**保存**。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

自定义移动安全使用条款

可以为下载、安装和使用移动安全客户端的用户自定义**使用条款**。

过程

1. 登录到管理 Web 控制台。
2. 单击**管理** > **设备注册设置**。
3. 在**使用条款自定义**选项卡上，单击**下载使用条款示例**并将 Eula_agreement.zip 文件保存在您的计算机中。
4. 将 Eula_agreement.zip 文件内容解压缩。
5. 使用 HTML 编辑器打开 Eula_agreement.html 文件，确保根据需要修改，然后保存文件。
6. 在**设备注册设置**窗口的**使用条款自定义**选项卡中，单击**浏览**，然后选择在此过程前面的步骤（步骤 5 第 4-12 页）中修改的文件，并单击**打开**。

   使用条款预览会更新为上传的文件内容。
7. 单击**保存**。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

配置 Active Directory (AD) 设置

趋势科技移动安全 9.5 允许您根据 Active Directory (AD) 配置用户身份验证。配置完成后，您还可以使用自己的企业 Active Directory 将移动设备添加到设备列表。

如果您不希望使用 Active Directory 进行用户身份验证，或是不希望从 Active Directory 添加用户，则无需配置此设置。

过程

1. 登录到管理 Web 控制台。
2. 单击**管理** > **Active Directory 设置**。
3. 键入主机名称或其 IP 地址、端口号以及域用户名和密码。
4. 单击**保存**。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

配置管理服务器设置

过程

1. 登录到管理 Web 控制台。
2. 单击**管理** > **管理服务器设置**。
3. 单击**连接**选项卡，并指定管理服务器名称或 IP 地址及其端口号。管理服务器的缺省端口号为 443。

   

   注意

   此窗口中的 IP 地址和端口号用于通过 Web 浏览器访问管理 Web 控制台。

4. 如果管理服务器使用代理服务器连接 Internet，在**代理**选项卡中指定代理设置：

   a. 在**代理**选项卡上，选择**使用以下管理服务器代理设置:**，并指定代理服务器名称或 IP 地址及其端口号。

b. 如果代理服务器需要身份验证，在**代理身份验证**部分键入用户标识和密码。

5. 单击**保存**。

现在，您需要使用新的 IP 地址和端口号登录管理 Web 控制台。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

配置 Exchange 服务器集成设置

过程

1. 在 **Exchange 连接器**部分下，选择**启用此选项以确保只有合规的移动设备才能访问 Exchange 服务器**。

   有关 **Exchange 服务器集成**窗口中显示的 Exchange 连接器的不同状态，请参阅Exchange 连接器状态 第 4-15 页。

2. 在 **Exchange 访问控制**下，根据需要进行如下更新：

   - 选择**自动阻止非托管设备访问 Exchange 服务器**。

     注意

     未注册到 Mobile Security 服务器的设备称为非托管设备。这包括最近注册到 Exchange 服务器的设备。

   - 选择**允许访问以下设备的公司数据(电子邮件、日历和联系人等)**，然后选择以下任一选项：

     - 仅限正常设备
     - 正常和不合规设备

注意

有关不同的移动设备注册状态，请参阅*《管理员指南》*中的*控制台信息*主题。

- 选择**自动为所有托管设备启用自动允许/阻止访问选项**。

注意

启用此选项将根据托管设备的状态自动允许或阻止访问 Exchange 服务器。

- 使用下拉列表指定被阻止的设备将在多少天之后无法访问 Exchange 服务器。

3. 单击**保存**。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

有关设置 Exchange 服务器集成的其他步骤，请参阅设置 Exchange 服务器集成 第 3-14 页。

Exchange 连接器状态

下表列出了 **Exchange 服务器集成**窗口上显示的不同 Exchange 连接器状态。

表 4-2. Exchange 连接器状态

状态	描述
正常	Exchange 连接器已与管理服务器连接。
正在等待 Exchange 连接器	管理服务器正在等待 Exchange 连接器连接到管理服务器。
警告	Exchange 连接器超过五分钟未与管理服务器连接。

状态	描述
已断开	Exchange 连接器超过九分钟未与管理服务器连接。
已禁用	Exchange 连接器已与管理服务器连接，但已在移动安全 Exchange 服务器集成设置中禁用。

配置通知和报告设置

可以配置通知源以便向管理员发送通知电子邮件消息。

过程

1. 登录到管理 Web 控制台。
2. 单击**通知和报告** > **设置**。
3. 键入**发件人**电子邮件地址、SMTP 服务器 IP 地址和端口号。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。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

有关设置移动安全客户端的其他步骤，请参阅设置移动安全客户端 第 5-3 页。

配置管理员通知

您可以配置“管理员通知和报告”设置，从而通过电子邮件接收错误消息通知和日常预设报告。

过程

1. 登录到管理 Web 控制台。

2. 单击**通知和报告** > **管理员通知和报告**。

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。完成后单击**保存**，以返回到**管理员通知和报告**窗口。

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。

4. 单击**保存**。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

验证移动安全配置

移动安全提供**配置和验证**窗口，以验证您配置的所有设置是否都正确。

过程

1. 登录到管理 Web 控制台。

2. 单击**管理** > **配置和验证**。

3. 单击**验证移动安全配置**。

后续步骤

有关下一个配置任务，请参阅初始服务器安装 第 4-3 页。

第 5 章

处理移动安全客户端

本章提供移动安全客户端支持的移动设备要求和型号，并讨论了不同平台上不同的移动安全客户端部署方法。

本章包含以下几节内容：

支持的移动设备和平台

注意

请确保移动设备可以通过 Wi-Fi、3G/GPRS，或使用主机计算机上的 Internet 连接，连接到通信服务器。

在移动设备上安装和使用移动安全移动安全代理程序（也称为移动安全代理）前，请确保移动设备满足以下要求。

移动设备的存储卡和内存要求

表 5-1. 系统要求

操作系统	内存 (MB)	存储 (MB)
Android	10	8
iOS	4	3

注意

Windows Phone 移动设备不要求安装任何移动安全客户端软件（移动安全客户端）。

设置移动安全客户端

表 5-2. 设置移动安全客户端的过程

步骤	处理措施	描述	
步骤 1	（可选）为移动设备配置通知设置。	如果要使用电子邮件向用户发送安装和注册详细信息，请执行这些步骤。	有关详细步骤，请参阅配置通知和报告设置 第 4-16 页。
步骤 2	（可选）配置移动安全在电子邮件和/或短信中发送给用户的安装消息。		此安装消息包括用户可用于访问以下载和安装 MDA 安装软件包的 URL。 有关详细步骤，请参阅配置安装消息 第 5-3 页。
步骤 3	（可选）向移动设备发送邀请。		有关详细步骤，请参阅向移动设备发送邀请 第 5-4 页。
步骤 4	在移动设备上安装 MDA。	有关详细步骤，请参阅在移动设备上安装 MDA 第 5-6 页。	
步骤 5	在移动安全管理服务器上注册 MDA。	有关详细步骤，请参阅在移动安全管理服务器中注册 MDA 第 5-10 页。	

为邀请消息配置服务器（可选）

可以设置邀请消息，以使用电子邮件向用户发送安装和注册详细信息。

如果不想使用 MDA 安装和注册邀请消息，可以跳过此节。

配置安装消息

使用**安装消息**窗口键入您要显示的消息。

此任务是设置移动安全客户端过程中的一个步骤。

请参阅 设置移动安全客户端 第 5-3 页。

过程

1. 登录到管理 Web 控制台。
2. 单击**通知和报告** > **用户通知**。
3. 单击文本**移动设备注册**，以打开**移动设备注册配置**窗口。
4. 检查相关文本框中的缺省主题、电子邮件和/或短信，并根据需要进行修改。

   注意

   编辑**消息**字段时，如果您加入标记变量 `<%DOWNLOADURL%>`，它将替换为实际 URL，以允许用户从服务器下载移动安全客户端安装文件。

   示例：`<a href=<%DOWNLOADURL%>><%DOWNLOADURL%></a>`

   注意

   电子邮件通知只发送用于下载客户端安装文件的下载链接，不会在注册窗口中自动填写服务器 IP 地址和端口号。

5. 单击**保存**。
6. 单击**通知和报告** > **用户通知**。
7. 选择**移动设备注册**并单击**保存**。

向移动设备发送邀请

此任务是设置移动安全客户端过程中的一个步骤。

请参阅 设置移动安全客户端 第 5-3 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. 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**。

移动安全向邀请的设备的用户发送邀请电子邮件。

在移动设备上安装 MDA

此任务是设置移动安全客户端过程中的一个步骤。

请参阅 设置移动安全客户端 第 5-3 页。

iOS 移动设备

可以从苹果商店为 iOS 移动设备安装 MDA。要下载和安装 MDA，转到苹果商店，搜索应用程序 **Trend Micro ENT Security**，并点击**安装**。

Android 移动设备

可以使用以下方法之一安装 Android 移动设备的 MDA：

- **安装方法 I** — 直接在移动设备上从 Google Play 商店下载和安装 MDA。在 Google Play 上搜索**趋势科技移动安全企业版**，然后从趋势科技下载和安装**移动安全企业版**应用程序。
- **安装方法 II** — 直接在移动设备上从管理服务器下载和安装 MDA。有关步骤，请参阅安装方法 II 第 5-7 页。
- **安装方法 III** — 使用 Web 浏览器在计算机上下载 MDA 安装包，然后将其传输到移动设备并进行安装。有关步骤，请参阅安装方法 III 第 5-8 页。
- **安装方法 IV** — 使用移动设备管理控制台在计算机上下载 MDA 安装包，然后将其传输到移动设备并进行安装。有关步骤，请参阅安装方法 IV 第 5-9 页。

发送给用户的缺省邀请电子邮件将指示用户如何从 Google Play 商店下载和安装 MDA 应用程序（方法 I）。如果希望用户使用另一种方法安装该应用程序，请修改发送给用户的邀请电子邮件。请参阅*《管理员指南》*中的**配置用户通知**主题。

安装方法 I

通过此方法，您能够直接在移动设备上从 Google Play 商店下载和安装 MDA。

有关其他方法，请参阅 Android 移动设备 第 5-6 页。

过程

1. 在移动设备上，打开 Google **Play 商店**。
2. 搜索**趋势科技移动安全企业版**，然后点击搜索结果中的**移动安全企业版**。
3. 点击**安装**，然后点击**接受**启动安装过程。

   安装过程完成后，点击**打开**启动应用程序。

安装方法 II

通过此方法，您能够直接在移动设备上从移动安全管理服务器下载和安装 MDA。

有关其他方法，请参阅 Android 移动设备 第 5-6 页。

过程

1. 执行下列操作之一：
   - 如果您正在使用本地通信服务器或云通信服务器，打开从移动安全收到的短信或电子邮件，并在要安装 MDA 的移动设备上访问该 URL，以下载安装包。
   - 如果您正在使用本地通信服务器，请在要安装 MDA 的移动设备中使用 Web 浏览器访问以下任一 URL，以下载安装包：

http://External_domain_name_or_IP_address:HTTP_port/mobile

或

https://External_domain_name_or_IP_address:HTTPS_port/mobile

注意

- 替换您在**管理** > **通信服务器设置** > **通用设置** > **通信服务器与移动设备之间的通信设置**中配置的 **External_domain_name_or_IP_address**、**HTTP_port** 和 **HTTPS_port**。
- 如果使用 HTTPS 下载移动安全客户端，必须配置公共证书。有关详细信息，请参阅以下 URL：

  http://esupport.trendmicro.com/solution/en-us/1106466.aspx

2. 如果安装没有自动开始，启动安装包并完成安装。

安装方法 III

如果您正在使用本地通信服务器，则通过此方法，您能够使用 Web 浏览器在计算机上下载 MDA 安装包，然后将其传输到移动设备并进行安装。

有关其他方法，请参阅 Android 移动设备 第 5-6 页。

过程

1. 打开计算机，导航到以下任一 URL，以下载安装包：

   http://External_domain_name_or_IP_address:HTTP_port/mobile

   或

   https://External_domain_name_or_IP_address:HTTPS_port/mobile

注意

- 使用分配给 **External_domain_name_or_IP_address**、**HTTP_port** 和 **HTTPS_port** 的值。要检查值，请转到**管理** > **通信服务器设置** > **通用设置** > **通信服务器与移动设备之间的通信设置**。
- 如果使用 HTTPS 下载移动安全客户端，必须配置公共证书。有关详细信息，请参阅以下 URL：

  http://esupport.trendmicro.com/solution/en-us/1106466.aspx

2. 选择移动设备的操作系统，以下载安装包。
3. 将安装包复制到移动设备。
4. 启动安装包并完成安装。

安装方法 IV

通过此方法，您能够使用管理 Web 控制台在计算机上下载 MDA 安装包，然后将其传输到移动设备并进行安装。

有关其他方法，请参阅 Android 移动设备 第 5-6 页。

过程

1. 登录到管理 Web 控制台。
2. 单击**管理** > **设备注册设置**。
3. 在**代理安装**选项卡上，选择代理安装包，并单击**下载**，将 ZIP 文件下载到您的计算机。
4. 将 ZIP 文件解压缩，并将安装包复制到移动设备中。
5. 启动安装包并完成安装。

在移动安全管理服务器中注册 MDA

如果手动安装 MDA 或者自动注册过程失败，则需要手动将 MDA 注册到移动安全。

此任务是设置移动安全客户端过程中的一个步骤。

Android 移动设备

可以使用以下方法之一注册 MDA：

- 使用 QR 码注册。

  如果正在使用本地通信服务器或云通信服务器，则使用此方法。

- 使用服务器地址注册。

  如果正在使用本地通信服务器，则使用此方法。

- 不使用服务器地址注册。

  如果正在使用云通信服务器，则使用此方法。

使用 QR 码进行注册

过程

1. 启动移动设备上的移动安全客户端程序。
2. 点击**使用 QR 码注册**。
3. 在计算机或其他移动设备上打开邀请电子邮件，并使用移动设备的摄像头扫描邀请电子邮件中收到的 QR 码。
4. 如果需要，在提供的文本框中键入用户名和密码，并点击**确定**。

   移动安全客户端将在移动安全管理服务器上注册。

使用服务器地址注册

过程

1. 启动移动设备上的移动安全客户端程序。
2. 点击**手动注册**。
3. 点击**本地服务器**选项卡，在相关文本框中键入服务器地址和端口号，然后点击**下一步**。
4. 在相关文本框中键入注册密钥或用户名和密码，并点击**下一步**。

   移动安全客户端将在移动安全管理服务器上注册。

不使用服务器地址注册

过程

1. 启动移动设备上的移动安全客户端程序。
2. 点击**手动注册**。
3. 点击**云服务器**选项卡，键入邀请电子邮件中收到的注册密钥，然后点击**下一步**。

   移动安全客户端将在移动安全管理服务器上注册。

iOS 移动设备

若希望从移动安全管理服务器管理 iOS 移动设备，就必须在移动设备上安装配置概要文件。该配置概要文件必须（通过开发证书）识别您，并（通过列举唯一设备标识符）识别您的设备。

警告!

iOS 移动设备上的 Safari 必须启用 JavaScript 才能进行注册。否则无法成功注册。

可以使用以下方法之一注册 MDA：

- 使用 QR 码注册。

  如果正在使用本地通信服务器或云通信服务器，则使用此方法。

- 使用服务器地址注册。

  如果正在使用本地通信服务器，则使用此方法。

- 不使用服务器地址注册。

  如果正在使用云通信服务器，则使用此方法。

使用 QR 码进行注册

过程

1. 启动移动设备上的移动安全客户端程序。
2. 点击**使用 QR 码注册**。
3. 在计算机或其他移动设备上打开邀请电子邮件，并使用移动设备的摄像头扫描邀请电子邮件中收到的 QR 码。

   注意

   可能会弹出对话框，要求您安装为本地通信服务器配置的根 CA。如果未看到此对话框，则跳过步骤 4 到 6，直接从步骤 7 继续。

4. 点击**确定**。

   显示 **TMMSMDM-CA** 的**安装配置概要文件**窗口。

5. 在**安装配置概要文件**窗口上，点击**安装**，然后在**警告**窗口上点击**安装**。
6. 配置文件安装完成后，单击**配置文件已安装**窗口上的**完成**。
7. 如果需要，在提供的文本框中键入用户名和密码，并点击**登录**。

   显示 **MDM 注册配置文件**的**安装配置概要文件**窗口。

8. 在**安装配置概要文件**窗口上，点击**安装**，然后在弹出的确认对话框上点击**立即安装**。
9. 如果移动设备需要密码，则在显示的**输入密码**窗口键入密码，然后点击**完成**。

   显示**正在安装配置概要文件**窗口。
10. 点击**警告**确认窗口上的**安装**。

    开始配置文件安装过程。过程完成后，会显示**配置文件已安装**窗口。
11. 点击**完成**。

使用服务器地址注册

过程

1. 启动移动设备上的移动安全客户端程序。
2. 点击**手动注册**。
3. 点击**本地服务器**选项卡，在相关文本框中键入服务器地址和端口号，然后点击**注册**。
4. 在相关文本框中键入注册密钥或用户名和密码，并点击**下一步**。

   会弹出对话框，要求您安装为通信服务器配置的根 CA。

   注意

   可能会弹出对话框，要求您安装为本地通信服务器配置的根 CA。如果未看到此对话框，则跳过步骤 5 到 7，直接从步骤 8 继续。
5. 单击**确定**。

   显示 **TMMSMDM-CA** 的**安装配置概要文件**窗口。
6. 在**安装配置概要文件**窗口上，点击**安装**，然后在**警告**窗口上点击**安装**。
7. 配置文件安装完成后，单击**配置文件已安装**窗口上的**完成**。

8. 如果需要，在提供的文本框中键入用户名和密码，并点击**登录**。

   显示 **MDM 注册配置文件**的**安装配置概要文件**窗口。

9. 在**安装配置概要文件**窗口上，点击**安装**，然后在弹出的确认对话框上点击**立即安装**。

10. 如果移动设备需要密码，则在显示的**输入密码**窗口键入密码，然后点击**完成**。

    显示**正在安装配置概要文件**窗口。

11. 点击**警告**确认窗口上的**安装**。

    开始配置文件安装过程。过程完成后，会显示**配置文件已安装**窗口。

12. 点击**完成**。

不使用服务器地址注册

过程

1. 启动移动设备上的移动安全客户端程序。

2. 点击**手动注册**。

3. 在**云服务器**选项卡上，键入验证码，然后单击**注册**。

   显示 **MDM 注册配置文件**的**安装配置概要文件**窗口。

4. 在**安装配置概要文件**窗口上，点击**安装**，然后在弹出的确认对话框上点击**立即安装**。

5. 如果移动设备需要密码，则在显示的**输入密码**窗口键入密码，然后点击**完成**。

   显示**正在安装配置概要文件**窗口。

6. 点击**警告**确认窗口上的**安装**。

   开始配置文件安装过程。过程完成后，会显示**配置文件已安装**窗口。

7. 点击**完成**。

Windows Phone 移动设备

可以使用本地通信服务器地址注册 Windows Phone 移动设备：

注意

移动安全不支持对云通信服务器使用 Windows Phone。

注册 Windows Phone 8.0

过程

1. 在主窗口上，点击**设置**图标。
2. 点击“公司应用程序”。
3. 在**公司应用程序**窗口中，点击**添加帐户**，然后键入以下信息：
   - **电子邮件地址**：您的公司电子邮件地址
   - **密码**：您的域帐户密码或注册密钥
4. 点击**注册**。
5. 在下一个窗口中，输入以下信息：
   - **用户名**：如果您是使用 Active Directory 进行注册的，则键入域帐户用户名；如果是使用注册密钥注册的，则将此文本框留空。
   - **域**：如果您是使用 Active Directory 进行注册的，则键入帐户域名；如果是使用注册密钥注册的，则将此文本框留空。
   - **服务器**：**<ip_address:port>/mobile**。

注意

将 **<ip_address:port>** 替换为服务器 IP 地址和端口号。

6. 点击**注册**。
7. 如果显示**证书存在问题**消息，则点击**继续**。
8. 如果显示**创建新密码**窗口，点击**设置**，然后在**新密码**和**确认密码**文本框中输入新密码，并点击**完成**。
9. 在**已添加帐户**窗口中，点击**完成**。

注册 Windows Phone 8.1

过程

1. 在主窗口上，点击**设置**。
2. 点击**工作区**。
3. 在**工作区**窗口上，点击**添加帐户**，然后输入电子邮件地址，并点击**注册**。
4. 在下一个窗口中，在**服务器**文本框中输入以下信息：**<ip_address:port>/mobile**，然后点击**注册**。

   注意

   将 **<ip_address:port>** 替换为服务器 IP 地址和端口号。

5. 如果显示**证书存在问题**消息，则单击**继续**。
6. 在下一个窗口中，输入以下信息：
   - **密码**：您的域帐户密码或注册密钥。
   - **用户名**：如果您是使用 Active Directory 进行注册的，则键入域帐户用户名；如果是使用注册密钥注册的，则将此文本框留空。
   - **域**：如果您是使用 Active Directory 进行注册的，则键入帐户域名；如果是使用注册密钥注册的，则将此文本框留空。
7. 点击**注册**。
8. 如果显示**创建新密码**窗口，点击**设置**，然后在**新密码**和**确认密码**文本框中输入新密码，并点击**完成**。

9. 在**已添加帐户**窗口中，点击**完成**。

在移动设备上升级 MDA

升级移动安全管理服务器后，请在移动设备上执行以下步骤升级 MDA。

Android 移动设备

移动安全管理服务器升级后，服务器会自动向 Android 移动设备发送升级通知。

过程

1. 在 Android 移动设备上，点击从服务器收到的升级通知。
2. 在弹出消息中点击**确定**开始升级。

iOS 移动设备

iTunes 商店中有新版本可用时，iOS 移动设备会收到自动升级通知。

过程

1. 在 iOS 移动设备上打开**应用程序商店**。
2. 点击**更新**。
3. 在**企业移动安全**后点击**更新**开始更新。

Windows 移动设备

Windows 移动设备不需要 MDA 来连接到移动安全管理服务器。因此，不需要对 Windows 移动设备进行升级。

附录 A

网络端口配置

本附录提供安装趋势科技移动安全所需的所有网络端口配置。

本附录包含以下几个部分：

包含云通信服务器的增强安全型号的网络端口配置

如果您使用的是包含云通信服务器的增强安全型号（双服务器安装），则请为移动安全组件配置以下网络端口：

组件	网络端口	详细信息

管理服务器	打开以下端口：
	• 适于以下情况的 HTTP 端口 443：
	  • 到管理服务器的入站连接。
	  • 如果要添加来自 Google Play 的外部应用程序。
	  Google Play 商店的主机名为：play.google.com.
	  • 如果要利用趋势科技的移动应用程序信誉服务 (MARS)，并查看上传的 APK 文件的安全信息。
	  MARS 服务器的主机名为：rest.mars.trendmicro.com
	注意
	这是缺省 HTTPS 端口号。如果要更改要用于管理服务器的 HTTPS 端口号，请参阅配置管理服务器设置 第 4-13 页，获取详细信息。
	• 适于以下情况的 HTTP 端口 80：
	  • 使用授权服务器
	  使用授权服务器的主机名为：licenseupdate.trendmicro.com
	  • 如果使用趋势科技 ActiveUpdate 服务器作为更新源。
		用于访问移动安全管理 Web 控制台。

组件	网络端口	详细信息
	ActiveUpdate 服务器的主机名为 mobilesecurity.activeupdate.trendmicro.com。	

管理服务器	打开以下端口：
	• 适于以下情况的 HTTP 端口 80 和 HTTPS 端口 443：
	  • 到云通信服务的出站连接
	  • 如果要添加来自苹果应用程序商店的外部 iOS 应用程序
	  苹果应用程序商店的主机名为：itunes.apple.com.
	  • 如果要针对 iOS 移动设备进行基于类别的应用程序控制
	在防火墙例外中添加以下两个云通信服务主机：
	• ccs01.trendmicro.com
	• ccs02.trendmicro.com
		用于访问移动安全管理 Web 控制台。

简单证书注册协议 (SCEP) 服务器	打开通信服务器和 iOS 移动设备的 HTTP 端口 80。	用于进行 iOS 移动设备注册。 如果您不使用 SCEP 服务器来管理 iOS 移动设备，则无需使用此端口。
SQL Server	打开以下端口： • 管理服务器的 TCP 端口 1433。 • 管理服务器的 UDP 端口 1434。 **注意** 这是连接 SQL Server 的缺省 TCP 端口。但是如有需要，也可以使用其他端口来连接 SQL Server。	在管理服务器与远程 SQL Server 之间建立连接。

包含本地通信服务器的增强安全型号的网络端口配置

如果您使用的是包含本地通信服务器的增强安全型号（双服务器安装），则请为移动安全组件配置以下网络端口：

组件	网络端口	详细信息

管理服务器	打开以下端口：
	• 适于以下情况的 HTTP 端口 443：
	  • 到管理服务器的入站连接。
	  • 如果要添加来自 Google Play 的外部应用程序。
	  Google Play 商店的主机名为：play.google.com.
	  • 如果要利用趋势科技的移动应用程序信誉服务 (MARS)，并查看上传的 APK 文件的安全信息。
	  MARS 服务器的主机名为：rest.mars.trendmicro.com
	注意
	这是缺省 HTTPS 端口号。如果要更改要用于管理服务器的 HTTPS 端口号，请参阅配置管理服务器设置 第 4-13 页，获取详细信息。
	• 适于以下情况的 HTTP 端口 80：
	  • 使用授权服务器
	  使用授权服务器的主机名为：licenseupdate.trendmicro.com
	  • 如果使用趋势科技 ActiveUpdate 服务器作为更新源。
		用于访问移动安全管理 Web 控制台。

组件	网络端口	详细信息
	ActiveUpdate 服务器的主机名为 mobilesecurity.activeupdate.trendmicro.com。	

管理服务器	打开以下端口：
	• 适于以下情况的 HTTP 端口 80 和 HTTPS 端口 443：
	  • 如果要添加来自苹果应用程序商店的外部 iOS 应用程序
	  苹果应用程序商店的主机名为：itunes.apple.com.
	  • 如果要针对 iOS 移动设备进行基于类别的应用程序控制
		用于访问移动安全管理 Web 控制台。

通信服务器	打开 HTTP 端口 8080。 **注意** 这是双服务器配置的缺省 HTTP 端口号。在安装过程中，如果要更改移动设备与通信服务器通信所使用的 HTTP 端口号，请参阅配置通用通信服务器设置 第 4-6 页，获取详细信息。	用于实现移动设备与通信服务器之间的通信。
	打开 HTTPS 端口 4343。 **注意** 这是双服务器配置的缺省 HTTPS 端口号。	用于实现移动设备与通信服务器之间的安全通信。
	打开苹果推送通知服务 (APNs) 服务器的 TCP 端口 2195。苹果推送通知服务的主机名为 `gateway.push.apple.com`。	启用苹果的苹果推送通知服务服务器，以管理 iOS 移动设备。 如果您不使用苹果推送通知服务服务器来管理

组件	网络端口	详细信息
		iOS 移动设备，则无需使用此端口。
	打开 TCP 端口 4343。这是可以建立管理服务器到通信服务器的入站连接的缺省端口。在安装过程中，如果要更改移动设备与通信服务器通信所使用的 HTTP 端口号，请参阅配置通用通信服务器设置 第 4-6 页，获取详细信息。	在管理服务器与通信服务器之间建立连接。
	打开 TCP 端口 443。	在本地通信服务器与云通信服务器之间建立连接。
Active Directory	打开以下任一端口： • 管理服务器的 TCP 端口 389（域控制器） • 管理服务器的 TCP 端口 3268（全局类别）	用于实现使用 Active Directory 进行的用户身份验证。 如果您不使用 Active Directory 对用户进行身份验证或导入用户，则无需使用此端口。
简单证书注册协议 (SCEP) 服务器	打开通信服务器和 iOS 移动设备的 HTTP 端口 80。	用于进行 iOS 移动设备注册。 如果您不使用 SCEP 服务器来管理 iOS 移动设备，则无需使用此端口。
SQL Server	打开以下端口： • 管理服务器的 TCP 端口 1433 • 管理服务器的 UDP 端口 1434 **注意** TCP 端口 1433 是连接 SQL Server 的缺省端口。但是如有需要，也可以使用其他 TCP 端口来连接 SQL Server。	在通信服务器和管理服务器与远程 SQL Server 之间建立连接。

基本安全型号的网络端口配置

如果您使用的是基本安全型号（单服务器安装），则请为移动安全组件配置以下网络端口：

组件	网络端口	详细信息

管理服务器和本地通信服务器	打开以下端口：
	• 适于以下情况的 HTTP 端口 443：
	  • 到移动安全管理服务器的入站连接。
	  • 如果要添加来自 Google Play 的外部应用程序。
	  Google Play 商店的主机名为：play.google.com.
	  • 如果要利用趋势科技的移动应用程序信誉服务 (MARS)，并查看上传的 APK 文件的安全信息。
	  MARS 服务器的主机名为：rest.mars.trendmicro.com
	注意
	这是缺省 HTTPS 端口号。如果要更改要用于管理服务器的 HTTPS 端口号，请参阅配置管理服务器设置 第 4-13 页，获取详细信息。
	• 适于以下情况的 HTTP 端口 80：
	  • 使用授权服务器
	  使用授权服务器的主机名为：licenseupdate.trendmicro.com
	  • 如果使用趋势科技 ActiveUpdate 服务器作为更新源。
		用于访问移动安全管理 Web 控制台的用户。

组件	网络端口	详细信息
	ActiveUpdate 服务器的主机名为 mobilesecurity.activeupdate.trendmicro.com。	

管理服务器和本地通信服务器	打开以下端口：
	• 适于以下情况的 HTTP 端口 80 和 HTTPS 端口 443：
	  • 如果要添加来自苹果应用程序商店的外部 iOS 应用程序
	  苹果应用程序商店的主机名为：itunes.apple.com.
	  • 如果要针对 iOS 移动设备进行基于类别的应用程序控制
		用于访问移动安全管理 Web 控制台的用户。

管理服务器和本地通信服务器	打开 HTTP 端口 8080。 **注意** 这是双服务器配置的缺省 HTTP 端口号。	用于实现移动设备与移动安全通信服务器之间的通信。
	打开 HTTPS 端口 4343。 **注意** 这是双服务器配置的缺省 HTTPS 端口号。在安装过程中，如果要更改移动设备与通信服务器通信所使用的 HTTP 端口号，请参阅配置通用通信服务器设置 第 4-6 页，获取详细信息。	用于实现移动设备与移动安全通信服务器之间的安全通信。
	打开苹果推送通知服务 (APNs) 服务器的 TCP 端口 2195。苹果推送通知服务的主机名为 `gateway.push.apple.com`。	启用苹果的苹果推送通知服务服务器，以管理 iOS 移动设备。 如果您不管理 iOS 移动设备，则无需使用此端口。

组件	网络端口	详细信息
	打开 TCP 端口 443。	在本地通信服务器与云通信服务器之间建立连接。
Active Directory	打开以下任一端口： • 管理服务器的 TCP 端口 389（域控制器） • 管理服务器的 TCP 端口 3268（全局类别）	用于实现使用 Active Directory 进行的用户身份验证。 如果您不使用 Active Directory 对用户进行身份验证或导入用户，则无需使用此端口。
简单证书注册协议 (SCEP) 服务器	打开通信服务器和 iOS 移动设备的 HTTP 端口 80。	用于进行 iOS 移动设备注册。 如果您不使用 SCEP 服务器来管理 iOS 移动设备，则无需使用此端口。
SQL Server	打开以下端口： • 移动安全管理服务器的 TCP 端口 1433。 • 移动安全管理服务器的 UDP 端口 1434。 **注意** 这是连接 SQL Server 的缺省 TCP 端口。但是如有需要，也可以使用其他端口来连接 SQL Server。	在移动安全管理服务器与远程 SQL Server 之间建立连接。

附录 B

可选配置

本附件列出了您在安装趋势科技移动安全时可执行的可选配置流程。

本附录包含以下几个部分：

对 SQL Server 使用 Windows 身份验证

趋势科技建议对 SQL Server 使用 SQL Server 身份验证方法，而非 Windows 身份验证。但是，您也可以为 SQL Server 配置 Windows 身份验证。

过程

1. 在 Active Directory 服务器中创建具有移动安全数据库访问权限的用户帐户。如果已经拥有具有所需访问权限的用户帐户，则可以跳过此步骤。

   a. 在 Active Directory 服务器中创建用户帐户。

   b. 启动 SQL Server Management Studio 并连接到移动安全数据库。

   c. 从对象资源管理器的树中展开安全文件夹。

   d. 右击**登录**，然后单击**新登录**。

   e. 从左侧的**选择页面**中单击**常规**，并执行以下操作：

      i. 在**登录名**文本框中键入在此过程步骤 a 第 B-2 页 中创建的用户名并单击**搜索**。

         显示**选择用户或组**对话框。

      ii. 将用户名和域名一起（例如：*domainname**username*）键入**输入要选择的对象名称**文本框中，并单击**检查名称**。

      iii. 单击**确定**。

   f. 从左侧的**选择页面**中选择**服务器角色**，并选择以下角色：

      - public
      - sysadmin

   g. 单击**确定**。

      对象资源管理器的登录文件夹中会显示用户帐户。

2. 将移动安全管理服务器添加到与 Active Directory 服务器相同的域中。

3. 在管理服务器中，导航到**开始** > **管理员工具** > **计算机管理**，并执行以下操作。

   a. 从左侧的树中展开“本地用户和组”文件夹，然后双击**组**。

   b. 右击**管理员**并单击**属性**。

   c. 单击**常规**选项卡上的**添加**按钮，并执行以下操作：

      i. 在**登录名**文本框中键入在此过程步骤 a 第 B-2 页 中创建的用户名并单击**搜索**。

         显示**选择用户、计算机、服务、帐户或组**对话框。

      ii. 将用户名和域名一起（例如：*domainname**username*）键入**输入要选择的对象名称**文本框中，并单击**检查名称**。

      iii. 单击**确定**。

   d. 单击**管理员属性**对话框上的**确定**。

4. 在管理服务器中，转到以下位置：

   C:\Program Files\Trend Micro\ Mobile Security\

   或

   C:\Program Files(x86)\Trend Micro \Mobile Security\)

5. 在文本编辑器中打开 TmDatabase.ini。如果 TmDatabase.ini 文件不存在，使用文本编辑器创建一个文件，将其命名为 TmDatabase.ini。

6. 将以下文本添加到 TmDatabase.ini 文件：

```
ConnectionStringFormat=Provider=sqloledb;Data Source=
%server%;Initial Catalog=%database%;Integrated
Security=SSPI;
```

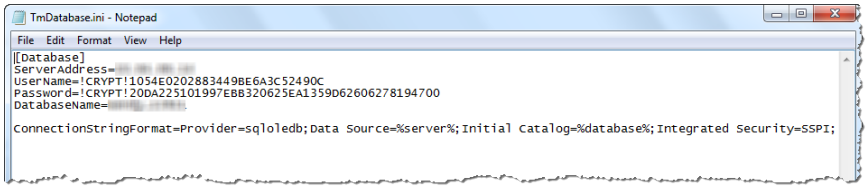

图 B-1. TmDatabase.ini 文件

7. 在管理服务器上，打开“Windows 服务”，然后双击**移动安全管理服务**。
8. 在**登录**选项卡上，选择**此帐户:**，然后键入将访问数据库的帐户名称，并在**密码**和**确认密码**字段中键入密码，然后点击**确定**。
9. 右击服务列表中的**移动安全管理服务**，然后单击**重新启动**。
10. 在管理 Web 控制台中配置数据库设置：
    a. 登录到管理 Web 控制台。
    b. 单击**管理** > **数据库设置**。
    c. 键入数据库服务器 IP 地址、用户名、密码和数据库名称。
    d. 单击**保存**。

配置通信服务器端口

趋势科技移动安全 9.5 使您能够自定义通信服务器用于与管理服务器建立连接的端口。

过程

1. 在安装通信服务器的计算机上，在文本编辑器中打开 configuration.xml 文件（位于 C:\Program Files\Trend Micro\Communication Server\ 或 C:\Program Files(x86)\Trend Micro\Communication Server\ 中）
2. 将 **mdms_https_port** 的值修改为所需的端口号。
3. 保存，然后关闭 configuration.xml 文件。
4. 打开“Windows 服务”窗口，右击**移动安全通信服务**，然后单击**重新启动**。
5. 登录到管理 Web 控制台。
6. 单击**管理** > **通信服务器设置** > **通用设置**。
7. 在**通信服务器与管理服务器之间的通信设置**部分下，将 **HTTPS 端口**的值更改为您在此过程的步骤 2 第 B-5 页 中配置的端口号。
8. 单击**保存**。

设置 SCEP

设置简单证书注册协议 (SCEP) 可以为 iOS 移动设备提供额外的安全性。

请参阅 设置 iOS 移动设备的环境（可选） 第 2-3 页。

过程

1. 安装证书颁发机构

   有关详细的证书颁发机构安装过程，请参阅以下 URL：

   http://msdn.microsoft.com/zh-cn/library/ff720354.aspx

   注意

   如果您不想使用 SCEP，则无需安装证书颁发机构。

2. 配置简单证书注册协议 (SCEP)

   若已在 Windows Server 2008 上设置了 SCEP，请安装 Windows 服务器网络设备注册服务。有关网络设备注册服务的安装与部署过程，请参阅以下 URL：

   http://esupport.trendmicro.com/solution/en-us/1060187.aspx

   或

   http://technet.microsoft.com/zh-cn/library/ff955646(WS.10).aspx

   注意

   如果您想要使用 SCEP，趋势科技建议您在 Windows Server 2008 上使用 SCEP。

3. 验证系统时钟

   确保 SCEP 服务器、通信服务器和管理服务器的系统时钟的时间设置正确。

4. 修改证书颁发机构的策略模块属性：

   a. 在安装有证书颁发机构的计算机上，打开**证书颁发机构**管理控制台。

   b. 单击**策略模块**选项卡，然后单击**属性**。

   c. 选中**遵循证书模板中的设置（如果适用）。否则，自动颁发证书**。

   d. 单击**确定**。

5. 应用以下几组规则：

   - iOS 移动设备应能够连接通信服务器。
   - 通信服务器应能够连接 SCEP 服务器。
   - 当注册到移动安全管理服务器时，iOS 移动设备应能够直接连接 SCEP 服务器。

6. 验证 SCEP 安装（可选）：

   对于在 Windows Server 2008 上运行的 SCEP，请从通信服务器访问以下 URL：

http://SCEPServerIP/certsrv/mscep_admin

注意

将 *SCEPServerIP* 替换为 URL 中的实际 SCEP 服务器 IP 地址。

若显示类似于以下内容的网页，则说明您的服务器配置正确：

图 B-2. 配置验证

注意

iOS 移动设备注册后，将能够访问以下 URL：

http://SCEPServerIP/certsrv/mscep

iOS 移动设备只需要连接 SCEP 就可进行注册，无需将此连接用于其他用途。

附录 C

生成和配置苹果推送通知服务证书

趋势科技移动安全需要拥有苹果推送通知服务 (APNs) 证书，才能管理 iOS 移动设备。本附录介绍生成苹果推送通知服务证书并将其上传至移动安全管理服务器的详细过程。

有关其他设置要求，请参阅设置 iOS 移动设备的环境（可选） 第 2-3 页。

本附录包含以下几个部分：

了解苹果推送通知服务证书

配置苹果推送通知服务 (APNs) 后，趋势科技移动安全企业版服务器便可以安全地与您的设备进行无线 (OTA) 通信。每个组织需要自己的苹果推送通知服务证书，以确保它们的设备通过苹果推送通知网络进行通信的安全机制。

当管理员索取信息或管理您的 iOS 设备时，趋势科技移动安全企业版使用您的苹果推送通知服务证书向您的设备发送通知。仅有通知才通过 APNs 服务器发送。

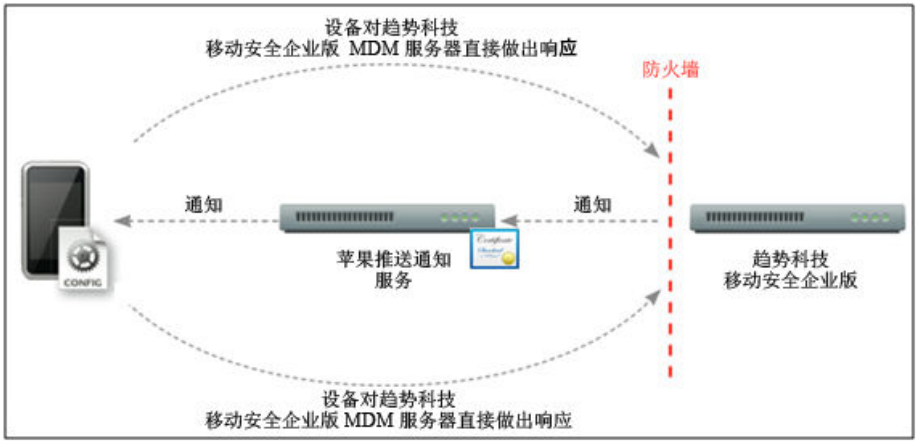

图 C-1. 通知流程

生成苹果推送通知服务证书

本节说明了为 iOS 移动设备管理生成苹果推送通知服务证书的流程。

过程

1. 从 Windows 服务器或 Mac 工作站生成证书签名请求 (CSR)。
2. 让趋势科技或苹果对 CSR 进行签名。

- **使用由趋势科技签名的证书**：趋势科技提供了简单的 CSR 签名流程：

  a. 转到趋势科技苹果推送通知服务证书签名门户，以提供企业信息、产品激活码和 CSR 副本：

  http://forms.trendmicro.com/download_trials/csr/?dom=us

  请求提交到该门户后，系统将向您发送一封包含已签名 CSR 的电子邮件。

  b. 使用经验证的苹果 ID 将已签名的 CSR 上传到苹果推送证书门户。

  Apple 将生成苹果推送通知服务证书。

- **使用由苹果签名的证书**：如果要使用由苹果签名的证书，在继续之前，确保您拥有以下内容：

  - 现有苹果企业开发者帐户 (http://developer.apple.com/programs/ios/enterprise)
  - 作为代理分配的开发者帐户角色（管理员角色不起作用）
  - Windows 服务器或 Mac OS X 工作站的管理员权限

  要使用由苹果签名的证书，请参阅使用由苹果签名的证书 第 C-10 页（适用于 Windows）或使用由苹果签名的证书 第 C-19 页（适用于 Mac）。

3. 在 Windows 服务器或 Mac 工作站上安装苹果推送通知服务证书，然后导出证书，并将其保存在计算机中。

   导出证书后，继续将此证书上传到趋势科技移动安全管理服务器。

从 Windows 服务器生成苹果推送通知服务证书

以下步骤将指导您从 Windows 服务器生成苹果推送通知服务证书。如果您已经从 Mac OS X 工作站生成了证书，您可以跳过本节，并将您的证书上传至趋势科技移动安全企业版 MDM 服务器。

步骤 1：生成证书签名请求

过程

1. 导航到**开始管理工具 Internet 信息服务 (IIS) 管理器**，并选择服务器名称。

2. 双击**服务器证书**图标。

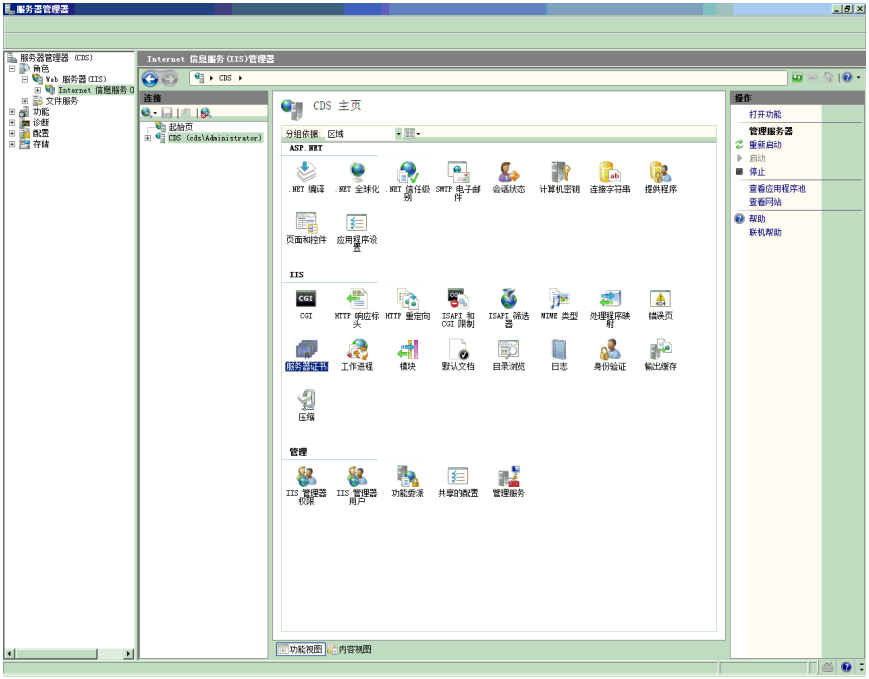

图 C-2. 访问服务器证书

注意

本文档中使用 IIS 7.0 版进行苹果推送通知服务证书配置。

3. 在右边的**处理措施**窗格中单击**创建证书请求**。

显示**申请证书**向导。

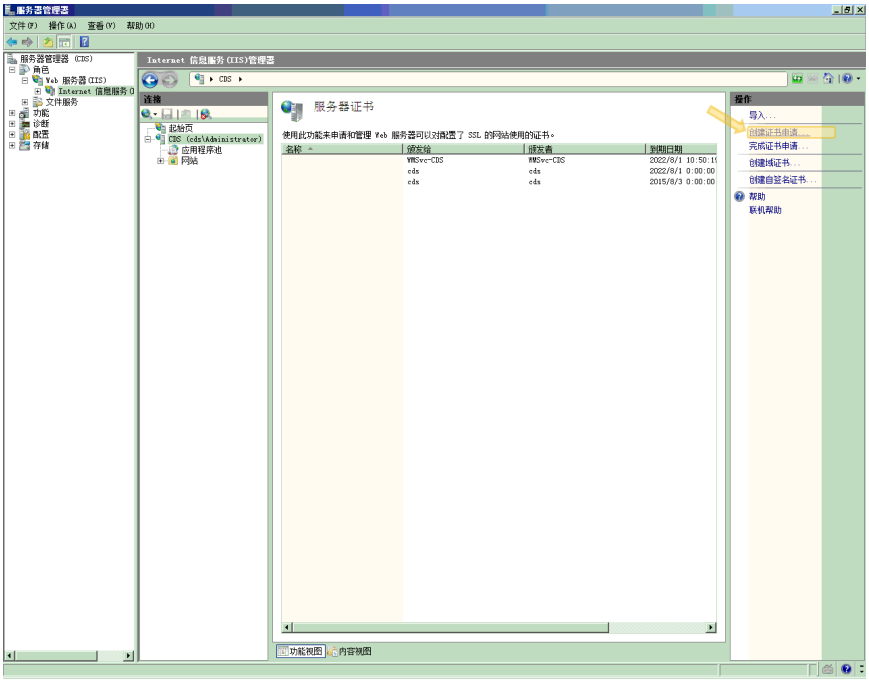

图 C-3. 启动“申请证书”向导

4. 在**可分辨名称属性**窗口中，键入以下内容：

   - **通用名称** — 与您的苹果开发者帐户相关的名称
   - **组织** - 贵组织/公司的合法注册名称
   - **组织部门** - 组织中您所在的部门名称
   - **市/县** - 贵组织所在的市或县
   - **州/省** - 贵组织所在的州或省

- **国家/地区** - 贵组织所在的国家或地区

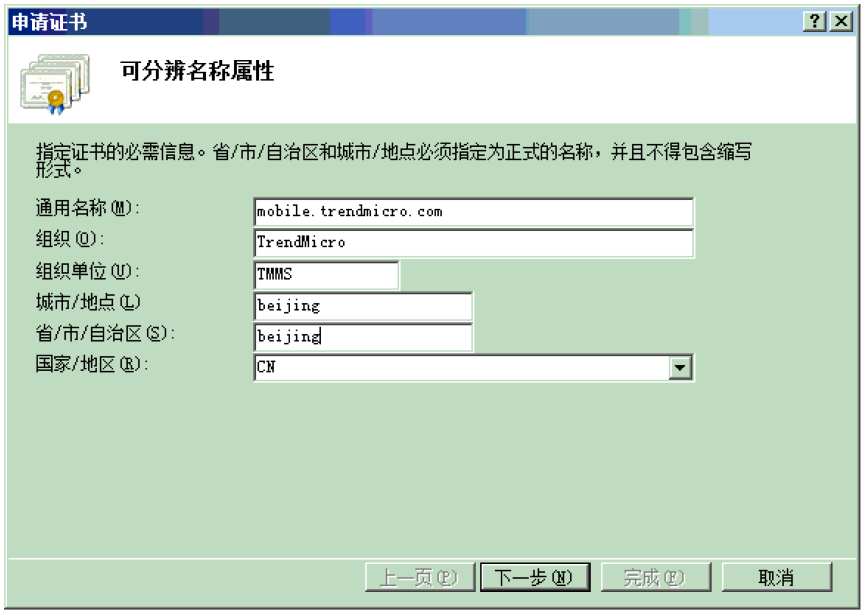

图 C-4. “可分辨名称属性”窗口

5. 单击**下一步**。

   显示**加密服务提供程序属性**窗口。

6. 在**加密服务提供程序属性**文本框中选择 **Microsoft RSA SChannel Cryptographic Provider**，在**位长**文本框中选择 **2048**，然后单击**下一步**。

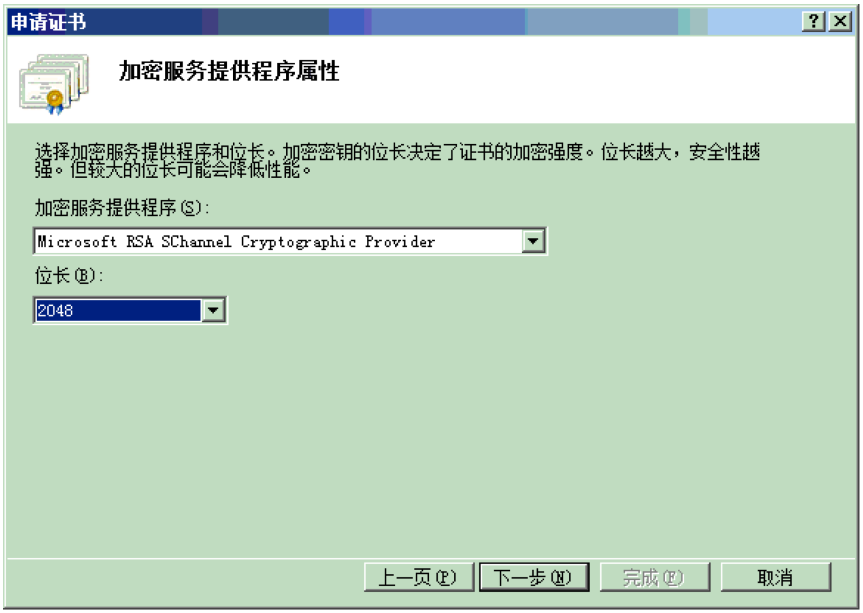

图 C-5. “加密服务提供程序属性”窗口

7. 选择证书申请文件的保存位置。

   请牢记文件名和文件的保存位置。

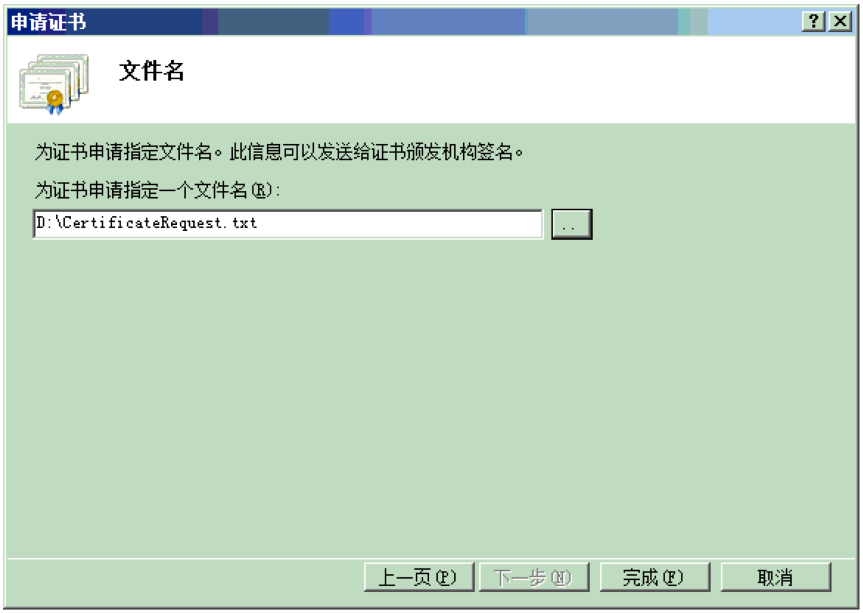

图 C-6. “文件名”窗口

8. 单击**完成**。

现在您已创建了一个 CSR 并准备将其上传至您的苹果开发门户。

重要信息

趋势科技建议您将刚刚创建的 CSR 文件保存在安全的位置。下一次续订苹果推送通知服务证书时，您需要再次使用该文件。使用不同的苹果推送通知服务证书需要将所有 iOS 移动设备再次注册到移动安全管理服务器。有关详细信息，请参阅续订苹果推送通知服务证书 第 C-24 页。

步骤 2：上传 CSR 并生成苹果推送通知服务证书

生成 CSR 之后，您便可以执行以下任一操作：

- 将 CSR 上传到趋势科技 CSR 签名门户，以获取趋势科技的签名，然后用其生成苹果推送通知服务证书。
- 将 CSR 上传到苹果开发门户，以获取苹果的签名，然后用其生成苹果推送通知服务证书。

注意

以下过程假设您使用的是由趋势科技签名的苹果推送通知服务证书。

如果要使用苹果签名的苹果推送通知服务证书，请跳过此过程，并参阅使用由苹果签名的证书 第 C-10 页（适用于 Windows）或使用由苹果签名的证书 第 C-19 页（适用于 Mac）。

过程

1. 在 Web 浏览器中导航至以下 URL：

   http://forms.trendmicro.com/download_trials/csr/?dom=us

2. 填写相应的文本框并上传刚刚生成的 CSR，然后单击**继续**。

   趋势科技将签署证书并将签名的证书返回。

3. 从趋势科技门户或从收到的电子邮件中下载签名的证书。

4. 将 CSR 上传至苹果推送证书门户：

   a. 打开 Web 浏览器并导航至以下 URL：

      https://identity.apple.com/pushcert/

   b. 输入您的苹果 ID 和密码登录。

      显示**入门**页面。

   c. 单击**创建证书**按钮。

      显示**使用条款**窗口。

   d. 单击**接受**以示同意条款。

      显示**创建新的推送证书**窗口。

e. 单击**浏览**，选择已由趋势科技签名的文件，然后单击**上传**。等待门户生成苹果推送通知服务证书 (.pem) 文件。

f. 单击**下载**将 .pem 文件保存至计算机。

g. 将已下载的 .pem 文件重命名为 .cer，然后继续步骤 3：安装苹果推送通知服务证书 第 C-11 页（适用于 Windows）。

使用由苹果签名的证书

注意

如果您已经获得由趋势科技签名的苹果推送通知服务证书，则可以跳过此过程。

过程

1. 在 Web 浏览器中导航至以下 URL：

   https://developer.apple.com/

2. 单击**成员中心**链接。
3. 输入您的苹果 ID 和密码登录。
4. 单击 **iOS 配置门户**。

   注意

   如果您未看到 iOS 配置门户，则表示该 iOS 开发的开发帐户尚未创建。

5. 在左窗格中，单击**应用程序 ID**，然后单击**新建应用程序 ID**。
6. 填写合适的字段。**捆绑标识符(应用程序 ID 后缀)标记**文本框必须为：com.apple.mgmt.mycompany.tmms.

   - 用您的公司名称替换 **mycompany**。
   - 记下**捆绑标识符(应用程序 ID 后缀)标记**值。配置移动安全管理服务器时您将需要使用此值。

7. 单击**提交**。

   您刚刚添加的**应用程序 ID** 出现在列表中。

8. 单击**配置**。

> **提示**
> 如果您未看到或无法单击**配置**，请确认您是否以代理角色登录。

9. 选择**启用苹果推送通知服务**，然后单击“生产推送 SSL 证书”的**配置**。

   如果您无法选择**启用苹果推送通知服务**，尝试使用 Safari 或 Firefox Web 浏览器，并确认您是否使用代理角色登录。

10. 显示 **SSL 证书助手**向导，其将指导您创建证书签名请求（您已经在步骤 1：生成证书签名请求 第 C-17 页中创建）。单击**继续**。

11. 单击**选择文件**并上传您在步骤 1：生成证书签名请求 第 C-17 页中创建的证书签名请求文件。（例如，CertificateSigningRequest.certSigningRequest2。）

12. 单击**生成**。

    完成后，将显示确认已生成苹果推送通知服务 SSL 证书的窗口。

13. 单击**继续**。

    显示**下载并安装苹果推送通知服务服务器 SSL 证书**窗口。

14. 单击**下载**将 .cer 文件保存至计算机，然后继续步骤 3：安装苹果推送通知服务证书 第 C-21 页（适用于 Mac）。

步骤 3：安装苹果推送通知服务证书

过程

1. 导航到**开始** > **管理工具** > **Internet 信息服务 (IIS) 管理器**，并选择服务器名称，然后双击**服务器证书**。

2. 在右边的**处理措施**窗格中单击**完成证书申请**。

显示“完成证书申请”向导。

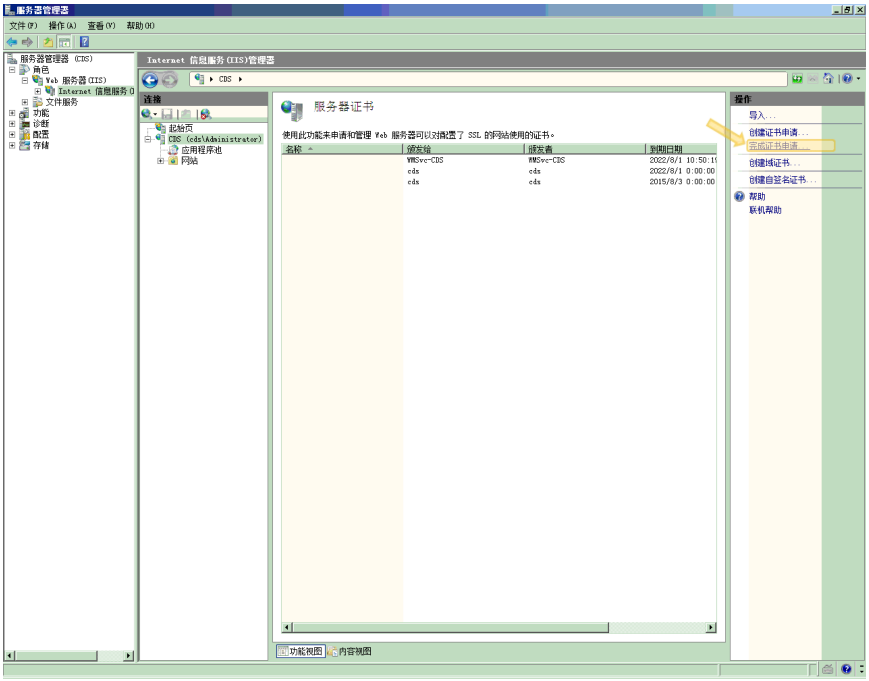

图 C-7. 完成证书申请

注意

如果您使用的是 IIS 7.5，则单击**完成证书申请**可能会显示以下错误消息：

无法建立到受信任根颁发机构的证书链。

如果出现这种情况，请参阅为苹果推送通知服务证书安装配置 IIS 7.5 第 C-16 页，了解解决此问题的过程。

---

3. 选择从苹果开发者门户上下载的 .cer 证书文件，然后在**友好名称**文本框中键入**趋势科技移动安全企业版 MDM APN**。

注意

如果要从 Mac 工作站生成证书文件，您必须将 .pem 文件扩展名手动更改为 .cer。

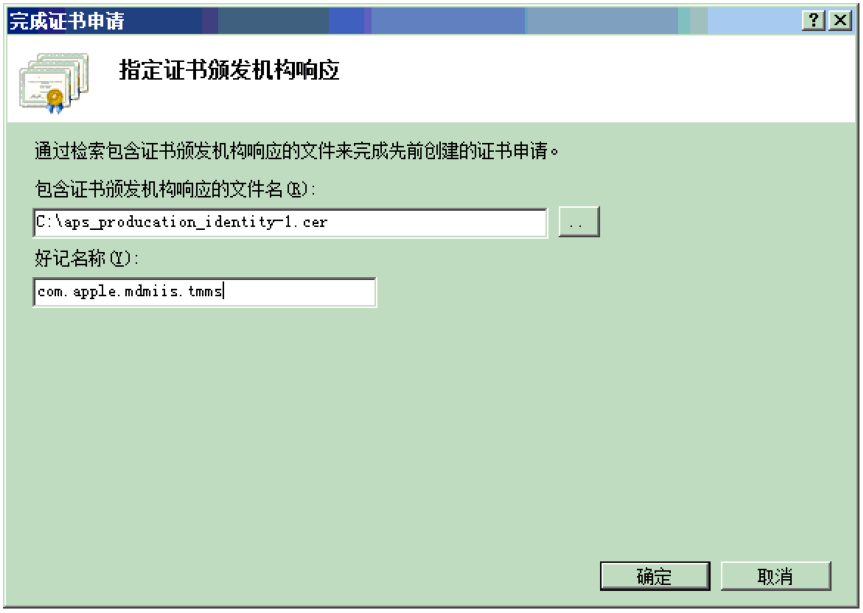

图 C-8. “指定证书颁发机构响应”窗口

提示

友好名称不属于证书本身的一部分，被服务器管理员用来简单地识别证书。

4. 单击**确定**。

   证书将安装至服务器。

5. 确认您的苹果生产推送服务证书出现在**服务器证书**列表中。如果您能看到证书，按照后续步骤导出证书并将其上传到趋势科技移动安全企业版管理服务器。

6. 在**服务器证书**列表中右击证书，然后单击**导出**。

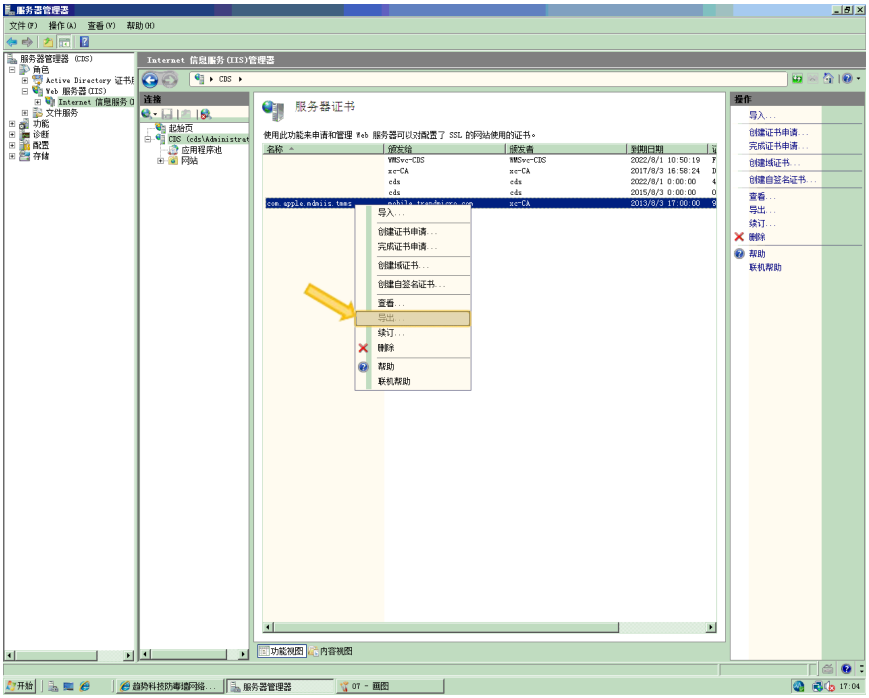

图 C-9. 导出证书

7. 选择文件的保存位置，选择一个导出密码，然后单击**确定**。

图 C-10. 指定证书的密码

提示

如果只有另存为 .cer 文件的选项，而没有 .pfx 选项，则说明您未正确导出证书。确定您选择了正确的文件导出。

注意

请牢记或妥善保存密码。将证书上传至趋势科技移动安全企业版管理服务器时需要密码。

完成所有这些步骤后，您应获得以下几项内容：

- 苹果推送通知服务证书（.pfx 格式，而非 .cer 格式）
- 导出证书时您设置的密码

现在您可以将您的证书上传至趋势科技移动安全管理服务器。有关步骤，请参阅将苹果推送通知服务证书上传至移动安全管理服务器 第 C-22 页。

为苹果推送通知服务证书安装配置 IIS 7.5

如果您使用的是 IIS 7.5，则将证书上传至 IIS 时可能会失败，并显示以下消息：

无法建立到受信任根颁发机构的证书链。

发生这种情况的原因可能有以下几种：

- 苹果推送通知服务证书由苹果根证书颁发机构 (CA) 签名，而非公用 CA 签名。
- IIS 7.5 针对受信任根 CA 执行增强检查。

过程

1. 从以下 URL 下载 **苹果根**证书和**应用程序集成**证书：

   http://www.apple.com/certificateauthority/

2. 双击 **苹果根**证书，然后在**证书**窗口上单击**安装证书**。
3. 在欢迎窗口上，单击**下一步**。
4. 选择**将所有的证书放入下列的存储**，然后单击**浏览**。
5. 在**选择证书存储**窗口中，选择**显示物理存储区**，然后单击**受信任的根证书颁发机构** > **本地计算机**，然后单击**确定**。
6. 单击**证书导入向导**窗口中的**下一步**，然后单击**完成**。
7. 针对**应用程序集成**证书重复步骤 2 第 C-16 页至步骤 5 第 C-16 页。但是在步骤 4 第 C-16 页 中，请单击**中级证书颁发机构** > **本地计算机**，而非**受信任的根证书颁发机构** > **本地计算机**。

从 Mac 工作站生成苹果推送通知服务证书

以下步骤将指导您使用 Mac OS X 工作站生成苹果推送通知服务证书。若使用的是 Windows 服务器，您可以跳过此部分，查看从 Windows 服务器生成苹果推送通知服务证书 第 C-3 页。

步骤 1：生成证书签名请求

过程

1. 在 Mac 计算机上，转到**应用程序** > **公用程序** > **密钥链访问**。
2. 在左窗格中，在**密钥链**部分选择“登录”，然后在**类别**部分选择**证书**。
3. 从顶部的菜单栏中选择**密钥链访问** > **证书助手** > **从证书颁发机构请求证书**。

   显示**证书助手**向导。
4. 在**用户电子邮件地址**和**通用名称**文本框中键入电子邮件地址和注册的苹果开发者帐户名称，选择**保存至磁盘**，然后单击**继续**。
5. 选择您想要保存该文件的位置，然后单击**保存**。

   现在您已创建了一个 CSR 并准备将其上传至您的苹果开发门户。

重要信息

趋势科技建议您将刚刚创建的 CSR 文件保存在安全的位置。下一次续订苹果推送通知服务证书时，您需要再次使用该文件。使用不同的苹果推送通知服务证书需要将所有 iOS 移动设备再次注册到移动安全管理服务器。有关详细信息，请参阅续订苹果推送通知服务证书 第 C-24 页。

步骤 2：上传 CSR 并生成苹果推送通知服务证书

生成 CSR 之后，您便可以执行以下任一操作：

- 将 CSR 上传到趋势科技 CSR 签名门户，以获取趋势科技的签名，然后用其生成苹果推送通知服务证书。
- 将 CSR 上传到苹果开发门户，以获取苹果的签名，然后用其生成苹果推送通知服务证书。

注意

以下过程假设您使用的是由趋势科技签名的苹果推送通知服务证书。

如果要使用苹果签名的苹果推送通知服务证书，请跳过此过程，并参阅使用由苹果签名的证书 第 C-10 页（适用于 Windows）或使用由苹果签名的证书 第 C-19 页（适用于 Mac）。

过程

1. 在 Web 浏览器中导航至以下 URL：

   http://forms.trendmicro.com/download_trials/csr/?dom=us

2. 填写相应的文本框并上传刚刚生成的 CSR，然后单击**继续**。

   趋势科技将签署证书并将签名的证书返回。

3. 从趋势科技门户或从收到的电子邮件中下载签名的证书。

4. 将 CSR 上传至苹果推送证书门户：

   a. 打开 Web 浏览器并导航至以下 URL：

      https://identity.apple.com/pushcert/

   b. 输入您的苹果 ID 和密码登录。

      显示**入门**页面。

   c. 单击**创建证书**按钮。

      显示**使用条款**窗口。

   d. 单击**接受**以示同意条款。

      显示**创建新的推送证书**窗口。

e. 单击**浏览**，选择已由趋势科技签名的文件，然后单击**上传**。等待门户生成苹果推送通知服务证书 (.pem) 文件。

f. 单击**下载**将 .pem 文件保存至计算机。

g. 将已下载的 .pem 文件重命名为 .cer，然后继续步骤 3：安装苹果推送通知服务证书 第 C-21 页（适用于 Mac）。

使用由苹果签名的证书

注意

如果您已经获得由趋势科技签名的苹果推送通知服务证书，则可以跳过此过程。

过程

1. 在 Web 浏览器中导航至以下 URL：

   https://developer.apple.com/

2. 单击**成员中心**链接。

3. 输入您的苹果 ID 和密码登录。

4. 单击 **iOS 配置门户**。

   注意

   如果您未看到 iOS 配置门户，则表示该 iOS 开发的开发帐户尚未创建。

5. 在左窗格中，单击**应用程序 ID**，然后单击**新建应用程序 ID**。

6. 填写合适的字段。**捆绑标识符(应用程序 ID 后缀)标记**文本框必须为：com.apple.mgmt.mycompany.tmms.

   - 用您的公司名称替换 **mycompany**。
   - 记下**捆绑标识符(应用程序 ID 后缀)标记**值。配置移动安全管理服务器时您将需要使用此值。

7. 单击**提交**。

   您刚刚添加的**应用程序 ID** 出现在列表中。

8. 单击**配置**。

   提示

   如果您未看到或无法单击**配置**，请确认您是否以代理角色登录。

9. 选择**启用苹果推送通知服务**，然后单击“生产推送 SSL 证书”的**配置**。

   如果您无法选择**启用苹果推送通知服务**，尝试使用 Safari 或 Firefox Web 浏览器，并确认您是否使用代理角色登录。

10. 显示 **SSL 证书助手**向导，其将指导您创建证书签名请求（您已经在步骤 1：生成证书签名请求 第 C-17 页中创建）。单击**继续**。

11. 单击**选择文件**并上传您在步骤 1：生成证书签名请求 第 C-17 页中创建的证书签名请求文件。（例如，CertificateSigningRequest.certSigningRequest2。）

12. 单击**生成**。

    完成后，将显示确认已生成苹果推送通知服务 SSL 证书的窗口。

13. 单击**继续**。

    显示**下载并安装苹果推送通知服务服务器 SSL 证书**窗口。

14. 单击**下载**将 .cer 文件保存至计算机，然后继续步骤 3：安装苹果推送通知服务证书 第 C-11 页（适用于 Windows）。

    注意

    要在 Windows 计算机上安装苹果推送通知服务证书，您必须将文件扩展名从 .pem 手动更改为 .cer。

步骤 3：安装苹果推送通知服务证书

过程

1. 转到下载文件的位置，双击文件，自动将它上传到密钥链访问并完成签名请求。
2. 导航到**应用程序** > **公用程序** > **密钥链访问**。
3. 在左窗格中，在**密钥链**部分选择**登录**，然后在**类别**部分选择**证书**。
4. 确认您的苹果生产推送服务证书出现在列表中，并且当您展开它时，在下方会出现一个相关的私人密钥。如果您能看到证书，按照后续步骤导出证书并将其上传到移动安全管理服务器。

注意

如果您没有看到您的苹果推送通知服务证书或未显示私人密钥，请确认您已选择了登录密钥链，选择了证书类别，并且您的证书密钥已扩展。如果您仍无法看到您的证书，重复以上所有的步骤。

5. 右击（或按住 Ctrl 键并单击）私人密钥并单击**导出**。
6. 选择文件名和您想要保存文件的位置，然后选择**个人信息交换 (.p12)** 文件格式。

提示

如果只有保存为 .cer 文件的选项，而没有 .p12 选项，则说明您没有正确导出证书。确保在最后的步骤中您选择了导出私人密钥，并且您的文件格式为**个人信息交换 (.p12)**。

7. 单击**保存**。
8. 选择导出密码，然后单击**确定**。

提示

请牢记或妥善保存密码。将证书上传到移动安全企业版管理服务器时，将需要输入密码。

完成所有这些步骤后，您应获得以下几项内容：

- 苹果推送通知服务证书（.p12 格式，而非 .cer 格式）
- 导出证书时您设置的密码

现在，您已准备好将证书上传到移动安全管理服务器。有关步骤，请参阅将苹果推送通知服务证书上传至移动安全管理服务器 第 C-22 页。

将苹果推送通知服务证书上传至移动安全管理服务器

本节说明了将苹果推送通知服务 (APNS) 证书上传至趋势科技移动安全企业版服务器的流程，上传该证书后便可以开始管理 iOS 设备。

注意

在您开始之前，确保您具备以下各项：

- 苹果推送通知服务证书文件（.pfx 或 .p12 格式，不是 .cer 格式）
- 导出证书时您设置的密码
- 趋势科技移动安全企业版 MDM 服务器的管理员帐户

过程

1. 登录到管理 Web 控制台。
2. 执行下列操作之一：

- 单击**管理** > **证书管理**，单击**添加**，从硬盘上选择苹果推送通知服务器证书，然后单击**保存**。

图 C-11. 通过证书管理添加证书

- 单击**管理** > **通信服务器设置**，单击 **iOS 设置**选项卡，然后在**证书**字段中从硬盘选择苹果推送通知服务器证书，然后单击**保存**。

图 C-12. 通过通信服务器设置添加证书

完成这些步骤后，您现在就可以管理 iOS 移动设备。

续订苹果推送通知服务证书

您需要在过期之前续订苹果推送通知服务证书，才能继续管理 iOS 移动设备。

要续订苹果推送通知服务证书，请执行与创建新证书相同的步骤。然后，访问**苹果推送证书门户**并上传新证书。

登录后，您将看到现有证书，也可能看到从之前的苹果开发者帐户导入的证书。在**证书门户**上，续订证书时的唯一差异是您需要单击**续订**。

注意

您必须具有证书门户的开发者帐户才能访问该站点。

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: TSCM97240/151028