



9.0 趋势科技™ 邮件安全网关 (IMSA)

安装指南

Hybrid SaaS 电子邮件安全



Messaging Security

趋势科技（中国）有限公司/Trend Micro Incorporated 保留对本文档以及此处所述产品进行更改而不通知的权利。在安装并使用产品之前，请阅读自述文件、发布说明和/或最新版本的适用文档，这些文档可以通过趋势科技的以下 Web 站点获得：

<http://docs.trendmicro.com/en-us/enterprise/intercan-messaging-security.aspx>

Trend Micro、Trend Micro 地球徽标、Control Manager、eManager、InterScan 和 TrendLabs 是趋势科技（中国）有限公司/Trend Micro Incorporated 的商标或注册商标。所有其他产品或公司名称可能是其各自所有者的商标或注册商标。

© 2014. 趋势科技（中国）有限公司/Trend Micro Incorporated。保留所有权利。

文档编号：MSCM96870/150302

发布日期：2014 年 10 月

受美国专利号：正在申请的专利

此文档介绍产品的主要功能，和/或提供产品环境的安装说明。在安装或使用产品之前，请仔细阅读该文档。

有关如何使用产品内的特定功能的详细信息，可通过趋势科技联机帮助中心和/或趋势科技知识库获取。

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 docs@trendmicro.com 与我们联系。

我们始终欢迎您的反馈。

目录

关于本手册

关于本手册	vii
新增内容	viii
适用读者	ix
趋势科技邮件安全网关文档	ix
文档约定	x

第 1 章：介绍趋势科技邮件安全网关

关于趋势科技邮件安全网关	1-2
IMSA 主要功能和优势	1-2
关于云端过滤	1-8
关于电子邮件加密	1-8
关于间谍软件/灰色软件	1-9
间谍软件/灰色软件如何侵入您的网络	1-10
潜在风险和威胁	1-10
关于 Web 信誉服务	1-11
关于电子邮件信誉	1-11
电子邮件信誉类型	1-11
关于趋势科技防毒墙控制管理中心	1-13
防毒墙控制管理中心支持	1-13
关于趋势科技云安全智能防护	1-15
需要新的解决方案	1-16
Trend Micro Smart Protection Network	1-16
关于灰色邮件扫描	1-17
关于命令和控制 (C&C) 联系人警报服务	1-18

第 2 章：组件描述

关于 IMSA 组件	2-2
云端过滤服务概述	2-2
发件人过滤	2-2
基于信誉的源过滤	2-2
病毒和垃圾邮件防护	2-2
关于垃圾邮件阻止解决方案	2-3
垃圾邮件阻止解决方案技术	2-3
使用垃圾邮件阻止解决方案	2-3
关于 IP 过滤	2-3
IP 分类器的工作原理	2-4
关于电子邮件信誉	2-5
电子邮件信誉类型	2-5
电子邮件信誉技术的工作原理	2-6
关于终端用户隔离 (EUQ)	2-7
关于集中式报告	2-8

第 3 章：计划部署

部署清单	3-2
网络拓扑考虑事项	3-4
使用云端过滤的 IMSA 部署	3-4
在网关处或在网关后面进行部署	3-5
在没有防火墙的情况下安装	3-8
在防火墙前面安装	3-9
在防火墙后面安装	3-10
在外围安全区域中安装	3-11
关于设备角色	3-12
关于设备服务	3-12
服务选择	3-13
使用 IP 过滤部署	3-13
了解内部通信端口	3-14
了解 POP3 扫描	3-14
POP3 扫描的要求	3-15

配置通过 IMSA 接收电子邮件的 POP3 客户端	3-15
打开 IMSA 管理控制台	3-16

第 4 章：安装 IMSA 9.0

系统要求	4-2
其他要求和工具	4-3
安装 IMSA	4-4
设置单个父设备	4-19
步骤 1：配置系统设置	4-20
步骤 2：配置部署设置	4-22
步骤 3：配置 SMTP 路由设置	4-23
步骤 4：配置通知设置	4-24
步骤 5：配置更新源	4-25
步骤 6：配置 LDAP 设置	4-27
步骤 7：配置内部地址	4-30
步骤 8：配置防毒墙控制管理中心服务器设置	4-31
步骤 9：激活产品	4-33
步骤 10：查看设置	4-34
设置子设备	4-34
验证是否已成功部署	4-36

第 5 章：从先前版本升级

从评测版升级	5-2
从 IMSA 8.5 Service Pack 1 进行升级	5-4
备份 IMSA 8.5 Service Pack 1	5-5
升级单个 IMSA	5-6
升级分布式环境	5-17
批量升级	5-20
脱机升级	5-27
还原升级	5-32
从先前版本迁移	5-33
迁移过程	5-34
从 IMSS for Windows 中迁移	5-36
从 IMSS for Linux 中迁移	5-37

从 IMSA 8.0 Patch 2、IMSA 8.2 Service Pack 2 或 IMSA 8.5 Service Pack 1 迁移	5-38
导出调试文件	5-40

第 6 章：故障排除

故障排除实用程序	6-2
组中设备间通信故障排除	6-2
子设备注册故障排除	6-3
子设备取消注册故障排除	6-4
硬件标识错误故障排除	6-5
故障排除网络连接	6-8

附录 A：技术支持

故障排除资源	A-2
趋势社区	A-2
使用支持门户	A-2
安全信息社区	A-3
威胁百科全书	A-3
与趋势科技联系	A-4
加快支持呼叫处理速度	A-4
将可疑内容发送给趋势科技	A-5
文件信誉服务	A-5
电子邮件信誉服务	A-5
Web 信誉服务	A-5
其他资源	A-6
TrendEdge	A-6
下载专区	A-6
TrendLabs	A-6

附录 B：在 VMware ESX 下为 IMSA 创建新的虚拟机

创建新的虚拟机	B-2
---------------	-----

附录 C：在 Microsoft Hyper-V 下为 IMSA 创建新的虚拟机

了解 Hyper-V 安装 C-2

 Hyper-V 的 IMSA 支持 C-2

在 Microsoft Hyper-V 上安装 IMSA C-2

 创建虚拟网络分配 C-2

 创建新的虚拟机 C-6

索引

索引 IN-1

前言

关于本手册

欢迎阅读《趋势科技™ 邮件安全网关安装指南》。本手册包含有关趋势科技邮件安全网关 (IMSA) 的功能、系统要求的信息以及安装和升级 IMSA 设置的相关说明。

有关配置 IMSA 设置的信息，请参考《IMSA 9.0 管理员指南》；有关用户界面中每个字段的详细信息，请参考管理控制台中的“联机帮助”。

包括以下主题：

- [新增内容 第 viii 页](#)
- [适用读者 第 ix 页](#)
- [趋势科技邮件安全网关文档 第 ix 页](#)
- [文档约定 第 x 页](#)

新增内容

表 1. IMSA 9.0 新增功能

新增功能	描述
传输层安全增强功能	IMSA 同时对进入和退出其中的邮件应用传输层安全 (TLS)。IMSA 提供详细的 TLS 设置，例如安全级别和密码级。
证书管理	IMSA 可让您管理 SMTP 和 HTTPS 证书以及可信的 CA 证书。
沙盒虚拟平台集成改进	IMSA 可让您定义规则，以将具有指定附件类型的电子邮件发送给沙盒虚拟平台进行分析。
社会工程学攻击防护	社会工程学攻击防护会在电子邮件中检测与社会工程学攻击相关的可疑行为。当启用社会工程学攻击防护时，趋势科技反垃圾邮件引擎会扫描传输的每封电子邮件的多个部分（包括电子邮件标头、主题行、正文、附件和 SMTP 协议信息）是否存在可疑行为。如果反垃圾邮件引擎检测到与社会工程学攻击关联的行为，则会向 IMSA 返回有关该邮件的详细信息以进一步采取处理措施以及进行策略实施或报告。
已知主机支持	已知主机包括部署在网络上的 IMSA 前面的可信邮件传输代理 (Mail Transfer Agent, MTA) 和云端过滤。IMSA 可让您指定已知主机，以便使这些主机免于 IP 过滤和灰色邮件扫描。
增强的邮件投递	IMSA 支持邮件交换器记录 (MX 记录) 查找和静态路由两种邮件投递方法，因此可提供更强大的负载平衡和故障转移功能。
增强的数据丢失防护 (DLP)	IMSA 支持基于多个数据标识符的预定义和自定义 DLP 合规性模板。
灰色邮件	灰色邮件是指请求的批量电子邮件，但它们不属于垃圾邮件。IMSA 会分开管理来自常见垃圾邮件的灰色邮件，以使管理员能够识别灰色邮件。灰色邮件例外列表中指定的 IP 地址将绕过扫描。

新增功能	描述
域名密钥识别邮件 (DKIM) 签名	IMSA 支持对传出电子邮件使用 DKIM 签名。

适用读者

本 IMSA 文档是面向大中型企业的 IT 管理员而编写的。本文档假定读者已深入了解电子邮件网络方面的知识，包括与以下各项相关的详细信息：

- SMTP 和 POP3 协议
- 邮件传输代理 (MTA)，例如 Postfix 或 Microsoft™ Exchange
- LDAP
- 数据库管理
- 传输层安全

本文档假定读者没有任何防病毒或反垃圾邮件技术的知识。

趋势科技邮件安全网关文档

IMSA 包含以下文档：

管理员指南

通过提供有关如何配置和管理 IMSA 的安装后指导信息来帮助您启动和运行 IMSA。

安装指南

包含对 IMSA 功能和系统要求的说明，并提供如何在各种网络环境中部署和升级 IMSA 的指导信息。

联机帮助

提供有关各字段以及如何通过用户界面配置所有功能的详细说明。要访问联机帮助，请打开 Web 管理控制台，然后单击帮助图标。

自述文件

包含其他文档可能未涵盖的最新产品信息。主题包括功能描述、安装提示、已知问题以及产品发布历史。

通过以下网址可以获得这些文档：

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

文档约定

本文档使用以下约定：

表 2. 文档约定

约定	描述
大写	首字母缩写词、缩写、特定命令名称以及键盘上的键名
粗体	菜单和菜单命令、命令按钮、选项卡和选项
<i>斜体</i>	对其他文档的引用
等距	示例命令行、程序代码、Web URL、文件名和程序输出
导航 > 路径	访问特定窗口的导航路径 以 文件 > 保存 为例，请在界面上单击 文件 ，然后单击 保存
 注意	配置注意事项
 提示	建议或推荐
 重要信息	有关必需或缺省配置设置及产品限制的信息
 警告!	关键操作和配置选项

第 1 章

介绍趋势科技邮件安全网关

本章介绍趋势科技邮件安全网关特性、功能和技术，并提供有关其他可增强反垃圾邮件功能的趋势科技产品的基本信息。

包括以下主题：

- [关于趋势科技邮件安全网关 第 1-2 页](#)
- [IMSA 主要功能和优势 第 1-2 页](#)
- [关于云端过滤 第 1-8 页](#)
- [关于电子邮件加密 第 1-8 页](#)
- [关于间谍软件/灰色软件 第 1-9 页](#)
- [关于 Web 信誉服务 第 1-11 页](#)
- [关于电子邮件信誉 第 1-11 页](#)
- [关于趋势科技防毒墙控制管理中心 第 1-13 页](#)
- [关于趋势科技云安全智能防护 第 1-15 页](#)
- [关于灰色邮件扫描 第 1-17 页](#)
- [关于命令和控制 \(C&C\) 联系人警报服务 第 1-18 页](#)

关于趋势科技邮件安全网关

趋势科技邮件安全网关 (IMSA) 将多层垃圾邮件防护和防网络钓鱼与屡获殊荣的防病毒和防间谍技术集成在一起。内容过滤可以实施合规性并防止数据泄漏。该易于部署的产品基于可集中式管理的高度可扩展平台实施，使得管理工作变得更为轻松。此产品在高性能和持久安全性方面进行了优化，因此可以提供全面的网关电子邮件安全防护。

IMSA 主要功能和优势

下表概述了 IMSA 可为您的网络提供的主要功能和优势。

表 1-1. 主要功能和优势

功能	说明	优势
数据和系统保护		
邮件的云端过滤	云端过滤与 IMSA 集成，在电子邮件通信到达您的网络之前扫描所有电子邮件通信。	云端过滤可防止大多数垃圾邮件和恶意邮件（高达总邮件通信的 90% ）到达您的网络。
电子邮件加密	趋势科技电子邮件加密与 IMSA 集成，对进入及离开网络的所有电子邮件通信进行加密和解密。	趋势科技电子邮件加密使 IMSA 能够加密所有离开网络的电子邮件。通过加密所有离开网络的电子邮件，管理员可以防止泄露敏感数据。
高级反恶意软件保护	高级威胁扫描引擎 (ATSE) 结合使用基于特征码的扫描和主动型启发式扫描，以检测文档利用及针对性攻击中使用的其他威胁。	ATSE 可识别已知与未知的高级威胁，从而使您的系统免受尚未添加到特征码的新威胁的攻击。
命令和控制 (C&C) 联系人警报服务	通过使用 C&C 联系人警报服务， IMSA 可以检查邮件头中的发件人、收件人和回复地址以及邮件正文中的 URL ，以确认这些信息是否与已知的 C&C 对象匹配。	C&C 联系人警报服务为 IMSA 提供了增强的检测和警报功能，能够减轻高级持久威胁和针对性攻击造成的损失。

功能	说明	优势
灰色邮件	灰色邮件是指请求的批量电子邮件，但它们不属于垃圾邮件。IMSA 会将营销邮件、新闻稿和社交网络通知检测为灰色邮件。	IMSA 会分开管理来自常见垃圾邮件的灰色邮件，以使管理员能够识别灰色邮件。灰色邮件例外列表中指定的 IP 地址将绕过扫描。
合规性监管服务	管理员可使用新的缺省策略扫描条件 <i>合规性模板</i> 满足政府的监管要求。	合规性模板为管理员提供合规性监管服务。有关可用模板的详细信息列表，请参阅 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx 。
云安全扫描	云安全扫描有助于更高效地执行扫描处理，因为它将以往存储在 IMSA 服务器上的大量威胁特征码分流到云端。	云安全扫描可利用云安全智能防护网络实现以下功能： • 在云端提供快速、实时安全状态查询功能 • 缩短防范新兴威胁所需的时间 • 降低服务器上的内存消耗
IntelliTrap	病毒编程人员经常会尝试使用不同的文件压缩算法规避病毒过滤。IntelliTrap 可对这些压缩文件进行启发式评估。 由于 IntelliTrap 可能会将非威胁文件识别为安全风险，因此趋势科技建议在 IntelliTrap 启用时隔离此类别的邮件附件。此外，如果您的用户经常交换压缩文件，您可能希望禁用此功能。 缺省情况下，IntelliTrap 作为防病毒策略的扫描条件之一启用，并配置为隔离可能被归类为安全危险的邮件附件。	IntelliTrap 可帮助降低使用不同文件压缩算法压缩的病毒通过电子邮件进入网络的风险。
内容管理	IMSA 分析进入和离开网络的电子邮件及其附件的内容是否适当。	您认为不适当的内容（如个人通信、大型附件等）可使用 IMSA 有效阻止或延后。

功能	说明	优势
实时统计数据 和监控	管理员可以在管理控制台监控所有 IMSA 设备（在同一组内）的扫描性能和 IP 过滤性能。	IMSA 为管理员提供系统概览，使管理员在最先出现邮件处理问题迹象时就能够知晓。详细的日志记录可帮助管理员在问题变严重之前积极进行处理。
针对其他电子邮件威胁进行防护		
DoS 攻击	通过使用大型附件对邮件服务器进行泛滥攻击或发送含有多种病毒或递归压缩文件的邮件，具有恶意目的的个人可干扰邮件处理。	IMSA 允许您配置希望在 SMTP 网关处阻止的邮件特性，从而降低 DoS 攻击的几率。
恶意电子邮件 内容	多种文件附件（如，可执行程序 and 带有嵌入宏的文档）可能包含病毒。带有 HTML 脚本文件、 HTML 链接、 Java applet 或 ActiveX 控件的邮件也可能执行有害操作。	IMSA 允许您配置可通过 SMTP 网关的邮件类型。
服务降级	许多组织中都存在非业务相关电子邮件通信问题。垃圾邮件可占用网络带宽并影响员工工作效率。部分员工使用公司邮件系统发送个人邮件、传输大型多媒体文件或在工作时间做私事。	大多数公司都拥有适当的邮件系统使用策略— IMSA 提供的工具可促进并确保符合现有策略。
法律责任和商业 信誉	不恰当使用电子邮件也能将公司置于法律责任风险中。员工可能参与性骚扰、种族骚扰或其他违法活动中。不忠实的员工可能使用公司邮件系统泄露机密信息。从公司的邮件服务器发出的不适当邮件可损害公司声誉，即使邮件中表达的观点并不是公司的观点也会如此。	IMSA 提供监控和阻止工具，可帮助降低允许含有不适当或机密材料的邮件通过网关的风险。

功能	说明	优势
群发邮件病毒遏制	清除可自动通过公司邮件系统传播仿冒邮件的电子邮件病毒费用昂贵并且可能造成用户恐慌。 IMSA 检测到群发邮件病毒时，对此类病毒执行的处理措施与对其他种类病毒执行的处理措施不同。 例如，如果 IMSA 检测到含有重要信息的 Microsoft Office 文档中存在宏病毒，您可以将程序配置为隔离邮件而不是删除整个邮件，以确保重要信息不会丢失。但是，如果 IMSA 检测到群发邮件病毒，程序可自动删除整个邮件。	通过自动删除含有群发邮件病毒的邮件，您就可以不使用服务器资源扫描、隔离或处理邮件以及没有补偿值的文件。 已知群发邮件病毒的标识在群发邮件病毒码中，TrendLabsSM ActiveUpdate 服务器会对群发邮件病毒码进行更新。通过选择自动删除这些类型的病毒及其电子邮件容器，您可以节省资源、避免有关员工致电咨询台以及省去爆发后的清除工作。
对间谍软件和其他类型的灰色软件进行防护		
间谍软件和其他类型的灰色软件	除了病毒，您的客户端还面临来自间谍软件、广告软件和拨号程序等潜在威胁的风险。有关详细信息，请参阅关于间谍软件/灰色软件 第 1-9 页。	IMSA 能够保护您的环境免受间谍软件和其他类型灰色软件的损害，能够大幅降低您组织的安全、保密和法律风险。
集成式反垃圾邮件功能		
垃圾邮件阻止解决方案 (SPS)	垃圾邮件阻止解决方案 (SPS) 是趋势科技的授权产品，可为其他趋势科技产品提供垃圾邮件检测服务。要使用 SPS，请获取 SPS 激活码。有关详细信息，请联系您的销售代表。 SPS 的工作原理是，使用可在注册并激活 SPS 许可证时自动变为活动的内置垃圾邮件过滤程序。	垃圾邮件阻止解决方案 (SPS) 使用的检测技术基于精密的内容处理和统计分析。与识别垃圾邮件的其他方法不同的是，内容分析可提供适应力非常强的高性能实时检测，即使垃圾邮件发件人更改其技术也是如此。

功能	说明	优势
带 IP 分类器的垃圾邮件过滤和电子邮件信誉	IP 分类器是一种自学习式全面可配置功能，可主动阻止发送垃圾邮件和其他类型潜在威胁的计算机的 IP 地址。电子邮件信誉可阻止趋势科技保留在中心数据库中的已知垃圾邮件发件人的 IP 地址。  注意 请先激活 SPS，然后配置 IP 分类器和电子邮件信誉。	凭借与 IP 过滤（包括 IP 分类器和电子邮件信誉）的集成，IMSA 可在 IP 级别阻止垃圾邮件制造者。
社会工程学攻击防护	社会工程学攻击防护会在电子邮件中检测与社会工程学攻击相关的可疑行为。	当启用社会工程学攻击防护时，趋势科技反垃圾邮件引擎会扫描传输的每封电子邮件的多个部分（包括电子邮件标头、主题行、正文、附件和 SMTP 协议信息）是否存在可疑行为。如果反垃圾邮件引擎检测到与社会工程学攻击关联的行为，则会向 IMSA 返回有关该邮件的详细信息以进一步采取处理措施以及进行策略实施或报告。
管理和集成		
LDAP 和基于域的策略	如果您将 Lotus Domino™ 或 Microsoft™ Active Directory™ 等 LDAP 目录服务用于用户组定义和管理员权限，则可以配置 LDAP 设置。	使用 LDAP，您可以定义多个规则以实施您公司的电子邮件使用准则。您可以基于发件人和收件人地址为个人或组定义规则。
基于 Web 的管理控制台	管理控制台可让您便捷地配置 IMSA 策略和设置。	管理控制台可与 SSL 兼容。与 SSL 兼容意味着可以更安全地访问 IMSA。

功能	说明	优势
终端用户隔离 (EUQ)	IMSA 提供基于 Web 的 EUQ 以改进垃圾邮件管理。通过基于 Web 的 EUQ 服务，终端用户可以管理个人帐户及他们所属的分发列表的垃圾邮件隔离。IMSA 可以隔离被软件确定为垃圾邮件的邮件。EUQ 会在数据库中为这些邮件编制索引。之后，终端用户即可查看、删除或允许投递这些邮件。	凭借基于 Web 的 EUQ 管理控制台，终端用户可管理 IMSA 隔离的邮件。 使用 IMSA，用户还可以通过 EUQ 摘要中的链接将处理措施应用于隔离邮件并将发件人添加到许可发件人列表。
委派管理	IMSA 可创建不同的访问管理控制台的权限。您可以选择各个管理员登录帐户可访问控制台的哪些部分。	通过将管理角色委派给不同员工，可以促进管理职责的共同分担。
集中式报告	集中式报告可让您灵活地生成一次性（按需）报告或预设报告。	帮助您分析 IMSA 如何执行。 一次性（按需）报告可让您根据需要指定报告内容的类型。或者，您可以将 IMSA 配置为每日、每周或每月自动生成报告。
系统可用性监控	内置代理监控 IMSA 服务器的运行状况，当错误情况迫使邮件流中断时，它将通过电子邮件或 SNMP 陷阱发出通知。	在检测到系统故障时发出电子邮件和 SNMP 通知可让您立即采取纠正性处理措施并尽量缩短停机时间。
POP3 扫描	您可以从管理控制台选择启用或禁用 POP3 扫描。	除了 SMTP 网络通信之外，IMSA 还可以在网络中的邮件客户端检索 POP3 邮件时在网关扫描这些邮件。
群集体系结构	当前版本的 IMSA 采用了便于开展分布式部署的设计。	您可以将各个 IMSA 组件安装在不同计算机上，而且某些组件可以位于多台计算机上。例如，如果邮件量很大，您可以在其他服务器上安装额外的 IMSA 扫描程序组件，而且所有服务器都使用同样的策略服务。

功能	说明	优势
与沙盒虚拟平台集成	IMSA 与沙盒虚拟平台集成，该平台是一个隔离的虚拟环境，用于在 Deep Discovery Advisor 和 Deep Discovery Analyzer 中管理和分析样本。	IMSA 会将包括附件的可疑邮件发送给沙盒虚拟平台以作进一步分析。沙盒虚拟平台在隔离的虚拟环境中执行内容模拟与分析，以识别通常与多种类型的恶意软件关联的特征。尤其，沙盒虚拟平台会检查邮件附带的文件是否包含攻击代码。
与趋势科技防毒墙控制管理中心集成	趋势科技防毒墙控制管理中心 (TMCN) 是一种软件管理解决方案，无论程序的物理位置在何处或为何平台，均可让您从中心位置控制防毒和内容安全程序。本应用程序可简化企业病毒和内容安全策略管理。	趋势科技防毒墙控制管理中心提供的爆发阻止服务可降低爆发风险。当趋势科技产品检测到新的电子邮件病毒时，TrendLabs 会拟定一个使用 IMSA 中高级内容过滤程序的策略，以通过识别这些邮件中的可疑字符来阻止邮件。这些规则可在更新的病毒码文件发布前帮助降低感染几率。

关于云端过滤

云端过滤是一种云安全解决方案，此解决方案与 IMSA 进行了集成，可在云中提供主动防护，并且可保护公司范围内的虚拟设备的隐私并对其进行控制。

通过阻止网络外部的垃圾邮件和恶意软件，云端过滤最多可减少 90% 的进站电子邮件量。云端过滤与 IMSA 在网关方面进行了集成，可灵活控制敏感信息。本地隔离可确保您的电子邮件保持隐私性。电子邮件并不存储在云中。凭借云端过滤，您可以降低复杂性和总开销，以大幅节省成本。

关于电子邮件加密

趋势科技电子邮件加密使 IMSA 能够对电子邮件进行加密和解密。凭借电子邮件加密，无论电子邮件来自哪个电子邮件客户端或平台，IMSA 都能够对其进行加密和解密。趋势科技电子邮件加密上的电子邮件加密和解密受控于策略管

理器，此策略管理器使管理员能够基于多个参数（如，发件人和收件人电子邮件地址、关键词或电子邮件（或附件）中哪里含有信用卡号码）配置策略。趋势科技电子邮件加密本身是一种简单邮件传输协议 (SMTP) 接口，通过 SMTP 将电子邮件发送至配置的出站邮件传输代理 (MTA)。这样就可以轻松与其他基于电子邮件服务器的产品（内容扫描程序、邮件服务器或归档解决方案）进行集成。

关于间谍软件/灰色软件

您的客户端会受到除病毒/恶意软件以外的潜在威胁。灰色软件可能对网络上的计算机性能造成不利影响，并给您的组织带来较大的安全、保密和法律风险。

表 1-2. 灰色软件类型

类型	描述
间谍软件	收集帐户用户名和密码等数据，并将其传送给第三方
广告程序	显示广告并通过 Web 浏览器收集用户 Web 冲浪首选项等数据，以便向用户投递广告
拨号程序	更改计算机 Internet 设置，可强制计算机通过调制解调器拨打预配置的电话号码
恶作剧程序	导致计算机出现异常行为，如关闭和打开 CD-ROM 托盘以及显示多个消息框
黑客工具	帮助黑客侵入计算机
远程访问工具	帮助黑客远程访问并控制计算机
密码破解程序	帮助黑客破解帐户用户名和密码
其他	以上未提到的其他类型

间谍软件/灰色软件如何侵入您的网络

间谍软件/灰色软件经常在用户下载安装包中带有灰色软件应用程序的正版软件时侵入企业网络。

大多数软件程序包括用户在下载前必须接受的终端用户许可协议 (EULA)。通常情况下，EULA 确实包含关于应用程序及其预期用途的信息，以便收集个人信息；但用户往往忽略该信息或根本不理解这些法律术语。

潜在风险和威胁

如果您的网络中存在间谍软件/灰色软件，则有可能引发下列风险和威胁：

表 1-3. 风险类型

类型	描述
计算机性能下降	为了执行任务，间谍软件/灰色软件应用程序往往需要使用较高的 CPU 和系统内存资源。
与 Web 浏览器相关的崩溃增多	某些类型的灰色软件（如广告程序）通常用于在浏览器框架或窗口中创建弹出窗口或显示信息。根据应用程序中的代码与系统进程的互动方式，灰色程序经常会导致浏览器崩溃或冻结，甚至需要重新启动系统。
用户效率降低	由于需要频繁关闭不断弹出的广告并处理恶作剧程序带来的负面影响，用户可能会受到不必要的干扰，进而影响主要任务的执行。
网络带宽降低	间谍软件/灰色软件应用程序往往会定期将其收集到的数据发送给您网络上运行的其他应用程序，或者您网络以外的地点。
个人信息和企业信息的丢失	间谍软件/灰色软件应用程序收集的数据不全是用户所浏览网站的列表等无关紧要的信息。间谍软件/灰色软件还会收集用户在访问其银行帐户、企业帐户等个人帐户以获取网络资源时键入的用户名和密码。

类型	描述
法律责任风险加大	如果黑客获取了您网络中计算机资源的访问权，则可能会利用您的客户端计算机发起攻击，或在您网络之外的计算机上安装间谍软件/灰色软件。如果您的网络资源在非愿意的情况下参与了此类活动，则对于其他方造成的损失，您的组织可能需要承担法律责任。

关于 Web 信誉服务

趋势科技 Web 信誉技术会分析域，并根据分析得出的 URL 可信度评估结果，为 Web 站点分配一个“信誉”，因而有助于打断感染链。Web 信誉可防范基于 Web 的威胁，包括零日攻击，以免此类威胁影响到网络。趋势科技 Web 信誉技术会跟踪数百万 Web 域的生命周期，将成熟的趋势科技反垃圾邮件功能延伸到 Internet 领域。

关于电子邮件信誉

趋势科技电子邮件信誉用于在垃圾邮件进入计算机网络之前识别并阻止该垃圾邮件，方法是通过将传入邮件连接的因特网协议 (IP) 地址路由到趋势科技云安全智能防护网络，来根据内容广泛的信誉评价数据库进行验证。

电子邮件信誉类型

有两种类型的电子邮件信誉：[标准类型 第 1-11 页](#)和[高级类型 第 1-12 页](#)。

电子邮件信誉：标准

此服务针对趋势科技信誉评价数据库验证请求的 IP 地址，从而帮助阻止垃圾邮件。其中信誉评价数据库由趋势科技云安全智能防护网络提供技术支持。这个不断扩大的数据库当前包含超过 10 亿个具有信誉等级（基于垃圾邮件活

动) 的 IP 地址。趋势科技垃圾邮件调查人员会不断审核并更新这些等级以确保准确性。

电子邮件信誉：标准电子邮件信誉是基于 DNS 单个查询的服务。每当从未知主机接收到传入电子邮件时，指定电子邮件服务器都会对标准信誉数据库服务器进行 DNS 查询。如果标准信誉数据库中列有该主机，则电子邮件信誉会将该电子邮件报告为垃圾邮件。



提示

趋势科技建议将 IMSA 配置为阻止（不接收）来自标准信誉数据库所含 IP 地址的电子邮件。

电子邮件信誉：高级

电子邮件信誉：高级电子邮件信誉可以在垃圾邮件源发送数百万邮件的过程中，识别并阻止垃圾邮件源。

这是一种动态、实时的反垃圾邮件解决方案。为了提供此项服务，趋势科技不断地监视网络和通信特征，并在新垃圾邮件源出现时立即更新动态信誉数据库（通常是在发现垃圾邮件后几分钟内）。如果垃圾邮件活动迹象的停止，动态信誉数据库会相应地进行更新。

同电子邮件信誉一样：**标准电子邮件信誉：**高级电子邮件信誉是基于 DNS 查询的服务，但可以对两个不同的数据库进行两个不同的查询：标准信誉数据库和动态信誉数据库（实时进行动态更新的数据库）。这两个数据库具有不同的条目（没有重叠的 IP 地址），从而允许趋势科技保持非常高效和有效的数据库，从而对垃圾邮件的高度动态源做出快速响应。**电子邮件信誉：**高级电子邮件信誉已经阻止了客户网络中超过 80% 的总传入连接（全部为恶意连接）。根据传入电子邮件流中垃圾邮件的数量，结果会有所不同。收到的垃圾邮件越多，看到的阻止连接的百分比越高。

关于趋势科技防毒墙控制管理中心

Trend Micro™ 防毒墙控制管理中心是一种软件管理解决方案，无论程序的物理位置在何处或为何平台，均可让您从中心位置控制防毒和内容安全程序。本应用程序可简化企业病毒/恶意软件和内容安全策略管理。

- **防毒墙控制管理中心服务器：**防毒墙控制管理中心服务器指安装防毒墙控制管理中心应用程序的计算机。基于 Web 的防毒墙控制管理中心管理控制台由此服务器托管。
- **代理：**代理是指安装在被管理产品上的应用程序，其中被管理产品允许防毒墙控制管理中心管理产品。代理从防毒墙控制管理中心服务器接收命令，然后将其应用至被管理产品上。代理可从产品收集日志，并将其发送至防毒墙控制管理中心。
- **实体：**实体代表“产品目录”链接上的被管理产品。每个实体在目录树上都有图标。目录树可显示防毒墙控制管理中心控制台上驻留的所有被管理实体。

防毒墙控制管理中心支持

下表展示了 IMSA 支持的防毒墙控制管理中心功能。

表 1-4. 受支持的防毒墙控制管理中心功能

功能	描述	受支持?
双向通信	使用双向通信，IMSA 或防毒墙控制管理中心可能会发起通信进程。	否。 仅 IMSA 能够利用防毒墙控制管理中心发起通信进程。

功能	描述	受支持?
爆发阻止策略	爆发阻止策略 (OPP) 是由 TrendLabs 开发的针对爆发的快速应对策略, 该策略包含一个列表, 内容为 IMSA 为了降低 IMSA 服务器或其代理受感染几率应执行的处理措施。 趋势科技 ActiveUpdate 服务器通过防毒墙控制管理中心将此策略部署至 IMSA。	是
以查询为目的上传日志	以查询为目的将 IMSA 病毒日志、内容安全日志和电子邮件信誉日志上传至防毒墙控制管理中心。	是
单次登录	从防毒墙控制管理中心直接管理 IMSA, 无需首先登录至 IMSA 管理控制台。	否。 您需要首先登录至 IMSA 管理控制台, 然后才能从防毒墙控制管理中心管理 IMSA。
复制配置内容	从防毒墙控制管理中心将配置设置从现有 IMSA 服务器复制到新的 IMSA 服务器。	是
病毒码更新	从防毒墙控制管理中心更新 IMSA 使用的病毒码文件。	是
引擎更新	从防毒墙控制管理中心更新 IMSA 使用的引擎。	是
产品组件更新	从防毒墙控制管理中心更新补丁和修补程序等 IMSA 产品组件。	否。 有关如何更新产品组件的说明, 请参阅特定补丁或修补程序的自述文件。
通过用户界面重定向进行配置	通过可从防毒墙控制管理中心访问的 IMSA 管理控制台配置 IMSA。	是
续订产品注册	从防毒墙控制管理中心续订 IMSA 产品使用授权。	是

功能	描述	受支持?
从防毒墙控制管理中心自定义报告	防毒墙控制管理中心为电子邮件相关数据提供自定义报告和日志查询。	是
防毒墙控制管理中心代理安装/卸载	从防毒墙控制管理中心安装或卸载 IMSA 防毒墙控制管理中心代理。	否。 当您安装 IMSA 时，会自动安装 IMSA 防毒墙控制管理中心代理。要启用/禁用代理，请从 IMSA 管理控制台执行以下操作： 1. 转到管理 > 连接。 2. 单击 TMCN 服务器选项卡。 3. 要启用/禁用代理，请选中/清除启用 MCP 代理旁的复选框。
事件通知	从防毒墙控制管理中心发送 IMSA 事件通知。	是
对所有命令进行命令跟踪	跟踪防毒墙控制管理中心提交给 IMSA 的命令状态。	是

关于趋势科技云安全智能防护

趋势科技通过云安全智能防护服务提供下一代内容安全。通过在云端处理威胁信息，趋势科技云安全智能防护可降低对系统资源的需求并避免非常耗时的签名下载。

云安全智能防护服务包括以下服务：

文件信誉服务

文件信誉服务会从本地扫描引擎分离特征码文件，并向趋势科技云安全智能防护网络执行特征码文件查找。高性能内容交付网络可使检查过程中的延迟缩至最短并提供更加即时的防护。

趋势科技会持续增强文件信誉服务以改进恶意软件检测。智能反馈可使趋势科技能够使用几百万用户对文件的社区反馈来识别紧密相关的信息，从而帮助确定文件属于恶意文件的可能性。

Web 信誉服务

凭借世界上最大的信誉数据库之一，趋势科技 Web 信誉技术可基于如下因素跟踪域的可信性：存在时间、历史位置更改以及通过恶意软件行为分析发现的可疑活动标志。趋势科技将为特定页面分配信誉评分，而不是对整个站点进行分类，从而提高准确度并减少误判。

Web 信誉技术可防止用户执行以下操作：

- 访问受到危害或感染的站点
- 与用于网络犯罪的命令与控制 (C&C) 服务器通信

需要新的解决方案

传统的威胁处理方法使用按预设计划传递到客户端并存储到本地的恶意软件特征码或定义。为确保持续获得保护，您需要定期接收新的更新并将其重新加载到防恶意软件中。

虽然这种方法有效，但威胁数量会不断增加，从而降低服务器和工作站的性能以及网络带宽使用率并延长提供强大防护所需的总体时间。为了应对威胁的指数式增长速率，趋势科技开创了可将恶意软件签名的存储卸载到云端的智能方法。在此过程中，趋势科技利用相关的技术和体系结构针对大量新出现的恶意软件威胁为客户提供更强大的防护。

Trend Micro™ Smart Protection Network™

趋势科技通过趋势科技云安全智能防护网络向 IMSA 提供文件信誉服务和 Web 信誉服务。

趋势科技云安全智能防护网络是下一代云客户端内容安全架构，用于为客户提供针对安全风险和 Web 威胁的防护。它支持公司范围内及趋势科技受托管的解决方案，无论用户是在网络上、在家或在途中，都可以为其提供防护。云安全智能防护网络使用轻量级客户端访问其独特的云服务（结合了电子邮件技术、

Web 技术、文件信誉技术和威胁数据库）。随着更多产品、服务和用户访问网络，客户的防护会自动更新并增强，从而为用户创造实时的邻里监视防护服务。

云安全智能防护网络通过托管大多数恶意软件特征码定义来提供文件信誉服务。当客户端自身的特征码定义无法确定文件的风险时，它会向云安全智能防护网络发送扫描查询。

云安全智能防护网络通过托管 Web 信誉数据（以前只通过由趋势科技托管的服务器提供）来提供 Web 信誉服务。客户端会向云安全智能防护网络发送 Web 信誉查询，以检查用户正在尝试访问的 Web 站点的信誉。客户端会将 Web 站点的信誉与计算机上实施的 Web 信誉策略相关联，以确定是允许还是阻止访问该站点。

有关云安全智能防护网络的详细信息，请访问：

www.smartprotectionnetwork.com

关于灰色邮件扫描

灰色邮件是指请求的批量电子邮件，但它们不属于垃圾邮件。IMSA 会将营销邮件、新闻稿和社交网络通知检测为灰色邮件。IMSA 通过以下两种方法识别灰色邮件：

- 由电子邮件信誉服务对源 IP 地址进行评分
- 由趋势科技反垃圾邮件引擎识别消息内容



注意

请注意，当 IMSA 检测到这些类型的电子邮件时，这些邮件不会标记为垃圾邮件。

管理员可以定义规则标准，以对这些电子邮件采取处理措施。每个灰色邮件规则都有一个例外列表，此列表包含将绕过邮件过滤的地址对象。地址对象是单个 IP 地址或地址范围（IPv4 或 IPv6），或者是无类别域间路由（Classless Inter-Domain Routing, CIDR）块。

管理员可以选择通过几个途径了解网络中的灰色邮件通信。报告会显示发送和接收的灰色邮件数量最多的内部或外部发件人和收件人。管理员还可以查询详细的日志消息或查看电子邮件隔离，并且可以在必要时释放标识为允许的灰色邮件的邮件。

可以导出和导入灰色邮件例外列表。

**注意**

请确保 IMSA 可以查询外部 DNS 服务器以执行灰色邮件扫描。如果您更改了任何 DNS 服务器设置，请重启扫描程序服务器以加载新设置。

关于命令和控制 (C&C) 联系人警报服务

趋势科技命令和控制 (C&C) 联系人警报服务为 IMSA 提供了增强的检测和警报功能，能够减轻高级持久威胁和针对性攻击造成的损失。它利用趋势科技云安全智能防护网络编制、测试和评级的全球信息网络列表来检测回调地址。

通过使用 C&C 联系人警报服务，IMSA 可以检查邮件头中的发件人、收件人和回复地址以及邮件正文中的 URL，以确认这些信息是否与已知的 C&C 对象匹配。管理员可配置 IMSA 隔离此类邮件并在邮件被标记时发送通知。IMSA 会将所有检测到的电子邮件连同 C&C 对象及对这些邮件采取的措施记录到日志中。IMSA 会将这些日志发送到防毒墙控制管理中心以供查询。

第 2 章

组件描述

本章介绍了管理 IMSA 所需的要求以及该产品需要运行的各种软件组件。

包括以下主题：

- [关于 IMSA 组件 第 2-2 页](#)
- [云端过滤服务概述 第 2-2 页](#)
- [关于垃圾邮件阻止解决方案 第 2-3 页](#)
- [关于 IP 过滤 第 2-3 页](#)
- [关于电子邮件信誉 第 1-11 页](#)
- [关于终端用户隔离 \(EUQ\) 第 2-7 页](#)
- [关于集中式报告 第 2-8 页](#)

关于 IMSA 组件

IMSA 的新体系结构将产品区分为不同的组件，每个组件均在邮件处理中执行特定的任务。以下各部分提供了每个组件的概述。

云端过滤服务概述

云端过滤服务是一种由趋势科技电子邮件安全平台提供技术支持的受管电子邮件安全服务。通过借助此服务为您的入站邮件提供路径，您就可以在威胁到达网络之前保护您的域免受垃圾邮件、网络钓鱼、恶意软件和其他邮件威胁的困扰。

发件人过滤

通过许可发件人，云端过滤服务用户可以自动允许来自受信任邮件服务器或电子邮件地址的邮件。不对来自许可发件人的邮件进行垃圾邮件或源信誉检查。对来自许可发件人的邮件进行病毒扫描。

通过阻止发件人，用户可以自动阻止来自非信任源的邮件。

基于信誉的源过滤

凭借趋势科技电子邮件信誉，云端过滤服务可以针对动态、自更新信誉数据库验证电子邮件源，以阻止来自最新僵尸网络以及由垃圾邮件发送者、钓鱼网站制造者和恶意软件发布者控制的其他 IP 地址的邮件。

病毒和垃圾邮件防护

凭借趋势科技防病毒技术，云端过滤服务可以抵御感染了群发邮件蠕虫的邮件或包含特洛伊木马、间谍软件或其他恶意代码的经过特殊制作的邮件。

云端过滤服务通过检查邮件是否具有垃圾邮件特性，可以有效减少不请自来的邮件量。

关于垃圾邮件阻止解决方案

垃圾邮件阻止解决方案 (SPS) 是趋势科技的授权产品，可为其他趋势科技产品提供垃圾邮件检测服务。SPS 使用授权随附于**趋势科技杀毒专家**和**内容过滤程序**使用授权中。有关详细信息，请联系您的销售代表。

垃圾邮件阻止解决方案技术

SPS 使用的检测技术基于精密的内容处理和统计分析。与识别垃圾邮件的其他方法不同的是，内容分析可提供适应力非常强的高性能实时检测，即使垃圾邮件发件人更改其技术也是如此。

使用垃圾邮件阻止解决方案

SPS 的工作原理是，使用可在注册并激活**垃圾邮件阻止解决方案**使用授权时自动变为活动的内置垃圾邮件过滤程序。

关于 IP 过滤

IMSA 包含的可选 IP 过滤由以下两部分构成：

IP 分类器

可以配置用于分析电子邮件通信的阈值设置。当来自某个 IP 地址的网络通信违反此设置时，IP 分类器会将发件人的 IP 地址添加到其数据库中，然后阻止来自该 IP 地址的传入连接。

IP 分类器可以检测以下四种潜在 Internet 威胁：

- **垃圾邮件：**包含不受欢迎的广告内容的电子邮件。

- **病毒：**各种病毒威胁，包括特洛伊木马程序。
- **目录收集攻击 (DHA)：**垃圾邮件发送者收集有效电子邮件地址所使用的一种方法，收集方式为将有效域名与随机电子邮件名称组合起来生成随机电子邮件地址。然后，将电子邮件发送至这些生成的电子邮件地址。如果邮件投递成功，则可以确定该电子邮件地址是真实的，从而添加至垃圾邮件数据库中。
- **退回的邮件：**一种攻击，使用您的邮件服务器生成在“发件人”字段中具有目标电子邮件域的电子邮件。虚构地址发送电子邮件，当返回时，它们将泛滥攻击目标邮件服务器。

电子邮件信誉

在 IP 级别阻止来自已知垃圾邮件发件人的电子邮件。

IP 分类器的工作原理

IP 分类器可以主动识别发送包含[关于 IP 过滤](#) 第 2-3 页部分所述威胁的电子邮件的计算机的 IP 地址。您可以自定义几个标准，用于确定 IMSA 何时开始对 IP 地址采取指定措施。标准会根据潜在威胁的不同而有所差异，但通常包括 IMSA 监视 IP 地址和阈值的持续时间。

在 IMSA 接收到来自发送邮件服务器的连接请求后，将执行以下步骤：

1. FoxProxy 会查询 IP 分类器的 DNS 服务器，以查看 IP 地址是否在阻止列表中。
2. 如果 IP 地址在阻止列表中，则 IMSA 将拒绝连接请求。

如果 IP 地址不在阻止列表中，则 IMSA 将根据为 IP 分类器指定的阈值标准来分析电子邮件通信。

3. 如果电子邮件通信违反了标准，则 IMSA 会将发件人 IP 地址添加到阻止列表中。

关于电子邮件信誉

趋势科技电子邮件信誉用于在垃圾邮件进入计算机网络之前识别并阻止该垃圾邮件，方法是通过对传入邮件连接的因特网协议 (IP) 地址路由到趋势科技云安全智能防护网络，来根据内容广泛的信誉评价数据库进行验证。

电子邮件信誉类型

有两种类型的电子邮件信誉：[标准类型 第 1-11 页](#)和[高级类型 第 1-12 页](#)。

电子邮件信誉：标准

此服务针对趋势科技信誉评价数据库验证请求的 IP 地址，从而帮助阻止垃圾邮件。其中信誉评价数据库由趋势科技云安全智能防护网络提供技术支持。这个不断扩大的数据库当前包含超过 10 亿个具有信誉等级（基于垃圾邮件活动）的 IP 地址。趋势科技垃圾邮件调查人员会不断审核并更新这些等级以确保准确性。

电子邮件信誉：标准电子邮件信誉是基于 DNS 单个查询的服务。每当从未知主机接收到传入电子邮件时，指定电子邮件服务器都会对标准信誉数据库服务器进行 DNS 查询。如果标准信誉数据库中列有该主机，则电子邮件信誉会将该电子邮件报告为垃圾邮件。



提示

趋势科技建议将 IMSA 配置为阻止（不接收）来自标准信誉数据库所含 IP 地址的电子邮件。

电子邮件信誉：高级

电子邮件信誉：高级电子邮件信誉可以在垃圾邮件源发送数百万邮件的过程中，识别并阻止垃圾邮件源。

这是一种动态、实时的反垃圾邮件解决方案。为了提供此项服务，趋势科技不断地监视网络和通信特征，并在新垃圾邮件源出现时立即更新动态信誉数据库

（通常是在发现垃圾邮件后几分钟内）。如果垃圾邮件活动迹象的停止，动态信誉数据库会相应地进行更新。

同电子邮件信誉一样：标准电子邮件信誉：高级电子邮件信誉是基于 DNS 查询的服务，但可以对两个不同的数据库进行两个不同的查询：标准信誉数据库和动态信誉数据库（实时进行动态更新的数据库）。这两个数据库具有不同的条目（没有重叠的 IP 地址），从而允许趋势科技保持非常高效和有效的数据库，从而对垃圾邮件的高度动态源做出快速响应。电子邮件信誉：高级电子邮件信誉已经阻止了客户网络中超过 80% 的总传入连接（全部为恶意连接）。根据传入电子邮件流中垃圾邮件的数量，结果会有所不同。收到的垃圾邮件越多，看到的阻止连接的百分比越高。

电子邮件信誉技术的工作原理

趋势科技电子邮件信誉技术是一种基于域名服务 (DNS) 查询的服务。在 IMSA 接收到来自发送邮件服务器的连接请求后，将执行以下步骤：

1. IMSA 记录请求连接的计算机的 IP 地址。
2. IMSA 将 IP 地址转发到趋势科技电子邮件信誉 DNS 服务器并查询信誉数据库。如果 IP 地址已经被报告为垃圾邮件源，则在查询时数据库中已记录该地址。
3. 如果已经记录，则电子邮件信誉将指示 IMSA 永久或暂时阻止该连接请求。阻止请求的决定取决于垃圾邮件源的类型、其历史记录、当前活动级别和其他监测参数。

下图展示了电子邮件信誉的工作原理。

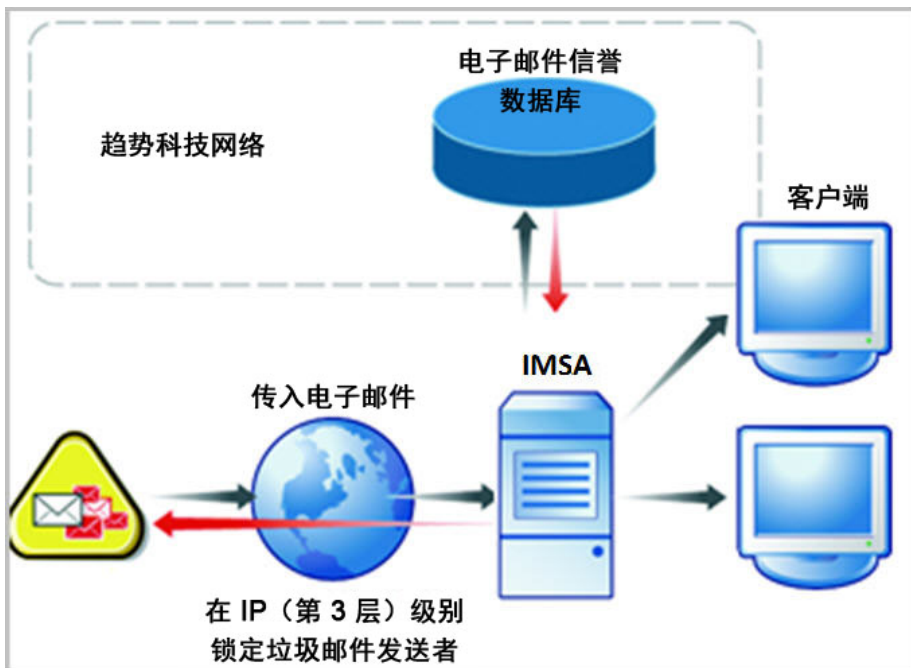


图 2-1. 电子邮件信誉的工作原理

有关趋势科技电子邮件信誉操作的详细信息，请访问 <https://ers.trendmicro.com/>。

关于终端用户隔离 (EUQ)

IMSA 提供基于 Web 的 EUQ 以改进垃圾邮件管理。通过基于 Web 的 EUQ 服务，终端用户可以管理他们自己的垃圾邮件隔离。垃圾邮件阻止解决方案（单独通过 IMSA 授权）或管理员创建的内容过滤程序确定为垃圾邮件的邮件会被

隔离。EUQ 代理会在数据库中为这些邮件编制索引，然后终端用户可对这些邮件进行查看、删除或批准投递。

关于集中式报告

集中式报告功能有助于分析 IMSA 的执行方式。您可以配置一次性报告（按需）或自动生成报告（每天、每周和每月）。

第 3 章

计划部署

本章介绍如何计划 IMSA 部署。有关执行初始配置的说明，请参阅《管理员指南》。

包括以下主题：

- [部署清单 第 3-2 页](#)
- [网络拓扑考虑事项 第 3-4 页](#)
- [关于设备角色 第 3-12 页](#)
- [关于设备服务 第 3-12 页](#)
- [了解 POP3 扫描 第 3-14 页](#)
- [打开 IMSA 管理控制台 第 3-16 页](#)
- [设置单个父设备 第 4-19 页](#)
- [设置子设备 第 4-34 页](#)
- [验证是否已成功部署 第 4-36 页](#)

部署清单

部署清单提供有关部署 IMSA 的安装前和安装后任务的逐步说明。

1. 部署 IMSA 及云端过滤

当完成时标记	任务	可选	参考资料
	使用云端过滤部署	是	使用云端过滤的 IMSA 部署 第 3-4 页

2. 确定 IMSA 的位置

当完成时标记	任务	可选	参考资料
	从网络中的下列位置选择一个您希望安装 IMSA 的位置。		
	网关处		在网关处或在网关后面进行部署 第 3-5 页
	网关后面		在网关处或在网关后面进行部署 第 3-5 页
	在没有防火墙的情况下		
	防火墙前面		
	防火墙后面		
	在外围安全区域中		

3. 计划范围

当完成时标记	任务	可选	参考资料
	决定您是希望安装单个 IMSA 设备还是多个设备。		

当完成时 标记	任务	可选	参考资料
	单个设备安装		关于设备角色 第 3-12 页
	多个 IMSA 设备		关于设备角色 第 3-12 页

4. 部署或升级

当完成时 标记	任务	可选	参考资料
	部署新 IMSA 设备或从之前的版本升级。		
	从之前的版本升级		从先前版本升级 第 5-1 页

5. 启动服务

当完成时 标记	任务	可选	参考资料
	激活 IMSA 服务，开始帮助您的网络抵御各种威胁。		
	扫描程序		《管理员指南》的“IMSA 服务”部分
	策略		
	EUQ	是	

6. 配置其他 IMSA 设置

当完成时 标记	任务	可选	参考资料
	配置各种 IMSA 设置，以启动 IMSA 并运行。		
	IP 过滤规则	是	《管理员指南》的“IP 过滤服务”部分
	SMTP 路由		《管理员指南》的“扫描 SMTP 邮件”部分

当完成时 标记	任务	可选	参考资料
	POP3 设置	是	《管理员指南》的“扫描 POP3 邮件”部分
	策略和扫描例外		《管理员指南》的“管理策略”部分
	对组件执行手动更新和配置 预设更新		《管理员指南》的“更新扫描引擎和特征码文件”部分
	日志设置		《管理员指南》的“配置日志设置”部分

7. 备份 IMSA

当完成时 标记	任务	可选	参考资料
	执行 IMSA 备份，作为对系统故障的预防措施。		
	备份 IMSA 设置		《管理员指南》的“备份 IMSA”部分。

网络拓扑考虑事项

决定您希望在现有电子邮件和网络拓扑中如何使用 IMSA。下面是处理 SMTP 网络通信的常见方案。

使用云端过滤的 IMSA 部署

云端过滤对部署 IMSA 的方式不产生任何影响。

**注意**

云端过滤将端口 9000 用作 Web 服务侦听端口。在 IMSA 的防火墙上此端口必须打开，以连接云端过滤。

但是，当添加云端过滤策略时，必须将此策略中定义的域的 MX 记录更改为云端过滤的入站地址。“云端过滤策略列表”窗口底部提供了该地址。单击 IMSA 管理控制台中的云端过滤以显示“云端过滤策略列表”窗口。

**提示**

趋势科技建议将 IMSA 的地址添加到域的 MX 记录中，并将 IMSA 的优先级设置为低于云端过滤的优先级。这样 IMSA 就能够提供电子邮件服务连续性，作为云端过滤的备份。

在网关处或在网关后面进行部署

表 3-1. 处理 SMTP 网络通信的常见方案

	单个设备	多个设备
网关处	要将 IP 过滤应用于设备，必须执行该设置。在网关处部署 IMSA，以提供防病毒、内容过滤、垃圾邮件阻止和 IP 过滤服务，其中包含网络信誉服务和 IP 分类器。请参阅图 3-1：网关处的单个 IMSA 设备 第 3-6 页。	要将 IP 过滤应用于至少一台设备，必须执行该设置。您可以启用或禁用不同设备上的服务。参见以下各项： - 图 3-3：网关处的 IMSA 组 第 3-7 页 - 服务选择 第 3-13 页
网关后面	最常见的设置。在上游 MTA 和下游 MTA 之间部署 IMSA，以提供防病毒、内容过滤和垃圾邮件阻止服务。请参阅图 3-2：网关后面的单个 IMSA 设备 第 3-7 页。	最常见的组设置。在上游 MTA 和下游 MTA 之间部署 IMSA 设备，以提供防病毒、内容过滤和垃圾邮件阻止服务。您可以启用或禁用不同设备上的服务。参见以下各项： - 图 3-4：网关后面的 IMSA 组 第 3-8 页 - 服务选择 第 3-13 页
趋势科技防毒墙控制管理中心方案		

	单个设备	多个设备
如果您有多个组，则可以使用趋势科技防毒墙控制管理中心 (TMCM) 来管理设备。		

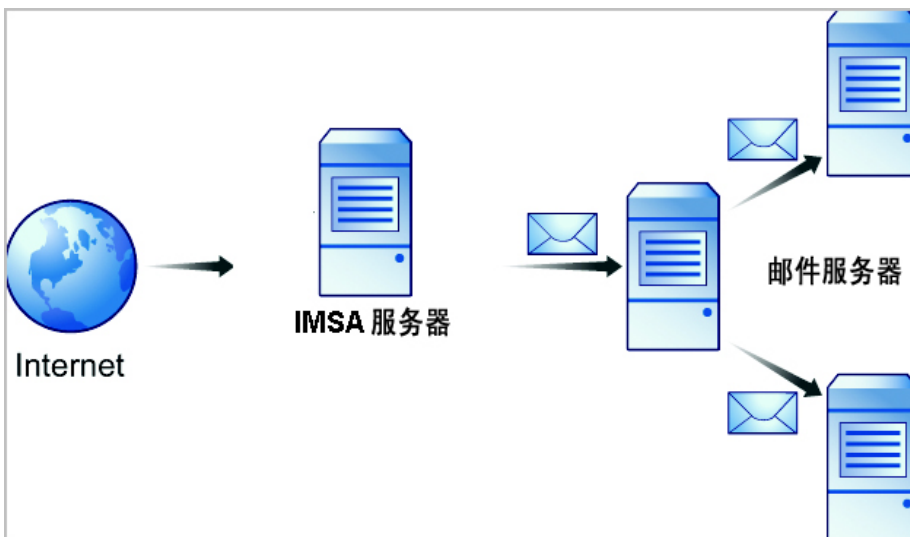


图 3-1. 网关处的单个 IMSA 设备

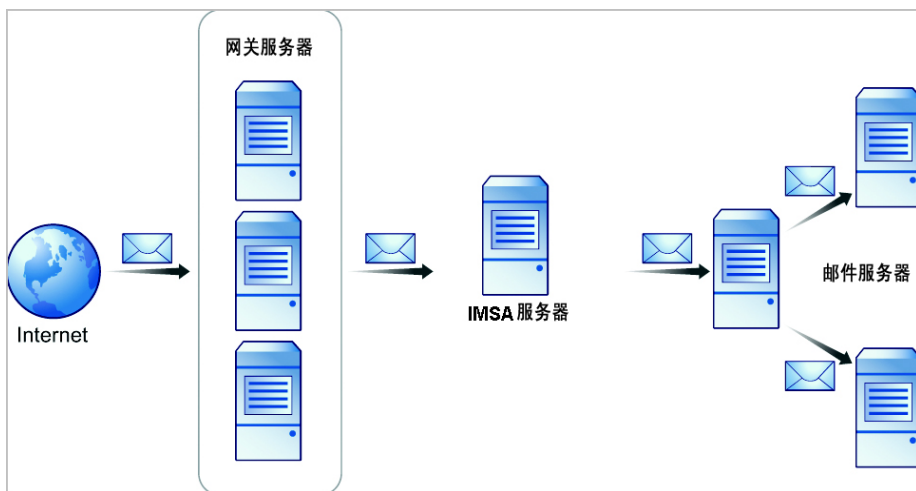


图 3-2. 网关后面的单个 IMSA 设备

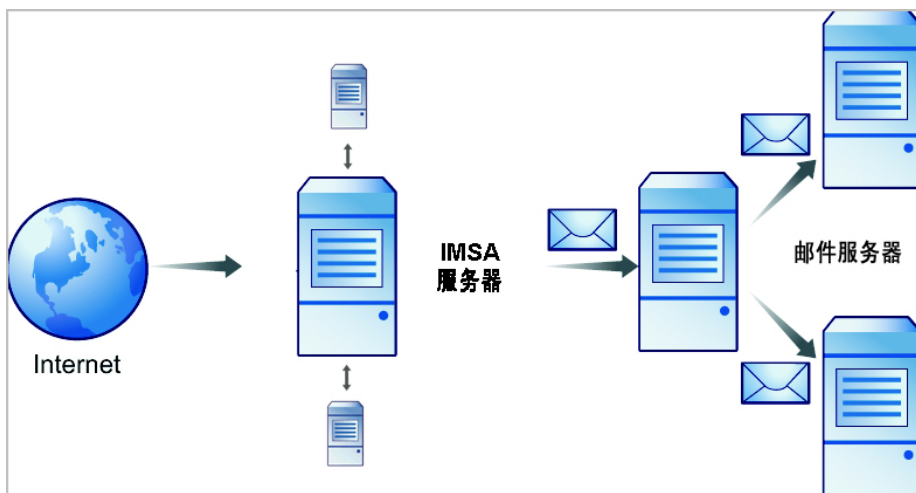


图 3-3. 网关处的 IMSA 组

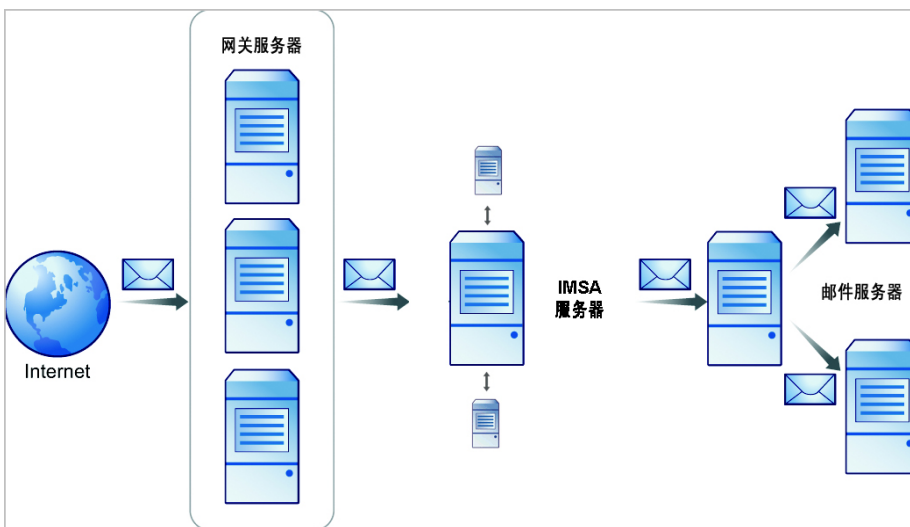


图 3-4. 网关后面的 IMSA 组

在没有防火墙的情况下安装

下图展示了当网络没有防火墙时如何部署 IMSA 和 Postfix。

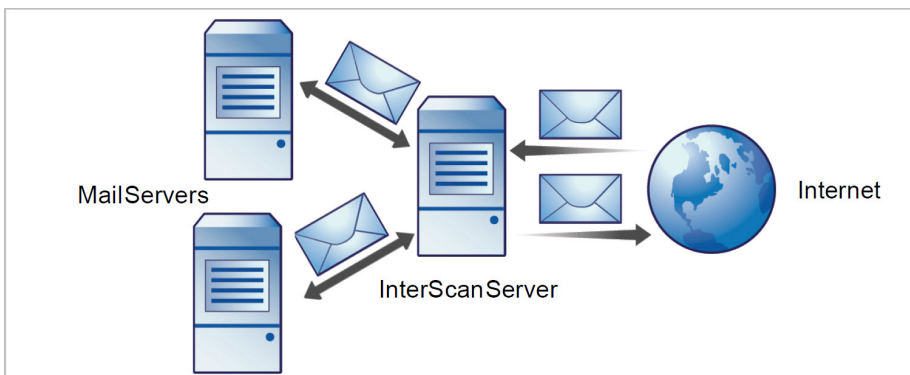


图 3-5. 安装拓扑：无防火墙



注意

趋势科技建议不要在没有防火墙的情况下安装 IMSA。将托管 IMSA 的服务器放在网络边缘可能使面临安全威胁。

在防火墙前面安装

下图展示了在防火墙前面安装 IMSA 时的安装拓扑。

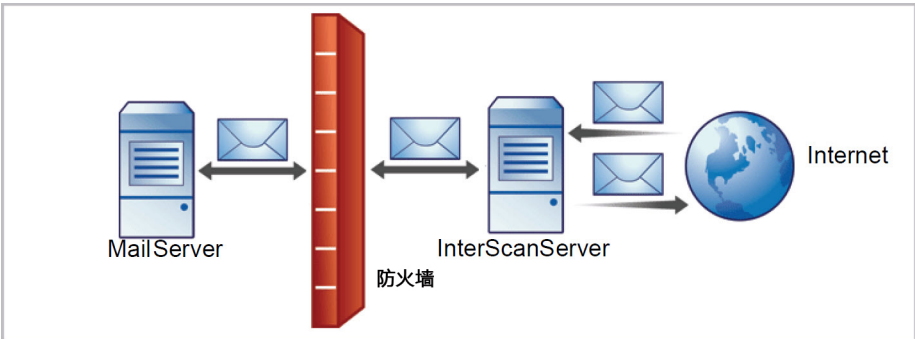


图 3-6. 安装拓扑：防火墙前面

传入网络通信

- Postfix 应该首先接收到传入邮件，然后将邮件传输到 IMSA。将 IMSA 配置为参考您的 SMTP 服务器，并将防火墙配置为允许来自 IMSA 服务器的传入通信。
- 将中继控制设置配置为只允许针对本地域进行中继。

传出网络通信

- 配置防火墙（基于代理服务器），使所有出站邮件路由到 IMSA，这样：
 - 传出 SMTP 邮件只能先转到 Postfix，然后才能转到 IMSA 服务器。

- 传入的 SMTP 邮件仅来自 IMSA 服务器。
- 配置 IMSA，以允许内部 SMTP 网关（通过 Postfix）通过 IMSA 中继到任意域中。

**提示**

有关详细信息，请参阅《IMSA 管理员指南》的*配置 SMTP 路由*部分。

在防火墙后面安装

下图展示了如何在防火墙后面部署 IMSA。

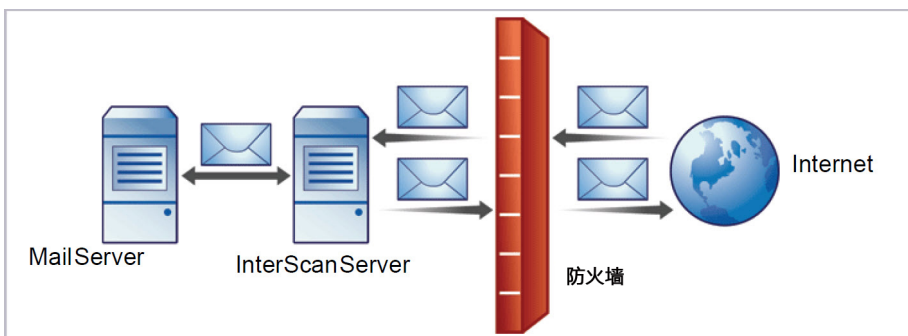


图 3-7. 安装方案：防火墙后面

传入网络通信

- 配置基于代理服务器的防火墙，步骤如下：
 - 传出 SMTP 邮件首先转到 Postfix，然后转到 IMSA 服务器，或者执行扫描程序之间负载平衡的切换器。
 - 传入 SMTP 邮件首先转到 Postfix，接着转到 IMSA，然后转到域中的 SMTP 服务器。

- 配置 IMSA，将发送至本地域的邮件路由到 SMTP 网关或内部邮件服务器。
- 将中继限制配置为只允许针对本地域进行中继。

传出网络通信

- 配置所有内部 SMTP 网关，将传出邮件发送到 Postfix，然后再到 IMSA 服务器。
- 如果用 IMSA 替代 SMTP 网关，则配置您的内部邮件服务器，将传出邮件通过 Postfix 发送到 IMSA 服务器。
- 配置 Postfix 和 IMSA，使其将所有传出邮件（发向域的邮件，而非发向本地的邮件）路由到防火墙或投递这些邮件。
- 将 IMSA 配置为允许内部 SMTP 网关中继到任何使用 IMSA 的域。



提示

有关详细信息，请参阅《IMSA 管理员指南》的**配置 SMTP 路由**部分。

在外围安全区域中安装

还可以在外围安全区域 (DMZ) 中安装 IMSA 和 Postfix 。

传入网络通信

- 配置基于数据包的防火墙。
- 配置 IMSA，使其将发送至本地域的电子邮件路由到 SMTP 网关或内部邮件服务器。

传出网络通信

- 配置 Postfix，将所有传出邮件（发送至除本地域之外的邮件）路由至防火墙，或者使用 IMSA 来投递传出电子邮件。
- 配置所有内部 SMTP 网关，将传出邮件转发到 Postfix，然后再到 IMSA。
- 将 IMSA 配置为允许内部 SMTP 网关通过 Postfix 和 IMSA 中继到任何域中。



提示

有关详细信息，请参阅《IMSA 管理员指南》的**配置 SMTP 路由**部分。

关于设备角色

IMSA 可以充当父设备或子设备。父设备和子设备构成一个组，其中父设备可以为向其注册的子设备提供集中管理服务。

- **父设备：**管理子设备。如果您正在部署单个 IMSA 设备，请在设置过程中选择**父模式**，以便部署所有 IMSA 组件。
- **子设备：**由单个父设备管理，而且将会使用您通过父设备的管理控制台配置的所有全局设置。

组是指至少注册了一个子设备的父设备。

关于设备服务

您可以启用 IMSA 设备上的各种服务。

仅限父设备的服务：

- **管理用户界面服务（管理控制台）：**管理全局设置。

父设备和子设备服务：

- **策略服务：**管理您所配置的规则。
- **扫描程序服务：**扫描电子邮件通信。
- **EUQ 服务：**管理终端用户隔离，通过该服务用户可以查看被 IMSA 确定为垃圾邮件的电子邮件。
- **命令行接口 (CLI) 服务：**提供对 CLI 功能的访问。

只有向父设备注册后，子设备才能起作用。

服务选择

您可以启用父设备和子设备上不同类型的服务。例如，要增加吞吐量，请添加更多的子设备，启用其所有服务并允许子设备扫描网络通信以及提供 EUQ 服务。

在任一部署方案中，均可以在父设备/子设备组中部署 IMSA 设备。但是，如果在父设备和子设备中启用扫描程序服务，则必须针对单个组中的所有设备使用同一类型的部署。某些子设备无法在网关处部署，而另外一些无法在网关后面部署。

除上述 SMTP 扫描方案外，您可能还希望 IMSA 扫描 POP3 网络通信。查看[了解 POP3 扫描 第 3-14 页](#)了解详细信息。

使用 IP 过滤部署

趋势科技 IP 过滤（包括 IP 分类器和电子邮件信誉）可在 IP 级别阻止连接。

要使用 IP 过滤，IMSA 与网络边缘之间的任何防火墙都不能修改相关的 IP 地址，因为 IP 过滤与使用网络地址转换 (NAT) 的网络不兼容。例如，如果 IMSA 接受来自同一源 IP 地址的 SMTP 连接，则 IP 过滤将不起作用，因为对于每个接收到的邮件来说地址都将相同，而且 IP 过滤软件将无法确定 SMTP 会话的原始发起人是否为已知的垃圾邮件发件人。

了解内部通信端口

IMSA 支持多个网络接口。这意味着一个 IMSA 设备可以具有多个 IP 地址。因此，如果设备尝试使用唯一的 IP 地址通信，就会出现問題。IMSA 采用了内部通信端口，从而克服了这一问题。

- 用户必须指定一个网络接口卡 (NIC) 作为内部通信端口，从而在安装过程中识别 IMSA 设备。
- 安装后，用户可以通过配置向导或命令行接口 (CLI) 来更改 IMSA 管理控制台中的内部通信端口。
- 在组方案中，父设备和子设备必须使用它们的内部通信端口来彼此通信。当向父设备注册子设备时，用户必须指定父设备内部通信端口的 IP 地址。



提示

趋势科技建议在组的每个 IMSA 设备上均配置一个主机路由项，以确保父设备与子设备之间的通信使用内部通信端口。

- IMSA 设备使用内部通信端口的 IP 地址注册到控制管理中心服务器。当用户希望通过防毒墙控制管理中心管理控制台来配置 IMSA 设备时，需要启用内部通信端口中的管理控制台服务。缺省情况下，所有端口上的管理控制台服务均处于启用状态。

了解 POP3 扫描

除 SMTP 通信外，IMSA 还可以在客户端检索 POP3 邮件时在网关扫描这些邮件。即使您的公司不使用 POP3 邮件，您的员工也可能会访问其个人的基于 Web 的 POP3 电子邮件帐户，如果未扫描来自这些帐户的邮件，可能会在网络上产生漏洞点。

最常见的电子邮件扫描部署在缺省情况下将使用 IMSA 扫描 SMTP 网络通信。但是，要扫描您的组织可能从 Internet 上的 POP3 服务器接收到的 POP3 网络通信，请启用 POP3 扫描。

在启用 POP3 扫描的情况下，IMSA 可以充当邮件客户端和 POP3 服务器之间的代理服务器，在客户端检索邮件时对邮件进行扫描。

要扫描 POP3 网络通信，请将您的电子邮件客户端配置为连接到 IMSA 服务器 POP3 代理，该 POP3 代理连接到 POP3 服务器来检索和扫描邮件。

POP3 扫描的要求

要使 IMSA 扫描 POP3 网络通信，必须在网络上安装防火墙，并将其配置为阻止除 IMSA 之外的所有计算机发出的 POP3 请求。此配置确保所有 POP3 网络通信都经过防火墙到达 IMSA，并且仅使用 IMSA 扫描 POP3 网络通信。



注意

如果禁用 POP3 扫描，则客户端将无法接收 POP3 邮件。

配置通过 IMSA 接收电子邮件的 POP3 客户端

要配置使用通用 POP3 连接的 POP3 客户端，请配置以下内容：

- **IP 地址/域名：**IMSA IP 地址或域名
- **端口：**IMSA 通用 POP3 端口
- **帐户：**account_name#POP3_Server_Domain-name

例如：user#10.18.125.168

要配置使用专用 POP3 连接的 POP3 客户端，请配置以下内容：

- **IP 地址：**IMSA IP 地址
- **端口：**IMSA 专用 POP3 端口
- **帐户：**account_name

例如：user

打开 IMSA 管理控制台

可以从您部署 IMSA 管理控制台的服务器使用 Web 浏览器查看该程序，或者通过网络以远程方式查看管理控制台。

要在浏览器中查看控制台，请转到以下 URL：

`https://{IMSA}:8445`

其中 {IMSA} 指 IP 地址或全限定域名。

例如：`https://196.168.10.1:8445` 或 `https://IMSVA1:8445`

使用 IP 地址的另一种方式是使用目标服务器的全限定域名 (FQDN)。要使用 SSL 查看管理控制台，请在域名前面键入 “https://”，并在域名后面附上端口号。

缺省的登录凭据如下所示：

- 管理员用户名：**admin**
- 密码：**imsva**

键入第一次打开控制台时的登录凭据，然后单击**登录**。为了防止您的策略出现未授权更改，趋势科技建议在部署后立即设置一个新的登录密码。



注意

如果正在使用 Internet Explorer (IE) 7.0 访问管理控制台，则 IE 将阻止访问并显示一个弹出对话框，说明证书是从一个不同的 Web 地址发出的。只需忽略此消息，然后单击**继续到此 Web 站点**以继续。



提示

要防止对您的策略的未授权更改，趋势科技建议定期更改该密码。

第 4 章

安装 IMSA 9.0

本章介绍如何在不同方案下安装 IMSA。

包括以下主题：

- [系统要求 第 4-2 页](#)
- [安装 IMSA 第 4-4 页](#)

系统要求

下表提供了运行 IMSA 的建议系统要求及最低系统要求。

表 4-1. 系统要求

规范	描述
操作系统	IMSA 提供了使用标准 CentOS Linux 操作系统的独立安装程序。此专用操作系统安装有 IMSA，可以提供整套解决方案。不需要 Linux、Windows 或 Solaris 等单独的操作系统。  注意 IMSA 使用 64 位操作系统。在 ESX/ESXi 上安装 64 位操作系统时，需要输入 BIOS 并启用 VT（虚拟化技术）。
CPU	• 建议：8 核 Intel™ Xeon™ 处理器或同等处理器 • 最低：双核 Intel™ Xeon™ 处理器或同等处理器
内存	• 建议：8GB 内存 • 最低：4GB 内存
磁盘空间	• 建议：250GB  注意 IMSA 会按照建议的 Linux 做法对检测到的磁盘空间进行自动分区。 • 最低：120GB  注意 IMSA 会按照建议的 Linux 做法对检测到的磁盘空间进行自动分区。
监控	显示器应支持 800 x 600 的分辨率，256 色，或者更高配置

规范	描述
趋势科技防毒墙控制管理中心	• 版本 5.5（Service Pack 1 Patch 4 或更高版本） • 版本 6.0（Service Pack 1 或更高版本）

其他要求和工具

下表列出了访问 CLI 和管理控制台接口以及使用防毒墙控制管理中心管理 IMSA 所需的最低应用程序要求。

表 4-2. 最低软件要求

应用程序	系统要求	详细信息
SSH 通信应用程序	第 2 版 SSH 协议	要通过 SSH 连接充分查看 IMSA CLI，请将终端窗口大小设置为 80 列和 24 行。
VMware™ ESX 服务器	• VMware ESX/ESXi 4.0 和 4.1 • VMware ESXi 5.0 • VMware ESXi 5.5	要将 IMSA 安装为虚拟机，请将 IMSA 安装在 VMware ESX Server 4.0/4.1、VMware ESXi 5.0 或 VMware ESXi 5.5 上。
Hyper-V	• Windows Server 2008 R2 SP1 • Windows Server 2012 • Windows Server 2012 R2 • Microsoft Hyper-V Server 2008 R2 SP1 • Microsoft Hyper-V Server 2012 R2	IMSA 在以下操作系统上支持 Hyper-V：Windows Server 2008 R2 SP1、Windows Server 2012、Windows Server 2012 R2、Microsoft Hyper-V Server 2008 R2 SP1 和 Microsoft Hyper-V Server 2012 R2。

应用程序	系统要求	详细信息
Internet Explorer™	9.0 版 10.0 版 11.0 版	要访问 Web 控制台以便从中配置所有 IMSA 设置，请使用 Internet Explorer 9.0 或更高版本，或者使用 Firefox 27.0 或更高版本。如果使用了在初始配置期间设置的数据端口 IP 地址，请输入以下 URL： https://[IP 地址]:8445
Mozilla Firefox™	27.0 版	
Java™ 虚拟机	版本 5.0 或更高版本或 SUN JRE 1.4+	要查看 Web 控制台中的某些项目，计算机必须安装有 JVM。
趋势科技防毒墙控制管理中心	- 版本 5.5 SP1 Patch 4 或更高版本 - 版本 6.0 SP1 或更高版本	使用趋势科技防毒墙控制管理中心 5.5 SP1 或 6.0 SP1 来管理 IMSA。

安装 IMSA

IMSA 9.0 仅支持从 IMSA 8.5 SP1 进行升级，并且会在升级期间迁移现有配置和策略数据。

IMSA 安装过程将格式化现有系统，以安装 IMSA。裸机与 VMware ESX 虚拟机平台的安装步骤基本相同。裸机安装从 IMSA 安装 DVD 启动，从而开始安装步骤，VMware 安装需要在安装之前创建虚拟机。



警告!

在安装过程中，任何现有数据或分区都将被清除。在安装 IMSA 之前，请对系统中的所有现有数据进行备份（若有）。

过程

1. 开始 IMSA 安装。
有关系统要求，请参阅[系统要求 第 4-2 页](#)。
 - 在裸机服务器上

- a. 确保裸机服务器支持 CentOS 6.4 x86_64。
- b. 将 IMSA 安装 DVD 插入所需服务器的 DVD 驱动器。
- c. 启动裸机服务器。
- 在 VMware ESX 虚拟机上

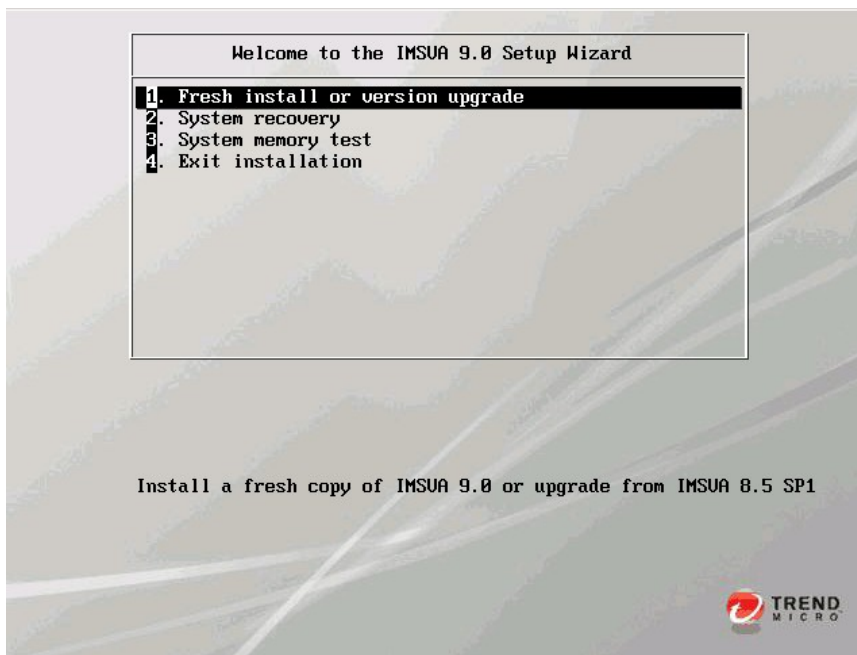
**警告!**

如果将 IMSA 安装在 ESX 服务器上，请禁用虚拟机的快照功能，因为快照会耗尽硬盘空间。

- a. 在 VMware ESX 服务器上创建虚拟机。
- b. 启动虚拟机。
- c. 通过以下方法之一，将 IMSA 安装 DVD 插入虚拟 DVD 驱动器。
 - 将 IMSA 安装 DVD 插入 ESX 服务器的物理 DVD 驱动器，然后将虚拟机的虚拟 DVD 驱动器连接到物理 DVD 驱动器。
 - 将虚拟机的虚拟 DVD 驱动器连接至 IMSVA-9.0-xxxx-x86_64.iso 文件。可从以下网址获取 IMSVA-9.0-xxxx-x86_64.iso 文件：
<http://www.trendmicro.com/download/zh-cn/>
- d. 单击 VMware Web 控制台上的 **VM > 发送 Ctrl+Alt+Del**，重新启动虚拟机。

对于 VMware ESX 虚拟机和裸机服务器安装，都将出现一个页面，该页面显示带有下列选项的 **IMSA 9.0 设置向导**：

- **全新安装或版本升级**：选择此选项可将 IMSA 安装到新硬件或虚拟机上，或者升级现有 IMSA。
- **系统恢复**：选择此选项可修复操作系统错误并恢复管理密码。
- **系统内存测试**：选择此选项可执行内存诊断测试。
- **退出安装**：选择此选项可以退出安装过程并从本地磁盘启动。



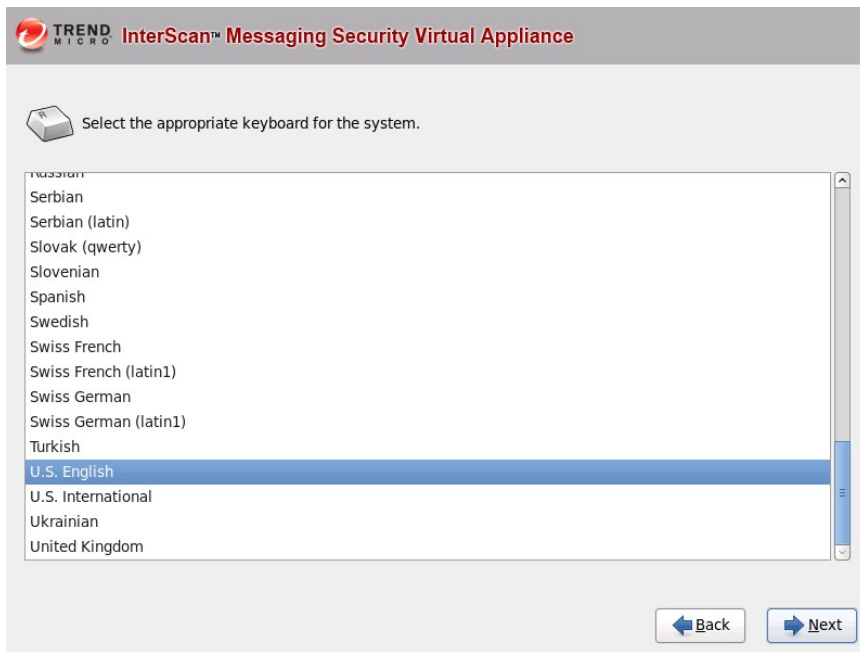
2. 选择全新安装或版本升级。

此时将显示许可协议页面。



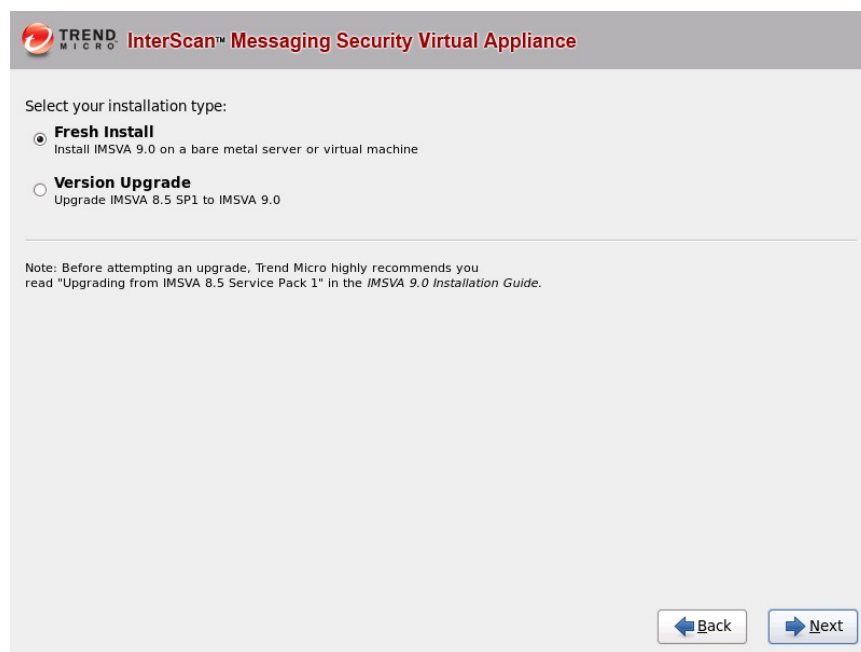
3. 单击**接受**以继续。

将显示键盘语言选择窗口。



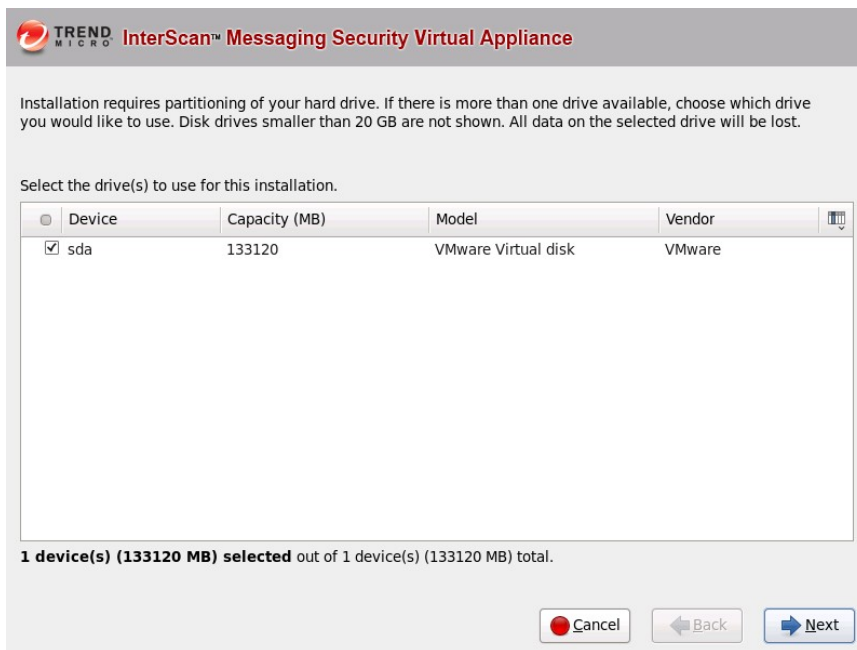
4. 选择系统的键盘语言，然后单击下一步。

此时将显示一个窗口，您可以在其中选择安装类型。



5. 选择全新安装，然后单击下一步。

此时将显示一个窗口，您可以在其中选择用于安装的驱动器。



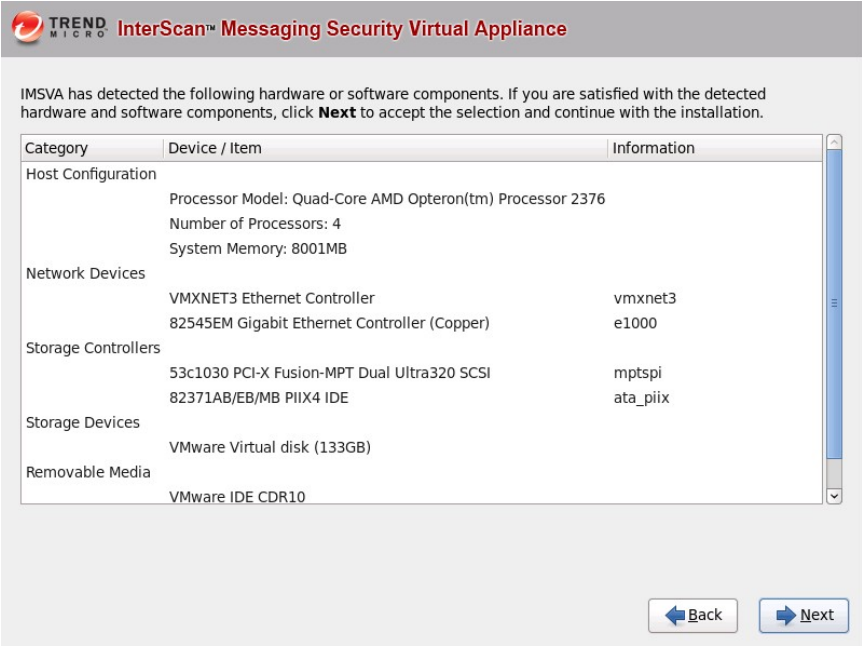
6. 选择驱动器，然后单击下一步。

将显示一个警告对话框。



7. 单击是继续。

IMSA 安装程序将扫描硬件和软件，以确定是否满足最低要求，并显示结果。如果硬件或软件包含任何不满足最低要求的组件，安装程序将高亮显示这些组件并停止安装。



8. 确保硬件和软件信息正确无误，然后单击下一步。

将显示网络设备配置窗口。

 **InterScan™ Messaging Security Virtual Appliance**

Host name:

Network Devices Configuration

Active on Boot	Device	Link Status	Description
☒	eth0	up	VMware VMXNET3 Ethernet Controller
☐	eth1	up	Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)

IPv4 Settings

IPv6 Settings

IPv4 address:

Netmask:

Gateway:

Primary DNS:

Secondary DNS:

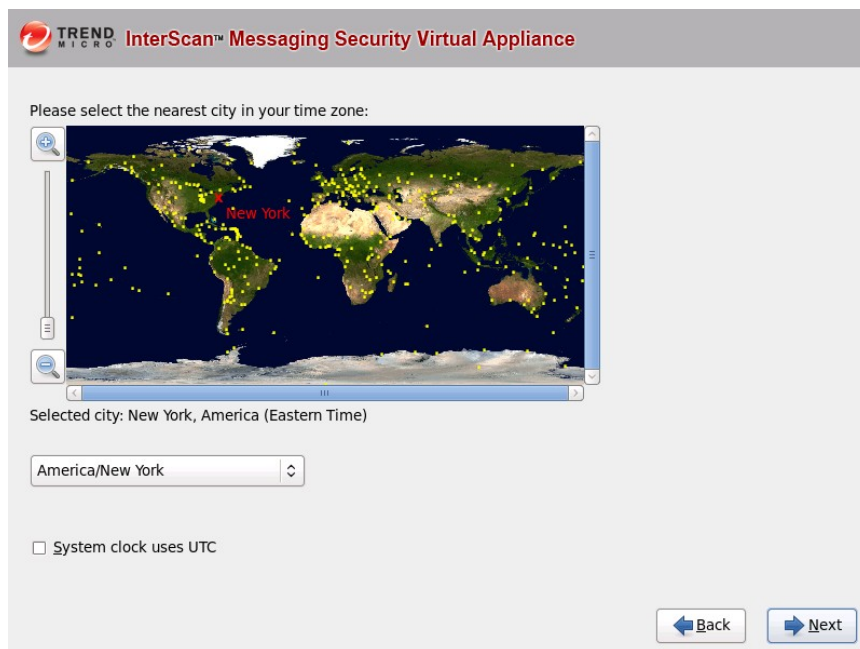
Back

Next

表 4-3. 网络设备配置

配置参数	描述
IPv4 Address	键入 IMSA 管理 IP 地址和子网掩码。
Hostname	为此 IMSA 主机键入适用的 FQDN。
Gateway	键入适用的 IP 地址以用作此 IMSA 安装的网关。
Primary DNS	键入适用的 IP 地址以用作此 IMSA 安装的主 DNS 服务器。
Secondary DNS	键入适用的 IP 地址以用作此 IMSA 安装的辅助 DNS 服务器。

9. 提供安装 IMSA 所需的所有信息，然后单击**下一步**。
将显示时区配置窗口。



10. 指定 IMSA 服务器的时间和时钟设置
 - a. 选择 IMSA 服务器的位置。
 - b. 通过选中或清除**系统时钟使用 UTC** 复选框，指定服务器系统时钟是否使用 UTC。
11. 单击**下一步**。

将显示帐户设置窗口。

TREND MICRO InterScan™ Messaging Security Virtual Appliance

Create passwords for the administrative accounts below to prevent unauthorized access. Each password must be a string of at least 6 characters.

Root Account: Used to safeguard access to the operating system shell. Has full operating system privileges.

Password: Not Entered

Confirm:

Enable Account: Used to gain access to the Command Line Interface (CLI) privilege mode. Has access to all CLI commands.

Password: Not Entered

Confirm:

Back Next

12. 指定根帐户和启用帐户的密码。

IMSA 使用两种不同级别的管理员帐户来保护系统。

密码最少必须为 6 个字符，最多为 32 个字符。



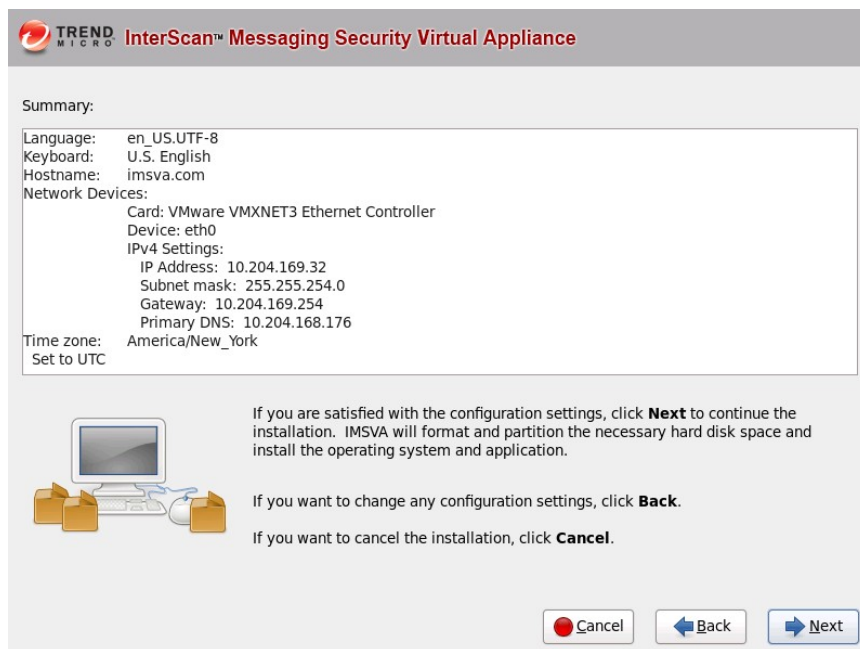
提示

为保证最佳安全性，请创建一个只有您自己知道的高度唯一的密码。可以使用大写和小写字母字符、数字以及键盘上的任何特殊字符来创建密码。

- **根帐户：**用于获取对操作系统 Shell 的访问权限，并享有该服务器的所有权利。这是系统上最强大的用户。
- **启用帐户：**用于获取对命令行接口的授权模式的访问权限。该帐户具有执行任何 CLI 命令的所有权利。

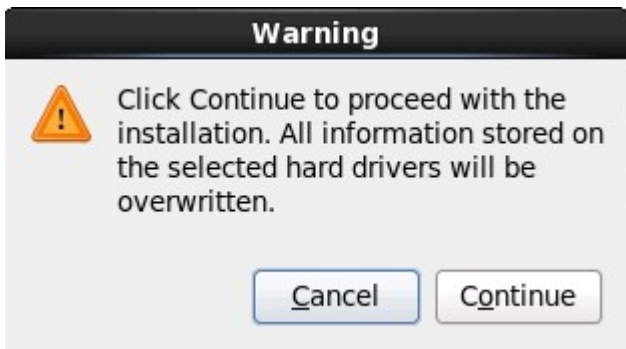
13. 单击下一步。

此时将显示一个窗口，其中显示配置设置的摘要。



14. 验证设置，然后单击下一步。

此时将显示一个对话框，询问您是否要继续安装。



重要信息

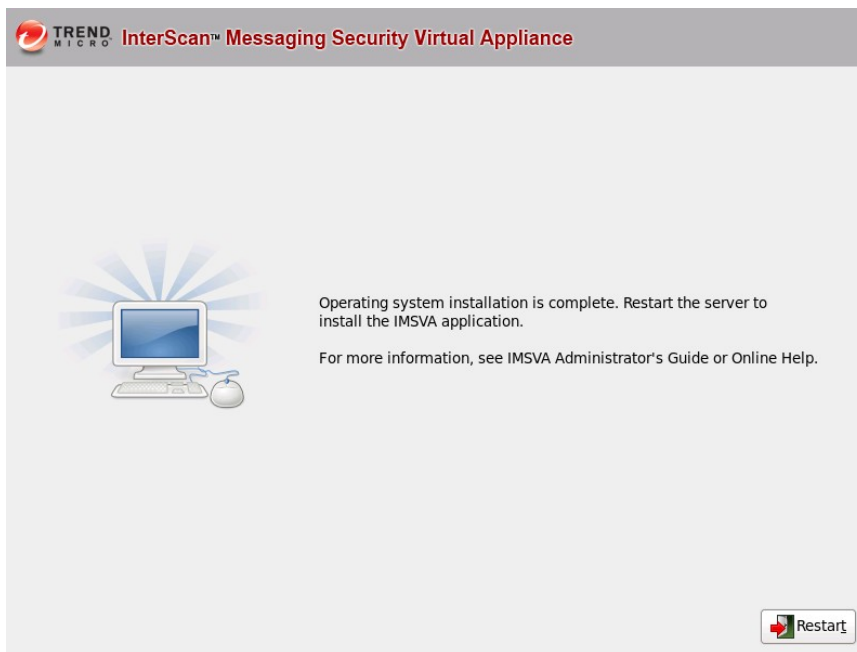
选择**继续**将清除硬盘分区上的所有数据并且格式化硬盘。如果硬盘上有您希望保留的数据，则取消安装并备份信息，然后继续。

15. 单击**继续**。

将出现一个窗口，该窗口提供用于 IMSA 安装的本地磁盘驱动器的格式化状态。完成格式化后，IMSA 安装开始。



安装完成之后，将显示摘要窗口。安装日志会保存到 `/var/app_data/installlog` 文件以供参考。



16. 单击**重新启动**以重新启动系统。

- 裸机安装：

DVD 自动弹出。从驱动器中移除 DVD 以防止重新安装。

- 虚拟机安装：

趋势科技建议从虚拟机中断开 DVD-ROM 设备的连接，因为已经安装了 IMSA。

在 IMSA 重新启动后，将显示初始 CLI 登录窗口。

```
Trend Micro InterScan Messaging Security Virtual Appliance (IMSVa)

To manage IMSVa through the graphical user interface (GUI), open a browser window and choose any URL from the following list:

    https://10.204.169.32:8445

You will be prompted for your administrator account and password.
Refer to the Administrator's Guide for the default account and password.

To manage IMSVa through the Command Line Interface (CLI),
log on using the following logon prompt. Refer to the Administrator's Guide
for the default account and password.

test login: _
```

17. 通过 CLI 或 IMSA 管理控制台登录以启动 IMSA。



提示

登录到 CLI Shell 以执行其他配置、故障排除或家务管理任务。

设置单个父设备

IMSA 提供一个**配置向导**，可帮助您配置使 IMSA 启动并运行所需的所有设置。

过程

1. 确保您的管理计算机可以 ping 在安装过程中配置的 IMSA 的 IP 地址。
2. 在管理计算机上，打开 Internet Explorer（版本 8.0 或更高版本）或 Firefox（版本 27.0 或更高版本）。

- 键入以下 URL（如果需要，请接受安全证书）：

https://<IP 地址>:8445

此时会显示“登录”窗口。

- 选中**打开配置向导**复选框。
- 键入下面的缺省用户名和密码：

- 用户名：admin
- 密码：imsva

此时将显示**配置向导**窗口。



图 4-1. “配置向导”窗口

- 请按**配置向导**窗口中的步骤来配置设置。

步骤 1：配置系统设置

过程

- 阅读过欢迎窗口之后，单击**下一步**。此时将显示**本地系统设置**窗口。

配置向导

步骤 1 (共 10 步)

本地系统设置

网络和系统时间的下列设置将在单击“保存”/“下一步”按钮之后立即被应用到本地系统

网络设置

网络接口配置

设备名称	IP 地址	网络掩码
eth0		

内部通信端口

设备名称: eth0

网络子系统配置

主机名:*

缺省网关:*

主 DNS 服务

辅:*

辅助 DNS 服务

辅:

系统时间

可以在“部署设置”窗口上启用 NTP，子设备使用其父设备的 NTP 设置，如果没有在“部署设置”窗口上为父设备启用 NTP，则子设备无法使用 NTP。

本地时区:*

Asia

China

Chongqing

大洲

国家/地区

省/市

日期和时间:*

2008/07/18

10:06:12

yyyy/mm/dd

小时:分钟:秒

< 上一步

跳过

保存

图 4-2. 本地系统设置

2. 如果需要，请修改设备主机名、IP 地址和网络掩码。另外，请配置网络设置并设置设备系统时间。



注意

单击**下一步 >** 按钮后，本地系统设置会立即生效。如果 IP 地址或时间设置已更改，IMSA 将重新启动。一直等到 IMSA 进入联机状态，然后重新登录。

步骤 2：配置部署设置

过程

1. 单击**下一步**。

此时将显示**部署设置**窗口。



图 4-3. 部署设置

2. 选择**父设备**或**子设备**。如果这是您要设置的第一个设备，则必须选择**父设备**。可以稍后配置其他子设备。

请决定您是否要使用 NTP 服务。

步骤 3：配置 SMTP 路由设置

过程

- 1. 单击下一步。

此时将显示 SMTP 路由设置窗口。

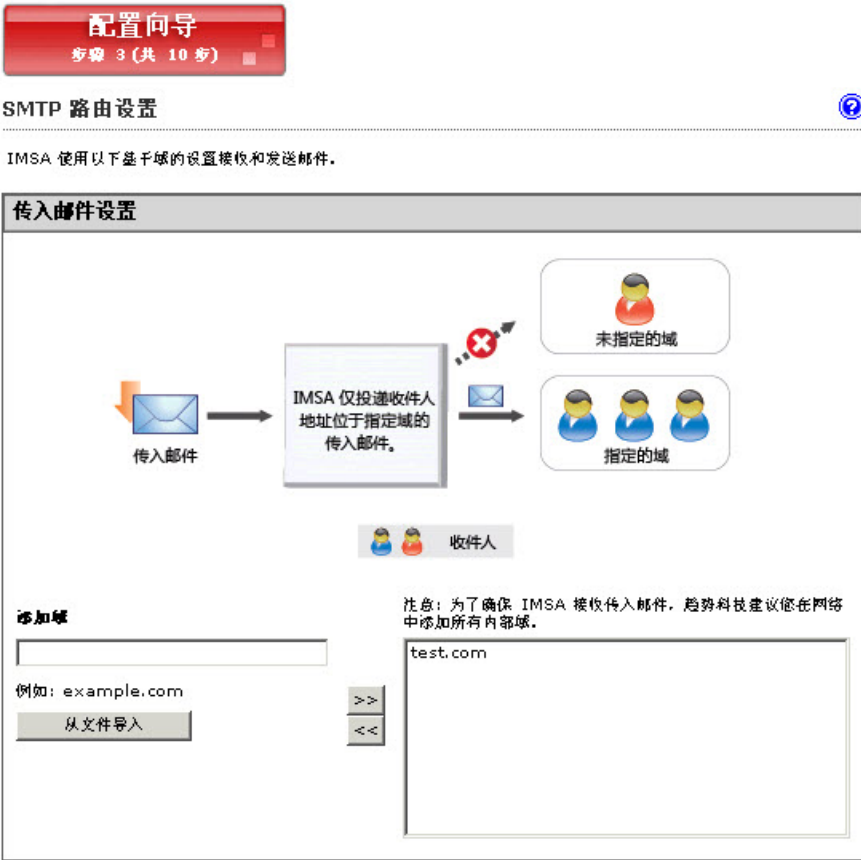


图 4-4. SMTP 路由设置

邮件投递设置

要投递的邮件

IMSA 根据收件人的域和电子邮件地址来选择目标服务器

邮件服务器 A

邮件服务器 B

邮件服务器 C

电子邮件地址 A

域 B

收件人

添加

删除

导入

1-2 / 2 页 1

域或电子邮件地址	描述
☐ test.com	MX 记录查找
☐ 其他域	取 DNS 响应

添加

删除

导入

1-2 / 2 页 1

显示: 每页 15 个

< 上一步

下一步 >

- 2. 指定传入邮件设置。
- 3. 指定邮件投递设置。

步骤 4：配置通知设置

过程

- 1. 单击下一步。

此时将显示通知设置窗口。

配置向导
步骤 4 (共 10 步)

通知设置

为缺省系统通知配置电子邮件 和 SNMP 陷阱通知。

电子邮件设置

收件人地址:*

使用半角分号 ";" 隔开多个地址

发件人电子邮件地址:*

postmaster@imsva.trendmicro.com

服务器名称或 IP 地址:*

127.0.0.1

SMTP 服务器端口:*

10026

首选字符集:*

UTF-8 (utf-8)

邮件头:

邮件脚注:

SNMP 陷阱

服务器名称 (IP 或 FQDN):

团体:

public

< 上一步

跳过

下一步 >

步骤

1. 系统设置

2. 部署设置

3. SMTP 端口

4. 通知设置

5. 更新源

6. LDAP 设置

7. 内部地址

8. TCMCM 设置

9. 产品推送

10. 查看设置

图 4-5. 通知设置

2. 如果您希望接收系统和策略事件通知，请配置电子邮件或 SNMP 陷阱通知设置。

步骤 5：配置更新源

过程

1. 单击下一步。

此时将显示**更新源**窗口。



图 4-6. 更新源

2. 配置下列更新设置，这些设置将确定 IMSA 将从哪里接收其组件更新以及 IMSA 需要通过哪个代理（如果有）连接以访问 Internet：
- **源：**单击**趋势科技 ActiveUpdate (AU) 服务器**以直接从趋势科技接收更新。或者，单击**其他 Internet 源**并键入更新源的 URL，该 URL 将检查趋势科技 ActiveUpdate 服务器是否存在更新。可以指定所选择的更新源，或键入控制管理中心服务器的 URL `http://<TMCM 服务器地址>/TvcsDownload/ActiveUpdate/`（如果适用）。
 - **代理服务器设置：**选择**使用代理服务器**复选框，并配置代理服务器类型、服务器名称、端口、用户名和密码。

步骤 6：配置 LDAP 设置

过程

1. 单击下一步。

此时将显示 LDAP 设置窗口。

配置向导
步骤 6 (共 10 步)

LDAP 设置

仅当您打算将 LDAP 用于 用户组 定义、管理员权限或 Web 隔离身份验证，您必须启用 LDAP 以使用 Web 隔离工具。如果您需要定义一个以上 LDAP 服务器，请使用：管理 > 连接 > LDAP 窗口。

LDAP 说明

说明：*

LDAP 设置

LDAP 服务器类型：*

Microsoft Active Directory

启用 LDAP1

LDAP 服务器：*

示例：example.com 或 123.123.123.123

侦听端口号：*

389

注意：如果 LDAP 服务器类型为 Microsoft Active Directory，请使用全局侦听端口 3268。

启用 LDAP2

LDAP 服务器：*

示例：example.com 或 123.123.123.123

侦听端口号：*

389

注意：如果 LDAP 服务器类型为 Microsoft Active Directory，请使用全局侦听端口 3268。

策略服务和 EUQ 服务的 LDAP 缓存有效期

以分钟为单位的缓存期限：*

1440

步骤

1. 系统设置

2. 部署设置

3. SMTP 路由

4. 通知设置

5. 更新源

6. LDAP 设置

7. 内部地址

8. TCM 设置

9. 产品迁移

10. 查看设置

LDAP 管理

LDAP 管理帐户: *
示例: Domain_Name\Account_Name 或 Account_Name@Domain_Name

密码: *

连接标识名: *
示例: DC=foo, DC=foonet, DC=org

身份验证方法: * ☒ 简单 ☐ 高级: 为 Active Directory
使用 Kerberos 身份验证
Kerberos 身份验证缺省范围:
缺省域:
KDC 和管理服务器:
KDC 端口号:

< 上一步 跳过 下一步 >

2. 为 LDAP 服务器指定一个有意义的描述。
3. 完成下列各项以启用 LDAP 设置:
 - a. 对于 LDAP 服务器类型, 请选择以下某项:
 - Domino
 - Microsoft Active Directory
 - Microsoft AD 全局编录
 - OpenLDAP
 - Sun iPlanet Directory
 - b. 要启用一个或全部两个 LDAP 服务器, 请选中**启用 LDAP 1**或**启用 LDAP 2**旁边的复选框。
 - c. 指定 LDAP 服务器的名称以及它们所侦听的端口号。
 - d. 在**策略服务和 EUQ 服务的 LDAP 缓存有效期**下, 以分钟为单位的存在**期限**字段的旁边, 键入代表存在期限的一个数值。

- e. 在 **LDAP 管理** 下，键入管理员帐户、其相应的密码以及基准标识名。有关为 LDAP 管理设置指定的内容的指导，请参阅下表。

表 4-4. LDAP 管理设置

LDAP 服务器	LDAP 管理帐户（示例）	基准标识名（示例）	认证方法
Active Directory	不使用 Kerberos: user1@domain.com (UPN) 或 domain \user1 使用 Kerberos: user1@domain.com	dc=domain、 dc=com	简单 高级（使用 Kerberos）
Active Directory 全局编目	不使用 Kerberos: user1@domain.com (UPN) 或 domain \user1 使用 Kerberos: user1@domain.com	dc=domain、 dc=com dc=domain1、 dc=com（如果存在多个唯一域）	简单 高级（使用 Kerberos）
Lotus Domino	cn=manager、 dc=test1、dc=com	dc=test1、dc=com	简单
Lotus Domino	user1/domain	不适用	简单
Sun iPlanet Directory	uid=user1、 ou=people、 dc=domain、dc=com	dc=domain、 dc=com	简单

- f. 对于认证方法，请单击**简单**或**高级**认证。对于 Active Directory 高级认证，请配置 Kerberos 认证缺省范围、缺省域、KDC 和管理服务器以及 KDC 端口号。



注意

仅当您将 LDAP 用于用户组定义、管理员权限或 Web 隔离认证时，才指定 LDAP 设置。

步骤 7：配置内部地址

过程

1. 单击下一步。

此时将显示**内部地址**窗口。

图 4-7. 内部地址

2. IMSA 使用内部地址来确定某个策略或某个事件是入站的还是出站的。
 - 如果正在为传出邮件配置规则，则内部地址列表适用于发件人。
 - 如果正在为传入邮件配置规则，则内部地址列表适用于收件人。

要定义内部域和用户组，请执行下列操作之一：

- 从下拉列表中选择**输入域**，在文本框中键入域，然后单击 >>。
 - 从下拉列表中选择**搜索 LDAP 组**。此时将显示一个用于选择 LDAP 组的窗口。在文本框中键入要搜索的 LDAP 组名，然后单击**搜索**。搜索结果将显示在列表框中。要将其添加到**已选择**列表中，请单击 >>。
-

步骤 8：配置防毒墙控制管理中心服务器设置

过程

1. 单击**下一步**。

此时将显示 **TMCM 服务器设置** 窗口。

配置向导

步骤 8 (共 10 步)

TMCM 服务器设置

趋势科技™ 防毒墙控制管理中心™ (TMCM) 是一项软件管理解决方案。使用该方案可以从一个中心位置控制 IMSA 设备及其他防毒和内容安全程序。

TMCM 服务器设置

要通过控制管理中心管理 IMSA，请启用控制管理中心 MCP 代理并配置所有控制管理中心服务器设置。

☐ 启用 MCP 代理

服务器: *

通信协议: *

HTTP 端口: 80

HTTPS 端口: 443

Web 服务器认证:

用户名:

密码:

☐ 启用代理服务

代理服务类型: *

HTTP

代理服务: *

端口: *

用户名:

密码:

< 上一步

跳过

下一步 >

图 4-8. TMCM 服务器设置

2. 如果您将使用防毒墙控制管理中心来管理 IMSA，请执行下列操作：
- a. 选中**启用 MCP 代理**（缺省情况下附于 IMSA 中）。

b. 在**服务器**旁边，键入防毒墙控制管理中心 IP 地址或 FQDN。

c. 在**通信协议**旁边，选择 **HTTP** 或 **HTTPS** 并键入相应的端口号。用于 HTTP 访问的缺省端口号为 80，而用于 HTTPS 访问的缺省端口号为 443。

- d. 在 **Web 服务器认证**下，为 Web 服务器键入用户名和密码（如果该服务器需要认证）。
- e. 如果代理服务器位于 IMSA 和防毒墙控制管理中心之间，请选中**启用代理服务器**。
- f. 键入代理服务器端口号、用户名和密码。

步骤 9：激活产品

过程

1. 单击**下一步**。
此时将显示**产品激活**窗口。

配置向导

步骤 9 (共 10 步)

产品激活

要获取激活码，请使用注册码在线注册产品。

在线注册

激活

云端过检：

趋势科技杀毒专家和内容过检程序：

垃圾邮件阻止解决方案：

趋势科技电子邮件加密：

合规性监管服务：

< 上一步

下一步 >

图 4-9. 产品激活

2. 为要激活的产品或服务键入激活码。如果您没有激活码，请单击**在线注册**，并按“趋势科技注册”Web 站点上的说明操作。

步骤 10：查看设置

过程

1. 单击下一步。

此时将显示查看设置窗口。



图 4-10. 查看设置

2. 如果设置正确，请单击完成。

要修改任一设置，请单击上一步，并一直在窗口中移动，直到设置完成。在您单击完成并退出向导后，IMSA 即可使用。

设置子设备

此部分介绍如何设置子设备并将其注册到父设备。

过程

1. 确定子设备的 IP 地址。
2. 在父设备上，执行下列操作：
 - a. 在设置父设备之后（请参见[设置单个父设备 第 4-19 页](#)），确保父设备是可操作的。
 - b. 登录到管理控制台。确保您正在登录到父设备管理控制台。
 - c. 转到**管理 > IMSA 配置 > 连接 > 子 IP**。
 - d. 在**添加 IP 地址**下，添加子设备的内部通信端口 IP 地址。
3. 在子设备上，执行下列操作：
 - a. 就像对父设备所执行的操作一样，将管理计算机连接到子设备，然后登录到管理控制台。所有 IMSA 设备都具有相同的缺省管理控制台登录凭据。
 - b. 在**设置向导**中，配置本地系统设置，然后单击**下一步>**。
 - c. 在“部署设置”窗口上，选择**子服务器**，并添加父设备的**内部通信端口** IP 地址。
 - d. 单击**完成**。
4. 在父设备上，执行下列操作：
 - a. 转到**系统状态**。
 - b. 验证子设备是否显示在**被管理服务**下，以及在“连接”下是否有一个绿色复选标记。您可以启动或停止扫描程序、策略或 EUQ 服务。



注意

如果在父设备上启用 EUQ，则也将在子设备上启用它。

5. 如果希望在子设备上使用 EUQ，请在 EUQ 数据库之间重新分配数据：
 - a. 在父设备上，导航到**管理 > 终端用户隔离**。
缺省情况下会显示 **EUQ 管理**选项卡。

- b. 选择**重新分配全部**或仅**重新分配允许的发件人**。趋势科技建议选择**重新分配全部**。
- c. 单击**重新分配**。



注意

如果已将某个启用 EUQ 的子设备注册到其父设备，请将发件人添加到许可发件人列表中，然后重新分配 EUQ 数据，某些新添加的允许的发件人可能不会出现。

趋势科技建议执行下列操作：

- 在重新分配 EUQ 之后，管理员通知所有终端用户验证新添加的允许的发件人是否仍可用。
 - 当管理员正在添加子设备以及正在重新分配 EUQ 时，管理员应通知所有终端用户不要添加 EUQ 许可发件人列表。
-

验证是否已成功部署

在您设置了 IMSA 设备之后，服务应该自动启动。

过程

1. 转到**系统状态**。
 2. 在**被管理服务**下，确保扫描程序和策略服务处于活动状态。否则，请单击**启动**按钮将其激活。
-



注意

您可以选择启用或禁用 EUQ 服务。

第 5 章

从先前版本升级

本章提供从 IMSA 先前版本升级的说明。

包括以下主题：

- [从评测版升级 第 5-2 页](#)
- [从 IMSA 8.5 Service Pack 1 进行升级 第 5-4 页](#)
- [从先前版本迁移 第 5-33 页](#)

从评测版升级

如果之前已提供评测版激活码激活 IMSA，则已开始评估期，可以尝试使用产品的全部功能。评估期根据使用的激活码类型而异。

在评估期到期前十四 (14) 天，IMSA 会在管理控制台显示一条警告消息，提醒您产品即将到期。

要继续使用 IMSA，请购买产品的完全版使用授权。随后会获得新激活码。

过程

1. 转到**管理 > 产品使用授权**。

将显示产品使用授权窗口。

产品使用授权

云端过滤

在线查看使用授权详细信息

产品:云端过滤

版本:完全

激活码:

输入新激活码

座席数:000100

状态:已激活

维护过期:2005-12-28

在线检查状态

上次状态检查日期 2015-3-7

垃圾邮件阻止解决方案 (SPS)

在线查看使用授权详细信息

产品:垃圾邮件阻止解决方案 (SPS)

版本:完全

激活码:

输入新激活码

座席数:000100

状态:已激活

维护过期:2005-12-28

在线检查状态

上次状态检查日期 2015-3-7

趋势科技电子邮件加密

在线查看使用授权详细信息

产品:趋势科技电子邮件加密

版本:完全

激活码:

输入新激活码

座席数:000100

状态:已激活

维护过期:2005-12-28

在线检查状态

上次状态检查日期 2015-3-7

注意: 成功激活趋势科技电子邮件加密后, 请转到加密设置, 注册服务和域。

合规性监管服务

在线查看使用授权详细信息

产品:合规性监管服务

版本:完全

激活码:

输入新激活码

座席数:000100

状态:已激活

维护过期:2005-12-28

在线检查状态

上次状态检查日期 2015-3-7

2. 在要激活的产品或服务部分，单击[输入新激活码](#)超链接。

5-3

将显示**输入新激活码**窗口。

输入新激活码

如果没有激活码，请使用产品随附的注册码 [在线注册](#)。

产品：趋势科技杀毒专家和内容过滤程序

当前的激活码：XXXXXXXX-XXXX-XXXX-XXXX-XXXX-XXXX

新激活码：

< 上一步

激活

3. 在提供的框中输入新激活码。



注意
购买 IMSA 的完全授权版本后，趋势科技会通过电子邮件向您发送新激活码。为了防止输入激活码（格式为 xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx）时出现错误，可以从电子邮件中复制激活码并将其粘贴到提供的框中。

4. 单击**激活**。
5. 对于所有要激活的产品或服务，重复步骤 2 至 5。

从 IMSA 8.5 Service Pack 1 进行升级

可以将 IMSA 8.5 Service Pack 1 作为单个设备进行升级，也可以升级整个分布式环境。

**注意**

在升级过程完成之前，请勿重新启动 IMSA。

在升级过程中，不会迁移任何自定义操作系统设置，但主机设置、网络设置和网关设置除外。要保留原始设置，请执行以下操作：

1. 将原始根分区挂载到升级后的服务器上的某个路径，例如 `/root/original_root`：

```
mount /dev/mapper/IMSSVA-Root2 /root/original_root
```
2. 在挂载的路径中找到原始设置。
3. 将原始设置添加到升级服务器上。

备份 IMSA 8.5 Service Pack 1

IMSA 8.5 Service Pack 1 会备份配置设置，并在升级不成功时执行自动还原。但是，趋势科技建议在尝试升级至 IMSA 9.0 之前备份 IMSA 8.5 Service Pack 1：

过程

1. 备份 IMSA 8.5 Service Pack 1 以防止升级过程中可能发生的任何问题。
 - 对 IMSA 8.5 Service Pack 1 安装到的整个计算机进行 Ghost 备份。
 - 如果 IMSA 8.5 Service Pack 1 安装在虚拟机上，则执行克隆。
 - 备份 IMSA 8.5 Service Pack 1 `app_data` 分区。要执行此任务，请打开操作系统 Shell 控制台并运行以下命令：

```
/opt/trend/imss/script/imssctl.sh stop  
  
service crond stop  
  
cp -rf --preserve /var/app_data/* /var/udisk/  
app_data_backup/
```

2. 备份后启动所有 IMSA 服务。

升级单个 IMSA

此过程说明了如何将单个 IMSA 升级至版本 9.0。

过程

1. 备份 IMSA 8.5 Service Pack 1。



注意

有关详细信息，请参阅[备份 IMSA 8.5 Service Pack 1 第 5-5 页](#)。

2. 在 CLI 控制台中使用以下命令，以验证 postfix 队列中无任何电子邮件：

```
postqueue -p
```

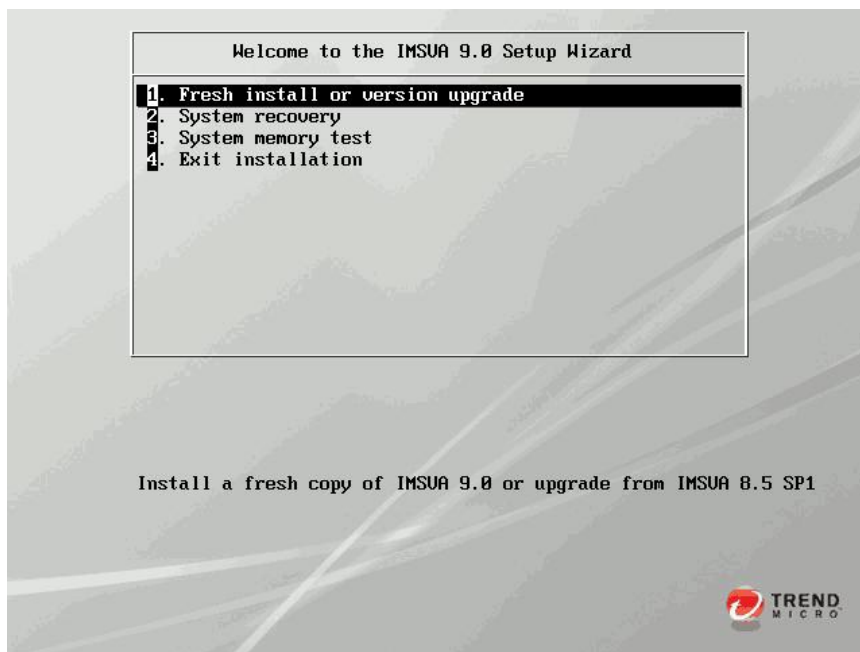
3. 重新启动要使用 IMSA 安装 DVD 进行升级的服务器。



注意

有关详细信息，请参阅[安装 IMSA 第 4-4 页](#)中的“步骤 1”。

将显示 IMSA 9.0 设置向导窗口。



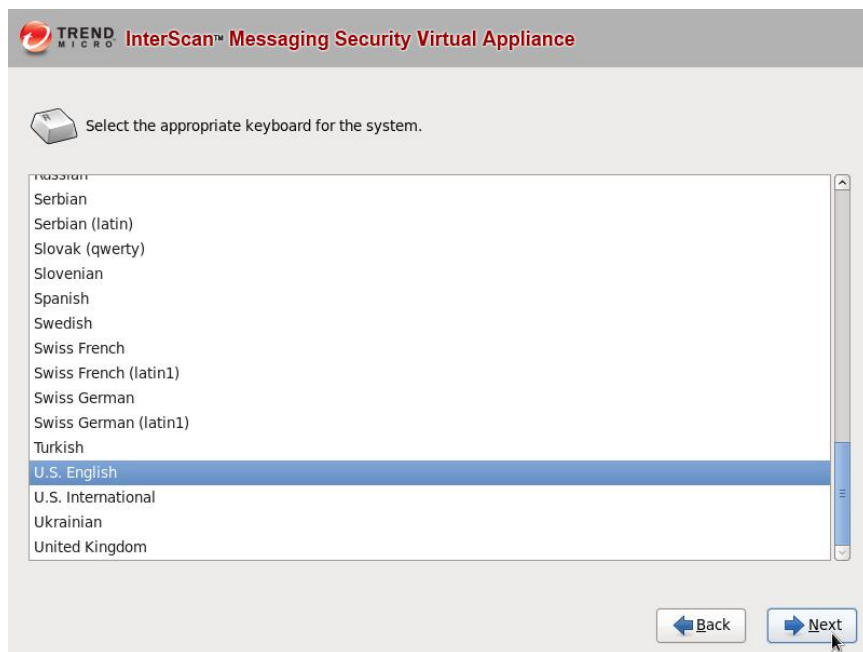
4. 选择全新安装或版本升级。

将显示许可协议窗口。



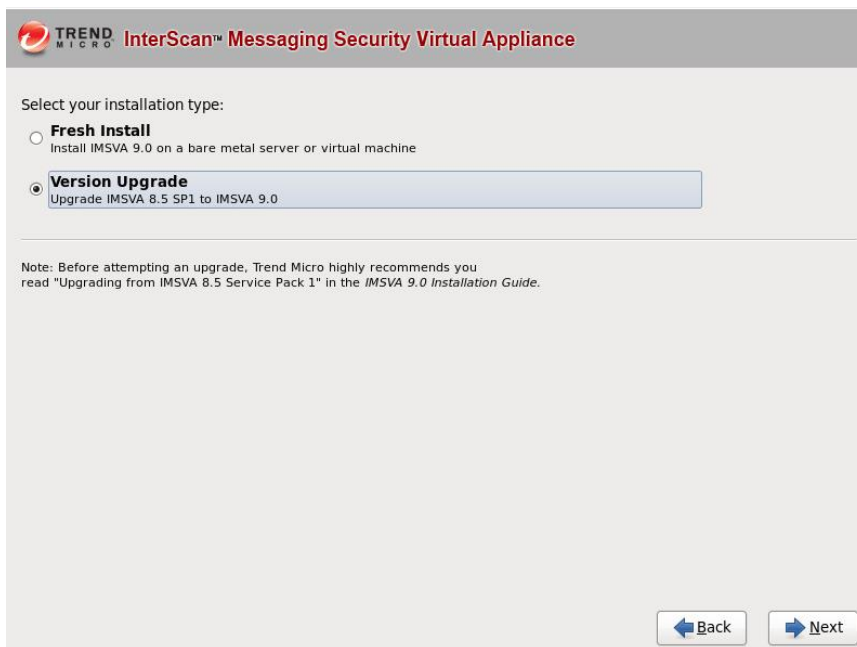
5. 单击接受以继续。

将显示键盘语言选择窗口。



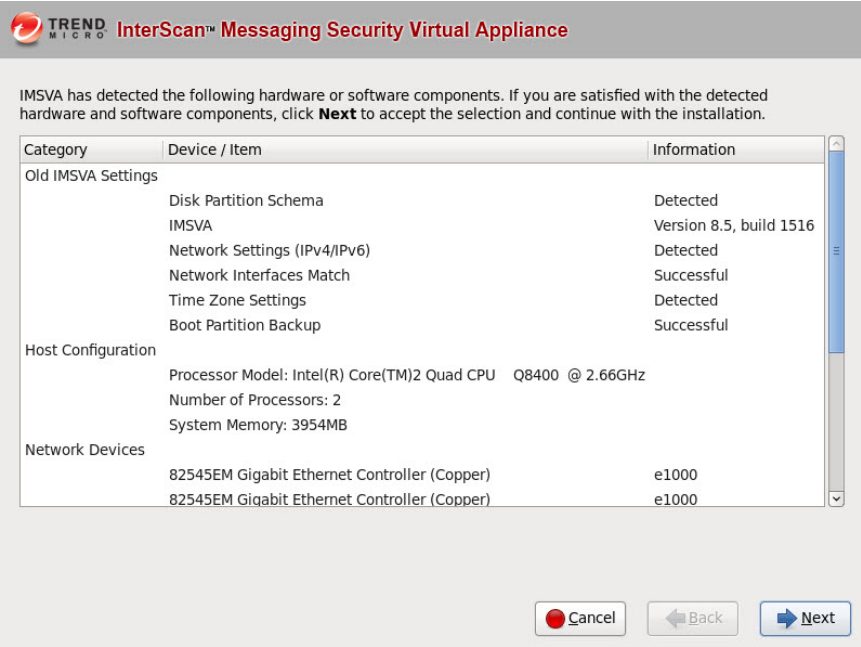
6. 选择系统的键盘语言，然后单击下一步。

此时将显示一个窗口，您可以在其中选择安装类型。



7. 选择**版本升级**，然后单击**下一步**。

IMSA 升级程序将扫描硬件和软件，以确定是否满足最低要求，并显示结果。如果硬件或软件包含任何不满足最低要求的组件，升级程序将高亮显示这些组件并停止升级。



8. 确保硬件和软件信息正确无误，然后单击下一步。

将显示帐户设置窗口。

TREND MICRO InterScan™ Messaging Security Virtual Appliance

Create passwords for the administrative accounts below to prevent unauthorized access. Each password must be a string of at least 6 characters.

Root Account: Used to safeguard access to the operating system shell. Has full operating system privileges.

Password: Not Entered

Confirm:

Enable Account: Used to gain access to the Command Line Interface (CLI) privilege mode. Has access to all CLI commands.

Password: Not Entered

Confirm:

Password Strength

Good

Poor

[Back](#) [Next](#)

9. 指定根帐户和启用帐户的密码。

IMSA 使用两种不同级别的管理员类型来保护系统的安全。

密码最少必须为 6 个字符，最多为 32 个字符。



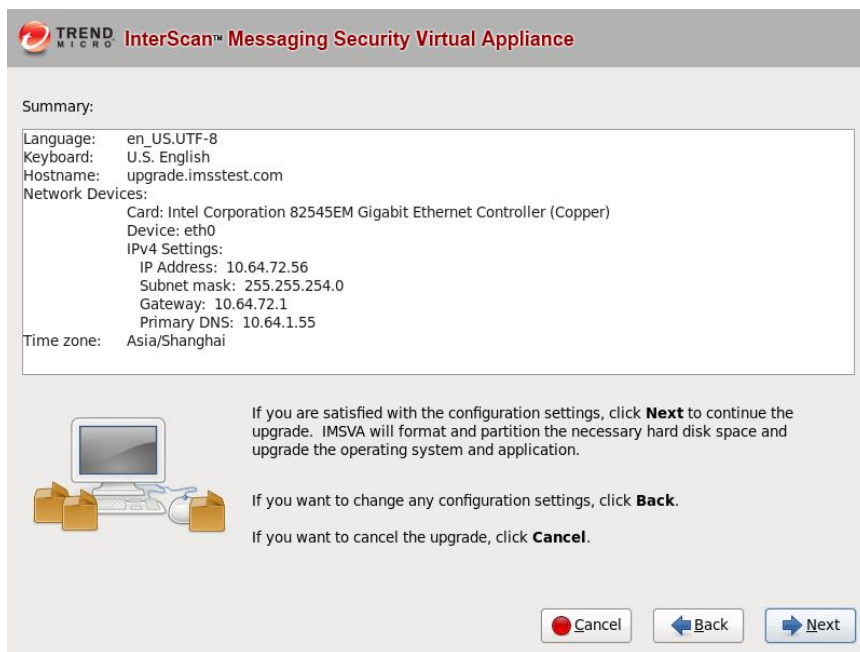
提示

为保证最佳安全性，请创建一个只有您自己知道的高度唯一的密码。可以使用大写和小写字母字符、数字和任何特殊字符来创建密码。

- **根帐户：**用于获取对操作系统 Shell 的访问权限，并享有该服务器的所有权利。这是系统上最强大的用户。
- **启用帐户：**用于获取对命令行接口的授权模式的访问权限。该帐户具有执行任何 CLI 命令的所有权利。

10. 单击下一步。

此时将显示一个窗口，其中显示配置设置的摘要。



TREND MICRO InterScan™ Messaging Security Virtual Appliance

Summary:

Language: en_US.UTF-8
Keyboard: U.S. English
Hostname: upgrade.imsstest.com
Network Devices:
Card: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)
Device: eth0
IPv4 Settings:
IP Address: 10.64.72.56
Subnet mask: 255.255.254.0
Gateway: 10.64.72.1
Primary DNS: 10.64.1.55
Time zone: Asia/Shanghai

If you are satisfied with the configuration settings, click **Next** to continue the upgrade. IMSVa will format and partition the necessary hard disk space and upgrade the operating system and application.

If you want to change any configuration settings, click **Back**.

If you want to cancel the upgrade, click **Cancel**.

11. 验证设置，然后单击下一步。

此时将显示一个窗口，其中提供用于 IMSA 升级的本地驱动器的格式化状态。



格式化完成后，将显示摘要窗口。



12. 单击**重新启动**以重新启动系统。

升级过程会在系统重新启动之后继续。当显示以下信息时，表明升级已完成。

```
Bringing up interface eth0: [ OK ]
Starting auditd: [ OK ]
Starting system logger: [ OK ]
Starting rpcbind: [ OK ]
Starting NFS statd: [ OK ]
Starting RPC idmapd: [ OK ]
Mounting other filesystems: [ OK ]
Retrigger failed udev events [ OK ]
Adding udev persistent rules [ OK ]
Generating SSH1 RSA host key: [ OK ]
Generating SSH2 RSA host key: [ OK ]
Generating SSH2 DSA host key: [ OK ]
Starting sshd: [ OK ]
Starting crond: [ OK ]
Applying firewall rules... [ OK ]
Exporting configuration settings from the database...
Export of configuration settings from the database is complete.
Starting pre-installation check...
Starting the upgrade process.
Installing the RPM "imsva-9.0-1.i386.rpm".
The RPM "rpm/imsva-9.0-1.i386.rpm" is installed successfully.
Refer to the Installation Guide for information on how to start 2 hours' dry run
period for IMSUA.
Press any key to enter the operating system shell command line interface.
```

13. 请按任何键进入系统 Shell 命令行接口。

14. 请使用以下命令验证升级状态：

```
# tail -1 /var/app_data/installllog
```

15. IMSA 升级完成后，在 CLI 控制台中使用以下命令以重新启动 IMSA 服务：

```
/mnt/backup/dry_run.sh
```

16. 验证 IMSA 在升级后是否正常工作。

17. 要还原至 IMSA 8.5 Service Pack 1，请使用以下命令：

```
/mnt/backup/confirm.sh
```

```
"no"
```

18. 如果 IMSA 在升级后正常工作，请使用以下命令完成升级：

```
/mnt/backup/confirm.sh
```

“yes”

如果您未在 2 小时内还原至 IMSA 8.5 Service Pack 1，所有 IMSA 服务将会自动停止。这样，您必须使用以下命令决定是还原至 IMSA 8.5 Service Pack 1 还是完成升级：

```
/mnt/backup/confirm.sh
```

键入 **yes** 完成升级或输入 **no** 进行还原。

升级分布式环境

IMSA 现在支持升级整个分布式部署，例如，在父子部署中使用 IMSA 的网络中。

过程

1. 做好升级准备工作。
 - a. 备份 IMSA 8.5 Service Pack 1。



注意

有关详细信息，请参阅[备份 IMSA 8.5 Service Pack 1 第 5-5 页](#)。

- b. 在 CLI 控制台中使用以下命令，以验证 postfix 队列中无任何电子邮件：

```
postqueue -p
```

- c. 确保所有 IMSA 服务都在管理控制台上正常工作。

在**系统状态**窗口上，**被管理服务**下的所有服务都处于活动状态。

页面关键词

控制台

系统状态

云端过滤

策略

IP 过滤

报告

日志

邮件区与队列

管理

系统状态

启用连接

☒ 接受 POP3 连接

☒ 启用 IP 过滤

☒ 电子邮件传输

☒ IP 分类器

保存

组件

上次刷新: 2015-3-12 9:06:34

刷新

更新

还原

名称	当前版本	可用性	更新时间表
☐ 病毒扫描引擎	9.750.1005	0.0	15 分钟
☐ 高级威胁扫描引擎	9.755.1246	9.755.1246	15 分钟
☐ 病毒码	11.452.60	11.452.60	15 分钟
☐ 间谍软件特征码	1.555.00	1.572.00	15 分钟
☐ IntelliTrap 特征码	0.205.00	0.215.00	15 分钟
☐ IntelliTrap 例外特征码	1.123.00	1.155.00	15 分钟
☐ 反垃圾邮件引擎	7.600.1031	7.600.1031	15 分钟
☐ 反垃圾邮件特征码	21300.000	21300.000	15 分钟
☐ URL 过滤引擎	3.500.1047	3.000.1029	15 分钟
☐ 云安全客户端病毒码	11.209.00	0	15 分钟

被管理服务

主机名	连接	扫描程序服务	策略服务	EUQ 服务
imsva9sc.com	☒	☒ 停止	☒ 停止	已禁用

d. 使用以下命令停止子设备上的所有服务：

```
# /opt/trend/imss/script/imssctl.sh stop
```



注意

在分布式部署中，必须先升级父设备再升级子设备。



警告!

执行此步骤会中断电子邮件通信。如果要避免通信中断，请执行[批量升级 第 5-20 页](#)或[脱机升级 第 5-27 页](#)。

e. 使用以下命令在子设备上启动数据库服务：

```
# /opt/trend/imss/script/dbctl.sh start
```

2. 升级父设备和子设备。

a. 升级父设备。请参阅[升级单个 IMSA 第 5-6 页](#)中的步骤 3 到 13。

- b. 使用以下命令验证父设备上的数据库是否正常工作：

```
# ps -ef | grep imss
```

将显示如下信息：

```
imss 26303 1 0 18:22 ?00:00:00 /opt/trend/imss/  
PostgreSQL/bin/postmaster -D /var/imss/pgdata -i
```

- c. 通过以下方式升级所有子设备：一次升级一个、一次升级几个或全部同时升级。



警告!

在所有设备完成升级之前，请勿重新启动 IMSA 服务。

在所有设备完成升级之前，请勿对任何父设备或子设备运行 /mnt/backup/dry_run.sh 或 /mnt/backup/confirm.sh。

如果其中一个子设备在升级期间遇到问题，请使用 CLI 取消注册该子设备。

3. 验证升级是否成功。

- a. 使用以下命令打开安装日志文件：

```
# tail -1 /var/app_data/installlog
```

- b. 查看安装日志中指示升级是否成功的信息。

4. 完成升级。

- a. 升级所有设备后，请使用以下命令先后在父设备和子设备上重新启动 IMSA 服务：

```
/mnt/backup/dry_run.sh
```

- b. 验证 IMSA 在升级后是否正常工作。

- c. 要还原至 IMSA 8.5 Service Pack 1，请使用以下命令先后还原所有子设备和父设备：

```
/mnt/backup/confirm.sh
```

“no”

- d. 如果 IMSA 在升级后正常工作，请使用以下命令完成升级：

```
/mnt/backup/confirm.sh
```

“yes”

如果您未在 2 小时内还原至 IMSA 8.5 Service Pack 1，所有 IMSA 服务将会自动停止。这样，您必须使用以下命令决定是还原至 IMSA 8.5 Service Pack 1 还是完成升级：

```
/mnt/backup/confirm.sh
```

键入 **yes** 完成升级或输入 **no** 进行还原。

批量升级

批量升级允许升级父设备和两个或更多子设备。此选项可保留升级过程中的日志信息，并且不会造成停机。

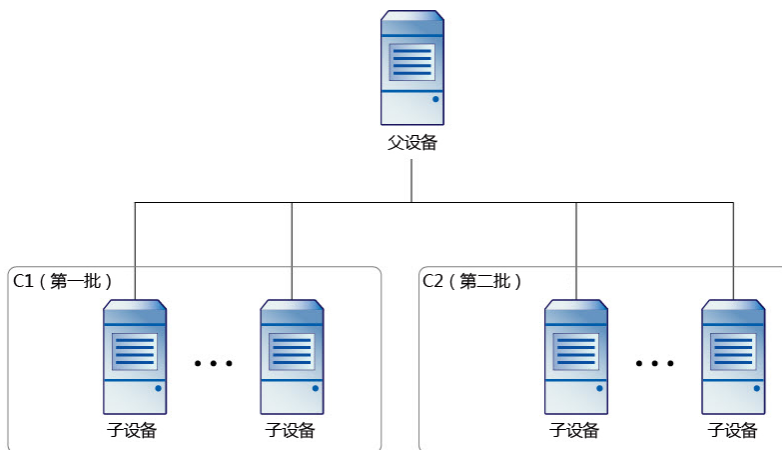


提示

趋势科技建议在电子邮件通信处于最低水平时执行批量升级。评估要在第一批之后升级的 IMSA 设备是否能够处理升级过程中总的电子邮件流量。

最好在凌晨 4:00 到晚上 22:00 之间执行批量升级。在此推荐的时间段之外，子设备上的守护程序服务可能会重新启动，从而导致这些子设备无法连接到父设备。

以下是批量升级过程的概述：



1. 选择第一批进行升级的子设备。
2. 阻止父设备与子设备之间的连接（使用 IP 表或防火墙），但在步骤 1 中选择的设备除外。

**注意**

在此阶段，子设备应当无法连接到父设备。但是，父设备可以连接到子设备以执行升级前检查。

3. 对在步骤 1 中选择的父设备和子设备执行脱机升级。
4. 将升级后的设备部署到生产环境中。
5. 对其余子设备执行脱机升级。
6. 恢复升级后的父设备与子设备之间的连接。
7. 将升级后的设备部署到生产环境中。

8. 重复以上步骤，直至父设备和所有子设备都已升级。

**注意**

在批量升级过程中，必须阻止父设备与子设备之间的连接，这点很重要。

将父设备和子设备的防火墙配置为阻止第二批子设备升级。阻止连接之前，不能重新启动子设备。

步骤 1：阻止父设备与子设备之间的连接

**注意**

在此过程中，C1 是指第一批进行升级的子设备，而 C2 是指第二批子设备。

过程

1. 选择第一批进行升级的设备（下文称为 C1）。
 - a. 选择父设备。
 - b. 选择子设备。
 - c. 修改 DNS 记录，以停止向选定设备发送邮件。
2. 更改第二批子设备（下文称为 C2）上的 iptable。
 - a. 更改 iptable。

```
# vi /etc/init.d/rcFirewall
```

在 `start()` 的结尾添加以下规则：

```
iptables -I INPUT -s [父设备的 IP] -j REJECT
```

```
iptables -I INPUT -s [C1 的 IP] -j REJECT
```

```
iptables -I INPUT -s [父设备的 IP] -p tcp --sport 5432 -j  
ACCEPT
```

```
iptables -I INPUT -s [父设备的 IP] -p tcp --dport 5432 -j  
ACCEPT
```

```
iptables -I OUTPUT -d [C1 的 IP] -j REJECT
```

```
iptables -I OUTPUT -d [父设备的 IP] -p tcp --sport 5432 -j ACCEPT
```

- b. 应用添加的规则。

```
# /etc/init.d/rcFirewall restart
```

3. 更改父设备上的 iptable。

- a. 在父设备上，添加以下规则：

```
iptables -I INPUT -s [C2 的 IP] -p tcp --sport 5432 -j ACCEPT
```

- b. 应用添加的规则。

```
# /etc/init.d/rcFirewall restart
```

步骤 2：执行内联升级



注意

在此过程中，C1 是指第一批进行升级的子设备，而 C2 是指第二批子设备。

过程

1. 验证父设备和 C1 设备上的 Postfix 队列中是否都没有任何邮件。

- a. 在 CLI 控制台上检查 Postfix 队列。

```
# postqueue -p
```

只有在 Postfix 队列为空时，升级过程才会继续。否则，Postfix 队列中的邮件可能会丢失。

2. 使用以下命令在 C1 设备上停止除数据库服务以外的所有 IMSA 服务：

```
# /opt/trend/imss/script/imssctl.sh stop
```

```
# /opt/trend/imss/script/dbctl.sh start
```

3. 执行到 IMSA 9.0 的内联升级。



注意

有关详细的升级过程，请参阅[升级单个 IMSA 第 5-6 页](#)。

4. 执行 IMSA 9.0 测试部署。

- a. 成功升级 C1 设备后，修改父设备上的 iptable 以与远程服务器建立连接。随后便可以从该远程服务器更新父设备的数据库数据。

```
# iptables -I INPUT -s [远程服务器的 IP] -p tcp --sport  
5432 -j ACCEPT
```

```
# iptables -I INPUT -s [远程服务器的 IP] -p tcp --dport  
5432 -j ACCEPT
```

- b. 登录到父设备的 SQL 数据库并更新表。

```
# select * from tb_component_list;  
  
# update tb_component_list set app_ver='9.0.0.xxxx'  
where ip_addr='[C2 的 IP]';
```



注意

此步骤可使 IMSA 绕过在试运行之前执行的检查。

记录 C2 设备的原始 IMSA 版本 (app_ver)，以供在[步骤 3: 对其他子设备执行内联升级 第 5-25 页](#)（子步骤 4-b）中参考。然后将 9.0.0.xxxx 替换为您要安装的 IMSA 9.0 的 Build 号。

- c. 在 CLI 控制台上重新启动所有 IMSA 服务。

```
# /mnt/backup/dry_run.sh
```



注意

首先重新启动父设备，然后重新启动所有子设备。

5. 检查 Build 号。

- a. 转到**管理 > 更新 > 系统和应用程序**。
 - b. 在**当前状态**下，检查应用程序版本是否为 9.0.0.xxxx。
6. 完成内联升级。
- a. 要在父设备和所有 C1 设备上完成升级，请运行以下命令（首先在父设备上运行，然后在所有 C1 设备上运行）：

```
# /mnt/backup/confirm.sh  
"yes"
```
 - b. 要还原至 IMSA 8.5 SP1，请先后还原所有子设备和父设备。

```
# /mnt/backup/confirm.sh  
"no"
```
 - c. 修改 DNS 记录，以开始向升级后的父设备和 C1 设备发送邮件而停止向 C2 设备发送邮件。

步骤 3：对其他子设备执行内联升级



注意

逐个升级或批量升级子设备。

在此过程中，C1 是指第一批进行升级的子设备，而 C2 是指第二批子设备。

过程

1. 选择子设备。
2. 修改 DNS 记录，以停止向选定设备发送邮件。
3. 验证 Postfix 队列中是否都没有任何邮件。
 - a. 在 CLI 控制台上检查 Postfix 队列。

```
# postqueue -p
```

4. 修改 C2 设备的设置。

- a. 要绕过内联升级检查，请更改 C2 设备上的 iptable。

```
# iptables -I OUTPUT -d [父设备的 IP] -p tcp --dport 5432  
-j ACCEPT
```

- b. 在父设备上，更改 C2 设备的 IMSA 版本。

```
# /opt/trend/imss/PostgreSQL/bin/psql imss sa  
  
# select * from tb_component_list;  
  
# update tb_component_list set app_ver='8.5.0.1516'  
where ip_addr='[C2 的 IP]';
```



注意

IMSA 版本 (app_ver) 应反映您在[步骤 2: 执行内联升级 第 5-23 页](#)（子步骤 4b）中记录的版本。

5. 执行到 IMSA 9.0 的内联升级。



注意

有关详细的升级过程，请参阅[升级单个 IMSA 第 5-6 页](#)。

6. 执行 IMSA 9.0 测试部署。

- a. 在 CLI 控制台上重新启动所有 IMSA 服务：

```
# /mnt/backup/dry_run.sh
```

7. 检查 Build 号。

- a. 转到**管理 > 更新 > 系统和应用程序**。
- b. 在**当前状态**下，检查应用程序版本是否为 9.0.0.xxxx。

8. 完成内联升级。

- a. 要在所有设备上完成升级，请运行以下命令：

```
# /mnt/backup/confirm.sh
```

“yes”

- b. 要还原至 IMSA 8.5 SP1，请运行以下命令：

```
# /mnt/backup/confirm.sh
```

“no”

9. 恢复 C2 设备。

- a. 修改 DNS 记录并开始向 C2 设备发送邮件。
- b. 继续升级其他子设备，直至批量升级过程完成。

脱机升级

在脱机升级期间，临时 IMSA 设备用于处理电子邮件通信。IMSA 会记录所有信息，并且不会在升级过程中造成停机。



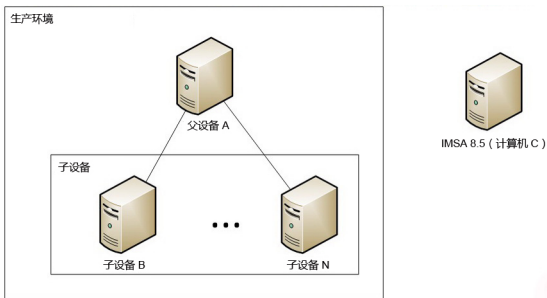
提示

趋势科技建议在电子邮件通信处于最低水平时执行脱机升级。评估临时 IMSA 设备是否能够处理升级过程中总的电子邮件流量。

当使用脱机升级时：

1. 备份文件，然后再将 IMSA 部署到虚拟机。
 2. 使用 NTP 服务器，以确保生产 IMSA 设备和临时 IMSA 设备使用相同的系统时间。
-

以下是脱机升级过程的概述：



1. 在临时设备上安装 IMSA 9.0。
2. 从生产 IMSA 设备导入配置设置。
3. 修改 DNS MX 记录，以将电子邮件通信重定向到临时设备。
4. 断开生产设备与网络的连接。
5. 对设备进行升级。
6. 重新将电子邮件通信重定向到生产设备。
7. 将临时设备中的日志文件夹和队列文件夹复制到其中一个生产子设备上。



注意

将数据恢复到子设备后，可能会出现数据鸿沟。如果启用了沙盒虚拟平台通知，您可能会在恢复数据后收到沙盒虚拟平台服务邮件。

步骤 1：在临时设备上安装 IMSA 9.0

过程

1. 使用 ISO 文件在临时设备上安装 IMSA 9.0。
2. 备份临时 IMSA 9.0 设备的缺省设置。

- a. 登录到父设备的管理控制台。
 - b. 转到**管理 > 导入/导出**。
 - c. 单击**导出**并保存导出的文件。
3. 导出现有父设备和子设备的设置。
 - a. 登录到父设备的管理控制台。
 - b. 转到**管理 > 导入/导出**。
 - c. 单击**导出**并保存导出的文件。
 4. 将父设备的设置导入到临时设备上。
 - a. 登录到临时设备的管理控制台。
 - b. 转到**管理 > 导入/导出**。
 - c. 单击**导入**。

**注意**

如果导入过程中出现问题，请使用在步骤 2 中创建的备份文件恢复 IMSA 9.0 缺省设置。

步骤 2：将邮件通信重定向到临时 IMSA 设备

趋势科技建议在电子邮件通信处于最低水平时升级生产服务器。

过程

1. 修改 DNS MX 记录，以将电子邮件通信重定向到临时 IMSA 设备。
 2. 停止向父设备和子设备发送邮件。
-

步骤 3：执行脱机升级

过程

1. 在脱机状态下升级父设备和子设备。有关详细信息，请参阅[升级分布式环境 第 5-17 页](#)。
2. 修改 DNS MX 记录，以将邮件通信重定向到父设备和子设备（但其中一个子设备除外）。
3. 配置在升级过程中丢失的任何自定义设置。
4. 停止向临时 IMSA 设备发送邮件。

步骤 4：将 IMSA 9.0 日志和队列文件夹复制到子设备

过程

1. 停止子设备（下文称为 Machine B）上的监控服务、管理中心服务和邮件跟踪服务。

```
[root@machine B ~]# S99MONITOR stop
```

```
[root@machine B ~]# S99MANAGER stop
```

```
[root@machine B ~]# S99CMAGENT stop
```

```
[root@machine B ~]# S99MSGTRACING stop
```

2. 如果在临时设备上启用了沙盒虚拟平台，请验证沙盒虚拟平台的上传文件夹中是否没有任何邮件。

```
[root@machine C ~]# ls -l /var/app_data/imss/dtas_upload/
```



注意

趋势科技建议在临时 IMSA 设备上禁用沙盒虚拟平台，以防止在导入日志后收到通知。如果要保持启用沙盒虚拟平台，请忽略通知。

3. 复制临时 IMSA 设备中的队列文件夹，并将其合并到 Child B 设备。

```
[root@machine C ~]# scp -r /opt/trend/imss/queue
root@machine B:/opt/trend/imss/
```

```
[root@machine B ~]# chown -R imss:imss /opt/trend/imss/
queue
```

4. 复制临时 IMSA 设备的策略事件日志，并将其附加到 Child B 设备最新的策略事件日志的结尾。

例如：

```
[root@machine C ~]# scp /opt/trend/imss/log/polevt.imss.
20130325.0001 root@machine B:/root/
```

```
[root@machine B ~]# cat /root/polevt.imss.20130325.0001 >>
/opt/trend/imss/log/polevt.imss.20130325.0001
```

5. 复制临时 IMSA 设备的邮件日志，并将其附加到 Child B 设备的邮件日志的结尾。

```
[root@machine C ~]# scp /var/log/maillog root@machine B:/
root/
```

```
[root@machine B ~]# cat /root/maillog >> /var/log/maillog
```

6. 复制临时 IMSA 设备的 fox* 日志，并将其附加到 Child B 设备最新的 fox* 日志的结尾。

例如：

```
[root@machine C ~]# scp /opt/trend/imss/log/foxmsg.
20130325.0001 root@machine B:/root/
```

```
[root@machine B ~]# cat /root/foxmsg.20130325.0001>>
/opt/trend/imss/log/foxmsg.20130325.0001
```

7. 在 Child B 设备上，启动监控服务、管理中心服务和邮件跟踪服务。附加的日志将很快导入到数据库中。

```
[root@machine B ~]# S99MANAGER start
```

```
[root@machine B ~]# S99MONITOR start
```

```
[root@machine B ~]# S99CMAGENT start
```

```
[root@machine B ~]# S99MSGTRACING start
```

8. 将附加的日志导入到数据库后，通过修改 DNS MX 记录来恢复 Child B 设备的设置。
-

还原升级

如果升级过程中遇到问题，IMSA 会自动还原。但是，如果自动还原遇到问题，则需要执行手动还原。

过程

1. 如果已创建了 ghost 镜像或拥有原始 IMSA 的虚拟机镜像，请使用原始镜像替换升级镜像。
2. 使用以下命令停止计时程序服务：

```
service crond stop
```

3. 检查计时程序设置备份文件 `/var/spool/cron/root.bakForUpgrade`。找到该文件后，使用以下命令恢复计时程序设置：

```
rm -rf /var/spool/cron/root && /bin/mv -f /var/spool/cron/  
root.bakForUpgrade /var/spool/cron/root
```

4. 检查日志备份文件 `/var/app_data/imss/log.bakForUpgrade`。找到该备份文件后，使用以下命令恢复日志文件：

```
rm -rf /var/app_data/imss/log/ && /bin/mv -f /var/app_data/  
imss/log.bakForUpgrade /var/app_data/imss/log/
```

5. 使用以下命令停止数据库服务：

```
killall postmaster
```

6. 在父设备上检查数据库备份文件 `/var/app_data/imss/db/pgdata.bakForUpgrade`。找到该文件后，使用以下命令恢复数据库文件：

```
rm -rf /var/app_data/imss/db/pgdata && /bin/mv -f /var/  
app_data/imss/db/pgdata.bakForUpgrade /var/app_data/  
imss/db/pgdata
```

7. 使用以下命令挂载 IMSA 8.5 Service Pack 1 的根分区（如果未挂载）：

```
mkdir -p /var/tmp/orig_root  
  
mount -t ext3 /dev/mapper/IMSVa-Root2 /var/tmp/orig_root
```

8. 使用以下命令恢复 **/boot** 文件夹：

```
/bin/cp -af /var/tmp/orig_root/boot-imsva-8.5-backup-  
for-9.0/* /boot
```

9. 重新启动计算机。

从先前版本迁移

IMSA 9.0 支持从先前 IMSS 和 IMSA 版本迁移。

下表列出了支持迁移到 IMSA 9.0 的最低版本：

表 5-1. 支持的迁移平台和版本

平台	版本
IMSS for Solaris	7.0 Service Pack 1 Patch 4
IMSS for Linux	7.1 Service Pack 2
IMSS for Windows	7.1 Patch 3
IMSS for Windows	7.5
IMSA	8.0 Patch 2
IMSA	8.2 Service Pack 2 Patch 1
IMSA	8.5 Service Pack 1

迁移过程

迁移过程需要执行以下任务：

- **步骤 1：** 从先前版本的 IMSS 或 IMSA 中导出设置
- **步骤 2：** 将设置导入 IMSA 9.0 中

从先前版本的 IMSS 或 IMSA 中导出设置

以下设置不迁移：

表 5-2. 无法迁移的设置

MTA 设置	未迁移的设置
MTA 设置	SMTP 接口的 IP 地址
配置设置	数据库设置（示例：内部文件路径）
	管理控制台密码
	防毒墙控制管理中心设置
	激活码
	 注意 所有早期版本的 IMSA 都会将云端过滤激活码迁移至 IMSA 9.0



重要信息

导出配置设置时，确保 IMSS 或 IMSA 服务器：

- 未执行数据库相关任务。
- 未终止或启动。

子设备使用的证书无法导出。

过程

1. 在要从其迁移的 IMSS 服务器或 IMSA 中转到**管理 > 导入/导出**。

将显示**导入/导出**窗口。

2. 单击**导出**。

配置设置将导出到 IMSA 可以导入的包中。

从 IMSS 7.0 Service Pack 1 Patch 4 for Solaris 中导出设置

过程

1. 将迁移工具包 (export_tool_sol_70.tar.gz) 复制到 IMSS 7.0 for Solaris 服务器上。

2. 使用以下命令解压缩导出工具。

```
gzip -d export_tool_sol_70.tar.gz
tar xf export_tool_sol_70.tar
```



注意

该工具将配置设置导出至可将这些设置复制至其他趋势科技邮件安全产品的加密包中。

3. 使用以下命令更改当前工作目录。

```
cd export70sol
```

4. 运行以下命令。

```
./export_tool_70.sh
```

该工具将在当前目录中创建导出的设置包 (imss_config_70.tar.gz) 和一个详细的日志文件 (export_70.<xxxxxxx>.log)。

将设置导入 IMSA 9.0 中

过程

1. 对 IMSA 9.0 执行全新安装。



提示

趋势科技建议将配置包导入到全新安装的 IMSA 9.0 中，因为导入的配置设置会覆盖所有现有设置。

2. 检索包含要迁移的配置设置的包。
3. 在 IMSA 9.0 管理控制台上转到**管理 > 导入/导出**。

将显示**导入/导出**窗口。

4. 导入配置包。



注意

缺省情况下，所有子设备在迁移后都使用父设备的证书。如果不希望使用这些证书，请为子设备分配其他证书。

从 IMSS for Windows 中迁移

要从 IMSS for Windows 迁移至 IMSA 9.0，请参阅[迁移过程 第 5-34 页](#)。

发生更改的 IMSS for Windows 设置

下表提供有关迁移过程中发生更改的所有 IMSS for Windows 设置的信息。

表 5-3. 发生更改的 IMSS for Windows 设置

设置	更改
电子邮件信誉	在迁移过程中，IMSA 9.0 会将所有自定义处理措施更改为 缺省智能处理措施 ，除非自定义处理措施为 连接被拒绝 ，并显示（在这种情况下，设置将保持不变）。
基于域的投递	• 设置了智能主机的缺省投递，更改为 * • 如果为某个域设置了多个智能主机，则列表中的所有智能主机都会迁移至 IMSA 9.0 并将静态路由设为投递方式
邮件规则设置	将减少每个连接的最大数据大小/最大邮件数设置。
其他设置	以下 管理 > 连接 > 组件 内部端口不迁移： • IMSS 管理器端口 • 策略服务端口
通知	任何扫描程序上的可用磁盘空间 低于在 IMSA 9.0 中更改为以下内容： 任何主机上的数据分区可用空间 低于
策略迁移	BATV 规则和所有相关设置不迁移。

从 IMSS for Linux 中迁移

要从 IMSS for Linux 迁移至 **IMSA 9.0**，请参阅[迁移过程 第 5-34 页](#)。

发生更改的 IMSS 7.1 for Linux 设置

下表提供有关迁移过程中发生更改的所有 **IMSS 7.1 for Linux** 设置的信息。

表 5-4. 发生更改的 IMSS 7.1 for Linux 设置

设置	更改
通知	管理 > 通知 > 事件通知： 任何扫描程序上的可用磁盘空间低于在 IMSA 9.0 中更改为以下内容： 任何主机上的数据分区可用空间低于

发生更改的 IMSS 7.1 SP2 for Linux 设置

除了以下设置外，所有 IMSS 7.1 SP2 for Linux 设置都会迁移至 IMSA 9.0：

- IPv6 网络设置
- 传输层安全性 (TLS) 设置
- 审核日志设置
- 邮件跟踪日志支持的附件名称设置
- 登录通知设置
- 营销邮件例外列表中的电子邮件地址

从 IMSA 8.0 Patch 2、IMSA 8.2 Service Pack 2 或 IMSA 8.5 Service Pack 1 迁移

要从以前版本的 IMSA 迁移至 IMSA 9.0，请参阅[迁移过程 第 5-34 页](#)。

发生更改的 IMSA 8.0 设置

所有 IMSA 8.0 设置都迁移至 IMSA 9.0。

发生更改的 IMSA 8.2 设置

除了以下设置外，所有 IMSA 8.2 设置都会迁移至 IMSA 9.0:

- 所有防毒墙控制管理中心代理设置
- 管理员帐户用户名和密码
- 特征码和引擎
- SMTP 接口和端口号
- 一些影响系统性能的内部设置
- 加密设置
- Deep Discovery Advisor 设置
- TLS 设置
- 营销邮件设置



注意

IMSA 8.2 修补程序 Build 14400 或更高版本中的营销邮件设置无法迁移至 IMSA 9.0。

发生更改的 IMSA 8.5 SP1 设置

除了以下设置外，所有 IMSA 8.5 SP1 设置都会迁移至 IMSA 9.0:

- 所有防毒墙控制管理中心代理设置
- 管理员帐户用户名和密码
- 特征码和引擎
- SMTP 接口和端口号
- 一些影响系统性能的内部设置
- 加密设置

- Deep Discovery Advisor 设置
- TLS 设置
- IPv6 网络设置
- 营销邮件设置

导出调试文件

如果需要分析调试文件以进行故障排除，则可以导出父设备或任何注册到父设备的设备在过去多达两天的调试日志。



注意

调试日志包含在受密码保护的 Zip 文件中。文件的缺省密码为 `trend`。

过程

1. 转到**管理** > **导出调试文件**。
2. 在**扫描程序**旁边，选择一台设备。
3. 选择要导出的天数。
4. 单击**导出**。

该进程可能需要花费 10 分钟到 1 小时或更多，具体取决于日志文件总大小。

第 6 章

故障排除

本节有助于解决您可能会在安装、配置或管理 IMSA 时遇到的常见问题。如有其他问题，请查看趋势科技知识库。

包括以下主题：

- [故障排除实用程序 第 6-2 页](#)
- [组中设备间通信故障排除 第 6-2 页](#)
- [子设备注册故障排除 第 6-3 页](#)
- [子设备取消注册故障排除 第 6-4 页](#)
- [硬件标识错误故障排除 第 6-5 页](#)

故障排除实用程序

请谨慎使用以下与故障排除有关的实用程序和命令。趋势科技建议在修改任何内部 IMSA 文件之前联系支持提供商。

- 防火墙设置检查：

```
iptables -nvxL
```

- PostgreSQL 命令行工具：

```
/opt/trend/imss/PostgreSQL/bin/psql -U sa -d imss
```

- cdt（密码：“trend”）—收集以下信息：

- 配置信息
- 日志
- 内存信息转储

- 其他实用程序：

- **pstack**：显示进程的调用堆栈，包括所有线程
- **ipcs**：列出当前系统中的所有 IPC
- **gdb**：调试程序
- **tcpdump**：嗅探网络软件包
- **netstat**：列出当前网络连接

组中设备间通信故障排除

如果多个 IMSA 设备部署在一个组中，它们必须能够与彼此通信。

过程

1. 确认可访问所有设备上的以下端口：

- 5060: 策略服务
 - 15505: IMSA 控制服务
 - 53 UDP/TCP:IP 分类器
 - 5432: 数据库服务
 - 8009: EUQ 内部服务
 - 389: LDAP 本地缓存服务
 - 999: TLS 设置服务
 - 10030: 邮件投递设置服务
 - 8891: DKIM 设置服务
2. 验证以下内容:
- 当前防火墙设置为“iptables”。
 - `/etc/conf/fw.rules` 中的防火墙配置文件。
 - 数据库中的表“`tb_trusted_ip_list`”有正确设备的 IP 地址。尝试访问此设备的所有其他设备的 IP 地址都必须位于列表中。
3. 验证相关服务是否可访问所有必要端口。
-

子设备注册故障排除

过程

1. 打开父设备的管理控制台并导航到**管理 > IMSA 配置 > 连接 > 子 IP**。
2. 确认子设备的 IP 地址位于子 IP 地址列表中。
3. 在**配置向导**中，确认设备角色选择为**子**。
4. 确认可访问**管理数据库**。

5. 取消注册 MCP 代理（若 MCP 代理已启用）。
6. 确认没有任何注册到父设备的子设备与您尝试注册的设备 IP 地址相同。
7. 删除所有日志和隔离邮件。
8. 更改配置并重新启动服务。
9. 父设备管理控制台（位于配置向导中）进行初始请求。如果遇到任何注册问题，请运行以下命令从控制台获取错误消息：

```
/opt/trend/imss/script/cfgtool.sh reg IPADDR sa postgreSQL
```

子设备取消注册故障排除

过程

1. 通过命令行接口连接至子设备。
2. 检查是否可访问管理数据库。如果可以访问，则从父管理控制台的子 IP 列表中删除子设备，然后更新可信子列表。
3. 救援设备，将其强行从父设备处取消注册。
4. 更新补丁。
5. 要验证子设备是否已从父设备处取消注册，请执行以下任一操作：
 - 尝试访问子设备上的管理控制台。如果可访问该控制台，则设备已成功取消注册。
 - 运行以下命令：

```
/opt/trend/imss/script/cfgtool.sh dereg
```

硬件标识错误故障排除

如果 IMSA 无法识别诸如存储或网络设备等硬件，请先加载驱动程序磁盘，然后再再次尝试安装 IMSA。

与硬件供应商联系，以获取适用于 CentOS 6.4 (x86_64) 的硬件启动程序。然后参考驱动程序的安装指南加载驱动程序磁盘。

以下是加载驱动程序磁盘的示例。

过程

1. 准备好可移动磁盘，例如 USB 软盘。确保可移动磁盘的文件系统可用。
2. 将驱动程序映像复制到 USB 软盘。

```
cp dd.iso /mnt/usb
```

3. 将 IMSA 安装 DVD 插入到 DVD 驱动器中并开始 IMSA 安装。

将显示设置向导窗口。

4. 选择**全新安装或版本升级**，然后按 Tab 键进入编辑模式。
5. 将 **dd** 附加到显示在设置向导窗口底部的信息中。



- 按 Enter 键。

将显示驱动程序磁盘窗口。



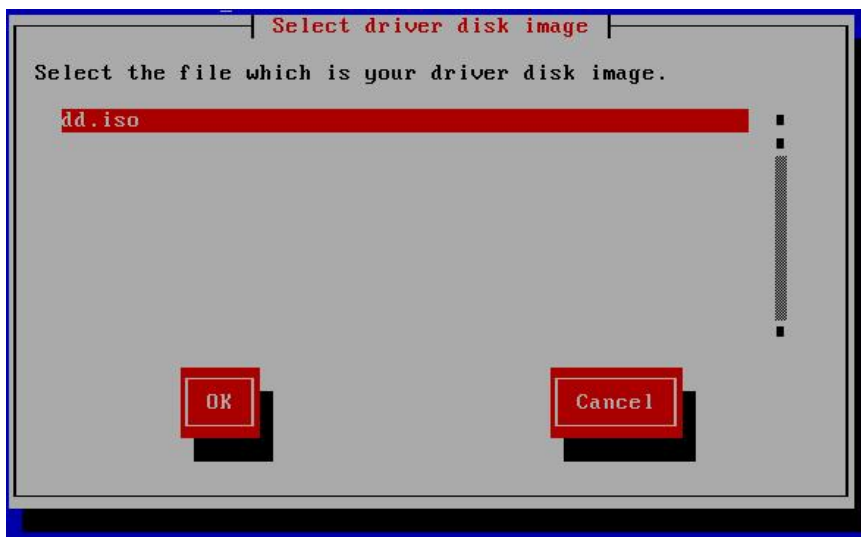
- 插入 USB 软盘并选择是。

将显示驱动程序磁盘来源窗口。



8. 选择 USB 软盘（例如 sdb）并选择**确定**。

将显示**选择驱动程序磁盘镜像**窗口。



9. 选择驱动程序磁盘镜像。

将显示**更多驱动程序磁盘**窗口。



10. 拔出 USB 软盘并单击否，以继续 IMSA 安装。

故障排除网络连接

如果虚拟机出现网络连接问题，请检查分配至 NIC 卡的 MAC 地址是否已发生更改。

有时自动分配至虚拟机的 MAC 地址会发生动态更改。但是，在界面配置文件中记录的 MAC 地址或 udev 永久性网络规则文件中记录的 MAC 地址不会发生更改。因此，NIC 卡可能不可用。

趋势科技 建议使用静态 MAC 地址。如果 MAC 地址发生更改，请执行以下操作以确保 NIC 卡正常工作：

过程

1. 使用以下命令移除 udev 规则文件：

```
rm -rf /etc/udev/70-persistent-net.rules
```

2. 从 /etc/sysconfig/network-scripts/ifcfg-eth<x> 文件中移除以下行：

```
HWADDR=<MAC>
```

```
UUID=<UUID>
```



注意

这些界面配置文件名为 /etc/sysconfig/network-scripts/ifcfg-eth<x>，其中 <x> 是与特定网络接口卡对应的唯一编号。

3. 在 /lib/udev/rules.d/75-persistent-net-generator.rules 文件中找到以下信息：

```
ATTR{addr_assign_type}=="0",  
GOTO="globally_administered_whitelist"
```

4. 在找到的信息前面添加以下行：

```
# ignore VMWare virtual interfaces  
ENV{MATCHADDR}=="00:0c:29:*|00:50:56:*",  
GOTO="persistent_net_generator_end"  
  
# ignore Hyper-V virtual interfaces  
ENV{MATCHADDR}=="00:15:5d:*",  
GOTO="persistent_net_generator_end"
```

5. 重新启动虚拟机以验证网络连接状态。

附录 A

技术支持

本附录介绍趋势科技的各种资源和技术支持信息。

包括以下主题：

- [故障排除资源 第 A-2 页](#)
- [与趋势科技联系 第 A-4 页](#)
- [将可疑内容发送给趋势科技 第 A-5 页](#)
- [其他资源 第 A-6 页](#)

故障排除资源

联系技术支持前，请考虑访问以下趋势科技在线资源。

趋势社区

要获得帮助、分享经验、提出问题以及与其他用户、爱好者和安全专家一起讨论安全问题，请访问：

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

使用支持门户

趋势科技支持门户是一个全天候在线资源，含有常见问题和罕见难题的最新信息。

过程

1. 转到 <http://cn.trendmicro.com/cn/support/techsupport/index.html>。
2. 从相应下拉列表中选择产品或服务，然后指定其他任何相关信息。
此时将显示**技术支持**产品页面。
3. 使用**搜索支持**框搜索可用解决方案。
4. 如果未找到解决方案，请在左侧导航区中单击**提交支持案例**并添加相关详细信息，或在此处提交支持案例：

<http://esupport.trendmicro.com/zh-cn/srf/cnbizmain.aspx>

趋势科技支持工程师会调查案例，并在 24 小时内做出响应。

安全信息社区

趋势科技网络安全专家隶属安全信息精英团队，致力于威胁检测和分析、云和虚拟化安全及数据加密。

转到 <http://www.trendmicro.com/us/security-intelligence/index.html> 了解以下信息：

- 趋势科技博客、Twitter、Facebook、YouTube 和其他社交媒体
- 威胁报告、学术论文和焦点文章
- 来自全球安全领域业内人士的解决方案、播客和新闻简报
- 免费工具、应用和插件。

威胁百科全书

今天，大多数恶意软件都由“混合性威胁”构成，也就是综合使用了两种或更多技术，以期绕过计算机安全协议。为了应对此类复杂的恶意软件，趋势科技推出了能够创建自定义防御战略的产品。威胁百科全书提供了一个全面的混合性威胁名称和症状列表，包括已知的恶意软件、垃圾邮件、恶意 URL 和已知的漏洞。

转到 <http://www.trendmicro.com/vinfo/zh-cn/> 了解更多信息：

- 当前正在活动或肆虐的恶意软件和恶意传播代码
- 全面介绍 Web 攻击的相关威胁信息页面
- 有关针对性攻击和安全威胁的 Internet 威胁建议
- Web 攻击和在线趋势信息
- 每周恶意软件报告。

与趋势科技联系

您可以通过电话、传真或电子邮件与趋势科技销售代表取得联系：

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

- 全球技术支持办公室：
http://cn.trendmicro.com/cn/about/contact_us/index.html
- 趋势科技产品文档：
<http://docs.trendmicro.com/zh-cn/home.aspx>

加快支持呼叫处理速度

为了更好地解决问题，请准备好以下信息：

- 重现问题的步骤
- 网关或网络信息
- 计算机品牌、型号及连接至端点的任何附加硬件
- 内存容量及可用硬盘空间
- 操作系统和 Service Pack 版本
- 端点客户端版本
- 序列号或激活码

- 详细的安装环境说明
- 收到的任何错误消息的确切文本。

将可疑内容发送给趋势科技

可使用几个选项将可疑内容发送至趋势科技以作进一步分析。

文件信誉服务

收集系统信息并将可疑文件内容提交给趋势科技：

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

记录案例编号，以便追踪之用。

电子邮件信誉服务

查询特定 IP 地址的信誉，并指定邮件传输代理，以添加到全局许可列表：

<https://ers.trendmicro.com/>

请参阅下列知识库条目，将邮件样本发送至趋势科技：

<http://esupport.trendmicro.com/solution/zh-CN/1036097.aspx>

Web 信誉服务

查询疑似为网络钓鱼网站或其他所谓的“恶意站点”（故意的 Internet 威胁源，例如间谍软件和恶意软件）的 URL 的安全等级和内容类型：

<http://global.sitesafety.trendmicro.com/>

如果分配的等级不正确，请向趋势科技发送重新分类请求。

其他资源

除了解决方案和支持外，还可在线访问诸多其他有用资源，以便始终掌握各类动态、了解最新创新成果以及洞悉最新安全趋势。

TrendEdge

查找与趋势科技产品和服务有关的不受支持的创新技术、工具和最佳方法。TrendEdge 数据库含有大量文档，覆盖众多主题，可供趋势科技合作伙伴、员工和感兴趣的其他方查阅。

请参阅添加至 TrendEdge 的最新信息：

<http://trendedge.trendmicro.com/>

下载专区

趋势科技可能会不定期地发布一些针对报告的已知问题的补丁或适用于特定产品或服务的升级。要了解补丁是否可用，请转到：

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

如果补丁尚未应用（补丁注有日期），请打开自述文件，确定其是否与您的环境相关。自述文件也包括安装说明。

TrendLabs

TrendLabsSM 是一个全球研究、开发网络及处理措施中心，致力于提供全天候威胁监测、攻击预防以及及时无缝的解决方案。作为趋势科技服务架构的支柱，TrendLabs 包括数百名工程师和获得认证的支持人员，能够提供各类产品和技术支持服务。

TrendLabs 可监控全球威胁环境，进而提供更为有效的安全措施以检测、抢占及消除攻击。每天，这些努力结成的硕果都会通过频繁的病毒码文件更新和扫描引擎优化与客户分享。

通过以下地址了解 TrendLabs 的更多信息：

<http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs>

附录 B

在 VMware ESX 下为 IMSA 创建新的虚拟机

本附录描述了如何为 IMSA 创建新的虚拟机。

包括以下主题：

- [创建新的虚拟机 第 B-2 页](#)

创建新的虚拟机

本文档未涵盖 ESX 4.1/4.0 的实际安装。请参考 VMware 的产品文档来安装此产品。

下列步骤详细说明了在 VMware ESX 下创建用以安装 IMSA 的新虚拟机的过程。请按照以下步骤的指导来创建适用于您的环境的虚拟机。所选 CPU 和 NIC 卡的数量以及内存和硬盘空间的大小应当能够反映您的部署要求。此处输入的值仅作参考。

过程

1. 在菜单栏中，选择**文件 > 新建 > 虚拟机**。

将显示**新建虚拟机向导**。

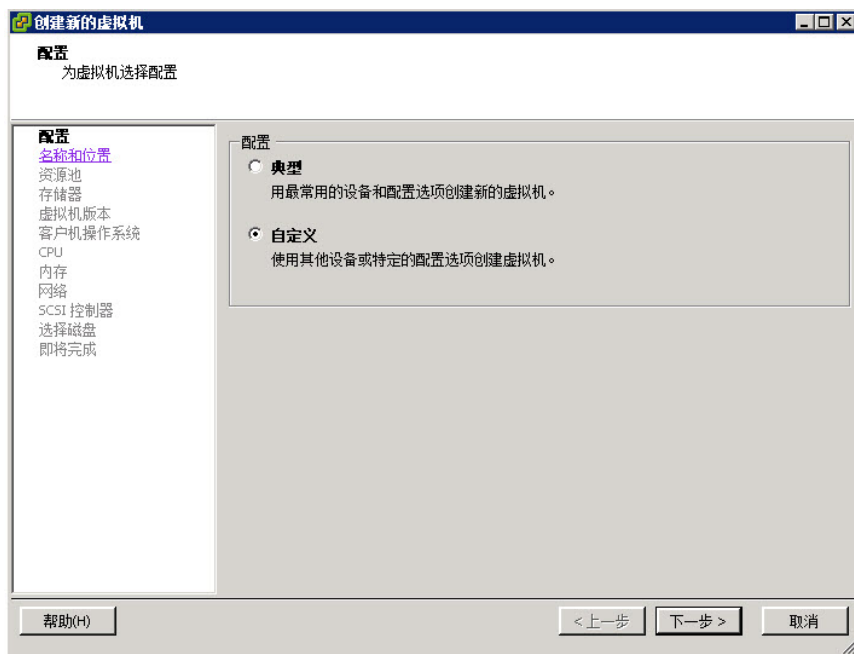


图 B-1. 虚拟机配置

2. 在**虚拟机配置**下，选中**典型**单选按钮。
3. 单击**下一步**。

将显示**名称和位置**窗口。

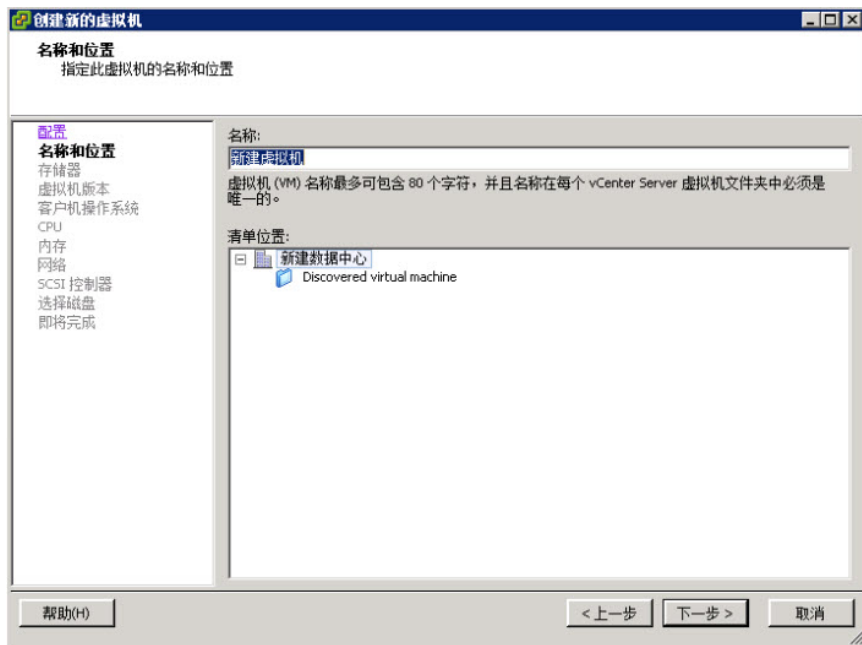


图 B-2. 为该虚拟机选择名称和位置

4. 在**名称**字段中，键入相应的虚拟机名称，然后单击**下一步**。

将显示**数据存储**窗口。

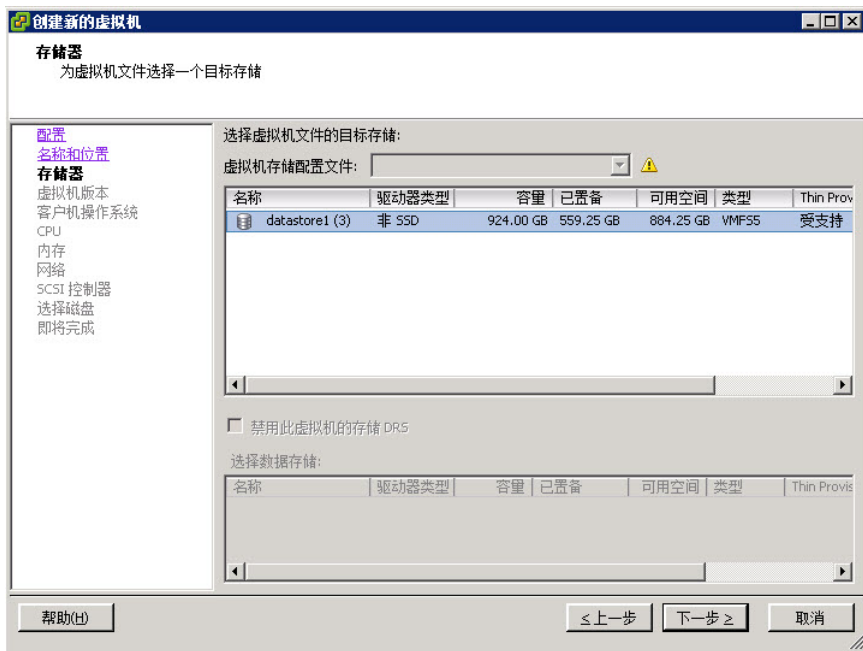
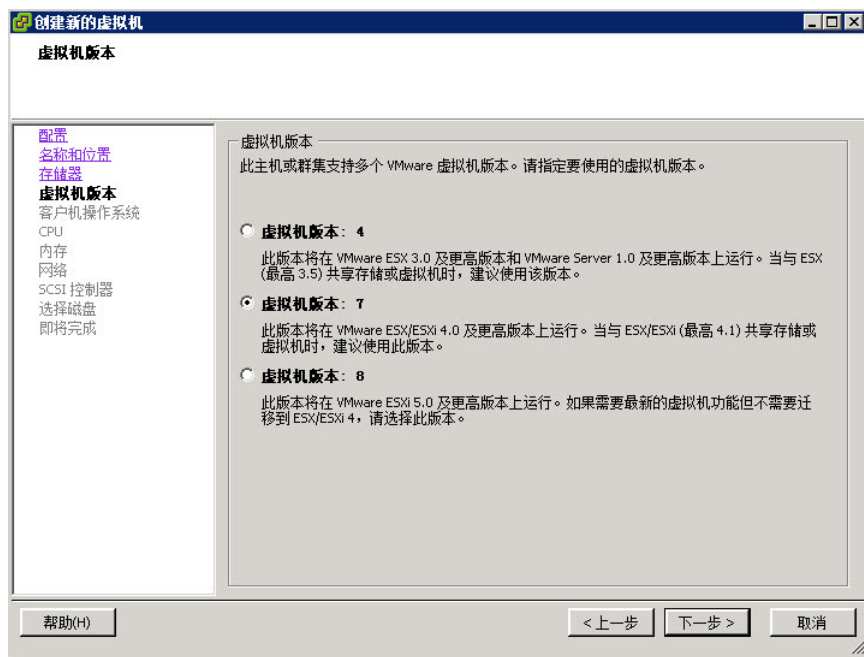


图 B-3. 虚拟机数据存储

5. 选择虚拟机驻留的数据存储。
6. 单击下一步。

将显示**虚拟机版本**窗口。



7. 指定要使用的虚拟机版本。
8. 单击**下一步**。

将显示子操作系统窗口。

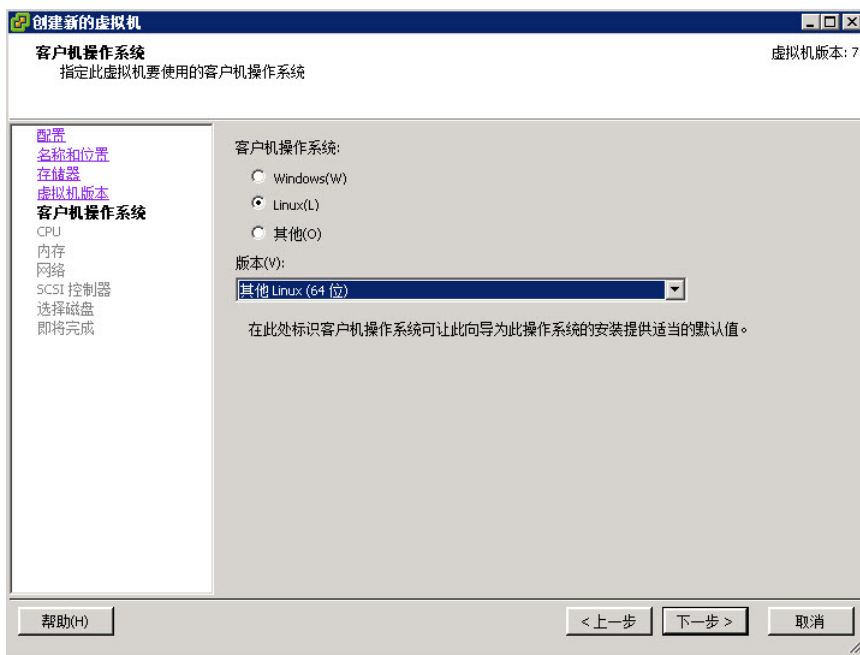


图 B-4. 虚拟机子操作系统

9. 对于子操作系统，请选择 **Linux**，然后选择**其他 Linux (64 位)** 或 **CentOS 4/5/6 (64 位)**。
10. 单击**下一步**。

将显示 CPU 窗口。

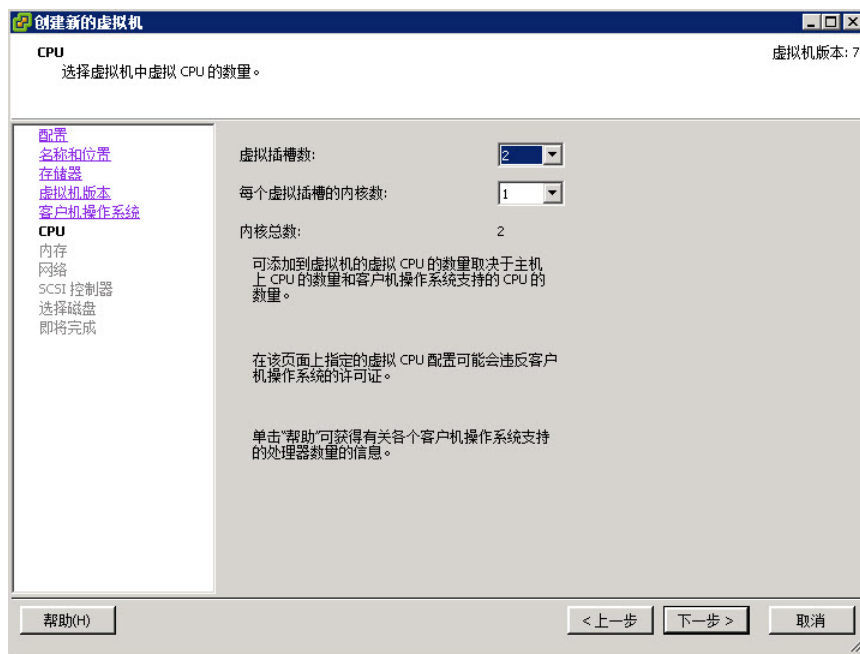


图 B-5. 虚拟机 CPU

11. 选择虚拟机的处理器数量。IMSA 使用了 Virtual SMP，因此，请选择可用虚拟处理器的最大数量。
12. 单击下一步。

将显示内存窗口。

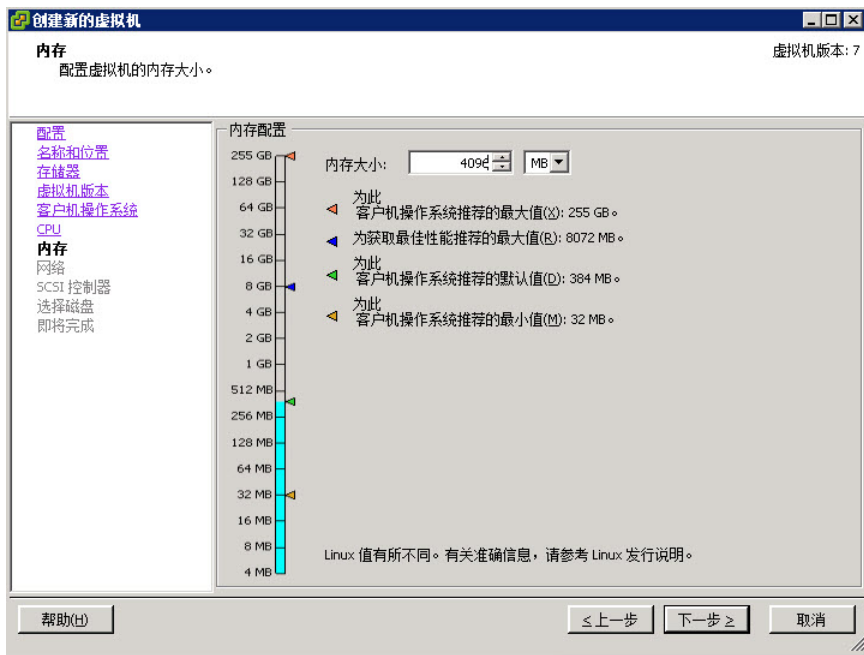


图 B-6. 虚拟机内存

13. 至少为 IMSA 分配 4,096MB 内存。



提示

为了提高性能，趋势科技建议至少 8,192MB 内存。

14. 单击下一步。

将显示**网络**窗口。

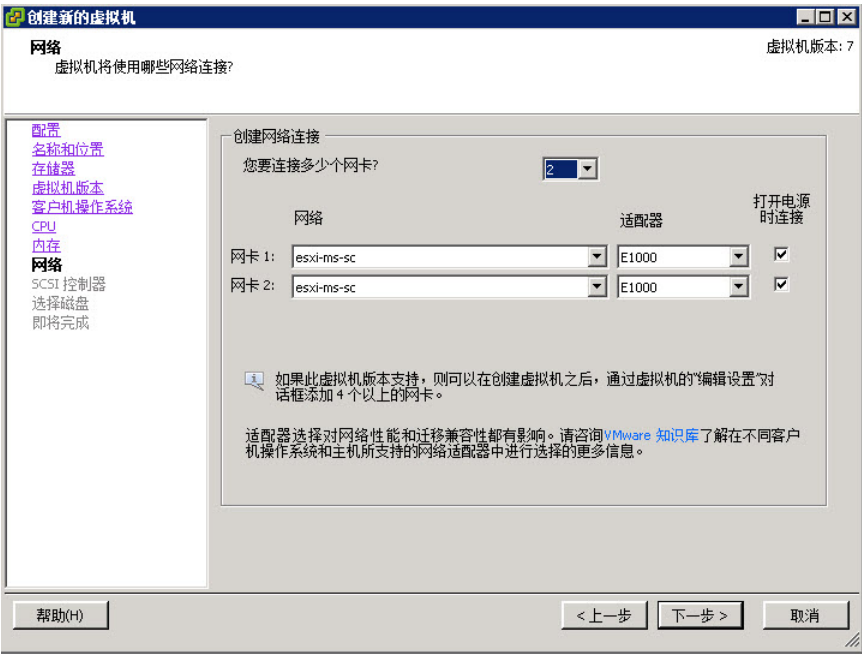
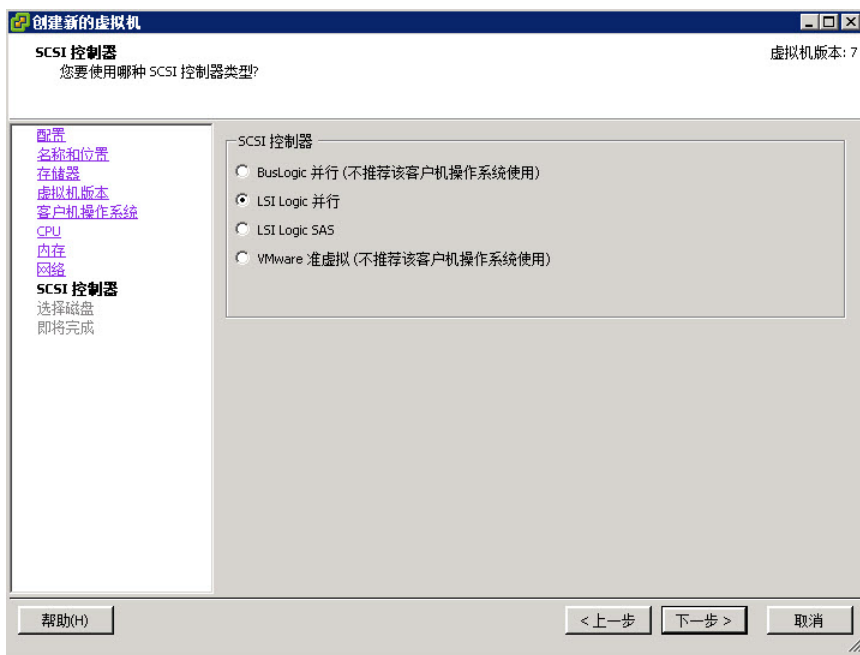


图 B-7. 虚拟机网络

15. 接受缺省网络设置。
16. 单击下一步。

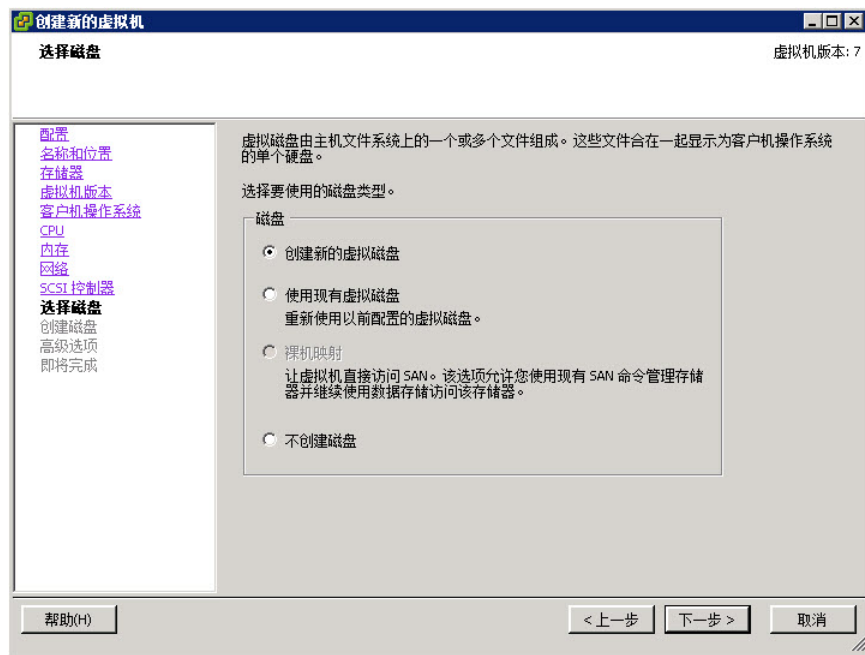
将显示 **SCSI 控制器** 窗口。



17. 选择 **LSI Logic Parallel**。

18. 单击**下一步**。

将显示**选择磁盘**窗口。



19. 选择**创建新的虚拟磁盘**。

20. 单击**下一步**。

将显示**创建磁盘**窗口。

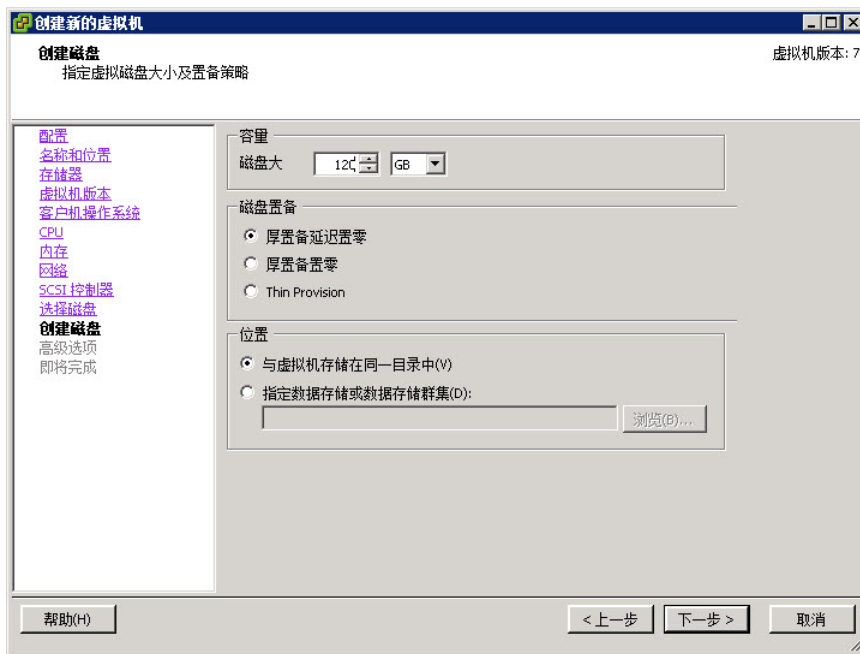


图 B-8. 虚拟磁盘容量

21. 至少指定 120GB 磁盘空间。IMSA 需要至少 120GB 磁盘空间。有关磁盘空间分配的更多信息，请参阅。

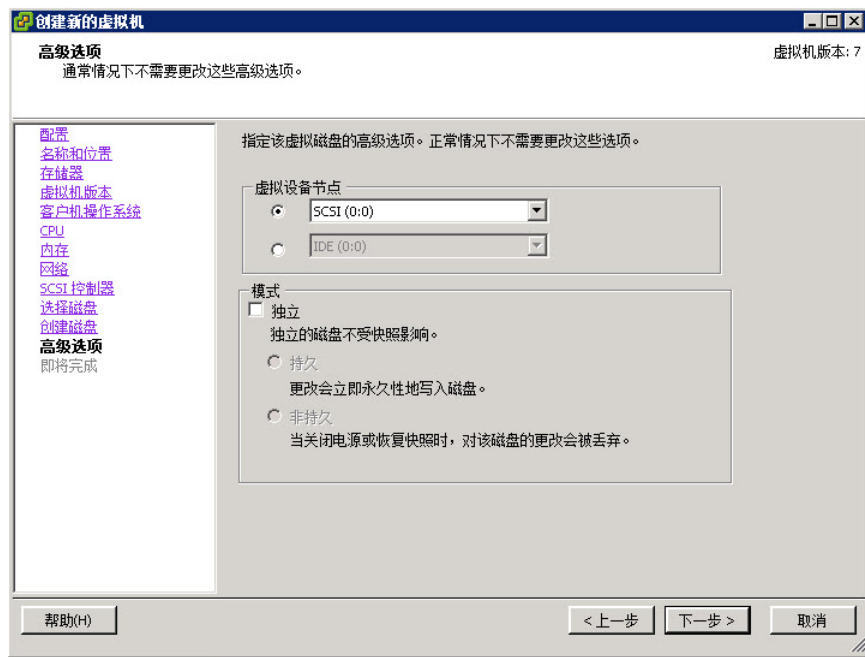


提示

趋势科技建议至少分配 250 GB 磁盘空间用于邮件隔离和日志记录。

22. 单击下一步。

将显示高级选项窗口。



23. 根据需要指定高级选项。通常不需要更改这些选项。

24. 单击下一步。

将显示**准备完成**窗口。

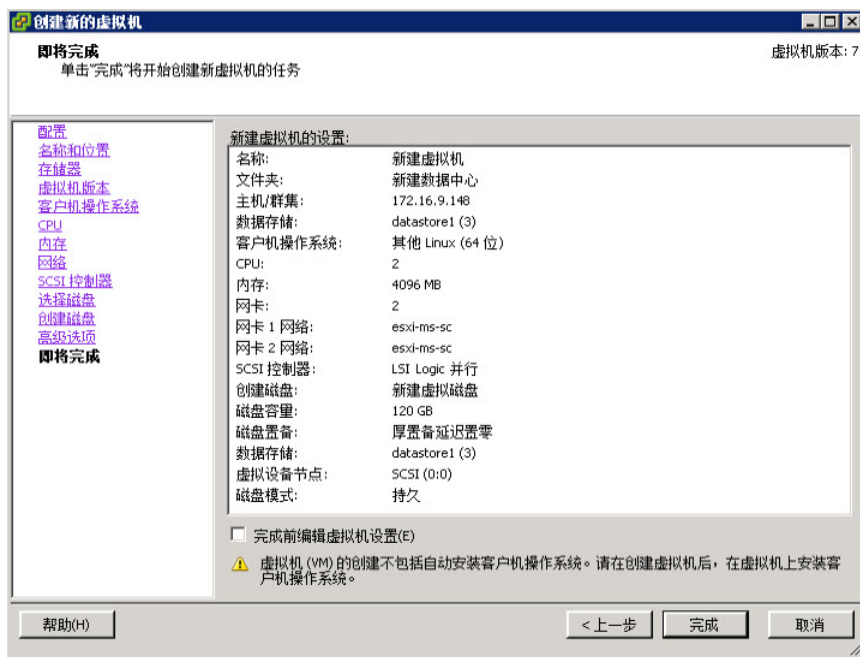


图 B-9. 准备完成

25. 单击**继续**。

如果您要修改系统组件设置，请选中**提交前编辑虚拟机设置**复选框，然后单击**继续**。

26. 验证您的设置，然后单击**完成**。

新虚拟机现在已准备就绪并配置好，可供使用并开始安装过程。

附录 C

在 Microsoft Hyper-V 下为 IMSA 创建新的虚拟机

本附录描述了如何在 Microsoft Hyper-V 下为 IMSA 创建新的虚拟机。

包括以下主题：

- [了解 Hyper-V 安装 第 C-2 页](#)
- [在 Microsoft Hyper-V 上安装 IMSA 第 C-2 页](#)

了解 Hyper-V 安装

IMSA 支持在基于 Microsoft Hyper-V 的虚拟平台上安装。本附录提供了在基于 Hyper-V 的虚拟机上安装 IMSA 的逐步说明。本文档未涵盖 Hyper-V 的实际安装。请参考 Microsoft 产品文档来安装 Hyper-V。本附录中所述的过程介绍了如何在 Windows Server 2008 R2 SP1 Hyper-V 服务器上安装 IMSA。

Hyper-V 的 IMSA 支持

IMSA 在以下平台上支持 Hyper-V:

- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2
- Microsoft Hyper-V Server 2008 R2 SP1
- Microsoft Hyper-V Server 2012 R2

在 Microsoft Hyper-V 上安装 IMSA

请按照以下步骤的指导来创建适用于您的环境的虚拟机。所选 CPU 和 NIC 卡的数量以及内存和硬盘空间的大小应当能够反映您的部署要求。所提供的值仅作参考指导。

创建虚拟网络分配

过程

1. 从 Hyper-V **服务器管理器** 菜单，右击 **Hyper-V 管理器**。

将显示菜单。



图 C-1. 连接至服务器

2. 选择**连接至服务器**。

将显示对话框，提示您选择要连接的虚拟服务器的位置。

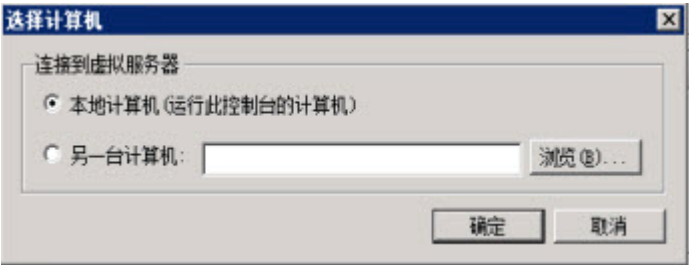


图 C-2. 虚拟服务器的位置

3. 指定虚拟服务器的位置并单击**确定**。
4. 右键单击 Windows 2008 R2 SP1 服务器并选择**虚拟网络管理器**。

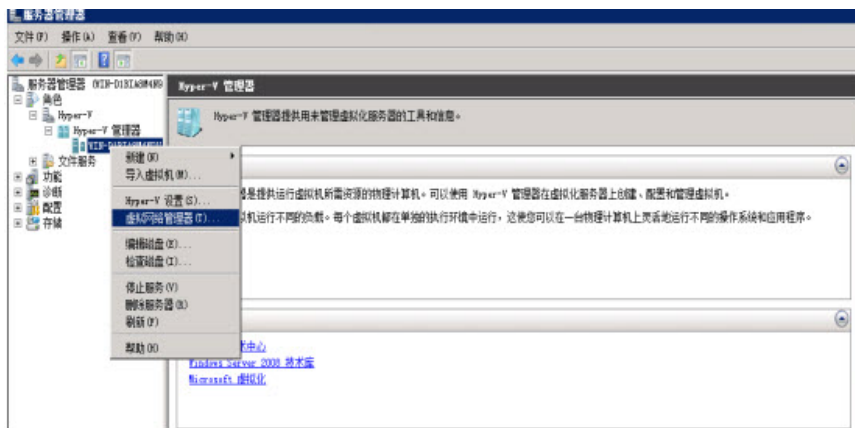


图 C-3. 选择虚拟网络管理器

5. 从选项列表中选择**外部**并单击**添加**创建新的虚拟网络。

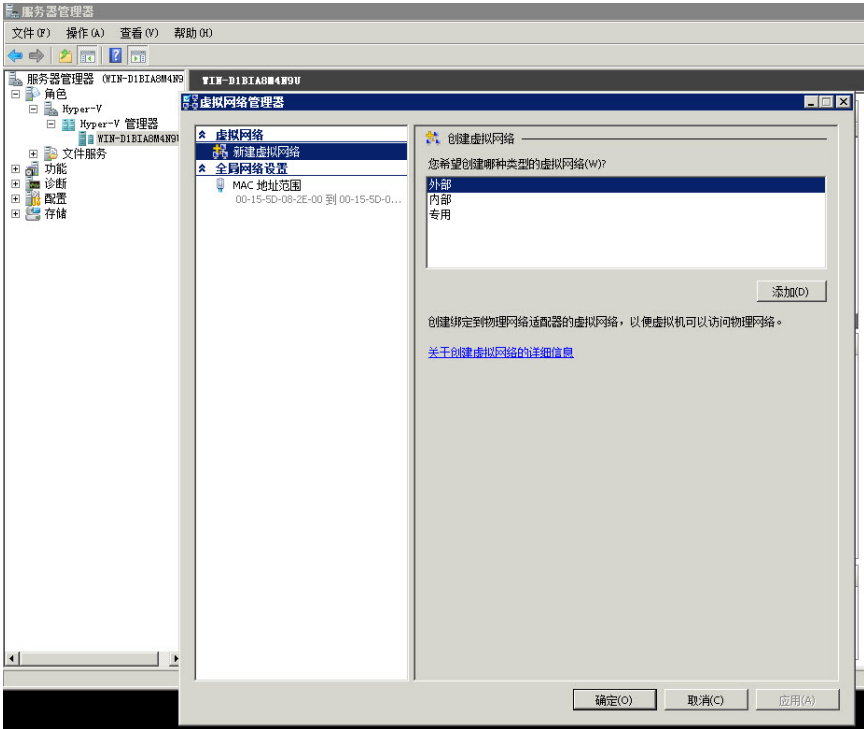


图 C-4. 添加“外部”虚拟网络

6. 从外部下拉菜单中，选择要连接的物理网络适配器。



注意

物理适配器必须连接至网络，并且拥有访问企业网络和 Internet 的权限。

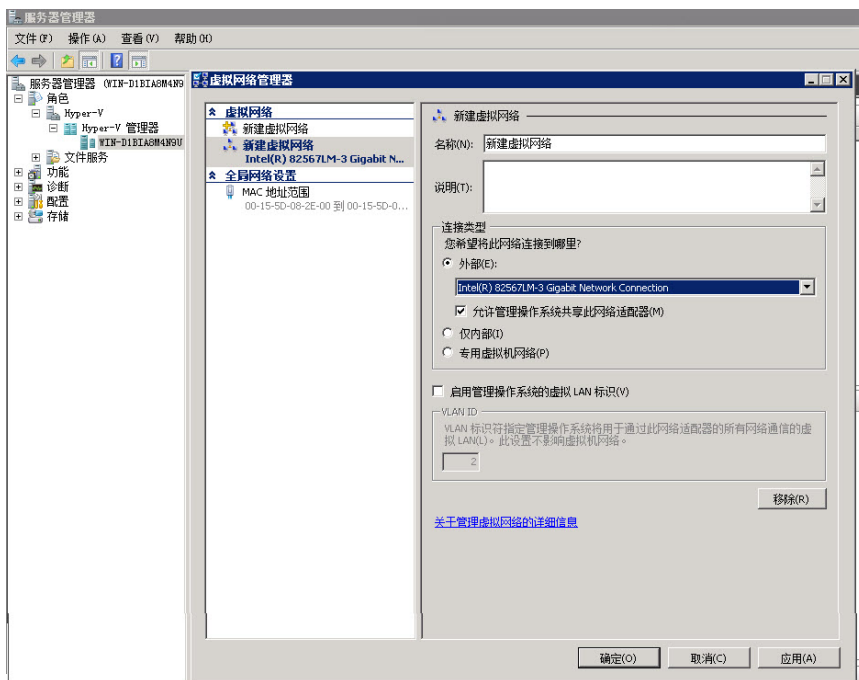


图 C-5. 物理网络适配器选择

创建新的虚拟机

过程

1. 从“Hyper-V 服务器管理器”菜单中，右键单击 Windows 2008 R2 SP1 服务器，然后选择**新建** > **虚拟机**。

将显示**新建虚拟机向导**。



图 C-6. 新建虚拟机向导

2. 单击**下一步**。

将显示**指定名称和位置**窗口。

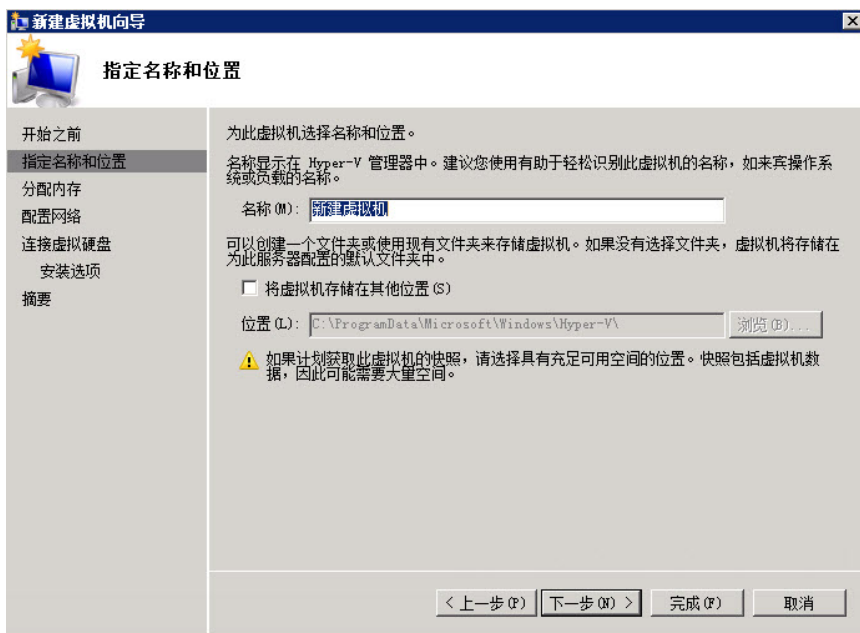


图 C-7. 指定名称和位置

3. 在**名称**字段中，键入有意义的虚拟机名称。如果打算将虚拟机存储在其他文件夹中，请选择**将虚拟机存储在其他位置**并提供正确位置。
4. 单击**下一步**。

将显示**分配内存**窗口。



图 C-8. 分配内存

5. 至少为 IMSA 分配 4,096MB 内存。



提示

趋势科技建议分配 8,192MB 内存。

6. 单击**下一步**。

将显示**配置网络**窗口。



图 C-9. 配置网络

7. 选择在[创建虚拟网络分配](#) 第 C-2 页中创建的虚拟网络。
8. 单击**下一步**。

将显示**连接虚拟硬盘**窗口。



图 C-10. 连接虚拟硬盘

9. 至少为 IMSA 指定 120GB 磁盘空间。



提示

趋势科技建议至少分配 250 GB 磁盘空间用于邮件隔离和日志记录。

10. 指定存储虚拟硬盘的位置，然后单击**下一步**。

将显示**安装选项**窗口。



图 C-11. 安装选项

11. 单击**从引导 CD/DVD-ROM 安装操作系统**，指定安装 ISO 文件以供 IMSA 使用，然后单击**下一步**。

将显示**完成新建虚拟机向导**窗口。



图 C-12. 完成新建虚拟机向导

12. 验证您的设置，然后单击**完成**。

虚拟机现在已准备好启动以开始安装过程。

索引

C

CPU 要求, 4-2

I

IMSA

关于, 1-2

IP 分类器

工作原理, 2-4

关于, 2-3

检测, 2-3

IP 过滤

关于, 2-3

P

POP3

部署规划, 3-14

T

TrendLabs, A-6

W

Web 信誉服务, 1-16

A

安全风险

间谍软件/灰色软件, 1-9

安装

防火墙后面, 3-10

防火墙前面, 3-9

无防火墙, 3-8

在 DMZ 中, 3-11

B

拨号程序, 1-9

C

磁盘空间要求, 4-2

D

电子邮件威胁

垃圾邮件, 1-4

无收益的电子邮件, 1-4

电子邮件信誉

关于, 1-11, 2-5

类型, 1-11, 2-5

E

恶作剧程序, 1-9

F

防毒墙控制管理中心

请参阅趋势科技防毒墙控制管理中
心, 1-13

防毒墙控制管理中心版本要求, 4-3

G

故障排除, 6-1

关于 IMSA, 1-2

Y

广告程序, 1-9

G

过滤, 工作原理, 1-5

H

黑客工具, 1-9

灰色邮件, 1-17

J

集中式报告, 2-8

间谍软件/灰色软件, 1-9

拨号程序, 1-9

恶作剧程序, 1-9

风险和威胁, 1-10

- 广告程序, 1-9
- 黑客工具, 1-9
- 密码破解程序, 1-9
- 侵入网络, 1-10
- 远程访问工具, 1-9

L

- 联机帮助, ix

M

- 密码破解程序, 1-9
- 命令和控制 (C&C) 联系人警报服务, 1-18

N

- 内存要求, 4-2

Q

- 迁移

- 从 IMSA, 5-38
 - 从 IMSS for Linux, 5-37
 - 从 IMSS for Windows, 5-36

- 趋势科技防毒墙控制管理中心, 1-13

- 代理, 1-13
 - 服务器, 1-13

- 群发邮件病毒

- 病毒码, 1-5

S

- 社区, A-2

G

- 适用读者, ix

W

- 文档, ix
- 文件信誉服务, 1-15

X

- 系统要求, 4-2

- 新增功能, viii

- 新增内容, viii

Y

- 要求, 4-2
- 远程访问工具, 1-9
- 云安全智能防护, 1-15
- 云安全智能防护网络, 1-16
- 云端过滤服务, 2-2

Z

- 在线

- 社区, A-2

- 支持

- TrendLabs, A-6
 - 更快解决问题, A-4
 - 知识库, A-2

- 终端用户隔离, 2-7

- 自述文件, x

- 最低要求, 4-2



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: MSCM96870/150302