



安装手册
修订版 C

McAfee® Email Gateway 7.x VMtrial Appliances

版权

Copyright © 2013 McAfee, Inc. 未经许可不得复制。

商标特性

McAfee、迈克菲、McAfee 徽标、McAfee Active Protection、McAfee CleanBoot、McAfee DeepSAFE、ePolicy Orchestrator、McAfee ePO、McAfee EMM、Foundscore、Foundstone、Policy Lab、McAfee QuickClean、Safe Eyes、McAfee SECURE、SecureOS、McAfee Shredder、SiteAdvisor、McAfee Stinger、McAfee Total Protection、TrustedSource、VirusScan 和 WaveSecure 是 McAfee, Inc. 或其子公司在美国和其他国家或地区的商标或注册商标。其他名称和商标可能已声明为其他公司的财产。

产品和功能的名称及说明如有更改，恕不另行通知。请访问 mcafee.com 获取最新的产品和功能。

许可信息

许可协议

致全体用户：请仔细阅读与您所购买的许可相关的法律协议，以了解使用许可软件的一般条款和条件。如果您不清楚所购买的许可属于哪一类，请查看软件包装盒中或购买产品时单独提供的销售文档以及其他相关的许可授权或订单文档，这些文档既可以是小册子、产品光盘上的文件，也可以是软件包下载网站提供的文件。如果您不接受该协议规定的所有条款和条件，请勿安装本软件。根据情况，您可以将产品退回 McAfee, Inc. 或原购买处以获得全额退款。

目录

1	VMtrial 简介	5
	McAfee Email Gateway 的说明	5
	支持的平台	5
	McAfee Email Gateway 功能	6
	评估期	8
	性能	8
	关于 McAfee	9
	关于 VMware	9
	所含内容	9
2	安装 VMtrial	11
	决定如何使用评估版	11
	安装 VMtrial 之前的注意事项	11
	需要收集的网络信息	11
	系统要求	12
	在 VMware vSphere 上安装 VMtrial	12
	在 VMware Player 上安装 VMtrial	13
	配置虚拟设备	14
3	VMtrial 入门	15
	信息显示板	15
	使用信息显示板的好处	16
	信息显示板 Portlet	17
	测试配置	17
	任务 - 测试连接性	17
	任务 - 更新 DAT 文件	18
	使用测试电子邮件生成器	18
	使用测试电子邮件生成器的好处	18
	生成测试电子邮件	18
	任务 - 生成大批测试电子邮件	19
	任务 - 查看已扫描电子邮件通讯的摘要	19
	任务 - 查找特定的测试电子邮件	19
	浏览设备功能	20
	策略简介	20
	加密	20
	合规性设置	22
	Data Loss Prevention 设置	24
	任务 - 识别隔离的电子邮件	25
	索引	27

1

VMtrial 简介

McAfee Email Gateway Appliance (VMtrial) 可让您在 VMware vSphere 或 VMware Player 上评估最新的 McAfee Email Gateway Appliance。

目录

- ▶ McAfee Email Gateway 的说明
- ▶ 支持的平台
- ▶ McAfee Email Gateway 功能
- ▶ 评估期
- ▶ 性能
- ▶ 关于 McAfee
- ▶ 关于 VMware
- ▶ 所含内容

McAfee Email Gateway 的说明

McAfee Email Gateway 是一个易于管理的集成设备，它能够针对 SMTP 和 POP3 提供全面的企业级保护，以抵御电子邮件中存在的威胁。

如果您在完成本次评估之后购买 McAfee Email Gateway，McAfee 可以提供设备附带的相关硬件及其他物品；或者您也可以通过虚拟设备访问此软件。

支持的平台

McAfee Email Gateway Appliance (VMtrial) 可在以下虚拟平台上运行：

- VMware vSphere (ESX) 4.x
- VMware vSphere Hypervisor (ESXi) 4.x
- VMware Player 3.x

McAfee Email Gateway 功能

下面的信息将说明产品的各项功能及它们在产品界面中的位置。

电子邮件扫描功能

功能	说明
全面扫描保护	针对下列网络协议提供防病毒和反垃圾邮件保护： • SMTP • POP3
防病毒保护	“Email” “Email Policies” “Anti-Virus” 使用下列设置减少对所有协议通讯的威胁： • 防病毒设置：用以识别存档文件与其他类型文件中已知和未知的病毒威胁 • 其他威胁检测设置：用以检测病毒、潜在有害程序、打包程序和其他恶意软件 • McAfee Global Threat Intelligence 文件信誉：让设备可以访问大量云签名，从而弥补 DAT 签名的不足之处；这将缩短从 McAfee 检测出新的恶意软件威胁到该威胁纳入 DAT 文件之间的延迟时间，拓广覆盖范围
反垃圾邮件保护	“Email” “Email Policies” “Spam” 使用下列技术减少 SMTP 和 POP3 电子邮件通讯中的垃圾邮件： • 反垃圾邮件引擎、反垃圾邮件和反网络钓鱼规则集 • 允许和拒绝的发件人列表 • McAfee Global Threat Intelligence 邮件信誉：用以识别垃圾邮件的发件人 • 管理员和用户可以使用 Microsoft Outlook 插件创建的允许和拒绝列表（仅限用户级别） 检测网络钓鱼攻击并采取相应措施。
加密	“电子邮件” “加密” McAfee Email Gateway 提供了数种加密方法： • 服务器到服务器加密 • Secure Web Mail • 提取传递 • 推送传递 加密功能可以设置为向其他扫描功能提供加密服务，也可以设置为仅用于加密邮件的仅加密服务器。
McAfee Global Threat Intelligence 反馈	“Email” “Email Policies” “Policy Options” “McAfee GTI feedback” “系统” “安装向导” McAfee 会从大量客户那里收集并分析检测项和警报数据、威胁详细信息及使用率统计信息，以对抗电子攻击、保护脆弱的系统免遭漏洞攻击，并挫败网络犯罪活动。只要在产品中启用此项反馈服务，即可帮助改善 McAfee Global Threat Intelligence，从而提高 McAfee 产品的效率，并协助 McAfee 与执法机构合作以解决电子威胁。

功能	说明
合规性设置	“Email” “Email Policies” “Compliance” 此版本产品包含的增强功能对设备使用合规性规则的方式进行了改进： - 在“合规性”策略中，可以使用“规则创建向导”指定要遵从的内置字典，也可以使用现有规则作为模板创建新规则。 - 使用“邮件大小过滤”和“文件过滤”策略可以检查 SMTP 电子邮件的真实文件类型，并根据附件大小和数目执行操作。
Data Loss Prevention	“电子邮件” “DLP 与合规性” 使用“Data Loss Prevention”策略可以上载并分析您的敏感文档（称为“学习”），然后创建每份文档的指纹。
邮件搜索	“报告” “邮件搜索” 借助“邮件搜索”功能，您在用户界面中的一个位置便可以确认流经设备的电子邮件的状态。它可以向您提供电子邮件的相关信息，包括电子邮件是已传递、遭阻止、已退回、已隔离，还是排在队列中等待进一步操作。
隔离功能	“电子邮件” “隔离配置” “隔离选项” “隔离摘要” - 允许用户在没有电子邮件管理员参与的情况下处理隔离项目。 “McAfee Quarantine Manager” - 将各种 McAfee 产品的隔离管理功能整合在一起。
消息传输代理	- 根据管理员设置的条件实时重新路由通讯。例如，可以重新路由加密邮件以进行解密。 - 允许管理员决定每封邮件的最终状态。 - 按域查看入站电子邮件（各域可逐级展开）和未发送电子邮件的快速视图摘要。 - 根据域确定重新发送未发送电子邮件的优先级。 - 将多封电子邮件一并传送到每个域。 - 根据管理员定义的正则表达式重写入站和出站电子邮件上的电子邮件地址。 - 清除出站邮件上的电子邮件报头，从而隐藏内部网络基础架构。 - 使用 TLS 传递邮件。 - 管理证书。

报告和系统功能

功能	说明
计划报告	“报告” “计划的报告” 安排报告定期运行，并发送给一个或多个电子邮件收件人。
日志记录选项	“系统” “日志记录、警报和 SNMP” 您可以配置设备，让其通过电子邮件发送与病毒及其他检测到的威胁相关的信息，并使用 SNMP 传输设备中的信息。
信息显示板统计数据	“信息显示板” 信息显示板可让您在一个位置查看设备的活动摘要，包括流经设备的电子邮件和设备的总体系统状况等。您还可以直接转到用户界面上您经常使用的各区域。

功能	说明
ePolicy Orchestrator 的设备管理功能	“系统” “安装向导” 选择“ePO 托管设置”选项可通过 ePolicy Orchestrator 监控设备状态并对设备进行管理。 设备可以直接通过 ePolicy Orchestrator 进行管理，而无需启动每台设备的界面。 在 ePolicy Orchestrator 中，用于配置和管理设备的用户界面页面在外观和操作上都与设备中的页面类似。
群集管理	“系统” “系统管理” “群集管理” 群集管理允许您设置多个协同工作的设备组以分担扫描工作负载，并在发生硬件故障时提供冗余。 您可以使用这些页面备份和还原配置、将配置从一台设备推送到其他设备，以及设置设备之间的负载均衡。
虚拟主机	“系统” “虚拟主机托管” “虚拟主机” 对于 SMTP 协议，您可以指定设备用于接收或截取入站地址池上的通讯的地址。 通过虚拟主机功能，一台设备可以发挥多台设备的效用。每台设备可以管理指定 IP 地址池中的通讯，这样设备便能够为众多客户的通讯提供扫描服务。
基于角色的访问控制	“系统” “用户” “用户和角色” “系统” “用户” “登录服务” 除了 Kerberos 身份验证方法外，还可以使用 RADIUS 身份验证。

评估期

评估期间，您可以不受限制地使用 McAfee® Email Gateway Appliance (VMtrial) 的各项功能，保护您组织免受垃圾邮件、网络钓鱼、病毒、不良内容、数据丢失及其他威胁的侵扰。

评估期为 30 天，期满后 Virtual Appliance 将停止运行。评估期结束时，VMtrial 登录页面上的“到期信息”对话框会提示您“此试用版现已到期”。届时，所有功能都会停止运行。通讯将继续流经 VMtrial 设备，但不会经过扫描。



如果评估到期时您尚未完成评估工作，可以保存配置，然后启动下一个评估过程并应用您原先的配置设置。

如果要在评估的基础上购买产品，请联系您首选的代理商。要查找代理商，请转至 <http://www.mcafee.com> 查找代理商或分销商合作伙伴，或者联系销售代表。

性能

使用虚拟软件可模拟 McAfee 设备对设备性能和通讯吞吐量的影响。

评估期间的扫描吞吐量并不代表相似硬件规格下 McAfee 设备可达到的性能。性能和通讯吞吐量还会受主机规格和 Internet 连接带宽的影响。

关于 McAfee

McAfee 是 Intel Corporation (NASDAQ:INTC) 的全资子公司，也是全球最大的专业安全技术公司。McAfee 提供具有前瞻性且经实践检验的解决方案和服务，保护全球各地的系统、网络和移动设备的安全，使用户能够更安全地连接 Internet 并在网上冲浪与购物。McAfee 凭借其无以媲美的 Global Threat Intelligence，为家庭用户、企业、公共部门及服务提供商提供创新产品和强大支持，协助他们遵从法规、保护数据、防止运营中断、发现漏洞，以及持续监控安全问题并提高安全性。McAfee 致力于不断探寻新方法来确保用户安全。

关于 VMware

VMware (NYSE:VMW) 是全球领先的虚拟化和云基础架构解决方案提供商，所提供的经客户验证的解决方案可以大幅降低复杂性，并实现更灵活快捷的服务交付，从而加速 IT 发展。VMware 可让企业采用合适的云模式以应对其特有的业务挑战。VMware 加快了组织机构向云计算的过渡，使其既能保护现有的 IT 投资，又能提高安全性和控制能力。VMware 目前拥有超过 250,000 万家客户和 250,000 万家合作伙伴，所提供的解决方案能够帮助各种规模的组织降低成本、提高业务活力并确保选择的自由。

所含内容

评估版 .zip 文件中包含以下几项内容：

- McAfee Email Gateway Appliance (VMtrial) 安装文件
- McAfee Email Gateway Appliance (VMtrial) 安装手册

信息来源

安装和配置信息可参阅：

- **联机帮助**
 - 配置控制台包含页面相关帮助信息，可引导您完成整个安装过程。
 - 安装完成后，产品界面上会提供详细的上下文相关帮助，并带有“搜索”与“索引”功能。其中提供产品及其功能简介、软件配置的详细说明、重复性任务的相关信息以及操作程序。
- **知识库** - 在 McAfee 知识库中查找 McAfee Email Gateway Appliance 相关问题的答案。
转至 <https://mysupport.mcafee.com/>，然后单击“Browse the KnowledgeBase”（浏览知识库）。在“Product”（产品）列表中，选择“Email Gateway”。
- **文档** - 您可以访问最新版本的 McAfee Email Gateway Appliance 文档。
转到 <https://mysupport.mcafee.com/>，然后单击“Product Documentation”（产品文档）并选择“Email Gateway”。



有关 VMware vSphere 或 VMware Player 的帮助，请转到 <http://www.vmware.com>，在“Search VMware Knowledge Base”（搜索 VMware 知识库）方框中键入您的问题，然后单击“Search”（搜索）。

2

安装 VMtrial

以下信息可帮助您筹备评估环境，并列举了在安装 McAfee Email Gateway Appliance (VMtrial) 之前需要考虑的几个因素。

目录

- ▶ 决定如何使用评估版
- ▶ 安装 VMtrial 之前的注意事项
- ▶ 需要收集的网络信息
- ▶ 系统要求
- ▶ 在 VMware vSphere 上安装 VMtrial
- ▶ 在 VMware Player 上安装 VMtrial
- ▶ 配置虚拟设备

决定如何使用评估版

开始安装评估版时，您必须确定是否要实现以下目标：

- 使用 McAfee Email Gateway Appliance (VMtrial) 扫描网络中的电子邮件通讯。
- 只评估 McAfee Email Gateway Appliance 的功能和界面选项。

安装 VMtrial 之前的注意事项

如果要让 McAfee Email Gateway Appliance (VMtrial) 扫描网络中的电子邮件通讯，请在开始安装之前考虑以下因素：

- 要扫描的协议有哪些？请在 SMTP 和 POP3 中进行选择。
- 是否要在不更改客户端或服务器设置的情况下扫描这些协议？
- 您的网络是否有 DMZ？如果有，其中配置了哪些服务器？
- 是否有内部 DNS 服务器？
- 要使用的操作模式。选择显式代理模式、透明网桥模式或透明路由器模式。有关各种操作模式的特点，请参阅 <https://mysupport.mcafee.com> 上提供的《McAfee Email Gateway 虚拟设备安装手册》。



如果 VMware vSphere 已安装并在操作环境中正常运行，McAfee 建议您使用它来运行 McAfee Email Gateway Appliance (VMtrial)。

需要收集的网络信息

开始安装前应收集以下信息：

- 要扫描的协议 (SMTP、POP3)
- 主机名
- 域名
- 默认网关
- 设备运行模式：显式代理、透明路由器、透明网桥。



有关操作模式的信息，请参阅 <http://mysupport.com> 上提供的《McAfee Email Gateway 虚拟设备安装手册》“”。

- LAN1 端口 IP 地址和子网掩码
- LAN2 端口 IP 地址和子网掩码
- DNS 服务器 IP 地址
- 任何转发电子邮件服务器 IP 地址

系统要求

如果您计划在生产环境中使用 VMtrial，请注意，通讯吞吐量和性能会低于具有相似硬件规格的设备。



VMtrial 无法在 FAT32 文件系统中运行。

组件	值
处理器	2.8 GHz Pentium 4 处理器，支持物理地址扩展 (PAE)
可用内存	1 GB
可用硬盘空间	50 GB
虚拟环境	如果 VMware vSphere 已安装并在操作环境中正常运行，McAfee 建议您使用它来运行 McAfee Email Gateway Appliance (VMtrial)。
浏览器	设备的界面经过优化，适用于 Microsoft Internet Explorer 7.0 (或更高版本) 以及 Mozilla Firefox 3.6 (或更高版本)。

在 VMware vSphere 上安装 VMtrial

使用下列任务可将 McAfee Email Gateway Appliance (VMtrial) 安装到运行 VMware vSphere 4.x 或 VMware vSphere Hypervisor (ESXi) 4.x 的主机上。

开始之前

- 从 McAfee 下载站点下载 McAfee Email Gateway Appliance (VMtrial) 包的 .zip 文件，然后将其解压缩到 VMware vSphere Client 可以访问的位置。
- 安装 VMware vSphere 4.x 或 VMware vSphere Hypervisor (ESXi) 4.x 的完整授权版。

McAfee Email Gateway Appliance (VMtrial) 会使用 DHCP 自动配置以下参数：

- 主机名
- 域名
- 默认网关
- DNS 服务器

设备重新启动时会显示控制台，直到您完成设置。

任务

- 1 启动 VMware vSphere Client 应用程序。
- 2 登录 VMware vSphere 服务器或 vCenter Server。
- 3 在“Inventory”（库存）列表中，选择要导入 Virtual Appliance 软件的主机或群集。
- 4 单击“File”（文件）|“Deploy OVF Template”（部署 OVF 模板）|“Deploy From File”（从文件部署），然后单击“Browse”（浏览）转至从 McAfee 下载站点下载的 .zip 文件的解压缩位置。
- 5 打开 .zip 文件中的 VMtrial 子文件夹，然后选择“McAfee_MEG_VMtrial.vSphere_ESX.ovf”文件并单击“Open”（打开）。
- 6 单击两次“Next”（下一步），选择性地输入一个新名称。
- 7 选择要使用的资源池（如有配置）。
- 8 选择要使用的数据存储器，然后单击“Next”（下一步）。
- 9 选择 Virtual Appliance NIC 将连接到的虚拟网络：
- 10 单击“Next”（下一步），阅读摘要，然后单击“Finish”（完成）并等待导入完成。



您可以在多个 VMware vSphere 服务器上安装 Virtual Appliance。

在 VMware Player 上安装 VMtrial

使用下列任务可将 McAfee Email Gateway Appliance (VMtrial) 安装到运行 VMware Player 的主机上。

开始之前

从 McAfee 下载站点下载 McAfee Email Gateway Appliance (VMtrial) 包的 .zip 文件，然后将其解压缩到您计划运行评估版的计算机上。

从 <http://www.vmware.com/go/get-player> 下载 VMware Player。

McAfee Email Gateway Appliance (VMtrial) 会使用 DHCP 自动配置以下参数：

- 主机名
- 域名
- 默认网关
- DNS 服务器

设备重新启动时会显示控制台，直到您完成设置。

任务

- 1 以管理员身份登录计算机。
- 2 安装 VMware Player：
 - a 双击 VMware Player 安装文件，然后单击“Run”（运行）启动安装程序。
 - b 单击“Next”（下一步），并在安装程序的后续页面中选择所需的选项。
 - c 在最后一页中，单击“Continue”（继续）开始安装。



您必须重新启动计算机才能运行 McAfee Email Gateway Appliance (VMtrial)。

- 3 运行 VMtrial 安装文件：
 - a 浏览到解压缩的 McAfee Email Gateway Appliance (VMtrial) 包 .zip 文件所在的文件夹。
 - b 打开“VMtrial”文件夹。
 - c 双击“McAfee_MEG_VMtrial.VMware_Player.vmx”文件。

VMware Player 即会启动，然后开始安装。



您可以在多个 VMware Player 服务器上安装 Virtual Appliance。

配置虚拟设备

使用下列任务可以配置 Virtual Appliance。

开始之前

确保您的虚拟环境已安装并正常运行。

任务

- 1 启动 Virtual Appliance。安装将会自动启动。
- 2 阅读最终用户许可协议以继续安装，然后单击 **y** 加以接受并开始安装。
- 3 在安装菜单中，选择“**a**”可执行完整安装，选择“**y**”可继续。
- 4 安装完成后，Virtual Appliance 将重新启动。
- 5 在“欢迎”屏幕中，选择要使用的语言。
- 6 接受许可协议的条款。
- 7 在图形配置向导中配置虚拟设备。
- 8 将配置应用于 Virtual Appliance。根据输入的设置，设备可能会重新启动。您可以在多个 VMware vSphere、VMware vSphere Hypervisor 或 VMware Player 服务器上安装 Virtual Appliance。为此，请执行下列操作：
 - a 按照本任务中的步骤在另一个 VMware vSphere、VMware vSphere Hypervisor 或 VMware Player 服务器上执行操作。
 - b 返回到先前安装的 Virtual Appliance 的用户界面。
 - c 选择“系统”|“系统管理”|“配置推送”将配置详细信息发送到另一台 Virtual Appliance。

3

VMtrial 入门

以下信息介绍构成 McAfee Email Gateway Appliance (VMtrial) 的各个界面元素。

目录

- ▶ 信息显示板
- ▶ 测试配置
- ▶ 使用测试电子邮件生成器
- ▶ 浏览设备功能

信息显示板

“信息显示板”提供设备活动的摘要。



“信息显示板”

使用此页面可以访问用于控制设备的大多数页面。

在群集主设备上，使用此页面还可以查看有关设备群集的活动摘要。

使用信息显示板的好处

“信息显示板”为您提供了一个可通过一系列 Portlet 查看设备活动摘要的单个位置。

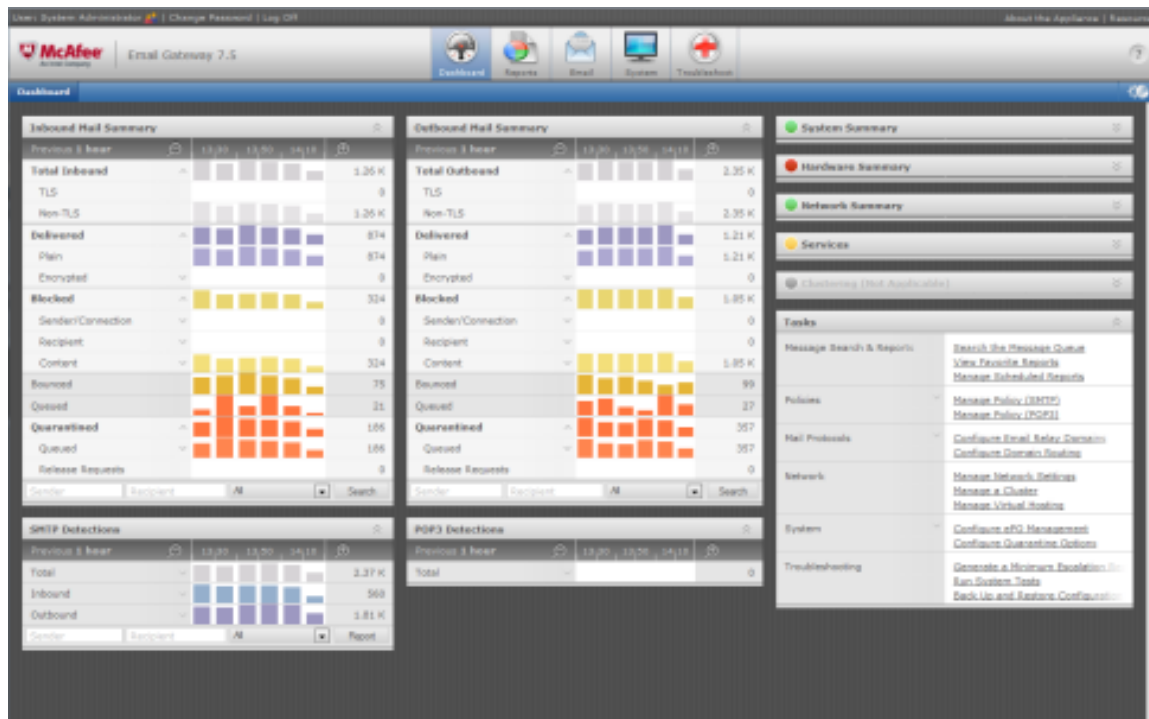


图 3-1 信息显示板 Portlet

一些 Portlet 会显示图形，展示以下时间段内设备的活动：

- 1 小时
- 2 周
- 1 天 (默认)
- 4 周
- 1 周

在“信息显示板”中，您可以对显示的信息和图形进行更改：

- 使用 Portlet 右上角的 和 图标展开和折叠 Portlet 数据。
- 使用 和 按钮深入查看特定数据。
- 查看状态指示符，了解项目是否需要处理：
 - “健康” - 所报告的项目当前运行正常
 - “需要注意” - 已超出某个警告阈值
 - “需要立即处理” - 已超出某个重要阈值
 - “已禁用” - 服务未启用
- 使用 和 可放大和缩小信息的时间轴。更新视图时，可能会发生短暂的延迟。“信息显示板”默认显示与前一天相关的数据。
- 将 Portlet 移到“信息显示板”上的其他位置。

- 双击 Portlet 顶栏，将其扩展至整个“信息显示板”的顶端。
- 设置自己的警报和警告阈值以触发事件。方法是突出显示项目并予以单击，编辑警报和警告阈值字段，然后单击“保存”。一旦某项目超出所设的阈值，就会触发事件。



根据用于查看 McAfee Email Gateway 用户界面的浏览器，“信息显示板”会“记住”每个 Portlet 的当前状态（是展开的还是收叠的，您是否深入查看了特定数据）；如果您浏览至用户界面的其他页面，然后在同一浏览会话中回到“信息显示板”，则它会尝试重新展现原先的视图。

信息显示板 Portlet

了解 McAfee Email Gateway 用户界面中信息显示板上的 Portlet。

选项	定义
“入站邮件摘要”	使用“入站邮件摘要” Portlet 可以获取有关发送到您组织的邮件的传递和状态信息。
“出站邮件摘要”	使用“出站邮件摘要” Portlet 可以获取有关从您组织发出的邮件的传递和状态信息。
“SMTP 检测项”	使用“SMTP 检测项” Portlet 可了解共有多少邮件因发件人（或连接）、收件人或内容而触发相应的检测，并可查看入站或出站 SMTP 通讯中的特定数据。
“POP3 检测项”	使用“POP3 检测项” Portlet 可查看有多少邮件因存在病毒、打包程序或潜在的不良图像等威胁而触发检测。
“系统摘要”	使用“系统摘要” Portlet 显示负载平衡、每个分区已用的磁盘空间、CPU 总使用率、已用和可用内存的相关信息，以及交换率的详细信息。
“硬件摘要”	使用“硬件摘要” Portlet 通过状态指示符显示有关网络接口、UPS 服务器、网桥模式（若已启用）以及 RAID 状态的信息。
“网络摘要”	使用“网络摘要” Portlet 提供有关连接、网络吞吐量以及与内核阻止模式相关的计数器的信息。
“服务”	使用“服务” Portlet 根据设备所用的协议和外部服务器来显示更新和服务状态统计信息。
“群集”	使用“群集” Portlet，在您已将设备配置为某个群集的一部分或者在您使用刀片服务器硬件时，将会提供有关整个群集的信息。
“任务”	使用“任务” Portlet 直接链接到用户界面上的各区域，以搜索邮件队列、查看报告、管理策略、配置邮件协议设置与网络和系统设置，以及访问故障排除功能。

测试配置

以下信息介绍如何测试设备在安装后是否正确运行。

目录

- 任务 - 测试连接性
- 任务 - 更新 DAT 文件

任务 - 测试连接性

使用下列任务可确认基本连接。

McAfee Email Gateway 会检查它能否与网关、更新服务器和 DNS 服务器进行通信，并确认设备名称和域名是否有效。

任务

- 1 在导航栏中选择“故障排除”，或在信息显示板的“任务”区域中选择“运行系统测试”。
- 2 单击“测试”选项卡。
- 3 单击“开始测试”。

每项测试都应能正确返回值。

任务 - 更新 DAT 文件

使用下列任务可确保 McAfee Email Gateway 拥有最新的检测定义 (DAT) 文件。建议在配置扫描选项之前先更新这些 DAT 文件。

使用 McAfee Email Gateway 进行更新期间，您可以选择更新个别类型的定义文件，并根据需求更改默认的计划更新。

任务

- 1 选择“系统”|“组件管理”|“更新状态”。
 - 2 若要更新防病毒引擎和防病毒数据库，可单击“立即更新”。
- 若要检查更新是否正确应用，则在信息显示板中打开“服务”Portlet，并展开“更新”状态。防病毒组件的状态将显示为绿色。

使用测试电子邮件生成器

McAfee® Email Gateway Appliance (VMtrial) 提供一个测试电子邮件生成器，使用它您无需配置外部基础结构来发送及接收电子邮件便可充分测试试用版软件。



“故障排除”|“工具”|“生成测试电子邮件”

使用测试电子邮件生成器的好处

测试电子邮件生成器通过模拟持续发送及接收各类电子邮件通讯，演示 McAfee Email Gateway Appliance (VMtrial) 的报告和检测功能。

电子邮件的内容是随机的，由一系列检测类型和合法数据组成。这些检测类型会针对病毒内容、垃圾邮件内容、合规性触发定义的操作，或 Data Loss Prevention (DLP) 操作。



这些测试邮件不包含任何病毒内容、而是包含旨在确保防病毒检测正常运行的测试字符串。

当您启用测试电子邮件生成器时，系统会自动创建策略。这些策略用于定义设备扫描测试电子邮件通讯时会应用到其中的设置。

所生成电子邮件的连接和信封属性也是随机的，从而确保扫描邮件时会触发不同的策略。



您可以编辑创建的策略来测试电子邮件通讯，但执行此操作会影响所扫描测试电子邮件通讯的结果。

生成测试电子邮件

生成大批邮件以测试扫描策略的效果。

表 3-1 选项定义 - 诊断: 生成连续的测试邮件

选项	定义
“启用连续生成功能”/“重置连续生成功能”	创建新策略以定义用于扫描使用连续生成功能所生成的测试电子邮件的配置。启用连续生成功能及创建策略后，通过单击“重置连续生成功能”，您可以将这些策略重置为其初始化状态。
“启动连续生成功能”	创建测试电子邮件通讯。
“禁用状态窗口提醒”	生成测试电子邮件通讯后，“状态窗口”每分钟都会出现一条提醒消息。单击此选项可禁用提醒消息。
“停止连续生成功能”	停止生成测试电子邮件通讯。

任务 - 生成大批测试电子邮件

配置 McAfee Email Gateway Appliance (VMtrial) 软件以连续生成一批测试电子邮件。

要充分评估和了解 McAfee Email Gateway 中的某些功能，需要让设备对电子邮件进行扫描。使用“生成测试电子邮件” | “诊断: 生成连续的测试电子邮件”以持续创建一批测试电子邮件，供设备扫描。

任务

- 1 选择“故障排除” | “工具” | “生成测试电子邮件”
- 2 单击“启用连续生成功能”。
- 3 单击“确定”以接受策略自定义将被覆盖的通知。



电子邮件生成功能的启用以及所需扫描策略的创建需要数分钟时间才能完成。

新策略现已创建完成。这些策略用于配置针对持续生成的测试电子邮件的扫描。

- 4 单击“启动连续生成功能”。

您的 McAfee Email Gateway Appliance (VMtrial) 即会生成开始大批的电子邮件供设备扫描。

任务 - 查看已扫描电子邮件通讯的摘要

使用“信息显示板”获取由 McAfee® Email Gateway Appliance (VMtrial) 所扫描的电子邮件通讯的简要概述。

开始之前

安排外部电子邮件通过 Virtual Appliance 传递，或使用“生成测试电子邮件” | “诊断: 生成连续的测试邮件”功能生成大批测试电子邮件。

任务

- 1 选择“信息显示板”。
- 2 查看“Mail Summary” (邮件摘要) Portlet 中显示的计数器。

计数器会随着已扫描的电子邮件通讯递增。

任务 - 查找特定的测试电子邮件

使用“邮件搜索”获得由 McAfee® Email Gateway Appliance (VMtrial) 扫描的电子邮件通讯的详细信息。

开始之前

安排外部电子邮件通过 Virtual Appliance 传递，或使用“生成测试电子邮件” | “诊断: 生成连续的测试电子邮件”功能生成大批测试电子邮件。

任务

- 1 选择“报告” | “邮件搜索”。
 - 2 单击“搜索/刷新”。
- 设备会从其数据库读取当前信息，并将其显示在页面上。
- 3 若仅想查看所采取的特定操作的相关信息，例如已隔离或退回的电子邮件，请使用可用的过滤选项，然后单击“搜索/刷新”。

即会显示有关扫描电子邮件通讯的详细信息。有关详细信息，请查看“邮件搜索”的联机帮助。

浏览设备功能

本节将通过一些任务来演示 McAfee Email Gateway 所提供的扫描功能，逐步说明如何创建和测试某些示例策略，并介绍如何生成适用的报告。

目录

- 策略简介
- 加密
- 合规性设置
- Data Loss Prevention 设置
- 任务 - 识别隔离的电子邮件

策略简介

本设备使用策略说明该设备针对各种威胁（如病毒、垃圾邮件、有害文件和机密信息的丢失）必须采取的措施。



“Email” | “Email Policies”

策略是可以应用到特定通讯类型或用户组的规则或设置的集合。

加密

“加密”页面可让您将 McAfee Email Gateway 设置为使用支持的加密方法安全地传递电子邮件。



“电子邮件” | “加密”

McAfee Email Gateway 提供了数种加密方法，可以设置为向其他扫描功能提供加密服务，也可以设置为仅用于加密邮件的仅加密服务器。

任务 - 将发给特定客户的所有电子邮件通讯进行加密处理

加密功能的一个常见用途是配置对发给特定客户的电子邮件进行加密的策略。

本组任务介绍如何配置 McAfee Email Gateway，以便将要发给特定客户的所有电子邮件都以加密方式发送。

任务 - 创建新的扫描策略

了解如何创建新的扫描策略。

设备使用您创建的策略来扫描通过设备的电子邮件。您可以创建多个策略来控制不同用户使用电子邮件的方式，或指定特定环境下要执行的不同操作。

任务

- 1 选择“电子邮件” | “电子邮件策略” | “扫描策略”。
- 2 通过执行“任务 - 查看 SMTP、POP3 或 McAfee Secure Web Mail 的策略”中的步骤来选择所需的协议。
- 3 单击“添加策略”。
- 4 在“扫描策略 - 新策略”页面中，输入以下信息：
 - a 命名该策略。
 - b 为新策略撰写说明（可选）。

- c 指定新策略所继承设置的来源策略。



如果您已设置类似策略，请选择此项以便新策略能继承其设置。

- d 选择策略是应用于入站电子邮件通讯还是出站电子邮件通讯。（仅限 SMTP）
- e 为策略选择所需的“匹配逻辑”。
- f 选择规则类型、匹配方式和规则要测试的值。
- g 如有必要，请添加其他规则并使用 和 按钮将规则正确排序。

- 5 单击“确定”。

新策略即会添加到策略列表的顶端。

任务 - 配置加密设置

配置 McAfee Email Gateway 以使用加密功能。

任务

- 1 选择“电子邮件”|“加密”|“Secure Web Mail”|“基本设置”。
- 2 选择“启用 Secure Web Mail Client”。
- 3 选择“电子邮件”|“加密”|“Secure Web Mail”|“用户帐户设置”。



系统会自动注册收件人，并向其发送 HTML 格式的、经过数字签名的通知。管理员可以选择执行推送加密和/或提取加密。

- 4 选择“电子邮件”|“加密”|“Secure Web Mail”|“密码管理”。



最短密码长度为八个字符。密码将在 365 天后过期。

任务 - 对符合合规性规则的邮件启用加密

在 McAfee Email Gateway 上对符合某个合规性规则的邮件启用必要的加密功能。

在本例中，将对符合 HIPAA 合规性规则的电子邮件进行加密。

任务

- 1 选择“Email”|“Email Policies”|“Compliance”。
- 2 单击“启用合规性”，然后选择“根据模板创建新规则”。
- 3 搜索“HIPAA 合规性”规则并予以选中。
- 4 单击“下一步”完成向导中的步骤。
- 5 选择“允许通过(监控)”作为主要操作。
- 6 在“以及”中，选择“以加密方式传递邮件”。
- 7 单击“完成”，然后单击“确定”以关闭对话框。
- 8 选择“Email”|“Email Policies”|“Policy Options”|“Encryption”。
- 9 在“何时加密”中，选择“仅当由扫描程序操作触发时”。
- 10 在“本地加密选项”中选择“Secure Web Mail”，然后单击“确定”。
- 11 应用更改。

合规性设置

使用此页面可以创建和管理合规性规则。



“Email” | “Email Policies” | “Compliance” | “Compliance”

合规性设置的好处

合规性扫描可以帮助您遵从法规合规性和公司运营合规性。您可以从预定义的合规性规则库中进行选择，也可以针对贵组织的实际情况自行创建特定规则和字典。

合规性规则的复杂度各不相同，有的会在检测到字典中的特定术语时直接触发，有的建立于多个基于分数的字典基础之上，只在达到特定阈值时才会触发。在合规性规则高级功能中，各字典可通过逻辑操作“任一”、“全部”和“除外”结合使用。

任务 - 限制字典术语的分数比重

使用下列任务可以对字典术语的分数进行限制。

开始之前

此任务假设您的规则引入的是基于分数阈值触发操作的字典，例如“薪酬和福利”字典。

您可以限制术语计入总分的次数。

例如，如果字典中的“testterm”分数为 10，它在一封电子邮件中出现 5 次，则会在总分中计入 50。您也可以加以限制，例如将“最大术语计数”设为 2 后，最多只有两次会计入总分。

任务

- 1 选择“Email” | “Email Policies” | “Compliance”。
- 2 展开要编辑的规则，然后单击要更改分数的字典旁边的“编辑”图标。
- 3 在“最大术语计数”中，键入术语计入分数的最大次数。

任务 - 编辑现有规则的阈值

使用下列任务可以编辑与现有规则相关联的阈值。

开始之前

此任务假设您的规则引入的是基于阈值触发操作的字典，例如“薪酬和福利”字典。

任务

- 1 选择“Email” | “Email Policies” | “Compliance”。
- 2 展开要编辑的规则，然后在要更改分数的字典旁边选择“编辑”图标。
- 3 在“字典阈值”中，键入规则触发须达到的分数，然后单击“确定”。

任务 - 创建一个根据阈值进行监控或阻止的规则

对于基于分数的字典，您可能希望在低阈值时监控触发器，而只在达到高阈值时才阻止电子邮件。

任务

- 1 选择“Email” | “Email Policies” | “Compliance”。
- 2 单击“创建新规则”，并键入规则名称，例如不满 - 低，然后单击“下一步”。

- 3 选择“不满”字典，然后在“阈值”中键入 20。
- 4 单击“下一步”，然后再次单击“下一步”。
- 5 在“如果触发合规性规则”中，接受默认操作。
- 6 单击“完成”。
- 7 重复步骤 2 到步骤 4 以创建另一个新规则，将其命名为不满 - 高，阈值分配为 40。
- 8 在“如果触发合规性规则”中，选择“拒绝连接(阻止)”。
- 9 单击“完成”。
- 10 单击“确定”，应用更改。

任务 - 在规则中添加字典

使用下列任务可以在现有规则中添加新字典。

任务

- 1 选择“Email” | “Email Policies” | “Compliance”。
- 2 展开要编辑的规则。
- 3 选择“添加字典”。
- 4 选择要包含的新字典，然后单击“确定”。

任务 - 创建复杂自定义规则

使用此任务可以创建复杂规则，它会在同时检测到“字典 A”和“字典 B”中的术语时触发，仅当检测到“字典 C”中的术语时除外。

任务

- 1 选择“电子邮件” | “电子邮件策略” | “扫描策略”，然后选择“合规性”。
- 2 在“默认合规性设置”对话框中，单击“是”以启用策略。
- 3 单击“创建新规则”以打开“规则创建向导”。
- 4 键入规则的名称，然后单击“下一步”。
- 5 选择规则要包含的两个字典，然后单击“下一步”。
- 6 在排除项列表中选择规则要排除的字典。
- 7 选择规则触发时要执行的操作。
- 8 从“和(有条件)”下拉框中选择“全部”，然后单击“完成”。

任务 - 创建简单自定义规则

使用下列任务可以创建简单自定义规则以阻止包含社会保险号码的邮件。

任务

- 1 选择“Email” | “Email Policies” | “Compliance”。
- 2 在“默认合规性设置”对话框中，单击“是”以启用策略。
- 3 单击“创建新规则”以打开“规则创建向导”。
- 4 键入规则的名称，然后单击“下一步”。

- 5 在“搜索”字段中键入社会。
- 6 选择“社会保险号码”字典，然后单击两次“下一步”。
- 7 选择“拒绝连接(阻止)”操作，然后单击“完成”。

任务 - 阻止违反策略的邮件

使用下列任务可以阻止违反“威胁性言语”策略的邮件。

任务

- 1 选择“Email” | “Email Policies” | “Compliance”。
- 2 在“默认合规性设置”对话框中，单击“是”以启用策略。
- 3 单击“根据模板创建新规则”打开“规则创建向导”。
- 4 选择“允许使用 - 威胁性言语”策略，然后单击“下一步”。
- 5 (可选) 更改规则名称，然后单击“下一步”。
- 6 将主要操作更改为“拒绝连接(阻止)”，然后单击“完成”。
- 7 单击“确定”，应用更改。

Data Loss Prevention 设置

使用此页面可以创建一条策略，用于对已注册文档类别分配 Data Loss Prevention 操作。



“Email” | “Email Policies” | “Compliance” | “Data Loss Prevention”

使用 Data Loss Prevention (DLP) 的好处

您可以选择使用 Data Loss Prevention 功能针对设备上通过 SMTP 发送的电子邮件限制敏感信息的传播。例如，阻止传输要发送到组织之外的财务文档之类的敏感文档。无论是将原始文档作为电子邮件附件，还是只从原始文档截取部分文字内容，都会触发检测。

请在以下两个阶段配置 DLP：

- 注册要保护的文档
- 设置要执行的 DLP 策略并控制检测 (本主题)



如果上载的已注册文档包含内嵌文档，则系统还会探测其内容的指纹，因此在计算扫描期间的百分比匹配时，会使用组合内容。要单独处理内嵌文档，则必须分别注册这些文档。

任务 - 防止泄漏敏感文档

使用此任务可以阻止将敏感的财务文档发送到组织外部。

开始之前

本示例假定您已经创建了“财务”类别。

任务

- 1 选择“Email” | “Email Policies” | “Compliance” | “Data Loss Prevention”。
- 2 在“默认 Data Loss Prevention 设置”对话框中，单击“是”以启用策略。
- 3 单击“创建新规则”并选择“财务”类别，然后单击“确定”，“规则”列表中即会出现该类别。

- 4 选择与类别关联的操作，将主要操作更改为“拒绝连接(阻止)”，然后单击“确定”。
- 5 再次单击“确定”并应用更改。

任务 - 阻止文档的一部分

使用此任务可以阻止将一小部分文档发送到组织外部。

任务

- 1 选择“Email” | “Email Policies” | “Compliance” | “Data Loss Prevention”。
- 2 在“默认 Data Loss Prevention 设置”对话框中，单击“是”以启用策略。
- 3 启用连续签名设置，然后键入会引起 DLP 策略触发检测的连续签名数。默认情况下，此阈值设为“10”。
- 4 单击“创建新规则”并选择“财务”类别，然后单击“确定”，“规则”列表中即会出现该类别。
- 5 选择与类别关联的操作，将主要操作更改为“拒绝连接(阻止)”，然后单击“确定”。
- 6 再次单击“确定”并应用更改。

任务 - 针对某个策略排除特定文档

使用此任务可以防止特定财务文档触发 DLP 策略设置。

任务

- 1 选择“Email” | “Email Policies” | “Compliance” | “Data Loss Prevention”。
- 2 在“默认 Data Loss Prevention 设置”对话框中，单击“是”以启用策略。
- 3 单击“创建文档排除项”，为此策略选择要忽略的文档，然后单击“确定”。
- 4 再次单击“确定”并应用更改。

任务 - 识别隔离的电子邮件

使用此任务可以发现哪些电子邮件已被 McAfee Email Gateway Appliance 隔离。

查看所有已隔离的邮件的列表：

任务

- 1 单击“报告” | “邮件搜索”。
- 2 从“邮件状态”下拉列表中选择“已隔离”。
- 3 单击“搜索/刷新”。

所有已隔离的邮件都会显示在页面下方。

任务

- [任务 - 优化搜索第 25 页](#)
- [任务 - 查看特定的电子邮件第 26 页](#)
- [任务 - 释放隔离的电子邮件第 26 页](#)
查看已隔离的电子邮件之后，您可能想从隔离区释放电子邮件。为此可执行此任务。

任务 - 优化搜索

您可以针对已隔离的电子邮件进一步优化搜索，从而只显示因特定触发而隔离的电子邮件。在此例中，查找因合规性问题而被隔离的电子邮件：

任务

- 1 完成“**任务 - 查找隔离的电子邮件**”中的步骤。
- 2 从“类别”下拉列表中选择“合规性”。
- 3 单击“搜索/刷新”。

屏幕下方即会刷新，只显示因合规性问题而被隔离的邮件。

任务 - 查看特定的电子邮件

可以查看隔离电子邮件的内容。

任务

- 1 完成“**任务 - 优化搜索**”中的步骤。
- 2 使用页面左侧的复选框选择相应的已隔离邮件。
- 3 单击“查看邮件”。

选择的邮件即会显示在一个新窗口中。您可以在这里查看电子邮件的内容，也可以选择查看详细的电子邮件报头信息。查看邮件后，只需单击相应按钮，就可以选择要在电子邮件上执行的其他操作。

任务 - 释放隔离的电子邮件

查看已隔离的电子邮件之后，您可能想从隔离区释放电子邮件。为此可执行此任务。

从隔离区释放所选邮件：

任务

- 1 完成“**任务 - 查看特定的电子邮件**”中的步骤。
- 2 单击“释放所选项目”。

所选电子邮件将从隔离区释放。



电子邮件如果包含病毒内容，则无法从隔离区释放，否则可能会对系统造成损害。

索引

- A**
 - 安装
 - 配置 Virtual Appliance [14](#)
- C**
 - 测试电子邮件生成器 [18](#)
 - 好处 [18](#)
 - 产品功能 [6](#)
 - 策略
 - 简介 [20](#)
 - 状态 [15](#)
- D**
 - Data Loss Prevention
 - 好处 [24](#)
 - Data Loss Prevention 的好处 [24](#)
 - 电子邮件策略
 - 合规性 [22](#)
 - 电子邮件生成器 [18](#)
 - DLP
 - 好处 [24](#)
 - DLP (Data Loss Prevention) [24](#)
 - Data Loss Prevention (DLP) [24](#)
 - DLP 的好处 [24](#)
 - 电子邮件队列 [15](#)
 - 电子邮件状态 [15](#)
- G**
 - 功能说明 [6](#)
- H**
 - 合规性 [22](#)
 - 好处 [22](#)
 - 扫描 [22](#)
 - 环境
 - 支持的平台 [5](#)
- J**
 - 加密 [20](#)
 - 检测
 - 比率和统计信息 [15](#)
- 警告消息
 - 信息显示板 [15](#)
- M**
 - McAfee Global Threat Intelligence [15](#)
- P**
 - 配置 Virtual Appliance [14](#)
 - 配置更改消息 [15](#)
- Q**
 - 群集配置
 - 统计信息 [15](#)
- S**
 - 扫描
 - 对于合规性 [22](#)
- T**
 - 统计信息
 - 信息显示板 [15](#)
 - 图形
 - 电子邮件和网络统计信息 [15](#)
- V**
 - Virtual Appliance
 - 初始配置 [14](#)
- W**
 - Web 策略
 - 合规性 [22](#)
 - 网络状态 [15](#)
 - 威胁反馈 [15](#)
- X**
 - 信息显示板 [15](#)
 - 虚拟平台
 - 支持的 [5](#)

Z

字典

编辑分数和术语 [22](#)

字典

添加到策略 [22](#)

支持的平台 [5](#)

