产品手册

McAfee Security for Microsoft Exchange 8.6.0

目录

目录

1 简介

McAfee® Security for Microsoft Exchange (MSME) 保护 Microsoft Exchange 服务器抵御多种会对计算机、网络或员工造成负面影响的威胁。

MSME 使用高级启发式方法抵御病毒、有害内容、潜在有害程序和禁止文件类型或邮件。 它还扫描以下内容：

- 电子邮件的主题行和正文
- 电子邮件附件（基于文件类型、文件名和文件大小）
- 电子邮件附件中的文本
- 电子邮件正文中的 URL

软件还包含 McAfee Anti-Spam 插件，可保护 Exchange 服务器抵御垃圾邮件和网络钓鱼电子邮件。

目录

产品功能

本章节描述了 MSME 的主要功能。

- **用于进行文件信誉检查的 McAfee® Threat Intelligence Exchange (TIE) 集成** — 支持对电子邮件附件的 TIE 文件信誉检查。 它根据从连接到您环境中 TIE 服务器的几个来源收到的信息验证文件信誉，从而快速分析文件并做出明智的决策。 电子邮件中包含压缩文件时，会解压文件，并发送支持类型的文件，以获得 TIE 信誉。 有关支持的压缩文件列表，请参见 KB89577。
- **针对文件的 McAfee® Advanced Threat Defense 信誉检查** — MSME 现在支持 Advanced Threat Defense（一种内部部署装置，有助于通过 TIE 检测和阻止恶意软件）。 借助 Advanced Threat Defense 保护，您可以保护系统免遭已知、近零日和零日恶意软件的威胁，而且不会影响为网络用户提供的服务质量。
- **防止电子邮件欺诈** — 保护您的系统免遭欺诈电子邮件的威胁。
- **从扫描中排除大型电子邮件** — 您现在可以根据电子邮件的大小从按访问扫描中排除电子邮件。
- **阻止来自特定 IP 地址的电子邮件** — 您现在可以将向贵组织发送电子邮件使用的特定 IP 地址或 IP 地址范围列入黑名单，而不管 IP 地址信誉分数为何。
- **支持 Microsoft Exchange 2016** — 支持 Microsoft Exchange 2016 累积更新 (CU) 3 和更高版本。
- **支持 Microsoft Windows Servers 2016** — 支持 Microsoft Windows 2016 64 位服务器操作系统。
- **浏览器增强** — Microsoft Internet Explorer 11.1066、Mozilla Firefox 54.0.1 和 Google Chrome 59.0.3071.115。

请确保在浏览器设置中禁用了弹出窗口阻止程序以访问产品 Web 界面。

其他功能

- **抵御病毒** — 扫描所有电子邮件中的病毒，通过拦截、清理和删除检测到的病毒以保护 Exchange 服务器。 MSME 使用高级启发式方法，识别并阻止未知病毒或疑似病毒项目。
- **反垃圾邮件保护** — 通过在扫描每封电子邮件时为其分配垃圾邮件分数并对其采取预配置操作，帮助减少 Exchange Server 所需的带宽和存储空间。
- **反网络钓鱼保护** — 检测试图以欺诈方式获取您的个人信息的网络钓鱼电子邮件。
- **抵御恶意 URL** — 保护系统抵御恶意 URL。 启用后，MSME 会扫描电子邮件正文中的每条 URL、获取链接的信誉分数、将分数与定义的阈值进行比较并根据配置采取相应操作。
- **检测打包程序和潜在有害程序的功能** — 检测对可执行文件的源代码进行压缩并加密的打包程序。它也检测潜在有害程序 (PUP)，即由合法公司编写的、改变计算机的安全状态或隐私状态的软件程序。
- **内容过滤** — 扫描主题行中的内容和文本、电子邮件的正文以及电子邮件附件。 MSME 支持基于正则表达式 (regex) 的内容过滤。
- **文件过滤** — 根据文件名、类型和附件大小来扫描电子邮件附件。 MSME 还可以过滤包含加密、损坏、受密码保护和数字签名内容的文件。
- **DLP 和合规性** — 可以确保电子邮件内容符合组织的机密性和合规性策略。 预定义的合规性字典包括：
  - 新添加的 60 部新 DLP 和合规性字典
  - 支持行业特定的合规性字典 — HIPAA、PCI、源代码（Java、C++ 等）
  - 改进了现有的短语检测。
  - 根据阈值分数及最大术语计数（出现次数），增强了检测不兼容内容的功能，从而减少了误报。

  自定义内容安全和数据丢失防护 (DLP) 策略。
- **IP 信誉** — 一种根据发送服务器 IP 地址检测电子邮件威胁的方法。 IP 信誉分数反映了网络连接存在威胁的可能性。 IP 信誉利用 McAfee Global Threat Intelligence (GTI) 根据最近电子邮件服务器的源 IP 地址，在网关阻止电子邮件，从而阻止数据损坏和偷窃。 MSME 根据 IP 信誉分数阻止或断开连接，从而在消息进入组织前进行处理。
- **高级按需扫描** — 在 Exchange Server 2010 和 2013 上执行精确级别的按需扫描，从而加快按需扫描的速度。 您可以根据以下过滤方式计划按需扫描：主题、附件、发件人/收件人/抄送、邮件大小、消息 ID、未读项目和时长。
- **后台扫描** — 扫描信息存储区中的所有文件。 您可以计划后台扫描以使用最新的引擎更新内容和扫描配置对选定的消息集进行定期扫描。 在 MSME 中，可以排除不想要扫描的邮箱。
- **产品运行状况警报** — 这些是产品运行状况状态的通知。 您可以配置和计划这些警报。
- **与 McAfee ePolicy Orchestrator 5.1.x、5.3.x 和 5.9.x 集成** — 与 ePolicy Orchestrator 5.1.x、5.3.x 和 5.9.x 集成以提供跨 Exchange 服务器的 MSME 集中管理和更新方法， 这样可以降低各种系统管理和更新的复杂性，并减少所需的时间。
- **基于 Web 的用户界面** — 提供基于 DHTML 的、用户友好的、基于 Web 的用户界面。
- **策略管理** — 产品用户界面中的“策略管理器”菜单选项列出了可以在 MSME 中进行设置和管理的不同策略。
- **集中式扫描程序、过滤规则及增强的警报设置** — 通过扫描程序，您可以配置扫描项目时策略可应用的设置。通过文件过滤规则，您可以设置适用于文件名、文件类型和文件大小的规则。
- **按需/基于时间的扫描和操作** — 在方便的时间或以固定时间间隔扫描电子邮件。
- **多用途 Internet 邮件扩展 (MIME) 扫描** — 一种通信标准，用于在仅支持 7 位 ASCII 字符的协议（例如 SMTP）上传输非 ASCII 格式。
- **隔离管理** — 您可以指定本地数据库用作隔离被感染的电子邮件的存储库。 您可以选择将隔离的邮件存储在运行 McAfee Quarantine Manager 的自有服务器上（称为机下隔离）。

- **自动更新病毒定义、Extra DAT、防病毒和反垃圾邮件引擎** — 定期提供更新后的 DAT 文件、防病毒扫描程序引擎和反垃圾邮件引擎来检测和清理最新威胁。
- **保留和清除旧 DAT** — 根据需要，将旧 DAT 文件保留定义的时间段或清除它们。
- **站点列表编辑器支持** — 指定下载 MSME 自动更新的位置。
- **Small Business Server 支持** — MSME 可兼容 Small Business Servers。
- **检测报告** — 生成可以查看有关检测到项目的信息的状态报告和图形报告。
- **配置报告** — 对产品配置进行总结，例如有关以下内容的信息：服务器、版本、许可证状态和类型、产品、调试日志记录、按访问设置、按访问策略和网关策略。您可以指定服务器需要向管理员发送配置报告的时间。
- **拒绝服务攻击检测** — 检测对网络中常规通信进行洪水攻击和造成中断的额外请求或攻击。 拒绝服务攻击常使用错误的连接请求覆盖其目标，从而使目标忽略合法的请求。 MSME 将以下三种情况视为拒绝服务攻击：
  - 扫描时间超出定义的时间
  - 嵌套级别超出定义的级别
  - 存档文件的可扩展文件大小限制超出定义大小
- **高级通知** — 根据检测类别，将用于合规性审核的隔离电子邮件转发给多个用户。
- 支持 VMware Workstation 7.0 或更高版本以及 VMware ESX 5.5。

为何需要 MSME

您的组织容易面临许多威胁，这些威胁会影响组织的信誉、员工、计算机和网络。

- 泄露机密信息或可能导致法律诉讼的权限滥用可以使组织的信誉受到影响。
- 分散注意力的电子产品以及不加限制地使用电子邮件和互联网会影响员工的生产效率。
- 病毒和其他潜在有害软件可以损坏计算机，使计算机无法使用。
- 在网络上不加控制地使用各种类型的文件可以导致整个组织出现性能问题。

组织面临的威胁

了解可能影响组织的各种威胁。

威胁的类型	说明
公司的信誉	员工轻率的或一知半解的言论可能会导致法律问题，除非在免责声明中明述。
垃圾邮件（未经请求的电子邮件）	未经请求的商业电子邮件相当于电子形式的垃圾邮件。它们通常包含收件人未预期的广告。尽管这更像是一种干扰而不是威胁，垃圾邮件还是会降低网络的性能。
大型电子邮件	大型电子邮件或包含大量附件的邮件可以降低电子邮件服务器的性能。
群发邮件病毒	尽管可以像任何其他病毒一样清除这些病毒，但它们的传播速度很快并会快速降低网络的性能。
来自有害的来源的电子邮件	如果心怀不满的离职员工和无良的个人知道员工的电子邮件地址并发送恶意电子邮件，则会使人出现焦虑和注意力分散。
非业务目的使用电子邮件	如果大多数员工在组织外使用收件人电子邮件地址，此类电子邮件很可能是出于个人或非业务目的。
泄露公司机密信息	员工可能会泄露有关未发布的产品、客户或合作伙伴的机密信息。
无礼的语言	无礼的词语或短语可能会出现在电子邮件和附件中。除了令人厌恶外，还可能引起法律行动。
传输娱乐文件	以娱乐为目的的大型视频或音频文件可能会降低网络的性能。

威胁的类型	说明
低效率的文件类型	有些文件使用大量内存并且传输速度可能很慢，不过通常都有可用的备用类型。例如，GIF 和 JPEG 文件比相同的 BMP 文件小很多。
传输大型文件	传输大型文件会降低网络性能。
拒绝服务攻击	大型文件恶意泛滥会严重影响网络性能，使合法用户无法使用网络。 扫描大型压缩文件时，MSME 将使用三种参数来认定拒绝服务 (DOS) 攻击： • 压缩文件的扫描时间超出阈值。 • 确定存在压缩文件的嵌套级别。 例如，.zip 压缩文件包含另一个压缩的文件，并且接连不断地包含更多压缩文件。 • 存档文件的可扩展大小限制超出阈值。
色情文本	在电子邮件中不得使用粗俗的语言或词汇。
病毒和其他潜在有害软件	病毒和其他潜在有害软件可以很快使计算机和数据无法使用。
遭破坏的或加密内容	无法扫描此类型的内容。必须指定适当的策略来处理它。

MSME 如何保护 Exchange Server

了解 MSME 如何通过访问所有到达 Exchange Server 的电子邮件，以及从邮箱读取和写入邮箱的电子邮件来保护您的 Exchange Server。

保护 Microsoft Exchange Server

MSME 使用 Exchange 服务器的病毒扫描界面获取完整权限，从而访问 Exchange 服务器邮箱读取和编写的所有电子邮件。

- 防病毒扫描引擎将电子邮件与 DAT 中存储的所有已知病毒特征码相比较。
- 内容管理引擎在电子邮件中扫描 MSME 内容管理策略指定的阻止内容。

如果这些检查在电子邮件中发现任何病毒或阻止的内容，MSME 会采取特定的操作。 如果未检测到项目，MSME 会将信息返回至病毒扫描界面以完成 Microsoft Exchange 中的原始邮件请求。

实时检测

MSME 集成 Exchange 服务器并实时运作以检测和删除病毒或其他有害代码。 还通过扫描 Exchange 服务器上的数据库帮助您维持无病毒的环境。 每次从源发送或接收电子邮件时，MSME 会扫描电子邮件并与已知病毒和可疑病毒行为列表进行比较，从而在被感染的文件传播前对其进行拦截和清理。 它还可以使用本软件中定义的规则和策略扫描电子邮件（及其附件）中的内容。

电子邮件扫描

- 在内容写入文件系统或被 Microsoft Exchange 用户读取前，反垃圾邮件、防病毒和内容管理引擎会先扫描电子邮件并将结果提交至 MSME。
- 防病毒和反垃圾邮件扫描引擎可以将电子邮件与当前已安装的病毒定义文件 (DAT) 中存储的所有已知特征码和反垃圾邮件规则相比较。防病毒引擎还使用所选的启发式检测方法扫描邮件。
- 内容管理引擎在电子邮件中扫描软件内运行的内容管理策略所指定的阻止内容。 如果电子邮件中没有病毒、禁止/有害的内容，MSME 会将信息返回至 Microsoft Exchange。 如果检测到项目，MSME 会采取配置设置中定义的操作。

扫描工作原理

- MSME 的核心是扫描引擎和 DAT 文件。 引擎是个复杂的数据分析程序。 DAT 文件包含大量信息（其中包括数千个不同的驱动程序），每个驱动程序包含有关如何识别病毒或病毒类型的详细说明。
- 扫描引擎与 DAT 文件一起工作。它标识扫描的项目的类型，然后将该对象的内容解码以了解该项目。然后，它使用 DAT 文件中的信息搜索和查找已知病毒。每个病毒具有独特的特征码。病毒有对应的唯一字符序列，引擎会搜索该特征码。引擎使用称为启发式分析的技术搜索未知病毒。这涉及分析对象的程序代码以及搜索通常会在病毒中发现的独特特征。
- 当引擎确认病毒的身份后，会尽可能清理目标。例如，从附件中删除被感染的宏，或者删除可执行文件中的病毒代码。

扫描内容和扫描时间

- 病毒中的威胁来自四面八方，例如被感染的宏、共享程序文件、网络共享文件、电子邮件和附件、软盘驱动器、从互联网下载的文件等。 各类 McAfee 安全防病毒软件产品针对不同方面的漏洞。 建议采取多层方案，从而提供所需的全面病毒检测、安全和清理功能。
- MSME 提供一系列选项，您可以根据系统需求对其进行详细配置。 根据系统的组件部件何时及如何运行、它们之间如何交互以及如何与外部世界交互（特别是通过电子邮件和互联网访问），这些需要将有所不同。
- 您可以配置或启用多种操作，从而确定 MSME 服务器如何处理不同项目以发现检测到或可疑的项目时所采取的操作。

如何扫描电子邮件

MSME 扫描电子邮件的方式会有不同，具体取决于电子邮件是入站、出站还是内部。

每次从源发送或接收电子邮件时，MSME 会根据已知病毒和可疑病毒行为列表对其进行扫描。 MSME 还可以使用软件内定义的规则和策略扫描电子邮件中的内容。

MSME 接收到电子邮件时，会按此顺序扫描：

1 IP 地址信誉

2 反垃圾邮件或网络钓鱼

3 反欺诈

4 遭破坏的或加密内容

5 文件过滤器

6 内容扫描（DLP 和合规性）

7 防病毒

8 邮件 URL 信誉

虽然以此顺序扫描电子邮件，但如果某个项目首先被文件过滤扫描程序检测到，在被隔离前也会进行防病毒扫描。

在 MSME 中启用 IP 信誉功能后，可以根据源 IP 地址检测电子邮件。 安装 McAfee Anti-Spam 组件后，即可使用该功能。

扫描入站电子邮件

关于如何处理到达您的组织的电子邮件，以及 MSME 如何对电子邮件进行扫描以确定它是否干净或受感染的分步信息。

下述流程中假定贵组织已在以下所有角色上安装 MSME。

Microsoft Exchange Server 2010：

- 边缘传输
- 集线器传输
- 邮箱

Microsoft Exchange Server 2013 和 2016：

- 边缘传输
- MBX

如果您在边缘或集线器传输角色上没有安装 Exchange 服务器，MSME 会忽略与该角色相关的步骤。

任务

1 由具有边缘角色的 EdgeTransport.exe 托管的 SMTP 堆栈接收电子邮件。

2 MSME IP 代理 (McTxIPAgent) 会针对来源 IP 地址信誉进行检查。 IP 代理检查在 TxAgent 操作之前执行。

3 MSME 传输代理 (McAfeeTxAgent) 会扫描电子邮件中的垃圾邮件、网络钓鱼或邮件大小。

4 如果有检测，它将被丢弃，否则它会返回到 SMTP 堆栈。

5 如果电子邮件干净，McAfeeTxRoutingAgent 将对其进行处理。

6 MSME 会收到相同的数据流，并扫描以进行文件过滤、内容扫描、防病毒 (AV) 扫描和 URL 过滤。

7 如果有检测，将根据产品配置采取操作。

8 MSME 根据 Microsoft 规范为电子邮件添加 AV 戳。

9 现在，电子邮件就发送到了具有集线器服务器角色的 Exchange。

10 由具有集线器服务器角色的 EdgeTransport.exe 托管的 SMTP 堆栈接收电子邮件。

11 MSME 传输代理 (McAfeeTxAgent) 对电子邮件进行垃圾邮件、网络钓鱼或邮件大小扫描。只有在 EdgeSync（边缘和集线器服务器）的情况下，会在跳过反垃圾邮件扫描的地方验证会话。此时，原始发件人检查被用于会话验证。

12 如果有检测，电子邮件将被丢弃，否则它会返回到 SMTP 堆栈。

13 如果电子邮件干净，McAfeeTxRoutingAgent 将对其进行处理并检查 AV 戳（如有）。

14 如果存在 AV 戳，它将使用具有集线器服务器角色的引擎/DAT 检查 MSME 戳形式并加以比较。

15 如果戳不同， MSME 将接收相同的数据流，并进行文件过滤、内容扫描以及防病毒扫描。

16 在传输时， MSME 会查找 AV 戳，而在 VSAPI 上，由 Exchange 存储区执行此项工作；如果 AV 戳匹配， MSME 将不会收到扫描调用。

17 如果有检测，将根据产品配置采取操作。

18 MSME 根据 Microsoft 规范为电子邮件添加 AV 戳。

19 电子邮件被路由到 Exchange 邮箱服务器角色。

20 Exchange 存储区接收邮件，并在将邮件保存到数据库前检查 AV 戳。

21 如果 AV 戳匹配，Exchange 存储区将保存邮件而不进行扫描。

22 如果 AV 戳不匹配，Exchange 存储库会调用 VSAPI（病毒扫描 API）并扫描电子邮件。

VSAPI 检查仅适用于 Microsoft Exchange 2010 服务器。

23 如果进行检测，会根据产品配置替换或删除该电子邮件。

对于 Microsoft Exchange Server 2013 和 2016，集线器传输和邮箱角色不适用。

扫描出站电子邮件

关于如何处理组织发送的电子邮件，以及 MSME 如何对电子邮件进行扫描以确定它是否干净或受感染的分步信息。

任务

1 最终用户使用电子邮件客户端向外部用户发送电子邮件。

2 Exchange 存储区接收电子邮件，并在发件箱文件夹中进行扫描。

3 如果有检测，它将会根据产品配置被替换或删除；如果被替换，则会将其提交至传输队列。

4 集线器/MBX 角色上由 EdgeTransport.exe 托管的 SMTP 堆栈会收到电子邮件。

5 MSME 传输代理 (McAfeeTxRoutingAgent) 会扫描电子邮件，以进行文件过滤、内容扫描、防病毒扫描，还会扫描 URL 信誉以及添加的免责声明。

6 如果有检测，它将被丢弃或替换，并相应地返回到 SMTP 堆栈。

7 如果电子邮件干净，它将返回到 SMTP 堆栈以进行进一步路由。

8 如果电子邮件从此集线器服务器路由至 Edge 服务器角色，那么：

   a 由具有边缘服务器角色的 EdgeTransport.exe 托管的 SMTP 堆栈接收电子邮件。

   b MSME 传输代理 (McAfeeTxRoutingAgent) 检查 AV 戳（如有）。

   c 如果存在 AV 戳，它将使用具有边缘服务器角色的引擎/DAT 检查 MSME 戳形式并加以比较。

   d 如果 AV 戳不同，那么 MSME 会收到相同的数据流，并扫描以进行文件过滤、内容扫描、防病毒扫描，然后执行 URL 信誉检查。

   e 如果有检测，将根据产品配置采取操作。

   f MSME 根据对边缘服务器角色的 Microsoft 规范，为电子邮件添加 AV 戳。

9 现在，电子邮件就返回到了由具有边缘服务器角色的 EdgeTransport.exe 托管的 SMTP 堆栈。

扫描内部电子邮件

关于如何处理组织中发送的电子邮件，以及 MSME 如何对电子邮件进行扫描以确定它是否干净或受感染的分步信息。

任务

1 最终用户使用电子邮件客户端向内部用户发送电子邮件。

2 对于 Exchange Server 2010，Exchange 会收到电子邮件并在发件箱文件中扫描它。 对于 Exchange Server 2013 和 2016，电子邮件会定向至发件箱文件夹中的传输队列。

3 如果有检测，它将会根据产品配置被替换或删除；如果被替换，则会将其提交至传输队列。

4 由具有集线器服务器角色的 EdgeTransport.exe 托管的 SMTP 堆栈接收电子邮件。

5 MSME 传输代理 (McAfeeTxRoutingAgent) 对电子邮件进行文件过滤、内容扫描以及防病毒扫描。

6 如果有检测，它将被丢弃或替换，并相应地返回到 SMTP 堆栈。

7 MSME 根据对集线器服务器角色的 Microsoft 规范，为电子邮件中添加 AV 戳。

8 如果电子邮件干净，它将返回到 SMTP 堆栈以进行进一步路由。

9 Exchange 邮箱服务器接收电子邮件。

10 Exchange 存储库会检查 AV 戳，如果 AV 戳匹配，不会发送电子邮件进行针对 VSAPI 的 MSME 扫描；否则，会扫描电子邮件，由 VSAPI 进行防病毒、URL 信誉、文件过滤和内容扫描。

2 信息显示板

信息显示板以易于查看和解读的方式组织并显示信息。

MSME 信息显示板提供了相关重要信息，如服务器在面对垃圾邮件、网络钓鱼、病毒、潜在有害程序、恶意 URL 和有害内容时所受安全保障的稳固程度。 还提供关于检测统计信息、产品中安装的其他组件、组件的版本信息（例如引擎和 DAT 文件）、产品许可信息以及最近扫描的项目的信息。

目录

检测到的项目的统计信息

提供关于由 MSME 扫描的电子邮件总数，以及根据检测类别触发检测和被隔离的电子邮件数量的详细信息。为便于解释和监视检测率，信息显示板还会以图形的形式提供这一统计信息。

“统计” 选项卡分类为以下部分：

- “检测”
- “扫描”
- “图形”

单击 “重置” 将清除 “检测” 部分中所有计数器的统计信息，并将值重置为零。重置统计信息将不会从 “检测到的项目” 删除任何隔离的项目。这些计数器与数据库路径有关，所以如果您更改了 “设置和诊断” | “检测到的项目” | “本地数据库” 下的数据库路径，计数器将重置为零。

要修改信息显示板设置，例如：刷新率； “近期已扫描的项” 中显示的最大项目；图形标尺单位；3D 饼图、分解饼图、透明度等图形和图表设置，请转到 “设置和诊断” | “User Interface Preferences（用户界面首选项）”。

检测

显示所有统计信息，包括 MSME 扫描为干净的电子邮件数量和触发检测的项目数量。 相应的计数器会根据检测类别增加。

报告的数字表示触发任意检测方法的电子邮件和文档的数目。例如，如果一封电子邮件包含两个受病毒感染的附件，“病毒” 的统计信息将增加一而不是二。报告统计信息是基于电子邮件而不是基于单个文件或检测，这在邮件服务器环境中较为直观。

如果 MSME 服务器由 ePolicy Orchestrator 托管，并且如果重新启动服务或单击 “重置” 按钮，根据 McAfee ePO 中存储的历史数据，这些统计信息在 McAfee ePO 报告中可能会有所不同。 有关 McAfee ePO 报告的更多信息，请参见 “集成 MSME 与 ePolicy Orchestrator”。

表 2-1 使用的图标 — 检测部分

图标	说明
	如果将光标移至该图标上，会提供检测项类别的更多信息。
	表示相应检测类别的统计信息在图形中可用。
	表示相应检测类别的统计信息在图形中不可用。

只有选择了“图形”下拉列表中的“<选择检测项>”选项时，才会出现图形图标 和 。

下表可为您提供关于每个检测类别的详细信息。

表 2-2 检测定义

类别	其他信息	说明
“干净”	如果电子邮件流具有的干净电子邮件要比检测项多，针对干净电子邮件启用该 图标会抑制其他类别的图形。 在这种情况下，禁用“干净”类别旁的 图标。	对于用户而言不存在威胁并且不会触发任何 MSME 扫描程序的合法电子邮件。
“垃圾邮件”	只有安装了 McAfee Anti-Spam 插件后，才能使用该计数器。	通常以群发方式发送给多个未请求或未对其注册的收件人的未经请求的电子邮件。
	“扫描垃圾邮件”	由 MSME 进行垃圾邮件扫描的所有电子邮件。
	“检测为垃圾邮件”	被识别为垃圾邮件，但由于策略设置而未被隔离的电子邮件。
	“作为垃圾邮件被阻止”	被识别为垃圾邮件，且由于策略设置而被隔离的电子邮件。
“网络钓鱼”	只有安装了 McAfee Anti-Spam 插件后，才能使用该计数器。	网络钓鱼是个人为了获取私人信息而采用的不正当或欺诈手段。 这些私人信息包括信用卡详细信息、密码、银行账户登录详细信息。 这些电子邮件冒充银行与合法公司等受信任的来源。 通常会要求您单击某个链接，以验证或更新特定的个人详细信息。 与垃圾邮件一样，网络钓鱼电子邮件也是以群发方式发送的。
	“检测到网络钓鱼”	被识别为网络钓鱼，但由于策略设置而未被隔离的电子邮件。
	“已阻止网络钓鱼”	被识别为网络钓鱼，且由于策略设置而被隔离的电子邮件。
“欺诈邮件”	只有安装了 McAfee Anti-Spam 插件后，才能使用该计数器。	
	“检测到 SPF 硬故障”	被识别为硬故障欺诈邮件的电子邮件。
	“检测到 SPF 软故障”	被识别为软故障欺诈邮件的电子邮件。
“IP 信誉”	只有安装了 McAfee Anti-Spam 插件后，才能使用该计数器。	一种根据发送服务器的 IP 地址检测来自电子邮件的威胁的方法。IP 信誉分数可反映网络连接构成威胁的可能性。 IP 信誉利用 McAfee Global Threat Intelligence (GTI) 根据最近电子邮件服务器的源 IP 地址，在网关阻止电子邮件，从而阻止数据损坏和偷窃。 MSME 根据 IP 信誉分数阻止或断开连接，从而在消息进入组织前进行处理。
	“IP 已接收”	达到 MSME 服务器的所有电子邮件。
	“IP 已丢弃”	由于 IP 信誉功能而被 MSME 隔离的电子邮件。 在这种情况下，发件人不会收到关于电子邮件发送状态的通知。

表 2-2 检测定义 *（续）*

类别	其他信息	说明
	“IP 已拒绝”	由于 IP 信誉功能而被 MSME 隔离的电子邮件。 在这种情况下，将通知发件人电子邮件的传递状态。
“病毒”		一种计算机程序文件，会附加至磁盘或其他文件，并反复自行复制，通常在用户不知情或未获得用户允许的情况下执行这些操作。 一些病毒会附加至文件，因此在执行被感染的文件时，也会执行病毒。 其他病毒会驻留在计算机的内存中，并且在计算机打开、修改或创建文件时感染文件。 有些病毒会出现征兆，有些病毒会破坏文件和计算机系统，但是无论哪个都不是界定病毒的必要条件，无破坏性的病毒仍然是病毒。
	“检测到病毒”	在传入的电子邮件中检测到，并根据策略设置对其采取适当操作的病毒。
	“病毒已清理”	从传入的电子邮件中删除，并根据策略设置对其采取适当操作的病毒。
“TIE 和 ATD 检测”	“文件信誉”	发送至 TIE 服务器以进行文件信誉检查的受支持文件类型附件。
	“证书信誉”	发送至 TIE 服务器以进行证书信誉检查的受支持已签名文件类型附件。
	“ATD 提交”	发送至 ATD 服务器以根据接受类别和文件大小进行信誉检查的受支持文件类型附件。
	“TIE 检测总计”	通过 TIE 验证的受支持文件类型附件信誉。
“潜在有害程序”		潜在有害程序 (PUP) 是合法公司编写的软件程序，意外安装在计算机上后，可能会改变计算机的安全或隐私策略。 这些程序可以与您可能需要的合法程序一起下载。
	“检测到 PUP”	在传入的电子邮件中检测到，并根据策略设置对其采取适当操作的潜在有害程序。
	“PUP 已阻止”	从传入的电子邮件中删除，并根据策略设置对其采取适当操作的潜在有害程序。
“禁止的文件类型和消息”		部分文件附件类型可能为病毒。 通过文件扩展名阻止附件是邮件系统的另一层安全性。 系统会检查内部和外部电子邮件中是否存在禁止的文件类型或邮件。
	“禁止的文件类型”	某些类型的文件附件容易感染病毒。按文件扩展名阻止附件的功能是邮件系统的又一层安全措施。
	“禁止的消息”	您想要阻止进入邮件系统的特定电子邮件。 系统将检查内部和外部邮件中的阻止的内容。
“DLP 和合规性”	若要查看可用的字典，请在“策略管理器”	“共享资源”	“DLP 和合规性字典”中，单击“类别”下拉列表。	阻止通过电子邮件丢失敏感信息。 MSME 拥有行业领先的电子邮件内容分析，为任意形式的敏感内容提供最紧密的控制，从而符合众多国家、地区和国际法规。 通过行业内最广泛的电子邮件数据丢失防护（DLP，执行模式匹配来检测数据），以及防止出站数据丢失的基于策略的邮件处理方式来防止数据泄露。
“有害内容”		有害内容指用户不希望通过电子邮件收到的任何内容。 可以使用特定的词语或短语来定义规则，以便触发相应的策略并阻止此类电子邮件。
	“打包程序”	打包的可执行文件，运行时它将在内存中自行解压缩和/或解密，因此磁盘上的文件永远与其内存映像不相同。 打包程序是为了绕过安全软件并防止反向工程而专门设计的。
	“加密/遭破坏的内容”	无法分类为已加密或已遭破坏内容的电子邮件。
	“加密内容”	有些电子邮件可能已加密，这表示无法扫描这些电子邮件的内容。 加密内容策略可以指定检测后如何处理加密的电子邮件。

表 2-2 检测定义 *（续）*

类别	其他信息	说明
	“签名的内容”	当信息以电子方式发送时，可能会无意或有意被改变。 为了解决此问题，有些电子邮件软件使用数字签名，即手写签名的电子形式。 数字签名是添加到发件人的邮件中的附加信息，用于标识和验证发件人以及邮件中的信息。它已加密并充当数据的唯一摘要。通常情况下，收到的电子邮件的末尾显示一长串字母和数字。然后，电子邮件软件重新检查发件人的邮件中的信息并创建数字签名。如果该签名与原始签名相同，则数据没有更改。 如果电子邮件包含病毒、已损坏内容或过大，软件可能会清理或删除邮件的某一部分。电子邮件仍然有效并可以阅读，不过原始数字签名“已损坏”。收件人无法信任电子邮件的内容，因为这些内容也可能以其他方式更改过。
	“损坏的内容”	有些电子邮件的内容可能已损坏，这表示无法扫描电子邮件的内容。 遭破坏的内容策略可以指定检测后如何处理内容已遭破坏的电子邮件。
	“拒绝服务”	一种针对计算机、服务器或网络的攻击方法。 这类攻击是产品附带的有意或无意构架代码，可通过单独网络或连接互联网的系统启动，或直接通过主机启动。 该攻击旨在禁用或关闭目标，并且中断系统响应合法连接请求的功能。 拒绝服务攻击常使用错误的连接请求覆盖其目标，从而使目标忽略合法的请求。
	“受保护的内容”	有些电子邮件的内容受到保护，这表示无法扫描电子邮件的内容。 受保护的内容策略可以指定检测后如何处理具有受保护的内容的电子邮件。
	“受密码保护的文件”	可以对电子邮件发送的文件进行密码保护。 无法扫描受密码保护的文件。 受密码保护的文件策略指定如何处理包含受密码保护的文件的电子邮件。
	“不完整的 MIME 邮件”	多用途互联网邮件扩展 (MIME) 是一种通信标准，允许通过仅支持 7 位 ASCII 字符的协议（例如 SMTP）传输非 ASCII 格式。 MIME 定义编码非 ASCII 格式的不同方法，这样可以使用 7 位 ASCII 字符集中的字符表示非 ASCII 格式。 如果 MIME 邮件正文中的内容太大而无法通过邮件传输系统时，可以用一系列较小 MIME 邮件的方式使正文通过。 这些 MIME 邮件被称为部分或不完整的 MIME 邮件，因为每条 MIME 邮件仅包含整体邮件中必须传输的片段。
“邮件 URL 信誉”	“检测到的 URL”	URL 信誉检测到的电子邮件中的可疑 URL。

计划软件更新

计划自动更新，让软件始终更新为最新的防病毒 DAT、防病毒引擎、更多驱动程序和反垃圾邮件引擎。

默认情况下，根据“SiteList 编辑器”中指定的存储库设置进行产品更新。 若要更改存储库设置，请使用“开始”|“所有程序”|“McAfee”|“Security for Microsoft Exchange”选项中的“SiteList 编辑器”。 但是，如果您的计算机由 ePolicy Orchestrator 服务器托管，则根据 ePolicy Orchestrator 中提供的设置进行产品更新。

任务

1 单击“信息显示板” | “统计和信息”。

2 在 “版本 & 更新”部分，单击 “更新信息”选项卡。

3 在 “更新频率”中，选择 “编辑计划”。

将显示 “编辑计划”页面。

4 在“选择时间”中，根据所需的软件更新频率，选择相应的选项。

最佳方法是计划每天更新，方法是选择“天数”并在“每” “天”文本框下指定 1。 请在非业务时间或网络通信量低的时候执行软件更新。

5 单击 “保存”，然后单击 “应用”。

现在，您已成功计划了软件更新。

按需扫描及其视图

按需扫描程序是您在方便时手动启动或定期启动的安全扫描程序。通过它，您可以设置不同的配置，并扫描特定邮件或邮箱。

使用 MSME，您可以创建计划的按需扫描。您可以创建多个计划，每个计划在预定的时间段或时间自动运行。

您可以计划在服务器活动水平相对较低和不干扰您的工时间定期执行扫描操作。

该功能仅适用于具有邮箱角色的 Exchange Server。您不能在只具有边缘传输或集线器传输角色的 Exchange Server 上计划按需扫描。

何时执行按需扫描

当您的组织由于恶意活动而出现运转中断的情况时，强烈建议您执行按需扫描。它能确保 Microsoft Exchange 数据库干净，并且在运转中断期间不会受到感染。

McAfee 建议您在非业务时间执行按需扫描任务。当在非业务时间计划按需扫描任务，并且在高峰工作时间继续执行该任务时，您必须重新考虑被扫描的数据库，并通过修改被扫描的数据来创建替代计划。

您可以在周末计划按需扫描，以确保 Exchange 数据库干净，较早的电子邮件也会由最新的防病毒特征码扫描。管理员计划按需扫描时必须记住 Exchange Server、数据库和邮件流的数量。您的目标是必须在业务时间前完成此任务。

为何执行按需扫描？

您可能会出于多个原因执行按需扫描。例如：

- 检查已上载或发布的一个或多个特定文件。
- 检查 Microsoft Exchange Server 中的邮件是否有病毒，您可能需要执行 DAT 更新以便可以检测到新病毒。
- 已检测并清理病毒并且希望检查计算机是否是完全干净的。

查看按需扫描任务

查看为 MSME 配置的按需扫描任务列表。

任务

- 单击“信息显示板” | “按需扫描”。 “按需扫描”页面会列出配置的按需扫描任务。

  默认情况下，安装 MSME 时会创建计划的、名为“默认扫描”的按需扫描任务。

  在 “按需扫描”页面中，您可以使用以下选项：

表 2-3 选项定义

选项	定义
“名称”	指示按需扫描任务的名称。
“状态”	指示按需扫描任务的当前状态，包括 “空闲”、 “正在运行”、 “已停止”或 “完成”。
“上次运行时间”	指示上次执行按需扫描的日期和时间。
“下次运行时间”	指示下一次按需扫描计划运行的日期和时间。
“操作”	列出下面这些适用于所有可用按需扫描任务的选项： • “修改” • “删除” • “立即运行” • “显示状态” “停止” 选项只有在按需扫描任务正在运行时才会显示。
“修改”	指示按需扫描任务的设置。
“删除”	删除所选的按需扫描任务。
“立即运行”	立即启动选定的按需扫描任务。 “立即运行”仅在创建和应用计划外的按需扫描任务后适用。
“显示状态”	显示按需扫描任务的当前状态。将显示 “任务状态”页面，其中包括以下选项卡： • “常规” — 提供关于按需扫描任务的详细信息，例如：任务的总运行时间、任务进程、用于扫描的 DAT 和引擎版本、扫描结果、扫描的项目总数、违反的规则和扫描的文件夹。 • “设置” — 提供关于扫描的数据库和使用的策略的详细信息。 “显示状态” 选项只有在启动按需扫描任务以后才可用。
“停止”	停止正在运行的按需扫描任务。
“刷新”	刷新具有最新按需扫描信息的页面。
“New Scan（新建扫描）”	计划新的按需扫描任务。

您现已成功查看为 MSME 配置的所有可用的按需扫描任务。

创建按需扫描任务

计划按需扫描任务可按适当的时间间隔查找或删除邮箱中的病毒和阻止的内容。

开始之前

请确保您没有从 Active Directory 删除产品安装过程中创建的 “MSMEODuser”。对邮箱执行按需扫描时需要此用户。

任务

1 单击“信息显示板” | “按需扫描”。 此时会出现“按需扫描”页面。

2 单击“新建扫描”。此时将显示“选择扫描时间”页。

3 在“选择时间”选项卡中，指定您希望运行扫描的时间。 可用选项包括：

- “未计划” — 如果您尚未确定执行按需扫描或禁用现有按需扫描的计划的时间，请选择此选项。
- “一次” — 指定计划一次按需扫描的日期和时间。
- “小时” — 如果每天必须多次执行按需扫描任务，请选择该选项以按小时计划任务。 例如，假设当前时间为 14:00，并且您必须创建满足以下三个条件的按需扫描任务：
  - 按需扫描必须于 14:30 准时开始
  - 一天必须进行两次按需扫描

  要实现这一操作，将小时指定为 12，将分钟指定为 30。
- “天” — 根据每周必须执行的扫描频率，选择该选项以计划任务。 例如，如果想要每三天执行一次按需扫描，在“天”中指定 3 并选择开始任务的时间。
- “周” — 根据每月必须执行的扫描频率，选择该选项以计划任务。 例如，如果想要每两周执行一次按需扫描，在“周”中指定 2 并选择开始任务的具体时间。
- “月” — 根据每年必须执行的扫描频率，选择该选项以计划任务。 例如，如果想要每月第二个周六执行一次按需扫描，在 “计划于”下拉列表中选择“第二个”，在“星期”下拉列表中选择“星期六”，然后选择所有月份和任务开始时间。

启用“在任务运行”<n>“小时” <n>“分钟后停止”，以停止超过特定时间的按需扫描任务。

4 单击“下一步”。 此时会显示“选择扫描内容”页面。 可用选项包括：

- “扫描所有文件夹” — 选择此选项可扫描 Exchange Server 中的所有邮箱。
- “扫描所选文件夹” — 选择此选项可扫描 Exchange Server 中的特定邮箱。
- “扫描除所选以外的所有文件夹” — 选择此选项可扫描除添加到“要扫描的文件夹”列表的特定邮箱以外的所有邮箱。

在 Microsoft Exchange 2013 和 2016 中，公共文件夹显示为邮箱的一部分，并且公共文件夹的按需扫描始终是递归的。 在 Microsoft Exchange 2010 中，可以选择文件夹或子文件夹级别的公共文件夹以运行递归按需扫描。

5 单击“下一步”。此时将显示“配置扫描设置”页。

6 在“要使用的策略”下拉列表中，根据扫描要求选择任一策略选项。

策略	说明
“默认”	所有扫描程序和过滤器的默认设置，以下扫描程序除外： • “DLP 和合规性扫描程序” • “文件过滤”
“查找病毒”	防病毒设置和过滤器。 这些策略提供检查数据库中的病毒内容的简单方法。
“删除病毒”	防病毒设置和过滤器。 这些策略提供删除数据库中的病毒内容的简单方法。
“查找非兼容内容”	内容扫描设置。 如果想要查看新创建/分配的内容扫描规则效果，这些策略会非常有用。

策略	说明
“删除非兼容内容”	内容扫描设置。 如果想要查看新创建/分配的内容扫描规则效果以及删除不兼容的内容，这些策略会非常有用。
“完全扫描”	所有扫描程序和过滤器的设置。 这些策略通常用于定期进行的扫描。

设置和要采取的操作在“策略管理器”下的按需策略中指定。

7 选择“可恢复扫描”和“从上一项目重新启动”选项在邮箱数据库上以多任务形式运行按需扫描任务。

有时，您可能想要针对所有邮箱运行按需扫描任务。 在一个任务中扫描所有邮箱可能会花费较长时间，从而影响系统的效率。 您可以通过多个任务计划扫描，而不是在一个任务中扫描所有邮箱。

8 在 Exchange Server 中，您现在可以选择执行精细按需扫描任务。 使用以下字段可缩小扫描范围：

- 主题
- 发件人
- 收件人
- 消息 ID
- 收件人
- 日期范围
- 邮件大小
- 附件
- 未读项目

执行精细的按需扫描可节省时间，并获取特定的扫描结果。

9 单击“下一步”。此时将出现“输入扫描的名称”页。

10 根据您在上一页中选择的策略，指定有意义的按需扫描任务名称。例如，如果您正在创建在周末执行全方位扫描的按需扫描任务，可将任务名称指定为 Weekend Full Scan。

11 单击“完成”，然后单击“应用”。

执行完以上步骤，您就成功创建了按需扫描任务。

状态报告

状态报告是在特定时间发送给管理员的计划的报告。报告包含该指定时间范围内的检测统计信息。

通过使用 “状态报告”，您可以自动执行定期查询统计信息的任务。您可以计划定期收集简单的统计信息（如特定日期的检测数量）的任务，并向 Exchange 管理员或分发列表发送电子邮件。

这些报告有助于了解哪些 Exchange Server 受到的威胁较多，您可以使用什么来提供用于减少威胁情况的机制。

您可以指定时间、将报告发送到哪个收件人电子邮件地址或分发列表以及电子邮件的主题。状态报告将以 HTML 或 CSV 格式发送给收件人。

根据您的配置，状态报告电子邮件将包含关于检测到的项目的统计信息，例如：病毒、垃圾邮件、网络钓鱼、IP 信誉、PUP、禁止的文件类型、不需要的内容、DLP 和合规性、干净的电子邮件以及扫描的电子邮件总数。有关计划状态报告的方法的详细信息，请参阅 “计划新的状态报告”。

安装 MSME 后，状态报告需要至少 24 小时时间才能在通知电子邮件中填充统计信息。

查看状态报告任务

查看针对 MSME 配置的状态报告任务列表。

任务

- 单击“信息显示板” | “状态报告”。 显示的“状态报告”页面会列出配置的状态报告任务。

  在 “状态报告”页面中，您可以使用以下选项：

表 2-4 选项定义

选项	定义
“名称”	表示报告任务的名称。
“状态”	表示报告任务的状态，分为“空闲”、“正在运行”、“已停止”或“已完成”。
“上次运行”	表示上次执行报告任务的日期和时间。
“下次运行”	表示下次计划运行报告任务的日期和时间。
“操作”	列出以下选项，适用于所有可用的报告任务： • “修改” • “删除” • “立即运行” • “显示状态” “停止” 选项只有在报告任务正在运行时才会显示。
“修改”	单击“修改”以编辑按需扫描任务的设置。
“删除”	删除所选报告任务。
“立即运行”	立即启动所选报告任务。
“显示状态”	显示报告任务的状态。 “任务状态”页面包含该选项卡： • “常规” — 提供关于开始和结束时间、任务运行时、当前操作和任务进程等报告任务的详细信息。 “显示状态”选项仅在报告任务启动后可用。
“刷新”	刷新页面以显示最新的报告信息。
“新建报告”	计划新的状态报告任务。

您已成功查看针对 MSME 配置的所有可用状态报告任务。

计划新的状态报告

计划新的状态报告任务可按适当的时间间隔，将检测统计信息发送到特定的电子邮件地址或分发列表。

任务

1 单击 “信息显示板” | “状态报告”。将显示 “状态报告”页面。

2 单击 “新建报告”。将显示 “报告”页面。

3 在 “报告时间”选项卡中，指定要运行状态报告任务的时间。可用选项包括：

- “Not scheduled（未计划）” — 如果您尚未决定执行状态报告任务或禁用现有状态报告任务计划的时间，请选择此选项。
- “一次” — 指定计划一次状态报告任务的日期和时间。

- “小时” — 如果您一天之内要多次执行状态报告任务，选择此选项可按小时计划任务。例如，假设当前时间是 14:00，您需要创建满足以下条件的报告任务：
  - 状态报告任务必须于 14:30 准时开始
  - 一天必须执行两次状态报告任务

  要实现这一操作，可将小时指定为 12，将分钟指定为 30。
- “天” — 选择此选项可根据一周内要执行状态报告任务的频率来计划任务。例如，如果您希望三天执行一次状态报告任务，可将 “天”指定为 3，并选择任务开始的时间。
- “周” — 选择此选项可根据一月内要执行状态报告任务的频率来计划任务。例如，如果您希望两周执行一次状态报告任务，可将 “周”指定为 2，并选择任务开始的日期和时间。
- “月” — 选择此选项可根据一年内要执行状态报告任务的频率来计划任务。例如，如果您希望在每个月的第二个星期六执行状态报告任务，可从 “在”下拉列表中选择 “第二个”，从 “星期”下拉列表中选择 “星期六”，然后选择任务开始的所有月份和时间。

启用 “在任务运行” <n> “小时” <n> “分钟后停止”，可在状态报告任务超出指定小时数时将其停止。

4 单击 “下一步”。将显示 “报告设置”页面。可用选项包括：

表 2-5 选项定义

选项	定义
“收件人电子邮件”	指定收件人电子邮件地址或分发列表的 SMTP 地址。在大多数情况下，这一项应是 Exchange 管理员的电子邮件地址。 默认情况下，使用 “设置和诊断” | “通知” | “设置” | “常规” | “管理员电子邮件”中的电子邮件地址作为收件人电子邮件地址。
“报告的主题行”	为电子邮件指定有意义的主题行。例如，如果您希望每天接收 HTML 格式的状态报告，可指定 MSME Daily Status Report (HTML)。
“行数”	指定在状态报告电子邮件中显示的行数 (n)。状态报告中的每行显示特定日期的检测总数。报告包含最近 (n) 天的检测计数，不包括触发状态报告的那一天。例如：如果您指定 1，状态报告将包含一行，显示昨天的检测。 您可以指定的最大值是 365。
“报告类型”	指定发送给收件人的状态报告的格式。可用选项包括： • “CSV” — 如果您希望状态报告以逗号分隔值格式作为 .csv 文件附件发送给收件人，请选择此选项。 • “HTML” — 如果您希望状态报告以 HTML 格式作为 .html 文件附件发送给收件人或出现在电子邮件正文中，请选择此选项。

5 单击 “下一步”。此时将显示 “请输入任务名称”页。

6 根据您在之前的页面中选择的计划和格式，指定有意义的状态报告任务名称。例如，如果您要创建以 HTML 格式提供工作日检测统计信息的周状态报告任务，可将任务名称指定为 Weekly Status Report (HTML)。

7 单击 “完成”，然后单击 “应用”。

完成以上步骤后，您就成功创建了新的状态报告任务。

状态报告电子邮件通知

根据计划的状态报告，收件人会收到一封电子邮件，包含特定时间段内 MSME 扫描和检测到的所有电子邮件的统计信息。

根据您的状态报告配置，状态报告电子邮件将包含检测到的项目、干净电子邮件总数以及当天扫描的电子邮件总数的统计信息。

表 2-6 选项定义

选项	定义
“自”	显示“设置和诊断”	“通知”	“设置”	“常规”	“发件人电子邮件”中指定的电子邮件地址。
“至”	显示“设置和诊断”	“通知”	“设置”	“常规”	“管理员电子邮件”中指定的收件人电子邮件地址。
“主题”	显示“信息显示板”	“状态报告”	“报告设置”	“报告主题行”中指定的状态报告电子邮件通知主题。
“服务器扫描统计信息”	显示安装了 MSME 的“计算机名称”。
“日期”	以 MM/DD/YYYY 格式显示日期。
“检测”	显示邮件正文中“病毒”、“垃圾邮件”、“网络钓鱼”、“IP 信誉”、“潜在有害程序”、“禁止文件类型”、“有害内容”和 “DLP 和合规性”。 只有安装了 McAfee Anti-Spam 插件后，才能使用“垃圾邮件”、“网络钓鱼”和“IP 信誉”统计信息。
“干净”	显示 MSME 检测为干净并且不存在威胁的干净电子邮件总数。 例如，即使是发送给管理员的状态报告电子邮件，在统计信息中也会被视为干净的电子邮件。
“总计扫描”	显示 MSME 当天扫描的电子邮件总数。

如果在“设置和诊断” | “反垃圾邮件” | “McAfee GTI IP 信誉”中将 “IP 信誉阈值”值设置为“受信任的 IP（低于 0）”或“中性 IP（等于或高于 0）”，状态报告电子邮件将被阻止。

配置报告

配置报告是在特定时间发送给管理员的计划报告。 该报告包含 MSME 产品信息、策略设置和系统信息。

通过使用 “配置报告”，您可以自动执行定期查看产品配置摘要的任务。

如果组织中有多个管理员并且您想跟踪 MSME 配置相关设置，该功能会非常有用。 如果 ePolicy Orchestrator 托管多个 MSME 产品并且您想要跟踪产品配置，也会非常有用。

您可以选择电子邮件的时间、收件人电子邮件地址或发送报告的分配列表和主题。

根据您的配置，配置报告将包含产品和系统信息，例如：服务器信息、产品版本信息、产品许可证状态和类型、修补程序信息、调试日志记录信息、按访问扫描程序设置、按访问策略设置和网关策略设置。有关计划配置报告的方法的详细信息，请参阅 “计划新的配置报告”。

查看配置报告任务

查看针对 MSME 配置的配置报告任务列表。

任务

- 单击“信息显示板” | “配置报告”。 显示的“配置报告”页面列出了已配置的配置报告任务。

  在 “配置报告”页面中，您可以使用以下选项：

表 2-7 选项定义

选项	定义
“名称”	表示报告任务的名称。
“状态”	表示报告任务的状态，分为“空闲”、“正在运行”、“已停止”或“已完成”。
“上次运行”	表示上次执行报告任务的日期和时间。
“下次运行”	表示下次计划运行报告任务的日期和时间。
“操作”	列出以下选项，适用于所有可用的报告任务： • “修改” • “删除” • “立即运行” • “显示状态” “停止” 选项只有在报告任务正在运行时才会显示。
“修改”	单击“修改”以编辑按需扫描任务的设置。
“删除”	删除所选报告任务。
“立即运行”	立即启动所选报告任务。
“显示状态”	显示报告任务的状态。 “任务状态”页面包含该选项卡： • “常规” — 提供关于开始和结束时间、任务运行时、当前操作和任务进程等报告任务的详细信息。 “显示状态”选项仅在报告任务启动后可用。
“刷新”	刷新页面以显示最新的报告信息。
“新建报告”	计划新的配置报告任务。

您已成功查看针对 MSME 配置的所有可用配置报告任务。

计划新的配置报告

计划新的配置报告任务可按适当的时间间隔，将产品配置和系统信息发送到特定的电子邮件地址或分发列表。

任务

1 单击“信息显示板” | “配置报告”。此时将显示“配置报告”页。

2 单击 “新建报告”。将显示 “报告”页面。

3 在 “报告时间”选项卡中，指定要运行配置报告任务的时间。可用选项包括：

- “Not scheduled（未计划）” — 如果您尚未决定执行配置报告任务或禁用现有配置报告任务计划的时间，请选择此选项。
- “一次” — 指定计划一次配置报告任务的日期和时间。
- “小时” — 如果您一天之内要多次执行配置报告任务，选择此选项可按小时计划任务。例如，假设当前时间是 14:00，您需要创建满足以下条件的报告任务：
  - 配置报告任务必须于 14:30 准时开始
  - 一天必须执行两次配置报告任务

  要实现这一操作，可将小时指定为 12，将分钟指定为 30。

- “天” — 选择此选项可根据一周内要执行配置报告任务的频率来计划任务。例如，如果您希望三天执行一次配置报告任务，可将 “天”指定为 3，并选择任务开始的时间。
- “周” — 选择此选项可根据一月内要执行配置报告任务的频率来计划任务。例如，如果您希望两周执行一次配置报告任务，可将 “周”指定为 2，并选择任务开始的日期和时间。
- “月” — 选择此选项可根据一年内要执行配置报告任务的频率来计划任务。例如，如果您希望在每个月的第二个星期六执行配置报告任务，可从 “在”下拉列表中选择 “第二个”，从 “星期”下拉列表中选择 “星期六”，然后选择任务开始的所有月份和时间。

启用 “在任务运行” <n> “小时” <n> “分钟后停止”，可在配置报告任务超出指定小时数时将其停止。

4 单击 “下一步”。将显示 “报告设置”页面。可用选项包括：

表 2-8 选项定义

选项	定义
“收件人电子邮件”	指定收件人电子邮件地址或分发列表的 SMTP 地址。在大多数情况下，这一项应是 Exchange 管理员的电子邮件地址。 默认情况下，使用 “设置和诊断” | “通知” | “设置” | “常规” | “管理员电子邮件”中的电子邮件地址作为收件人电子邮件地址。
“报告的主题行”	为电子邮件指定有意义的主题行。例如，如果您希望每周接收配置报告，可指定 MSME Weekly Configuration Report。

5 单击 “下一步”。将显示 “Please enter a task name（请输入任务名称）”页面。

6 根据您在之前的页面中选择的计划和格式，指定有意义的配置报告任务名称。例如，如果您要创建提供关于每个月第一个星期一的产品和系统信息的月配置报告任务，可将名称指定为 Monthly Configuration Report (First Monday)。

7 单击 “完成”，然后单击 “应用”。

完成以上步骤后，您就成功创建了新的配置报告任务。

配置报告电子邮件通知

根据计划的配置报告，收件人将收到一封包含指定持续时间内的 MSME 产品信息、策略设置和系统信息的电子邮件。

表 2-9 选项定义

选项	定义
“服务器信息”	显示服务器信息，例如计算机名称、IP 地址和 Exchange 版本。
“版本信息”	显示 MSME 信息，例如产品版本、DAT 版本和日期、引擎版本、反垃圾邮件规则和引擎信息（如果有）。
“许可状态”	显示产品许可信息，例如 MSME 和 Anti-Spam 插件组件许可类型。
“产品信息”	显示有关是否安装了任何 Service Pack 或修补程序的其他产品信息。
“调试日志记录”	显示 “调试日志记录”信息，例如级别、日志文件的最大大小以及文件位置。
“按访问设置”	显示指定启用或禁用哪项设置的当前的 “按访问设置”配置。
“基于访问的策略”	显示为 “按访问” “主策略”启用的核心扫描程序和过滤器。
“网关策略”	显示 “网关” | “主策略”的反垃圾邮件和反网络钓鱼扫描程序的当前状态。 此选项仅在您安装了 McAfee Anti-Spam 插件组件后才可用。

图形报告

生成图形报告以了解特定时间范围内的威胁级别。以 “柱状图” 或 “饼图” 的形式提供检测到的项目的直观视图。

这些报告与状态报告一起可帮助您和您的组织识别面临较高威胁的服务器，并帮助您找出减小损失的方法。

当您只想查看当前威胁级别而不想对检测到的项目采取任何操作时，请使用图形报告。 通过 “图形报告”，您可以根据某些过滤器进行查询，并在其中查看 不同检测的 “前 10” 个报告。

“图形报告” 的类别包括：

- “简单” — 使用有限的搜索过滤器查看一天或一周的前 10 个报告。
- “高级” — 使用更多搜索选项对不同的过滤器、时间范围和图表选项进行查询。

使用简单搜索过滤器查看图形报告

使用简单搜索过滤器生成每天或每周的关于检测的图形报告。

任务

1 单击 “信息显示板” | “图形报告”。将显示 “图形报告” 页面。

2 单击 “简单” 选项卡。

3 在 “时间范围” 下拉列表中，选择 “今天” 或 “本周”，查看当天或本周隔离的检测。

4 在 “过滤器” 下拉列表中，选择要查看的报告。 可用的选项包括：

- “Top 10 Viruses（前 10 个病毒）” — 列出按检测计数排列的前 10 个病毒名称。
- “Top 10 Spam Detections（前 10 个垃圾邮件检测）” — 列出按垃圾邮件计数排列的前 10 个检测到的垃圾邮件电子邮件。
- “Top 10 Spam Recipients（前 10 位垃圾邮件收件人）” — 列出按收到的垃圾邮件计数排列的前 10 位垃圾邮件收件人。
- “Top 10 Phish Detections（前 10 个网络钓鱼检测）” — 列出按网络钓鱼邮件计数排列的前 10 个检测到的网络钓鱼电子邮件。
- “前 10 个已阻止的 IP 地址” — 列出按退回电子邮件的已阻止计数排列的前 10 个 IP 地址。
- “前 10 个不需要的程序” — 列出可能是威胁的前 10 个可能不需要的程序。
- “前 10 个 TIE 检测” — 列出 TIE 检测到的前 10 个潜在威胁。
- “前 10 个欺诈检测” — 列出检测到的前 10 个欺诈电子邮件。
- “前 10 个 DLP 和合规性检测” — 列出按触发规则的检测计数排列的前 10 个数据丢失防护和合规性违规事件。
- “前 10 个被感染的文件” — 按检测计数列出排名前 10 的文件名。
- “前 10 个阻止的 URL” — 列出检测到的可能有威胁的前 10 个 URL。
- “前 10 个检测项” — 按检测计数列出排名前 10 的检测项。 该图包含所有类别，例如上述的病毒、垃圾邮件检测、垃圾邮件收件人、网络钓鱼检测、阻止的 IP 地址、有害程序、DLP 和合规性、恶意 URL 和被感染的文件。

5 单击 “搜索”。 搜索结果显示在 “查看结果” 窗格中。

在 “Magnify Graph（放大图形）” 中，选择缩放比例，以放大或缩小 “查看结果” 窗格中的图形视图。

使用高级搜索过滤器

使用高级搜索过滤器生成关于检测的图形报告。

任务

1 单击“信息显示板” | “图形报告”。 此时会显示“图形报告”页面。

2 单击 “高级”选项卡。

3 从列表中选择过滤器（至少一个，最多三个）：

表 2-10 主过滤器

过滤器	说明
“主题”	使用电子邮件的“主题”进行搜索。
“收件人”	使用收件人的电子邮件地址进行搜索。
“原因”	使用检测触发器或使用项目被隔离的原因进行搜索。 如果选择“原因”过滤器，会启用辅助过滤器以进一步细化搜索。 例如，您可能希望搜索以下项目：由于作为原因触发的“邮件大小”规则而被隔离的所有项目。
“票证编号”	使用票证编号进行搜索。 票证号是本软件为每个检测自动生成的 16 位字母数字条目。
“检测项名称”	按检测到的项目的名称搜索。
“垃圾邮件分数”	根据垃圾邮件分数进行搜索。 例如，您可能希望搜索在“垃圾邮件分数”等于 3 时隔离的所有项目。

“垃圾邮件分数”表示电子邮件中包含的潜在垃圾邮件的数量。 引擎会将反垃圾邮件规则应用到所扫描的每封电子邮件。 每条规则都与一个分数关联。 要评估电子邮件包含垃圾邮件的风险，需将分数相加以得出该电子邮件的垃圾邮件总分。 垃圾邮件总分越高，电子邮件包含垃圾邮件的风险越大。 垃圾邮件分数范围在 0 ~ 100 之间。 收到的邮件从垃圾邮件分数为 0 开始。每次邮件违反过滤器时，其垃圾邮件分数都会增加。

辅助过滤器仅适用于“原因”过滤器。 如果不想指定辅助过滤器，请确保该字段留空以便查询所有检测项。

表 2-11 辅助过滤器

过滤器	说明
“防病毒”	搜索当在邮件中发现潜在病毒时被隔离的项目。
“DLP 和合规性”	搜索当在邮件中发现禁止的内容时被隔离的项目。 例如：不合适的字词。
“文件过滤器”	搜索当在邮件中发现禁止的文件时被隔离的项目。
“反垃圾邮件”	搜索当发现垃圾邮件时被隔离的项目。 例如：连锁电子邮件
“IP 信誉”	搜索当 IP 信誉超出定义的阈值时被隔离的项目。
“已加密或已损坏”	搜索当在电子邮件中发现加密或损坏的内容时被隔离的项目。
“潜在有害程序”	搜索当在电子邮件中发现潜在有害程序时被隔离的项目。
“网络钓鱼”	搜索当在电子邮件中发现网络钓鱼内容时被隔离的项目
“打包程序”	搜索当在电子邮件中发现打包程序（小程序、压缩的可执行文件、加密代码）时被隔离的项目。
“邮件大小”	搜索当邮件大小超出最大限制设置时被隔离的项目。
“已加密”	搜索当在电子邮件中发现加密内容时被隔离的项目。
“已签名”	搜索当在电子邮件中发现已签名内容时被隔离的项目。
“已损坏”	搜索当在电子邮件中发现损坏的内容时被隔离的项目。
“拒绝服务”	搜索当发生拒绝服务威胁时被隔离的项目。 例如：想要检索事件中被隔离的所有电子邮件。
“受保护的内容”	搜索当发现受保护的内容时被隔离的项目，不会访问该内容进行详细审查。
“受密码保护”	搜索当发现受密码保护的内容时被隔离的项目，不会访问该内容进行详细审查。
“被阻止的 MIME”	搜索当在电子邮件中发现被阻止的 MIME（多用途互联网邮件扩展）时被隔离的项目。
“URL 信誉”	搜索当 URL 信誉超出定义的阈值时被隔离的项目。
“TIE 信誉”	搜索当 TIE 信誉超出定义的阈值时被隔离的项目。

表 2-11 辅助过滤器 *（续）*

过滤器	说明
“SPF 软故障”	搜索当在电子邮件中发现欺诈内容时被隔离的项目。
“SPF 硬故障”	搜索当在电子邮件中发现欺诈内容时被隔离的项目。

有关搜索过滤器的更多信息，请参见“搜索过滤器”。

4 从下拉列表中选择“所有日期”或“日期范围”。

如果选择“所有日期”，查询会返回隔离数据库中从隔离任何检测到的项目第一天起的搜索结果。 如果选择“日期范围”，选择“从”和“到”字段中的**日期**、**月**、**年**、**小时**和**分钟**以启用查询以在日期范围内进行搜索。

5 根据需要，选择“柱状图”或“饼图”。

6 如果选择“饼图”，请从下拉列表中选择过滤器以进一步细化搜索：

表 2-12 查询条件

过滤器	说明
收件人	使用收件人电子邮件地址进行搜索。
发件人	使用发件人电子邮件地址进行搜索。
文件名	使用隔离的文件名进行搜索。
检测名称	使用检测到的项目的名称进行搜索。
主题	使用电子邮件的“主题”进行搜索。
原因	使用检测触发或隔离项目的原因进行搜索。
规则名称	使用触发检测的规则的名称进行搜索。
策略名称	使用做出检测的策略的名称进行搜索。

a 在 “Maximum Results（最大结果数）”中，指定要查看的搜索结果数量。您最多可以查看 99 条搜索结果，并且该字段仅在您选择饼图时可用。

7 单击 “搜索”。搜索结果将显示在 “查看结果”窗格中。在“Magnify Graph（放大图形）”中，选择缩放比例，以放大或缩小“查看结果”窗格中的图形视图。搜索结果将显示在 “查看结果”窗格中。

3 检测到的项目

查看包含潜在威胁（MSME 已检测到并已隔离）的所有电子邮件的信息。 可以使用不同的搜索过滤器来细化搜索以及查找所需的隔离项目，查看其结果并对隔离项目执行必要的操作。

在产品的用户界面中，单击 “检测到的项目”，根据检测类别查看隔离的项目。检测类别包括：

- “垃圾邮件”
- “IP 信誉”
- “网络钓鱼”
- “病毒”
- “TIE 和 ATD 检测”
- “欺诈邮件”
- “潜在有害程序”
- “有害内容”
- “禁止的文件类型和消息”
- “DLP 和合规性”
- “邮件 URL 信誉”
- “所有项目”

只有安装了 McAfee Anti-Spam 插件后，才能使用“垃圾邮件”、“网络钓鱼”、“SPF 过滤器”和“IP 信誉”选项。

目录

管理隔离的数据

根据您的要求，确定是使用本地数据库还是专用的隔离管理服务器（称为 McAfee Quarantine Manager）来隔离检测到的项目。

默认情况下，检测到的项目会本地隔离到 MSME 安装的 PostgreSQL 数据库。

配置隔离位置

根据“检测到的项目”配置相关设置，您可以选择在本地数据库隔离检测到的项目或使用 McAfee 的隔离管理软件（著名的 McAfee Quarantine Manager）在单独服务器上隔离检测到的项目。

对于托管系统，如果选择 MQM 服务器隔离检测到的项目，确保配置仅在指定的系统上实施。 否则，配置会应用到“系统树”中的所有 MSME 服务器。

在产品用户界面中，单击“设置和诊断” | “检测到的项目”并选择：

- “McAfee Quarantine Manager” — 在 MQM 服务器上隔离检测到的项目。
- “本地数据库” — 按照指定的路径，在本地 MSME 服务器上隔离检测到的项目。

本地数据与 McAfee Quarantine Manager — 何时使用

此表帮助您了解对于隔离管理，何时使用本地数据库或 McAfee Quarantine Manager：

使用本地数据库...	使用 McAfee Quarantine Manager...
管理一个 MSME 安装的隔离项目。	管理多个 MSME 安装中的隔离项目或组织中配置的以下任一 MSME 产品： • McAfee Security for Microsoft Exchange • McAfee Email and WebSecurity Appliance • McAfee Security for Lotus Domino (Windows) 如果您已购买上述任一产品，可以免费下载和安装 McAfee Quarantine Manager。
如果您要使用 PostgreSQL 数据库来隔离项目。	如果您要使用 MySQL 或 Microsoft SQL Server 数据库来隔离项目。

有关 McAfee Quarantine Manager 软件及其功能的更多信息，请参见其产品文档。

检测类型

检测到的项目是被 MSME 标识为潜在威胁的电子邮件，可能是病毒、垃圾邮件、网络钓鱼、非兼容内容、URL 或禁止文件类型。

MSME 中的检测项类型为：：

检测类型	说明
“垃圾邮件”	一种有害的电子消息，通常是未经许可的群发电子邮件。 通常，垃圾邮件会发送给不想要接收该邮件的多个收件人。 类型包含垃圾电子邮件、垃圾即时消息、Usenet 新闻组垃圾邮件、网页搜索引擎垃圾邮件、博客垃圾邮件和手机垃圾短信。 垃圾邮件包含合法广告、误导性广告和网络钓鱼消息，旨在诱骗收件人提供个人和财务信息。 如果用户已登记要接收这些电子邮件，则不会将其视为垃圾邮件。
“IP 信誉”	一种根据发送服务器的 IP 地址检测电子邮件的方法。 McAfee 收集数百万 IP 地址和网络端口中的数据，提供数以亿万计的独特视图并根据网络通信（包括端口、目的地、协议以及入站和出站连接请求。）计算信誉分数。 该分数被称为“IP 信誉分数”，反映了网络连接存在威胁的可能性。 MSME 使用该分数根据本地策略确定相关操作。
“网络钓鱼”	一种以欺诈性手段获取个人信息的方法，这些个人信息包括密码、社会保险号和信用卡详细信息。方法是发送看起来是来自受信任源（例如银行或合法公司）的欺诈邮件。 通常，网络钓鱼电子邮件要求收件人单击电子邮件中的链接以验证或更新联系人详细信息或信用卡信息。 与垃圾邮件一样，网络钓鱼邮件也会发送到大量电子邮件地址，期望有人对电子邮件中的信息采取操作，从而泄露其个人信息。
“病毒”	一种计算机程序文件，会附加至磁盘或其他文件，并反复自行复制，通常在用户不知情或未获得用户允许的情况下执行这些操作。 一些病毒会附加至文件，因此在执行被感染的文件时，也会执行病毒。 其他病毒会驻留在计算机的内存中，并且在计算机打开、修改或创建文件时感染文件。 有些病毒会出现征兆，有些病毒会破坏文件和计算机系统，但是无论哪个都不是界定病毒的必要条件，无破坏性的病毒仍然是病毒。 您无法从“病毒”检测类别中“下载”、“释放”、“转发”或“查看”隔离的项目。
“TIE 和 ATD 检测”	除了 DAT 和 McAfee GTI 之外，您现在可以使用 McAfee Global Threat Intelligence 和 McAfee Advanced Threat Defense 的增强检测功能。

检测类型	说明
“欺诈邮件”	电子邮件欺诈是通过使用其他发件人电子邮件地址发送电子邮件来吸引用户的常用方法。 用户可能在不知道电子邮件实际上来自非法来源的情况下，打开和回复电子邮件。
“潜在有害程序”	通常合法软件（非恶意软件）可能会针对其安装的系统的安全状态或隐私状况发出警报。 这种软件可能但并不一定包含间谍软件、广告软件、按键记录器、密码解密程序、黑客工具和拨号程序，通常会随用户想要的程序一起下载。 具有安全意识的用户可能希望了解此类程序，并在某些情况下将其删除。
“有害内容”	这是触发内容扫描规则的任何内容。 可能包含攻击、辱骂、脏话或甚至是公司的机密信息。 “有害内容”可归类为： • “打包程序” • “加密内容” • “经过签名的内容” • “遭破坏的内容” • “拒绝服务” • “受保护内容” • “受密码保护的文件” • “不完整的 MIME 邮件”
“禁止文件类型和邮件”	部分文件附件类型可能为病毒。 通过文件扩展名阻止附件是邮件系统的另一层安全性。 系统会检查内部和外部电子邮件中是否存在禁止的文件类型或邮件。
“DLP 和合规性”	阻止通过电子邮件丢失敏感信息。 MSME 拥有行业领先的电子邮件内容分析，为任意形式的敏感内容提供最紧密的控制，从而符合众多国家、地区和国际法规。 通过行业中最广泛使用的 Data Loss Prevention (DLP) 来阻止数据泄露，通过模式匹配来检测数据；阻止出站数据丢失的策略邮件处理方法。
“邮件 URL 信誉”	阻止发送包含有害 URL（可能包含有害链接、网络钓鱼链接或恶意软件）的电子邮件。

只有安装了 McAfee Anti-Spam 插件后，才能使用“垃圾邮件”、“网络钓鱼”、“SPF 过滤器”和“IP 信誉”选项。

另请参阅

*搜索过滤器对比图*第 37 页
*其他搜索选项*第 38 页

可用的主要搜索过滤器

通过搜索过滤器，您可以定义搜索条件，更加高效和有效地搜索隔离数据库。

可用的主要搜索过滤器选项视您选择的检测到的项目类别而有所不同。这些搜索过滤器显示在检测到的项目类别的“查看结果”部分。

使用“查看结果”部分中的“要显示的列”，选择要查看的搜索过滤器。

表 3-1 检测到的项目 — 主要搜索过滤器

搜索过滤器	定义
“已采取的操作”	根据对项目采取的操作来搜索某个项目。 MSME 采取的操作为： • “清理” • “已清理” • “已删除” • “已删除消息” • “已拒绝访问” • “已记录” • “已替换” • “已拒绝”
“反垃圾邮件引擎”	根据扫描电子邮件中的垃圾邮件和网络钓鱼攻击的反垃圾邮件引擎搜索项目。 若要查看当前使用的“反垃圾邮件引擎”，转至“信息显示板”	“版本和更新”	“更新信息”	“反垃圾邮件引擎	规则版本”。 例如，“反垃圾邮件引擎”版本显示的格式为：9286
“反垃圾邮件规则”	根据反垃圾邮件规则搜索项目，规则每隔几分钟会更新一次，以捕获垃圾邮件制造者发送的最新垃圾邮件活动。 若要查看当前使用的“反垃圾邮件规则”，转至“信息显示板”	“版本和更新”	“更新信息”	“反垃圾邮件引擎	规则版本”。 例如，规则版本显示的格式为：core:4373:streams:840082:uri:1245250
“防病毒 DAT”	根据具有独特特征码的防病毒 DAT 版本搜索项目。 若要查看当前使用的“防病毒 DAT”，转至“信息显示板”	“版本和更新”	“更新信息”	“防病毒引擎	DAT 版本	其他驱动程序”。 例如，DAT 版本显示的格式为：6860.0000
“防病毒引擎”	根据防病毒引擎搜索项目，该引擎具有与病毒/不需要的内容唯一对应的字符序列。 若要查看当前使用的“防病毒引擎”，转至“信息显示板”	“版本和更新”	“更新信息”	“防病毒引擎	DAT 版本	其他驱动程序”。 例如，“防病毒引擎”版本显示的格式为：5400.1158
“禁止的短语”	按照“策略管理器”	“共享资源”	“DLP 和合规性字典”下的“DLP 和合规性规则”中定义的禁止短语内容进行搜索。
“检测名称”	根据名称搜索检测到的项目。
“文件名”	在隔离的项目中按检测到的文件的名称搜索。 若要查看使用的“文件名”，转至“策略管理器”	“共享资源”	“DLP 和合规性字典”	“文件过滤规则”。
“文件夹”	按存储隔离的项目的文件夹（例如用户的邮箱）搜索。 如果电子邮件在按访问（传输）级别被隔离，文件夹将不可用。
“IP 信誉分数”	根据发件人的 “IP 信誉分数”扫描某个项目。 隔离的项目取决于“设置和诊断”	“反垃圾邮件”	“McAfee GTI IP 信誉”中指定的 “IP 信誉阈值”。 只有安装了 McAfee Anti-Spam 插件后，才能使用该过滤器。
“策略名称”	按检测项目的策略名称（例如：“主策略”或子策略）搜索。
“原因”	根据检测到项目的原因搜索项目。这可以基于扫描程序和过滤器，例如：“防病毒”、“反垃圾邮件”、“反网络钓鱼”、“DLP 和合规性”等。
“原因”	按照特定电子邮件触发的一条或多条规则进行搜索。 如果某个项目触发了多个扫描程序或过滤器时，使用该过滤器。 例如，如果垃圾邮件包含病毒，“原因”为“反垃圾邮件”和“防病毒”。
“收件人”	通过收件人的电子邮件地址搜索项目。
“信誉分数”	基于最新的可用信息给出的电子邮件来源可靠性级别进行搜索。 隔离的项目取决于“设置和诊断”	“反垃圾邮件”	“McAfee GTI 邮件信誉”中指定的 “邮件信誉阈值”。 只有安装了 McAfee Anti-Spam 插件后，才能使用该过滤器。
“规则名称”	根据触发一个或多个扫描程序/过滤器的规则搜索项目。触发扫描程序或过滤器的规则以为每个策略设置的“操作”为基础。

表 3-1 检测到的项目 — 主要搜索过滤器 *（续）*

搜索过滤器	定义
“扫描方式”	按检测项目的扫描程序名称搜索项目。
“发件人”	按发件人的电子邮件地址搜索项目。
“发件人 IP”	根据发件人系统的 IP 地址搜索项目。 隔离的项目取决于“设置和诊断”	“反垃圾邮件”	“McAfee GTI IP 信誉”中指定的 “IP 信誉阈值”。 只有安装了 McAfee Anti-Spam 插件后，才能使用该过滤器。
“服务器”	根据计算机名称搜索项目。
“垃圾邮件得分”	根据垃圾邮件得分搜索项目，该分数表示电子邮件中包含的潜在垃圾邮件的数量。 引擎会将反垃圾邮件规则应用到所扫描的每封电子邮件。 每条规则都与一个分数关联。 若要评估电子邮件包含垃圾邮件内容的风险，可以将这些分数相加在一起以得出该电子邮件的垃圾邮件总分。垃圾邮件总分越高，则电子邮件包含垃圾邮件内容的风险就越高。 只有安装了 McAfee Anti-Spam 插件后，才能使用该过滤器。
“状态”	根据当前状态搜索项目。 可用的项目状态包括： • “未定位” — 未对其采取清除、释放、转发或删除等操作的项目。所有项目的初始状态都将为“未定位”。 • “已释放” — 从隔离数据库释放的项目。 • “在 Quarantine Manager 队列中” — 当前位于 McAfee Quarantine Manager 数据库队列中的项目。 • “转发” — 转发给目标收件人的项目。
“主题”	根据电子邮件的主题行搜索项目。
“任务”	根据扫描任务搜索项目，可以是按访问 (VSAPI)、按访问（传输）扫描任务或按需扫描任务。 “查看结果”部分中显示的按访问扫描任务取决于“设置和诊断”	“按访问设置”中启用的设置。 若要了解项目是否因按需扫描任务检测到的，请转至“信息显示板”	“按需扫描”。
“票证号”	根据票证号搜索项目，票证号是分配给特定检测并通过电子邮件作为通知传递的唯一字母数字标识符。它有助于标识关联的检测。
“TIE 分数”	根据 TIE 分数信誉搜索项目。

只有安装了 McAfee Anti-Spam 插件组件后，才能使用“垃圾邮件”、“网络钓鱼”和“IP 信誉”检测类别适用的主要搜索过滤器。

另请参阅

*其他搜索选项*第 38 页

搜索过滤器对比图

提供关于哪一个搜索过滤器适用于所选检测到的项目类别的信息。

MSME 中可用的搜索过滤器取决于选定的检测到的项目类别。 如果您不确定哪一个搜索过滤器适用于特定的检测到的项目类别，使用此表作为参考材料。

快速查找此对比图有助于您了解特定检测类型的可用搜索过滤器。

表 3-2 对比图 — 各检测类型的搜索过滤器

过滤	垃圾邮件	IP 信誉	网络钓鱼	病毒	潜在有害程序	有害内容	禁止的文件类型和消息	DLP 和合规性	邮件 URL 信誉
“采取的操作”	✓	✓	✓	✓	✓	✓	✓	✓	✓
“反垃圾邮件引擎”	✓		✓						
“反垃圾邮件规则”	✓		✓						
“防病毒 DAT”				✓	✓				
“防病毒引擎”				✓	✓				
“禁止的短语”						✓		✓	✓
“检测项名称”				✓	✓				
“文件名”				✓	✓	✓	✓	✓	✓
“文件夹”				✓	✓	✓	✓	✓	✓
“IP 信誉分数”		✓							
“策略名称”	✓		✓	✓	✓	✓	✓	✓	✓
“收件人”	✓		✓	✓	✓	✓	✓	✓	✓
“信誉分数”	✓		✓						
“规则名称”	✓		✓		✓	✓	✓	✓	✓
“扫描方式”	✓		✓	✓	✓	✓	✓	✓	✓
“发件人”	✓		✓	✓	✓	✓	✓	✓	✓
“发件人 IP”	✓	✓	✓						
“服务器”	✓		✓	✓	✓	✓	✓	✓	✓
“垃圾邮件分数”	✓		✓						
“主题”	✓		✓	✓	✓	✓	✓	✓	✓
“票证编号”	✓		✓	✓	✓	✓	✓	✓	✓

搜索过滤器“原因”、“原因”、“状态”和“任务”不适用于该对比图表，仅适用于“检测到的项目” | “所有项目”类别。

另请参阅

*检测类型*第 34 页

其他搜索选项

提供有关其他搜索选项的信息，缩小检测到的项目搜索结果的范围。

表 3-3 选项定义

选项	定义
“和”	根据在前一个和后一个过滤选项中设置的条件搜索项目，其中搜索结果同时满足两个条件。
“或”	根据在前一个和后一个过滤选项中设置的条件搜索项目，其中搜索结果满足两个条件之一。

表 3-3 选项定义 *（续）*

选项	定义
“包含”	搜索包含主要搜索过滤器中的指定文本的项目。例如，如果您要搜索在**发件箱**文件夹中检测到的隔离项目，请选择“文件夹”作为主要搜索过滤器，从下拉列表中选择“包含”，然后在文本框中输入 out 并单击“搜索”，在“查看结果”部分查看搜索结果。
“未包含”	搜索在搜索结果中不包括的指定文本的项目。例如，如果您不希望搜索结果中显示记录项目，请选择“已采取的操作”作为主要搜索过滤器，从下拉列表选择“未包含”，然后输入 log 并单击“搜索”，在“查看结果”部分查看搜索结果。
“完全匹配”	搜索与指定文本完全匹配的项目。例如，如果您要搜索特定的“防病毒引擎”（版本号 5400.1158）检测到的隔离项目，请选择“防病毒引擎”作为主要搜索过滤器，从下拉列表中选择“完全匹配”，然后在文本框中输入 5400.1158 并单击“搜索”，在“查看结果”部分查看搜索结果。
“匹配正则表达式”	使用正则表达式搜索与特定模式匹配的项目。例如，如果您要根据有效电子邮件在检测的任意位置进行搜索，请选择“检测名称”作为主要搜索过滤器，从下拉列表中选择“匹配正则表达式”，然后在文本框中输入 \b[A-Z0-9._%+-]+@(?:[A-Z0-9-]+\.)+[A-Z]{2,4}\b 并单击“搜索”，在“查看结果”部分查看搜索结果。
“等于”	搜索包含的“垃圾邮件分数”、“信誉分数”或“IP 信誉分数”等于指定值的项目。
“小于”	搜索包含的“垃圾邮件分数”、“信誉分数”或“IP 信誉分数”小于指定值的项目。
“大于”	搜索包含的“垃圾邮件分数”、“信誉分数”或“IP 信誉分数”大于指定值的项目。
“区分大小写”	选择搜索条件是否区分大小写。
“所有日期”	选择您是否要搜索所有日期的项目。 搜索结果将根据隔离的项目数据库中存储的日期显示。
“日期范围”	根据需要，搜索指定日期范围内的项目。在此您可以通过参数“开始”和“结束”指定日期、月份、年份和时间。您也可以使用日历图标指定日期范围。 日期范围基于本地系统时间。
“搜索”	单击可查看“查看结果”部分中显示的与搜索条件相匹配的隔离项目列表。
“清除过滤器”	单击可返回默认搜索设置。

另请参阅

*可用的主要搜索过滤器*第 35 页

搜索检测到的项目

使用搜索过滤器可查找您感兴趣的特定隔离项目，并采取相应的操作。

您可以使用搜索过滤器组合，例如：布尔逻辑运算符、正则表达式、区分大小写的文本或日期范围。

任务

1 在产品的用户界面中，单击 “检测到的项目”。

2 在左窗格中单击所需的检测类别，例如 “垃圾邮件”、“网络钓鱼”或 “所有项目”。

3 在 “搜索”窗格中，从下拉列表中选择所需的搜索过滤器（如果需要）。可用的搜索选项包括：

表 3-4 搜索选项

搜索功能	说明
主要搜索过滤器	选择是否要基于特定过滤器（例如 “策略名称”、 “已采取的操作”、 “发件人”等）细化搜索条件。 有关所有主要搜索过滤器的详细信息，请参阅 “可用的主要搜索选项”部分。
布尔逻辑运算符	选择是否使用以下逻辑运算符来细化搜索： • “和” • “或” 有关这些过滤器选项的详细信息，请参阅 “其他搜索选项”部分。
辅助搜索过滤器	选择是否使用以下辅助过滤器来细化搜索： • “包含” • “未包含” • “完全匹配” • “匹配正则表达式” • “等于” • “小于” • “大于” 有关这些过滤器选项的详细信息，请参阅 “其他搜索选项”部分。
“区分大小写”	选择搜索条件是否区分大小写。
“日期范围”	选择是否要将搜索细化到所有日期或特定的时间范围。 • “所有日期” • “日期范围”

4 单击 “搜索”。

完成以上步骤后，您就成功搜索到了符合搜索条件的检测到的项目，这些项目现在显示在 “查看结果”部分中。

您可以对隔离的项目采取的操作

根据您定义的参数查看搜索结果，并对隔离的项目采取必要操作。

然后，您可以针对这些隔离的项目执行各种操作。

表 3-5 操作的类型

操作	定义
“释放”	释放被隔离的项目。 从 “查看结果”窗格选择适用的记录，然后单击 “释放”。 原始电子邮件将从数据库中释放，用于传递给预期收件人。 • 项目下载、释放或转发后，会对其进行病毒扫描并显示在 “信息显示板” | “最近扫描的项目”部分中。 • 成功释放后，项目会在 “检测到的项目” | “所有项目”类别中显示为 “已释放”状态。
“下载”	下载隔离的项目进行研究或分析。 从 “查看结果”窗格中选择适用的记录，然后单击 “下载”。 您无法一次从 “检测到的项目” | “所有项目”类别中 “下载”、 “转发”、 “查看”或 “释放”多个记录。 但是，您可以从特定类别中 “释放”多个记录。

表 3-5 操作的类型 *（续）*

操作	定义
“导出为 CSV 文件”	将搜索返回的所有隔离项目的相关信息导出并保存为 .CSV 格式。 如果数据库中有大量隔离的项目，您可以使用此选项将这些记录下载为 CSV 格式的文件，稍后在 Microsoft Excel 中生成自定义报告，而无需在多个页面中导航。 在“查看结果”窗格中，单击“导出为 CSV 文件”以“打开”或“保存”搜索结果至目标文件夹或位置。 若要指定“查看结果”中显示的隔离项目的数量限制，请在“设置和诊断” | “检测到的项目” | “本地数据库”中修改“最大查询大小（记录）”值。 • 如果您在 CSV 文件的搜索结果中未找到特定字段，请确保启用了“要显示的列”选项中的所需字段。 • 使用 Microsoft Excel 中的“导入数据”选项，打开不同区域的 CSV 文件。
“转发”	根据需要，将隔离的项目转发给所需的收件人。使用分号作为分隔符，将隔离的项目转发给多个收件人。执行此操作将把隔离的项目作为新电子邮件的附件（.eml 格式）发送。 要将隔离的项目转发至您组织内的分发列表 (DL)，请指定 DL 的 SMTP 地址。
“查看”	在独立的窗口中查看隔离的项目。
“添加到阻止的发件人”	将发件人的电子邮件地址添加到阻止发送电子邮件的地址的列表，也称为黑名单。
“添加到允许的发件人”	将发件人的电子邮件地址添加到允许发送电子邮件的地址的列表，也称为白名单。
“要显示的列”	选择要在“查看结果”窗格中列出的其他列标题。此选项具有“搜索”窗格中提供的所有过滤器的列表及其他一些选项。
“全选”	选择“查看结果”部分当前页面中显示的所有被隔离的项目。 例如，如果有 100 个被隔离的项目并且将“每页”查看的项目设为 10，则仅会选择“查看结果”部分中当前出现的 10 个项目。
“全都不选”	取消选择“查看结果”部分中显示的所有被隔离的项目。
“删除”	删除选定类别在“查看结果”部分当前页面中选定的被隔离项目。 长按 **Ctrl** 键以选择多个项目。
“全部删除l”	从数据库中删除所选类别的所有隔离项目。
查看“每页”	指定每页上要查看的隔离项目的最大数量。 选项包括： • “10” • “20” • “50” • “100”

“查看结果”窗格中的每条记录具有一个图像，含义如下：

图标	说明
	项目被隔离，但可以下载、转发、释放或查看。
	项目仅被记录，无法下载、转发、释放或查看。

3

检测到的项目
您可以对隔离的项目采取的操作

4 策略管理器

允许您配置或管理产品中不同的策略和相应的操作。确定当检测到不同类型的威胁后如何处理这些威胁。

策略一般是指引导决策并实现合理结果的原则或规则。在组织内采用策略有助于作出客观的决策。

在 MSME 中，策略指定使用的设置以及在 Exchange 环境中触发检测时采取的操作。您可以创建多个策略以及为特定策略定义特定设置和操作。例如，您可以为“按访问”菜单选项创建多个策略，并为每个策略设定不同的设置和操作。

简而言之，MSME 策略 = 扫描程序设置 + 要采取的操作。

使用“策略管理器”下的“共享资源”菜单选项从一个公共位置为扫描程序、过滤器和警报设置修改或创建规则。使用“共享资源”可节约创建和应用 MSME 策略的时间。

创建策略的步骤

要以管理员身份创建策略，您必须：

1 启用扫描程序或过滤器。

2 通过策略或“共享资源”编辑扫描程序或过滤器设置。

3 指定检测触发时要采取的操作。

4 指定将为其应用该策略的用户。

5 为需要的策略类别应用设置。

目录

处理威胁的策略类别

查看可用的策略类别，并将现有默认策略（称为 主策略）应用到整个组织。

MSME 使用称为策略的特殊规则和设置集帮助减轻电子威胁，您可以根据 Exchange 组织需求创建这些策略。

在 Exchange Server 上首次安装 MSME 时，以下菜单选项都有默认的“主策略”：

- “按访问”
- “按需(默认)”
- “按需(查找病毒)”
- “按需(删除病毒)”
- “按需(查找阻止的内容)”
- “按需(删除阻止的内容)”
- “按需(完全扫描)”
- “网关”

您可以在以下每个类别下自定义策略，从而准确地处理可能影响 Exchange 组织的特定威胁。

策略管理器视图

根据继承或优先级查看子策略并进行排序。

“策略管理器”视图的类型为：

- “继承视图”
- “高级视图”

继承视图

显示主策略和所有子策略的优先顺序和状态。 根据最优先级别子策略配置的设置，MSME 会电子邮件采取操作。 如果未满足子策略的规则，MSME 会继续套用下一顺序的子策略。 如果未满足任一子策略中的规则，则会应用“”主策略中配置的设置。

选择“继承视图”时，子策略将根据策略的继承显示。

在此视图中，您可以：

- 查看策略及其优先级
- 查看继承的子策略及其父策略
- 启用或禁用子策略
- 删除子策略

高级视图

根据优先级按升序显示所有策略，并提供更改子策略优先级的选项。

在此视图中，您可以：

- 查看按优先级排序的策略
- 修改策略的优先级

使用以下图标修改策略的优先级：

- — 提升策略的优先级。
- — 降低策略的优先级。

- 启用或禁用子策略
- 删除子策略
- 通过单击“详细信息”编辑策略名称、说明和父策略。

主策略和子策略

层级结构内部的策略设置一般从父传递到子，然后从子传递到子的下一级，以此类推。这种概念被称为继承。在 MSME 中，默认父策略称为“主策略”，子策略称为“子策略”。

主策略

所有策略类别可用的默认父策略，定义了如何扫描项目中的病毒、如何过滤文件以及各种其他设置。这些主策略可以应用到组织中的所有用户。

您无法删除“父策略”，因为父策略是创建子策略的基准。

子策略

从其他策略继承设置和操作的策略称为子策略。您可以根据需要使用不同的设置和操作创建更多子策略，以应用到特定用户。

如果需要“主策略”的例外情况以适应任何地理区域、功能、邮箱、域或组织中的部门，则需要创建子策略。在 MSME 中，此类其他策略的总称为策略组。

对电子邮件采取的操作基于为具有最高优先级的子策略配置的设置。在不满足具有最高优先级的子策略的规则时，MSME 将使用下一优先级的子策略。只有在子策略中的规则不满足时，才应用主策略中配置的设置。“”

如果选择扫描程序或过滤器设置页中的“从父策略继承所有设置”，继承的策略（子策略）使用的设置与父策略相同。但是，如果进行了检测，您可以采取其他操作。对父策略或“主策略”中设置所作的任何更改也会反映在这些子策略中。

示例：创建子策略，以对被 MSME 识别为威胁的所有电子邮件采取以下操作：

- 隔离 — 针对所有用户
- 记录、隔离并通知管理员 — 针对管理员

该简单示例提供了有关可能需要子策略的情况更多见解。

表 4-1 示例 — 需要子策略的情况

策略类型	扫描程序	保护级别	用户	要采取的操作
主策略	防病毒	中等级别保护	所有用户	“隔离”
子策略	防病毒	高级别保护	管理员	“记录”、“隔离”和“通知管理员”

将 MSME 恢复为默认设置将删除现有子策略。将 MSME 恢复为出厂设置之前，确保使用“设置和诊断” | “导入和导出配置” | “配置”选项卡中的“导出”备份策略和设置。

创建子策略

根据“主策略”或父策略创建其他策略，以满足组织任何部分的特定需求。为“主策略”未涵盖的任何例外情况创建子策略。

此方法在您不希望通过“主策略”为组织中的某些用户或组应用规则时非常有用。您可以创建例外，并允许 MSME 执行特定扫描。

关于何时创建子策略的一些示例：

- 在扫描后允许通过发送给组织中的执行级别用户的入站电子邮件，但对其他用户隔离这些入站电子邮件。
- 允许为特定用户组通过某些文件格式。例如，如需为除组织中特定部门以外的所有用户阻止 .wav 文件。

任务

1 从“策略管理器”中，选择要为其创建子策略的菜单项。

2 单击“创建子策略”。

此时将显示“创建子策略”页。

3 在“初始配置” | “标识” | “子策略名称”下指定标识策略及其用途的名称。

4 （可选）键入策略的“说明”。

5 从继承设置的位置为子策略选择“父策略”。

6 单击“下一步”。

7 在“触发规则” | “规则”下，单击“新规则”。

8 在“指定策略规则”中，您可以选择：

- “<选择规则模板>” — 基于发件人或收件人指定策略规则。您可以根据以下选项创建新规则：
  - “发件人的 SMTP 地址是电子邮件地址”
  - “发件人的 SMTP 地址不是电子邮件地址”
  - “任何收件人的 SMTP 地址都是电子邮件地址”
  - “任何收件人的 SMTP 地址都不是电子邮件地址”
  - “发件人在 Active Directory 组中”
  - “发件人不在 Active Directory 组中”
  - “任何收件人在 Active Directory 组中。”
  - “任何收件人不在 Active Directory 组中。”

  确保创建规则时不使用冲突的电子邮件地址或用户名。不支持通过正则表达式指定用户，仅支持通配符。

- “从其他策略复制规则” — 从其他的策略复制规则。

9 单击“添加”。

10 指定为用户触发策略的条件。您可以选择以下选项：

- “任何规则适用”
- “所有规则适用”
- “任何规则都不适用”

11 单击“下一步”。

12 在“扫描程序和过滤器”中，您可以选择以下选项：

- “从父策略继承所有设置” — 继承父策略的所有属性。
- “使用从其他策略复制的值初始化所选设置” — 从可用策略中选择特定扫描程序和过滤器。

13 单击“完成”。

核心扫描程序和过滤器

确定创建策略时可以应用的扫描程序和过滤器的类型。

核心扫描程序

在“策略管理器” | “共享资源” 中查看和配置以下扫描程序的设置。

扫描程序	定义
“防病毒扫描程序”	配置相关设置以检测病毒、特洛伊木马程序、蠕虫、打包程序、间谍软件、广告软件和其他威胁。
“DLP 和合规性扫描程序”	通过 60 种新的 “DLP 和合规性字典”创建或配置 “DLP 和合规性规则”以满足 Exchange 组织的机密和合规性策略。
“文件过滤”	创建新的文件过滤规则以满足 Exchange 组织需求。 根据文件名、文件类别或文件大小配置这些设置。
“邮件 URL 信誉”	配置相关设置以检测包含有害链接、网络钓鱼链接和恶意软件的 URL。
“反垃圾邮件”	配置相关设置以根据垃圾邮件分数、大小、规则和邮件列表检测被分类为垃圾邮件的电子邮件。
“反网络钓鱼”	为被分类为网络钓鱼邮件的电子邮件配置报告设置。

只有安装了 McAfee Anti-Spam 插件后，才能使用“反垃圾邮件”和“反网络钓鱼”选项。

过滤器

启用或禁用这些过滤器，根据 Exchange 组织的需求指定检测发生时采取的操作。

您可以启用或禁用部分过滤器，但无法配置自定义设置。 这些过滤器不会显示在 “共享资源” | “扫描程序和警报” | “扫描程序” | “类别”下拉列表中。

过滤器	定义
“遭破坏内容”	配置相关设置以对被检测为遭破坏的内容的电子邮件采取操作。
“受保护内容”	配置相关设置以对被检测为受保护的内容的电子邮件采取操作。
“加密内容”	配置相关设置以对被检测为加密的内容的电子邮件采取操作。
“经过签名的内容”	配置相关设置以对被检测为签名的内容的电子邮件采取操作。
“受密码保护文件”	配置相关设置以对包含受密码保护的文件的电子邮件采取操作。 您可以改写文件过滤策略，允许通过需要包含受密码保护文件附件的电子邮件。 有关更多信息，请参见“配置受密码保护文件设置”。
“邮件大小过滤”	创建或配置相关设置以对超过邮件大小过滤选项的电子邮件采取操作。 配置相关设置以根据邮件总大小、附件大小和附件数量隔离电子邮件。
“扫描程序控件”	创建或配置核心扫描程序设置，以根据嵌套级别、展开文件大小和扫描时间对电子邮件采取操作。
“MIME 邮件设置”	创建或配置相关设置以检测被分类为 MIME 邮件的威胁。
“HTML 文件”	创建或配置相关设置，以对包含备注、URL、元数据和脚本等 HTML 元素的电子邮件采取操作。

杂项

配置其他设置，如在检测发生时发送给最终用户的警报和免责声明。

其他	定义
“警报设置”	创建或配置存在检测项时的电子邮件警报设置。 配置警报电子邮件格式（HTML 或文本）、编码、文件名、页眉和页脚等设置。
“免责声明文本”	创建或配置在检测发生时必须显示在发送至最终用户的电子邮件中的免责声明文本。

扫描程序和过滤器对比图

提供关于在默认情况下每个策略类别的哪个搜索扫描程序或过滤器可用的信息。

MSME 中可用的扫描程序或过滤器可能不同，具体取决于选择的策略类别。

如果您不确定哪一个扫描程序或过滤器适用于特定的策略类别，则使用此对比图作为参考材料。快速查找此对比图有助于您了解每个策略类别的可用扫描程序和过滤器，其首字母缩写为：

- OA — “按访问”
- OD (D) — “按需（默认）”
- OD (FV) — “按需（查找病毒）”
- OD (RV) — “按需（删除病毒）”
- OD (FC) — “按需（查找不合规的内容）”
- OD (RC) — “按需（删除不合规的内容）”
- OD (FS) — “按需（完全扫描）”
- GW — “网关”

核心扫描程序

核心扫描程序	OA	OD (D)	OD (FV)	OD (RV)	OD (FC)	OD (RC)	OD (FS)	GW
“防病毒扫描程序”	✓	✓	✓	✓			✓	
“DLP 和合规性扫描程序”	✓	✓			✓	✓	✓	
“文件过滤”	✓	✓					✓	
“邮件 URL 信誉”	✓	✓					✓	
“反垃圾组件”								✓
“反网络钓鱼”								✓

尽管 “DLP 和合规性扫描程序”可用于“按访问”和“按需（默认）”策略类别，但在默认状态下为停用或禁用。 您必须创建需要的规则，然后指定规则触发时采取的操作并启用扫描程序。

过滤器

过滤器	OA	OD (D)	OD (FV)	OD (RV)	OD (FC)	OD (RC)	OD (FS)	GW
“遭破坏内容”	✓	✓					✓	
“受保护内容”	✓	✓			✓	✓	✓	
“加密内容”	✓	✓			✓	✓	✓	
“经过签名的内容”	✓	✓			✓	✓	✓	

过滤器	OA	OD (D)	OD (FV)	OD (RV)	OD (FC)	OD (RC)	OD (FS)	GW
“受密码保护文件”	✓	✓			✓	✓	✓	
“邮件大小过滤”	✓							✓
“扫描程序控件”	✓	✓	✓	✓	✓	✓	✓	✓
“MIME 邮件设置”	✓	✓			✓		✓	✓
“HTML 文件”	✓	✓			✓		✓	✓

警报和免责声明设置

其他设置	OA	OD (D)	OD (FV)	OD (RV)	OD (FC)	OD (RC)	OD (FS)	GW
“警报设置”	✓	✓		✓	✓	✓	✓	✓
“免责声明文本”	✓							

列出选定策略的所有扫描程序和过滤器

查看选定策略类别的可用扫描程序和过滤器的状态。
可用的设置类型取决于所选的策略。

任务

1 在产品的用户界面中，单击“策略管理器”和策略类别菜单项。

此时将显示选定菜单项的策略页。

2 单击“主策略”或所需的子策略。

此时会出现相应的策略页面。 适用的过滤器在各自的策略页面中提供。

3 在策略页面中，您可以使用以下选项卡：

- “列出所有扫描程序” — 查看策略启用了哪个扫描程序或过滤器。
- “查看设置” — 查看扫描程序或过滤器的设置以及指定的操作。
- “指定用户” — 指定应用于特定用户的策略规则。

您可以将用户仅指定到子策略。

4 在“列出所有扫描程序”选项卡中，可以使用以下项：

表 4-2 策略配置

选项	定义
“策略”	选择要配置的策略。
“添加扫描程序/过滤器”	配置策略使其仅适用于特定时间。例如，您可以使用不同的规则创建仅在周末适用的新防病毒设置。
“核心扫描程序”	为以下每个扫描程序配置策略： • “防病毒扫描程序” • “DLP 和合规性扫描程序” • “文件过滤” • “邮件 URL 信誉” • “反垃圾邮件” • “反网络钓鱼”
“过滤器”	为以下每个过滤器配置策略： • “遭破坏内容” • “受保护内容” • “加密内容” • “经过签名的内容” • “受密码保护的文件” • “邮件大小过滤” • “扫描程序控件” • “MIME 邮件设置” • “HTML 文件”
“其他设置”	配置策略的警报设置和免责声明消息。 “其他”选项包括： • “警报设置” • “免责声明文本”

添加扫描程序或过滤器

添加扫描程序或过滤器以创建 Exchange 组织中例外场景的设置。

在您需要此类其他扫描程序或过滤器时，添加扫描程序或过滤器非常有帮助：

- 具有不同的选项和规则
- 仅在特定时隙内启用

任务

1 在“策略管理器”中，选择策略类别。

2 单击“主策略”或任何子策略。

3 在“列出所有扫描程序”选项卡中，单击“添加扫描程序/过滤器”。

仅“按访问”和“网关”策略类别提供“添加扫描程序/过滤器”选项。

4 从“指定类别”下拉列表中，选择所需的扫描程序或过滤器。

5 从“使用此实例的时间”部分中，选择现有的时隙或创建新时隙。

6 单击“保存”。

7 单击“应用”。

编辑选项和规则，使之符合您组织的需求。

为特定用户创建新规则

创建新规则并指定为特定用户应用该规则的条件。

您可以为特定用户或组在策略中创建例外规则。

任务

1 在“策略管理器”中，选择策略类别。

2 单击您要为特定用户配置的子策略。

3 单击“指定用户”选项卡。

4 单击“新建规则”。

5 从“指定策略规则”中，您可以选择以下项：

- “<选择规则模板>” — 基于发件人或收件人指定策略规则。您可以根据以下选项创建新规则：
  - “发件人的 SMTP 地址是电子邮件地址”
  - “发件人的 SMTP 地址不是电子邮件地址”
  - “任何收件人的 SMTP 地址都是电子邮件地址”
  - “任何收件人的 SMTP 地址都不是电子邮件地址”
  - “发件人在 Active Directory 组中”
  - “发件人不在 Active Directory 组中”
  - “任何收件人在 Active Directory 组中。”
  - “任何收件人不在 Active Directory 组中。”

  确保创建规则时不使用冲突的电子邮件地址或用户名。不支持通过正则表达式指定用户，仅支持通配符。

- “从其他策略复制规则” — 从其他的策略复制规则。

6 单击“添加”。

7 指定应为用户触发策略时的条件。 您可以选择以下选项：

- “任何规则适用”
- “所有规则适用”
- “任何规则都不适用”

8 单击“应用”将规则保存到特定用户。

对检测可采取的操作

对于策略中每一个扫描程序和过滤器的设置，您都可以指定对检测采取的主要操作和辅助操作。您可以指定在电子邮件触发检测时要对该电子邮件及其附件采取的操作。

在根据扫描程序或过滤器设置触发策略规则时，MSME 将按照配置的主要操作和辅助操作对检测进行处理。

配置操作时，必须选择至少一个主要操作。还可以选择多个辅助操作。例如，如果主要操作是删除触发检测的电子邮件，则辅助操作可能是记录检测并通知管理员。

可用的主要操作取决于策略类别类型和配置的扫描程序或过滤器设置。

单击“重置”，将操作还原为策略类别和扫描程序的默认设置。

表 4-3 主要操作

操作	定义
“尝试清除任何检测到的病毒或特洛伊木马程序”	清理“防病毒扫描程序”检测到的含有病毒或特洛依木马程序的电子邮件。
“使用警报替换项目”	使用警报替换触发检测的电子邮件。
“删除内嵌项目”	删除触发检测的电子邮件的附件。
“删除消息”	删除触发检测的电子邮件。
“允许通过”	允许电子邮件继续进入下一个扫描阶段或抵达最终用户。
“基于分数的操作”	根据垃圾邮件分数采取操作。仅反垃圾邮件扫描程序可使用此选项，您必须在此选择“如果垃圾邮件分数为”“高”、“中”还是“低”。
“路由至系统垃圾文件夹”	将“反垃圾邮件”扫描程序检测到的电子邮件路由至“设置和诊断”	“反垃圾邮件”	“网关垃圾邮件过滤器”	“系统垃圾文件夹地址”下指定的电子邮件地址。
“路由至用户垃圾文件夹”	将“反垃圾邮件”扫描程序检测到的电子邮件路由至收件人的“垃圾电子邮件”文件夹。
“拒绝该消息”	拒绝电子邮件并发送通知给用户。
“使用警报替换附件”	如果因超出附件大小而触发了“邮件大小过滤”扫描程序，则使用警报替换电子邮件内的附件。
“使用单个警报替换所有附件”	如果因超出附件数量而触发了“邮件大小过滤”扫描程序，则使用单个警报替换含有多个附件的电子邮件。
“不允许进行会破坏签名的更改”	检测到包含“签名的内容”的电子邮件时，阻止 MSME 破坏签名。
“允许进行会破坏签名的更改”	检测到包含“签名的内容”的电子邮件时，允许 MSME 破坏签名。

表 4-4 辅助操作

操作	定义
“记录”	在日志中记录检测。
“隔离”	在隔离数据库中存储触发检测的电子邮件的副本。要查看所有隔离项目，请转至“检测到的项目”	“所有项目”或特定检测类别。 根据检测类别，选择“转发隔离电子邮件”将电子邮件发送至特定审阅者或分发列表。要配置基于检测类别的通知，请转至“设置和诊断”	“通知”	“设置”	“高级”。 “转发隔离电子邮件”选项不适用于“防病毒扫描程序”或“网关”策略。
“通知管理员”	将电子邮件副本发送至在“设置和诊断”	“通知”	“设置”	“常规”下“管理员电子邮件”中指定的管理员。
“通知内部发件人”	如果原始电子邮件来自 Exchange Server 的权威域内，则向内部发件人发送警报邮件。
“通知外部发件人”	如果原始电子邮件不是来自 Exchange Server 的权威域内，则向发件人发送警报邮件。
“通知内部收件人”	如果收件人在 Exchange Server 的权威域内，则向收件人发送警报邮件。
“通知外部收件人”	如果收件人不在 Exchange Server 的权威域内，则向收件人发送警报邮件。

共享资源

为扫描程序、过滤器、警报、DLP 和合规性字典以及时隙编辑设置的一个公共位置。设置策略时，您可能需要将相同的资源（扫描程序和过滤器设置）应用到多个策略。在此类情况下，使用“共享资源”。

例如，如果您要对内部收件人和外部收件人使用不同的免责声明，请创建不同的收件人免责声明，然后应用到需要的子策略中。

在产品的用户界面中，单击“策略管理器” | “共享资源”。您可以使用以下选项卡：

- “扫描程序和警报” — 编辑或创建新扫描程序和过滤器设置。
- “DLP 和合规性字典” — 编辑或创建新的“DLP 和合规性规则”以及“文件过滤规则”。
- “时隙” — 编辑或创建新的时隙，如工作日或周末。

对这些设置所作的任何更改将自动应用到使用这些配置的所有策略。

配置扫描程序设置

创建或修改扫描程序设置，使之符合 Exchange 组织的要求。

任务

1 在产品的用户界面中，单击“策略管理器” | “共享资源”。

此时将显示“共享资源”页。

2 单击“扫描程序和警报”选项卡。

3 从“类别”下拉列表的“扫描程序”部分下，选择您要配置的扫描程序。将显示扫描程序类型，以及设置名称、策略使用者和要配置的操作。您可以使用以下选项：

表 4-5 选项定义

选项	定义
“类别”	选择要配置的需要的扫描程序。
“新建”	根据要求，为扫描程序创建新设置。适用于需要设置某些扫描程序例外设置并将其应用于策略的情况。
“编辑”	为选定的扫描程序编辑设置。
“删除”	删除扫描程序设置。 在以下情况下无法删除扫描程序： • 扫描程序为默认扫描程序。 • 扫描程序被任何策略使用。如需了解哪些策略使用该扫描程序设置的信息，请参见“使用者”列。

4 配置扫描程序设置后，单击“保存”，然后单击“应用”。

您现已根据 Exchange 组织的要求成功配置扫描程序的设置。

配置警报设置

为选定扫描程序创建或修改警报设置，使之符合 Exchange 组织的要求。

任务

1 在产品的用户界面中，单击“策略管理器” | “共享资源”。

此时将显示“共享资源”页。

2 单击“扫描程序和警报”选项卡。

3 从“类别”下拉列表的“警报”部分下，选择您要为扫描程序配置的警报。将显示扫描程序类型，以及设置名称、策略使用者和要配置的操作。您可以使用以下选项：

表 4-6 选项定义

选项	定义
“类别”	选择要配置的需要的扫描程序。
“新建”	根据要求，为扫描程序创建新设置。适用于需要设置某些扫描程序例外设置并将其应用于策略的情况。
“查看”	查看扫描程序的默认警报设置。
“编辑”	为选定的扫描程序编辑设置。有关您可以在警报中使用的变量的更多信息，请参阅“可以使用的通知字段”部分。
“删除”	删除扫描程序设置。 在以下情况下无法删除警报： • 警报为默认扫描程序警报。 • 警报被任何策略使用。如需了解哪些策略使用该警报设置的信息，请参见“使用者”列。

4 配置扫描程序设置后，单击“保存”，然后单击“应用”。

您现已根据 Exchange 组织的要求成功配置警报的设置。

创建警报

创建扫描程序或过滤器所采取操作的警报消息。

任务

1 在产品用户界面中，单击“策略管理器” | “共享资源”。

此时会出现“共享资源”页面。

2 单击“扫描程序和警报”选项卡。

3 从“类别”下拉列表的“警报”部分下，选择您要为扫描程序配置的警报。

4 单击“新建”。

此时将显示“警报编辑器”页。

5 键入有意义的“警报名称”。

6 从相应的下拉列表中选择所需的“样式”、“字体”、“大小”和“令牌”。

只有从“显示”下拉菜单中选择“HTML 内容 (WYSIWYG)”时，这些选项才可用。

7 使用以下任何工具自定义警报：

表 4-7 工具栏选项

选项	说明
加粗	将所选文本设置为粗体。
倾斜	将所选文本设置为斜体。
下划线	为所选文本加下划线。
左对齐	将所选段落设置为左对齐。
居中	将所选段落设置为居中。
右对齐	将所选段落设置为右对齐。
两端对齐	调整所选的段落，使段落中的行以直左右边界填充指定宽度。
经过排序的列表	将所选文本设置为带编号的列表。
未经排序的列表	将所选文本设置为带项目符号的列表。
减少缩进	将所选文本向左移动预先设定好的距离。
缩进	将所选文本向右移动预先设定好的距离。
文本颜色	更改所选文本的颜色。
背景颜色	更改所选文本的背景颜色。
水平标尺	插入水平线。
插入链接	在光标当前位置插入超链接。在 “URL” 中，键入 “URL”。在 “文本” 中，键入希望在警报邮件中显示的超链接的名称。如果希望链接打开新窗口，请选择 “在新窗口中打开链接”，然后单击 “插入链接”。
插入图像	在光标当前位置插入图像。在 “图像 URL” 中，键入图像的位置。在 “代替文本” 中，键入当图像被抑制或在纯文本浏览器中显示警报邮件时用于代替图像的文本。如果要为图像指定标题，请在 “使用此文本作为图像标题” 中键入标题名称。单击 “插入图像”。
插入表格	在当前光标位置插入表格。在 “行”、“列”、“表格宽度”、“边框粗细”、“单元格边距” 和 “单元格间距” 中键入值以配置表格，然后单击 “插入表格”。

8 在 “显示” 下拉菜单中，指定警报消息在用户界面中的显示方式。 您可以选择以下选项：

- “HTML 内容(WYSIWYG)” - 隐藏基础 HTML 代码，仅显示警报邮件的内容。
- “HTML 内容(源代码)” - 以编译前的 HTML 代码显示警报邮件。
- “纯文本内容” — 将内容显示为纯文本。

您可以使用以下通知字段将这些内容包含在警报消息中。 例如，在警报消息中，如果想要获得检测到的项目名称和采取的相应操作，请在 “警报编辑器” 页面中使用 **%vrs%** 和 **%act%**。 有关通知字段选项的更多信息，请参见 “可以使用的通知字段” 部分。

McAfee 建议您以纯文本格式保存日志文件，这样所有电子邮件客户端都可查看该内容。

9 单击 “保存” 返回策略页。

单击 “重置” 撤消自上一次保存警报邮件后做出的所有更改。

配置 DLP 和合规性规则

创建或修改 DLP 和合规性规则及字典，使之符合您 Exchange 组织的要求。

任务

1 在产品用户界面中，单击“策略管理器” | “共享资源”。

此时会出现“共享资源”页面。

2 单击“DLP 和合规性字典”选项卡。

3 在 “DLP 和合规性规则”部分的“选择语言”下拉列表中，选择语言。

您还可以查看和编辑所有支持的区域设置字典。（支持的区域设置为简体中文、法语、德语、日语和西班牙语。）

4 在 “DLP 和合规性规则”部分的“类别”下拉列表中，选择要查看或配置的类别。 显示的规则组包含名称、策略使用方和配置的操作。 您可以使用：

表 4-8 选项定义

选项	定义
“类别”	选择要配置的扫描程序。 该版本拥有 60 多个 DLP 和合规性字典，可确保电子邮件内容符合您组织的机密性和合规性策略。 预定义的合规性字典包括： • 新添加的 60 部新 DLP 和合规性字典。 • 支持行业特定的合规性字典 — HIPAA、PCI、源代码（Java、C++ 等） 这些字典分类为： • 基于分数 — 在电子邮件超出阈值分数和最大词数时触发规则，从而减少误报。 • 不基于分数 — 在电子邮件中发现字词时触发规则。
“新建类别”	创建新的 “DLP 和合规性规则”字典。 创建的任何新类别或条件都没有分数。
“新建”	根据需求，创建选定类别的新规则组。 适用于需要特定规则触发检测并将其应用于策略的情况。
“编辑”	编辑选定 “DLP 和合规性”规则的设置。
“删除”	删除 “DLP 和合规性”规则。 您无法删除 “DLP 和合规性”规则，如果 • 规则已启用。取消选择规则， “应用”设置，然后单击“删除”。 • 规则被任何策略使用。如需了解哪些策略使用该扫描程序设置的信息，请参见“使用者”列。

例如，在“类别”下拉列表中选择“信用卡号码”或任何符合需求的字典，并查看可用的增强型“规则组”选项。

5 要创建新规则组，请对选定类别的“DLP 和合规性规则”单击“新建”。

将会出现选定类别的“新 DLP 和合规性扫描程序规则”。

6 键入规则的“规则名称”和“说明”。

7 选择“将此规则添加到此类别的规则组”将新规则添加到所选类别的规则组。

8 在“词语或短语”的“在发现以下词语或短语时将触发规则”中，指定要查找的词语或短语。 然后选择以下选项之一：

- “正则表达式” — 如果启用，则特定文本（正则表达式，regex）会触发规则。 正则表达式可以准确、简练地匹配文本字符串，例如词语、字符或字符模式。

  例如，字符序列“tree”连续出现在任何上下文中，比如 trees、street 或 backstreet。

  - 对于一些短语，正则表达式被禁用。
  - 更多详细信息，请参见 http://www.regular-expressions.info/reference.html or http://www.zytrax.com/tech/web/regex.htm。

- “使用通配符” — 如果启用，为包含通配符的指定字词触发规则。（当不知道实际字符或者不愿键入整个名称时，通常使用通配符代替一个或多个字符。）
- “开始字符” — 如果启用，为构成字词的开头的指定文本触发规则。
- “结束字符” — 如果启用，为构成字词的最后部分的指定文本触发规则。
- “区分大小写” — 如果启用，当指定的文本的大小写与字词匹配时触发规则。

  若要检测完全匹配的词语或短语，请同时选择“开始于”和“结束于”选项。

9 选择“指定其他上下文字词”，作为检测到主要字词时的辅助操作。指定可能与触发检测的主要字词伴随的任何其他字词。

10 从下拉菜单中，选择“如果存在所有短语则触发”、“如果存在任意短语则触发”或“如果不存在任何短语则触发”。

11 选择“在字符块中”指定要扫描的块中的“字符”数。

12 单击“添加上下文字词”键入其他词语或短语。

13 在“指定字词”中指定字词，选择一个条件（与步骤 7 中的选项相同），然后单击“添加”。

14 在“文件格式”下，选择“全部内容”启用所有文件类别及其子类别。您可以选择多个类别以及所选类别中要匹配的文件类型。在子类别选择器中选择“全部”将覆盖可能已做出的任何其他选择。

15 如果没有选择“全部”，则单击“清除选择”将取消选中任何所选的文件类型选项。

16 单击“保存”返回“共享资源”页面。

17 单击“应用”保存设置。

您现已成功配置符合您 Exchange 组织要求的 DLP 和合规性规则及字典。

配置文件过滤规则

创建新规则，以根据文件名、类型或大小检测文件。

开始之前

文件过滤规则仅在选择一个条件时触发。确保为以下每个类别创建单独的规则：

- 文件名
- 文件类别
- 文件大小

该任务提供了有关配置所有三种类别的信息。 根据 Exchange 组织的要求，仅为文件过滤规则选择一种类别，并为每种类别创建单独的规则。 如果某条规则包含多个标准，例如“文件名称过滤”、“文件类别过滤”和“文件大小过滤”，必须满足所有标准才能触发规则。

任务

1 在产品用户界面中，单击“策略管理器” | “共享资源”。

2 单击“DLP 和合规性字典”选项卡。

3 在“文件过滤规则”中，单击“新建”。

4 键入唯一的“规则名称”。为规则指定有意义的名称，这样可以轻松识别规则及其作用。例如，FilesOver5MB 或 Block MPP 文件。

5 启用“评估存档文件中的项目”。

如果文件过滤器规则适用于扫描存档文件，请选择此选项。 通过选择此规则，在存档文件上应用后续的文件过滤器规则。

6 在“文件过滤规则”页面中，可以使用以下项：

表 4-9 选项定义 — 文件名过滤

选项	定义
“启用文件名过滤”	根据文件名启用文件过滤。
“文件名匹配时采取操作”	指定触发该规则的文件名。 您可以使用通配符字符（* 或 ?）以匹配多个文件 名。 例如，如果想要过滤任意 Microsoft PowerPoint 文件，则输入 *.ppt。
“添加”	将“文件名匹配时采取操作”下指定的文件名，添加到文件名过滤列表。
“编辑”	编辑或修改现有文件过滤规则。
“删除”	删除过滤器列表中的文件名。 如果某条文件过滤规则被任意策略使用，则无法删除该规则。 对于要删除的规则，“使用方”栏必须显示为“0 策略”。 您必须先从策略删除文件过滤规则，然后再单击“删除”。

表 4-10 选项定义 — 文件类别过滤

选项	定义
“启用文件类别过滤”	启用根据文件类型进行文件过滤。
“根据文件类别采取操作”	指定影响该规则的文件类型。 文件类型分为类别和子类别。
“文件类别”	选择文件类型类别。 文件类型旁边显示星号 (*)，表示将过滤所选的文件类型。

表 4-10 选项定义 — 文件类别过滤 *（续）*

选项	定义
“子类别”	选择要过滤的子类别。 若要选择多个子类别，请使用“Ctrl”+“单击”或“Shift”+“单击”。 若要选择所有子类别，请单击“全部”。 单击“清除选择”撤消上一次选择。
“将此规则扩展到未识别的文件类别”	将该规则应用到类别和子类别列表中未提及的任何其他文件类别和子类别。

要允许通过包含受限制文件的受密码保护 .zip 文件，请确保“受密码保护的绕过规则”作为第一个规则显示在列表中。

表 4-11 选项定义 — 文件大小过滤

选项	定义
“启用文件大小过滤”	根据文件的大小过滤文件。
“根据文件大小采取操作”	在相邻文本框和下拉列表中指定一个值，然后选择： • “大于” — 指定只有当文件大于指定的大小时才应用操作。 • “小于” — 指定只有当文件小于指定的大小时才应用操作。

7 单击“保存”返回“共享资源”页。

8 单击“应用”创建文件过滤规则。

您现已成功创建满足您 Exchange 组织要求的文件过滤规则。

配置时隙

根据 Exchange 组织的要求，设置不同的时隙或配置可应用于策略的现有时隙。

通过“时隙”，您可以指定触发特定规则的时间。例如，您可能希望在办公时间限制大文件上载或下载。

由于用户及其地理位置或工作时间的不同，您可能会遇到需要更多时隙的情况。您可以根据工作时间、非业务时间、每周维护等创建更多时隙。

默认情况下，MSME 具有以下时隙：

- “所有时间”
- “工作日”
- “周末”

您无法删除或编辑默认时隙“所有时间”，因为“主策略”使用默认时隙。

任务

1 在产品的用户界面中，单击“策略管理器” | “共享资源”。

此时将显示“共享资源”页。

2 单击“时隙”选项卡。

3 单击“新建”。

此时将显示“时隙”页。

4 键入唯一的“时隙名称”，如工作时间或系统维护（每周）。

5 在“选择日期和时间”下，选择所需的日期。

6 选择“全天”或“选定的小时”。

7 如果选择“选定的小时”，请从下拉列表中指定“开始”和“结束”时间。

8 单击“保存”返回“共享资源”页。

9 单击“应用”保存设置。

您现已成功配置或创建满足您 Exchange 组织要求的时隙。

管理策略的核心扫描程序设置

创建或编辑扫描程序选项，然后指定策略触发时对检测到的项目采取的适当操作。

可用的核心扫描程序为：

- “防病毒扫描程序”
- “DLP 和合规性扫描程序”
- “文件过滤”
- “反垃圾邮件”
- “反网络钓鱼”

任务

- *配置防病毒扫描程序设置*第 60 页
  配置策略中的“防病毒扫描程序”设置，以识别、阻止、消除计算机病毒和其他恶意软件。
- *配置 DLP 和合规性扫描程序设置*第 63 页
  配置策略中的“DLP 和合规性扫描程序”设置，以识别电子邮件或附件中不合规的文本数据并采取必要的操作。
- *配置文件过滤设置*第 64 页
  配置策略中的设置，以根据文件名、类型或大小检测文件，并采取必要的操作。
- *配置邮件 URL 信誉设置*第 65 页
  配置“邮件 URL 信誉”设置以检测电子邮件正文中的恶意 URL。
- *针对电子邮件附件的 TIE 信誉检查*第 67 页
  MSME 现在利用 TIE 信誉检查对在网关、集线器和邮箱级别通过电子邮件发送的附件进行检查，从而提供其他威胁检测功能。
- *将 TIE 设置配置为扫描电子邮件附件*第 69 页
  根据文件信誉类别启用针对电子邮件附件的 TIE 信誉检查。
- *配置反垃圾邮件设置*第 70 页
  配置策略中的设置以检测垃圾电子邮件并采取必要的操作。
- *配置反网络钓鱼设置*第 73 页
  配置策略中的设置以使用反垃圾邮件规则和引擎阻止网络钓鱼邮件，并采取必要的操作。

配置防病毒扫描程序设置

配置策略中的“防病毒扫描程序”设置，以识别、阻止、消除计算机病毒和其他恶意软件。

任务

1 从“策略管理器”中，选择具有防病毒扫描程序的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“防病毒扫描程序”。

4 在“激活”中，选择“启用”以激活选定子菜单项目的防病毒扫描程序设置。

- 如果要配置子策略的设置，请选择“使用父策略中的配置”继承父策略的设置。
- 如果将新扫描程序添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用扫描程序的时隙。

5 在“选项”部分中，可以使用以下选项：

选项	定义
“高保护”	扫描所有文件、存档文件、未知病毒、未知宏病毒、群发邮件、潜在有害程序，并扫描所有文件以查找宏病毒。
“中等保护”	扫描所有文件、存档文件、未知病毒、未知宏病毒、群发邮件和潜在有害程序。
“低保护”	仅扫描默认的文件类型、存档文件、群发邮件和潜在有害程序。
“<create new set of options>”	创建自定义的防病毒扫描程序设置。
“编辑”	编辑现有保护级别。

6 如果选择编辑或修改扫描程序设置，则在“实例名称”中，为防病毒扫描程序设置实例输入唯一的名称。此字段是必填的。

7 在“指定要扫描的文件”的“基本选项”选项卡中，选择以下任一选项：

- “扫描所有文件” — 指定要扫描的所有文件，不考虑其类型。
- “默认文件类型” - 指定仅扫描默认文件类型。
- “定义的文件类型” — 指定要扫描哪些文件类型。

8 选择“扫描程序选项”中更多可用的扫描程序选项。 您可以选择以下选项：

- “扫描存档文件(ZIP、ARJ、RAR...)”
- “查找未知的文件病毒”
- “查找未知的宏病毒”
- “启用 McAfee Global Threat Intelligence 文件信誉” — 此选项可以启用由 McAfee Labs 收集的威胁情报，在特征码更新可用之前防止破坏和数据窃取。从可用的选项中选择“敏感度级别”。
- “扫描所有文件中的宏”
- “查找所有宏并视为已感染病毒”
- “从文档文件中删除所有宏”

“查找所有宏并将其视为受感染处理”和“从文档文件中删除所有宏”选项都具有合并的功能。 选择“查找所有宏并将其视为受感染处理”时，会自动选择“从文档文件中删除所有宏”选项。 启用此选项后，附件中的所有宏都将视为受感染处理。

9 在“自定义恶意软件类别”的“高级”选项卡中，指定被视为恶意软件的项目。 有以下两种方式选择恶意软件类型：

- 从复选框的列表中选择恶意软件类型。
- 选择“特定检测项名称”，键入恶意软件类别，然后单击“添加”。

当键入恶意软件类别名称时，您可以使用通配符进行模式匹配。

10 如果已清理的项目不得受自定义恶意软件检查的约束，请选中“如果对象已清理，则不执行自定义恶意软件检查”选项。

11 在“清理选项”中，指定当文件在清理后大小降至 0 字节时要执行的操作。 选择以下任一选项：

- “保留零字节文件” - 保留清理后为零字节的文件。
- “删除零字节文件” - 删除清理后为零字节的任何文件。
- “视为清理失败” — 将零字节文件视为无法清理，并应用清理失败操作。

12 在“打包程序”选项卡中，选择：

- “启用检测项” - 启用或禁用检测打包程序。
- “排除指定名称” — 指定哪些打包程序可以从扫描中排除。
- “仅包含指定的名称” - 指定希望软件检测哪些打包程序。
- “添加” - 将打包程序名称添加到列表。您可以使用通配符来找到匹配的名称。
- “删除” — 删除已添加的打包程序名称。如果单击“添加”，则激活此链接。

13 在“PUPs”选项卡中，选择以下选项：

- “启用检测项” — 启用或禁用对可能不需要的程序的检测。配置可能不需要的程序检测前，请单击免责声明链接并阅读免责声明。
- “选择要检测的程序类型” — 指定要检测还是忽略列表中每种类型的可能不需要的程序。
- “排除指定名称” — 指定可以将哪些可能不需要的程序从扫描中排除。例如，如果已启用间谍软件检测，则可以创建希望软件忽略的间谍软件程序的列表。
- “仅包含指定的名称” — 指定希望软件检测哪些可能不需要的程序。例如，如果启用间谍软件检测并指定仅检测指定的间谍软件程序，则会忽略所有其他间谍软件程序。
- “添加” — 将可能不需要的程序名称添加到列表。您可以使用通配符来匹配名称。
- “删除” — 删除已添加的可能不需要的程序名称。如果单击“添加”，则激活此链接。

McAfee Threat Intelligence 网站包含近期恶意软件名称的列表。使用“Search the Threat Library（搜索威胁库）”查看有关具体恶意软件的信息。

14 单击“保存”返回策略页。

15 在“要执行的操作”中，单击“编辑”。 在以下这些选项卡中，指定如果检测到病毒（或类似病毒的行为）必须执行的防病毒扫描程序操作：

- “清理” — 选择“尝试清理检测到的任何病毒或特洛伊木马程序”以激活多种操作。 从以下选项中选择要采取的操作：
  - “记录”
  - “隔离”
  - “通知管理员”
  - “通知内部发件人”
  - “通知外部发件人”
  - “通知内部收件人”
  - “通知外部收件人”
- “默认操作” — 在 “采取以下操作”下拉列表中，选择一个操作。
  - “将项目替换为警报”
  - “删除内嵌项目”

- “删除消息”
- “允许通过”

有关主要操作和辅助操作的更多信息，请参见“检测时可以采取的操作”部分。

16 选择对应警报文档或单击“创建”以建立新的警报文档。 在“以及”中，选择针对以下选项卡要执行的更多操作：
- “自定义恶意软件”
- “打包程序”
- “潜在有害程序(PUP)”

17 单击“保存”应用设置并返回策略设置页。

18 单击“应用”以将这些设置配置到策略。

配置 DLP 和合规性扫描程序设置

配置策略中的“DLP 和合规性扫描程序”设置，以识别电子邮件或附件中不合规的文本数据并采取必要的操作。

任务

1 从“策略管理器”中，选择具有“DLP 和合规性”扫描程序的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“DLP 和合规性扫描程序”。

4 在“激活”中，选择“启用”以激活选定子菜单项目的 DLP 和合规性扫描程序设置。

- 默认情况下，“DLP 和合规性扫描程序”的所有扫描程序设置选项已禁用。
- 如果要配置子策略的设置，请选择“使用父策略中的配置”继承父策略的设置。
- 如果将新扫描程序添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用扫描程序的时隙。

5 在“选项”中，您可以使用：
- “包括文档和数据库格式” — 扫描文档和数据库格式的内容中是否存在不合规的内容。
- “扫描所有附件的文本” — 扫描所有附件的文本。
- “创建” — 创建一则消息，用于在电子邮件内容因触发规则而被替换时显示。 详细说明请参见“创建警报”。
- “查看/隐藏” — 显示或隐藏警报邮件的预览。如果预览已隐藏，单击此链接可以显示预览。如果预览已显示，单击此链接可隐藏预览。

6 在“DLP 和合规性规则及关联操作”中，单击“添加规则”。

此时将显示“DLP 和合规性规则”页。

7 在“指定规则的操作”中，从“选择语言”下拉菜单中选择语言。

您还可以查看和编辑所有支持的区域设置字典。 （支持的区域设置为简体中文、法语、德语、日语和西班牙语。）

例如，如果 MSME 在安装时采用德语区域设置，您仍然可以查看和编辑其他支持的区域设置字典。 任何新建的类别均适用于所有支持的区域设置。

8 在“指定对规则的操作”中，从“选择规则组”下拉菜单中选择可触发操作的规则组（如果一个或多个规则被打破）。 每条短语可针对某个类别具有一个“分数”集，位于 “ DLP 和合规性扫描程序短语”中。

对于一些规则组，您可能需要指定以下选项：

- “阈值分数” — 指定将触发扫描程序的最大阈值分数。
- “最大词数” — 指定该规则组可触发的最大次数。超出该数量将触发扫描程序并采取指定的操作。

当前“阈值分数”的公式为 =“分数” x 术语计数（实例）。 当数值等于或超过“阈值分数”时，会触发规则。

如需了解“阈值分数”和“最大词数”如何帮助触发规则，试以 Pascal 语言字典为例。假设您已将“DLP 和合规性扫描程序短语”“PAnsiChar”的“分数”设置为 5。

如果您已在“选择规则组”下选择“Pascal Language（Pascal 语言）”字典，并将值设置为：

- “阈值分数” = 15
- “最大词数” = 4

如果在代码中两次找到 "PAnsiChar"，当前阈值分数为 10，不会触发规则。

如果在代码中五次找到 "PAnsiChar"，则当前阈值分数计算仍为“分数” x “最大术语计数”，即 5 * 4 = 20。 该值大于定义的阈值分数。 因此，规则会被触发。

假设您已将“PAnsiChar”的“分数”修改为 8。如果在代码中发现三次“PAnsiChar”，当前阈值分数变为 24，则会触发规则，因为分数已超出指定的“阈值分数”。

如果有多个规则，“阈值分数”即为一个字典所有规则分数的合并值。

只有当数值等于或超过“阈值分数”时才会触发规则，但即使电子邮件中的短语实例超过“最大术语计数”值，也不会触发规则。

9 从“如果检测到，请执行以下操作：”中，选择如果检测到电子邮件中的某些内容不合规时必须采取的 DLP 和合规性扫描程序操作。

10 从“以及”中，选择一个或多个操作。

11 单击“保存”应用设置并返回策略设置页。

12 单击“应用”以将这些设置配置到策略。

配置文件过滤设置

配置策略中的设置，以根据文件名、类型或大小检测文件，并采取必要的操作。

任务

1 从“策略管理器”中，选择具有“文件过滤”扫描程序的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“文件过滤”。

4 在“激活”中，选择“启用”以激活选定子菜单项目的文件过滤扫描程序设置。

- 如果要配置子策略的设置，请选择“使用父策略中的配置”继承父策略的设置。
- 如果将扫描程序添加到策略，您可以使用“您想要什么时候应用”下拉列表指定启用扫描程序的时隙。

5 选择“扫描嵌入式文件”，以扫描嵌入式电子邮件。

6 在“警报选择”中，单击以下选项：

- “创建” — 创建电子邮件附件因规则触发被替换时的警报消息。 详细说明请参见“创建警报”。
- “查看/隐藏” — 显示或隐藏警报邮件的预览。如果预览已隐藏，单击此链接可以显示预览。如果预览已显示，单击此链接可隐藏预览。

7 在“文件过滤规则及关联操作”中，从“可用规则”下拉菜单选择可用的规则。 如果想要创建新的文件过滤规则，请选择“<创建新规则...>”。 有关如何新建文件过滤规则的更多说明，请参见“配置文件过滤规则”。

文件过滤设置可以阻止以电子邮件附件形式出现的受限制的文件（例如 .exe 文件）。 如果 .exe 文件以受密码保护的 .zip 文件形式发送，即使“受密码保护的文件”设置配置为允许文件，文件过滤规则也可以阻止该文件。

有时合法受限制文件会以受密码保护的 .zip 文件形式出现，您可能需要允许这些文件。 若要运行包含受限制文件（例如 .exe 文件）的受密码保护 .zip 文件，必须添加“可用规则”下拉列表中的“密码保护绕过规则”。

请确保该规则位于列表的首位。 如果规则已在其他级别列出，请删除该规则，然后从“可用规则”下拉列表中选择该规则。

确保为每个类别创建单独的文件过滤规则，如文件名、类型和大小。

8 单击“更改”指定当电子邮件中的文件/附件触发扫描程序时必须采取的操作。

9 单击“删除”，将现有规则从策略中删除。

10 单击“应用”以将这些设置配置到策略。

配置邮件 URL 信誉设置

配置“邮件 URL 信誉”设置以检测电子邮件正文中的恶意 URL。

启用后，MSME 会扫描电子邮件正文中的每条 URL、获取信誉分数、将分数与定义的阈值进行比较并采取相应操作。

通过将 URL 从电子邮件正文中删除，软件会在邮件进入组织前对其进行处理。 如果某封电子邮件包含多个 URL，并且其中一个 URL 超过定义的阈值，会根据配置对该电子邮件采取操作。

启用该功能保护您的系统抵御拒绝服务 (DoS) 攻击、网络钓鱼链接、包含恶意软件的 URL 或有害 URL。

邮件 URL 信誉功能适用于以下策略：

- “按访问”
- “按需默认”和
- “按需（完全扫描）”

根据软件安装过程中选择的配置选项，默认情况下邮件 URL 信誉针对以下策略启用或禁用：

- 对于“默认配置” — 针对所有策略禁用。
- 对于“增强配置” — 仅针对按访问扫描策略启用。

第一次启用“邮件 URL 信誉”时，软件会从 McAfee GTI 服务器下载 URL 的本地缓存。

对于每条 URL，软件会按照本地数据库检查其信誉分数，并根据配置采取相应的操作。 如果本地数据库的信誉分数无法使用，那么软件会从 McAfee GTI 服务器获取分数。 软件通过 McAfee GTI 服务器进行检查并定期更新本地数据库。 如果本地数据库超过 30 天未进行更新，软件会在下次更新时下载整个数据库。 否则，会逐步进行更新。 默认情况下，本地数据库会每天更新一次。 您无法修改数据库的存储位置。

您无法使用 ePolicy Orchestrator 更新本地数据库，因为服务器需要直接连接到互联网。 但是，如果使用代理服务器下载反垃圾邮件规则，可使用相同的配置下载 URL 数据库。

任务

1 在“策略管理器”中，选择具有“邮件 URL 信誉”扫描程序的子菜单项目。

“邮件 URL 信誉”保护仅适用于“按访问”、“按需（默认）”和“按需（完整扫描）”策略。

2 单击“主策略”或任何要配置的“子策略”，单击“列出所有扫描程序”选项卡，然后单击“邮件 URL 信誉”。

3 在“激活”中，选择“启用”。

- 如果配置子策略的设置，选择“使用父策略中的配置”以继承父策略的设置。
- 如果将扫描程序添加到策略，您可以使用“您想要什么时候应用”下拉列表指定启用扫描程序的时间。

4 在“选项”下拉列表中，可以选择：

- “默认邮件 URL 设置” — 应用默认阈值。
- “创建新选项集” — 根据需要定义阈值。

如果编辑现有设置，请确保为扫描程序设置提供独特的“实例名称”。

5 若要定义扫描程序设置，请选择“创建新选项集”。

6 在“邮件 URL 信誉”页面，定义以下值并单击“保存”。

- “实例名称”
- “较高 URL 信誉阈值”
- “较低 URL 信誉阈值”
- “每封电子邮件的最大 URL 数”

“较高 URL 信誉阈值”应始终高于“较低 URL 信誉阈值”。

如果某个 URL 出现多次，则 URL 计分为 1 而不是出现的次数。 例如，如果电子邮件包含 50 条 URL 并且某条 URL 出现了 20 次，则 URL 的计分为 31 而不是 50。

7 在“要采取的操作”部分，单击“编辑”以定义操作。

您还可以应用默认设置。

8 在“邮件 URL 信誉操作”页面中，定义“邮件 URL 信誉分数高于较高阈值时”、“邮件 URL 信誉分数低于较低阈值时”以及“邮件 URL 查找计数超过限制”的设置。

a 在“采取以下操作”下拉列表中，选择：

- “将项目替换为警报”。
- “删除消息”。
- “允许通过”。

选择“将项目替换为警报”后，请选择警报格式：

- “默认邮件 URL 信誉警报” — 使用默认警报消息。
- “创建” — 根据需要定义警报消息。 为“警报名称”输入独特的名称，定义警报消息，从“显示”下拉列表中定义文本格式，然后单击“保存”。

McAfee 建议您以纯文本格式保存警报，这样所有电子邮件客户端都可查看文本内容。

b 在“并且”部分中，定义以下选项：

- “记录”
- “隔离”
- “转发隔离电子邮件”
- “通知管理员”
- “通知内部发件人”
- “通知外部发件人”
- “通知内部收件人”
- “通知外部收件人”

有关这些选项的定义，请参见“检测时可以采取的操作”。

9 单击“保存”以应用设置并返回至策略设置页面。

10 单击“应用”将这些设置实施到策略。

您可以在“检测到的项目” | “邮件 URL 信誉”页面中查看检测到的 URL。 在“查看结果”部分中，可以查看检测到的 URL 列表。 详细视图请单击“禁止的短语”列中的“阻止的 URL”。

较高和较低 URL 信誉阈值示例

将“较高 URL 信誉阈值”设置为 80，“较低 URL 信誉阈值”设置为 50。 如果 URL 的信誉分数：

GTI 信誉分数为	操作
高于 80	根据邮件 URL 信誉设置采取操作。
低于 50	MSME 允许带有该 URL 的电子邮件。
介于 50 至 80	MSME 怀疑该 URL 可能含有恶意，并根据设置采取操作。

“高度怀疑”阈值检测最危险的恶意 URL。 如果降低阈值，则误报的可能性会变大。 误报 - 某条 URL 可能合法，但数据库则认为是潜在恶意 URL。

针对电子邮件附件的 TIE 信誉检查

MSME 现在利用 TIE 信誉检查对在网关、集线器和邮箱级别通过电子邮件发送的附件进行检查，从而提供其他威胁检测功能。

什么是 TIE？

Threat Intelligence Exchange 通过执行全面的高级文件信誉检查，实时增强保护和检测功能，并防止威胁蔓延。 TIE 服务器可在网关、集线器和邮箱级别快速分析附件。 有关 Threat Intelligence Exchange 的信息，请参阅《“Threat Intelligence Exchange 2.0 产品手册”》。

TIE 信誉基于以下两个变体：

- 证书信誉
- 文件信誉

TIE 首先验证文件的证书信誉分数。 仅当证书信誉为已知恶意时，才会考虑文件信誉分数。

MSME 如何与 TIE 协作

如果在策略设置中启用 TIE，在应用文件过滤规则后，MSME 会通过 TIE 服务器检查电子邮件附件的信誉。 根据文件的 TIE 信誉，分数会映射到以下其中一个类别，并且 MSME 会根据为该类别定义的配置采取操作：

- 已知可信 - 99
- 很有可能可信 - 85
- 可能可信 - 70
- 未知 - 50
- 可能恶意 - 30
- 很有可能是恶意文件 - 15
- 已知恶意 - 1

为特定类别配置操作时，会针对 TIE 信誉分数低于指定类别的所有类别应用同一操作。 默认情况下，“达到或低于以下情况时执行操作”设置为“可能恶意”。

例如，当您将“达到或低于以下情况时执行操作”设置为“未知”且对于分数为 50 的文件将操作设置为“以警报替换”，则 TIE 信誉分数小于或等于 50 的所有附件都将以警报消息替换。 您还可以为警报选择辅助操作。

信誉分数会在本地缓存，并且 MSME 可以使用更新后的本地缓存进行信誉检查。

禁用 TIE 后，会根据策略设置执行扫描操作。 如果 TIE 已启用但 TIE 服务器无法连接，且本地缓存不包含文件的条目，则会跳过来自 TIE 的信誉检查，并且会根据策略设置扫描电子邮件。

有关如何映射信誉分数的详细信息，请参见“TIE 产品手册”。

MSME 仅发送以下文件类型以进行 TIE 信誉检查：

- exe
- pdf
- Microsoft Office 文档

有关支持的文件类型的列表，请参见 KB89578。

如果电子邮件包含压缩附件，则会将压缩文件解压，并仅发送附件中支持的文件类型，以进行 TIE 信誉检查。 有关支持的压缩文件类型的列表，请参见 KB89577。

对于其他类型的文件和后 TIE 信誉检查，MSME 会根据策略设置扫描附件。 当您根据 TIE 检测发布隔离项目时，在允许之前仅对文件执行病毒扫描。 您可以在“信息显示版”页面上查看 TIE 检测到的文件数目和发送至 ATD 检查信息的文件数目。

使用 Advanced Threat Defense 信誉

您还可以根据附件大小，针对选定信誉类别的文件启用 Advanced Threat Defense 检测。

对文件进行 TIE 信誉检查时，TIE 会返回信誉分数，并且可能推荐文件进行分析。 MSME 根据设置中配置的类别和文件大小，会将文件发送至 Advanced Threat Defense。 如果文件的信誉分数有改动，本地缓存会随该信誉分数更新。 从下一次查询开始将使用修改后的分数。 “达到或低于以下情况时执行操作”的默认设置为“可能恶意”，“文件大小”的默认设置为 8 MB。

有关对 MSME 进行 TIE 服务器部署的建议设置

McAfee 建议您：

- 在次要配置中部署 TIE 服务器，以在与 Exchange 服务器相同的数据中心中处理来自 MSME 的所有 TIE 信誉请求。 这使得 TIE 服务器能够在专门的基础架构中每秒处理最多电子邮件附件。

为获得 TIE 信誉而发送的每个电子邮件附件最多将调用 2 个 TIE 请求。

- MSME 服务器在本地缓存信誉后，将降低信誉流量。 但是，由于 MSME 在服务重新启动后会清除本地缓存，因此可能会遇到流量峰值。
- 使用 MSME 中的信息显示板计数器，估计来自 MSME 的请求。 有关如何测量每秒发送到 TIE 服务器的请求的信息，请在 McAfee ePO 中“TIE 服务器拓扑管理”页面中的“服务器设置”下查看“性能状态”下的“吞吐量”。 您还可以在“TIE 服务器数据清理”页面中查看“TIE 服务器新文件”。

将 TIE 设置配置为扫描电子邮件附件

根据文件信誉类别启用针对电子邮件附件的 TIE 信誉检查。

任务

1 在产品界面中，单击“设置和诊断” | “TIE 设置”。

2 从“达到或低于以下情况时执行操作”下拉列表中选择一项。

- “已知可信” — 文件的信誉为 99。
- “很有可能可信” — 文件的信誉为 85。
- “可能可信” — 文件的信誉为 70。
- “未知” — 文件的信誉为 50。
- “可能恶意” — 文件的信誉为 30。

  默认情况下，选择的是“可能恶意”。

- “很有可能是恶意文件” — 文件的信誉为 15。
- “已知恶意” — 文件的信誉为 1。

3 在“执行以下操作”中，根据需要定义以下设置。

- “将项目替换为警报” — 使用警报消息替换，并根据“以及”中的定义进行记录、隔离或通知。
- “删除嵌入的项目” — 删除电子邮件中的附件，并根据“以及”中的定义进行记录、隔离或通知。
- “删除邮件” — 删除电子邮件，并根据“以及”中的定义进行记录、隔离或通知。

4 在“此外”中，根据需要配置以下设置。

- “记录”
- “隔离”
- “转发隔离电子邮件”
- “通知管理员”
- “通知内部发件人”
- “通知外部发件人”
- “通知内部收件人”
- “通知外部收件人”

5 在“达到或低于以下情况时将文件提交到 ATD”中，针对 Advanced Threat Defense 信誉选择类别和文件大小。

配置反垃圾邮件设置

配置策略中的设置以检测垃圾电子邮件并采取必要的操作。

任务

1 从“策略管理器”中，选择具有“反垃圾邮件”扫描程序的子菜单项“网关”。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“反垃圾邮件”。

4 在“激活”中，选择“启用”激活所选的子菜单项的反垃圾邮件扫描程序设置。

- 如果要配置子策略的设置，请选择“使用父策略中的配置”继承父策略的设置。
- 如果将新扫描程序添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用扫描程序的时隙。

5 在“选项”下拉列表中，选择现有扫描程序设置或“<创建新的选项集>”。

此时将显示“反垃圾邮件设置”页。

6 在“实例名称”中，键入反垃圾邮件扫描程序设置实例的唯一名称。此字段是必填的。

7 在“选项”选项卡中的“评分”下，键入以下选项的值：

- “高分数阈值” — 如果总体垃圾邮件分数为 15 或更高。
- “中分数阈值” — 如果总体垃圾邮件分数介于 10 至 15 之间。
- “低分数阈值” — 如果总体垃圾邮件分数介于 5 至 10 之间。

若要使用垃圾邮件分数的默认值，请选择“使用默认值”选项。这些默认设置已经过精心优化，以维持高垃圾邮件检测率和低误报率之间的平衡。万一需要更改这些设置，可以从技术支持获取技术通告。

8 在“报告”中的“垃圾邮件报告阈值为”下拉列表下，选择“高”、“中”、“低”或“自定义”指定电子邮件应标记为垃圾邮件的点。

9 在“自定义分数”中，键入电子邮件应标记为垃圾邮件的特定垃圾邮件分数。仅当您选择“垃圾邮件报告阈值为”下拉列表中的“自定义”时，才启用此字段。

10 根据需要，选中或取消选中“向垃圾邮件主题添加前缀”。

11 从“添加垃圾邮件分数指示符”下拉列表中，选择以下选项：

- “从不” - 不向电子邮件的 Internet 标头添加垃圾邮件分数指示符。
- “仅至垃圾邮件” — 只向垃圾邮件的 Internet 标头添加垃圾邮件分数指示符。
- “仅至非垃圾邮件” — 只向非垃圾邮件的 Internet 标头添加垃圾邮件分数指示符。
- “至所有邮件” — 向所有电子邮件的 Internet 标头添加垃圾邮件分数指示符。

垃圾邮件分数指示符是垃圾邮件报告中使用的符号，它添加到电子邮件的 Internet 标头以表示电子邮件中包含的潜在垃圾邮件内容的数量。

12 从“附加垃圾邮件报告”下拉列表中，选择以下选项：

- “从不” - 不向电子邮件添加垃圾邮件分数指示符。
- “仅至垃圾邮件” — 只向垃圾邮件添加垃圾邮件报告。
- “仅至非垃圾邮件” — 只向非垃圾邮件添加垃圾邮件报告。
- “至所有邮件” — 向所有电子邮件添加垃圾邮件报告。

13 选择或取消选择“详细报告”可指定是否需要详细报告。详细报告包括已触发的反垃圾邮件规则的名称和说明。

对“附加垃圾邮件报告”选择“永不”将禁用“详细报告”。

14 在“高级”选项卡上，使用以下选项：

- “扫描的最大邮件大小(KB)” — 指定可以扫描的电子邮件的最大大小（以千字节为单位）。您可以键入最高为 999,999,999 KB 的大小，尽管垃圾邮件通常较小。默认值为 250 KB。
- “垃圾邮件标头的最大宽度(字节)” - 指定垃圾邮件标头可以达到的最大大小（以字节为单位）。您可以指定的最小标头宽度为 40 个字符，最大为 999 个字符。默认值为 76。

  垃圾邮件制造者通常会出于自己的目的向标头添加附加信息。

- “报告规则的最大数量” - 指定垃圾邮件报告中可以包含的反垃圾邮件规则的最大数目。您可以指定的最小规则数为 1，最大为 999。默认值为 180。
- “标头名称” - 为电子邮件标头指定其他名称。在跟踪电子邮件和对这些邮件应用规则时，您可以使用此电子邮件标头及其标头值（下方）。这些字段是可选的，并且最多可接受 40 个字符。
- “标头值” - 为电子邮件标头指定其他值。
- “添加标头” - 指定不向任何电子邮件添加标头、向所有电子邮件添加标头、仅向垃圾邮件添加标头或仅向非垃圾邮件添加标头。
- 根据需要，选中或取消选中“邮件不是垃圾邮件时使用备用标头名称”选项。

15 在“邮件列表”选项卡中的“列入黑名单的发件人”、“列入白名单的发件人”、“列入黑名单的收件人”和“列入白名单的收件人”下，键入列入黑名单和白名单的发件人和收件人的电子邮件地址。

发送到或来自黑名单上的电子邮件地址的电子邮件视为垃圾邮件，即使它们不包含类似垃圾邮件的特征。发送到或来自白名单上的电子邮件地址的电子邮件不视为垃圾邮件，即使它们包含类似垃圾邮件的特征。

单击“添加”向列表中添加电子邮件地址，单击每个地址旁边的复选框指定它是否处于启用状态。单击“全部删除”从列表中删除电子邮件地址。无法多次添加同一电子邮件地址。您可以使用通配符匹配多个地址。

16 在“规则”选项卡中，输入规则名称，然后选择“启用规则”激活它。单击“添加”显示可用的规则的列表。

单击“重置”返回到默认反垃圾邮件设置。

17 对于列表中的每个规则，单击“编辑”修改规则。

18 单击“删除”删除规则。

19 单击“保存”返回策略页。

20 在“检测到垃圾邮件时执行的操作”中，单击“编辑”。在以下选项卡中，指定如果检测到垃圾邮件必须采取的反垃圾邮件扫描程序操作：
- “高分数”
- “中分数”
- “低分数”

21 单击“保存”应用设置并返回策略设置页。

22 单击“应用”以将这些设置配置到策略。

任务

- *导入或导出黑名单和白名单*第 72 页
  导入或导出黑名单和白名单，以便进行备份或在任何其他 Exchange Server 上使用。
- *使用反欺诈保护*第 73 页
  电子邮件欺诈是在用户不知道电子邮件实际上来自非法来源的情况下，更改发件人电子邮件地址，哄骗用户打开电子邮件并回复电子邮件，从而吸引用户的一种常用方法。
- *配置反欺诈保护*第 73 页
  启用反欺诈保护，防止您的系统遭受欺诈电子邮件侵扰。

导入或导出黑名单和白名单

导入或导出黑名单和白名单，以便进行备份或在任何其他 Exchange Server 上使用。

任务

1 从“策略管理器”中，选择具有反垃圾邮件扫描程序的子菜单项“网关”。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“反垃圾邮件”。

4 在“选项”中，单击链接“阻止列表和允许列表”。

此时将显示“反垃圾邮件设置”页。

5 单击“邮件列表”选项卡。

6 选择以下需要的列表：
- “已列入黑名单的发件人”
- “已列入白名单的发件人”
- “已列入黑名单的收件人”
- “已列入白名单的收件人”

7 若要导入列表，请单击“导入”。在弹出窗口中，单击“浏览”导航到所需的 .cfg 文件，然后单击“确定”。

8 若要导出列表，请单击链接“导出”。

单击“删除”从数据库中删除列表。

9 单击“保存”应用设置并返回策略设置页。

使用反欺诈保护

电子邮件欺诈是在用户不知道电子邮件实际上来自非法来源的情况下，更改发件人电子邮件地址，哄骗用户打开电子邮件并回复电子邮件，从而吸引用户的一种常用方法。

MSME 现在使用 Internet 工程任务组中的发件人策略框架 (SPF) 机制支持反欺诈。 SPF 框架基于授权在电子邮件中使用域名的 RFC 7208。

基于对发件人域的 SPF 评估，结果分类为：

- 无
- 一般
- 通过
- 未通过或硬故障
- 软故障
- 临时错误
- 永久错误

使用 SPF 过滤器，您可以配置软故障和硬故障的操作。 为降低误报率，MSME 将其余类别视为通过。 启用 SPF 后，您可以在“Received-SPF”的电子邮件标题中查看 SPF 结果。

配置反欺诈保护

启用反欺诈保护，防止您的系统遭受欺诈电子邮件侵扰。

开始之前

您必须已在 Exchanger 服务器上安装 McAfee Anti-spam 组件。

任务

1 导航至“设置和诊断” | “反垃圾邮件”

2 在“SPF 过滤器”部分中，选择“启用”。

3 根据需要，配置“硬故障”和“软故障”的操作。

- “允许通过” — 允许将电子邮件发送给收件人。
- “允许通过和隔离” — 允许将电子邮件发送给收件人并在隔离项目中保留一份副本。
- “拒绝邮件和隔离” — 阻止并隔离电子邮件。

启用此选项可能会影响产品性能，因为反欺诈会查询 DNS 服务器，并且它依赖于网络延迟。

配置反网络钓鱼设置

配置策略中的设置以使用反垃圾邮件规则和引擎阻止网络钓鱼邮件，并采取必要的操作。

任务

1 从“策略管理器”中，选择具有“反网络钓鱼”扫描程序的子菜单项“网关”。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“反网络钓鱼”。

4 在“激活”中，选择“启用”激活所选的子菜单项的反网络钓鱼扫描程序设置。

- 如果要配置子策略的设置，请选择“使用父策略中的配置”继承父策略的设置。
- 如果将新扫描程序添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用扫描程序的时隙。

5 在“选项”下拉列表中，选择现有扫描程序设置或“<创建新的选项集>”。

此时将显示“反网络钓鱼设置”页。

6 在“实例名称”中，键入反网络钓鱼扫描程序设置实例的唯一名称。此字段是必填的。

7 在“报告选项”中，根据需要选择或取消选择以下选项：

- “向网络钓鱼邮件主题添加前缀” — 指定要在任何可能包含网络钓鱼信息的电子邮件的主题行的开始位置添加文本。
- “向邮件添加网络钓鱼指示标头” — 指定是否向任何可能包含网络钓鱼信息的电子邮件的 Internet 标头添加网络钓鱼指示符。
- “附加网络钓鱼报告” — 指定是否应生成网络钓鱼报告并将其添加到检测为网络钓鱼的电子邮件。
- “详细报告” — 指定在电子邮件中是否包含触发的反网络钓鱼规则的名称和详细说明。只有选择“附加网络钓鱼报告”选项时，此选项才可用。

8 单击“保存”返回策略页。

9 在“要采取的操作”中，单击“编辑”，然后指定如果检测到网络钓鱼必须采取的反网络钓鱼扫描程序操作。

10 单击“保存”应用设置并返回策略设置页。

11 单击“应用”以将这些设置配置到策略。

管理策略的过滤器设置

启用或禁用过滤器选项，然后指定策略触发时对检测到的项目采取的适当操作。

可用过滤器包括：

- “遭破坏的内容”
- “受保护的内容”
- “加密的内容”
- “签名的内容”
- “受密码保护的文件”
- “邮件大小过滤”
- “扫描程序控制”
- “MIME 邮件设置”
- “HTML 文件”

任务

- *配置遭破坏的内容的设置*第 75 页
  配置策略中的设置以识别带有遭破坏内容的电子邮件并采取必要的操作。
- *配置受保护的内容的设置*第 75 页
  配置策略中的设置以识别带有受保护内容的电子邮件并采取必要的操作。
- *配置加密的内容设置*第 76 页
  配置策略中的设置以识别带有加密的内容的电子邮件并采取必要的操作。
- *配置签名的内容的设置*第 76 页
  配置策略中的设置以识别带有签名的内容的电子邮件并采取必要的操作。
- *配置受密码保护的文件的设置*第 77 页
  配置策略中的设置以识别带有受密码保护存档的电子邮件并采取必要的操作。
- *配置邮件大小过滤设置*第 77 页
  策略中的邮件大小过滤设置根据邮件的大小、附件数量和附件大小对其进行检测。
- *配置扫描程序控制设置*第 78 页
  配置策略中的设置，该设置用于定义嵌套级别、展开文件大小和对电子邮件进行扫描时允许的最大扫描时间。
- *手动阻止 IP 地址*第 79 页
  您可以阻止特定 IP 地址或一个 IP 地址范围将电子邮件发送至您的组织，而不管其 IP 地址信誉为何。 要启用此选项，您必须更新以下注册表。
- *配置 MIME 邮件设置*第 80 页
  配置策略中的设置以识别编码的 MIME 邮件并采取必要的操作。
- *配置 HTML 文件设置*第 81 页
  配置策略中的设置，以扫描电子邮件 HTML 组件中的元素或删除其中的可执行文件，如 ActiveX、Java 小程序、VBScripts。

配置遭破坏的内容的设置

配置策略中的设置以识别带有遭破坏内容的电子邮件并采取必要的操作。

一些电子邮件的内容可能受损，无法对其进行扫描。遭破坏的内容策略可以指定检测后如何处理内容已遭破坏的电子邮件。

任务

1 从“策略管理器”中，选择具有过滤器的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“遭破坏的内容”。

如果将新过滤器添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用过滤器的时隙。

4 在“操作”中，单击“编辑”指定当检测到遭破坏的内容时必须采取的过滤操作。

5 单击“保存”返回策略页。

6 单击“应用”以将这些设置配置到策略。

配置受保护的内容的设置

配置策略中的设置以识别带有受保护内容的电子邮件并采取必要的操作。

受保护的内容策略可以指定检测后如何处理具有受保护的内容的电子邮件。

任务

1 从“策略管理器”中，选择具有过滤器的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“受保护的内容”。

如果将新过滤器添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用过滤器的时隙。

4 在“操作”中，单击“编辑”指定当检测到受保护的内容时必须采取的过滤操作。

5 单击“保存”返回策略页。

6 单击“应用”以将这些设置配置到策略。

配置加密的内容设置

配置策略中的设置以识别带有加密的内容的电子邮件并采取必要的操作。

电子邮件可进行加密以防止未经授权各方进行访问。加密的内容使用密钥和加密数学算法对其解密。加密的内容策略可以指定检测后如何处理加密的电子邮件。

任务

1 从“策略管理器”中，选择具有过滤器的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“加密的内容”。

如果将新过滤器添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用过滤器的时隙。

4 在“操作”中，单击“编辑”指定当检测到加密内容时必须采取的过滤操作。

5 单击“保存”返回策略页。

加密内容设置适用于内部电子邮件中的加密附件和加密的 Internet 电子邮件。

6 单击“应用”以将这些设置配置到策略。

配置签名的内容的设置

配置策略中的设置以识别带有签名的内容的电子邮件并采取必要的操作。

以电子方式发送信息时，信息有可能被意外或蓄意更改。为了解决此问题，有些电子邮件软件使用数字签名，即手写签名的电子形式。

数字签名是添加到发件人的邮件中的附加信息，用于标识和验证发件人以及邮件中的信息。它已加密并充当数据的唯一摘要。通常情况下，收到的电子邮件的末尾显示一长串字母和数字。然后，电子邮件软件重新检查发件人的邮件中的信息并创建数字签名。如果该签名与原始签名相同，则数据没有更改。

如果电子邮件包含病毒、已损坏内容或过大，软件可能会清理或删除邮件的某一部分。电子邮件仍然有效并可以阅读，不过原始数字签名“已损坏”。收件人无法信任电子邮件的内容，因为这些内容也可能以其他方式更改过。签名的内容策略可以指定如何处理具有数字签名的电子邮件。

任务

1 从“策略管理器”中，选择具有过滤器的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“签名的内容”。

如果将新过滤器添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用过滤器的时隙。

4 在“操作”中，单击“编辑”指定当检测到经过签名的内容时必须采取的过滤操作。

5 单击“保存”返回策略页。

签名的内容设置适用于签名的电子邮件和附件。

6 单击“应用”以将这些设置配置到策略。

配置受密码保护的文件的设置

配置策略中的设置以识别带有受密码保护存档的电子邮件并采取必要的操作。

受密码保护的文件无法在无密码的情况下访问，并且也无法进行恶意软件扫描。 受密码保护的文件的策略指定了如何处理包含受密码保护文件的电子邮件。

任务

1 从“策略管理器”中，选择具有过滤器的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“受密码保护的文件”。

如果将新过滤器添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用过滤器的时隙。

4 在“操作”中，单击“编辑”以指定检测到包含受密码保护文件的电子邮件时必须采取的过滤操作。

如果将操作设置为“允许通过”，请确保“文件过滤”扫描程序设置中“文件过滤规则和相关操作”下的“密码保护绕过规则”处于列表的首位。 如果规则已在其他级别列出，请删除规则并从“可用规则”下拉列表中选择规则。

5 单击“保存”返回策略页。

6 单击“应用”以将这些设置配置到策略。

配置邮件大小过滤设置

策略中的邮件大小过滤设置根据邮件的大小、附件数量和附件大小对其进行检测。

开始之前

确保在“按访问设置”页面上，选择了“扫描入站邮件”和“扫描出站邮件”选项。

您可以单独为“网关”策略和“按访问”策略配置邮件大小过滤设置。 为入站电子邮件配置“网关”设置，为出站电子邮件配置“按访问”设置。 例如：

- 若要阻止包含 5 个以上附件的所有入站电子邮件，在“网关”策略中配置“邮件大小过滤”设置。
- 若要阻止包含 3 个以上附件的所有出站电子邮件，在“按访问”策略中配置“邮件大小过滤”设置。

按访问扫描的邮件大小过滤不适用于邮箱服务器角色。

任务

1 从“策略管理器”中，选择具有防病毒扫描程序的子菜单项。

此时将显示子菜单项的策略页。

2 选择“按访问”或“网关”策略作为所需策略：

3 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

4 单击“邮件大小过滤”。

5 在“激活”中，选择“启用”激活所选的子菜单项的电子邮件大小过滤器设置。

如果将新过滤器添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用过滤器的时隙。

6 在“选项”中，可以使用：
   - “默认设置” — 查看默认情况下使用的邮件大小选项集的摘要。
   - “默认网关设置” — 查看网关策略所用的默认邮件大小选项摘要。
   - “<create new set of options>” — 配置邮件大小过滤选项。 选项包括：
     - “实例名称” — 键入邮件大小过滤器设置实例的唯一名称。此字段是必填的。
     - “最大邮件总大小 (KB)” — 指定电子邮件可以达到的最大大小（以千字节为单位）。您可以指定 2 KB 到 2 GB 之间的值，其默认值为 20,000 KB。
     - “最大附件大小 (KB)” — 指定电子邮件的附件可以达到的最大大小（以千字节为单位）。您可以指定 1 KB 到 2 GB 之间的值，其默认值为 4096 KB。
     - “附件的最大数量” — 指定电子邮件可以具有的附件的最大数目。最大可指定的值为 999，其默认值为 25。
   - “编辑” - 编辑所选的选项集。

7 在“操作”中，单击“编辑”。 指定如果值超出以下选项的指定设置，将采取的邮件大小过滤器操作：
   - “邮件大小”
   - “附件大小”
   - “附件计数”

8 单击“保存”以返回至策略页面。

邮件大小过滤规则不会检测内部电子邮件。

配置扫描程序控制设置

配置策略中的设置，该设置用于定义嵌套级别、展开文件大小和对电子邮件进行扫描时允许的最大扫描时间。

任务

1 从“策略管理器”中，选择具有扫描程序的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“扫描程序控制”。

如果将新过滤器添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用过滤器的时隙。

4 在“选项”中，单击 “<创建新选项集>”。

5 在“实例名称”中，键入扫描程序控制过滤器设置实例的唯一名称。此字段是必填的。

6 在“最大嵌套级别”中，指定当附件包含压缩文件、压缩文件中又包含其他压缩文件时，扫描程序应扫描的级别。您可以指定 2 到 100 之间的值，其默认值为 10。

7 在“最大展开文件大小 (MB)”中，指定将文件展开扫描时允许文件达到的最大大小。您可以指定 1 到 2047 之间的值，其默认值为 10。

8 在“最长扫描时间（分钟）”中，指定扫描任何文件允许的最大时间。您可以指定 1 到 999 之间的值，其默认值为 1。

9 单击“保存”返回策略页。

10 在“警报选择”中，您可以选择当触发扫描程序控制选项时使用的警报。您可以使用以下选项：

- “创建” - 为此策略创建新警报邮件。
- “查看/隐藏” - 显示或隐藏警报文本。如果文本已隐藏，单击此链接可以显示文本。如果文本已显示，单击此链接可以隐藏文本。

11 在“操作”中，单击“编辑”指定如果值超出以下选项的指定设置时要采取的操作：

- “最大嵌套级别”
- “最大扩展文件大小 (MB)”
- “最长扫描时间(分钟)”

12 单击“保存”返回策略页。

13 单击“应用”以将这些设置配置到策略。

手动阻止 IP 地址

您可以阻止特定 IP 地址或一个 IP 地址范围将电子邮件发送至您的组织，而不管其 IP 地址信誉为何。 要启用此选项，您必须更新以下注册表。

开始之前

手动阻止 IP 地址仅可用在 Exchange 角色、集线器、Edge、邮箱和 HubMB 上。 要手动将 IP 地址列入黑名单，McAfee Anti-spam 检测必须在 MSME 中可用。

任务

1 在安装 MSME 的系统上，导航至以下注册表项：

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\SystemState

2 添加字符串值 IPBlackList。

3 指定您要阻止其发送电子邮件的 IPv4 地址。

您可以使用分号阻止多个 IP 地址。 您还可以使用通配符 * 阻止一个 IP 地址范围。 例如：

- 10.21.22.* — 阻止从 10.21.22.0 到 10.21.22.255 的所有 IP 地址
- 10.21.*.* — 阻止从 10.21.0.1 到 10.21.255.255 的所有 IP 地址。

配置 MIME 邮件设置

配置策略中的设置以识别编码的 MIME 邮件并采取必要的操作。

多用途 Internet 邮件扩展 (MIME) 是一种通信标准，用于在仅支持 7 位 ASCII 字符的协议（例如 SMTP）上传输非 ASCII 格式。

MIME 定义编码非 ASCII 格式的不同方法，这样可以使用 7 位 ASCII 字符集中的字符表示非 ASCII 格式。

任务

1 从“策略管理器”中，选择具有过滤器的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“MIME 邮件设置”。

如果将新过滤器添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用过滤器的时隙。

4 在“选项”中，选择 “<创建新的选项集>”。

此时将显示“邮件设置”页。

5 在“实例名称”中，键入 MIME 电子邮件过滤器设置实例的唯一名称。此字段是必填的。

6 在“选项”选项卡中，输入“消息主题的前缀”。

a 在 “MIME 邮件中附件的首选重新编码”中，从可用的选项中选择当重新编码 MIME 邮件中的附件时使用的重新编码方法。

b 在“修改的主题标头的首选重新编码”中，从可用的选项中选择当重新编码 MIME 邮件中的主题标头时使用的重新编码方法。

c 在“如果重新编码主题标题失败”中，选择以下任一选项：

- “视为错误” — 如果 MIME 邮件被退回。
- “回退到 UTF-8” - 如果 MIME 邮件编码为 UTF-8。

7 在“高级”选项卡中，选择以下任一编码方式以在编码电子邮件的文本部分时使用：

- “Quoted-Printable” 最适合主要包含 ASCII 字符但也包含一些超出该范围的字节值的邮件。
- “Base64” 具有固定的处理时间，最适合非文本数据和 ASCII 文本含量不太多的邮件。
- “8 位”最适合与支持 8 位 MIME 传输 SMTP 扩展的 SMTP 服务器一起使用。

只有在“已修改主题标题的首选重新编码”中选择了“使用原始编码方案重新编码”或“使用以下字符集重新编码”，才能执行“步骤 6b”。

a 根据需要，选中或取消选中“如果文本是 7 位，则不编码”。

b 在“默认解码字符集”中，选择当 MIME 标头没有指定字符集时用于解码的字符集。

c 在“最大 MIME 部分数”中，指定 MIME 邮件中可以包含的 MIME 部分的最大数目。默认值为 10000 个 MIME 部分。

d 在 “MIME 邮件中标头损坏”中，选择所需的操作。

e 在 “MIME 邮件标头中的空字符”中，选择所需的操作。

f 在 “MIME 邮件中的 Quoted-Printable 字符编码”中，选择所需的操作。

8 在 “MIME 类型” 选项卡中，指定哪些 MIME 类型应视为文本附件，哪些视为二进制文件附件。

单击 “添加” 向列表中添加 MIME 类型，或单击 “删除” 从列表中删除 MIME 类型。不允许有重复条目。

9 在 “字符集” 选项卡中，选择 “字符集” 和 “备用”，取消选择 “固定” 勾选框，然后单击 “添加” 以指定备用字符集，用来映射至 MIME 消息中的字符集。

单击 “编辑” 以编辑字符映射，“删除” 以删除字符映射并单击 “保存” 将所作的任何更改应用至字符映射。只有当单击 “编辑” 时，“保存” 选项才可用。

10 单击 “保存”。

11 在 “警报选择项” 中，可以选择当 MIME 类型被阻止时要使用的警报。 您可以使用：

- “创建” - 为此策略创建新警报邮件。
- “查看/隐藏” - 显示或隐藏警报文本。如果文本已隐藏，单击此链接可以显示文本。如果文本已显示，单击此链接可以隐藏文本。

12 在 “不完整的邮件操作” 中，单击 “编辑” 指定当遇到部分 MIME 或外部 MIME 类型时必须采取的过滤操作。

13 单击 “保存” 返回策略页。

14 单击 “应用” 以将这些设置配置到策略。

配置 HTML 文件设置

配置策略中的设置，以扫描电子邮件 HTML 组件中的元素或删除其中的可执行文件，如 ActiveX、Java 小程序、VBScripts。

如果在 HTML 中发现任何此类内容，则将其删除。只有当启用 “内容扫描程序” 时，此过滤器才起作用。

任务

1 从 “策略管理器” 中，选择具有过滤器的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的 “主策略” 或任何子策略，然后单击 “列出所有扫描程序” 选项卡。

3 单击 “HTML 文件”。

4 在 “选项” 中，单击 “<创建新的选项集>”。

此时将显示 “HTML 文件” 页。

5 在 “实例名称” 中，键入过滤器设置实例的唯一名称。此字段是必填的。

6 在 “扫描以下元素” 中，选择以下选项之一：

- “注释” - 扫描 HTML 邮件中的注释元素。例如：

```
<!-- comment text --!>
```

- “元数据” - 扫描 HTML 邮件中的元数据元素。例如：

```
< META EQUI="Expires" Content="Tue, 04 January 2013 21:29:02">
```

- “链接 URL ("<ahref=...")” — 扫描 HTML 邮件中的 URL 元素。例如：

```
<a HREF="McAfee.htm">
```

- “来源 URL ("<img src=...")” — 扫描 HTML 邮件中的来源 URL 元素。例如：

```
<IMG SRC="..\..\images\icons\mcafee_logo_rotating75.gif">
```

- “JavaScript / VBScript” — 扫描 HTML 邮件中的 JavaScript 或 Visual Basic 脚本。例如：

```
<script language="javascript" scr="mfe/mfe.js">
```

7 在“删除以下可执行文件元素”中，选择以下选项之一：

- “JavaScript / VBScript” - 从 HTML 邮件中删除 JavaScript 或 Visual Basic 脚本元素。例如：

```
<script language="javascript" scr="mfe/mfe.js">
```

- “Java 小程序” — 从 HTML 邮件中删除 Java 小程序元素。例如：

```
<APPLET code="XYZApp.class" codebase="HTML ....."></APPLET>
```

- “ActiveX 控件” — 从 HTML 邮件中删除 ActiveX 控件元素。例如：

```
<OBJECT ID="clock" data="http://www.mcafee.com/vscan.png" type="image/png"> VirusScan Image </OBJECT>
```

- “Macromedia Flash” — 从 HTML 邮件中删除 Macromedia Flash 元素。如果已选择“ActiveX 控件”，则启用此选项。例如：

```
<EMBED SCR="somefilename.swf" width="500" height="200">
```

8 单击“保存”返回策略页。

9 单击“应用”以将这些设置配置到策略。

管理策略的其他设置

创建或编辑警报和免责声明等将在策略触发时应用的其他设置。

可用选项包括：

- “警报设置”
- “免责声明文本”

任务

- *配置警报邮件设置*第 82 页
  配置策略中的设置，在检测发生时通过警报邮件通知最终用户。
- *配置免责声明文本设置*第 83 页
  配置策略中的免责声明文本设置，免责声明即一段添加到所有出站电子邮件的文本，通常是法律声明。

配置警报邮件设置

配置策略中的设置，在检测发生时通过警报邮件通知最终用户。

任务

1 从“策略管理器”中，选择具有扫描程序的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“警报设置”。

4 选择“启用”激活所选子菜单项的警报邮件设置。

- 如果要配置子策略的设置，请选择“使用父策略中的配置”继承父策略的设置。
- 如果将新警报邮件设置添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用的时隙。

5 在“选项”中，选择可用的默认警报设置，或选择“<创建新的选项集>”定义警报设置。

有关如何创建新警报的步骤说明，请参阅“创建新警报”部分。

6 单击“编辑”修改现有警报。

此时将显示“警报设置”页。

7 选择 “HTML” 或“纯文本”作为“警报格式”。

8 从“字符编码”下拉菜单中，选择所需的字符集。

9 在“警报文件名”中，指定此警报的文件名，包括适当的 HTML (.htm) 或纯文本 (.txt) 文件扩展名。

10 选中或取消选中“启用警报标题”可启用警报标题的使用。

11 在“警报标题”文本输入框中，键入警报的标题。

12 根据在“警报标题”中 HTML 文本应显示为已编译的代码还是源代码，从“显示”中选择 “HTML 内容 (WYSIWYG)” 或 “HTML 内容(源代码)”。

只有已选择 “HTML” 作为警报邮件格式时，“显示”选项才可用。

13 根据需要，选择“启用警报尾注”启用警报尾注的使用。

14 在“警报尾注”文本输入框中，键入警报的尾注。

15 根据在“警报尾注”中 HTML 文本应显示为已编译的代码还是源代码，从“显示”中选择 “HTML 内容 (WYSIWYG)” 或 “HTML 内容(源代码)”。

只有已选择 “HTML” 作为警报邮件格式时，“显示”选项才可用。

16 单击“保存”返回策略页。

17 单击“应用”以将这些设置配置到策略。

配置免责声明文本设置

配置策略中的免责声明文本设置，免责声明即一段添加到所有出站电子邮件的文本，通常是法律声明。

分配至策略时，通过 MSME 服务器从 exchange 组织发出的所有电子邮件都将根据配置的设置应用免责声明文本。

免责声明文字设置仅适用于 Microsoft Exchange Transport 服务器。

任务

1 从“策略管理器”中，选择具有扫描程序的子菜单项。

此时将显示子菜单项的策略页。

2 单击要配置的“主策略”或任何子策略，然后单击“列出所有扫描程序”选项卡。

3 单击“免责声明文本”。

4 选择“启用”激活所选子菜单项的免责声明文本设置。

- 如果要配置子策略的设置，请选择“使用父策略中的配置”继承父策略的设置。
- 如果将新免责声明文本添加到策略，您可以通过“你希望应用此策略的时间”下拉列表指定启用的时隙。

5 在“选项”中，选择 “<创建新选项集>”。此时将显示“免责声明文本”页。

6 在“实例名称”中，键入免责声明文本设置实例的唯一名称。此字段是必填的。

7 您可以选择以下免责声明格式：

- “HTML” — 指定是否需要免责声明在通知电子邮件中以 HTML 格式显示。
- “纯文本” — 指定是否需要免责声明在通知电子邮件中以纯文本格式显示。

8 在“编辑免责声明内容”中，输入免责声明文本消息。

9 根据在“警报尾注”中 HTML 文本应显示为已编译的代码还是源代码，从“显示”中选择“HTML 内容(WYSIWYG)”或“HTML 内容(源代码)”。

只有已选择“HTML”作为免责声明文本格式时，“显示”选项才可用。

10 根据应在电子邮件中什么位置以及如何插入免责声明文本，从“插入免责声明”下拉列表中，选择“任何消息文本之前”、“任何消息文本之后”或“作为附件”。

11 单击“保存”返回策略页。

免责声明只适用于出站电子邮件。

12 单击“应用”以将这些设置配置到策略。

5 设置和诊断

“设置和诊断”的菜单包含 MSME 功能启用和禁用、功能配置、功能管理和日志。 根据您组织的安全策略配置这些设置。

若要修改或查看 MSME 产品设置，在产品的用户界面，单击“设置和诊断”。 该表简要地说明了在哪些情况下可配置这些设置：

表 5-1 设置和诊断

使用...	可...
“按访问设置” “按访问设置”仅可在 Microsoft Exchange 2010 服务器上使用。 由于 Microsoft VSAPI 支持已从 Microsoft Exchange 2013 和 2016 上删除，按访问 VSAPI 和后台扫描设置功能在 Exchange 2013 和 2016 服务器上已禁用。	定义扫描失败时对电子邮件执行的操作。 提供的选项有： • “允许通过” • “删除” 还包含适用于以下设置的启用或禁用子菜单： • “Microsoft Virus Scanning API (VSAPI)” • “后台扫描设置” • “传输扫描设置”
“按需设置”	修改 “MSMEODUser” 的密码凭据，并与 Active Directory 和其他交换服务器同步密码更新。
“邮箱排除设置”	定义要从按访问 VSAPI 扫描中排除的邮箱、文件夹或子文件夹。
“通知”	• 定义管理员电子邮件帐户，用于在检测到电子邮件时，接收通知或将通知电子邮件发送至特定审查者或 DL。 • 创建隔离电子邮件时，发送给用户的自定义通知电子邮件。 • 定义产品运行状况警报的发送频率，是每天发送给管理员还是发生特定事件时立即发送（例如 Postgres 数据库发生问题或加载服务失败）。
“反垃圾邮件”	• 定义垃圾电子邮件文件夹的设置，此文件夹用于转发边缘传输（网关）服务器上的垃圾邮件。 • 启用或禁用 “McAfee GTI 邮件信誉”功能。 • 启用或禁用“SPF 过滤器”功能。 • 启用或禁用 “McAfee GTI IP 信誉”功能。

表 5-1 设置和诊断 *（续）*

使用...	可...

“TIE 设置”	使用以下项配置和管理 TIE 检测设置：
	• “达到或低于以下情况时执行操作” — 在信誉分数小于或等于定义的阈值时启用操作。
	• “请执行以下操作”
	  • “使用警报替换项目”
	  • “删除嵌入的项目”
	  • “删除消息”
	  • “此外” — 提供各种选项，例如记录、隔离或通知。
	• “达到或低于以下情况时将文件提交到 ATD”和“将文件限制在” — 在 TIE 信誉阈值和文件大小限制匹配的情况下，发送文件以进行 Advanced Threat Defense 信誉检查。

“检测到的项目”	使用以下任一选项配置和管理隔离存储库： • “McAfee Quarantine Manager” — 配置 MSME 和 MQM 服务器（如果有）之间的通信设置。 • “本地数据库” — 管理本地隔离数据库的清除和优化等活动。
“用户界面首选项”	定义“信息显示板”中的设置，例如刷新速率、报告设置、图形单位比例、报告间隔、图形和图表设置。
“诊断”	定义调试事件和产品日志的设置，包括日志大小和存储位置等信息。 诊断设置包括： • “调试日志记录” • “事件日志记录” • “产品日志” • “错误报告服务”
“产品日志”	查看“产品日志”并根据日期、类型或描述过滤输出。
“DAT 设置”	每次更新时保留较旧的 DAT 而不进行覆盖，定义要保留的检测定义文件数量。
“导入和导出配置”	设置当前 MSME 服务器，使用与已建立服务器相同的配置、还原默认或增强设置或创建指向 DAT 下载站点的 Sitelist。
“代理服务器设置”	配置或修改 “McAfee Anti-Spam 规则更新程序服务”的代理服务器设置。

如果修改了以上任一设置，请确保单击“应用”以保存更改。 “应用”的背景颜色更改为：

- 黄色 — 如果您已更改现有设置或更改仍未应用。
- 绿色 — 如果您未更改现有设置或更改已应用。

目录

按访问设置

按访问扫描在网关处或每次电子邮件被访问时触发，以确定按访问策略是否检测到项目。按访问扫描也称为实时扫描。

根据安装了 MSME 的 Exchange 服务器的角色，每种扫描均各有优势。 该表可帮助您了解各种扫描类型及其作用，以及应用每一种扫描的情况：

Exchange Server 角色	适用策略	扫描类型	说明
边缘传输或集线器传输	• 按访问 • 网关	按访问传输扫描	在威胁达到邮箱服务器前进行扫描。 启用后，MSME 可在组织外围检测威胁，从而减少邮箱服务器的负载。
邮箱	• 按访问	按访问 VSAPI 扫描	当用户通过电子邮件客户端（例如 Outlook）访问电子邮件时，扫描威胁。
		主动式扫描	在电子邮件被写入 Microsoft Exchange 信息存储区时，扫描电子邮件是否存在威胁。
		发件箱扫描	对发件箱文件夹中的电子邮件进行威胁扫描。
		后台扫描	低优先级扫描，在后台扫描所有 Exchange 数据库上是否存在威胁。

在“常规”部分中，定义发生扫描失败时采取的操作。

引起扫描失败的原因可以是以下几种：

- “按常规失败” — 扫描程序无法扫描特定文件。
- “按产品失败” — 由于错误的 DAT 或引擎或错误的垃圾邮件规则而导致扫描失败。

部分原因可归结于技术问题，例如：

- 扫描超时
- 扫描引擎无法加载
- DAT 问题
- 电子邮件格式错误

例如，如果注册表和实际位置 (\bin\DATs) 中的 DAT 不匹配，将出现扫描失败的情况。

如果扫描失败，会根据“设置和诊断” | “按访问设置” | “常规”中指定的设置触发操作。

表 5-2 选项定义

选项	定义
“按常规扫描失败”	• “允许通过” — 扫描失败时，允许电子邮件发送至目标收件人。 • “删除” — 扫描失败时删除电子邮件。
“按产品扫描失败”	• “允许通过” — 扫描失败时，允许电子邮件发送至目标收件人。 • “删除” — 扫描失败时删除电子邮件。
McAfee 建议您始终将该选项设置为“允许通过”以避免扫描失败时隔离合法的电子邮件。 默认情况下，该选项设置为“允许通过”，这样电子邮件在扫描失败时就不会丢失了。	

在 “按访问设置”页面上还包括以下类别：

- “Microsoft Virus Scanning API (VSAPI)”
- “后台扫描设置”
- “传输扫描设置”

在“传输扫描设置”中，您可以排除已定义大小的电子邮件以进行扫描。 启用此选项后，要排除的默认文件大小为 4 MB。

有关扫描类型的更多信息，请参见 McAfee 知识库文章 KB51129。

Microsoft 病毒扫描 API (VSAPI) 设置

最终用户使用任何电子邮件客户端访问电子邮件时，Microsoft VSAPI 允许 MSME 对电子邮件进行扫描。

在 Microsoft Exchange 中，电子邮件存储在名为 Exchange 信息存储区的数据库中。接收到新的电子邮件时，Exchange Server 将通知 outlook 客户端所发生的变更。触发按访问扫描时会出现此情况。

此功能仅适用于具有邮箱角色的 Microsoft Exchange 2007/2010 服务器。

表 5-3 选项定义

选项	定义
“启用”	选择此选项可仅在最终用户使用电子邮件客户端（如 Outlook）访问电子邮件时对电子邮件进行扫描。此功能只会扫描 Microsoft Exchange 信息存储区中可用的电子邮件或扫描 AV 戳不匹配的电子邮件。
“主动式扫描”	选择此选项可在电子邮件被写入到 Microsoft Exchange 信息存储区之前进行扫描。 此功能可在下列情况下启用： • 未在集线器传输服务器上 配置 MSME，且受感染的电子邮件抵达邮箱服务器时，该电子邮件将在被写入 Exchange 信息存储区之前被检测到。 • 一般情况下，发布到公共文件夹数据库的内容通常不通过集线器传输服务器路由。为了确保在内容到达存储区之前对其进行扫描，建议您对公共文件夹数据库启用主动式扫描。
“发件箱扫描”	选择此选项可扫描发件箱文件夹中的电子邮件。 MSME 在电子邮件到达集线器传输服务器之前会自行对发件箱中的电子邮件进行扫描，从而减轻集线器服务器上的负载。
“使用期限下限（秒）”	指定一个值，仅对在此指定期限内收到的电子邮件进行扫描。将不会扫描在此指定时间之前收到的电子邮件。 默认情况下，该值设置为 86400 秒，即一天的时间。

表 5-3 选项定义 *（续）*

选项	定义
“扫描超时（秒）”	扫描电子邮件允许的最大时间。如果电子邮件扫描超出了指定的值，则会发生 在“设置和诊断”	“按访问设置”	“常规”	“扫描操作失败”下指定的操作。默认情况下，该值设置为 180 秒。
“扫描线程数”	指定用以处理按访问扫描和主动式扫描队列中项目的线程池的线程数。默认值为 2 * <处理器数量> + 1。McAfee 建议您选择 “默认”复选框以实现最佳性能。

后台扫描设置

系统性地扫描数据库中存储的所需消息。 对于每个数据库，在正常优先顺序下运行的线程会枚举数据库中的所有文件夹，然后根据需要请求 MSME 扫描内容。

表 5-4 选项定义

选项	定义
“启用”	选择在病毒爆发后对整个数据库进行后台扫描。默认情况下，该选项已禁用。
“计划”	计划启用或禁用后台扫描的时间。 • 单击 “启用时间”指定开始后台扫描的时间。 • 单击 “禁用时间”指定停止后台扫描的时间。 • 在工作日的非高峰时段或周末执行此计划。 • 如果您未创建计划，后台扫描将在进行任何 DAT 更新时开始。
“仅包含附件的邮件”	选择仅扫描包含附件的电子邮件。 如果您担心特定病毒会通过附件进行传播，该功能会非常有用。由于带有附件的电子邮件更容易受到攻击且可能含有恶意内容，因此该任务会替换任何病毒或可执行文件。 由于 MSME 仅扫描带附件的电子邮件，因此启用该功能可以节约时间。
“仅为扫描的项目”	选择扫描未扫描的电子邮件。 如果您已禁用邮箱服务器上的 Microsoft VSAPI 一段时间，并想扫描未经扫描项目，则可启用该功能。
“强制全部扫描”	选择以扫描项目，无论项目是否具有 AV 扫描戳。
“更新扫描戳”	选择更新带有最新 AV 戳的电子邮件。
“开始日期”	仅对从此指定日期开始接收的电子邮件进行后台扫描。
“结束日期”	仅对到此指定日期为止接收的电子邮件进行后台扫描。 选择“截止日期”以扫描到当前系统日期为止的电子邮件。

传输扫描设置

传输扫描可以在 SMTP 通信进入 Exchange 信息存储区之前对其执行扫描。SMTP 传输扫描可以对目的地并非本地服务器的已路由电子邮件执行扫描，并可以停止传递邮件。

表 5-5 选项定义

选项	定义
“启用”	选择此选项可启用 Exchange 传输级别的扫描。默认情况下，该选项已启用。 该选项将仅在具有边缘传输、集线器传输或邮箱和集线器角色的 Microsoft Exchange Server 上工作。
“传输扫描戳”	选择此选项，以将 DAT 特征码应用到电子邮件标题中，这样不会在邮箱角色中重新扫描电子邮件。 **建议设置：**如已启用传输扫描，请确保同时启用该选项。
“避免扫描大小超过以下值的电子邮件”	根据电子邮件大小，从按访问扫描中排除电子邮件。 您可以定义文件大小（单位：KB 或 MB）。 McAfee 建议您先扫描所有文件，然后再进行访问，这样可防止系统遭受任何潜在威胁的侵袭。
“基于方向的扫描”	根据电子邮件流配置按访问扫描。
“扫描入站邮件”	选择此选项可扫描任何进入 Exchange Server 或 Exchange 组织的电子邮件。
“扫描出站邮件”	选择此选项可扫描任何从 Exchange Server 或 Exchange 组织发出的电子邮件。只要有一个收件人的地址为外部电子邮件地址，就会将电子邮件指定为出站。
“扫描内部邮件”	选择此选项可扫描从您的域内一个位置发送到域内另一个位置的电子邮件。在 Exchange Server 权威域内的任何内容均被视为内部域。如果电子邮件来自域内并且所有收件人都位于域内，则将电子邮件指定为内部。

按需设置

访问“按需设置”页面修改 “MSMEODUser” 密码凭据。

McAfee Security for Microsoft Exchange 在邮箱服务器上安装产品时会在 Active Directory 中创建名为 “MSMEODUser” 的用户。 对邮箱执行按需扫描时需要此用户。

为符合组织的安全策略，可能需要定期更新 “MSMEODUser” 密码。

在界面中，浏览至“设置和诊断” | “按访问设置”。

选项	定义
“用户名”	“MSMEODUser” — 执行按需扫描的用户。 此为只读字段。
“键入密码”	键入密码。
“确认密码”	确认密码。
“在 LDAP 中也重置该密码”	选择该选项与 Active Directory 和其他交换服务器同步密码更新。 仅在通过“按需设置”页面初始化密码重置时勾选该选项。

更新 **MSMEODUser** 密码的方式有两种：

- 在 Active Directory 中重置密码，然后更新“按需设置”页面中的密码。
- 从“按需设置”页面重置密码。

使用 Active Directory 重置密码	使用按需设置页面重置密码
1 在 Active Directory 中更新密码。 **2** 转至同一 Active Directory 中任一邮箱角色系统。 **3** 启动 McAfee Security for Microsoft Exchange 界面。 **4** 在“设置和诊断”中，浏览至“按需设置”页面，然后更新密码。 **5** 取消选择“在 LDAP 中也重置该密码”选项。 **6** 单击“应用”。	**1** 启动 McAfee Security for Microsoft Exchange 界面。 **2** 在“设置和诊断”中，浏览至“按需设置”页面，然后更新密码。 **3** 勾选“在 LDAP 中也重置该密码”选项以确保密码更新与 Active Directory 同步。 **4** 单击“应用”。

对于托管系统，可以从 ePolicy Orchestrator 更新 “MSMEODUser” 密码。

将该设置应用到域内的所有交换服务器可能需要几分钟时间。 请在更新验证密码后，运行按需扫描。

有关 “MSMEODUser” 的更多信息，请参见 McAfee 知识库文章 KB82332。

配置邮箱排除项设置

配置要从 VSAPI 扫描中排除的邮箱或文件夹。

在以下特定情况下可配置邮箱排除项设置：

- 公司员工不希望对其电子邮件进行扫描。
- 公司政策确定了非扫描文件夹。
- 要从扫描中排除的文件夹。

McAfee 不建议排除邮箱，如果因排除设置而导致任何邮箱被感染，McAfee 概不负责。

任务

1 单击“设置和诊断” | “邮箱排除设置”。此时将显示“邮箱排除设置”页。

2 若要排除邮箱或子文件夹：

若要排除邮箱	若要排除邮箱中的文件夹
1 在“可用邮箱”窗格中，选择邮箱，然后单击“>>”。 选定的邮箱会移动至“要排除的邮箱”窗格。 为要从 VSAPI 扫描中排除的所有邮箱重复该步骤。 若要将邮箱从排除列表中删除，请选择“要排除的邮箱”窗格中的邮箱，然后单击 “<<” 将邮箱移至“可用邮箱”列表。 如果邮箱添加到“要排除的邮箱”窗格，则该邮箱中的所有文件夹都将从扫描中排除。	**1** 在“可用邮箱”窗格中，选择邮箱。 **2** 在“邮箱中要排除的文件夹”对话框中，输入要排除的文件夹名称，然后单击 “>>”。 选定的邮箱文件夹会移动至“要排除的邮箱”窗格。 您可以使用通配符将多个文件夹从 VSAPI 扫描中排除。 有关更多信息，请参见使用通配符排除邮箱文件夹。

如果通过 ePolicy Orchestrator 配置邮箱排除项，需要手动提供完整的路径。

3 单击“应用”以保存设置。

该排除项替代“按访问设置”页面中 “Microsoft Virus Scanning API (VSAPI)” 内已配置的“发件箱扫描”。 例如，如果排除某个用户的发件箱扫描，则邮箱排除项设置会替代全局发件箱扫描。

有关邮箱排除项示例的更多信息，请参见“为邮箱排除项使用通配符的示例”。

为邮箱排除项使用通配符的示例

您可以使用逗号分隔符或通配符 * 将文件夹从邮箱级别和数据库级别的 VSAPI 扫描中排除。

表 5-6 示例

级别...	若要排除...	请配置...
数据库级别	数据库中所有邮箱的“草稿”文件夹。	**1** 在产品界面中，单击“设置和诊断”	“邮箱排除项设置”。 **2** 在“可用邮箱”窗格中，选择数据库。 **3** 在“邮箱中要排除的文件夹”对话框中，输入“草稿”，单击“>>”，然后单击“应用”。 选定的邮箱文件夹会在“要排除的邮箱”窗格中列出。 您无法在未指定要排除的文件夹时，选择要排除的数据库。
	数据库中所有邮箱中以姓名“人物”起头的所有文件夹。	**1** 在产品界面中，单击“设置和诊断”	“邮箱排除项设置”。 **2** 在“可用邮箱”窗格中，选择数据库。 **3** 在“邮箱中要排除的文件夹”对话框中，输入“人物*”，单击“>>”，然后单击“应用”。 选定的邮箱文件夹会在“要排除的邮箱”窗格中列出。

表 5-6 示例 *（续）*

级别...	若要排除...	请配置...
邮箱级别	邮箱中使用逗号分隔符的多个文件夹。 例如，可以排除“收件箱”中的 Data1、Project1 和 Report1 文件夹。	1 在产品界面中，单击“设置和诊断” | “邮箱排除项设置”。 2 在“可用邮箱”窗格中，选择邮箱。 3 在“邮箱中要排除的文件夹”对话框中，输入 Inbox\Data1,Inbox\Project1,Inbox\Report1，单击 “>>”，然后单击“应用”。
	文件夹及其子文件夹。 • 您可以排除子文件夹中的电子邮件，但扫描文件夹中的电子邮件。 • 您可以排除文件夹中的电子邮件和子文件夹。	1 在产品界面中，单击“设置和诊断” | “邮箱排除项设置”。 2 在“可用邮箱”窗格中，选择邮箱。 • Inbox\Personal* — 在 VSAPI 扫描中排除“ Personal” 文件夹中的电子邮件和子文件夹。 • Inbox\Personal* — 在 VSAPI 扫描中排除 “Personal” 文件夹中的所有子文件夹。 “Personal” 文件夹中的电子邮件不会从 VSAPI 扫描中排除。

通知设置

您可以配置在电子邮件被隔离时管理员用以发送电子邮件通知的内容和 SMTP 地址。

在产品用户界面中，单击“设置和诊断” | “通知”以配置通知设置。

在 “通知”页面中，您可以使用以下选项：

- “设置” — 定义电子邮件被隔离时，接收通知的电子邮件帐户。 或者，由于电子邮件因特定扫描程序或过滤器被隔离时，可以将通知电子邮件发送至特定审查者或 DL。

  请确保电子邮件地址按照“通知”页面中系统或组系统的要求进行更新，以接收托管和单机系统的通知。

  将电子邮件通知发送到分发列表 (DL)，指定 DL 的 SMTP 地址。

- “模板” — 创建在电子邮件被隔离时发送给特定用户的自定义通知电子邮件。
- “产品运行状况警报” — 定义产品运行状况警报的发送频率，是每天发送给管理员还是发生特定事件时立即发送（例如 Postgres 数据库发生问题或加载服务失败）。

  配置产品时（例如通知或策略名称），请确保未使用可能导致跨站点脚本 (XSS) 漏洞的字符。 有关必须避免的字符列表，请查看 McAfee 知识库文章 KB82214。

配置通知设置

配置电子邮件帐户以在电子邮件被隔离时接收通知。 以及检测到电子邮件时，将通知电子邮件发送至特定审查者或 DL。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “通知”.

2 在“通知” | “设置”选项卡中，可以使用：

表 5-7 选项定义

选项	定义
“常规”	定义一般电子邮件通知设置。
“管理员电子邮件”	在发生隔离操作或警报等事件时通知 Microsoft Exchange 管理员。 • 将电子邮件通知发送给多个用户，使用分号 (;) 作为分隔符。 • 将电子邮件通知发送到分发列表 (DL)，指定 DL 的 SMTP 地址。
“发件人电子邮件”	指定通知电子邮件“从”字段的发件人电子邮件地址。 McAfee 建议不要修改“发件人电子邮件”地址，因为软件处于多种目的创建和使用该地址。 如果更改此电子邮件地址并且未在 Microsoft Exchange 中启用“匿名”接收连接器，则不会收到产品通知。
“启用任务结果通知”	发送包含按需扫描和更新任务结果的电子邮件。 该电子邮件为 HTML 格式并且与用于界面中的“任务结果”窗口具有相同的数据和格式。 该功能可通过此选项启用/禁用。 默认情况下，此功能已禁用。
“高级”	定义高级通知设置，如指定个人电子邮件地址和每个扫描程序或过滤器的主题行。
“邮件正文”	定义所有通知的通用电子邮件正文。

3 单击“应用”以保存设置。

MSME 通过不支持包含 XSS 漏洞的 HTML 标记，提高了安全性。 McAfee 建议您先从现有通知模板中删除包含 XSS 漏洞的 HTML 标记，然后再进行升级。 否则在升级后，如果想要修改包含不支持的标记的通知模板，系统会提示您从模板中删除不支持的标记或使用模板但不作修改。 有关不支持的 HTML 标记列表，请参阅 McAfee 知识库文章 KB82214。

编辑通知模板

查看或编辑发送给最终用户的通知邮件的正文。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “通知”。

2 在 “通知” | “模板”选项卡中，您可以使用以下选项：

表 5-8 选项定义

选项	定义
“模板”	查看特定最终用户的通知模板。可用选项包括： • “内部发件人” • “内部收件人” • “外部发件人” • “外部收件人” 您可以为每一种用户类型定义具体的通知文本。
“主题”	指定通知电子邮件的主题行。默认情况下，通知主题为 “McAfee Security for Microsoft Exchange 警报”。

表 5-8 选项定义 *（续）*

选项	定义
“通知文本”	根据选定的 “模板”，预览通知电子邮件的正文。通知文本包含隔离的项目的相关信息，如日期和时间、主题、已采取的操作等。
“编辑”	使用 HTML 以纯文本格式修改通知文本。根据公司要求编辑通知后，单击 “保存”应用更改。

3 单击 “应用”保存设置。

您现已成功查看或修改通知模板。有关可用通知字段的更多信息，请参阅 “可以使用的通知字段”部分。

可以使用的通知字段

使用这些字段，将其包括在通知中。例如，如果您需要检测到的项目的名称及其被检测到时所采取的操作，可使用 **%vrs%** 和 **%act%**（位于 “设置和诊断” | “通知” | “模板”页面）。

表 5-9 可以使用的通知字段

通知字段选项	说明
%dts%	日期和时间
%sdr%	发件人
%ftr%	过滤器
%fln%	文件名
%rul%	规则名称
%act%	已采取的操作
%fdr%	文件夹
%vrs%	检测名称
%trs%	状态（训练状态）
%tik%	票证号
%idy%	扫描方式
%psn%	策略名称
%svr%	服务器
%avd%	防病毒 DAT
%ave%	防病毒引擎
%rpt%	收件人
%rsn%	原因
%sbj%	主题
%ssc%	垃圾邮件分数
%ase%	反垃圾邮件引擎
%asr%	反垃圾邮件规则

启用产品健康状况警报

在产品的特定任务失败时立即发送通知或每天发送通知给 Microsoft Exchange 管理员。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “通知”。

2 在 “通知” | “产品健康状况警报”选项卡中，您可以使用以下选项：

表 5-10 选项定义

选项	定义
“启用”	启用在产品特定任务失败时发送产品健康状况警报通知给管理员。
“向 ePolicy Orchestrator 发出警报”	在产品特定任务失败时 向管理 MSME 服务器的 McAfee ePolicy Orchestrator 服务器（对该发出警报。
“向管理员发出警报”	将产品健康状况警报发送到 “设置和诊断”	“通知”	“设置”	“管理员电子邮件” 下指定的电子邮件地址。
“发生以下情况时通知”	在任何所选的产品特定任务失败时通知管理员。您可以选择以下选项，以将产品健康状况警报发送给管理员： 以下选项可能根据您的 Exchange Server 角色而异。 • “下载 DAT/防病毒引擎失败” • “下载反垃圾邮件规则失败” • “加载防病毒引擎失败” • “加载 TransportScan 模块失败” • “加载 VSAPI 模块失败” • “RPCServ 进程意外退出” • “DLLHost 进程意外退出” • “Postgres 进程失败” • “Postgres 无法隔离或记录检测” • “Postgres 数据库初始化失败” • “Postgres 无法存储记录” • “按需扫描失败” • “数据库磁盘空间低于阈值” • “产品服务无法启动” • “McAfee Global Threat Intelligence 文件信誉扫描失败”
“即时”	任务失败后立即向管理员发送通知。
“每日”	任务失败后在每天的特定时间向管理员发送通知。

3 单击 “应用” 保存设置。

您现已成功启用 “产品健康状况警报” 功能。

反垃圾邮件设置

定义垃圾电子邮件文件夹的设置，以转发边缘传输或集线器传输服务器上检测到的垃圾邮件。 同时启用或禁用 McAfee GTI 邮件信誉的设置以及 McAfee GTI IP 信誉功能。

表 5-11 选项定义

选项	定义
“系统垃圾文件夹地址”	指定将接收所有归类为垃圾邮件的电子邮件的电子邮件地址。
“McAfee GTI 邮件信誉”	McAfee Global Threat Intelligence 邮件信誉是 McAfee 提供的全面、实时、基于云的邮件和发件人信誉服务，帮助 MSME 保护 Exchange 服务器抵御已知和新兴的邮件威胁（例如垃圾邮件）。 MSME 每天会接收上百万条电子邮件查询，获取邮件内容的指纹（相对内容本身，出于隐私原因）并进行多维度分析。 将邮件信誉与垃圾邮件发送模式和 IP 行为等因素相结合，可确定问题邮件属于恶意邮件的可能性。 该分数不仅基于 Sensor 查询 McAfee 云收集的信息以及 McAfee Labs 研究者和自动工具执行的分析，而且还涉及文件、网页和网络威胁数据的相关矢量信息。 MSME 使用该分数根据 “策略管理器”	“网关” 策略确定相关操作。
“启用”	根据电子邮件的邮件信誉分数在网关处阻止电子邮件。

表 5-11 选项定义 （续）

选项	定义
“在反垃圾邮件后执行邮件信誉”	在根据本地 McAfee GTI 策略执行扫描后执行 MSME 邮件信誉。
“邮件信誉阈值”	根据邮件信誉分数，指定阈值以阻止电子邮件。 默认情况下，该数值设置为 80。
“采取的操作”	选择： • “Drop and Quarantine（丢弃并隔离）” — 丢弃电子邮件并在数据库中对其进行隔离。电子邮件由于该设置而被丢弃时，不会通知发件人该电子邮件的传递状态。 • “反垃圾邮件引擎分数线” — 将 McAfee GTI 检测到的邮件信誉分数发送至反垃圾邮件引擎。只有启用“在反垃圾邮件后执行邮件信誉”选项后，才能使用该选项。
“McAfee GTI IP 信誉”	IP 信誉作为 Exchange 环境的首道防线，保护 Exchange 服务器抵御不安全的电子邮件源。 它可让您利用 McAfee Global Threat Intelligence 收集的威胁信息，根据源 IP 地址，在网关阻止电子邮件，从而放置数据损坏和偷窃。
“启用”	根据来源 IP 地址在网关处阻止电子邮件。
“IP 信誉阈值”	指定根据 IP 信誉分数阻止电子邮件的阈值。 该操作将应用到信誉分数高于选定阈值的所有 IP 地址。 将允许其他所有电子邮件通过。 您可以修改注册表值，将“反垃圾邮件设置”中 “IP 信誉阈值”阻止的合法 IP 地址加入白名单。 将 IP 地址加入白名单后，列入白名单的 IP 地址发送的电子邮件将被允许通过，无论其信誉分数为何。 **重要**：将 IP 地址添加到白名单会仅替代 “IP 信誉阈值”设置。 MSME 会进一步扫描电子邮件中的损坏或加密内容、文件过滤器、内容扫描、URL 信誉和防恶意软件。 如果检测到项目，会根据产品配置采取操作。 在将 IP 地址列入白名单前，McAfee 建议您通过 www.trustedsource.org 验证 IP 地址的信誉分数，从而了解其合法性。 如果任何邮箱被列入白名单的 IP 地址感染，McAfee 概不负责。 有关使用注册表为 IP 代理配置 IP 地址白名单的更多信息，请参见 McAfee 知识库文章 KB82216。
“采取的操作”	根据来源 IP 地址的信誉分数，在以下选项中选择一项要对电子邮件采取的操作： • “丢弃连接并记录” — 丢弃检测到的 IP 地址发送的电子邮件，然后记录对项目采取的操作。 • “拒绝连接并记录” — 拒绝源 IP 地址的电子邮件，通知发件人并记录对项目采取的相关操作。
“SPF 过滤器”	保护您的系统免遭欺诈电子邮件侵扰，并且您可以针对硬故障和软故障邮件配置一些操作。

检测到的项目设置

指定存储库设置以存储 MSME 检测到的隔离的项目。

使用以下选项配置和管理隔离存储库：

- “McAfee Quarantine Manager” — 在 MQM 服务器上隔离检测到的项目。
- “本地数据库” — 在本地 MSME 服务器中隔离检测到的项目。

使用 McAfee Quarantine Manager 隔离

指定存储库设置以隔离 McAfee Quarantine Manager 服务器上 MSME 检测到的隔离项目。

McAfee 产品（例如 McAfee Security for Microsoft Exchange 和 McAfee Email Gateway）使用预分配的端口号将检测信息发送至 McAfee Quarantine Manager。 McAfee Quarantine Manager 随后使用默认的相同端口号，将检测到的电子邮件配置信息释放或发送到 McAfee 产品。

McAfee Security for Microsoft Exchange 和 McAfee Quarantine Manager 用户界面中提到的通信端口应相同。

您可以使用 McAfee Quarantine Manager 将隔离和反垃圾邮件功能整合到一起。 您可以从一个中心点对已隔离的电子邮件和文件进行分析并采取操作。

本手册并未提供有关安装或使用 McAfee Quarantine Manager 软件的详细信息。 更多信息，请参阅 McAfee Quarantine Manager 产品文档。

任务

1 在 <server 1> 上安装 McAfee Security for Microsoft Exchange 软件。

2 在 <server 2> 上安装支持的 McAfee Quarantine Manager 软件。

3 从 <server 1> 启动 MSME 用户界面。

4 在产品用户界面中，单击“设置和诊断” | “检测到的项目”。

此时会出现“检测到的项目”页。

5 在 “McAfee Quarantine Manager”部分，选择 “启用”。

6 在“通信模式”中，选择模式。

- “RPC” — 远程过程调用 (RPC) 是一种通信机制，需要与 McAfee Quarantine Manager 服务器不间断地连接通信。 如果与 McAfee Quarantine Manager 服务器发送通信故障，隔离和释放等过程会中断。
- “HTTP” — 一种与 McAfee Quarantine Manager 服务器进行通信的无状态通信机制。 如果与 McAfee Quarantine Manager 服务器发生通信故障，项目会存储在本地数据库中，直到连接还原为止。 MSME 会三次尝试将隔离的项目发送至 MQM。 如果所有三次尝试都失败，会创建产品日志条目并且项目会存储在本地数据库中。
- “HTTPs” — 一种安全的 HTTP 通信机制，数据以加密格式进行传输。

McAfee 建议您使用 HTTP/HTTPs 通信通道，因为无状态连接可确保软件能与 McAfee Quarantine Manager 进行无缝通信。

7 在 “IP 地址”中，指定 MQM 服务器的 IP 地址。

8 在“端口”和“回拨端口”，指定默认值。

通信模式	端口值	回拨端口	黑白名单更新间隔（小时）
RPC	49500	49500	-
HTTP	80	-	4
HTTPs	443	-	4

仅在 McAfee Quarantine Manager 服务器上配置了不同端口值时，修改该值。

9 单击“应用”保存设置。

您已成功配置 MSME 服务器开始隔离 MQM 服务器上检测到的项目。

使用本地数据库隔离

指定存储库设置以将 MSME 在本地 MSME 服务器上检测到的项目隔离到 PostgreSQL 数据库。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “检测到的项目”。

将显示 “检测到的项目”页面。

2 在 “本地数据库”部分，您可以使用以下选项：

表 5-12 选项定义

选项	定义
“指定数据库位置”	启用 “数据库位置”存储由 MSME 检测到的已隔离的项目。
“数据库位置”	指定数据库位置路径，该位置可存储 MSME 检测到的项目。您可以选择以下选项： • “<安装文件夹>” — 在 MSME 安装目录下创建数据库子文件夹。 • “<系统驱动器>” — 在 C:\Windows\system32 目录下创建数据库子文件夹。 • “<Program Files>” — 在 C:\Program Files (x86) 目录下创建数据库子文件夹。 • “<Windows 文件夹>” — 在 C:\Windows 目录下创建数据库子文件夹。 • “<数据文件夹>” — 在 C:\ProgramData\ 目录下创建数据库子文件夹。 • “<完整路径>” — 将 MSME 数据库存储到指定的完整路径中。 在下拉列表旁边的字段指定子文件夹路径。默认子文件夹路径指定为： McAfee \MSME\Data\
“Maximum item size (MB)（最大项目大小 [MB]）”	指定可存储在数据库上的隔离项目的最大大小。您可以指定 1 到 999 之间的值，其中默认值为 100。
“Maximum query size (records)（最大查询大小 [记录数]）”	指定您可以从 “检测到的项目”页面查询的记录或隔离的项目的最大数量。您可以指定 1 到 20000 之间的值，其中默认值为 1000。
“Maximum item age (days)（项目最长存储时间 [天]）”	指定在标记删除前，项目在本地隔离数据库中存储的最大天数。您可以指定 1 到 365 之间的值，其中默认值为 30。
“Disk size check interval (Minute)（磁盘大小检查时间间隔 [分钟]）”	指定 MSME 检查可用磁盘空间的频率。您可以指定 6 到 2880 之间的值，其中默认值为 6。
“Disk space threshold (MB)（磁盘空间阈值 [MB]）”	指定应向管理员发送低磁盘空间警告通知的阈值。您可以指定 1 到 512000 之间的值，其中默认值为 2048。 确保 “Database diskspace goes below the threshold（数据库磁盘空间低于阈值）”（位于 “设置和诊断”	“通知”	“产品健康状况警报”	“发生以下情况时通知”下）已启用。
“Purge of old items frequency（旧项目清除频率）”	指定将标记删除的旧项目从 MSME 数据库中删除的频率。默认值设置为 “每月”。

表 5-12 选项定义 *（续）*

选项	定义
“Optimization frequency（优化频率）”	恢复已删除的数据库记录占用的磁盘空间。如果您计划了清除任务，将根据“Maximum item age (days)（项目最长存储时间 [天]）”下设置的值删除旧记录。删除这些旧记录后， MSME 将仍然使用在 “Disk space threshold (MB)（磁盘空间阈值 [MB]）”字段下指定的磁盘空间，即使隔离数据库已达到大小限制。要优化和压缩数据库，请计划优化任务。默认值设置为 “每月”。 请始终在执行清除任务几小时后计划优化任务。
“编辑计划”	修改清除或优化任务的计划。修改计划后单击 “保存”。

3 单击 “应用”保存设置。

您现已成功配置 MSME 服务器，可开始将检测到的项目隔离到本地数据库。

用户界面首选项设置

定义 “信息显示板”中的设置，如刷新率、报告设置、图形的单位标尺、报告时间间隔、图形和图表设置。

配置信息显示板设置

配置 “信息显示板”中的设置，如统计信息、图形的单位标尺、 “近期已扫描的项”中可查看的项目以及状态报告时间间隔。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “User Interface Preferences（用户界面首选项）”。

将显示 “User Interface Preferences（用户界面首选项）”页面。

2 单击 “Dashboard Settings（信息显示板设置）”选项卡。您可以使用以下选项：

表 5-13 选项定义

选项	定义
“自动刷新”	指定是否要自动刷新 “信息显示板”	“统计”计数器上显示的信息。
“刷新率（秒）”	指定刷新信息显示板上的信息的时间间隔（以秒为单位）。您可以指定 30 到 3600 之间的值，其中默认值为 60。
“Maximum recently scanned items（最近扫描的最大项目数）”	指定在 “信息显示板”	“报告”	“近期已扫描的项”部分中显示的最大项目数。您可以指定 10 到 100 之间的值，其中默认值为 10。
“Graph scale (units)（图形标尺 [单位]）”	指定在 “消息显示板”	“图形”部分生成的柱状图的标尺的计量单位。您可以指定 100 到 500 之间的值，其中默认值为 100。
“Number of hours to report for（要报告的小时数）”	指定生成状态和配置报告等报告的报告生成时间间隔（以小时为单位）。您可以指定 1 到 24 之间的值，其中默认值为 7。

3 单击“应用”保存设置。

配置图形和图表设置

配置 “信息显示板” | “图形”部分的设置以强化图形和图表设置。

任务

1 单击 “设置和诊断” | “User Interface Preferences（用户界面首选项）”。

2 单击 “Graph and Chart Settings（图形和图表设置）”选项卡。您可以使用以下选项：

表 5-14 选项定义

选项	定义
“3D”	指定是否要将信息显示板图形显示为三维 (3D) 图形。
“Draw transparent（绘制透明）”	指定三维柱状图中的柱形显示为实心还是透明。实心柱会挡住后面的任何柱的一部分。透过透明柱可以看到后面的其他透明柱。
“Anti-alias（消除锯齿）”	指定显示饼图时是否要使用消除锯齿技术。使用消除锯齿时，饼图具有较平滑的曲线。如果不使用消除锯齿，饼图曲线显示粗糙。
“Explode pie（分解饼图）”	指定扇形是保留在饼图的圆形中，还是显示为分解的扇形。
“Pie angle (degrees)（饼图角度 [度]）”	指定显示饼图时使用的角度。您可以指定 1 到 360 之间的值，其中默认值为 45。

3 单击“应用”保存设置。

诊断设置

确定使用 MSME 时的症状原因、问题缓解情况和所面临问题的解决方案。

在 “设置和诊断” | “诊断”页面中，您可以使用：

- “调试日志记录” — 配置调试日志记录设置，如指定调试记录级别、日志文件的最大文件大小限制和文件位置。
- “Event Logging（事件日志记录）” — 配置设置以根据信息、警告或错误捕获与产品或事件相关的日志。
- “产品日志” — 配置 MSME 产品日志文件 (productlog.bin) 的设置。对该设置所作的更改将反映在 “设置和诊断” | “产品日志” 页面上。
- “Error Reporting Service（错误报告服务）” — 配置设置以确定是否捕获系统崩溃等异常并向用户报告。

配置调试日志设置

配置相关设置以指定调试日志级别、日志文件最大文件大小限制和日志文件位置。 如果想要对产品的问题进行故障排除或将日志提交至 McAfee 技术支持进行详细分析，请使用以下设置。

配置 “Debug Log（调试日志）”设置以进行故障排除，仅在一段有限的时间内适用。在捕获足够的用于进行故障排除的日志后，将 “级别”值设置为 “无”。不加选择地使用调试日志记录会耗尽硬盘空间，从而影响服务器的整体性能。应按照授权人员（McAfee 技术支持工程师）的建议将其启用一段有限的时间。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “诊断”.

将显示 “诊断”页面。

2 在“调试日志记录”选项卡中，可以使用：

表 5-15 选项定义

选项	定义
“级别”	启用或禁用调试日志记录并指定调试日志文件中捕获的信息级别。 您可以选择以下选项： • “无” — 禁用调试日志记录。 • “低” — 记录调试日志文件中的关键事件，如错误、例外和函数返回值。如果想使调试日志文件较小，请选择此选项。 • “中” — 记录 “低”状态下提及的事件和可能对技术支持团队有帮助的其他信息。 • “高” — 记录调试日志文件中的所有关键错误、警告和调试消息。其中包含产品进行的所有活动的信息。这是产品支持的详细级别最高的日志记录。
“启用大小限制”	如果要指定每个调试日志文件的最大文件大小限制，可选择此项。
“指定最大文件大小”	指定调试日志文件的大小。 您可以指定介于 1 KB 到 2000 MB 之间的值。 如果调试日志文件超出指定的文件大小，较早事件将因循环日志记录而被重写，通过删除最旧的日志条目将新日志条目添加到文件。
“启用调试日志记录”	如果要修改默认调试文件日志记录的位置，可选择此项。 如果该选项已禁用，调试日志文件将存储在 <Install Folder>\bin\debuglogs 默认目录下。
“指定文件位置”	指定调试日志文件位置路径，可存储 MSME 触发的事件。 您可以选择以下选项： • “<安装文件夹>” — 在 MSME 安装目录下创建调试日志文件。 • “<系统驱动器>” — 在 C:\Windows\system32 目录下创建调试日志文件。 • “<Program Files>” — 在 Windows C:\Program Files (x86) 目录下创建调试日志文件。 • “<Windows 文件夹）>” — 在 C:\Windows 目录下创建调试日志文件。 • “<数据文件夹>” — 在 C:\ProgramData\ 目录下创建调试日志文件。 • “<完整路径>” — 将调试日志文件存储在相邻文本框中指定的完整路径下。 要将调试日志文件存储到自定义位置或子文件夹，请在下拉列表旁边的字段中指定子文件夹名称或路径。

确保收集调试日志的文件夹对 NETWORK SERVICE 帐户有“写入”权限。

3 单击“应用”以保存设置。

有关生成按需扫描任务的 Exchange Web 服务 (EWS) 包装日志的更多信息，请参见 McAfee 知识库文章 KB82215。

您现已成功配置调试日志设置，可将其用于进行故障排除。

配置事件日志记录设置

配置设置以记录“产品日志” 和 Windows 事件查看器中的 MSME 事件类型。

事件是由 MSME 监控的可能执行的操作。 “Event Logging（事件日志记录）”提供有助于进行诊断和审核的信息。事件的不同分类包括：

- 错误
- 信息
- 警告

这允许系统管理员更轻松地获取有关所发生问题的信息。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “诊断”。

将显示 “诊断”页面。

2 单击 “Event Logging（事件日志记录）”选项卡。您可以使用以下选项：

表 5-16 选项定义

选项	定义
“产品日志”	记录 “产品日志” 中的 MSME 事件。这些事件可在 “设置和诊断”	“产品日志”	“查看结果”部分中进行查看。
“事件日志”	记录 Windows 事件查看器下的 MSME 事件。 要查找 Windows 事件查看器中的与 MSME 相关的事件： 1 请转到 “事件查看器（本地）”	“Windows 日志”	“应用程序”。 2 在 “应用程序”面板，与产品相关的事件在 “源”列下显示为 “MSME”。
“Write information events（写入信息事件）”	记录分类为 “信息”的事件。
“Write warning events（写入警告事件）”	记录分类为 “警告”的事件。
“Write error events（写入错误事件）”	记录分类为 “错误”的事件。

3 单击“应用”保存设置。

配置产品日志设置

通过指定生成产品日志所需的参数， 配置“设置和诊断” | “产品日志”页面中的设置。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “诊断”.

将显示 “诊断”页面。

2 单击 “产品日志”选项卡。您可以使用以下选项：

表 5-17 选项定义

选项	定义
“位置”	配置存储产品日志的位置。选择 “启用”指定自定义位置。
“指定数据库位置”	指定可存储产品日志事件的产品日志文件位置的路径。您可以选择以下选项： • “<安装文件夹>” — 在 MSME 安装目录下创建产品日志文件。 • “<系统驱动器>” — 在 C:\Windows\system32 目录下创建产品日志文件。 • “<Program Files>” — 在 Windows C:\Program Files (x86) 目录下创建产品日志文件。 • “<Windows 文件夹>” — 在 C:\Windows 目录下创建产品日志文件。 • “<数据文件夹>” — 在 C:\ProgramData\ 目录下创建产品日志文件。 • “<完整路径>” — 将产品日志文件存储在相邻文本框中指定的完整路径下。 要将产品日志文件存储到自定义位置或子文件夹，请在下拉列表旁边的字段中指定子文件夹名称或路径。

表 5-17 选项定义 *（续）*

选项	定义
“文件名”	指定不同的文件名以存储产品日志。选择 “启用” 指定自定义文件名。
“指定数据库文件名”	为产品日志指定自定义文件名。默认文件名为 productlog.bin（在 <安装文件夹>\Data\ 目录下）。 如果修改默认产品日志文件名或路径，“设置和诊断”	“产品日志” 页面中的日志条目将重设，并且不会显示较旧的日志条目。
“大小限制”	为产品日志文件指定其他大小限制。选择 “启用数据库大小限制” 指定自定义文件大小。
“指定最大数据库大小”	指定产品日志文件可达到的大小。您可以指定介于 1 KB 到 2000 MB 之间的值。 如果产品日志文件超出指定的文件大小，较旧的日志事件将因循环日志记录而被重写，这将通过删除最旧的日志条目来将新日志条目添加到文件。
“Limit age of entries（限制条目存在时间）”	在设定的时间段后删除产品日志条目。
“指定条目的最长存在时间”	指定条目删除前应在产品日志文件中保留的天数。您可以指定介于 1 到 365 之间的值。
“查询超时”	限制应答产品日志查询时允许的时长。选择 “启用” 指定持续时间。
“指定查询超时（秒）”	指定应答产品日志查询时允许的最大秒数。您可以指定介于 1 到 3600 之间的值。

3 单击 “应用” 保存设置。

您现已成功配置 “产品日志” 页面的设置。

配置错误报告服务设置

配置设置以向 McAfee 报告产品相关错误或异常。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “诊断”。

将显示 “诊断” 页面。

2 单击 “Error Reporting Service（错误报告服务）” 选项卡。您可以使用以下选项：

表 5-18 选项定义

选项	定义
“启用”	启用或禁用错误报告服务。
“捕获异常”	捕获有关异常事件（如系统崩溃）的信息。
“Report exceptions to user（向用户报告异常）”	指定是否应向管理员报告异常情况。

3 单击 “应用” 保存设置。

查看产品日志

使用有关事件、信息、警告和错误的日志条目查看产品的健康状况。例如，您可以查看任务启动或结束时的信息和产品服务错误等。

您可以使用可用的搜索过滤器查找感兴趣的日志条目。

要修改产品日志查询页面的相关设置，请转至 “设置和诊断” | “诊断” | “产品日志”。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “产品日志”。将显示 “产品日志”页面。

2 在 “产品日志”部分，您可以使用以下选项：

表 5-19 选项定义

选项	定义
“ID”	指定标识特定产品日志条目的编号。例如，如果仅需查看 ID 大于 2000 的产品日志，可指定：200*
“级别”	从下拉列表中选择 “信息”、 “警告”或 “错误”，这取决于您要查看的类型。
“说明”	指定相关的说明。例如，如果您要根据服务开始或停止查看日志，可键入 *service*
“所有日期”	包括基于产品日志文件中的条目的所有日期的事件。
“日期范围”	根据需要，搜索指定日期范围内的事件。在此您可以通过参数 “开始”和 “结束”指定日期、月份、年份和时间。您也可以使用日历图标指定日期范围。
“清除过滤器”	恢复默认搜索设置。
“导出到 CSV 文件”	将关于搜索返回的所有事件的信息以 .CSV 格式导出并保存。如果日志中有大量的事件，您可以使用此选项将这些事件下载为 CSV 格式的文件，稍后在 Microsoft Excel 中生成自定义报告，而无需在多个页面中导航。 • 如果您在 CSV 文件的搜索结果中未找到特定字段，请确保启用了 “要显示的列”选项中的所需字段。 • 使用 Microsoft Excel 中的 “导入数据”选项，打开不同位置的 CSV 文件。

3 单击 “搜索”。

可存储在产品日志中的最大记录数取决于日志文件大小。

与您的搜索标准相匹配的事件列表显示在 “查看结果”部分中。

配置 DAT 设置

指定系统中可保留的旧 DAT 的数量。

DAT 文件是检测定义文件（也称为特征码文件），用于标识防病毒和/或防间谍软件检测的代码以修复病毒、特洛伊木马程序以及可能不需要的程序 (PUP)。有关 .DAT 文件上的词汇信息，请转至： http://www.mcafee.com/us/mcafee-labs/resources/threat-glossary.aspx#dat

任务

1 在产品的用户界面中，单击 “设置和诊断” | “DAT 设置”。

将显示 “DAT 设置”页面。

2 使用 “Maximum number of old DATs（旧 DAT 的最大数量）” 可指定在常规更新过程中系统中应保留的 DAT 生成的最大数量。 MSME 将最新 DAT 与旧 DAT 一起保留在 <安装文件夹>\bin\DATs 目录下。只要进行新的 DAT 更新， MSME 都会验证可用 DAT 的数量。如果可用 DAT 数量超出 DAT 保留值，将删除最旧的 DAT。您可以指定 3 到 10 之间的值，其中默认值为 10。

3 单击 “应用” 保存设置。

导入和导出配置设置

配置相关设置以导出现有 MSME 配置（设置和策略）以在其他 MSME 服务器上导入和使用。 同时导入指定自动更新下载位置的站点列表。

在产品的用户界面中，单击 “设置和诊断” | “导入和导出配置”。在 “导入和导出配置” 页面中，您可以使用以下选项卡：

- “配置” — 导出、导入或还原产品设置。

表 5-20 配置选项卡 — 选项定义

选项	定义
“导出”	复制该服务器的 MSME 配置（设置和策略）并将其保存到可被其他 MSME 服务器导入的位置。默认 MSME 配置文件为 McAfeeConfigXML.cfg。
“还原默认值”	将产品的 MSME 设置重置回最佳性能。
“还原增强”	将产品的 MSME 设置重置回最大保护。
“浏览”	找到要导入的配置文件 (McAfeeConfigXML.cfg)。
“导入”	将其他 MSME 服务器的设置应用到该服务器。 例如，在 5 台系统上安装 MSME 8.5： **1** 在系统 1 上安装 MSME。 **2** 根据需要配置相关设置。 **3** 将配置导出为 cfg 文件。 有关导入配置的更多信息，请参见 “使用向导安装软件” 中的步骤 10。 导入设置时，两个产品版本必须相同。 例如，不得将 MSME 7.6 或 8.0 服务器的设置导入 MSME 8.5 服务器。

- “SiteList” — 导入 Sitelist，指定自动更新下载的位置。

表 5-21 SiteList 选项卡 — 选项定义

选项	定义
“浏览”	找到要使用的 Sitelist 文件 (SiteList.xml)。
“导入”	应用文件中指定的站点列表配置相关设置，以下载 DAT 更新。

导出现有 MSME 配置

导出 MSME 服务器的配置，并将其保存到一个位置，以便其他 MSME 服务器通过此位置进行导入。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “导入和导出配置”。

将显示 “导入和导出配置” 页面。

2 单击 “配置” 选项卡。

3 单击“导出”。

4 指定保存配置文件的位置。配置文件的默认名称为 McAfeeConfigXML.cfg。

5 单击 “保存”。

您现已成功将现有 MSME 设置和策略导出到配置文件，该配置文件可供其他 MSME 服务器进行导入。

从其他 MSME 服务器导入配置

将其他服务器的 MSME 配置应用至此 MSME 服务器。

您可以通过两种方式导入配置：

- 安装软件时导入配置。
- 安装软件后导入配置文件，即使用“设置和诊断”页面中的“导入和导出配置”选项导入。

- 导入设置时，两个产品版本必须相同。 例如，千万不要将 MSME 服务器设置从 MSME 7.6 服务器导入到 MSME 8.0 服务器中。
- 建议您使用具有相同 Exchange 角色的 MSME 服务器导入设置。

任务

1 在产品的用户界面中，单击 “设置和诊断” | “导入和导出配置”。

将显示 “导入和导出配置”页面。

2 单击“配置”选项卡。

3 在 “Import Configuration（导入配置）”部分，单击 “浏览”，查找配置文件。配置文件的默认名称为 McAfeeConfigXML.cfg。

4 单击 “导入”。

将出现一个对话框， 显示“The operation completed successfully（操作已成功完成）”消息。

5 单击 “确定”。

您已成功将其他 MSME 服务器的配置设置导入此服务器。

导入站点列表

导入指定自动更新下载位置的站点列表。

Sitelist 指定下载自动更新的位置。 默认情况下，MSME 使用指向 McAfee URL 的 “SiteList Editor” 进行自动更新。

如果 MSME 服务器由 McAfee ePO 托管，则使用 ePolicy Orchestrator 中的 Sitelistis 执行自动更新。 如果未使用 ePolicy Orchestrator 托管 MSME 服务器，创建将 MSME 服务器指向本地存储库的 Sitelist。

可以使用 McAfee AutoUpdate Architect 软件或 McAfee ePO 创建备用 Sitelist。

任务

1 单击“设置和诊断” | “导入和导出配置”。此时将显示“导入和导出配置”页。

2 单击 “SiteList”选项卡。

3 在“导入 SiteList” 部分，单击“浏览”以找到 Sitelist 文件 SiteList.xml。 该文件包含存储库设置的相关信息，如存储库名称、服务器 URL 等。

您可以在 C:\ProgramData\McAfee\Common FrameWork\ 目录下找到 SiteList.xml 文件。 “开始” | “所有程序” | “McAfee” | “Security for Microsoft Exchange” 下的 “SiteList 编辑器”使用该文件以显示应用程序中的存储库设置。

4 单击 “导入”。

将出现一个对话框， 显示“The operation completed successfully（操作已成功完成）”消息。

5 单击 “确定”。

您现已成功导入指向新存储库位置的站点列表，可下载产品更新。

配置反垃圾邮件代理服务器设置

如果组织使用代理服务器连接至互联网，请配置以下设置，这样 MSME 可下载反垃圾邮件规则。

软件还可使用该代理获取 IP 信誉、邮件信誉以及从 GTI 服务器下载本地 URL 数据库。

只有安装了 McAfee Anti-Spam 插件组件后，才能使用该功能。

任务

1 在产品的用户界面中，单击“设置和诊断” | “代理服务器设置”。

此时将显示“代理服务器设置”页。

2 选择“使用代理”。 在“代理服务器详细信息”部分，可以使用：

表 5-22 选项定义

选项	定义
“IP 地址”	指定代理服务器的 IP 地址。
“端口”	指定用于访问互联网的通信端口。
“身份验证详细信息”	指定身份验证类型。 您可以使用： • “匿名” — 不指定任何身份验证详细信息访问代理服务器计算机。 • “NTLM” — 使用 NT LAN Manager 凭据访问代理服务器计算机。 • “基本身份验证” — 为用户提供访问代理服务器计算机的系统“用户名”和“密码”。在“确认密码”中，重复输入密码。

3 单击“应用”保存设置。

6 程序维护

执行产品维护任务，例如修改安装、修复、卸载、还原默认设置、清除和优化数据库。

目录

修改安装

根据需要更改 MSME 程序，并更改在计算机上安装程序功能的方法，或在已修改 Exchange Server 角色情况下进行更改。

您还可以通过在“控制面板” | “程序和功能” | “卸载程序”控制台中单击“卸载/更改”来修改 MSME 安装。

任务

1 在包含安装文件的文件夹中，双击 setup_x64.exe。

2 单击欢迎屏幕中的“下一步”。

此时将显示“程序维护”屏幕。

3 选择“修改”，然后单击“下一步”。

4 选择需要修改的程序功能并单击“下一步”。

5 选择“我接受许可协议的条款”，然后单击“下一步”。

6 单击“安装”完成安装并具有修改后的程序功能。

7 安装结束时单击“完成”。

恢复默认设置

将产品恢复为默认设置并实现最佳性能。

任务

1 在产品的用户界面中，单击“设置和诊断” | “导入和导出配置”。此时将显示“导入和导出配置”页。

2 在“配置”选项卡中，单击“恢复默认值”。

恢复默认设置将删除配置的所有策略设置和子策略。建议您备份现有设置，以便稍后恢复设置。

此时将显示一个对话框，让您确认设置。

3 单击“确定”。

此时将显示一个对话框，确认默认配置设置已应用。

4 单击“确定”。

您现已成功将 MSME 服务器恢复为默认配置设置，以便实现最佳性能。

清除和优化

从数据库删除标记为要删除的旧项目，使用优化任务恢复已删除的数据库记录占用的磁盘空间。

任务

1 在产品用户界面中，单击“设置和诊断” | “检测到的项目”。

此时会出现“检测到的项目”页。

2 在“本地数据库”部分中，可以使用：

- “Purge of old items frequency（旧项目清除频率）” — 指定从 MSME 数据库删除标记为要删除的旧项目的频率。默认值设置为 “每月”。
- “Optimization frequency（优化频率）” — 恢复已删除的数据库记录占用的磁盘空间。如果您计划了清除任务，将根据 “Maximum item age (days)（项目最长存储时间 [天]）”下设置的值删除旧记录。删除这些旧记录后， MSME 将仍然使用在 “Disk space threshold (MB)（磁盘空间阈值 [MB]）”字段下指定的磁盘空间，即使隔离数据库已达到大小限制。要优化和压缩数据库，请计划优化任务。默认值设置为 “每月”。

请始终在执行清除任务几小时后计划优化任务。

3 单击 “编辑计划”以修改计划。

这些任务应定期执行以保持数据库中有足够的可用空间。

7 故障排除

确定使用 MSME 时的问题并进行故障排除。了解可用的性能计数器以及与本产品相关联的重要注册表项。

目录

默认和增强配置设置

根据您的需要，可以配置 MSME 执行最佳性能或最大保护。

若要修改 MSME 配置设置，转至“设置和诊断” | “导入和导出配置”。 您可以使用：

- “还原默认” — 配置 MSME 获得最佳性能。
- “还原增强” — 配置 MSME 获得最大保护。

表 7-1 默认和增强配置之间的差异

功能	默认	增强
邮件信誉	禁用	启用
IP 信誉	禁用	启用
最大嵌套级别	10	50
受密码保护的文件	允许通过	替换和隔离
受保护的文件	允许通过	替换和隔离
文件过滤器	禁用	对默认规则 (*.exe, *.com, *.bat, *.scr) 启用
加密文件	允许通过	替换和隔离
遭破坏的文件	允许通过	替换和隔离
邮件 URL 信誉	禁用	仅针对按访问扫描策略启用。

重要的注册表项

在重要性达到您的要求时创建这些注册表项。

表 7-2 MSME — 重要的注册表项

注册表项	路径	重要性
名称：DigestMail 类型：DWORD 值： 1	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\ADUserCache	保留用户别名与 SMTP 地址的缓存，当 MSME 与 MQM 集成且同一地址用于摘要邮件功能时，使用该缓存。
名称：ODUserID 类型：REG_SZ 值：[示例：<admin@domain.com>]	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\E2007	仅适用于所有 Exchange 邮箱服务器。 应该是通过产品创建的按需用户的电子邮件地址，用于与 Exchange Web 服务交互，以从 Exchange 数据库获得邮件数据。
名称：EWSUrl 类型：REG_SZ 值：https://<IP 地址>/EWS/Exchange.asmx	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\OnDemand	仅适用于 Exchange 2010 邮箱服务器。 此 URL 用于连接至由 CAS 服务器托管的 Exchange Web 服务。 该值在安装期间以及重新启动 MSME 服务后由 powershell 脚本 GetHubTxDetails.ps1 填充。
名称：SCLJunkThreshold 类型：DWORD 默认值： 4	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	仅适用于 Exchange 2010 邮箱服务器。 此为 SCL 垃圾邮件阈值，可以从 AD 检索且位于组织级别。 分数大于此值的邮件都将被视为垃圾邮件，这有助于 Exchange 2007/2010 集线器服务器上垃圾电子邮件的路由。 此值在安装期间以及某些频率之后由 powershell 脚本 GetSCLJunkThreshold.ps1 填充。
名称：IPBlackList 类型：REG_SZ 值：[例如：10.0.0.1]	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\SystemState	手动阻止通过特定 IP 地址或 IP 地址范围向贵组织发送的电子邮件，不管其 IP 信誉如何都是如此。
名称：SPFMaxTimeSec 类型：DWORD 默认值：5	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	允许 SPF 运行的最长时间。 如果时间超过定义的时间，则结果为 temperror，且会发送邮件。
名称：SPFCacheTimeoutSec 类型：DWORD 默认值：43200	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	缓存条目变为过时的持续时间。 默认持续时间为 12 小时。
名称：SPFCacheMaxEntries 类型：DWORD 默认值：5000	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	缓存中的最大条目数。

表 7-2 MSME 一 重要的注册表项 *（续）*

注册表项	路径	重要性
名称：SPFDNSTimeoutMS 类型：DWORD 默认值：1000	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	每个 DNS 请求的超时（单位：毫秒）。
名称：CacheTimeOutForNullRecords 类型：DWORD 默认值：60	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\MSME\AntiSpam	空记录（temperror 情况）的超时（单位：秒）。

仅当您安装了 McAfee Anti-Spam 组件或使用“完整安装”选项安装了软件时，才会创建注册表项 SPFMaxTimeSec、SPFCacheTimeoutSec、SPFCacheMaxEntries、SPFDNSTimeoutMS 和 CacheTimeOutForNullRecords。

8 常见问题解答

为您在安装或使用产品时可能遇到的常见情况提供解答。常见问题解答表中包含故障排除信息。

要查看与此版本相关的问题更新列表，请参阅 McAfee 知识库文章 KB76886。

目录

常规

以下是对一般常见问题的解答。

是否可以优先传递电子邮件？

否。无法优先传递，因为此为 Exchange 服务器任务。

是否仍需要启用 Exchange 服务器接收连接器的匿名访问权限？

MSME 不需要 Exchange 服务器接收连接器的匿名访问权限。 按需用户会处理这些功能。 有关配置匿名访问权限设置的更多信息，请参见 McAfee 知识库文章 KB81752。

电子邮件在集线器传输服务器上被扫描后，是否还会在邮箱服务器上对其进行扫描？

看情况。 如果在集线器服务器上扫描了电子邮件，并且该电子邮件具有相同的防病毒 (AV) 戳，则不会在邮箱服务器上进行扫描。 如果 AV 戳在 AV 供应商或引擎/DAT 版本方面存在差异，则就会在邮箱服务器上对其进行扫描。

在 Windows 2008 中，为什么应该使用“以管理员身份运行”选项打开 MSME 用户界面？

由于安全原因，MSME 将无法与 RPC 服务器进行通信。 这是因为 SID 没有与 RPC 进程进行进程间通信 (IPC) 的权限。

在哪个可执行文件下，MSME 的扫描模块会在所有 Exchange 版本中加载？

RPCServ.exe 进程加载所有扫描二进制文件。 若要查找扫描程序进程的进程 ID，请检查“任务管理器”中的命令行，并且查看具有命令参数 /EVENTNAME:Global\MSME_scanner_RPCEvent 的 RPCServ.exe 进程。

什么是最佳 MSME 配置？

它是指“增强保护”和“最佳性能”的配置。 默认配置为实现最佳性能。

如果在同一服务器上安装了 MSME 和文件级别的防病毒组件，应该排除哪些内容？

排除所有 MSME 二进制文件夹和子文件夹、Postgres 数据库、复制文件夹、Exchange 文件夹、McAfee ePO 事件文件夹以及产品日志。

在哪里获取有关电子邮件安全的更多信息？

有关电子邮件安全的产品解决方案，请参见 http://www.mcafee.com/us/products/email-and-web-security/email-security.aspx。

如何访问远程系统的产品界面？

若要访问远程 MSME 单机界面：

1 启动 “McAfee Security for Microsoft Exchange - 产品配置”。

2 在“更改服务器”菜单中，单击“新连接”。

3 在“浏览计算机”对话框中，输入远程系统的 IP 地址，然后单击“确定”

若要访问远程 MSME 网页界面：

1 启动 “McAfee Security for Microsoft Exchange - 产品配置（网页界面）”。

2 在地址栏中，输入：https://<Remote system IP Address>/MSME/0409/html/index.htm

3 出现提示时提供登录凭据。

MSME 如何与 TIE 服务器连接？

MSME 通过 Data Exchange Layer (DXL) 从 McAfee ePO 与 TIE 服务器连接。 管理 MSME 的 McAfee ePO 还应该管理 TIE 服务器。

如何在 MSME 中配置 TIE 服务器？

您无法直接从 MSME 配置 TIE 服务器。 但是，管理 MSME 的 McAfee ePO 服务器还应该管理 TIE 服务器。有关将 TIE 服务器与 McAfee ePO 集成的相关信息，请参见“McAfee Threat Intelligence Exchange 产品手册”。

策略管理器

以下是对“策略管理器”功能常见问题的解答。

如何创建和使用电子邮件策略？

始终使用 SMTP 地址在网关服务器上创建策略，以及使用 Active Directory (AD) 组在邮箱服务器上创建策略。在邮箱服务器上，根据 SMTP 地址设计策略会非常费时，因为产品无法获得 SMTP 地址并且为了解决这一问题，会进行 AD 查询。 进行此操作会降低邮箱服务器的性能。

策略中的域名是否影响性能？

是。 有关详细解释，请参阅上一问题“如何创建和使用电子邮件策略”。

策略优先级如何发挥作用？

基于解决方法的优先级满足子策略后，就不会对下一个策略进行评估。

具有多个策略是否有帮助，这是否会影响服务器性能？

是的，会影响性能。 策略评估期间，如果第一个子策略不满足并评估了下一个策略，则可能需要进行 AD 查询，进而导致性能降低。

如何配置 MSME 在精确级别阻止可执行文件？

您可以使用“文件过滤规则”选项执行此操作。 以如何过滤 Windows 可执行文件等特定执行文件为例。

1 在产品用户界面中，单击“策略管理器” | “按访问（主策略）”。

2 在“核心扫描程序”下，单击“文件过滤”并启用该选项。

3 在“选项（核心反垃圾邮件设置）”下，单击“编辑”。

4 在“可用规则”下拉列表中，选择“<创建新规则...>”。

5 指定规则名称，并在“文件类别过滤”下选择“启用文件类别过滤”。

6 从“文件类别”列表中，选择“其他特定格式”。

7 从“子类别”列表中，选择“Windows 可执行文件”。

8 单击“保存”。

什么文件类型会被检测为打包程序或 PUPs，该设置可从哪里进行控制？

打包程序和 PUPs 属于按类别检测到的恶意内容类别。 打包程序通常是压缩文件或使用部分加密方法打包的文件，然后在执行时会进行解压缩。

通过 MSME 用户界面中的“防病毒设置”控制此设置。

设置和诊断

以下是对“设置和诊断”功能常见问题的解答。

启用 McAfee GTI 是否会导致电子邮件延迟？

是，由于 McAfee GTI 会验证电子邮件，会产生延迟。

如何验证传输扫描程序是否会扫描垃圾电子邮件？

您可以使用以下任何方法从产品的用户界面对此进行验证：

- 从“近期已扫描的项”页面中，查看扫描的邮件并检查扫描电子邮件所使用的策略。“扫描方式”字段下应显示“网关”。
- 在“检测到的项目”数据库中，检查是否有检测到的任何垃圾邮件。 最后验证电子邮件是否未经过身份验证任务，并且记录在 MSME “调试日志记录”中。

是否可以将黑名单和白名单从一台 MSME 服务器导出到另一台？

是，可以将黑名单和白名单从一台 MSME 服务器导出到另一台。 操作方法：

1. 在产品用户界面中，单击 “策略管理器” | “网关（主策略）”。
2. 在“核心扫描程序”下，单击“反垃圾邮件”。
3. 在“选项（核心反垃圾邮件设置）”下，单击“编辑”。
4. 单击“邮件列表”选项卡，然后单击“导出”以将所有列入黑名单和白名单的发件人/收件人保存到 CSV 文件。

McAfee Anti-Spam 插件组件

以下是对 Anti-Spam 插件组件常见问题的解答。

如何手动更新反垃圾邮件引擎？

更新注册表项，并将新引擎放到在 MSME\SystemState 注册表的 SpamEngineVersion 注册表项下的注册表中输入的指定目录。这两个值应同步。例如，如果引擎版本是 9039，则在 MSME\Bin\AntiSpam\Engine 下创建名称为 9039 的目录，并将引擎文件 masecore.dll 复制到此目录。

能否手动编辑反垃圾邮件规则？

不能。

将电子邮件地址添加到黑名单前，我应该考虑些什么？

- 确保安装了 McAfee Anti-Spam 插件组件。
- Microsoft Exchange Server 必须是传输服务器。例如，使 Exchange Server 具有边缘传输或集线器传输角色。
- 具有未经身份验证的连接，电子邮件通过此连接直接从 Internet 到达服务器。

如何将电子邮件地址加入黑名单或白名单？

1 在产品的用户界面中，单击“策略管理器” | “网关（主策略）”。

2 在“核心扫描程序”下，单击“反垃圾邮件”。

3 在“选项（核心反垃圾邮件设置）”下，单击“编辑”。

4 单击“邮件列表”选项卡，然后对所需选项（例如列入黑名单或白名单的发件人/收件人）单击“添加”。

当少数几封电子邮件未被检测为垃圾邮件时，我应该如何操作？

在“设置和诊断” | “反垃圾邮件”中，选择“启用消息信誉”，并应用设置。同时，将垃圾邮件分数调整为 51 到 79 之间的值，将有助于提高检测率。

垃圾邮件分数较低 (51 – 59) 的电子邮件仍然是合法的，因此需要对分数稍作调整。

从何处可以获得 Anti-spam 插件许可？

如果您有有效的 McAfee Anti-spam 授权号，可以从 McAfee 下载站点下载 MSMEASA.ZIP 文件。如果您没有有效的 Anti-spam 授权号，请致电 McAfee 客户服务团队。

正则表达式 (regex)

以下是对正则表达式常见问题的解答。

启用正则表达式是否会引起电子邮件延迟？

是，启用正则表达式将引起电子邮件延迟，因为内容扫描配置极耗费进程。

从哪里找到有关正则表达式的更多信息？

互联网上有多个网站提供正则表达式的信息。

现列举一二，请访问：

- http://www.regular-expressions.info/reference.html
- http://www.regexbuddy.com/regex.html

如何使用正则表达式阻止某些信用卡号码和社会保险号码？

1 在产品用户界面中，单击“策略管理器” | “共享资源”。 此时会出现“共享资源”页面。

2 在“DLP 和合规性字典”选项卡中，单击“新类别”并指定新类别名称。

3 单击“确定”。

4 在“DLP 和合规性规则”中，单击“新建”。

5 指定“规则名称”、“描述”并在“单词或短语”中指定正则表达式。

表 8-1 示例：如何验证信用卡号码

信用卡类型	正则表达式	说明
Visa	^4[0-9]{12}(?:[0-9]{3})?$	所有 Visa 信用卡号码以数字 4 开始。新信用卡号码为 16 位。旧信用卡号码为 13 位。
MasterCard	^5[1-5][0-9]{14}$	所有 MasterCard 号码以 51 与 55 之间的数字开始。全部号码均为 16 位。
American Express	^3[47][0-9]{13}$	American Express 信用卡号码以 34 或 37 开始，该号码为 15 位。
Diners Club	^3(?:0[0-5]|[68][0-9])[0-9]{11}$	Diners Club 信用卡号码以 36、38 以及 300 与 305 之间的数字开始。所有号码均为 14 位。还有以 5 开始的 16 位 Diners Club 信用卡号码。Diners Club 与 MasterCard 之间的联营卡应视作 MasterCard 进行处理。
Discover	^6(?:011|5[0-9]{2})[0-9]{12}$	Discover 信用卡号码以 6011 或 65 开始。所有号码仅为 16 位。
JCB	^(?:2131|1800|35\d{3})\d{11}$	以 2131 或 1800 开始的 JCB 信用卡号码为 15 位。以 35 开始的 JCB 信用卡号码为 16 位。

根据上述示例，还可以为社会保险号码创建类似的正则表达式。 有关正则表达式的更多示例，请参见 http://www.regular-expressions.info/examples.html。

6 选择“正则表达式”选项并单击“保存”。

7 单击“策略管理器” | “按访问（主策略）” | “DLP 和合规性”添加到“策略管理器”中的 “DLP 和合规性”。

8 在“激活”下，选择“启用”。

9 在“DLP 和合规性规则及关联操作”下，单击“添加规则”。

10 在“选择规则组”下，选择之前在下拉列表中创建的正则表达式规则。

11 指定规则触发时要采取的操作。

12 单击“保存”。

索引

D

E

F

G

H

J

K

L

M

N

P

Q

R

S

T

V

W

X

Y

Z